

**ANEXO III – Formulário de Proposta de Preços**

RAZÃO SOCIAL: Clear Tecnologia da Informação S.A		
CNPJ: 30.088.923/0003-70	TELEFONE (S): 92 3042-0123	
E-MAIL: contratos@clearit.com.br		
ENDEREÇO: Q SIG QUADRA 1, 985, salas 256/257, Zona Industrial, Brasília - DF - CEP: 70.610-410		
BANCO: BRADESCO	AGÊNCIA: 1323	CONTA CORRENTE: 3860-1

**GRUPO 01**

ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE	VALOR UNITÁRIO (R\$)	VALOR TOTAL (R\$)
01	Licença base para habilitar os recursos de vulnerabilidade de aplicações	UN	01	R\$ 49.526,00	R\$ 49.526,00
02	10 aplicações para todos os recursos que utilizam aplicação. Requer uma licença base: aplicação	UN	04	R\$ 199.224,00	R\$ 796.896,00
03	Licença base para habilitar os recursos de ativos e vulnerabilidades de ameaças	UN	01	R\$ 11.521,00	R\$ 11.521,00
04	100 ativos para todos os recursos que utilizam ativo.	UN	06	R\$ 79.209,50	R\$ 475.257,00
05	Licença base para habilitar os recursos de ativos e vulnerabilidades de ameaças.	UN	01	R\$ 44.497,00	R\$ 44.497,00
06	1 domínio para todos os	UN	04	R\$ 8.101,75	R\$ 32.407,00

	recursos que utilizam domínio. Requer uma licença base: fraude, vazamento e/ou inteligência de ameaças.				
07	1 domínio para todos os recursos que utilizam domínio. Requer uma licença base: fraude, vazamento e/ou inteligência de ameaças.	UN	01	R\$ 59.827,00	R\$ 59.827,00
08	1 domínio para todos os recursos que utilizam domínio. Requer uma licença base: fraude, vazamento e/ou inteligência de ameaças.	UN	04	R\$ 6.848,75	R\$ 27.395,00
09	Módulo de treinamentos para os itens 01, 02, 03, 04 e 05	UN	01	R\$ 62.674,00	R\$ 62.674,00
<b>VALOR TOTAL (R\$)</b>				<b>R\$ 1.560.000,00</b>	

Valor total por extenso da Proposta de Preços: R\$ 1.560.000,00 (Um milhão, quinhentos e sessenta mil reais)

Validade da proposta: 60 (sessenta) dias.



Observação: Estão inclusos nos preços supramencionados todos os custos diretos e indiretos, inclusive de embalagens, transportes ou fretes, e ainda os resultantes da incidência de quaisquer tributos, contribuições ou obrigações decorrentes da legislação trabalhista, fiscal e previdenciária a que estiver sujeito.

Declaro que possuo capacidade operacional e técnica para atendimento a todos os requisitos deste Edital e seus anexos.

Brasília – DF, 02 de fevereiro de 2026.

---

CLEAR TECNOLOGIA DA INFORMAÇÃO S.A.

CNPJ/MF sob o nº 30.088.923/0003-70

Ricardo Cesar Dias

CEO

● **MANAUS**  
Rua Salvador, 440 - Sala 308  
Ed. Soberane - Torre Corporate  
Adrianópolis - Manaus – AM  
CEP 69057-040  
+55 (92) 3042-0123

● **BRASÍLIA**  
Centro Empresarial Parque Brasília  
SIG QUADRA 1985, Salas 256 e 257,  
Asa Sul – Brasília - DF  
CEP 70610-410  
+55 (61) 3020-2383

● **SÃO PAULO**  
Rua Mergenthaler, 625 – Sala 61 e 71  
Vila Leopoldina  
São Paulo - SP  
CEP 05311-030  
+55 (11) 4673-4999

● **SALVADOR**  
Av. Luis Viana Filho, 13223, Ed. Hangar  
Business Park – Hangar 5 – Sala 208  
São Cristovão – Salvador - BA  
CEP 41500-300  
+55 (92) 3042-0123



## PROPOSTA TÉCNICA

---

### DA GARANTIA E DO SUPORTE TÉCNICO

Conforme prescrito no Edital N° **006/2026 - TJAM**, nossa oferta contempla a garantia de 60 (sessenta) meses para os produtos apresentados nesta proposta comercial.

- E-mail para abertura de chamados (ClearIT): [pos-venda@clearit.com.br](mailto:pos-venda@clearit.com.br)
- Número para abertura de chamados (ClearIT): 0800 990 9000
- Website para abertura de chamados (ClearIT): <http://suporte.clearit.net.br/support/home>

### SERVIÇOS CORRELATOS

Declaramos que a oferta dos nossos serviços está em conformidade com os requisitos, premissas e níveis de qualidade descritos para todo escopo de serviços presentes no Termo de Referência Edital N° **006/2026 - TJAM**.

### LOCAL E PRAZO DE ENTREGA OU APLICAÇÃO

Declaramos que estamos cientes e em conformidade com os prazos e locais de entrega preconizados no Termo do Edital N° **006/2026 - TJAM**.

Declaramos que atendemos todos os itens do edital e termo de referência e seus anexos, incluindo instalação, configuração, suporte e garantia ao longo de período de contrato.

#### ● MANAUS

Rua Salvador, 440 - Sala 308 -  
Ed. Soberane - Torre Corporate  
Adrianópolis;  
Manaus - AM;  
CEP 69057-040;  
+55 (92) 3042-0123.

#### ● BRASÍLIA

Centro Empresarial Parque Brasília  
SIG QUADRA 1985, Salas 256 e 257,  
Asa Sul;  
Brasília - DF;  
CEP 70610-410;  
+55 (61) 3020-2383.

#### ● SÃO PAULO

Rua Mergenthaler, 625 - Sala 61 e 71,  
Vila Leopoldina;  
São Paulo - SP;  
CEP 05311-030;  
+55 (11) 4673-4999.

#### ● SALVADOR

Av Luis Viana Filho, 13223, Ed. Hangar  
Business Park - Hangar 5 - Sala 208,  
São Cristovão;  
Salvador - BA;  
CEP 41.500-300;  
+55 (92) 3042-0123.



## DESCRIPTIVO TÉCNICO

### Grupo 01 – Detecção e Mitigação de Vulnerabilidades em Aplicações para 12 meses

Item 01 - Licença base para habilitar os recursos de vulnerabilidade de aplicações.

**Marca:** Rainforest

**Modelo:** Rainforest Application

**Lista de Part Numbers:**

PART-NUMBER	QUANTIDADE ENTREGUE
RF-LIC-APPLICATION	01

### ITEM 02 – 10 aplicações para todos os recursos que utilizam aplicação

**Marca:** Rainforest

**Modelo:** Rainforest Application

**Lista de Part Numbers:**

PART-NUMBER	QUANTIDADE ENTREGUE
RF-ADD-APP-10	04

### Grupo 02 – Detecção e Mitigação de Vulnerabilidades em Infraestrutura para 12 meses

Item 03 - Licença base para habilitar os recursos de ativos e vulnerabilidades de ameaças.

**Marca:** Rainforest

**Modelo:** Rainforest Infra

**Lista de Part Numbers:**

PART-NUMBER	QUANTIDADE ENTREGUE
RF-LIC-INFRA	1

### ITEM 04 – 100 ativos para todos os recursos que utilizam ativo.

**Marca:** Rainforest

**Modelo:** Rainforest Infra

**Lista de Part Numbers:**

PART-NUMBER	QUANTIDADE ENTREGUE
RF-ADD-INFRA-100	6

#### ● MANAUS

Rua Salvador, 440 - Sala 308 -  
Ed. Soberane - Torre Corporate  
Adrianópolis;  
Manaus - AM;  
CEP 69057-040;  
+55 (92) 3042-0123.

#### ● BRASÍLIA

Centro Empresarial Parque Brasília  
SIG QUADRA 1985, Salas 256 e 257,  
Asa Sul;  
Brasília - DF;  
CEP 70610-410;  
+55 (61) 3020-2383.

#### ● SÃO PAULO

Rua Mergenthaler, 625 - Sala 61 e 71,  
Vila Leopoldina;  
São Paulo - SP;  
CEP 05311-030;  
+55 (11) 4673-4999.

#### ● SALVADOR

Av Luis Viana Filho, 13223, Ed. Hangar  
Business Park - Hangar 5 - Sala 208,  
São Cristovão;  
Salvador - BA;  
CEP 41.500-300;  
+55 (92) 3042-0123.



### Grupo 03 – Análise de Exposição de Credenciais para 12 meses

Item 05 - Licença base para habilitar os recursos de detecção de vazamento.

**Marca:** Rainforest

**Modelo:** Rainforest Leak

**Lista de Part Numbers:**

PART-NUMBER	QUANTIDADE ENTREGUE
RF-LIC-LEAK	1

### Grupo 04 – Detecção de Domínios Fraudulentos para 12 meses

Item 06 - 1 domínio para todos os recursos que utilizam domínio

**Marca:** Rainforest

**Modelo:** Rainforest Fraud

**Lista de Part Numbers:**

PART-NUMBER	QUANTIDADE ENTREGUE
RF-ADD-DOMAIN-1	4

### ITEM 07 – Licença base para habilitar os recursos de detecção de fraude

**Marca:** Rainforest

**Modelo:** Rainforest Fraud

**Lista de Part Numbers:**

PART-NUMBER	QUANTIDADE ENTREGUE
RF-LIC-FRAUD	1

### ITEM 08 – 5 palavras-chave para todos os recursos que utilizam palavra-chave.

**Marca:** Rainforest

**Modelo:** Rainforest Fraud

**Lista de Part Numbers:**

PART-NUMBER	QUANTIDADE ENTREGUE
RF-ADD-KEYWORD-5	4

#### ● MANAUS

Rua Salvador, 440 - Sala 308 -  
Ed. Soberane - Torre Corporate  
Adrianópolis;  
Manaus - AM;  
CEP 69057-040;  
+55 (92) 3042-0123.

#### ● BRASÍLIA

Centro Empresarial Parque Brasília  
SIG QUADRA 1985, Salas 256 e 257,  
Asa Sul;  
Brasília - DF;  
CEP 70610-410;  
+55 (61) 3020-2383.

#### ● SÃO PAULO

Rua Mergenthaler, 625 - Sala 61 e 71,  
Vila Leopoldina;  
São Paulo - SP;  
CEP 05311-030;  
+55 (11) 4673-4999.

#### ● SALVADOR

Av Luis Viana Filho, 13223, Ed. Hangar  
Business Park - Hangar 5 - Sala 208,  
São Cristovão;  
Salvador - BA;  
CEP 41.500-300;  
+55 (92) 3042-0123.



## Grupo 05 – Módulo de treinamentos

Item 09 - Módulo de treinamento para os grupos 01, 02, 03 e 04

**Marca:** Rainforest

**Modelo:** Rainforest Training

### Lista de Part Numbers:

PART-NUMBER	QUANTIDADE ENTREGUE
RF-SVC-8H	3

#### ● MANAUS

Rua Salvador, 440 - Sala 308 -  
Ed. Soberane - Torre Corporate  
Adrianópolis;  
Manaus - AM;  
CEP 69057-040;  
+55 (92) 3042-0123.

#### ● BRASÍLIA

Centro Empresarial Parque Brasília  
SIG QUADRA 1985, Salas 256 e 257,  
Asa Sul;  
Brasília - DF;  
CEP 70610-410;  
+55 (61) 3020-2383.

#### ● SÃO PAULO

Rua Mergenthaler, 625 - Sala 61 e 71,  
Vila Leopoldina;  
São Paulo - SP;  
CEP 05311-030;  
+55 (11) 4673-4999.

#### ● SALVADOR

Av Luis Viana Filho, 13223, Ed. Hangar  
Business Park - Hangar 5 - Sala 208,  
São Cristovão;  
Salvador - BA;  
CEP 41.500-300;  
+55 (92) 3042-0123.

## COMPROVAÇÃO TÉCNICA

Código	Descrição	Página do Manual Rainrorest.PDF de Comprovação
<b>Descrição Geral da Contratação</b>		
1.2.3.1	Fortalecimento da Postura de Segurança Cibernética: o TJAM passará a contar com um nível elevado de maturidade em segurança da informação, sustentado por uma solução integrada que permitirá a análise contínua de vulnerabilidades em aplicações, infraestrutura e ambientes de desenvolvimento, proporcionando visão centralizada e resposta proativa a incidentes	163
1.2.3.2	Integração com Práticas DevSecOps: os pipelines de desenvolvimento (CI/CD) estarão plenamente integrados a controles automatizados de segurança, permitindo que vulnerabilidades sejam identificadas e tratadas antes da publicação de novos sistemas ou atualizações, reduzindo significativamente o risco de exposição a ataques cibernéticos.	152
1.2.3.3	Mitigação de Riscos de Vazamento de Dados e Fraudes Digitais: o Tribunal contará com mecanismos permanentes de monitoramento de credenciais, detecção de domínios fraudulentos e proteção de marca em ambientes como surface, deep e dark web, prevenindo fraudes, clonagem de domínios e uso indevido da identidade institucional.	139
1.2.3.4	Automação na Gestão de Vulnerabilidades: a gestão de vulnerabilidades será marcada por alta automação, permitindo a priorização de riscos, a classificação de vulnerabilidades e a geração de recomendações de correção com maior agilidade e eficiência das equipes técnicas.	149
1.3.1	A justifica para o quantitativo a ser adquirido encontra-se no Estudo Técnico Preliminar, anexo a este termo.	
<b>1.3.2</b>	<b>GRUPO 01 - Detecção e Mitigação de Vulnerabilidades em Aplicações</b>	
1.3.2.1	A solução deve permitir análise de até 10 aplicações em desenvolvimento e/ou já existentes no ambiente de produção do TJAM.	145
1.3.2.2	Toda a análise de códigos fonte deverá ocorrer dentro do perímetro de segurança do TJAM e/ou fábrica de software onde a aplicação esteja sendo desenvolvida, de acordo com as políticas de segurança definidas pelo TJAM,	146
1.3.2.3	Para fins de análise do código-fonte, não deverá ser realizado envio (upload) para a nuvem da CONTRATADA ou de terceiros.	146
1.3.2.4	Deve ser compatível com protocolo Git com o objetivo de se conectar no repositório de código-fonte do TJAM.	137
1.3.2.5	A solução deverá ser apta e ter opção de contexto, e permitir que a CONTRATADA clique e armazene pequenos trechos de código-fonte a fim de	130

### ● MANAUS

Rua Salvador, 440 - Sala 308 -  
Ed. Soberane - Torre Corporate  
Adrianópolis;  
Manaus - AM;  
CEP 69057-040;  
+55 (92) 3042-0123.

### ● BRASÍLIA

Centro Empresarial Parque Brasília  
SIG QUADRA 1985, Salas 256 e 257,  
Asa Sul;  
Brasília - DF;  
CEP 70610-410;  
+55 (61) 3020-2383.

### ● SÃO PAULO

Rua Mergenthaler, 625 - Sala 61 e 71,  
Vila Leopoldina;  
São Paulo - SP;  
CEP 05311-030;  
+55 (11) 4673-4999.

### ● SALVADOR

Av Luis Viana Filho, 13223, Ed. Hangar  
Business Park - Hangar 5 - Sala 208,  
São Cristovão;  
Salvador - BA;  
CEP 41.500-300;  
+55 (92) 3042-0123.

	permitir ao desenvolvedor que identifique rapidamente o contexto em que a vulnerabilidade foi detectada.	
1.3.2.6	A solução deve permitir a integração direta (plug and play) com repositório de código-fonte (Git) e repositório de imagens (Docker) interdependente da esteira DevOps de desenvolvimento (Jenkins, Gitlab, Azure DevOps	137
1.3.2.7	A solução deve permitir, quando necessário, bloqueio de esteira para que a aplicação não siga em frente para produção (funcionalidade conhecida como gatekeeper), no mínimo nos seguintes cenários:	152
1.3.2.7	Bloquear a esteira caso seja detectado que a aplicação ou imagem foi gerada a partir de um código que não atendeu as etapas obrigatórias do processo de análise de segurança, garantindo a conformidade com as políticas de governança estabelecidas	152
1.3.2.7.2	Quando houver alguma vulnerabilidade considerada alta ou crítica não tratada.	152
1.3.2.7.3	Quando houver código sensível identificado na análise de código-fonte com objetivo de detectar e alertar sobre melhorias de qualidade de código.	152
1.3.2.8	A solução deve possuir funcionalidade para análise de código e detectar e alertar sobre vulnerabilidades de segurança (SAST – Static Application Security Testing).	145
1.3.2.9	A solução deve possuir funcionalidade para análise de segurança de terceiros (SCA – Software Composition Analysis).	145
1.3.2.10	A solução deve possuir funcionalidade para varredura de vulnerabilidades dinâmicas na aplicação (DAST – Dynamic Application Security Testing).	145
1.3.2.11	A solução deve possuir funcionalidade para varredura em containers, Docker, para detectar vulnerabilidades de segurança.	145
1.3.2.12	A solução deve possuir funcionalidade para análise de vulnerabilidades em aplicações móveis (MAST – Mobile Application Security Testing).	145
1.3.2.13	A solução deve possuir funcionalidade para análise de segurança em infraestrutura como código (IaC – Infrastructure as Code), por exemplo, Ansible e Terraform.	145
1.3.2.14	A solução deve ter capacidade de identificação de vulnerabilidades do OWASP TOP10.	141
1.3.2.15	A solução deve possuir funcionalidades para análise de código com recomendações de melhoria de qualidade.	145
1.3.2.16	A solução deverá fornecer recomendações para correções (utilizando a base de conhecimentos da própria plataforma ou implementando funcionalidades de inteligência artificial para apresentar tais recomendações).	129 / 130
1.3.2.17	A solução deve gerar alertas de vulnerabilidades via plataforma: e-mail, Telegram e/ou Slack.	165
1.3.2.18	A solução deve possuir painel (dashboard) que apresente o nível de risco de código-fonte e infraestrutura por criticidade.	117

● **MANAUS**

Rua Salvador, 440 - Sala 308 -  
Ed. Soberane - Torre Corporate  
Adrianópolis;  
Manaus - AM;  
CEP 69057-040;  
+55 (92) 3042-0123.

● **BRASÍLIA**

Centro Empresarial Parque Brasília  
SIG QUADRA 1985, Salas 256 e 257,  
Asa Sul;  
Brasília - DF;  
CEP 70610-410;  
+55 (61) 3020-2383.

● **SÃO PAULO**

Rua Mergenthaler, 625 - Sala 61 e 71,  
Vila Leopoldina;  
São Paulo - SP;  
CEP 05311-030;  
+55 (11) 4673-4999.

● **SALVADOR**

Av Luis Viana Filho, 13223, Ed. Hangar  
Business Park - Hangar 5 - Sala 208,  
São Cristovão;  
Salvador - BA;  
CEP 41.500-300;  
+55 (92) 3042-0123.

1.3.2.19	Deve apresentar painel (dashboard) do ciclo DevSecOps com painel de vulnerabilidades por etapa, com no mínimo as etapas “Quality”, “SAST”, “SCA”, “DAST”, “Image”, “MAST” e “IaC”.	169
1.3.2.20	A solução deve possuir funcionalidade para classificar as vulnerabilidades como falso-positivo, a priorizar ou mitigado em outro ambiente.	102
1.3.2.21	A solução deve permitir análise contínua, bastante a atualização do código pelo desenvolvedor, para que a plataforma inicie a análise de código.	152
1.3.2.22	A solução deve permitir o cadastro manual de vulnerabilidades.	97
1.3.2.23	A solução deve disponibilizar uma extensão (plugin) que permita acompanhar os achados de vulnerabilidade em ambiente de desenvolvimento integrado (Integrated Development Environment – IDE) suportando soluções como Microsoft Visual Studio Code.	85
<b>1.3.3</b>	<b>GRUPO 02 Detecção e Mitigação de Vulnerabilidades em Infraestrutura</b>	
1.3.3.1	A Solução deve analisar até 500 dispositivos da infraestrutura do TJAM a serem definidos pela SETIC.	74
1.3.3.2	Deve possibilitar o cadastro manual de redes e ativos de redes individuais, com cadastro do endereço IP, departamento, localização geográfica, nome e descrição do ativo.	62
1.3.3.3	Deve conter um cadastro manual de tecnologias instaladas em um ativo no inventário, com no mínimo informações como: fabricante, produto e versão.	59
1.3.3.4	Deve contar com funcionalidade própria de inventário automatizado dos ativos do ambiente, com suporte a inventário usando credenciais de acesso aos ativos.	50
1.3.3.5	Deve ser capaz de identificar ativos existentes em uma faixa (range) de rede e cadastrá-los na plataforma aos poucos.	51
1.3.3.6	Deve ser capaz de autenticar nos ativos encontrados e realizar o inventário automatizado de todas as tecnologias instaladas em cada um dos equipamentos servidores e estações de trabalho do escopo.	55
1.3.3.7	Deve reconhecer e inventariar tecnologias, como Java, Bancos de dados (SQL Server, MySQL, MariaDB, Oracle), Sistemas operacionais (Windows, Linux, MacOS, IOS, Android), Ferramentas de usuários (Pacotes Office, VSCode, Adobe Acrobat e Acrobat Reader).	59
1.3.3.8	Deve ser capaz de realizar varreduras de vulnerabilidades dos ativos identificados através do inventário, em períodos definidos no próprio sistema.	39
1.3.3.9	Deve possuir opção para iniciar varredura de vulnerabilidades via agendamento.	39 / 40
1.3.3.10	Deve permitir que sejam definidos janelas para execução das varreduras com o objetivo de limitar a data e horário de início e final das análises que serão realizadas no ativo.	39
1.3.3.11	Todas as vulnerabilidades detectadas pela análise de vulnerabilidades devem ser armazenadas pela plataforma para gestão.	55

● **MANAUS**

Rua Salvador, 440 - Sala 308 - Ed. Soberane - Torre Corporate Adrianópolis; Manaus - AM; CEP 69057-040; +55 (92) 3042-0123.

● **BRASÍLIA**

Centro Empresarial Parque Brasília SIG QUADRA 1985, Salas 256 e 257, Asa Sul; Brasília - DF; CEP 70610-410; +55 (61) 3020-2383.

● **SÃO PAULO**

Rua Mergenthaler, 625 - Sala 61 e 71, Vila Leopoldina; São Paulo - SP; CEP 05311-030; +55 (11) 4673-4999.

● **SALVADOR**

Av Luis Viana Filho, 13223, Ed. Hangar Business Park - Hangar 5 - Sala 208, São Cristovão; Salvador - BA; CEP 41.500-300; +55 (92) 3042-0123.

1.3.3.12	Armazenar, também, todas as vulnerabilidades vinculadas a uma determinada tecnologia já lida.	55
1.3.3.13	Deve ser capaz de identificar novas vulnerabilidades nos ativos inventariados, sem execução de varreduras e sem geração de tráfego baseando-se nas tecnologias do ativo.	74
1.3.3.14	A solução deve gerar alertas de vulnerabilidades via plataforma: e-mail, Telegram e/ou Slack.	165
1.3.3.15	Deve contar com opções de notificação, para que o gestor possa selecionar quais as suas preferências para recebimento de alertas.	165 / 166
1.3.3.16	Deve ser capaz de integrar com ferramentas de Endpoint Detection and Response (EDR).	36
1.3.3.17	Deve permitir a configuração do período, em dias, que um dispositivo será automaticamente descomissionado se permanecer inativo (sem análise de vulnerabilidade ou descoberta), ou seja, removido do inventário de dispositivos da plataforma a fim de sanitizá-la.	32
1.3.3.18	Deve permitir que este seja a quantidade de dias seja configurada especificamente por técnica de descoberta do ativo, por exemplo, aqueles que foram identificados por análise de vulnerabilidade (X dias) ou através da integração com EDR (Y dias).	33
1.3.3.19	Possibilitar a configuração de janelas (períodos) onde a análise de infraestrutura poderá ser executada. Caso a análise de vulnerabilidade ultrapasse a janela configurada, a plataforma deverá pausar a análise e retomá-la assim que possível (próxima janela de execução).	40
1.3.4	<b>ITEM 03 – Análise de Exposição Dados e Credenciais</b>	
1.3.4.1	A Solução deve detectar vazamentos de informações sensíveis do TJAM com base em definições de um domínio e até 05 palavras-chave a serem definidas pelo TJAM;	26
1.3.4.2	Detectar vazamento de credenciais com base nos domínios e palavras-chave a serem definidas em conjunto pelo TJAM e CONTRATADA.	13 / 23
1.3.4.3	Deve realizar busca em múltiplas fontes que monitorem surface, deep e/ou dark web.	23 / 26
1.3.4.4	Deve realizar a classificação das credenciais que foram descobertas, incluindo aquelas que são diretamente de servidores do TJAM, mas também aquelas que são de clientes/usuários do TRIBUNAL, ou seja, usuários que utilizam serviços do TJAM.	24
1.3.4.5	Deve implementar formas automatizadas para a classificação dos itens que foram identificados reduzindo, sempre que possível, o esforço da análise / categorização manual.	101
1.3.4.6	Deve permitir, de forma macro, visualizar e correlacionar as credenciais das listas de registros encontradas a fim de evitar que os mesmos registros que foram identificados sejam expostos.	24
1.3.4.7	Deve implementar monitoramento de grupos de Telegram, onde são divulgadas informações dessa natureza.	15

● **MANAUS**

Rua Salvador, 440 - Sala 308 -  
Ed. Soberane - Torre Corporate  
Adrianópolis;  
Manaus - AM;  
CEP 69057-040;  
+55 (92) 3042-0123.

● **BRASÍLIA**

Centro Empresarial Parque Brasília  
SIG QUADRA 1985, Salas 256 e 257,  
Asa Sul;  
Brasília - DF;  
CEP 70610-410;  
+55 (61) 3020-2383.

● **SÃO PAULO**

Rua Mergenthaler, 625 - Sala 61 e 71,  
Vila Leopoldina;  
São Paulo - SP;  
CEP 05311-030;  
+55 (11) 4673-4999.

● **SALVADOR**

Av Luis Viana Filho, 13223, Ed. Hangar  
Business Park - Hangar 5 - Sala 208,  
São Cristovão;  
Salvador - BA;  
CEP 41.500-300;  
+55 (92) 3042-0123.

1.3.4.8	As credenciais identificadas devem sempre que possível conter as seguintes informações: Classificação do vazamento, usuário (e-mail vazado), senha (password), alvo do acesso (site, URL, etc), descrição, data de vazamento e data da descoberta do vazamento.	25
1.3.4.9	Detectar vazamento de códigos-fonte de aplicações de desenvolvimento interno, com base em palavras-chave a serem definidas em conjunto pelo TJAM e CONTRATADA.	13
1.3.4.10	Deve verificar repositórios de códigos-fonte públicos como, por exemplo, GitHub, Gitlab, Postman e endereços de armazenamento de texto como, por exemplo, o site Pastebin com o objetivo de detectar compartilhamento indevido de informações corporativas.	140 / 141
1.3.4.11	Detectar referências (links) para os domínios e/ou palavras-chave que sinalizem uma possibilidade de vazamentos de documentos ou serviços do TJAM.	12
1.3.4.12	A solução deve possuir painéis que apresentem de forma consolidada um resumo do status atual da análise com base em classificações, indicando a evolução da análise dos achados, ou seja, quantos estão em análise e quantos foram fechados ou resolvidos.	139
1.3.4.13	Para as funcionalidades de monitoramento de fraude e vazamento de informação que permitam a classificação das informações identificadas pelo sistema, deve possibilitar a classificação de um item identificado, pelo menos, como:	101
1.3.4.13.1	sob análise, para itens que foram encontrados e precisam ser verificados;	101
1.3.4.13.2	confiável ou resolvido, para itens que foram encontrados, mas são confiáveis ou já foram resolvidos;	101
1.3.4.13.3	irrelevante, para itens que foram encontrados e não representam risco ou fraude.	101
1.3.4.14	Possibilidade de personalizar quais colunas serão exibidas e em qual ordem serão exibidas.	9
1.3.4.15	Possibilidade de exportar as informações da tabela que são apresentadas na tela para valores separados por vírgulas ou ponto e vírgula (CSV – comma separated values).	9
<b>1.3.5</b>	<b>GRUPO 04 – Detecção de Domínios Fraudulentos</b>	
1.3.5.1	A Solução deverá realizar as análises de Fraudes Web com base em definições de um domínio e até 05 palavras-chave a serem definidas pelo TJAM;	158
1.3.5.2	Deve realizar monitoramento de nomes de domínio cadastrados na Internet, para identificar nomes semelhantes aos domínios monitorados (tipo de ataque também conhecido como cybersquatting).	158
1.3.5.3	Deve detectar possíveis domínios fraudulentos e permitir a notificação através da própria plataforma, e-mail, Telegram e/ou Slack.	165
1.3.5.4	Deve, sempre que possível, fornecer uma foto (screenshot) da tela (homepage) do possível domínio fraudulento.	155

● **MANAUS**

Rua Salvador, 440 - Sala 308 -  
Ed. Soberane - Torre Corporate  
Adrianópolis;  
Manaus - AM;  
CEP 69057-040;  
+55 (92) 3042-0123.

● **BRASÍLIA**

Centro Empresarial Parque Brasília  
SIG QUADRA 1985, Salas 256 e 257,  
Asa Sul;  
Brasília - DF;  
CEP 70610-410;  
+55 (61) 3020-2383.

● **SÃO PAULO**

Rua Mergenthaler, 625 - Sala 61 e 71,  
Vila Leopoldina;  
São Paulo - SP;  
CEP 05311-030;  
+55 (11) 4673-4999.

● **SALVADOR**

Av Luis Viana Filho, 13223, Ed. Hangar  
Business Park - Hangar 5 - Sala 208,  
São Cristovão;  
Salvador - BA;  
CEP 41.500-300;  
+55 (92) 3042-0123.

1.3.5.5	Deve, sempre que possível, fornecer informações de cadastro do domínio (whois).	154
1.3.5.6	Utilizar de múltiplas inteligências (por exemplo: algoritmos de registro) para descoberta de possíveis domínios fraudulentos.	153
1.3.5.7	Consultar, no ato do registro, a legitimidade do domínio.	153
1.3.5.8	Apresentar uma pontuação (score) indicando a probabilidade de o IP para qual o domínio aponta ser utilizado para fraude, com o objetivo de possibilitar a priorização de ações.	154
1.3.5.9	Deve apresentar se o site em questão tiver selo seguro (HTTPS), qual a data de expiração do certificado SSL.	157
1.3.5.10	A funcionalidade de proteção de aplicações móveis deve ser capaz de permitir o cadastro de palavras-chave e nomes de aplicativos móveis (apps) que o TJAM tenha atualmente ou venha a ter para monitoramento.	158 / 159
1.3.5.11	Deve monitorar lojas de aplicativos (marketplaces) oficiais e não-oficiais, como Google Play, Apple Store e Aptoide, para detectar aplicativos que possam utilizar o nome do TJAM com objetivo de realizar fraudes.	148
1.3.5.12	Deve detectar possíveis aplicativos móveis falsos com o nome do TJAM, através da plataforma: e-mail, Telegram e/ou Slack.	148 / 165
1.3.5.13	A plataforma deverá executar o monitoramento periódico de tais informações de forma automatizada.	158
1.3.5.14	A funcionalidade de redes sociais (social networks) deve possibilitar o monitoramento de redes sociais com objetivo de identificar usuários, páginas e postagens (posts) que façam referência às palavras-chave que são monitoradas.	144
1.3.5.15	A solução deve realizar buscas, no mínimo nas seguintes redes sociais: Facebook, Instagram, TikTok, X (Twitter) e YouTube, trazendo informações que estejam disponíveis como “likes”, “comments”, “shares”, “posts”, “followers”, “following”.	144
1.3.5.16	Possibilidade de adicionar o usuário na lista de usuários permitidos (“add user to whitelist”) com o objetivo que todas as publicações do usuário já sejam automaticamente classificadas como permitidas (whitelisted).	159
1.3.5.17	A plataforma deverá executar o monitoramento periódico de redes sociais de forma automatizada.	158
1.3.5.18	A funcionalidade de web de superfície ou conteúdo indexado (surface web) deve possibilitar o monitoramento de conteúdos que estejam indexados em buscadores como, por exemplo, Google, repositórios de objetos ou arquivos (buckets AWS S3, por exemplo) e blogs.	12 / 142
1.3.5.19	Tal funcionalidade tem como objetivo identificar itens que não em categorias referenciadas anteriormente, contudo mesmo assim representem potencial risco de fraude ao TJAM.	142
1.3.5.20	Deve possibilitar a criação de marcação ou posicionamento específico, no momento da análise de páginas de fraudes que copie o conteúdo do TJAM ou conduta de redirecionamento da página e/ou que fazem referência a ela.	101 / 102

● **MANAUS**

Rua Salvador, 440 - Sala 308 -  
Ed. Soberane - Torre Corporate  
Adrianópolis;  
Manaus - AM;  
CEP 69057-040;  
+55 (92) 3042-0123.

● **BRASÍLIA**

Centro Empresarial Parque Brasília  
SIG QUADRA 1985, Salas 256 e 257,  
Asa Sul;  
Brasília - DF;  
CEP 70610-410;  
+55 (61) 3020-2383.

● **SÃO PAULO**

Rua Mergenthaler, 625 - Sala 61 e 71,  
Vila Leopoldina;  
São Paulo - SP;  
CEP 05311-030;  
+55 (11) 4673-4999.

● **SALVADOR**

Av Luis Viana Filho, 13223, Ed. Hangar  
Business Park - Hangar 5 - Sala 208,  
São Cristovão;  
Salvador - BA;  
CEP 41.500-300;  
+55 (92) 3042-0123.

1.3.5.21	Tal funcionalidade tem como objetivo reduzir o tempo de identificação de páginas falsas que são utilizadas pelos fraudadores.	101 / 102
1.3.5.22	A solução deve possuir dashboards que apresentem de forma consolidada um resumo do status atual da análise dos achados, ou seja, quantos estão em análise e quantos foram fechados ou resolvidos.	139
1.3.5.23	Para as funcionalidades de monitoramento de fraude e vazamento de informação que permitam a classificação das informações identificadas pelo sistema, deve possibilitar a classificação de um item identificado, pelo menos, como:	101
1.3.5.23.1	sob análise (under analysis), para itens que foram encontrados e precisam ser verificados;	101
1.3.5.23.2	confiável (trusted) ou resolvido (solved), para itens que foram encontrados, mas são confiáveis ou já foram resolvidos;	101
1.3.5.23.3	irrelevante (irrelevant), para itens que foram encontrados e não representam risco ou fraude.	101
1.3.5.24	Possibilidade de personalizar quais colunas serão exibidas e em qual ordem serão exibidas.	9
1.3.5.25	Possibilidade de exportar as informações da tabela que são apresentadas na tela para valores separados por vírgulas ou ponto e vírgula (CSV – comma separated values).	9 / 10
<b>1.3.6</b>	<b>Especificação técnica comum aos GRUPOS 01, 02, 03 e 04</b>	
1.3.6.1	Contratação de solução de segurança no modelo híbrido (parte SaaS (Software as a Service) e parte on-premise capaz de realizar análise, monitoramento e acompanhamento de parâmetros de segurança no processo de gestão de vulnerabilidade desde o desenvolvimento de software até a proteção da marca (reputação) do TJAM.	161 - 163
1.3.6.2	A solução contratada deverá atender, diretamente ou em composição, aos seguintes requisitos desta contratação:	
1.3.6.2.1	No caso de composição de soluções e necessidade de integração, a CONTRATADA fornecerá ao TJAM um painel único, seguro, com uma única autenticação que mostre as informações de vulnerabilidades e proteção de reputação centralizadas.	163
1.3.6.2.2	A solução deverá mostrar e possibilitar a integração de funcionalidades de vulnerabilidade incluindo infraestrutura, desenvolvimento seguro (DevSecOps) e proteção de reputação.	163
1.3.6.3	A solução deve contar com uma interface web intuitiva para acesso às funcionalidades.	5 - 10 / 131 - 134
1.3.6.3.1	A plataforma deverá atender os módulos dos GRUPOS 01, 02, 03 e 04.	4
1.3.6.4	Implementar controle de acesso baseado em permissões de usuários para as funcionalidades da solução.	115
1.3.6.5	Deverá conter, pelo menos, três papéis (funções) de usuário pré-definidas: administrador, operador e visualizador. Cada nível restringirá as configurações e ações que o usuário poderá realizar em cada um dos módulos da solução.	115 - 116

● **MANAUS**

Rua Salvador, 440 - Sala 308 - Ed. Soberane - Torre Corporate Adrianópolis; Manaus - AM; CEP 69057-040; +55 (92) 3042-0123.

● **BRASÍLIA**

Centro Empresarial Parque Brasília SIG QUADRA 1985, Salas 256 e 257, Asa Sul; Brasília - DF; CEP 70610-410; +55 (61) 3020-2383.

● **SÃO PAULO**

Rua Mergenthaler, 625 - Sala 61 e 71, Vila Leopoldina; São Paulo - SP; CEP 05311-030; +55 (11) 4673-4999.

● **SALVADOR**

Av Luis Viana Filho, 13223, Ed. Hangar Business Park - Hangar 5 - Sala 208, São Cristovão; Salvador - BA; CEP 41.500-300; +55 (92) 3042-0123.

1.3.6.6	Possibilidade de configurar um segundo fator de autenticação (2FA) com base em códigos baseados em chaves digitais (soft tokens) através de aplicativos como: Microsoft Authenticator e Google Authenticator.	105
1.3.6.7	Possibilidade de configurar o segundo fator de autenticação (2FA) como obrigatório para todos os usuários que utilizam a plataforma; ou	105
1.3.6.7.1	Possibilidade de configurar o segundo fator de autenticação como não obrigatório, podendo individual ape-nas para alguns usuários que utilizam a plataforma.	107
1.3.6.8	Possibilidade de configurar Single Sign On (SSO) para autenticação através de identidade federada com, no mínimo, as seguintes soluções:	4
1.3.6.8.1	Microsoft Active Directory Federation Services (ADFS)	87
1.3.6.8.2	Okta	76
1.3.6.9	Possibilidade de escolher o idioma de interface suportando, no mínimo, 2 idiomas: português e inglês.	72
1.3.6.9.1	Deve permitir que o usuário selecione um idioma padrão que já esteja salvo toda vez que ele abrir a solução.	72
1.3.6.10	Deve possuir uma área de consulta (referência rápida) onde o usuário realizará uma busca que inclua, no mínimo, as seguintes informações:	4
1.3.6.10.1	Sobre CVE (Common Vulnerabilities and Exposures): apresentar informações gerais sobre a vulnerabilidade como, por exemplo, pontuação (score), vetor de ataque (attack vector), referências externas, deverá manter-se atualizada sobre tendências, dispositivos e aplicações que são afetadas, além de exploits que já estejam disponíveis para explorar tal vulnerabilidade.	65
1.3.6.10.2	Sobre TTP (Tactics, Techniques and Procedures): referência geral à estrutura (framework) do MITRE ATT&CK sobre técnicas, táticas e procedimentos de atacantes para facilitar a consulta na solução sem que seja necessário visitar site externo.	56
1.3.6.11	Deve disponibilizar API (Application Programming Interface) para permitir integração com outras soluções do ambiente do TJAM podendo consumir os dados gerados pela plataforma.	47
1.3.6.12	Deve permitir a realização de ações em lote para a classificação dos achados da plataforma, possibilitando:	101
1.3.6.12.1	Seleção de múltiplos itens para classificação.	103
1.3.6.12.2	Seleção de múltiplos itens para edição de severidade, que se estenda para um ação possível da plataforma.	103
1.3.6.12.3	Incluir comentários em achados, sempre que possível.	11
1.3.6.12.4	Seleção de múltiplos itens para ações, sempre que se tratar de uma ação possível da plataforma.	103
1.3.6.13	Deve possibilitar a adição e visualização de comentários de atividade nos achados para que seja possível rastreabilidade e trabalho colaborativo entre os usuários da plataforma.	11
1.3.7	Especificação técnica comum aos GRUPOS 01 e 02.	

● **MANAUS**

Rua Salvador, 440 - Sala 308 -  
Ed. Soberane - Torre Corporate  
Adrianópolis;  
Manaus - AM;  
CEP 69057-040;  
+55 (92) 3042-0123.

● **BRASÍLIA**

Centro Empresarial Parque Brasília  
SIG QUADRA 1985, Salas 256 e 257,  
Asa Sul;  
Brasília - DF;  
CEP 70610-410;  
+55 (61) 3020-2383.

● **SÃO PAULO**

Rua Mergenthaler, 625 - Sala 61 e 71,  
Vila Leopoldina;  
São Paulo - SP;  
CEP 05311-030;  
+55 (11) 4673-4999.

● **SALVADOR**

Av Luis Viana Filho, 13223, Ed. Hangar  
Business Park - Hangar 5 - Sala 208,  
São Cristóvão;  
Salvador - BA;  
CEP 41.500-300;  
+55 (92) 3042-0123.

1.3.7.1	A solução deve implementar tecnologia para análise dos códigos-fonte, através de concentradores de análise que deverão ser instalados dentro da infraestrutura (on-premises ou cloud) do TJAM de forma centralizada utilizando recursos de máquinas virtuais do próprio TJAM.	41
1.3.7.2	Entende-se por forma centralizada, não ser necessária a instalação em cada equipamento do desenvolvedor e/ou servidor de repositório de código-fonte.	35
1.3.7.3	Os concentradores de análise deverão ser compatíveis, no mínimo, com as seguintes versões de Sistema Operacional:	
1.3.7.3.1	Ubuntu 18.04.6 LTS (Bionic), 20.04.2 LTS (Focal) e 22.04.5 (Jammy Jellyfish).	34
1.3.7.4	Todas as credenciais que forem cadastradas na plataforma para acesso aos serviços do TJAM deverão ser armazenadas de forma segura garantindo que, uma vez cadastradas pelo TJAM, não sejam exibidas novamente na interface web em texto claro.	29
1.3.7.5	Todo tráfego de informação como credenciais, descobertas de vulnerabilidades ou outros tipos de comunicação entre a plataforma e os concentradores de análise deverá ser realizado através de protocolo seguro usando criptografia.	35
1.3.7.6	Sempre que houver uma nova varredura de vulnerabilidades, deverá ser atualizada a lista de vulnerabilidades ativas aquelas que não forem mais detectadas, mantendo assim as informações atualizadas.	117
1.3.7.7	Permitir a classificação dos itens de vulnerabilidade como redes, ativos, aplicações, etc através do uso de marcações conhecidas como tags ou labels a fim de organizar e agrupá-los, devendo permitir a criação e customização de novas marcações.	17
1.3.7.8	Para cada conjunto de análise que a plataforma executar, deverá fornecer painel (dashboard) com visão geral do cenário atual de vulnerabilidades, bem como sua evolução e priorização. Tal painel deverá apresentar, no mínimo, as seguintes informações:	117
1.3.7.8.1	Achados por categoria (possibilitando filtrar: baixas, médias, altas e críticas).	117 - 127
1.3.7.8.2	Total de dispositivos ou achados.	117 - 127
1.3.7.8.3	Total de vulnerabilidades.	117 - 127
1.3.7.8.4	Classificação dos achados por família.	117 - 127
1.3.7.8.5	Priorização com base na criticidade da vulnerabilidade, na probabilidade (likelihood) e ativos do ambiente do TJAM através de um gráfico que agrupe: urgente (corrigir agora), alta (corrigir depois), média (planeje corrigir) e baixa (corrigir depois de todas as outras).	117 - 127
1.3.7.8.6	Vulnerabilidades ou achados novos ou resolvidos por período.	117 - 127
1.3.7.8.7	Evolução dos achados ao longo do tempo.	117 - 127
1.3.7.8.8	Lista configurável com, por exemplo, os 10, 15, 20, 50 ou 100 ativos com mais vulnerabilidades no ambiente.	117 - 127

● **MANAUS**

Rua Salvador, 440 - Sala 308 -  
Ed. Soberane - Torre Corporate  
Adrianópolis;  
Manaus - AM;  
CEP 69057-040;  
+55 (92) 3042-0123.

● **BRASÍLIA**

Centro Empresarial Parque Brasília  
SIG QUADRA 1985, Salas 256 e 257,  
Asa Sul;  
Brasília - DF;  
CEP 70610-410;  
+55 (61) 3020-2383.

● **SÃO PAULO**

Rua Mergenthaler, 625 - Sala 61 e 71,  
Vila Leopoldina;  
São Paulo - SP;  
CEP 05311-030;  
+55 (11) 4673-4999.

● **SALVADOR**

Av Luis Viana Filho, 13223, Ed. Hangar  
Business Park - Hangar 5 - Sala 208,  
São Cristovão;  
Salvador - BA;  
CEP 41.500-300;  
+55 (92) 3042-0123.

1.3.7.9	Para cada conjunto de análise que a plataforma executar, deverá fornecer uma visualização em lista de itens que ao clicar permite entender quais vulnerabilidades estão associadas com aquele dispositivo ou aplicação.	66 - 67
1.3.7.10	Tais vulnerabilidades ou achados deverão ser agrupados, no mínimo, pelos seguintes critérios: abertos, mitigados, transferidos, fechados, não aplicáveis ao ambiente do TJAM (falso-positivos) ou removidos por automação da plataforma (descomissionados).	102
1.3.7.11	Deve permitir filtrar as informações das vulnerabilidades com base nas seguintes informações:	117 - 120
1.3.7.11.1	Severidade (crítica, alta, média e baixa).	117 - 120
1.3.7.11.2	Família.	117 - 120
1.3.7.11.3	Tecnologia.	117 - 120
1.3.7.11.4	Status do achado (aberto, mitigado, transferido, fechado, falso-positivo e descomissionados).	117 - 120
1.3.7.11.5	Nome do achado/vulnerabilidade.	117 - 120
1.3.7.11.6	CVSS (pontuação da família ou conformidade).	117 - 120
1.3.7.11.7	Marcações (Tags ou Labels).	117 - 120
1.3.7.11.8	Datas: item criado, item em reanálise e/ou reintervenção e/ou intervenção e data que foi fechado.	117 - 120
1.3.7.12	Deve possibilitar a exportação das informações apresentadas na plataforma (com base nos filtros aplicados) para valores separados por vírgulas ou ponto e vírgula (CSV – comma separated values).	9 - 10
1.3.8	ITEM 05 – Módulo de Treinamento nos GRUPOS 01, 02, 03 e 04	
1.3.8.1	Será necessário treinamento à equipe que atuará com a solução. O TJAM irá definir a qual item deste objeto o módulo de treinamento irá abranger	De acordo
1.3.8.2	O módulo de treinamento deverá ser de no mínimo 8 horas de duração, podendo ser dividi-do em 4 horas diárias.	De acordo
1.3.8.3	Poderá ser realizado de forma presencial, na estrutura do TJAM, ou remoto, a ser definido pelo TJAM.	De acordo
1.3.8.4	Deverá possuir uma turma de até 10 participantes, a serem definidos pelo TJAM.	De acordo
1.3.8.5	O conteúdo do módulo de treinamento deverá abranger toda a solução fornecida no item a ser definido pelo TJAM, esclarecendo a arquitetura e configurações executadas.	De acordo
1.3.8.6	Os instrutores deverão possuir experiência e certificação na área de segurança da informação.	De acordo

● **MANAUS**

Rua Salvador, 440 - Sala 308 - Ed. Soberane - Torre Corporate Adrianópolis; Manaus - AM; CEP 69057-040; +55 (92) 3042-0123.

● **BRASÍLIA**

Centro Empresarial Parque Brasília SIG QUADRA 1985, Salas 256 e 257, Asa Sul; Brasília - DF; CEP 70610-410; +55 (61) 3020-2383.

● **SÃO PAULO**

Rua Mergenthaler, 625 - Sala 61 e 71, Vila Leopoldina; São Paulo - SP; CEP 05311-030; +55 (11) 4673-4999.

● **SALVADOR**

Av Luis Viana Filho, 13223, Ed. Hangar Business Park - Hangar 5 - Sala 208, São Cristovão; Salvador - BA; CEP 41.500-300; +55 (92) 3042-0123.

# Manual de Uso



**RAINFOREST**  
.TECH



Data do documento: Janeiro de 2026

Revisão: 2.1

## **Copyright © 2026 Rainforest Technologies LLC. Todos os direitos reservados.**

As informações contidas neste Manual de Uso são de propriedade exclusiva da **Rainforest Technologies** e estão protegidas pelas leis de direitos autorais e demais legislações aplicáveis.

Este documento, no todo ou em parte, **não pode ser reproduzido, distribuído, transmitido, armazenado em sistemas de recuperação de informações ou divulgado a terceiros**, por qualquer meio, eletrônico ou físico, sem a prévia e expressa autorização por escrito da **Rainforest Technologies**, exceto quando tal uso estiver explicitamente autorizado por contrato ou acordo vigente entre as partes.

O Cliente está autorizado a utilizar este Manual exclusivamente para fins de **operação, configuração e uso adequado da plataforma/solução fornecida pela Rainforest Technologies**, conforme os termos estabelecidos no contrato aplicável. Qualquer uso fora desse escopo é expressamente vedado.

A **Rainforest Technologies** mantém a titularidade e a propriedade intelectual integral deste Manual, incluindo, mas não se limitando a textos, descrições técnicas, fluxos operacionais, ilustrações e exemplos, excetuando-se apenas informações eventualmente fornecidas pelo Cliente e claramente identificadas como tal.

Este Manual tem como objetivo fornecer **orientações técnicas e operacionais** sobre o uso da plataforma e seus recursos. As informações aqui apresentadas possuem caráter **informativo** e podem ser alteradas a qualquer momento, sem aviso prévio, em decorrência de evoluções do produto, atualizações técnicas, melhorias funcionais ou mudanças em requisitos legais, técnicos ou de negócio.

A **Rainforest Technologies** não se responsabiliza por decisões, implementações ou ações realizadas com base exclusivamente neste Manual, sem a devida validação técnica, contratual ou operacional aplicável. Recomenda-se que quaisquer pontos críticos, dúvidas ou cenários específicos sejam previamente discutidos e formalmente validados junto à **Rainforest Technologies** ou conforme os canais oficiais de suporte.

## SUMÁRIO

Conhecendo a Plataforma Rainforest.....	5
Atividades em Achados.....	11
Encontrando Referências em Links.....	12
Vazamento de Código.....	13
Fraude em Serviços de Mensagens.....	15
Usando Labels para Classificar Redes e Ativos.....	17
Vazamento de Credenciais.....	23
Visão Geral Vazamento.....	26
Takedown.....	28
Configurando Credenciais Externas.....	29
Desativação de Ativos.....	32
Instalação de Analisadores (Agentes).....	35
Vulnerabilidades By-XDR.....	36
Janelas de Scan.....	39
Rainforest Analisadores (Agentes).....	41
Pré Requisitos de Acesso / Segurança.....	43
Configuração dos Agents.....	45
API Rainforest Plataforma.....	47
Vulnerabilidades By-VA (Vulnerability Assessment).....	50
TTP (Tactics, Techniques and Procedures).....	56
Vulnerabilidades By-Tech (Tecnologias).....	59
Cadastro de Ativos.....	62
CVE (Common Vulnerabilities and Exposures).....	65
Alterar idioma da interface.....	72
Visão Geral Infra.....	74
Configure Login Single Sign-On (SSO) com OKTA no Rainforest.....	76
Extensão Rainforest – Visual Studio Code.....	85
Configure Rainforest com SAML2 Azure.....	87
Registrar Vulnerabilidades em Aplicações.....	97
Classificação dos Itens Encontrados.....	101
Habilitar autenticação de dois fatores (2FA).....	105
Configurar usuários e permissões.....	115
Visualização das Vulnerabilidades.....	117
Entendendo descobertas.....	128

Primeiro Acesso .....	131
Opções no cadastro de uma aplicação.....	135
Quais módulos compõem a solução de Inteligência de Marca .....	139
Fontes, resultados e integrações da plataforma .....	140
Fraude na Surface Web.....	142
Fraude em Redes Sociais .....	144
Visão geral App .....	145
Fraude em Aplicativos Móveis (App) .....	148
O que é Inteligência de Vulnerabilidade.....	149
DevSecOps com Rainforest .....	150
Fraude em Domínios.....	153
Configurar a Monitoração de uma Marca .....	158
Sobre a Rainforest Technologies .....	161
Notificações na Plataforma Rainforest .....	164
Gráficos e filtros em Aplicações.....	169

# Conhecendo a Plataforma Rainforest

 [support.rainforest.tech/pt-br/kb/conhecendo-a-plataforma](https://support.rainforest.tech/pt-br/kb/conhecendo-a-plataforma)

## Conheça a estrutura da plataforma, como navegar entre os menus e módulos, realize configurações iniciais de seu usuário

Depois de ter realizado o processo de cadastrona plataforma Rainforest, os usuários podem logar-se e começar a usá-la. Através de um único login é possível ter acesso a um painel único e centralizado, mostrando informações relacionados a reputação da marca (fraudes e vazamentos), como também ter visão das vulnerabilidades que estão afetando o ambiente da empresa (cloud, infra e app.)

Antes disso é importante conhecer sua estrutura, distribuiçãodos módulos, como navegar por ela e algumas funcionalidades gerais que são comuns em determinadas telas do sistema.

### Estrutura

O Rainforest é estruturado em 4 partes principais, são elas:

- Cabeçalho
- Menu lateral esquerdo de módulos
- Centro
- Rodapé

### Cabeçalho

No cabeçalho encontramos respectivamente o botão para minimizar/maximizar o menu lateral esquerdo (1), botão home (logo Rainforest) (2) e uma sessão de configurações gerais do usuário (3).



- Para minimizar/maximizar o menu lateral esquerdo basta clicar no botão (1)
- O logo da Rainforest (2) corresponde ao botão **Home**, ou seja, se você estiver em qualquer tela do sistema, basta clica-lo que você irá para a tela inicial (**Inteligência de Marca**)

- No botão de perfil de usuário (3) você terá acesso a **configurações do perfil, atualizações** da plataforma e **Sair**
  - Em configurações você pode **mudar o tema, idioma e habilitar a autenticação de dois fatores**.
  - Em **atualizações**, fique por dentro de novas funcionalidades que são implementadas no Rainforest.
  - Caso queira deslogar do Rainforest, clique em **Sair**

## Menu Lateral

---

No menu lateral do Rainforest temos os módulos disponíveis da plataforma, como dito na sessão anterior, podemos minimizar/maximizar o menu deixando como desejado. Para visualizar as opções disponíveis em cada módulo, clique na opção desejada.

Todos os módulos (exceto **Inteligência de Marca** e **Inteligência de Vulnerabilidade**) possuem suas respectivas telas ao abri-los. Por exemplo o módulo de vazamento, possui ao abri-lo as telas **Código**, **Credenciais**, **Solicitações de Takedown**. Cada uma com suas respectivas funcionalidades.

Atualmente os módulos disponíveis são:

- [Fraude](#)
- [Vazamento](#)
- [Cloud](#)
- [Infra](#)
- [App](#)

## Painel Central

---

O centro da plataforma é onde as informações são apresentadas, como por exemplo gráficos, listagem de registros, filtros, funcionalidades, etc. Ao selecionar uma tela de um módulo, o centro atualizará para apresentar as informações/funcionalidades da opção selecionada., onde podemos ter gráficos, filtros, listagem de registros, telas de configurações, dependendo do módulo/tela selecionada. Exemplo da tela do módulo **Vazamento > Código**, onde temos uma listagem dos registros encontrados:

The screenshot displays the RAINFOREST TECH dashboard with a sidebar on the left containing navigation options like 'Surface Web', 'Solicitações de Takedown', 'Vazamento', 'Código', 'Credenciais', 'Cloud', 'Relatório', 'Infra', 'Dashboard', 'Ativos', and 'Nota da Empresa'. The main content area is titled 'Código' and shows a table of vulnerabilities categorized by status: DESCOBERTAS (46900), SOB ANÁLISE (7), CONFIÁVEL (113), IRRELEVANTE (386), TAKEDOWN (0), and TODOS (47406). The table has columns for selection, ID, Nome, Marca, Fonte, and Keyword. Below the table are pagination controls showing 20 items per page and navigation buttons for 'Primeira', 'Ant.', '1', '2', '3', '4', '5', 'Próx.', and 'Última'.

Exemplo de tela do módulo **Infra > Ativos**, onde podemos observar uma série de gráficos que trazem de forma compilada e organiza as informações do respectivo módulo junto com filtros que podem ser ajustados pelo usuário conforme a necessidade.

The screenshot shows the RAINFOREST TECH dashboard with a sidebar on the left containing navigation options like 'Brand Intelligence', 'Vulnerability Intelligence', 'Fraud', 'Leak', 'Cloud', 'Infra', 'Dashboard', 'Assets', 'Company Grade', 'Exposure', 'Vulnerability Scan', 'App', 'Reference', and 'Settings'. The main content area is titled 'Vulnerabilities' and features a risk matrix with the following data:

Critical	High	Medium	Low	Info
63 Assets, 81 Vulns	142 Assets, 222 Vulns	22 Assets, 24 Vulns	0 Assets, 0 Vulns	1 Assets, 18 Vulns

Below the matrix is a 'Likelihood by CVE' chart with a Likelihood y-axis and a Fix Later x-axis. The chart shows several data points, with a vertical line at Likelihood 7 labeled 'Plan to Fix' and a horizontal line at Fix Later 10 labeled 'Fix Now'. A 'Findings without CVE' section on the right contains the text 'Sorry, no results found'.

## Rodapé

Em qualquer tela da plataforma Rainforest teremos o rodapé do sistema, onde temos a funcionalidade de **alteração de idioma** da interface, podendo o usuário escolher entre os idiomas:

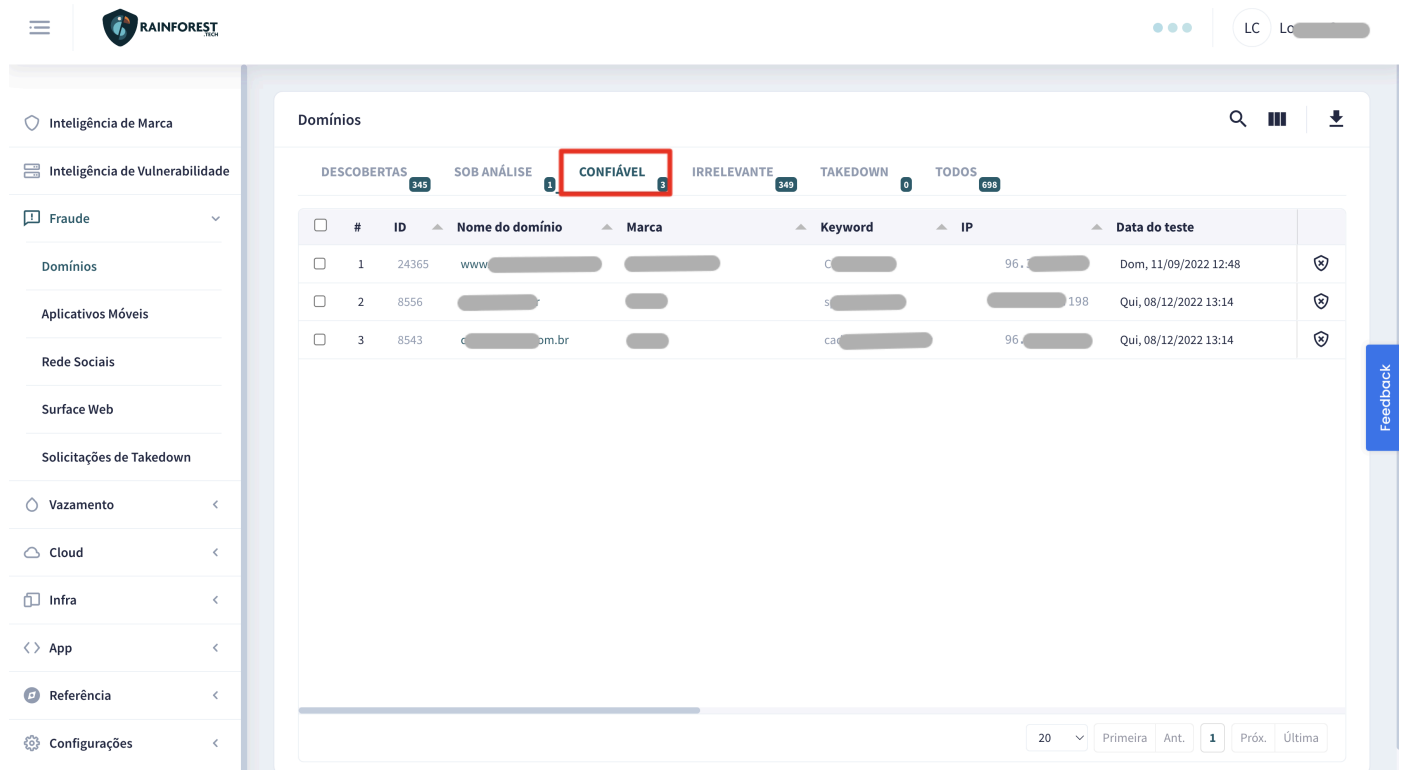
- Espanhol
- Inglês
- Português - Br

## Funcionalidades Gerais

No Rainforest há algumas funcionalidades que fazem parte de mais de um módulo do sistema, essas ferramentas ajudam o usuário na utilização da plataforma, facilitando seu trabalho, abaixo listaremos as principais.

### Classificação de registros

Em telas onde temos uma listagem de registros, temos logo acima do grid de informações as classificações, onde podemos clicar sobre uma classificação desejada que em seguida o Rainforest fará o filtro retornando somente os registros que foram classificados com a opção selecionada. No print abaixo temos o exemplo do módulo **Fraude > Domínios**, onde selecionamos a classificação **Confiável**.



The screenshot displays the Rainforest interface. On the left is a navigation menu with categories like 'Inteligência de Marca', 'Inteligência de Vulnerabilidade', 'Fraude', 'Vazamento', 'Cloud', 'Infra', 'App', 'Referência', and 'Configurações'. The main area shows the 'Domínios' (Domains) view. At the top, there are filter tabs: 'DESCOBERTAS' (345), 'SOB ANÁLISE' (1), 'CONFÍAVEL' (3) - highlighted with a red box, 'IRRELEVANTE' (349), 'TAKEDOWN' (0), and 'TODOS' (698). Below the filters is a table with the following data:

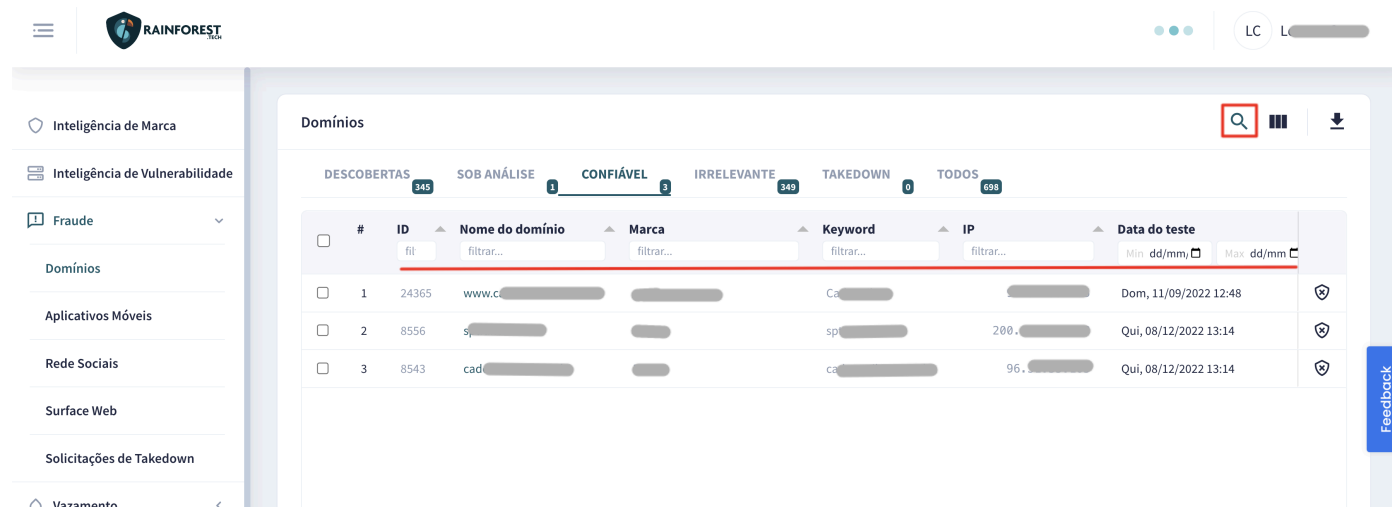
#	ID	Nome do domínio	Marca	Keyword	IP	Data do teste
1	24365	www.██████████	██████████	C ██████████	96.██████████	Dom, 11/09/2022 12:48
2	8556	██████████	██████████	s ██████████	██████████ 198	Qui, 08/12/2022 13:14
3	8543	██████████.br	██████████	ca ██████████	96.██████████	Qui, 08/12/2022 13:14

At the bottom right of the table, there is a pagination control showing '20' items per page, and buttons for 'Primeira', 'Ant.', '1', 'Próx.', and 'Última'. A vertical 'Feedback' button is visible on the right edge of the interface.

Para saber mais sobre classificação dos registros, consulte o artigo [Classificação dos itens encontrados](#)

## Alternar filtros (Lupa)

Nas telas que temos a listagem de registros, podemos clicar na opção e em seguida filtros serão habilitados abaixo de cada nome de coluna do grid de informações, com isso, podemos digitar o que desejamos na respectiva coluna para filtramos as informações.



The screenshot shows the Rainforest tool interface. On the left is a navigation menu with categories like 'Inteligência de Marca', 'Inteligência de Vulnerabilidade', 'Fraude', 'Domínios', 'Aplicativos Móveis', 'Rede Sociais', 'Surface Web', 'Solicitações de Takedown', and 'Vazamento'. The main area displays a table titled 'Domínios' with columns: '#', 'ID', 'Nome do domínio', 'Marca', 'Keyword', 'IP', and 'Data do teste'. Above the table are filter tabs: 'DESCOBERTAS' (545), 'SOB ANÁLISE' (3), 'CONFIÁVEL' (3), 'IRRELEVANTE' (549), 'TAKEDOWN' (0), and 'TODOS' (693). Each column has a search filter input. A 'Feedback' button is on the right side.

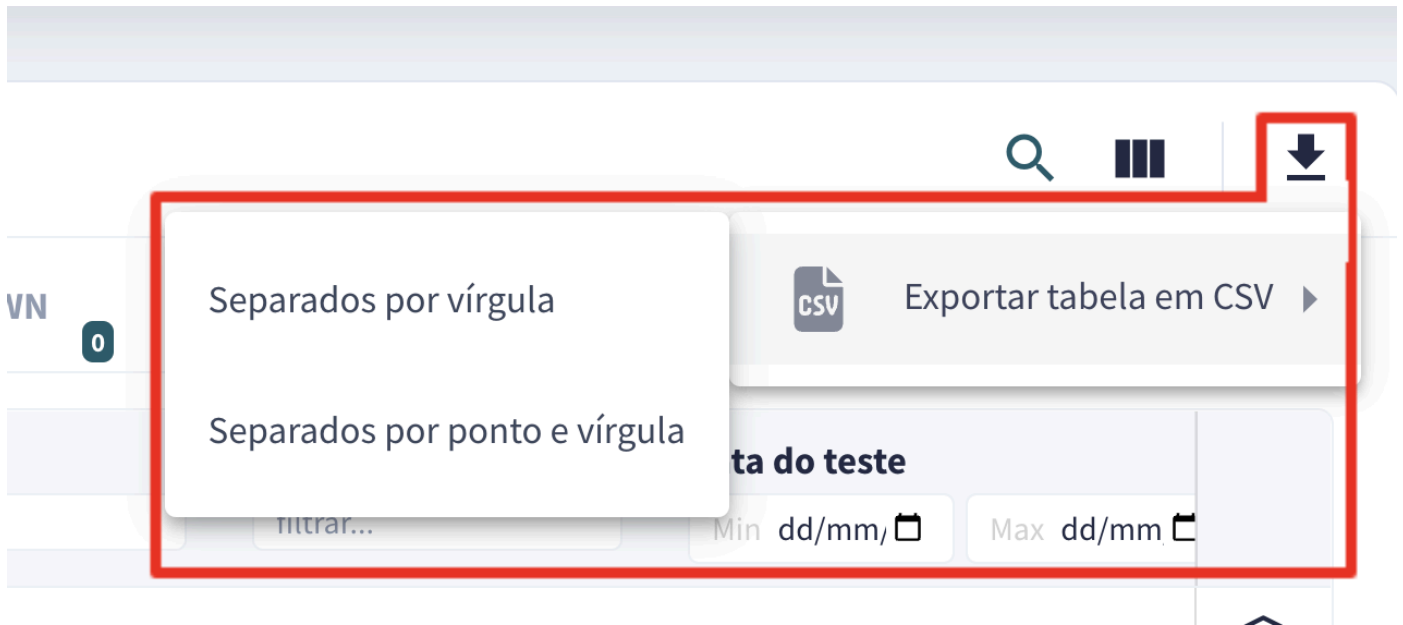
#	ID	Nome do domínio	Marca	Keyword	IP	Data do teste
1	24365	www.c...		Ca...		Dom, 11/09/2022 12:48
2	8556	s...		sp...	200.	Qui, 08/12/2022 13:14
3	8543	cad...		ca...	96.	Qui, 08/12/2022 13:14

## Personalizar colunas

O Rainforest possibilita aos usuários personalizarem o grid de informações com as colunas que acharem mais relevantes para suas análises, para isso clique em **Personalizar colunas**, um pop-up se abrirá com as colunas disponíveis, faça as alterações desejadas, marcando e desmarcando as colunas desejadas e movendo-as para a ordem que achar melhor.

## Exportar dados

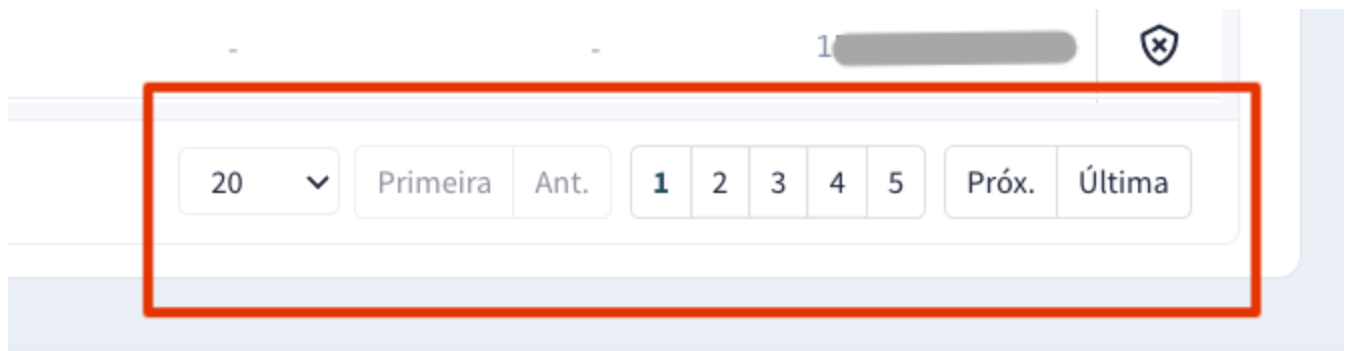
Caso o usuário deseje fazer uma análise mais detalhada dos registros encontrados, o Rainforest permite realizar a exportação dos registros para uma planilha eletrônica. Clique no ícone **Exportar dados > Exportar tabela em CSV > Selecione uma das opções disponíveis.**



**Atenção:** o Rainforest exportará somente os registros que estão visíveis em tela.

### Número de registros por página / Navegar entre páginas

Abaixo do grid de informações de registros, o Rainforest possibilita o usuário ajustar o número de registro por página desejado como também navegar entre as páginas disponíveis.

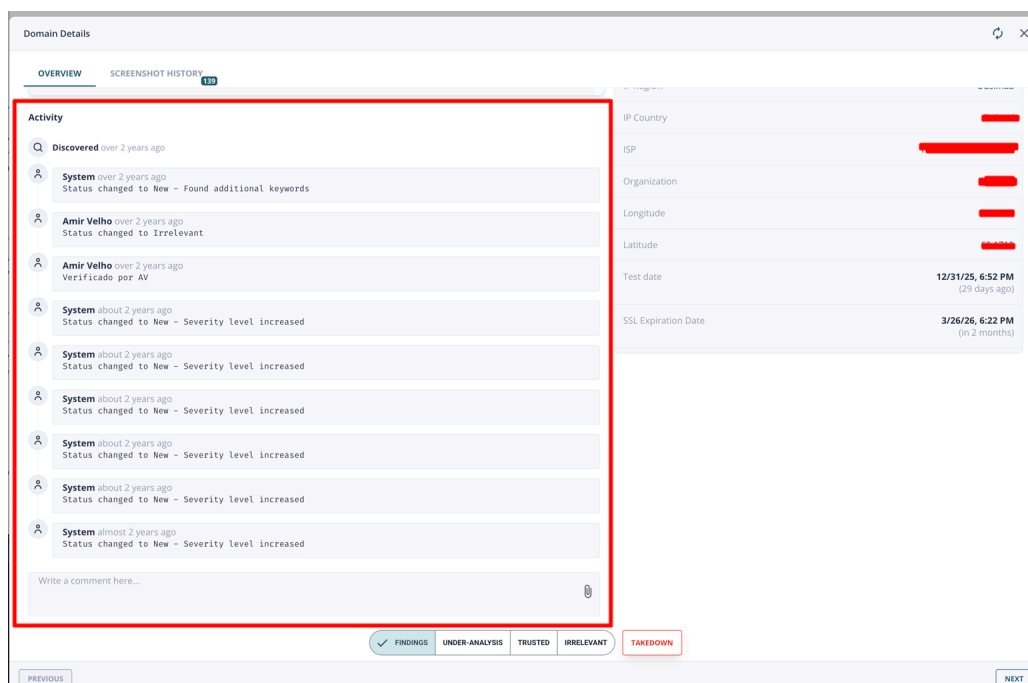


# Atividades em Achados

 support.rainforest.tech/en/kb/atividades-em-achados

## Registre e acompanhe o histórico de atividades em achados da Plataforma da Rainforest

A plataforma da Rainforest possibilita que os usuários registrem atividades nos achados. Desta forma é possível ter uma visão de todas as atualizações/atividades que houveram em determinado registro. Para isso acesse o registro desejado e vá até a sessão **Atividade**.



Você terá a visão das atividades registradas automaticamente pela plataforma e por outros usuários. Caso queira registrar uma nova, digite o conteúdo no campo de texto disponível e em seguida clique em **Comentar**.

Atividade manual registrada por usuário 

**COMMENT**

O registro será incluído na linha do tempo de atividades do achado.

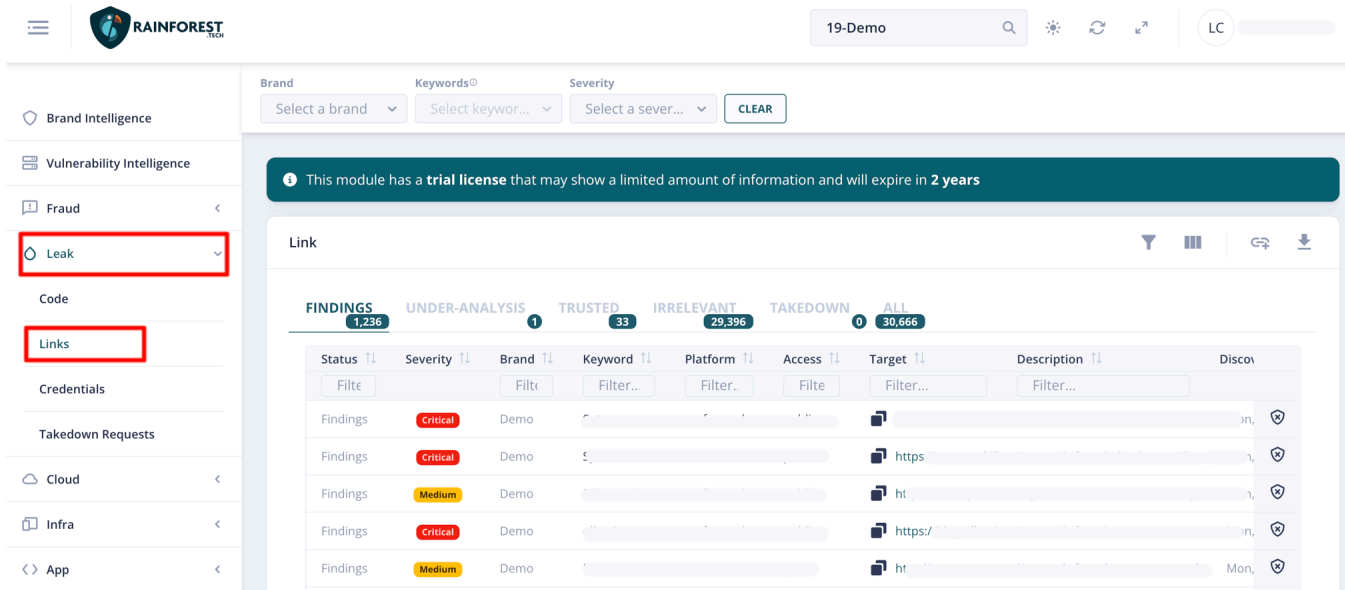
# Encontrando Referências em Links

 support.rainforest.tech/pt-br/kb/finding-link-references

## Veja referencias indexadas na internet que estão mencionando sua marca e/ou domínio.

A plataforma da Rainforest oferece para seus usuários dentro do pilar de Inteligência de Marca, a possibilidade de monitorar itens indexados na internet que estão mencionando a marca ou domínio da empresa.

Desta forma, a plataforma é capaz de encontrar links que fazem fazem menção a marca, podendo ser link de documentos e serviços que podem estar divulgando conteúdo confidencial. Para monitorar essa categoria de descoberta, logue na plataforma da Rainforest em seguida acesse o menu **Leak > Links**.



The screenshot shows the Rainforest platform interface. On the left, a navigation menu is visible with 'Leak' and 'Links' highlighted in red boxes. The main content area displays a search interface with filters for Brand, Keywords, and Severity. Below the filters, a notification states: 'This module has a trial license that may show a limited amount of information and will expire in 2 years'. The main section is titled 'Link' and shows a table of findings. The table has columns for Status, Severity, Brand, Keyword, Platform, Access, Target, Description, and Discover. The findings are categorized by status: FINDINGS (1,236), UNDER-ANALYSIS (1), TRUSTED (33), IRRELEVANT (29,396), TAKEDOWN (0), and ALL (30,666). The table lists several findings with their respective severity levels (Critical, Medium) and brands (Demo).

Status	Severity	Brand	Keyword	Platform	Access	Target	Description	Discover
Findings	Critical	Demo						
Findings	Critical	Demo				https://		
Findings	Medium	Demo				ht		
Findings	Critical	Demo				https://		
Findings	Medium	Demo				ht		Mon

A plataforma listará todos os registros encontrados, podendo a partir desse ponto o usuário analisá-los, categoriza-los e, se necessário, abrir uma solicitação de takedown.

# Vazamento de Código

---

 support.rainforest.tech/pt-br/kb/vazamento-codigo

## Entenda como a plataforma Rainforest identifica vazamento de código

---

Certamente você já ouviu falar de vazamento de código e dados.

Dia após dia empresas de todos os tamanhos vem enfrentando dificuldades com parte ou todo o código de uma ou mais aplicações expostos na web. Isso implica na segurança da aplicação que é uma das mais, se não a mais, importante ferramenta do negócio nos dias atuais. Muitas vezes a aplicação é o negócio, como em casos do Uber, Airbnb e diversos outros serviços.

Tais vazamentos ocorrem por diversos motivos:

- Má configuração dos sistemas que deixam pontos vulneráveis suscetíveis a ataques;
- Descuido do usuário (seja ele administrador, desenvolvedor ou usuário final);
- Ou mesmo, de forma intencional com o objetivo de prejudicar o negócio.

Tendo em vista este cenário, a plataforma Rainforest monitora repositórios de código públicos com o objetivo de identificar eventuais vazamentos de código sejam eles do desenvolvimento de uma aplicação, parte de um banco de dados ou mesmo compartilhamento através de serviços de colagem (*paste*) que permitem a troca de informação de forma anônima.

Buscando pelas termos, palavras-chaves (*keywords*), que foram configurados, a plataforma identifica possíveis vazamentos como dados pessoais, senhas, chaves de API (*Application Programming Interface*), acessos de VPN (*Virtual Private Network*), *tokens* e demais itens que possam representar um prejuízo para o negócio.

Tal funcionalidade está inclusa no módulo de Vazamento (*Leak*) e pode ser acessada em **Vazamento > Código**.

- Brand Intelligence
- Vulnerability Intelligence
- Fraud
- Leak
- Code**
- Credentials
- Takedown Requests
- Cloud
- Infra
- App
- Reference
- Settings
- Organizations
- Brands
- Users
- Notifications
- Connectors

Code

🔍 📄 📄

FINDINGS 46548 UNDER-ANALYSIS 7 TRUSTED 113 IRRELEVANT 350 TAKEDOWN 0 ALL 47454

<input type="checkbox"/>	#	ID	Name	Brand	Source	Keyword	URL	Description	Discovery date	<input type="checkbox"/>
<input type="checkbox"/>	1	2288119	Mapa...	Demo	Github	obovivo	https://github.com/Multi...	bus track	Fri, 6/3/22 4:45 AM	<input type="checkbox"/>
<input type="checkbox"/>	2	90796	Untitled	Demo	Pastebin	...	https://pastebin.com/RQNg...	-	Tue, 3/23/21 1:52 PM	<input type="checkbox"/>
<input type="checkbox"/>	3	92166	crash	Demo	Pastebin	Sptras	https://pastebin.com/AyE...	-	Tue, 4/13/21 12:42 AM	<input type="checkbox"/>
<input type="checkbox"/>	4	92177	aaa...	Demo	Pastebin	...	https://pastebin.com/dFr...	-	Tue, 4/13/21 4:15 AM	<input type="checkbox"/>
<input type="checkbox"/>	5	92383	Untitled	Demo	Pastebin	...	https://pastebin.com/mab...	-	Thu, 4/15/21 3:18 AM	<input type="checkbox"/>
<input type="checkbox"/>	6	2283348	MostraLiuhActivity.java	Demo	Github	obovivo	https://github.com/Multi...	bus track	Wed, 6/1/22 9:04 PM	<input type="checkbox"/>
<input type="checkbox"/>	7	2288123	MainActivity.java	Demo	Github	obovivo	https://github.com/Multi...	bus track	Fri, 6/3/22 4:45 AM	<input type="checkbox"/>

Page Size 20 First Prev 1 Next Last

Feedback

# Fraude em Serviços de Mensagens

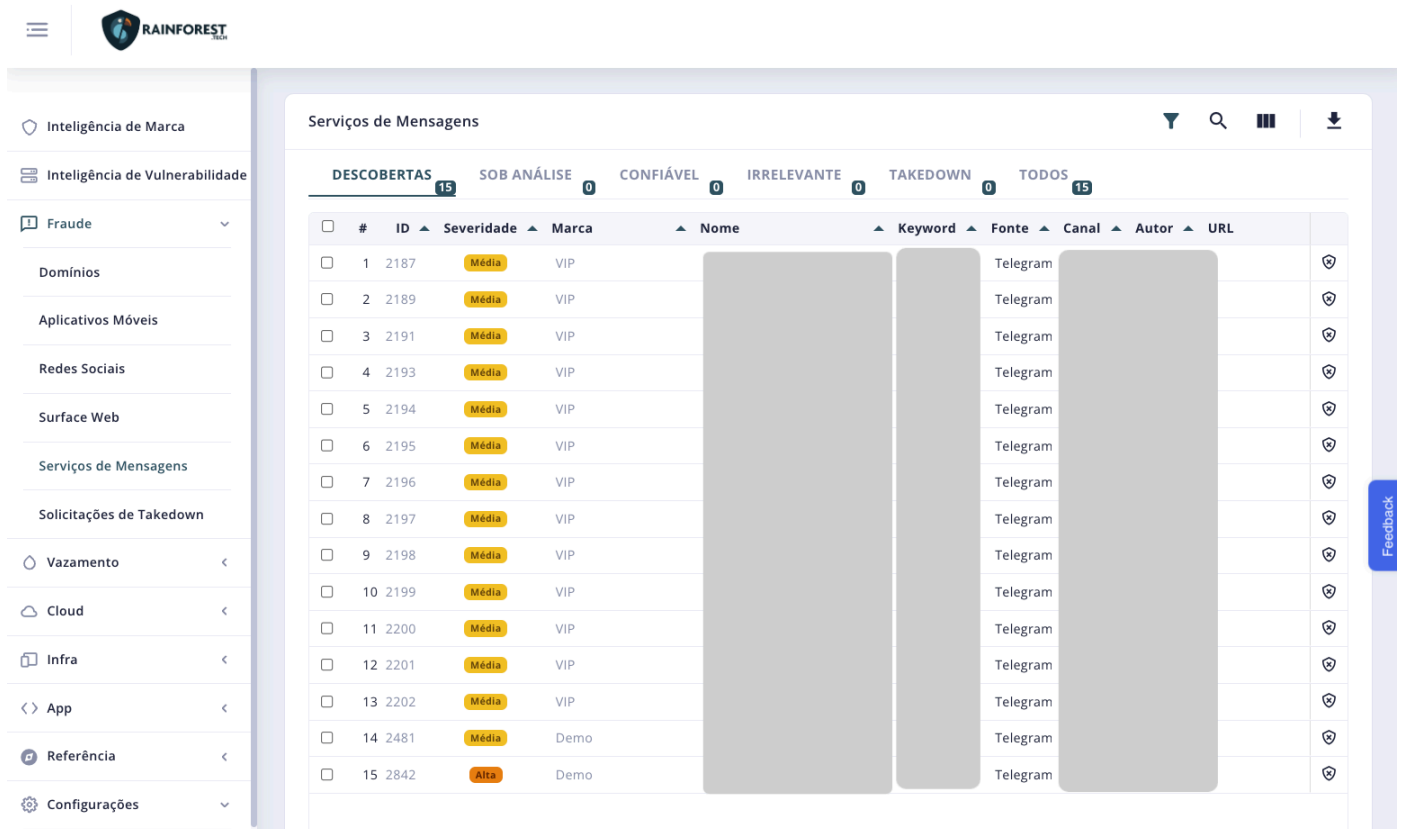
 support.rainforest.tech/pt-br/kb/fraude-servicos-mensagens

## Monitore grupos de mensagens onde pode ser divulgadas informações sobre sua empresa.

A Rainforest oferece para seus clientes a monitoração automática em grupos de serviços de mensageria, possibilitando o acompanhamento de perto e rápida detecção nessas aplicações que são largamente utilizadas atualmente em todo mundo.

Atualmente, a Rainforest fornece monitoramento a grupos apenas do **Telegram**

Na plataforma acesse **Fraude > Serviços de Mensagens**, será apresentado a listagem dos registros presentes na plataforma.



The screenshot displays the Rainforest platform interface. On the left is a navigation sidebar with categories like 'Inteligência de Marca', 'Inteligência de Vulnerabilidade', 'Fraude', 'Vazamento', 'Cloud', 'Infra', 'App', 'Referência', and 'Configurações'. The main area is titled 'Serviços de Mensagens' and shows a summary of findings: 15 discovered, 0 under analysis, 0 reliable, 0 irrelevant, 0 takedown, and 15 total. Below this is a table of detected messages.

	#	ID	Severidade	Marca	Nome	Keyword	Fonte	Canal	Autor	URL
<input type="checkbox"/>	1	2187	Média	VIP			Telegram			
<input type="checkbox"/>	2	2189	Média	VIP			Telegram			
<input type="checkbox"/>	3	2191	Média	VIP			Telegram			
<input type="checkbox"/>	4	2193	Média	VIP			Telegram			
<input type="checkbox"/>	5	2194	Média	VIP			Telegram			
<input type="checkbox"/>	6	2195	Média	VIP			Telegram			
<input type="checkbox"/>	7	2196	Média	VIP			Telegram			
<input type="checkbox"/>	8	2197	Média	VIP			Telegram			
<input type="checkbox"/>	9	2198	Média	VIP			Telegram			
<input type="checkbox"/>	10	2199	Média	VIP			Telegram			
<input type="checkbox"/>	11	2200	Média	VIP			Telegram			
<input type="checkbox"/>	12	2201	Média	VIP			Telegram			
<input type="checkbox"/>	13	2202	Média	VIP			Telegram			
<input type="checkbox"/>	14	2481	Média	Demo			Telegram			
<input type="checkbox"/>	15	2842	Alta	Demo			Telegram			

Ao acessar um registro, será apresentado maiores detalhes do registro encontrado pela plataforma. A partir disso você poderá classifica-lo e/ou realizar abertura de solicitação de takedown.



VISÃO GERAL

ATIVIDADE

ID: 2187

Status: **Descobertas**

Severidade: Média

Marca: [Redacted]

Origem: **telegram**

Fonte: **Telegram**

Canal: [Redacted]

Autor: [Redacted]

Keyword: [Redacted]

Nome: [Redacted]

DESCOBERTAS

SOB ANÁLISE

CONFIÁVEL

IRRELEVANTE

TAKEDOWN

ANTERIOR

PRÓXIMO

# Usando Labels para Classificar Redes e Ativos

 support.rainforest.tech/pt-br/kb/labels-redes-ativos

## Crie labels para classificar e organizar ativos na plataforma Rainforest.

As empresas que utilizam o módulo de **Infra** da Rainforest, tem a possibilidade de agrupar os ativos ou redes presentes na plataforma através de **labels**.

Cada empresa pode cadastrar labels de acordo com sua necessidade e cenário, isso possibilita organizar e agrupar de uma forma que faça sentido para o negócio.

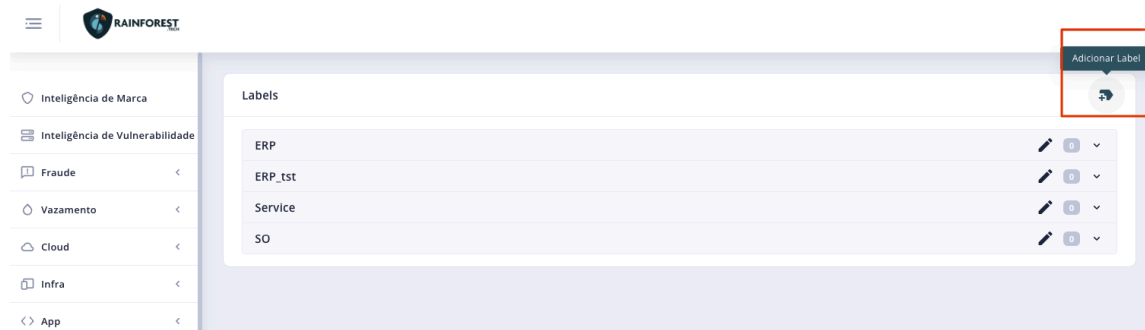
Além da possibilidade de realizar o cadastro e definição de labels nos ativos e redes como mencionado acima, a plataforma também permite realizar filtros por elas, trazendo informações mais detalhadas para os usuários.

Veremos a seguir como realizar o cadastro e utilizar as labels na plataforma da Rainforest.

## Cadastro

O registro de labels na plataforma pode ser feito acessando o menu **Configurações > Labels**.

Ao acessar o menu, será apresentado a lista das labels cadastradas, para iniciar o cadastro de uma nova clique em **Adicionar Label**.



Na tela de cadastro da label, informe os parametros **Key** e **Valor**. No campo key, ao digitar o nome da label, clique em **Use: Nome\_Label**.

### Criar Label ✕

Use este formulário para criar um novo rótulo. O rótulo tem uma chave e um ou mais valores.

**Key \*** **Valor \***

Label\_Test 🔍 Input a Value

**Use: Label\_Test** ADICIONAR VALOR

CANCELAR SALVAR

Cada label pode ter mais de um valor atribuído, adicione o(s) valor(es) desejado(s) e clique em **Salvar**.

### Criar Label ✕

Use este formulário para criar um novo rótulo. O rótulo tem uma chave e um ou mais valores.

**Key \*** **Valor \***

Label\_Test 🔍 Value 1 ✕

Value 2 ✕

Input a Value ✕

ADICIONAR VALOR

CANCELAR SALVAR

## Atribuindo Labels

Label cadastrada, você conseguirá atribuí-las dentro da plataforma. Para isso acesse sua listagem de assets/redes em **Infra > Ativos**,

Mostrando 7 de 7 itens 20 Primeira

**Ativos**

#	ID	Tipo	Nome	IP	Network	Exposto a
1	26	Ativo único	[Redacted]	[Redacted]	-	internal
2	918160	Ativo único	[Redacted]	[Redacted]	-	web
3	35	Ativo único	[Redacted]	[Redacted]	-	internal
4	34	Ativo único	[Redacted]	[Redacted]	-	internal
5	33	Ativo único	[Redacted]	[Redacted]	-	internal
6	32	Ativo único	[Redacted]	[Redacted]	-	internal
7	31	Ativo único	[Redacted]	[Redacted]	-	internal
8	30	Ativo único	[Redacted]	[Redacted]	-	internal
9	29	Ativo único	[Redacted]	[Redacted]	-	internal
10	28	Ativo único	[Redacted]	[Redacted]	-	internal
11	27	Ativo único	[Redacted]	[Redacted]	-	internal
12	16	Ativo único	[Redacted]	[Redacted]	-	internal
13	25	Ativo único	[Redacted]	[Redacted]	-	internal
14	24	Ativo único	[Redacted]	[Redacted]	-	internal

Mostrando 1 a 20 de 209 itens 20 Primeira Ant. 1 2 3 4 5 Próx. Última

Acesse o ativo desejado, na aba **Dados do Ativo** e clique em **Gerenciar Rótulos**.

**DADOS DO ATIVO** TECNOLOGIAS 3 VULNS POR TECH 2 VULNS POR VA VULNS POR SURFACE VULNS POR XDR X

Nome do Ativo [Redacted] Fonte system Tipo de Ativo Ativo único Endereço de IP [Redacted]

Departamento [Redacted] Coordenadas Latitude, longitude Network Seleccione uma rede

Exposto a Internal Impacto nos Negócios Média Ambiente Produção

Descrição [Redacted]

Technologies Discovery

**Labels** GERENCIAR RÓTULOS

Nenhum rótulo foi atribuído a este recurso ainda. Clique no botão acima para gerenciar rótulos.

Na tela de atribuição de labels, procure pela key cadastrada



Posteriormente selecione um dos valores cadastrados na label, aqui podemos atribuir quantas labels e valores quisermos. Por fim, clique em **Salvar**.



O ativo apresentará em seu cadastro as labels que foram atribuídas

**DADOS DO ATIVO**   TECNOLOGIAS <sup>3</sup>   VULNS POR TECH <sup>2</sup>   VULNS POR VA   VULNS POR SURFACE   VULNS POR XDR   X

Nome do Ativo

Fonte

Tipo de Ativo

Endereço de IP

Departamento

Coordenadas   
Ex.: 38.12024, -122.039998

Network

Exposto a

Impacto nos Negócios

Ambiente

Descrição

Technologies Discovery

**Labels** GERENCIAR RÓTULOS

## Filtrando Ativos com Labels Atribuídas

Ao atribuir labels nos ativos cadastrados na plataforma, você poderá filtrá-los por elas. Acesse o menu o filtro da plataforma e selecione a label/valor desejado, assim a plataforma retornará todos os assets relacionados.

The screenshot displays the Rainforest Security interface. On the left is a navigation menu with options like 'Inteligência de Marca', 'Inteligência de Vulnerabilidade', 'Fraude', 'Vazamento', 'Cloud', 'Infra', 'Dashboard', 'Ativos', 'Nota da Empresa', 'Exposição', 'Verificações de Vulnerabilidade', 'Configurações', 'App', 'Referência', 'Configurações', and 'Admin'. The main area is titled 'Probabilidade por CVE' and contains a chart with 'Probabilidade' on the y-axis and 'Pontuação' on the x-axis. The chart has a vertical line at 7 and a horizontal line at 5. A red dot is plotted at approximately (7.5, 5.5). Labels on the chart include 'Planeje corrigir' (7), 'Corrigir agora', 'Acelte riscos', and 'Corrigir mais tarde'. A 'Corrigir agora' button is visible in the top right of the chart area. To the right of the chart is a 'Filtros' sidebar with various filters. A red box highlights a filter labeled 'Rótulo' with the value 'Label\_Test=Value 1'. Below the chart is a table titled 'Ativos' with columns for '#', 'ID', 'Tipo', 'Nome', 'IP', and 'Network'. A red box highlights the 'Ativos' table. The table contains one row with ID 26 and Tipo 'Ativo único'. A red bar is present in the 'Nome' column of this row. A 'LIMPAR' button is at the bottom right of the filters sidebar.

Atualmente a funcionalidade de **labels** está disponível apenas para **ativos** dentro da plataforma da Rainforest. Em breve teremos disponível para outros módulos.

# Vazamento de Credenciais

---

 [support.rainforest.tech/pt-br/kb/vazamento-credenciais](https://support.rainforest.tech/pt-br/kb/vazamento-credenciais)

## Entenda como a plataforma Rainforest identifica vazamento de credenciais

---

Atualmente, é muito frequente receber notícias de grandes vazamentos de dados. Nestes é bem comum ouvir que foram vazados dados pessoais como nome, data de nascimento, números de documentos etc.

Contudo, além desse tipo de vazamento, tem crescido cada vez mais o número de base de usuários com credenciais vazadas. As credenciais são informações como usuário, senha, entre outras que dão acesso a um determinado sistema.

Além de bases vazadas, cada vez mais os atacantes roubam informações das máquinas dos próprios usuários utilizando artefatos maliciosos (*malwares*) que muitas vezes são instalados pelo acesso a sites comprometidos ou uso indevido de máquina como, por exemplo, software pirata ou sistemas de compartilhamento de arquivo.

Como se não bastasse, adiciona a este cenário práticas inseguras com a gestão da credencial onde boas práticas não são conhecidas ou praticadas.

Alguns exemplos de boas práticas com o uso das credenciais de acesso que normalmente não são seguidos são:

- Uso de senhas mais elaboradas (complexas) envolvendo todos os tipos de caracteres (letras maiúsculas e minúsculas, números e caracteres especiais) e um comprimento de senha que dificulte um atacante de chegar através de combinações àquela senha;
- Troca de senha periódica;
- Múltiplo fator de autenticação, onde usa um complemento de senha (token ou biometria) externo através de um dispositivo como o celular;
- Uso de senhas diferentes para diferentes serviços, evitando compartilhar a mesma senha de uso pessoal do site de compra para o sistema corporativo que tem a base de todos os clientes, por exemplo.

Com base neste cenário, a plataforma Rainforest monitora vazamento de credenciais na surface, deep e dark web através do nome de domínio corporativo que foi configurado na plataforma. Verifica se já houve algum vazamento de credencial conhecido na base que possui e adiciona tal domínio para monitoramento em eventuais vazamentos que venham a ocorrer.

O monitoramento possui níveis diferentes, a plataforma identifica informações vazadas de usuários diretamente ligados a empresa, ou seja, credenciais que estão vinculadas a usuários do domínio da empresa. Adicionalmente, a plataforma identifica vazamentos de terceiros, ou seja, clientes da empresa que utilizam algum software com o domínio da marca e que tiveram suas senhas vazadas.

Tal funcionalidade só é possível, através de ações automatizadas somadas ao trabalho de especialistas de segurança que monitoram grupos de mensagem, fóruns e outras fontes de informação que divulgam esses tipos de vazamento.

Tal funcionalidade está inclusa no módulo de Vazamento (*Leak*) e pode ser acessada em **Vazamento > Credenciais**.

The screenshot shows the Rainforest Security interface. The main content area is titled 'Credentials' and displays a table of leaked credentials. The table has the following columns: #, ID, Brand, Username, Password, Target, Description, Leakage Date, and File. The table is filtered to show 5 items under the 'FINDINGS' category. The interface includes a sidebar with navigation options like 'Brand Intelligence', 'Vulnerability Intelligence', 'Fraud', 'Leak', 'Code', 'Credentials', 'Takedown Requests', 'Cloud', 'Infra', 'App', 'Reference', 'Settings', 'Organizations', 'Brands', 'Users', 'Notifications', and 'Connectors'. The top right shows 'Demo' and 'User Demo'.

#	ID	Brand	Username	Password	Target	Description	Leakage Date	File
1	1830337	-	ta...@example.ci	*****	-	Deep Web	-	-
2	1830336	-	de...@example.com	*****	-	Deep Web	-	-
3	1830335	-	ma...@example.com	*****	-	Deep Web	-	-
4	1830334	-	ma...@example.cc	*****	-	Deep Web	-	-
5	1830332	-	tu...@example.cor	*****	-	Deep Web	-	-

Na tela de visualização de credenciais encontradas, o usuário pode, de forma macro, ocultar ou mostrar todas as credenciais encontradas, assim como seleciona-las e associa-las a uma categoria, facilitando a gestão e segurança.

19-Demo

Brand: Select a brand | Keywords: Select keyword... | Severity: Select a sever... | CLEAR

This module has a **trial license** that may show a limited amount of information and will expire in **2 years**

Credentials

FINDINGS 99,999 | UNDER-ANALYSIS 5 | IRRELEVANT 2,617 | SOLVED 17 | TAKEDOWN 0 | ALL 102,638

Actions: MARK AS UNDER-ANALYSIS | MARK AS IRRELEVANT | MARK AS SOLVED | CHANGE SEVERITY | ADD COMMENT | REPROCESS URL

<input checked="" type="checkbox"/>	#	ID	Status	Severity	Brand	Username	Password	Target	Descr
<input checked="" type="checkbox"/>	1	83165393	Findings	Critical	Demo				
<input checked="" type="checkbox"/>	2	81257728	Findings	Critical	Demo				
<input checked="" type="checkbox"/>	3	81329427	Findings	Critical	Demo				
<input checked="" type="checkbox"/>	4	81336478	Findings	Critical	Demo				
<input checked="" type="checkbox"/>	5	83519971	Findings	Critical	Demo				

Para ajudar na análise, categorização e tomada de decisão, a plataforma pode oferecer várias informações nos registros encontrados, dentre elas temos:

- Severidade
- Usuário
- Senha
- Alvo
- Descrição

Data do vazamento

Data da descoberta

# Visão Geral Vazamento

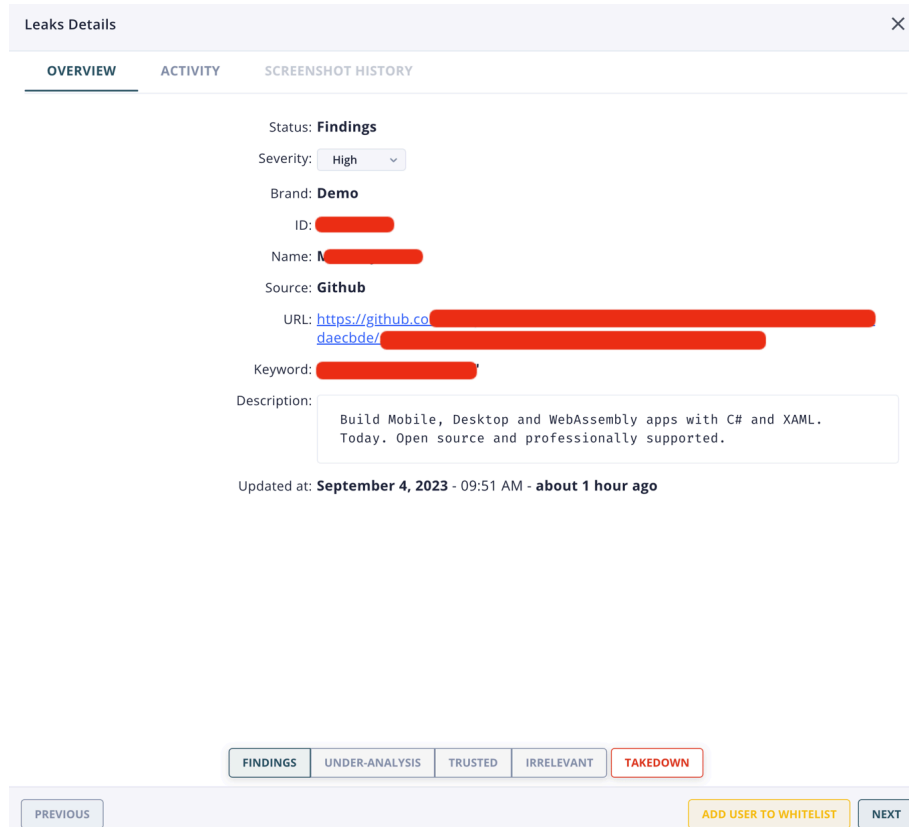
 support.rainforest.tech/pt-br/kb/visao-geral-vazamento

## Encontre e contenha o vazamento de informações, aumentando sua proteção contra riscos digitais

O módulo **Rainforest Leak** monitora a deep, dark e a surface web para encontrar e identificar vazamentos diversos que podem comprometer a reputação da sua empresa. Atualmente a plataforma organiza os vazamentos nas seguintes categorias.

### Vazamento de Código-Fonte

Encontre código proprietário em repositórios públicos e outros locais da web antes que agentes maliciosos tenham a chance de examinar e encontrar possíveis vulnerabilidades para explorar.



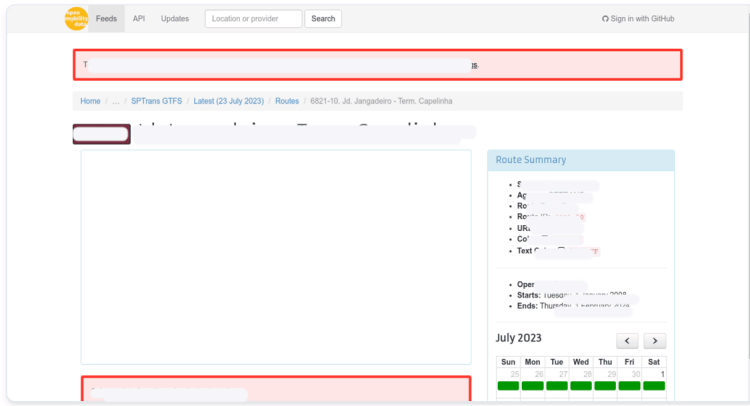
The screenshot displays the 'Leaks Details' window with the following information:

- Status:** Findings
- Severity:** High
- Brand:** Demo
- ID:** [Redacted]
- Name:** [Redacted]
- Source:** Github
- URL:** [https://github.com/\[Redacted\]](https://github.com/[Redacted])
- Keyword:** [Redacted]
- Description:** Build Mobile, Desktop and WebAssembly apps with C# and XAML. Today. Open source and professionally supported.
- Updated at:** September 4, 2023 - 09:51 AM - about 1 hour ago

At the bottom, there are navigation buttons: PREVIOUS, FINDINGS (selected), UNDER-ANALYSIS, TRUSTED, IRRELEVANT, TAKEDOWN, ADD USER TO WHITELIST, and NEXT.

### Vazamento Links

Descubra links que referenciam sua marca e/ou domínio e descubra se há vazamentos ocorrem através deles.



Activity

Created over 2 years ago

Write a comment here...

COMMENT

Status Findings

Severity Critical

Brand Demo

Keyword

ID

Platform surfaceweb

Access public

Target https://...321-10

Description

```
Keywords found: database
...
ility <b>Database</b> catalogs.
...
tps://<b>database.</b>mobilitydata.org/
...
```

Created 2023-07-24 03:41:31

Modified 10/7/25, 5:27 PM (4 months ago)

Last classification date 7/24/23, 9:41 AM (3 years ago)

- ✓ FINDINGS
- UNDER-ANALYSIS
- TRUSTED
- IRRELEVANT
- TAKEDOWN

PREVIOUS

NEXT

## Vazamento de Credenciais

Utilizando nossas inteligências nós buscamos por credenciais vazadas ou comprometidas disponíveis na Web e fóruns da Deep e Dark web.

Detalhes leak de credenciais

VISÃO GERAL ATIVIDADE

Severidade: Média

ID: [Redacted]

Nome do usuário: de [Redacted]

Senha: [Redacted]

Alvo: -

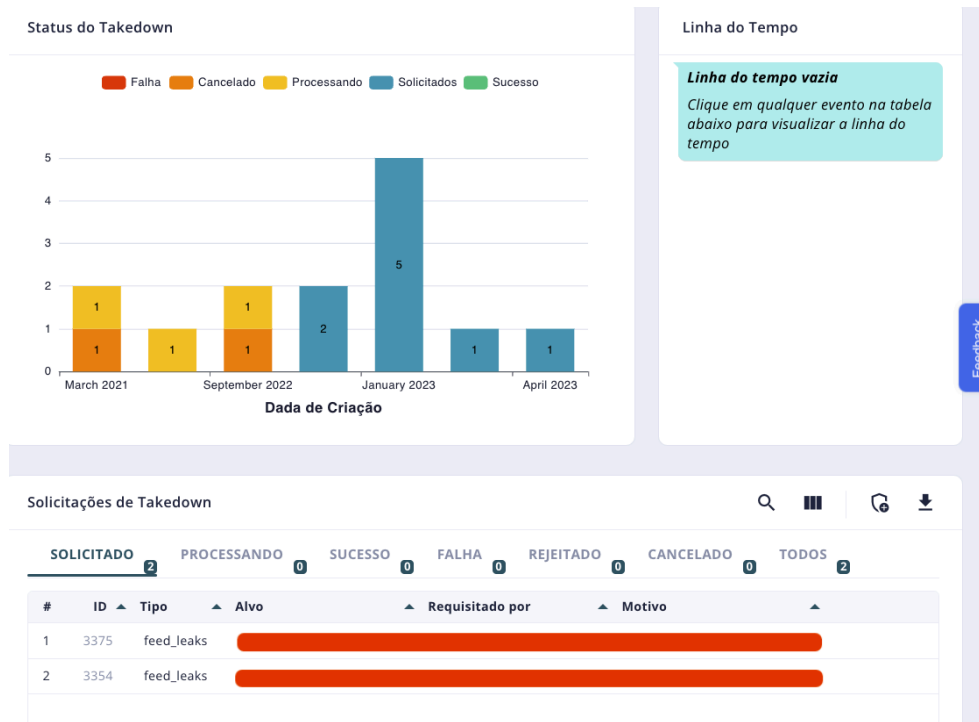
Descrição: Deep Web

Data da descoberta: March 31, 2021 - 04:13 PM - há mais de 2 anos

Status: Descobertas

## Takedown

Realize solicitações de takedown com evidências diretamente da plataforma e acompanhe o status em tempo real: poder de verdade para proteger seu negócio.



Apenas 4% da web está na superfície, o que significa milhões de websites. A maior parte do conteúdo não é facilmente encontrável e muitas vezes é mantida escondida na própria superfície web ou na Deep e Dark web, onde hackers comercializam informações.

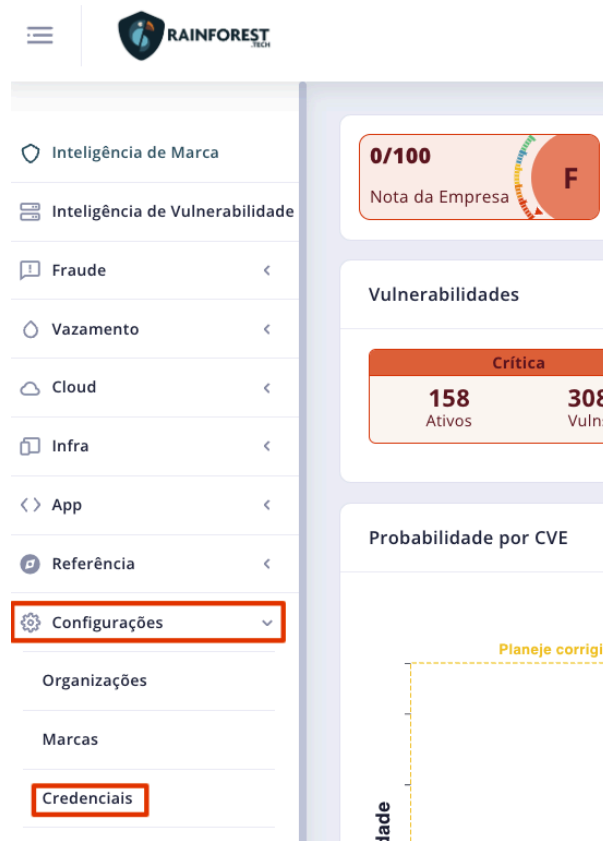
# Configurando Credenciais Externas

[support.rainforest.tech/pt-br/kb/configurando-credenciais](https://support.rainforest.tech/pt-br/kb/configurando-credenciais)

## Veja como configurar credenciais de acesso a outros sistemas.

A plataforma Rainforest permite realizar a integração com diversos sistemas externos, e alguns desses podem necessitar de autenticação.

Esses acessos podem ser configurados no menu **Configurações > Credenciais**.



Acessando o menu você verá todas as credenciais cadastradas na plataforma.

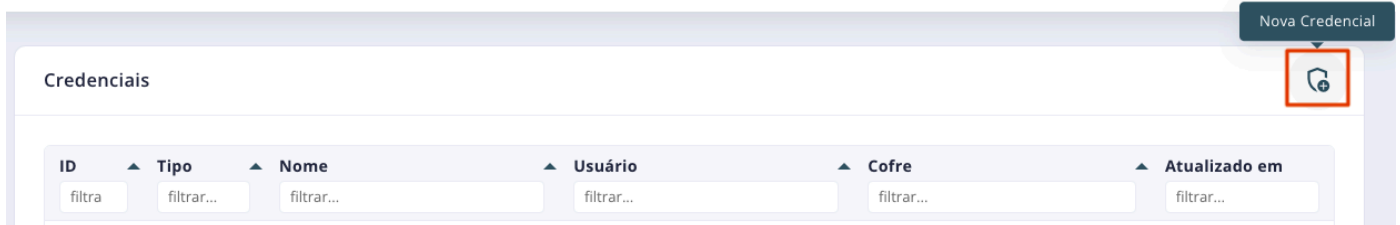


ID	Tipo	Nome	Usuário	Cofre	Atualizado em
16	git				Seg, 3/15/21 6:44 PM
101	git				ex, 8/20/21 10:16 AM
599	ssh				ar, 12/13/22 12:57 PM
600	ssh				er, 12/13/22 4:48 PM
608	ssh				eg, 12/26/22 2:34 PM
750	git				Qua, 6/14/23 2:16 PM

Mostrando 6 de 6 itens

20 Primeira Ant. 1 Próx. Última

Para realizar o cadastro de uma credencial, clique no ícone posicionado no canto superior direito do grid de credenciais



Depois preencha os campos e clique em **Salvar**

### Edit the credential

Name: UserExemple

Type: SSH

Vault: Local

User: root

Password or Certificate: .....

CANCEL DELETE SAVE

Para garantir a segurança das credenciais o sistema tem um menu dedicado para a configuração das mesmas e armazenamento dessas em cofre de senha interno e criptografado.

Uma vez cadastrada a senha ou certificado de uma credencial, não será possível visualizá-la novamente, caso necessite orientamos excluí-la e cadastrá-la novamente.

Essas credenciais podem ter a finalidade de realizar diversos tipos de login:

- **GIT** - sistema de versionamento de código;
- **ARTIFACT** - sistemas para versionamento de artefatos (JFROG, NUGET, ARTIFACTORY, ETC)
- **REGISTRY** - ve de imagens docker
- **SSH** - sistemas operacionais Linux;
- **SMB** - sistemas operacionais Windows;
- **ESX** - sistemas VMware.

Alguns clientes possuem os seus próprios cofres de senhas, os quais a plataforma Rainforest pode se integrar a partir de seus conectores.

Conectores com cofres de senhas externos e status atual da integração:

- **Hashicorp Vault** - pronto e homologado;
- **CyberArk** - pronto e homologado;
- **SenhaSegura** - em roadmap, conector foi criado, integração foi realizada mas ainda não foi homologado.
- **IBM Security Verify Privilege Vault** - em roadmap, conector foi criado, integração foi parcialmente realizada e ainda não foi homologado.
- **Outros**: Caso utilize algum outro cofre de senhas e queira ver ele nessa lista, favor abrir um feedback com a solicitação e a equipe da Rainforest vai verificar a possibilidade de inclusão no roadmap.

# Desativação de Ativos

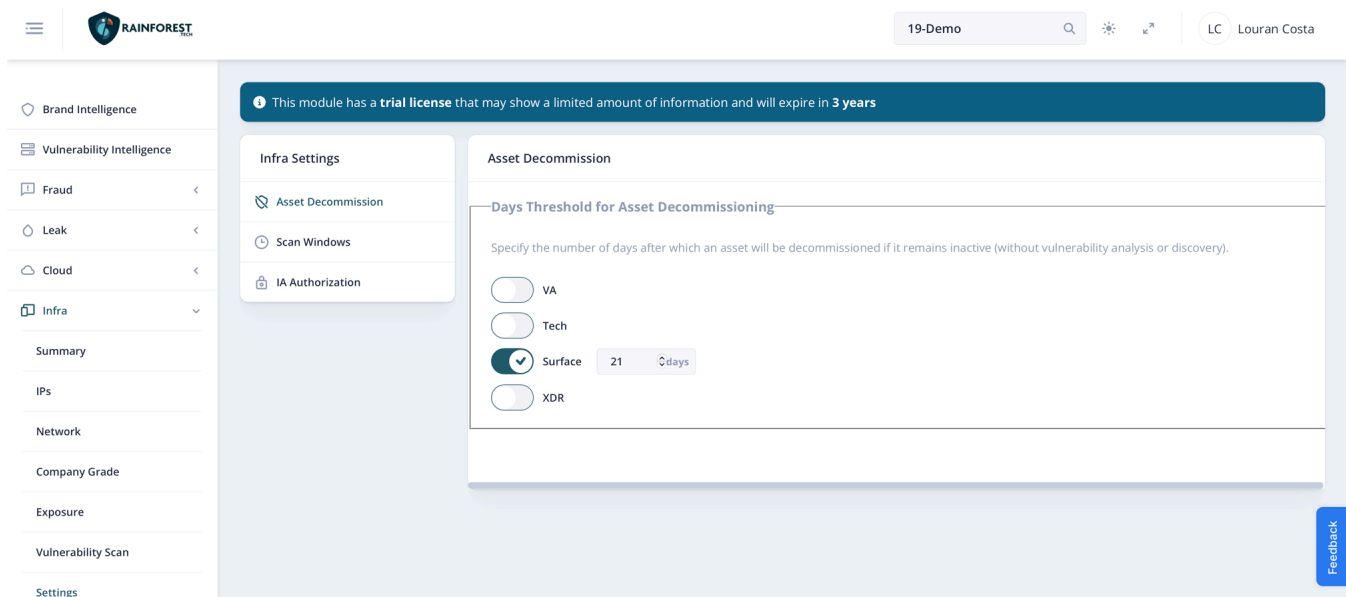
[support.rainforest.tech/pt-br/kb/pt-br/desativacao-ativos](https://support.rainforest.tech/pt-br/kb/pt-br/desativacao-ativos)

## Especifique o número de dias após os quais um ativo será desativado se permanecer inativo (sem análise ou descoberta de vulnerabilidade).

Durante as análises de varreduras de dispositivos na infraestrutura do cliente, a plataforma da Rainforest pode identificar itens inativos dentro de uma quantidade de dias e desativá-los. Possibilitando que a base da solução seja sanitizada evitando manter ativos que não foram mais identificados, consumindo assim licenças que não são necessárias.

Apenas dispositivos que não passarão por uma análise ou que não tiveram vulnerabilidades descobertas entram nos critérios do decomissionamento.

Para realizar a configuração acesse o menu **Infra > Settings > Asset Decommission**.



The screenshot displays the Rainforest platform's 'Asset Decommission' settings. A blue banner at the top states: "This module has a trial license that may show a limited amount of information and will expire in 3 years". The main content area is titled "Asset Decommission" and includes a section for "Days Threshold for Asset Decommissioning". Below this, there is a sub-section with the text: "Specify the number of days after which an asset will be decommissioned if it remains inactive (without vulnerability analysis or discovery)". There are four toggle switches: "VA", "Tech", "Surface", and "XDR". The "Surface" toggle is checked, and next to it is a dropdown menu showing "21 days". The left sidebar shows the navigation menu with "Infra" expanded to show "Settings".

Você terá disponível os tipos de análises que a plataforma realiza no módulo de infra, ao ativar uma das análises você deverá definir a quantidade de dias que a plataforma utilizará como base.

Ative os tipos de análises desejados e a quantidade de dias para a plataforma realizar o decomissionamento, em seguida clique em **Salvar**.

Infra Settings

- Asset Decommission
- Scan Windows
- IA Authorization

### Asset Decommission

#### Days Threshold for Asset Decommissioning

Specify the number of days after which an asset will be decommissioned if it remains inactive (without vulnerability analysis or discovery).

<input checked="" type="checkbox"/>	VA	30	days
<input type="checkbox"/>	Tech		
<input checked="" type="checkbox"/>	Surface	21	days
<input checked="" type="checkbox"/>	XDR	30	days

CANCEL SAVE

O decomissionamento de dispositivos baseado em dois critérios:

1. Na funcionalidade de análise (TECH, INFRA, SURFACE e XDR)
2. No número de dias necessário até que o dispositivo não seja mais visto

# Instalação de Analisadores (Agentes)

---

 [support.rainforest.tech/pt-br/kb/instalacao-analisadores](https://support.rainforest.tech/pt-br/kb/instalacao-analisadores)

## Procedimento para instalação dos analisadores Rainforest na infraestrutura do cliente.

---

Serão necessárias duas VMs Linux para instalação dos seguintes componentes de forma automatizada:

- RF-Agent-Manager (**mínimo de 4vCPUs, 8GB de RAM e 200 GB HD**)
- RF-Agent-Scanner (**mínimo de 4vCPUs, 8GB de RAM e 200 GB HD**) (para testes de infraestrutura das aplicações).

Os requisitos mínimos citados aqui nesse documento são para ambientes pequenos durante uma prova de conceito, para ambientes produtivos recomendasse mais hardware dependendo do tamanho da infraestrutura e quantidade de scan que serão realizados.

Atualmente, as distribuições e versões suportadas são:

- Ubuntu 18.04.6 LTS (Bionic) e 20.04.2 LTS (Focal);
- CentOS Linux 7 e 8;
- Oracle Linux 7 e 8;
- CIS Amazon Linux 2 Kernel 4.14 Benchmark - Level 1.

No menu **Configurações > Agentes** esta disponível os comandos de instalação, para realizar a instalação é necessário copiar esse comando e executar na VM de destino como root. Esse script vai realizar todos os passos necessários para realizar a instalação e configuração dos serviços.

The screenshot displays the Rainforest Tech dashboard with a sidebar menu on the left and a main content area on the right. The sidebar menu includes items like Takedown Requests, Leak, Cloud, Infra, App, Reference, Settings, Organizations, Brands, Credentials, Users, Notifications, Connectors, Scan Settings, Agents, API Access Token, Monitoring Config, and Privacy Operations Settings. The main content area contains three sections, each with a title and a terminal command for installation:

- Install RF-Agent-Manager:** To install, run the following command in a terminal of a Linux Ubuntu or CentOS VM with access to your network:  

```
curl -H "X-Job-Token: V29iaHZPYUZuei94ZjlxK1dUcEdObVBudXZhdDJDU3RMOUF4Z2d2aTjYOfhScINRQ2ZDQ3MvMng2K3Jea3ZGYU02VmxoQS85d1IEUkRsb3ZGxkMINjZ1RMWlc2MHR0M2EvUjFHcVFOSXhoa3dpenN2UndPUDJGcnlFaStOMTIPenhTL0pwb3VhSWhEWnNpV0I3bzhDVXg4bFdNb3pvY" -X GET "https://api.rainforest.tech/apibackend/pam/job/eagle-19-install/install_pipeline_agent.sh/" | bash
```
- Install RF-Agent-Runner:** To install, run the following command in a terminal of a Linux Ubuntu or CentOS VM with access to your network:  

```
curl -H "X-Job-Token: V29iaHZPYUZuei94ZjlxK1dUcEdObVBudXZhdDJDU3RMOUF4Z2d2aTjYOfhScINRQ2ZDQ3MvMng2K3Jea3ZGYTI1bXVvZXF1cHlzTWY5OFZzZGxkMINjZ1RMWlc2MHR0M2EvUjFHcVFOSXhoa3dpenN2UndPUDJGcnlFaStOMTIPenhTL0pwb3VhSWhEWnNpV0I3bzhDVXg4bFdNb3pvY" install/install_pipeline_agent.sh&install_node=true" | bash
```
- Install RF-Agent-Scanner:** To install, run the following command in a terminal of a Linux Ubuntu or CentOS VM with access to your network:  

```
curl -H "X-Job-Token: V29iaHZPYUZuei94ZjlxK1dUcEdObVBudXZhdDJDU3RMOUF4Z2d2aTjYOHbVa21pN016ZENvOTFDZHQ4ckF1aFJ1WWhNVzj0cExrUjF4WjM" GET "https://api.rainforest.tech/apibackend/pam/job/eagle-19-install/install_scanner_agent.sh/" | bash
```

A instalação dos analisadores (agentes), se faz necessário apenas nas máquinas virtuais fornecidas pelo cliente, dispensando a necessidade de realização de instalações em máquinas de usuários, desenvolvedores.

**Todos os analisadores (agentes) disponíveis são instalados única e exclusivamente de forma centralizada na infraestrutura do cliente, ou seja, apenas nas máquinas fornecidas pelo cliente.**

As comunicações entre os analisadores e a plataforma da Rainforest são realizadas por meio de uma conexão criptografada através do protocolo HTTPS, dando segurança para as informações que trafegam entre a estrutura do cliente e a plataforma da Rainforest.

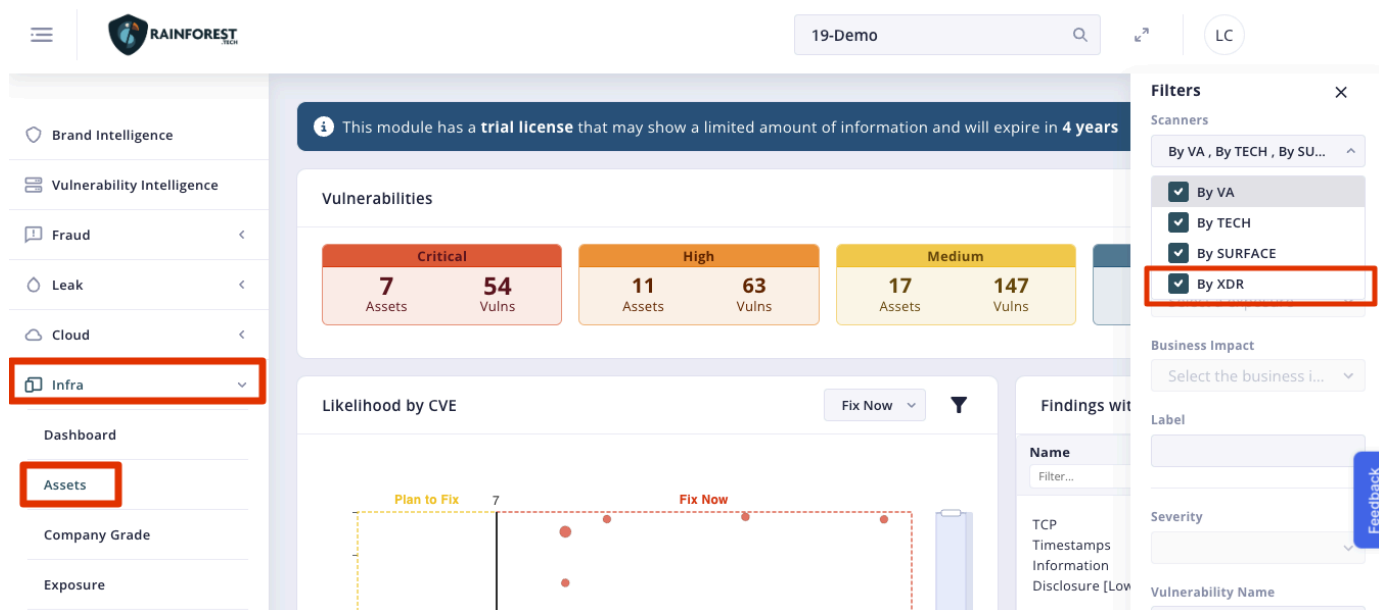
# Vulnerabilidades By-XDR

 support.rainforest.tech/pt-br/kb/vulnerabilidades-xdr

## Expanda e centralize vulnerabilidades na plataforma Rainforest

Quando você já possui algum tipo de segurança, como **TrendMicro** ou **Wazuh**, a plataforma da Rainforest possibilita a configuração de conectores dessas aplicações, assim ela permite importar e mostrar todas as vulnerabilidades de seus ativos de forma centralizada no Rainforest.

Na listagem de ativos cadastrados, você pode realizar o filtro apenas das vulnerabilidades By-XDR, para isso acesse **Infra > Ativos > Filtro** e deixe selecionado apenas a opção **Por XDR**



The screenshot shows the Rainforest platform interface. The sidebar on the left has 'Infra' and 'Assets' highlighted with red boxes. The main content area displays a 'Vulnerabilities' section with a summary of vulnerabilities categorized by severity: Critical (7 Assets, 54 Vulns), High (11 Assets, 63 Vulns), and Medium (17 Assets, 147 Vulns). Below this is a 'Likelihood by CVE' chart. On the right, a 'Filters' panel is open, showing 'By XDR' selected under the 'Scanners' section. A 'Feedback' button is visible on the right side of the interface.

As vulnerabilidades importadas dessas aplicações são agrupadas em uma sessão exclusiva, dando uma visão segmentada por categoria de vulnerabilidade.

ASSET DATA TECHNOLOGIES **VULNS BY TECH** VULNS BY VA VULNS BY SURFACE **VULNS BY XDR** X

Asset Name [Redacted] Asset Type Single Asset IP Address [Redacted]

Description [Redacted] Source system

Department [Redacted] Coordinates Latitude, longitude Network Select a network  
Ex.: 38.12024, -122.039998

Ports [Redacted]

① Press 'Enter' after typing the port to confirm and add.


**Exposure and Impact**

Exposure to Internal Business Impact Medium Environment Production

**Discovery**

Discovery Technologies

**Labels** [MANAGE LABELS](#)

 No labels have been assigned to this asset yet. Click the button above to manage labels.

CANCEL DELETE SAVE

61758 Single Asset 10.1.203.126 10.1.203.126 Intern

Para conectar o Rainforest ao **TrendMicro** ou **Wazuh**, acesse o menu **Configurações > Conectores**, na listagem clique sobre o conector desejado e cadastre uma credencial.



- Fraud
- Leak
- Cloud
- Infra
- App
- Reference
- Settings
- Organizations
- Brands
- Labels
- Credentials
- Users
- Notifications
- Connectors

### Connectors

+ New Credential



**TrendMicro**  
security  
Multinational cyber security software  
company



**Wazuh**  
wazuh  
Wazuh service

Sorry, no results found

Feedback

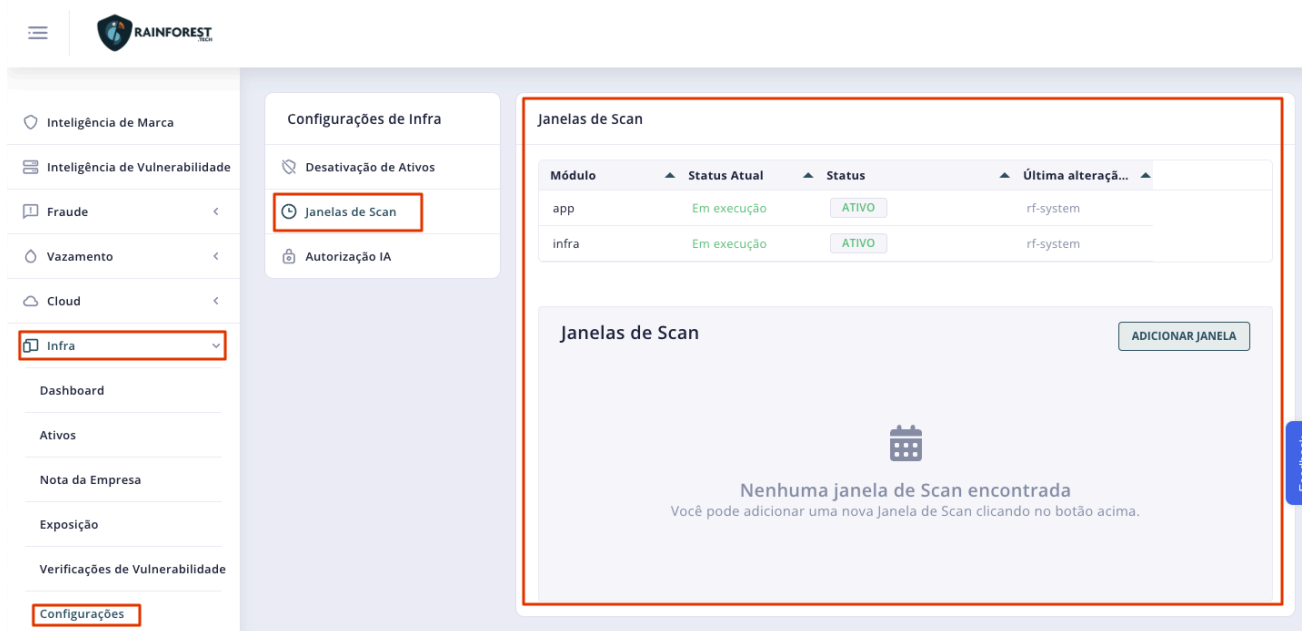
# Janelas de Scan

 support.rainforest.tech/pt-br/kb/pt-br/janelas-scan

## Configure janelas de tempo de execução em que a plataforma Rainforest realizará suas análises.

Na plataforma da Rainforest é possível que os usuários cadastrem janelas de escaneamento customizadas. Desta forma a empresa pode personalizar os momentos de análise da plataforma para a sua realidade.

Para acessar o menu de configuração acesse **Infra > Configurações > Janelas de Scan**.



The screenshot shows the Rainforest platform interface. On the left is a navigation menu with 'Infra' selected. The main content area is titled 'Configurações de Infra' and contains a sub-menu with 'Janelas de Scan' highlighted. Below this is a table of scan windows:

Módulo	Status Atual	Status	Última alteraçã...
app	Em execução	ATIVO	rf-system
infra	Em execução	ATIVO	rf-system

Below the table, there is a section titled 'Janelas de Scan' with a calendar icon and the text: 'Nenhuma janela de Scan encontrada. Você pode adicionar uma nova Janela de Scan clicando no botão acima.' A button labeled 'ADICIONAR JANELA' is visible.

Clique no botão **Adicionar Janela**, será apresentado as configurações disponíveis:

- **Nome:** defina um nome para a Janela de Scan
- **Habilitado:** defina se o scan cadastrado estará ou não habilitado.
- **Módulos:** defina quais módulos entrarão na janela de análise, **APP** ou **INFRA**
- **Data Inicial:** data de início da janela de scan
- **Data Final:** data final de janela de scan
- **Programação:** dias da semana que a janela de scan será executada

Janela de Scan ✕

Nome\*  Habilitado

Módulos

- APP
- INFRA

Data Inicial  Escolha uma Data Inicial

Data Final  Escolha uma Data Final

Programação

- Domingo
- Segunda
- Terça
- Quarta
- Quinta
- Sexta
- Sábado

Após preencher as informações, clique em **Salvar**. Depois de cadastrada, você poderá atualizar o status da janela configurada, podendo:

- Forçar como PAUSADO
- ATIVO
- Seguir programação da janela

Caso a janela de scam ultrapasse o horário configurado, a plataforma pausará o scan e retomará na próxima janela de execução

# Rainforest Analisadores (Agentes)

---

 [support.rainforest.tech/pt-br/kb/rainforest-agentes](https://support.rainforest.tech/pt-br/kb/rainforest-agentes)

## Veja como preparar o ambiente para realização de implantações ou PoV da plataforma da Rainforest.

---

Descreveremos qual o processo para realizar a instalação de analisadores (agentes) da Rainforest. Tais analisadores agrupam um conjunto de *containers* - com ferramentas e processos, que realizam as diversas análises.

### Tipos de Analisadores

---

Atualmente, existem quatro tipos de analisadores:

- **Rainforest Agent Manager:** responsável por realizar a verificação dos processos agendados na plataforma Rainforest e distribuí-los para que sejam executados internamente no cliente. O Agent Manager já inclui o que é necessário para execução das tarefas, ou seja, ele já traz uma instalação integrada de um Agent Runner. Sendo assim, em instalações mais simples ou mesmo para ambientes pequenos e médios não é necessária a instalação separada de Agent Runner.
- **Rainforest Agent Runner:** responsável por executar as tarefas que foram agendadas e distribuídas pelo Rainforest Manager. Faz-se necessário em ambientes mais complexos, que exijam escalabilidade para aumento de performance.
- **Rainforest Agent Scanner:** responsável por realizar análises de vulnerabilidade no ambiente.
- **Rainforest Agent Quality:** responsável por realizar análises de qualidade em código fonte.

As informações que seguem têm como objetivo apoiar a instalação desde um cenário mais simples, como em uma prova de valor (*Proof of Value* - PoV) ou ambientes menores, até conceitos para instalações mais complexas.

Atualmente, não cobrimos todos os tipos de cenários neste documento. Existem variações que poderão ser solicitadas pelo time da Rainforest ou de seus parceiros.

Caso haja qualquer dúvida na configuração, favor entrar em contato com o engenheiro de sistemas (SE) ou com o suporte seja do parceiro ou da Rainforest.

### Requisitos de Recursos

---

Existem duas opções para instalação dos analisadores da Rainforest cada uma com seus respectivos recursos mínimos necessários:

Todas os analisadores em apenas um recurso (*Virtual Machine – VM*) (**All In One**) – recomendado para ambientes de validação (PoV) ou ambientes produtivos menores.

RF-Agent (mínimo de 8vCPUs, 16GB de RAM e 400 GB HD)

Instalação de analisadores separados em dois ou mais recursos com base nas análises que serão realizadas (**Múltiplos Analisadores**) – recomendado para a maioria dos ambientes produtivos.

RF-Agent (mínimo de 4vCPUs, 12GB de RAM e 200 GB HD)

**Atenção:** nesta opção de instalação serão necessários no mínimo duas VMs com os recursos indicados acima:

1. para o Agent Manager
2. para o Agent Scanner.

Para instalações com análise de qualidade de código será necessário, minimamente, uma terceira VM para o Agent Quality também.

Independente da opção de instalação, cabe uma observação sobre o requisito de disco (*Hard Disk - HD*). O espaço em disco requerido deverá ser disponibilizado no seguinte ponto de montagem:

**/mnt/eagle**

Este é o diretório que utilizará maior parte dos recursos. Não há problema se toda alocação de recurso for realizada no ponto de montagem raiz ( / ), desde que o ponto de montagem **/mnt/eagle** esteja abaixo do / e que seja observado espaço em disco igual, ou superior, ao delimitado no requisito de instalação.

Além disso, atualmente, as seguintes distribuições e versões do Sistema Operacional Linux são suportadas:

- Ubuntu 18.04.6 LTS (Bionic) e 20.04.2 LTS (Focal)
- CentOS Linux 7 e 8
- Oracle Linux 7 e 8
- CIS Amazon Linux 2 Kernel 4.14 Benchmark - Level 1

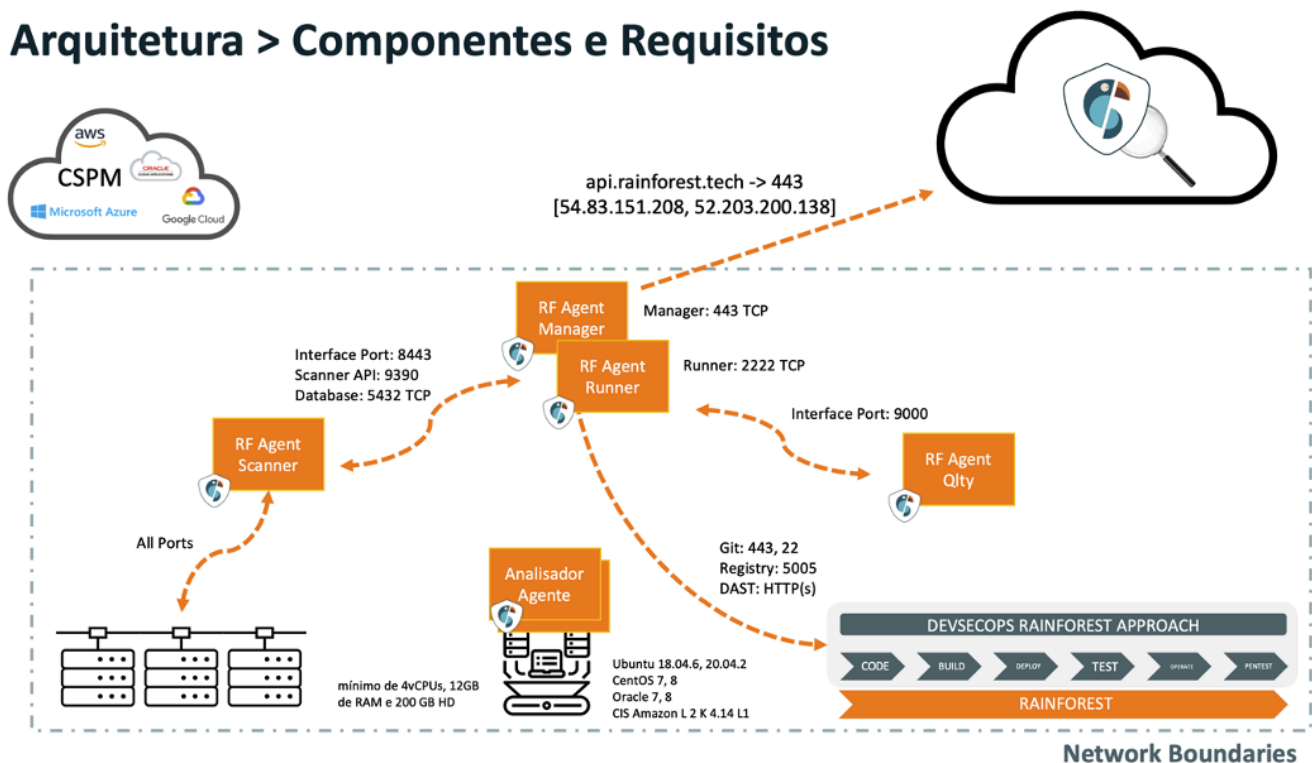
Já foram realizadas instalações em versões mais atuais dos sistemas listados, contudo para efeito de suporte, as versões recomendadas são as listadas acima.

## Pré Requisitos de Acesso / Segurança

Para que o ambiente funcione corretamente, é importante que as seguintes configurações de acesso e segurança sejam realizadas nos dispositivos que realizam filtragem ou bloqueio de pacotes (*firewalls, proxies, etc*) entre agentes, redes e plataforma da Rainforest.

Segue diagrama que ajuda a entender os diversos tipos de comunicação que estão presentes no ambientes:

### Arquitetura > Componentes e Requisitos



Durante a instalação a VM precisará ter acesso livre a internet com todas as portas liberadas, pois a máquina irá fazer *download* de repositórios diferentes.

Após a instalação, as URLs nas seguintes portas deverão permanecer liberadas:

**api.rainforest.tech [54.83.151.208 e 52.203.200.138] -> 443**

No cenários com múltiplos analisadores, as portas de comunicação entre agentes deverão ser liberadas:

- **Agent Manager <-> Agent Runner** (caso não estejam no mesmo recurso)  
Runner: 2222 TCP

- **Agent Manager/Runner <-> Agent Scanner**

- **Interface Port:** 8443 TCP (por padrão)
- **Scanner API:** 9390 TCP (por padrão)
- **Database:** 5432 TCP (por padrão)

**Atenção:** se qualquer uma das portas acima foi customizada no conector, será importante utilizar a porta específica que foi definida na configuração do conector.

- **Agent Manager/Runner <-> Agent Qlty**

Interface Port: 9000

- **Agent Manager/Runner <-> Esteira DevOps** (para análise de aplicação)

- **Git:** 443, 22 (por padrão)
- **Registry:** 5005 (por padrão)
- **DAST:** HTTP(S) - 80 e 443 (por padrão)

**Atenção:** se qualquer uma das portas acima é diferente no ambiente, será importante utilizar a porta específica e configurá-la para que o analisador tenha acesso.

**Agent Scanner <-> Network / Assets** (para análise de vulnerabilidade)

Todas as portas

Para *troubleshooting* remoto e direto através do time da Rainforest será necessário acesso **SSH (22)** e **HTTPS (443)** nos servidores: **RF-Agent-Manager** e **RF-Agent-Scanner**. Recomenda-se que tal acesso seja criado durante a PoV limitando o acesso ao seguinte IP público: **3.88.75.145** e 3.220.4.204.

Para ambiente produtivo, recomenda-se uso de soluções de segurança tal como cofre de senhas que permita um acesso seguro e controlado de um ambiente externo.

Cenários em que o analisador terá algum tipo de antivírus ou processo local que possa bloquear chamadas e/ou comunicação torna-se importante configurar as seguintes regras de exceção para instalação e upgrades periódicos:

- /tmp/eaglesetup-\*
- /tmp/vulnerability-feed-\*
- /tmp/docker-deploy-jenkins.tar.gz
- /mnt/eagle
- /etc/eagle

**Atenção:** além destas, todas as liberações necessárias para execução de container no agente, ou seja, regras para execução de Docker deverão ser configuradas.

## Configurações dos Agents

---

Após a liberação do tenant pelo engenheiro de sistemas (SE) responsável, serão necessárias as seguintes configurações:

1. **Setting > API Access Token:** criar Token (sem espaço e hífen)  
**Exemplo:** APITokenCliente.  
**Atenção:** copiar o token que não será exibido posteriormente
2. **Setting > Connector > jobManager:** colocar o ID e Token criado acima.
3. **Setting > Connector > Manager:** colocar IP RF-Agent-Manager > Definir um usuário e senha.
4. **Setting > Connector > Quality:** colocar IP RF-Agent-Quality > Definir um usuário e senha.
5. **Setting > Connector > Scanner:** colocar IP RF-Agent-Scanner > Definir um usuário e senha (por padrão, <IP>:9390).
6. **Setting > Assets > New Asset:** cadastrar a rede ou host e habilitar dois itens de Discovery Technologies e Discover Host (se rede).
7. **Setting > Vulnerability Scan:** New SCAN (Frequency Weekly) > "Basic configuration template with a minimum set of NVTs required for a scan".
8. **Setting > Agentes:** Rodar o setup nos dois servidores Pipeline (JobManager) e Scan Agent

## Configurações da Aplicação

---

As seguintes informações deverão ser obtidas antes da configuração da plataforma Rainforest. Só assim a plataforma poderá realizar cada uma das análises.

- **SAST e SCA** (Código da aplicação e dependências externas):
  - Acesso ao repositório GIT
  - Dependendo da linguagem, os comandos de build em *dockerfile*
- **QLTY** (Qualidade de código):  
Acesso ao *Sonarqube* local
- **DAST** (Aplicação em execução):  
URL onde é realizado os testes/homologação da aplicação
- **IMAGE** (Imagem Docker):  
Acesso ao registry de imagens

Para maiores detalhes sobre a configuração do cenário para App recomendamos os artigos:

- [Visão Geral App](#)
- [Registrar uma Aplicação](#)
- [Editar uma Aplicação](#)
- [Opções no Cadastro de uma Aplicação](#)

## Informações Necessárias para Análise de Cloud

---

Para a configuração de ambientes cloud na plataforma Rainforest, disponibilizamos artigos específicos para cada provedor que damos suporte.

**Para maiores detalhes sobre a configuração de cenários Cloud recomendamos os artigos:**

- [Configurando Cloud AZURE \(Microsoft\)](#)
- [Configurando Cloud AWS \(Amazon\)](#)
- [Configurando Cloud GCP \(Google\)](#)

# API Rainforest Plataforma

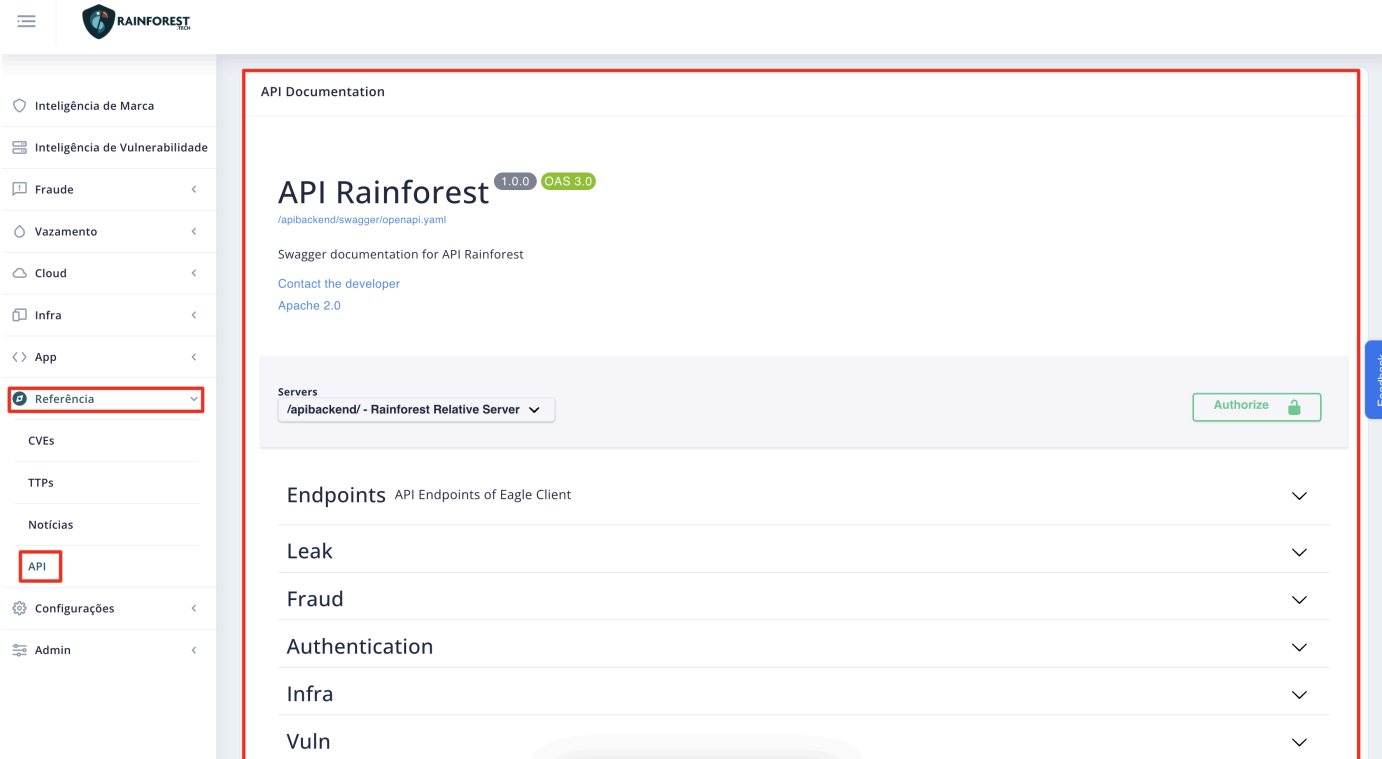
 [support.rainforest.tech/pt-br/kb/api-rainforest-plataforma](https://support.rainforest.tech/pt-br/kb/api-rainforest-plataforma)

## Documentação de referência de API da Plataforma Rainforest

Nossas APIs são desenvolvidas com o intuito de permitir que qualquer equipe seja capaz de criar integrações eficazes para personalizar e aproveitar ao máximo a plataforma Rainforest.

Todas as APIs do Rainforest são [criadas usando convenções REST](#) e projetadas para ter uma estrutura de URL previsível. Elas usam vários recursos HTTP padrão, inclusive métodos (**POST**, **GET**, **PUT**) e códigos de resposta de erro. Todas as chamadas de API do Rainforest são feitas em <https://api.rainforest.tech/> e todas as respostas retornam um JSON padrão.

Para ter acesso a documentação da API, acesse o menu **Referências > API**, após acessar verá detalhadamente a documentação, com seus métodos, exemplos de utilização, modelos de respostas.



Os métodos estão organizados em categorias, onde cada categoria corresponde ao módulo da plataforma da Rainforest.

Abrindo o menu do módulo desejado, será apresentado os métodos disponíveis para o respectivo módulo.



Leak



GET	/api/leak/credential	Get Credential Paginated	🔒	⌵
PUT	/api/leak/credential/changeStatus	Change status Credential	🔒	⌵
GET	/api/leak/summary/{type}	Get Leak Summary By Type	🔒	⌵
GET	/api/leak/summary/brand/{type}	Get Leak Summary Brand By Type	🔒	⌵
GET	/api/leak/summary	Get Leak Summary	📄 🔒	⌵
GET	/api/leak/takedown/summary	Get Leak Takedown Summary	🔒	⌵
GET	/api/leak/takedown/list/{status}	Get Leak Takedown By Status	🔒	⌵
GET	/api/leak/takedown/detail/{id}	Get Leak Takedown Detail	🔒	⌵
POST	/api/leak/takedown/create	Create Leak Takedown	🔒	⌵

Fraud



Authentication



Em seguida, ao abrir o menu de um método específico, terá maiores informações, como por exemplo parâmetros necessários, exemplo de corpo da requisição, exemplo de retornos com seus respectivos códigos e conteúdos.

Try it out

Parameters

Name	Description
id * required integer (path)	id

Responses

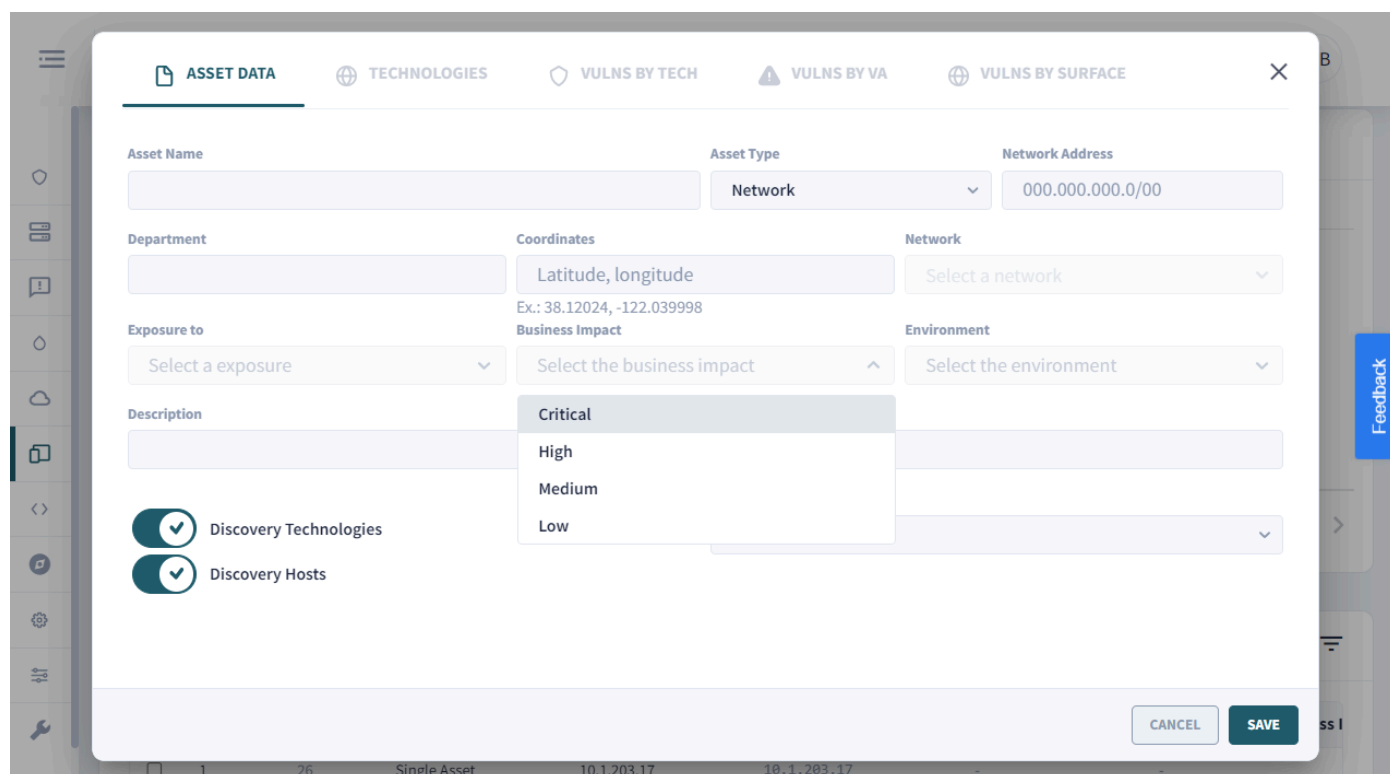
Code	Description	Links
200	Success Media type: application/json Controls Accept header. Example Value: <pre>{ "status": 200, "data": {} }</pre>	No links
204	No Content Media type: application/json Example Value: <pre>{ "status": 204, "data": {} }</pre>	No links
400	Bad Request	No links
401	Unauthenticated	No links
403	Forbidden	No links

# Vulnerabilidades By-VA (Vulnerability Assessment)

 support.rainforest.tech/pt-br/kb/inventario-scan-infraestrutura

## Detectando o Inventário da Infraestrutura e suas Vulnerabilidades

A plataforma Rainforest permite a detecção automática do inventário da rede e também o cadastro manual de endereços a serem monitorados.



The screenshot shows the 'ASSET DATA' form in the Rainforest platform. The form is divided into several sections:

- Asset Name:** A text input field.
- Asset Type:** A dropdown menu currently set to 'Network'.
- Network Address:** A text input field containing '000.000.000.0/00'.
- Department:** A text input field.
- Coordinates:** A text input field with the placeholder 'Latitude, longitude' and an example 'Ex.: 38.12024, -122.039998'.
- Network:** A dropdown menu with the placeholder 'Select a network'.
- Exposure to:** A dropdown menu with the placeholder 'Select a exposure'.
- Business Impact:** A dropdown menu with the placeholder 'Select the business impact'. A dropdown menu is open, showing options: 'Critical', 'High', 'Medium', and 'Low'.
- Environment:** A dropdown menu with the placeholder 'Select the environment'.
- Description:** A text input field.
- Discovery Technologies:** A toggle switch that is checked.
- Discovery Hosts:** A toggle switch that is checked.

At the bottom right of the form, there are 'CANCEL' and 'SAVE' buttons. The bottom of the screenshot shows a table with columns for asset ID, name, and IP address, with the first row containing '1', '26', and 'Single Asset'.

A detecção automática pode ser tanto dos IPs disponíveis em uma rede quanto das tecnologias sendo executadas nesses IPs.

Já no cadastro manual, o usuário pode optar por registrar uma rede ou um único ativo, fazendo a alteração no campo **Tipo de Ativo**, além de poder informar os outros campos como **nome do ativo**, **departamento**, **endereço de rede**, **coordenadas** e **descrição**.

Nome do Ativo

Tipo de Ativo

Network

Network

Ativo único

Endereço de rede

000.000.000.0/00

Departamento

Coordenadas

Latitude, longitude

Ex.: 38.12024, -122.039998

Exposto a

Internal

Impacto nos Negócios

Média

Ambiente

Produção

Descrição



Technologies Discovery



Hosts Discovery

## Labels

GERENCIAR RÓTULOS



Nenhum rótulo foi atribuído a este recurso ainda.  
Clique no botão acima para gerenciar rótulos.

No cenário de ser necessário o cadastro de uma rede (Tipo de Ativo **Network**), a plataforma possibilita cadastrar uma faixa de rede (range) e habilita o scan automatizado de ativos na rede através da opção **Hosts Discovery**, identificando os ativos existentes nessa faixa de rede cadastrada.

Habilitando essa funcionalidade, será possível escolher a **frequência** desejada para que a plataforma realize a identificação automática dos ativos.

**DADOS DO ATIVO**   TECNOLOGIAS   VULNS POR TECH   VULNS POR VA   VULNS POR SURFACE   VULNS POR XDR   ✕

Nome do Ativo    **Tipo de Ativo**    Endereço de rede

Departamento    Coordenadas    Network

Ex.: 38.12024, -122.039998


Exposto a    Impacto nos Negócios    Ambiente

Descrição

Technologies Discovery

**Hosts Discovery**

**Labels**

 Nenhum rótulo foi atribuído a este recurso ainda. Clique no botão acima para gerenciar rótulos.

**Frequência**

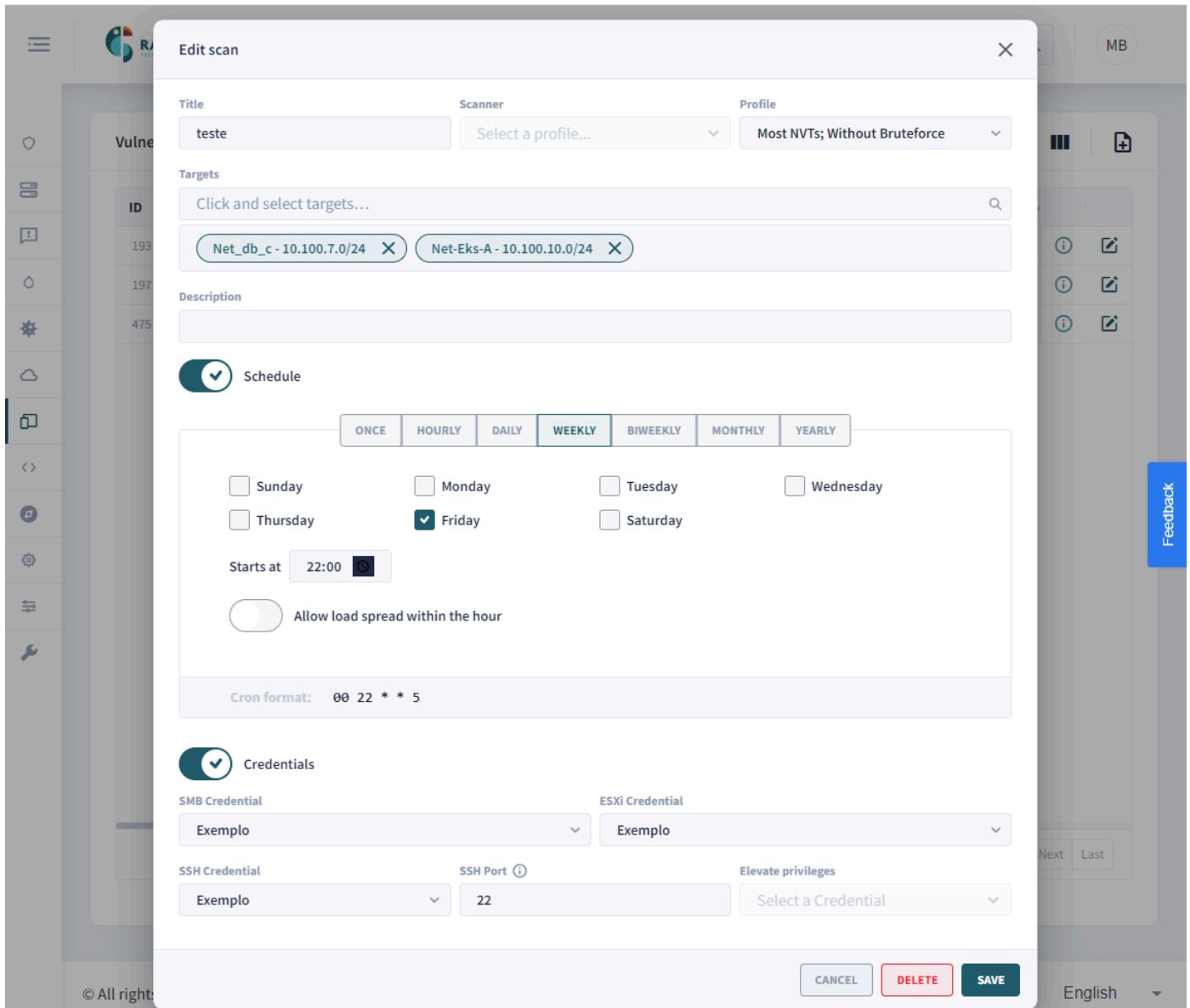
Selecione uma opção

- One day
- Two days
- Three days
- Four days
- Five days
- Six days
- Seven days**
- Fifteen days
- Thirty days
- One year

## Parametrização de Scan

Uma vez que foi realizado o inventário da infraestrutura, também é possível agendar **scans de vulnerabilidades** (com ou sem autenticação) desses endereços, independente de serem endereços públicos ou privados:



Os scans podem ser agendados com as seguintes opções:

**Perfil:**

- o *Network Host Discovery scan configuration* - scan de rede com foco em identificar novos hosts;
- o *CPE Inventory* - scan dedicado para descobrir as tecnologias sendo executadas em cada host;
- o *Basic configuration* - scan básico com foco em identificar algumas das principais vulnerabilidades, recomendado para um primeiro scan de vulnerabilidade de todo o ambiente;

- *Most NVTs, Without Bruteforce* - scan avançado, utilizado para encontrar vulnerabilidades sem sobrecarregar os servidores com requisições (esse é normalmente o o scan mais utilizado);
- *Most NVTs* - scan avançado, podendo eventualmente sobrecarregar alguns serviços ao tentar realizar força-bruta para identificar algumas vulnerabilidades;
- **Agendamento** (*Schedule*), a plataforma permite diversas opções de agendamento com os horários que os scan devem ser iniciados, podendo ser em um único horário ou agendado com frequências.



Schedule

ONCE   HOURLY   DAILY   WEEKLY   BIWEEKLY   MONTHLY   YEARLY

Sunday    Monday    Tuesday    Wednesday

Thursday    Friday    Saturday

Starts at 13:39

Allow load spread within the hour

Cron format: 39 13 \* \* 2,5

- **Credencial (Credentials)**

- Sem autenticação a plataforma irá realizar um scan pela rede tentando descobrir as tecnologias e vulnerabilidades da mesma forma que um atacante iria realizar o ataque (similar ao *Blackbox*). Habilitando as opções de credencial, a plataforma permite realizar o scan de forma autenticada (similar ao *WhiteBox*), podendo assim conhecer melhor o sistema e verificar configurações adicionais (*local security checks*).
- A quantidade de itens adicionais que serão verificados localmente no host dependem de uma série de fatores:
  - permissões do usuário, recomenda-se que esse usuário tenha a máxima permissão de leitura e auditoria do host de destino, quanto mais permissões o usuário tiver maior será a quantidade de verificações que serão possíveis realizar.
  - *Hardening* de segurança são importantes, mas muitas vezes podem limitar as verificações que estão sendo realizadas, para isso é importante permitir os acessos para o usuário que estiver sendo utilizado para o scan;
  - Novas vulnerabilidades são descobertas diariamente e essas podem necessitar de novas permissões para serem identificadas, caso o usuário já não tenha essa permissão.
- A autenticação pode ser realizada para:
  - SMB:** para sistemas operacionais Windows;

- 

- - **SSH:** para sistemas operacionais Linux, com opção de utilizar senha ou certificado e também a elevação de privilégios;
  - **ESX:** para sistemas da VMware;
- Para selecionar uma credencial, primeiro ela precisa estar cadastrada no cofre de credenciais da plataforma ou configurada em um dos conectores de cofres de senhas externos suportados. Veja mais detalhes na documentação do menu **Configurações > Credenciais**.
- Após os scan realizado, a plataforma permite visualizar as informações em diferentes formatos, com gráficos, relatórios e opção de exportar para CSV.

## Autenticação em Ativos

A plataforma da Rainforest realiza a varredura com ou sem autenticação. Quando é possível autenticar no dispositivo, obtemos uma quantidade maior de informações, por exemplo, quais são as tecnologias instaladas no asset. Isso possibilita também o cruzamento de informações de tecnologias que estão presentes no dispositivo com a base de vulnerabilidades armazenada na plataforma da Rainforest, evitando assim pontos cegos.

# TTP (Tactics, Techniques and Procedures)

---

 support.rainforest.tech/pt-br/kb/referencia-ttp

## Compreenda as táticas, técnicas e procedimentos envolvidos em uma cadeia de ataques cibernéticos

---

### O que é TTP?

---

Em cibersegurança, TTP é uma sigla que se refere a Táticas, Técnicas e Procedimentos (em inglês, Tactics, Techniques, and Procedures). Essa terminologia é frequentemente usada para descrever as diferentes abordagens e estratégias que os atacantes cibernéticos empregam ao realizar atividades maliciosas, como invasões, ataques de phishing, exploração de vulnerabilidades e outras atividades relacionadas à segurança cibernética.

Aqui está uma breve explicação de cada componente das TTP em cibersegurança:

- **Táticas (Tactics):** São as estratégias gerais ou os objetivos de um atacante cibernético. Isso inclui o que eles estão tentando alcançar, como roubar dados, interromper serviços ou comprometer sistemas.
- **Técnicas (Techniques):** As técnicas são as maneiras específicas pelas quais os atacantes realizam suas táticas. Isso envolve os métodos e ferramentas que eles usam para atingir seus objetivos. Por exemplo, uma técnica comum é usar malware para infectar um sistema alvo.
- **Procedimentos (Procedures):** Os procedimentos são os passos detalhados que os atacantes seguem para implementar suas técnicas. Isso pode incluir etapas específicas, como enviar um e-mail de phishing para um alvo, explorar uma vulnerabilidade conhecida ou usar credenciais roubadas para obter acesso a sistemas.

O entendimento das TTP é fundamental para os profissionais de segurança cibernética, pois ajuda a identificar e responder a ameaças de maneira mais eficaz. Ao analisar as TTP usadas por atacantes conhecidos ou grupos de ameaças, as organizações podem desenvolver estratégias de defesa mais sólidas, identificar indicadores de comprometimento (IoCs) e ajustar suas políticas de segurança para proteger melhor seus ativos de informações contra ataques cibernéticos.

### Como consultar a base TTP na plataforma Rainforest?

---

A plataforma Rainforest oferece internamente o framework de técnicas e suas combinações usadas em ataques cibernéticos desenvolvida pela Mitre Corporation. Para consultar acesse o menu **Referência > TTPs**.



The screenshot displays the Rainforest Tech dashboard. On the left is a sidebar menu with the following items: Inteligência de Marca, Inteligência de Vulnerabilidade, Fraude, Vazamento, Cloud, Infra, App, Referência (highlighted with a red box), CVEs, and TTPs (highlighted with a red box). The main content area shows:

- 0/100** Nota da Empresa (with a gauge and 'F' indicator)
- 9100** Credenciais (with a gauge and envelope icon)
- Vulnerabilidades** section with three boxes:
  - Crítica**: 158 Ativos, 308 Vulns
  - Alta**: 67 Ativos
- Probabilidade por CVE** section with a horizontal scale and a vertical line at 7, with the text "Planeje corrigir" above it.

Com isso você terá disponível internamente na plataforma para consulta toda a base de técnicas utilizadas, podendo por exemplo selecionar grupos específicos e identificar quais técnicas ele utilizam em seus ataques.

- Inteligência de Marca
- Inteligência de Vulnerabilidade
- Fraude
- Vazamento
- Cloud
- Infra
- App
- Referência**
- CVEs
- TTPs
- Notícias
- API
- Configurações
- Admin

Táticas, Técnicas e Procedimentos

MITRE ATTACK Framework

Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 13 techniques	Defense Evasion 35 techniques	Credential Access 16 techniques	Discovery 26 techniques	Lateral Movement 9 techniques	Collection 15 techniques	Command and Control 16 techniques	Exfiltration 8 techniques
Drive-by Compromise	Command and Scripting Interpreter (2/7)	Account Manipulation (0/3)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/3)	Account Discovery (2/3)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (3/4)	Automated Exfiltration
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (2/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (1/3)	Communication Through Removable Media	Data Transfer Size Limit
External Remote Services	Inter-Process Communication (0/7)	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Credentials from Password Stores (1/7)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Exfiltration Over Alternating Protocols	Exfiltration Over Network
Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Debugger Evasion	Exploitation for Credential Access	Debugger Evasion	Remote Service Session Hijacking (0/2)	Automated Collection	Data Encoding (0/2)	Exfiltration Over C2 Channel
Phishing (1/3)	Scheduled Task/Job (1/4)	Browser Extensions	Create or Modify System Process (0/4)	Deobfuscate/Decode Files or Information	Forced Authentication	Domain Trust Discovery	Remote Services (3/6)	Browser Session Hijacking	Data Obfuscation (0/3)	Exfiltration Over OOB HTTP
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Domain Policy Modification (0/2)	Direct Volume Access	Forge Web Credentials (0/2)	File and Directory Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (0/3)	Exfiltration Over Network Medium
Supply Chain Compromise (0/2)	System Services (1/2)	Create Account (0/2)	Escape to Host	Execution Guardrails (0/1)	Input Capture (1/4)	Group Policy Discovery	Data from Information Repositories (1/1)	Data from Local System	Encrypted Channel (0/2)	Exfiltration Over Physical Medium
Trusted Relationship	User Execution (0/2)	Create or Modify System Process (0/4)	Event Triggered Execution (0/16)	Exploitation for Defense Evasion	Modify Authentication Process (1/7)	Network Service Discovery	Software Deployment Tools	Data from Network Shared Drive	Fallback Channels	Exfiltration Over Web Service (1)
Valid Accounts	Windows Management Instrumentation	Event Triggered Execution (0/16)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (0/2)	Multi-Factor Authentication Interception	Network Share Discovery	Taint Shared Content	Data from Removable Media	Ingress Tool Transfer	Schedule Transfer
	External Remote Services	Hijack Execution Flow (1/12)	Hijack Execution Flow (1/12)	Hide Artifacts (0/10)	Multi-Factor Authentication Request Generation	Network Sniffing	Use Alternate Authentication Material (1/2)	Data Staged (2/2)	Non-Application Layer Protocol	
	Hijack Execution Flow (1/12)	Process Injection (0/12)	Process Injection (0/12)	Impair Defenses (0/8)	Multi-Factor Authentication Request Generation	Peripheral Device Discovery		Email Collection (2/3)	Non-Standard Port	
	Scheduled Task/Job (1/4)	Modify Authentication Process (1/7)	Scheduled Task/Job (1/4)	Indicator Removal (3/9)	Network Sniffing	Permission Groups Discovery (1/2)		Input Capture (1/4)	Protocol Tunneling	
	Office Application Startup (0/6)	Valid Accounts (1/1)	Valid Accounts (1/1)	Indirect Command Execution	OS Credential Dumping (1/8)	Process Discovery		Screen Capture	Proxy (0/4)	
	Pre-OS Boot (0/3)			Masquerading (1/8)	Steal or Forge Authentication Certificates	Query Registry		Video Capture	Remote Access Software	
	Scheduled Task/Job (1/4)			Modify Authentication Process (1/7)	Steal or Forge Kerberos Tickets (0/4)	Remote System Discovery			Traffic Signaling (0/2)	
	Server Software Component (0/5)			Modify Registry	Steal Web Session Cookie	Software Discovery (0/1)			Web Service (0/3)	
	Traffic Signaling (0/2)			Obfuscated Files or Information (1/11)	Plist File Modification	System Information Discovery				
	Valid			Plist File Modification	Pre-OS Boot (0/3)	System Location Discovery (0/1)				
				Process Injection (0/12)	Unsecured Credentials (0/5)	System Network				

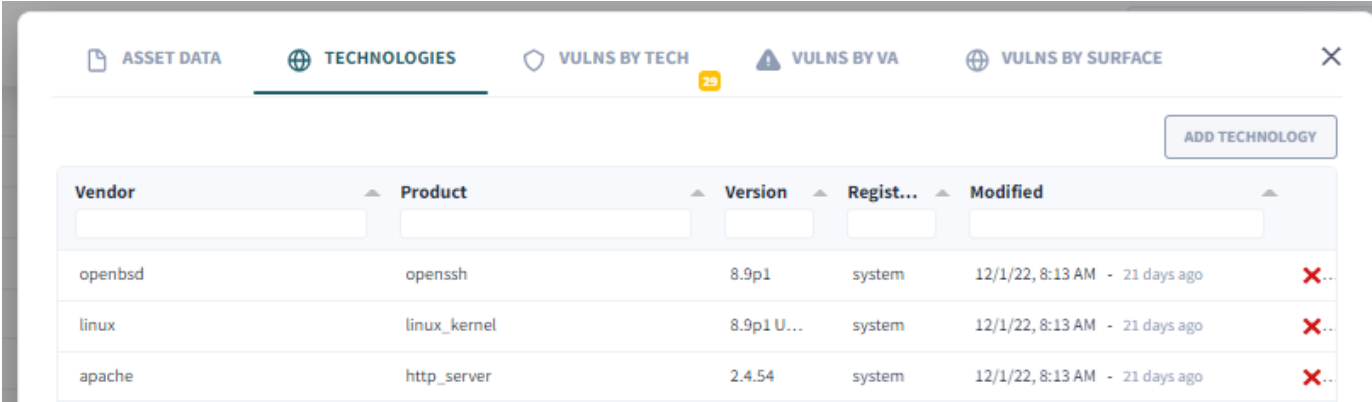
Feedback

# Vulnerabilidades By-Tech (Tecnologias)

 support.rainforest.tech/pt-br/kb/scan-by-tech

## Scan de Vulnerabilidades por Tecnologia

A plataforma da Rainforest permite identificar automaticamente versões dos softwares em execução em cada servidor, sistemas operacionais, banco de dados. Tanto pela rede quanto autenticado e a partir da lista das versões gera a lista de vulnerabilidades que afetam esses softwares e exibi junto com as demais vulnerabilidade nos relatórios.



Vendor	Product	Version	Regist...	Modified	
openbsd	openssh	8.9p1	system	12/1/22, 8:13 AM - 21 days ago	✖
linux	linux_kernel	8.9p1 U...	system	12/1/22, 8:13 AM - 21 days ago	✖
apache	http_server	2.4.54	system	12/1/22, 8:13 AM - 21 days ago	✖

Além da identificação automática realizada toda vez que as análises são executadas, a plataforma realiza o cruzamento das tecnologias identificadas com as vulnerabilidades catalogadas, indicando possíveis vulnerabilidades no ambiente sem a necessidade de execução das análises, consequentemente sem a geração de tráfego no ambiente

## Cadastrando Tecnologias Manualmente

Além de realizar a identificação automática das tecnologias usadas nos ativos, é possível realizar o cadastro manual.

Para isso temos que acessar o ativo no qual queremos cadastrar a tecnologia, para isso acesse o menu **Infra > Ativos**, na listagem dos ativos, clique sobre o desejado.

The screenshot shows the RAINFOREST dashboard. On the left is a navigation menu with categories like 'Inteligência de Marca', 'Inteligência de Vulnerabilidade', 'Fraude', 'Vazamento', 'Cloud', and 'Infra'. The 'Infra' category is selected. The main area features a risk score chart with a score of 8 and a recommendation to 'Corrigir mais tarde'. To the right, there are alerts for 'Expired SSL Certificate [Low]' and 'Revoked SSL Certificate - Detect [Low]'. Below the chart is a table of assets:

#	ID	Tipo	Nome	IP	Network	Exposto a	Impacto nos N...	Ambiente
1	26	Ativo único						production
2	885047	Ativo único						production
3	35	Ativo único						production
4	34	Ativo único						production
5	33	Ativo único						production
6	32	Ativo único						production
7	31	Ativo único						production
8	30	Ativo único						production
9	29	Ativo único						production
10	28	Ativo único						production

Depois de acessar o ativo desejado, clique na aba **Tecnologias**, posteriormente clique em **Adicionar Tecnologia**.

The screenshot shows the 'Tecnologias' tab selected in the asset details view. The 'ADICIONAR TECNOLOGIA' button is highlighted. Below it is a table with the following columns: Fornecedor, Produto, Versão, Regist..., and Modificado.

Fornecedor	Produto	Versão	Regist...	Modificado
nginx	nginx	1.18.0	system	5/13/21, 11:33 PM
jenkins	jenkins	2.263.4	system	5/13/21, 11:33 PM
iattv	edlinc	9.4.33.2020	system	3/17/21 10:22 PM

Preencha as informações de **Fornecedor**, **Produto** e **Versão**, depois clique em **Adicionar**. A tecnologia será adicionada no ativo desejado.

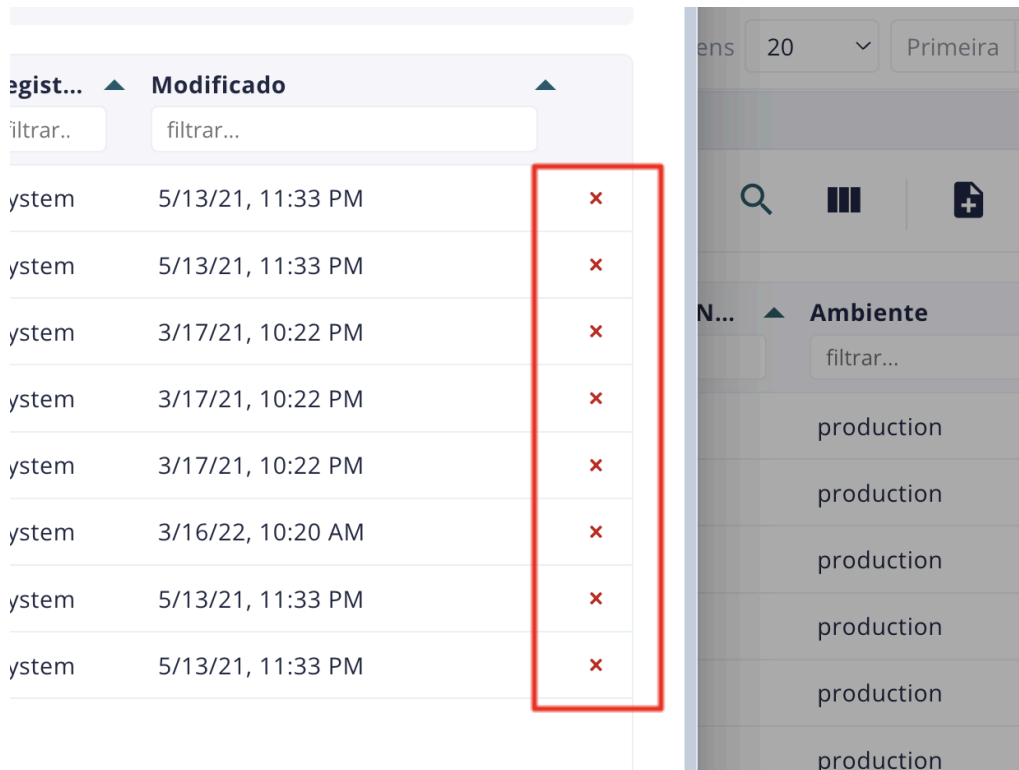
The screenshot shows the 'Adicionar Tecnologia' form with the following fields:

- Fornecedor**: A text input field with a search icon and a dropdown arrow.
- Produto**: A dropdown menu.
- Versão**: A dropdown menu.

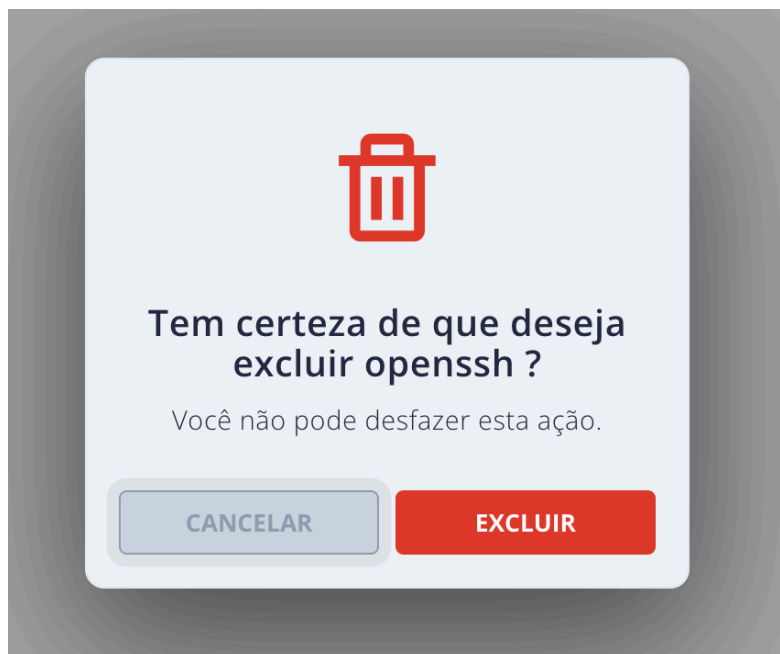
Buttons for 'CANCELAR' and 'ADICIONAR' are visible at the top right of the form.

## Excluindo Tecnologias

Caso seja necessário excluir uma tecnologia listada, clique no ícone de exclusão ( X ) localizado no final da linha de cada tecnologia.



Posteriormente clique em **Excluir**.



# Cadastro de Ativos

 support.rainforest.tech/pt-br/kb/cadastro-ativos

## Veja como realizar o cadastro de ativos/redes dentro da plataforma Rainforest.

Para empresas que tenham em seu portal o módulo **Infra** da Rainforest habilitado, elas tem a possibilidade de realizar o cadastro de ativos e de redes manualmente. Veremos a seguir como realizar o cadastro e suas particularidades.

Para acessar a tela de cadastro acesse o menu **Infra > Ativos > Novo Ativo**




The screenshot shows the Rainforest platform interface. On the left, there is a navigation menu with the following items: Inteligência de Marca, Inteligência de Vulnerabilidade, Fraude, Vazamento, Cloud, and Infra (highlighted with a red box). Below the menu, there are sections for Dashboard, Ativos (highlighted with a red box), and Nota da Empresa. The main content area displays a risk score chart with a score of 5 and a recommendation to 'Corrigir mais tarde'. Below the chart, there is a table of assets with the following columns: #, ID, Tipo, Nome, IP, Network, Exposto a, and Impacto nos I. The table contains two rows of data, both of which are redacted with orange bars. A 'Novo Ativo' button is highlighted with a red box in the top right corner of the main content area.

Acessando o menu teremos a tela de cadastro de ativos com seus respectivos campos, veremos abaixo quais são:

- **Nome do Ativo**
- **Tipo de Ativo**
  - **Ativo Único:** cadastre um único dispositivo informando seu endereço IP
  - **Network:** cadastre um endereço de rede para que a plataforma identifique todos os ativos da rede
- **Endereço IP** ou **Endereço de Rede:** conforme o que for selecionado no campo **Tipo de Ativo**.
- **Departamento**
- **Coordenadas** (localização geográfica)
- **Network:** selecione uma rede para os casos de cadastro de ativos únicos

- **Exposto a:**
  - Web
  - Internal
  - None
- **Impacto nos Negócios**
  - Crítica
  - Alta
  - Média
  - Baixa
- **Ambiente:**
  - Desenvolvimento
  - Teste
  - Produção
- **Descrição**
- **Tecnologies Discovery:** para casos de cadastro de ativos únicos ative essa opção caso queira que a plataforma da Rainforest identifique as tecnologias que são utilizadas no ativo que esta sendo cadastro
  - Frequência:** se habilitado o campo **Tecnologies Discovery**, defina a frequência na qual a plataforma realizará o scan de tecnologias.
- **Hosts Discovery:** nos casos de cadastro de redes, a plataforma disponibilizará esse parâmetro para que, se habilitado, faça a descoberta de ativos presente na rede cadastrada.
- **Labels**

Nome do Ativo	Tipo de Ativo	Endereço de rede
<input type="text"/>	Network	000.000.000.0/00
Departamento	Coordenadas	Network
<input type="text"/>	Latitude, longitude Ex.: 38.12024, -122.039998	Selecione uma rede
Exposto a	Impacto nos Negócios	Ambiente
Internal	Média	Produção
Descrição		
<input type="text"/>		
<input checked="" type="checkbox"/> Technologies Discovery	Frequência	
<input checked="" type="checkbox"/> Hosts Discovery	Seven days	
Labels		GERENCIAR RÓTULOS
<div> Nenhum rótulo foi atribuído a este recurso ainda. Clique no botão acima para gerenciar rótulos.</div>		

Preencha as informações necessárias para o seu cadastro atual e clique em **Salvar**. A partir desse momento a plataforma identificará esse ativo/rede e começará a fazer suas análises para identificação de vulnerabilidades.

# CVE (Common Vulnerabilities and Exposures)

---

 support.rainforest.tech/pt-br/kb/referencia-cve

## Conheça o que são e como utilizar as CVE's na plataforma Rainforest

---

### O que é CVE?

---

CVE ou *Common Vulnerabilities and Exposures* (Exposições e Vulnerabilidades Comuns) é um banco de dados que registra e referencia vulnerabilidades e exposições conhecidas publicamente relacionadas à segurança da informação.

As CVE's são identificadas através de um número que é único para cada uma delas. Tal identificador apresenta em qual ano aquela vulnerabilidade foi catalogada, por exemplo, **CVE-2021-44228** que faz referência a vulnerabilidade Log4js.

A CVE pode ter uma nota atribuída que indica qual a sua severidade. Essa nota é atribuída através de uma conhecida por CVSS (*Common Vulnerability Scoring System*)

### Como as CVE's são Referenciadas na Plataforma Rainforest?

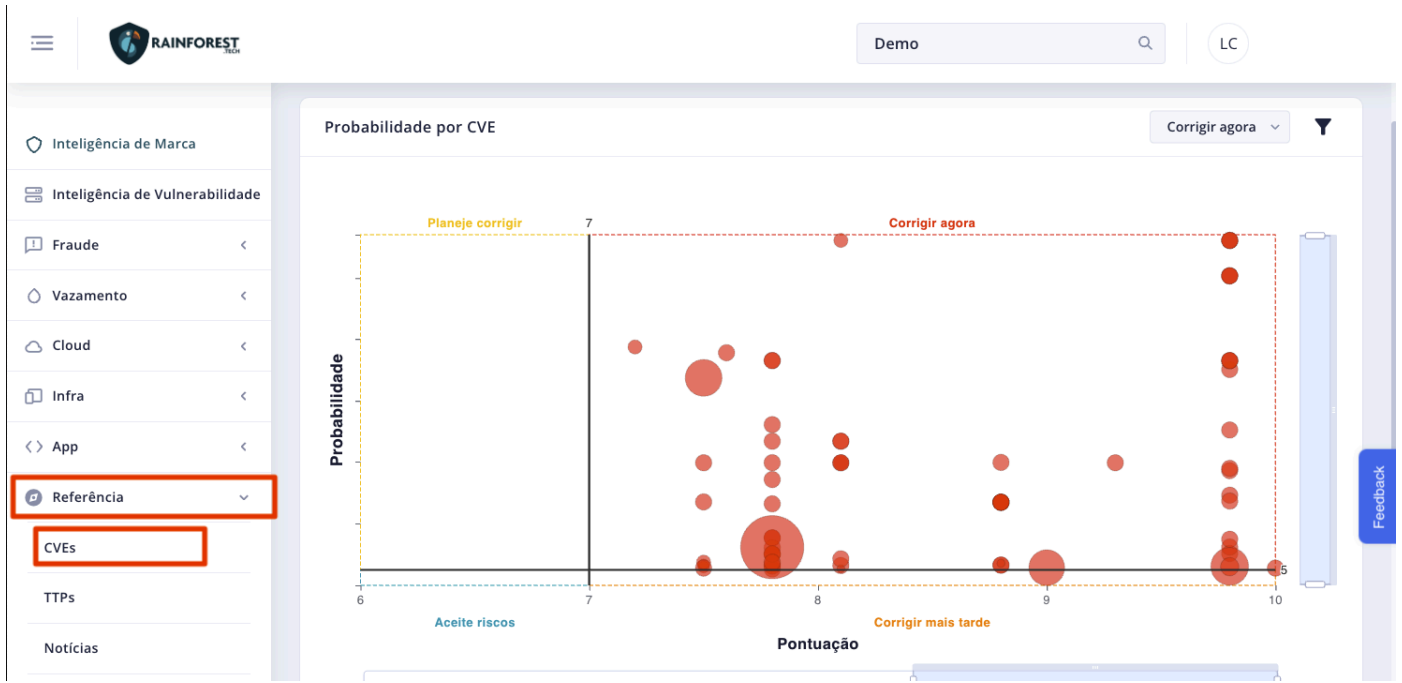
---

A plataforma Rainforest sincroniza as CVE's periodicamente com a base **NVD** (*National Vulnerability Database*) do **NIST** (*National Institute of Standards and Technology*).

Tais informações são utilizadas para correlacionar vulnerabilidade de ativos e aplicações com o objetivo de suportar uma gestão de vulnerabilidades do ambiente.

Ao ter uma relação de Exposições e Vulnerabilidades confiáveis pode-se utilizar estes dados para priorização das vulnerabilidades mais críticas e/ou com vulnerabilidades que afetam um número maior de aplicações/dispositivos.

Para acessar o menu com a base de CVEs, acesse o menu **Referência > CVEs**



Acessando o menu você verá ter disponível duas abas,

- **ALL CVEs:** listagem de todas as CVEs publicadas.

CVEs ↓

**ALL CVEs**    **AFFECTED ASSETS CVEs** 4337

Nome	Pontuação	Severidade	Fornecedor	Known Exploits	Descrição	Últim
<input type="text" value="filtrar..."/>	<input type="text" value="filtrar..."/>	<input type="text" value="filtrar..."/>	<input type="text" value="filtrar..."/>		<input type="text" value="filtrar..."/>	<input type="text" value="filtrar..."/>
CVE-2023-32236		Não disponível		0	Unauth. Reflected Cross-Site Scripting (XSS) v	8/23.
CVE-2023-32496		Não disponível		0	Auth. (admin+) Stored Cross-Site Scripting (XS	8/23.
CVE-2023-32497		Não disponível		0	Auth. (admin+) Stored Cross-Site Scripting (XS	8/23.
CVE-2023-32498		Não disponível		0	Auth. (admin+) Stored Cross-Site Scripting (XS	8/23.
CVE-2023-32499		Não disponível		0	Unauth. Reflected Cross-Site Scripting (XSS) v	8/23.
CVE-2023-28994		Não disponível		0	Unauth. Reflected Cross-Site Scripting (XSS) v	8/23.
CVE-2023-32300		Não disponível		0	Unauth. Reflected Cross-Site Scripting (XSS) v	8/23.

- **AFFECTED ASSETS CVEs:** listagem de CVEs publicadas que afetam dispositivos e/ou aplicações cadastradas na plataforma da Rainforest.

CVEs



ALL CVEs    **AFFECTED ASSETS CVEs** 4337

Nome	Pontuação	Severidade	Fornecedor	Ativos afetados	Known Exploits	Probabilidade	Descrição
<input type="text" value="filtrar..."/>	<input type="text" value="filtrar..."/>	<input type="text" value="filtrar..."/>	<input type="text" value="filtrar..."/>				<input type="text" value="filtrar..."/>
CVE-2023-35359	7.8	HIGH	microsoft	4	0	2896	Windows Ke
CVE-2023-35376	6.5	MEDIUM	microsoft	4	0	0	Microsoft M
CVE-2023-35377	6.5	MEDIUM	microsoft	4	0	0	Microsoft M
CVE-2023-35379	7.8	HIGH	microsoft	4	0	0	Reliability A
CVE-2023-35380	7.8	HIGH	microsoft	4	0	2896	Windows Ke
CVE-2023-35381	8.8	HIGH	microsoft	4	0	0	Windows Fa
CVE-2023-35383	7.5	HIGH	microsoft	4	0	0	Microsoft M
CVE-2023-35384	6.5	MEDIUM	microsoft	4	0	0	Windows HT
CVE-2023-35385	9.8	CRITICAL	microsoft	4	0	2895	Microsoft M
CVE-2023-36876	7.1	HIGH	microsoft	4	0	0	Reliability A

Ao acessar uma CVE publicada, a plataforma apresenta maiores detalhes e correlações, como por exemplo ativos e/ou aplicações registradas no Rainforest que podem estar sendo impactadas pela CVE.

- **Dados CVE:** principais informações sobre a CVE publicada, dentre elas temos pontuação, severidade, vetor de ataque, impacto de confidencialidade, data de publicação, produtos afetados, entre outros.

CVE-2023-35385
✕

DADOS CVE
 ATIVOS AFETADOS 4
 APLICAÇÕES AFETADAS
 EXPLOITS

---

Pontuação <span style="background-color: #f00; color: white; padding: 2px 5px; border-radius: 3px;">9.8</span>	Severidade <span style="background-color: #f00; color: white; padding: 2px 5px; border-radius: 3px;">CRÍTICA</span>	Pontuação de Explorabilidade <span style="background-color: #0070c0; color: white; padding: 2px 5px; border-radius: 3px;">3.9</span>	Pontuação de Impacto <span style="background-color: #ffc000; color: white; padding: 2px 5px; border-radius: 3px;">5.9</span>	Vetor de Ataque <span style="background-color: #0070c0; color: white; padding: 2px 5px; border-radius: 3px;">REDE</span>	Complexidade de Ataque <span style="background-color: #0070c0; color: white; padding: 2px 5px; border-radius: 3px;">BAIXA</span>
Privilégios Necessários <span style="background-color: #90ee90; color: white; padding: 2px 5px; border-radius: 3px;">NENHUM</span>	Interação com o Usuário <span style="background-color: #0070c0; color: white; padding: 2px 5px; border-radius: 3px;">NENHUM</span>	Escopo <span style="background-color: #0070c0; color: white; padding: 2px 5px; border-radius: 3px;">INALTERADO</span>	Impacto de Confidencialidade <span style="background-color: #ffc000; color: white; padding: 2px 5px; border-radius: 3px;">ALTA</span>	Impacto de Integridade <span style="background-color: #ffc000; color: white; padding: 2px 5px; border-radius: 3px;">ALTA</span>	Impacto da Disponibilidade <span style="background-color: #ffc000; color: white; padding: 2px 5px; border-radius: 3px;">ALTA</span>

Descrição  
**Microsoft Message Queuing Remote Code Execution Vulnerability**

Referências  
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35385>

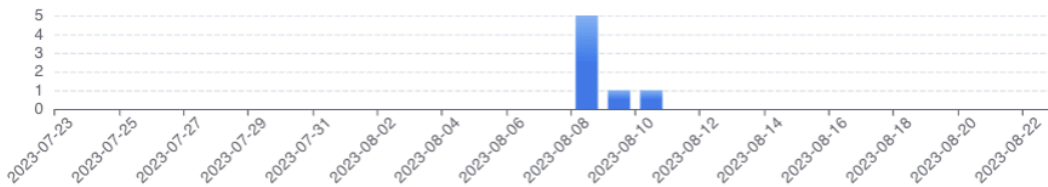
Publicado

**August 8, 2023** - 06:15 PM - há 15 dias

Modificado

**August 10, 2023** - 08:39 PM - há 13 dias

### Tendências de Vulnerabilidade



### Produtos Afetados Conhecidos

Fornecedor ▲	Produto ▲	Versões ▲
<input type="text" value="filtrar..."/>	<input type="text" value="filtrar..."/>	<span>Apenas ▲</span> <span>De (incluindo) ▲</span> <span>Até (incluindo) ▲</span> <span>De (excluindo) ▲</span> <span>Até (excluin... ▲</span>

- **Ativos Afetados:** dispositivos cadastrados na plataforma que estão sendo afetados pela vulnerabilidade publicada.

CVE-2023-35385 X

DADOS CVE
**ATIVOS AFETADOS** 4
APLICAÇÕES AFETADAS
EXPLOITS
↓

Ativo	Descrição	IP	Localização
<input type="text" value="filtrar..."/>	<input type="text" value="filtrar..."/>	<input type="text" value="filtrar..."/>	<input type="text" value="filtrar..."/>
[REDACTED]	-	[REDACTED]	[REDACTED]_2008:r2
[REDACTED]	-	[REDACTED]	[REDACTED]_server_2008:r2
[REDACTED]	-	[REDACTED]	[REDACTED]ws_server_2008:r2
[REDACTED]	-	[REDACTED]	[REDACTED]ndows_server_2008:r2

- **Aplicações Afetadas:** aplicações cadastradas na plataforma que estão sendo afetadas pela vulnerabilidade publicada.

CVE-2022-25883 X

DADOS CVE
ATIVOS AFETADOS
**APLICAÇÕES AFETADAS** 1
EXPLOITS
↓

App	Grupo	URL
<input type="text" value="filtrar..."/>	<input type="text" value="filtrar..."/>	<input type="text" value="filtrar..."/>
ter [REDACTED]	[REDACTED]	https://github.c [REDACTED]

- **Exploits:** explorações realizadas e divulgadas no site **exploit-db-com** que estão relacionadas a respectiva CVE.

CVE-2019-0708
✕

📄 DADOS CVE
📁 ATIVOS AFETADOS 4
📁 APLICAÇÕES AFETADAS
🗨️ EXPLOITS 9
⬇️

Nome	URL	Criado
<input type="text" value="filtrar..."/>	<input type="text" value="filtrar..."/>	<input type="text" value="filtrar..."/>
Microsoft Windows Remote Desktop - 'BlueKeep' Denial of	<a href="https://www.exploit-db.com/exploits/46946">https://www.exploit-db.com/exploits/46946</a>	6/26/22, 6:24 AM
Analysis of CVE-2019-0708 (BlueKeep)	<a href="https://www.exploit-db.com/exploits/46947">https://www.exploit-db.com/exploits/46947</a>	6/26/22, 6:24 AM
Microsoft Windows Remote Desktop - 'BlueKeep' Denial of	<a href="https://www.exploit-db.com/exploits/47120">https://www.exploit-db.com/exploits/47120</a>	6/26/22, 6:26 AM
BlueKeep - Technical Analysis (Potential Path For Exploitati	<a href="https://www.exploit-db.com/exploits/47156">https://www.exploit-db.com/exploits/47156</a>	6/26/22, 6:26 AM
Low-level Reversing of BLUEKEEP vulnerability (CVE-2019-0	<a href="https://www.exploit-db.com/exploits/47245">https://www.exploit-db.com/exploits/47245</a>	6/26/22, 6:27 AM
Exploitation of Windows CVE-2019-0708 (BlueKeep): Three '	<a href="https://www.exploit-db.com/exploits/47336">https://www.exploit-db.com/exploits/47336</a>	6/26/22, 6:28 AM
BlueKeep: A Journey from DoS to RCE (CVE-2019-0708)	<a href="https://www.exploit-db.com/exploits/47360">https://www.exploit-db.com/exploits/47360</a>	6/26/22, 6:28 AM
Microsoft Windows - BlueKeep RDP Remote Windows Kerni	<a href="https://www.exploit-db.com/exploits/47416">https://www.exploit-db.com/exploits/47416</a>	6/26/22, 6:29 AM
Microsoft Windows 7 (x86) - 'BlueKeep' Remote Desktop Pr	<a href="https://www.exploit-db.com/exploits/47683">https://www.exploit-db.com/exploits/47683</a>	6/26/22, 6:32 AM

## Histórico de Vulnerabilidades

Na plataforma da Rainforest, temos a possibilidade de consultar o histórico de vulnerabilidades divulgadas pelo **NIST** por tecnologia. Deste modo os usuários podem ter acesso a primeira versão com criticidade por exemplo.

Acesse o menu **Referência > CVEs**, na coluna **Fornecedor**, pesquise pelo fabricante desejado, neste exemplo pesquisaremos por **Microsoft**. Com isso teremos todo o histórico de CVEs publicadas por fornecedor e suas respectivas tecnologias.



- Inteligência de Marca
- Inteligência de Vulnerabilidade
- Fraude
- Vazamento
- Cloud
- Infra
- App
- Referência**
- CVEs**
- TTPs
- Notícias
- API
- Configurações
- Admin

### CVEs



TODOS OS CVEs

CVEs DE ATIVOS AFETADOS

4394

Nome	Pontuação	Severidade	Fornecedor	Exploits Conhecidos	Descrição	Última atualização
filtrar...	filtrar...	filtrar...	microsoft		filtrar...	filtrar...
CVE-2020-19725	7.8	HIGH	microsoft	0	There is a use-after-free vulnerability in file p	8/25/23, 2:46 AM
CVE-2023-36787	8.8	HIGH	microsoft	0	Microsoft Edge (Chromium-based) Elevation of	8/24/23, 9:39 PM
CVE-2023-38158	3.1	LOW	microsoft	0	Microsoft Edge (Chromium-based) Informatio	8/24/23, 9:39 PM
CVE-2023-21709	9.8	CRITICAL	microsoft	0	Microsoft Exchange Server Elevation of Privile	8/10/23, 6:29 PM
CVE-2023-29328	8.8	HIGH	microsoft	0	Microsoft Teams Remote Code Execution Vuln	8/10/23, 6:42 PM
CVE-2023-29330	8.8	HIGH	microsoft	0	Microsoft Teams Remote Code Execution Vuln	8/10/23, 6:42 PM
CVE-2023-35359	7.8	HIGH	microsoft	0	Windows Kernel Elevation of Privilege Vulneri	8/10/23, 6:33 PM
CVE-2023-35368	8.8	HIGH	microsoft	0	Microsoft Exchange Remote Code Execution \	8/11/23, 3:58 PM
CVE-2023-35371	7.8	HIGH	microsoft	0	Microsoft Office Remote Code Execution Vuln	8/10/23, 6:29 PM
CVE-2023-35372	7.8	HIGH	microsoft	0	Microsoft Office Visio Remote Code Executio	8/10/23, 6:32 PM
CVE-2023-35376	6.5	MEDIUM	microsoft	0	Microsoft Message Queuing Denial of Service	8/10/23, 8:26 PM
CVE-2023-35377	6.5	MEDIUM	microsoft	0	Microsoft Message Queuing Denial of Service	8/10/23, 8:27 PM
CVE-2023-35378	7	HIGH	microsoft	0	Windows Projected File System Elevation of P	8/10/23, 6:27 PM
CVE-2023-35379	7.8	HIGH	microsoft	0	Reliability Analysis Metrics Calculation Engine	8/10/23, 6:22 PM

Mostrando 1 a 250 de 10858 itens

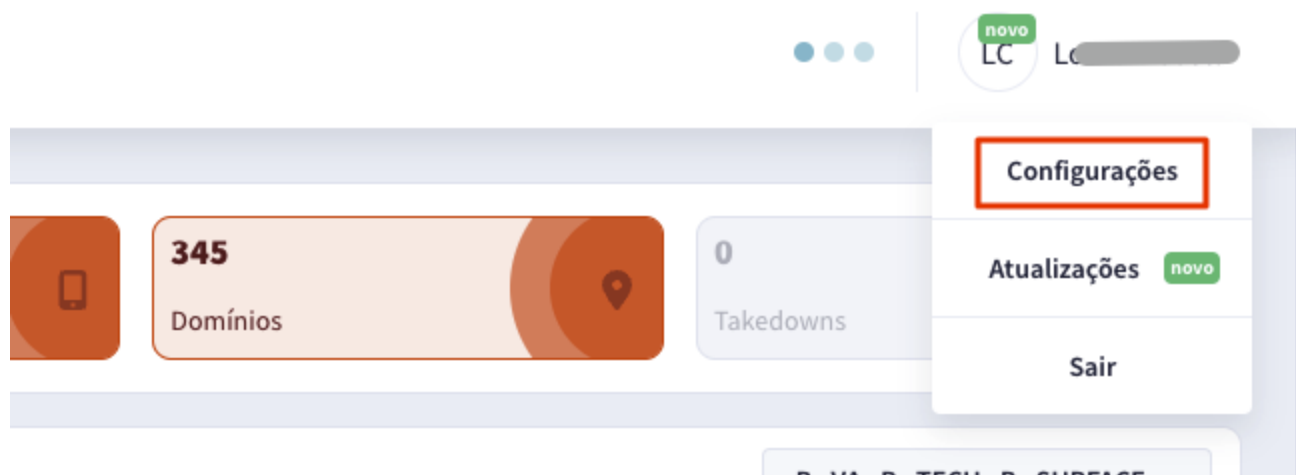
250 Primeira Ant. 1 2 3 4 5 Próx. Última

# Alterar idioma da interface

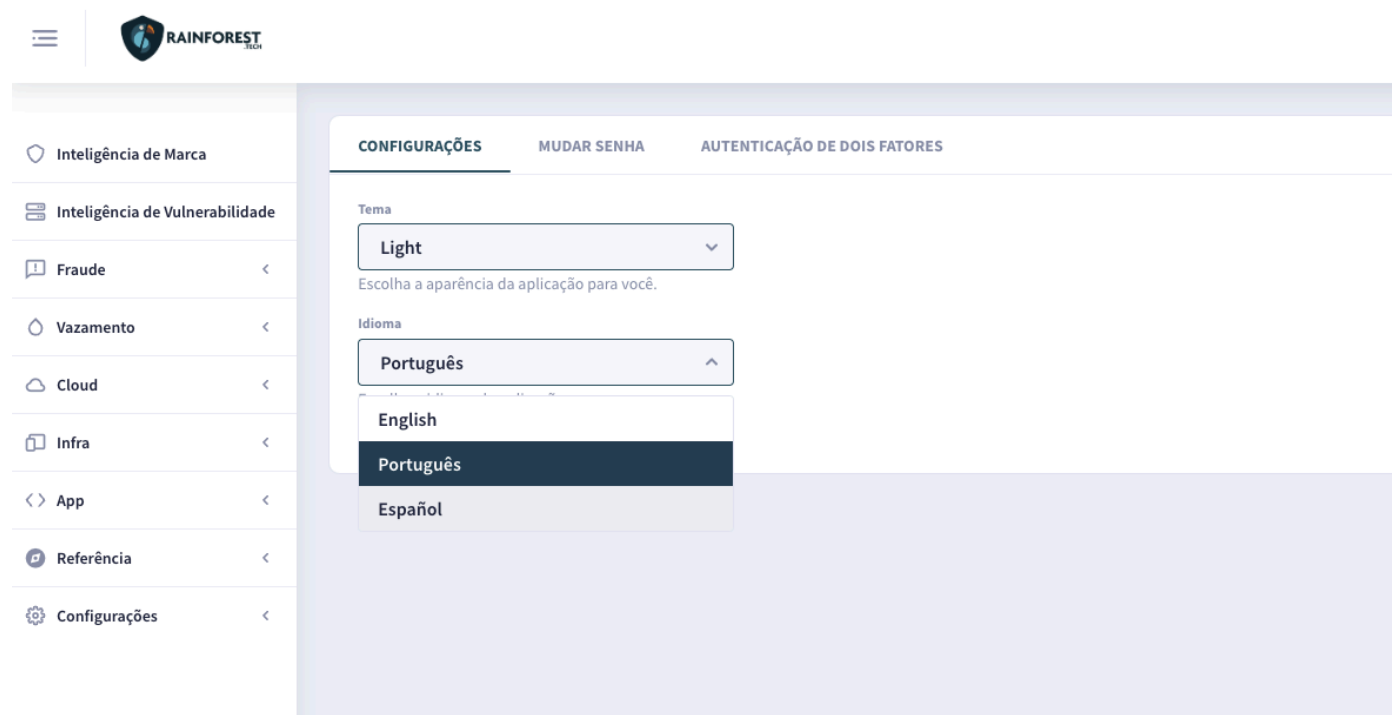
 support.rainforest.tech/pt-br/kb/alterar-idioma-interface

## Aprenda como alterar o idioma da interface Rainforest!

Cada usuário do Rainforest pode alterar o idioma da interface. Podemos alterar de duas formas, a primeira consiste ir em nas configurações de usuário, **Nome do Usuário > Configurações**.



Na aba **Configurações**, clique no botão idioma e selecione a opção desejada.



**Observação:** atualmente temos disponíveis os idiomas espanhol, inglês e português.

Após selecionar o idioma desejado, a interface atualizará automaticamente para o novo idioma.

Uma outra forma de realizar a alteração do idioma da interface é através do rodapé da interface. No final de todas as telas do Rainforest, no canto inferior direito, você verá o idioma atualmente selecionado.

Para realizar a alteração, basta clicar sobre o idioma apresentando e selecionar a nova opção desejada.

The screenshot displays the Rainforest application interface. On the left is a sidebar with navigation options: Brand Intelligence, Vulnerability Intelligence, Fraud, Leak, Code, Credentials, Takedown Requests, Cloud, Infra, App, Reference, and Settings. The main content area features a timeline at the top and a 'Latest feeds' section with several news items. At the bottom right, there is a language selection dropdown menu currently set to 'English'.

© All rights reserved.

English

# Visão Geral Infra

---

 [support.rainforest.tech/pt-br/kb/visao-geral-infra](https://support.rainforest.tech/pt-br/kb/visao-geral-infra)

## **Receba atualizações em tempo real sobre vulnerabilidades em sua infraestrutura, cobrindo pontos cegos que podem aparecer entre scans.**

---

Enquanto as organizações se esforçam para reduzir sua suscetibilidade a ataques, não é incomum que implementem várias soluções para diferentes propósitos. No entanto, isso pode levar ao acúmulo de milhares de informações desconectadas, dificultando o acompanhamento de tudo pelas equipes responsáveis pela proteção de ativos digitais.

O módulo Rainforest Infra oferece uma abordagem abrangente e integrada para a detecção de vulnerabilidades que ajuda a orientar as equipes de segurança e conformidade em relação a possíveis vulnerabilidades com base em sua importância para os negócios.

Sempre que ocorre uma nova busca por vulnerabilidades, a plataforma identifica aquelas que foram detectadas em varreduras anteriores e que não foram identificadas na mais recente, removendo-as da listagem de vulnerabilidades. Isso agiliza o processo de identificação e resolução de vulnerabilidades, tornando mais eficiente para as equipes protegerem seus ativos.

Além da identificação automática realizada toda vez que as buscas são executadas, a plataforma realiza o cruzamento das tecnologias identificadas com as vulnerabilidades catalogadas, indicando possíveis vulnerabilidades no ambiente sem a necessidade de execução das análises, consequentemente sem a geração de tráfego no ambiente

Alguns dos recursos disponíveis no módulo de Infra são:

- Avaliações ilimitadas
- Arquitetura em nuvem
- Resultados ao vivo
- Sem pontos cegos
- Relatórios personalizados
- Scan de infraestrutura de nuvem
- Personalização com suas políticas
- Fácil de usar

A plataforma da Rainforest permite verificar o histórico das análises que foram realizadas nos dispositivos de infraestrutura e a análise dos achados de determinada varredura.

## Casos de Uso do Rainforest Infra

---

### Pen Testers

---

Usando uma variedade de métodos, como varredura de portas e bancos de dados de vulnerabilidades para identificar pontos fracos e fornecer um relatório detalhado de suas descobertas, o módulo Rainforest Infra ajuda os testadores de penetração a identificar e relatar vulnerabilidades às partes relevantes.

No geral, Rainforest Infra é uma ferramenta inestimável para testadores de caneta, ajudando-os a agir com rapidez e precisão.

### Gerentes de Infraestrutura

---

Identifique pontos fracos e vulnerabilidades em sua rede e tome medidas preventivas para correção antes que sejam exploradas.

Execute verificações regulares e sistemáticas em sua rede ou sistema buscando por vulnerabilidades. Rainforest Infra é um meio de garantir que quaisquer pontos fracos sejam identificados e resolvidos em tempo hábil, minimizando o risco de uma brecha de segurança ou outro incidente, além de ajudar gerentes de infraestrutura a cumprir os regulamentos relevantes e padrões do setor.

### Consultores de Segurança

---

Diversos consultores de segurança usam o Rainforest Infra para identificar potenciais vulnerabilidades que poderiam passar despercebidas na rede de seus clientes.

### PME'S

---

Para empresas de todos os tamanhos, o módulo Rainforest Infra pode ajudar a gerenciar seus ativos, personalizando scans e relatórios para atender as necessidades do negócio.

# Configure Login Single Sign-On (SSO) com OKTA no Rainforest

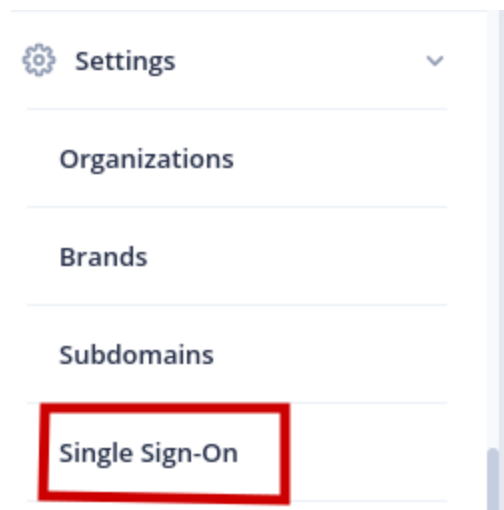
 [support.rainforest.tech/pt-br/kb/login-ss0-rainforest-okta](https://support.rainforest.tech/pt-br/kb/login-ss0-rainforest-okta)

**Permita a liberdade do Single Sign-On (SSO), mantendo o controle e a segurança aprimorados de seu ambiente..**

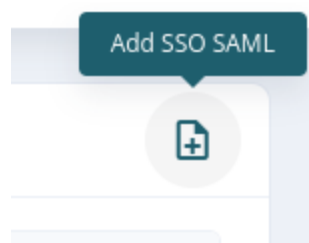
O Single Sign On (SSO), permite que os usuários simplesmente façam login uma vez e usem todos os aplicativos para os quais receberam acesso. Veja abaixo como realizar a configuração na plataforma.

## Configurações necessárias no Rainforest

1. Acesse o menu de configuração em **Configurações > Single Sign-On**



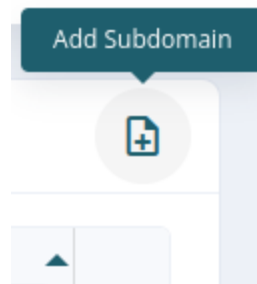
2. Clique no botão "Add SSO"



3. Siga as instruções da etapa 1 e crie um subdomínio clicando em "here"

The screenshot shows a configuration window titled "Add SSO SAML" with a close button in the top right. On the left, there is a vertical list of steps: 1. Select The Subdomain, 2. SAML Service Provider (SP) Information, 3. Identity Provider (IdP) Configuration, and 4. Extra Settings. The main content area is titled "Select The Subdomain" and contains the instruction: "Choose the specific subdomain where this Single Sign-On configuration will be implemented." Below this is a form field with a red border and an information icon. The message inside the field reads: "No subdomains available. Click [here](#) to create a new subdomain. You will be redirected to the subdomain creation page." A red asterisk and the text "\* Required field" are positioned below the field. A "NEXT" button is located in the bottom right corner.

4. Na tela que abrirá, clique em "Add Subdomain"



5. Em seguida informe o subdomínio desejado

The screenshot shows a dialog box titled "Add subdomain" with a close button in the top right. It features a text input field with the label "Subdomain" above it. The input field contains the text "teste" followed by ".rainforest.tech". At the bottom of the dialog, there are two buttons: "CANCEL" and "SAVE".

6. Na etapa 2, utilize as informações para a configuração do seu provedor de identidade

### Add SSO SAML ✕

- ✓ Select The Subdomain
- 2 SAML Service Provider (SP) Information**
- 3 Identity Provider (IdP) Configuration
- 4 Extra Settings

#### SAML Service Provider (SP) Information

Copy this information and apply it to your SAML Service Provider.

**ACS URL**  
`https://example.rainforest.tech/api/sso/51473c2d-7d8e-4db3-bdad-c78c70e6`

**Metadata URL**  
`https://example.rainforest.tech/api/sso/51473c2d-7d8e-4db3-bdad-c78c70e6`

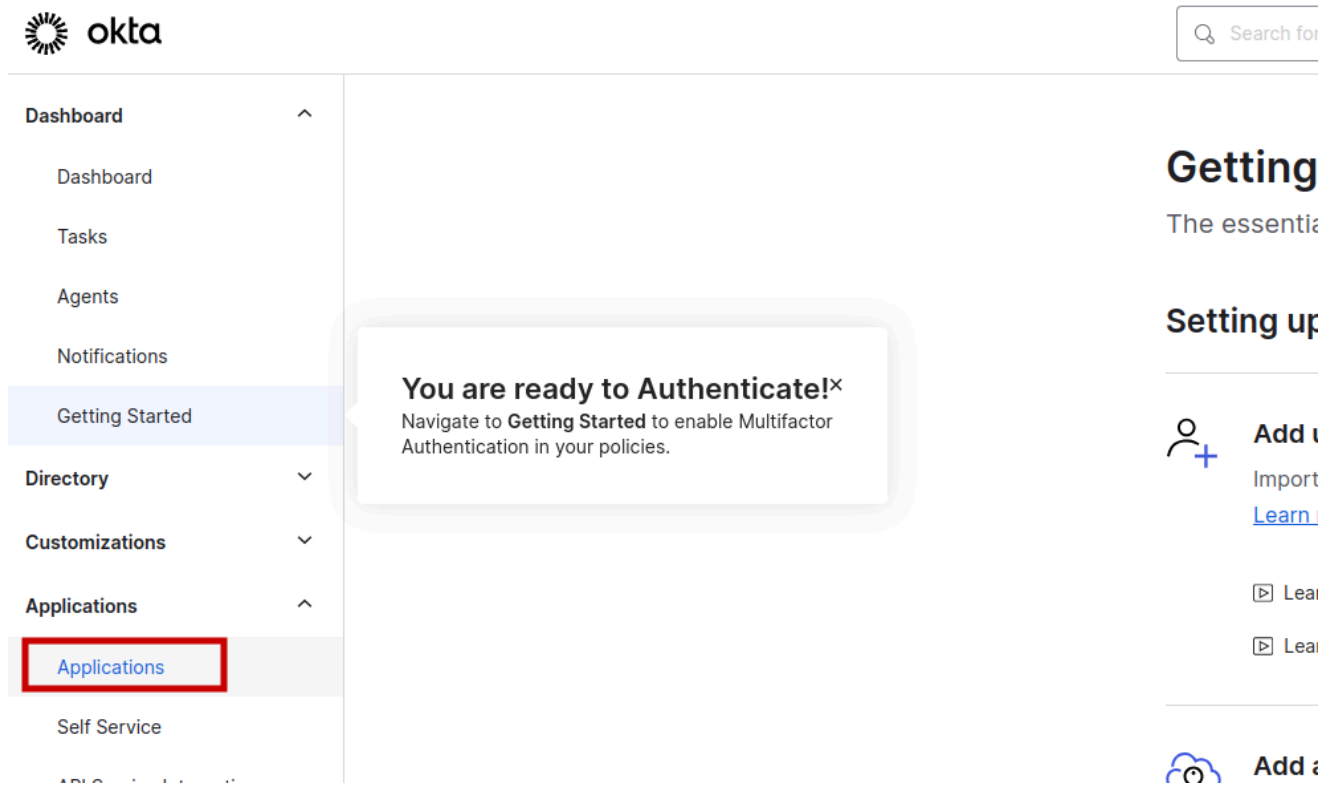
**Login URL**  
`https://example.rainforest.tech/api/sso/51473c2d-7d8e-4db3-bdad-c78c70e6`

**Logout URL**  
`https://example.rainforest.tech/api/sso/51473c2d-7d8e-4db3-bdad-c78c70e6`

[PREVIOUS](#) [NEXT](#)

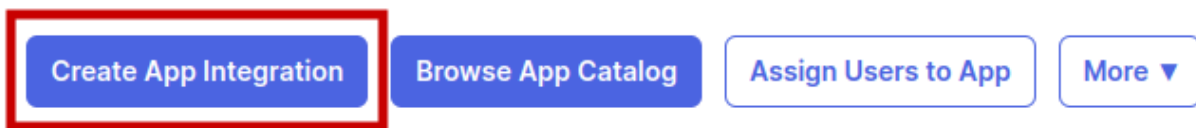
# Configurando Single Sign-On OKTA com Rainforest



1. Acesse a área de aplicações pelo menu **Applications > Applications**



2. Selecione a opção **"Create App Integration"**

## Applications



STATUS			
ACTIVE	1		Okta Admin Console
INACTIVE	0		Okta Browser Plugin

### 3. Siga as etapas iniciais do OKTA

#### ⚙️ Edit SAML Integration

1 General Settings      2 Configure SAML      3 Feedback

**1 General Settings**

App name: RFTeste

App logo (optional):

App visibility:  Do not display application icon to users

[Cancel](#) [Next](#)

This wizard walks you through editing the properties in your SAML app. All of your app's properties are prepopulated in the wizard.

### 4. Na etapa 2 do OKTA, utilize as informações das URL's informadas na etapa 2 (passo 6) no App da Rainforest, após isso, conclua a configuração do OKTA.

#### ⚙️ Edit SAML Integration

1 General Settings      **2 Configure SAML**      3 Feedback

**A SAML Settings**

**General**

Single sign-on URL:   Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID):

Default RelayState:  If no value is set, a blank RelayState is sent

Name ID format:

Application username:

Update application username on:

[Show Advanced Settings](#)

#### What does this form do?

This form generates the XML needed for the app's SAML request.

#### Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

5. Na tela do app no OKTA, acesse a aba do “Sign On”

The screenshot shows the Okta application settings interface. At the top, there is a search bar and navigation links for 'Active', 'View Logs', and 'Monitor Imports'. Below this is a tabbed menu with 'General', 'Sign On', 'Import', and 'Assignments'. The 'Sign On' tab is selected and highlighted with a red box. The main content area is titled 'Settings' and includes an 'Edit' link. Under the 'Sign on methods' section, there is explanatory text about sign-on methods and a link to 'Configure profile mapping'. A radio button is selected for 'SAML 2.0', and below it is a text input field labeled 'Default Relay State'. On the right side, there is an 'About' section with text partially visible, including 'SAML 2.0 s', 'user experi', 'the user to', 'credentials', 'their crede', 'is configure', 'Additional c', '3rd party a', 'required to', 'integration', 'Application I', 'Choose a fi', 'default use', and 'assigning ti'.

6. Copie as informações e faça o download do certificado para configurar na **etapa 3** no app da Rainforest

? UU luiz.rain

Default Relay State

**Metadata details**

Metadata URL https://trial-7299392.okta.com/app/exka8wxaskvuark5o697/sso/saml/metadata  
[Copy](#)

▼ Hide details

Sign on URL https://trial-7299392.okta.com/app/trial-7299392\_rfteste\_1/exka8wxaskvuark5o697/sso/saml  
[Copy](#)

Sign out URL https://trial-7299392.okta.com  
[Copy](#)

Issuer http://www.okta.com/exka8wxaskvuark5o697  
[Copy](#)

Signing Certificate [Download](#) [Copy](#)

🔍 Certificate fingerprint

**Credentials Details**

Application username format Okta username

Metadata application username format Okta username

Choose a format  
default username  
assigning the ap  
users.

If you select **Non**  
prompted to ent  
manually when a  
application with  
profile push prov  
features.

**SAML Setup**

Single Sign On u  
not work until yc  
app to trust Okta

[View SAML si](#)

7. Voltando para a plataforma da Rainforest, informe os dados obtidos no OKTA

Add SSO SAML

Select The Subdomain

SAML Service Provider (SP) Information

### Identity Provider (IdP) Configuration

Key \*

exka8wxaskvuark5o697

IdP Entity ID \*

IdP Login URL \*

IdP Logout URL \*

IdP Certificate \*

8. Ainda na **etapa 3**, coloque a informação com o nome do campo que terá a identificação do usuário e do e-mail

3 Identity Provider (IdP) Configuration

4 Extra Settings

### User Attributes & Claims

Name \*

name

Email \*

email

\* Required field

PREVIOUS NEXT

9. Preencha a última etapa de configuração para concluir o processo

### Add SSO SAML ✕

- ✓ Select The Subdomain
- ✓ SAML Service Provider (SP) Information
- ✓ Identity Provider (IdP) Configuration
- 4 Extra Settings

#### Default Role For New Users

Default Role \*

 🔍

**This field is required.**

#### Direct Login

Allow direct login for non-admin users

\* Required field

PREVIOUS SAVE

# Extensão Rainforest - Visual Studio Code

---

 [support.rainforest.tech/pt-br/kb/extensao-rainforest-vscode](https://support.rainforest.tech/pt-br/kb/extensao-rainforest-vscode)

## Eleve sua jornada de DevOps para DevSecOps com a extensão para VSCode da Rainforest.

---

A extensão **Rainforest Application Security** para o **Visual Studio Code** (VSCode) oferece uma solução integrada para identificar e corrigir vulnerabilidades de código em projetos cadastrados na plataforma da Rainforest.

Com esta extensão, os desenvolvedores podem realizar verificações de segurança diretamente no ambiente de desenvolvimento, facilitando a identificação e correção de potenciais ameaças à segurança.

A extensão Rainforest Application Security requer a versão 1.84.0 ou posterior do Visual Studio Code para instalação. Certifique-se de que o seu Visual Studio Code esteja atualizado para a versão especificada ou uma versão mais recente para instalar e utilizar a extensão com sucesso.

## Instalação

---

Para instalar e configurar a extensão, siga os passos através do link abaixo:

Certifique-se de que seu projeto está cadastrado na plataforma Rainforest.tech. A extensão se conectará automaticamente aos projetos registrados. [Processo Instalação](#)

## Verificação de Vulnerabilidades

---

1. Abra o projeto desejado no VSCode.
2. Clique no ícone da extensão Rainforest Application Security na barra lateral.

A extensão identificará automaticamente o projeto aberto e solicitará uma verificação de vulnerabilidades.

## Visualização de Resultados

---

Após a verificação, a extensão exibirá uma lista de vulnerabilidades de código encontradas no projeto. Cada vulnerabilidade será acompanhada por informações detalhadas sobre o problema identificado.

## Correção de Vulnerabilidades

---

O desenvolvedor pode clicar em cada vulnerabilidade para ser direcionado ao local específico do código-fonte, em seguida faça as correções necessárias no código.

## Atualização e Revisão

---

Após realizar as correções, clique no botão "**Refresh**" na extensão para atualizar os resultados. A extensão indicará quais vulnerabilidades foram corrigidas e quais persistem.

## Caso de Uso

---

Suponha que você seja um desenvolvedor trabalhando em um projeto web crítico. Ao usar a extensão **Rainforest Application Security**, você pode, rapidamente, identificar - e resolver -, vulnerabilidades de código sem sair do ambiente de desenvolvimento. Isso não apenas agiliza o processo de correção, mas também garante que a segurança seja uma parte integrada do ciclo de desenvolvimento.

## Suporte

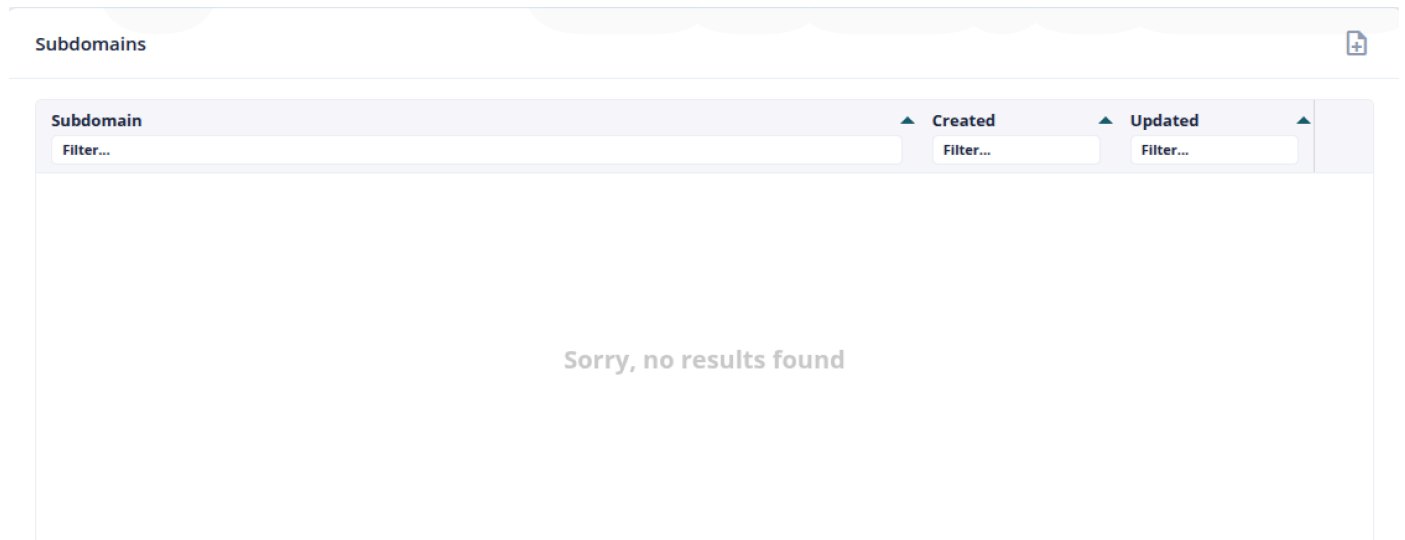
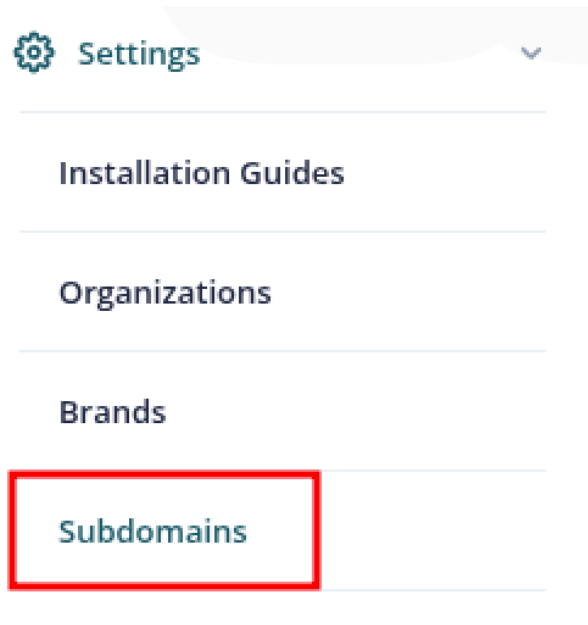
---

Para obter suporte adicional ou relatar problemas, entre em contato com nossa equipe de suporte pelo e-mail [support@rainforest.tech](mailto:support@rainforest.tech).

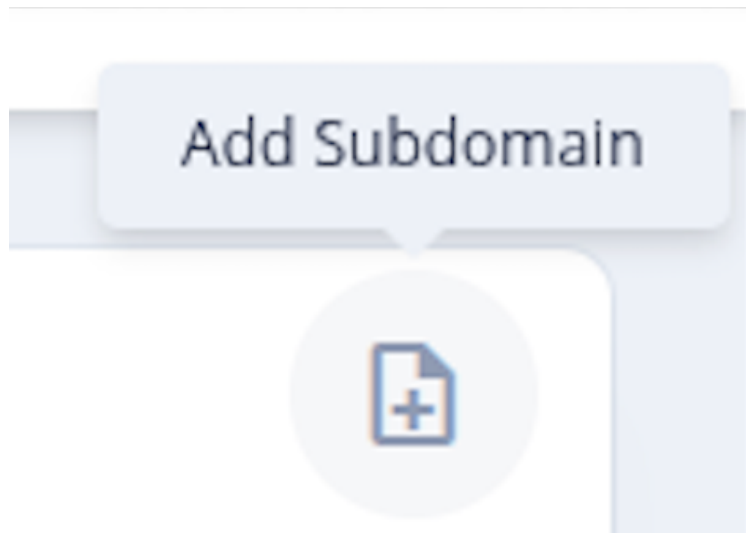
# Configure Rainforest com SAML2 Azure

 support.rainforest.tech/pt-br/kb/rainforest-saml2-azure

1 - Caso ainda não tenha um subdomain cadastrado acesse a tela de cadastro de subdomains em Settings > Subdomains



2 - Click no botão de **Add Subdomain**



3 - Informe o subdomain desejado e clique em **Save**

Add subdomain ✕

Subdomain

.rainforest.tech

CANCEL SAVE

4 - Acesse a tela de Single Sign-On na plataforma da Rainforest pelo menu **Settings > Single Sign-On**

Settings

Installation Guides

Organizations

Brands

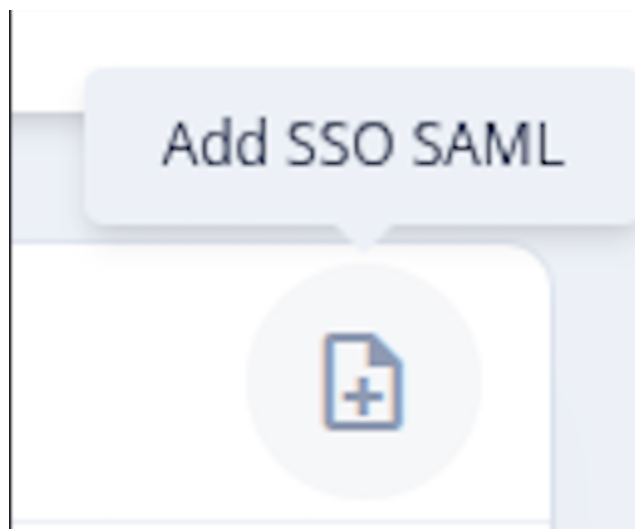
Subdomains

Single Sign-On

Single Sign-On SAML

Key	Subdomain	IdP Entity ID	IdP Login URL	IdP Logout URL	Created at	Updated at
Filter...	Filter...	Filter...	Filter...	Filter...	Filter...	Filter...

5 - Click no botão de **Add SSO SAML**



6 - Na tela de **Single Sign-On** siga com a seleção do seu **subdomain** e clique no botão **Next**

**Add SSO SAML** ✕

- 1 Select The Subdomain**
- 2 SAML Service Provider (SP) Information**
- 3 Import SSO Configuration (Optional)**
- 4 Identity Provider (IdP) Configuration**
- 5 Extra Settings**

**Select The Subdomain**  
Choose the specific subdomain where this Single Sign-On configuration will be implemented.

**Subdomain \***

  
**rftests**

**NEXT**

6.1 - Na etapa 2, guarde as informações para a configuração do seu provedor de identidade

7 – Acesse o Portal da Azure para criar sua aplicação

Home > Enterprise applications

## Enterprise applications | All applications

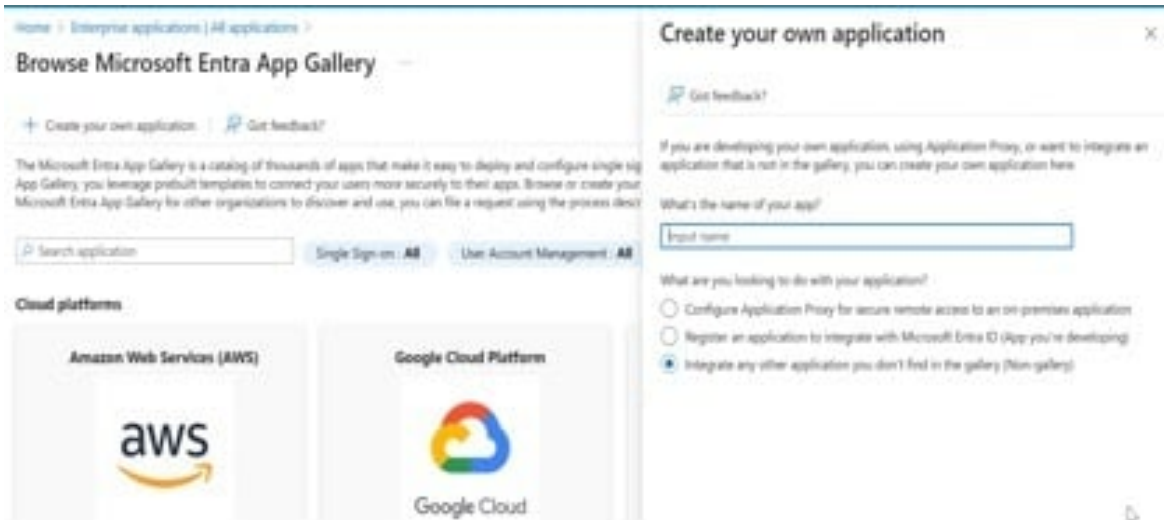
Rainforest Data Systems LLC

[+ New application](#) [Refresh](#) [Download \(Export\)](#)

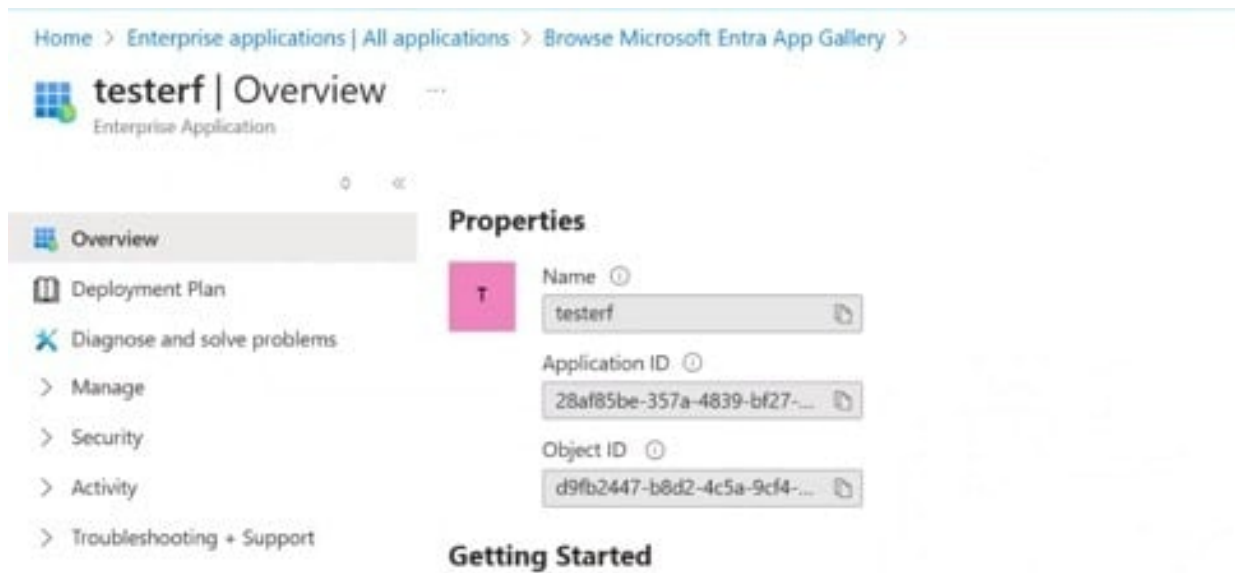
- > Overview
- ▼ Manage
- All applications**

View, filter, and search applications in your organization that are maintained by your organization

8 – Insira as informações básicas para criação da aplicação



9 – Após criação, guarde o “Application ID” para usar nas etapas da Rainforest



10 – Acesse a opção **Single sign-on** no portal da Azure

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
  - Properties
  - Owners
  - Roles and administrators
  - Users and groups
  - Single sign-on**
  - Provisioning
  - Application proxy

## 11 – Selezione SAML





Home > Enterprise applications | All applications > Browse Microsoft Entra App-Gallery > testerf

testerf | Single sign-on  
Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
  - Properties
  - Owners
  - Roles and administrators
  - Users and groups
  - Single sign-on**
  - Provisioning
  - Application proxy
  - Self-service
  - Custom security attributes

Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. [Learn more.](#)

Select a single sign-on method [Help me decide](#)

 <b>Disabled</b> Single sign-on is not enabled. The user won't be able to launch the app from My Apps.	 <b>SAML</b> Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.
 <b>Password-based</b> Password storage and replay using a web browser extension or mobile app.	 <b>Linked</b> Link to an application in My Apps and/or Office 365 application launcher.

## 12 - Preencha os dados com as informações da etapa 2 da Rainforest

The screenshot shows the 'testerf | SAML-based Sign-on' configuration page in the Microsoft Entra Admin Center. The left-hand navigation pane is expanded to 'Single sign-on'. The main content area is titled 'Set up Single Sign-On with SAML' and includes a sub-section 'Basic SAML Configuration'. This section contains a table of configuration fields:

Field	Requirement
Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State (Optional)	Optional
Logout URL (Optional)	Optional

An 'Edit' button is visible next to the 'Basic SAML Configuration' section. A callout box points to this button with the text 'Edit basic SAML configuration'. Below the SAML configuration, there is a section for 'Attributes & Claims' with a warning icon and the text 'Fill out required fields in Step 1'. A table shows a claim named 'givenname' with a value of 'user.givenname'.

## 13 – Faça o download do Federation Metadata XML

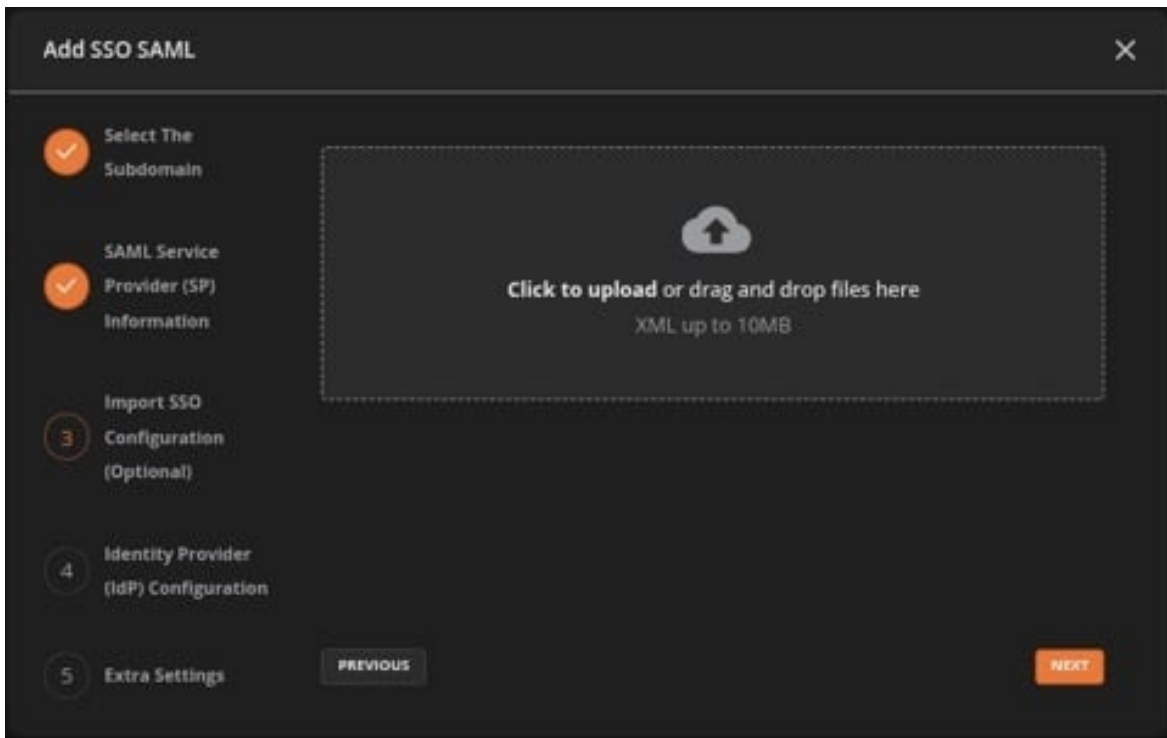
The screenshot shows the 'SAML Certificates' configuration page in the Microsoft Entra Admin Center. The left-hand navigation pane is expanded to 'Single sign-on'. The main content area is titled 'SAML Certificates' and contains a table of certificate information:

Field	Value
Token signing certificate	Active
Status	Active
Thumbprint	3E854A7A2AC83AF993C8B43D18D05E9C1C288189
Expiration	3/18/2030, 9:25:02 PM
Notification Email	
App Federation Metadata URL	<a href="https://login.microsoftonline.com/032e7ba3-0da1-4...">https://login.microsoftonline.com/032e7ba3-0da1-4...</a>
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Below this table, there is a section for 'Verification certificates (optional)' with a table:

Field	Value
Required	No
Active	0
Expired	0

## 14 - Faça o upload do arquivo XML na etapa 3 na Rainforest



15 – Preencha o restante dos campos na etapa 4 (Obs: No campo Key o Application ID precisa ter o prefixo “spn:” conforme imagem abaixo)

**Add SSO SAML** ✕

- 1 Select The Subdomain
- 2 SAML Service Provider (SP) Information
- 3 Import SSO Configuration (Optional)
- 4 Identity Provider (IdP) Configuration**
- 5 Extra Settings

### Identity Provider (IdP) Configuration

**Key \***

**IdP Entity ID \***

**IdP Login URL \***

**IdP Logout URL \***

**IdP Certificate \***

### User Attributes & Claims

**Name \***

**Email \***

\* Required field

16 - Na etapa 5, a última etapa, insira a role **Application Operator** e click em **SAVE**

1 Select The Subdomain

2 SAML Service Provider (SP) Information

3 Import SSO Configuration (Optional)

4 Identity Provider (IdP) Configuration

5 Extra Settings

### Default Role For New Users

Default Role \*

Application Operator

APPLICATION OPERATOR X

### Direct Login

Allow direct login for non-admin users

\* Required field

Previous

Next

### Status

The status of the SAML Service Provider (SP) determines whether the SAML Service Provider (SP) is active or inactive. You can set the status to active or inactive at any time.

Enabled

Created at 10/3/25 and last modified at 10/3/25

CANCEL

DELETE

SAVE

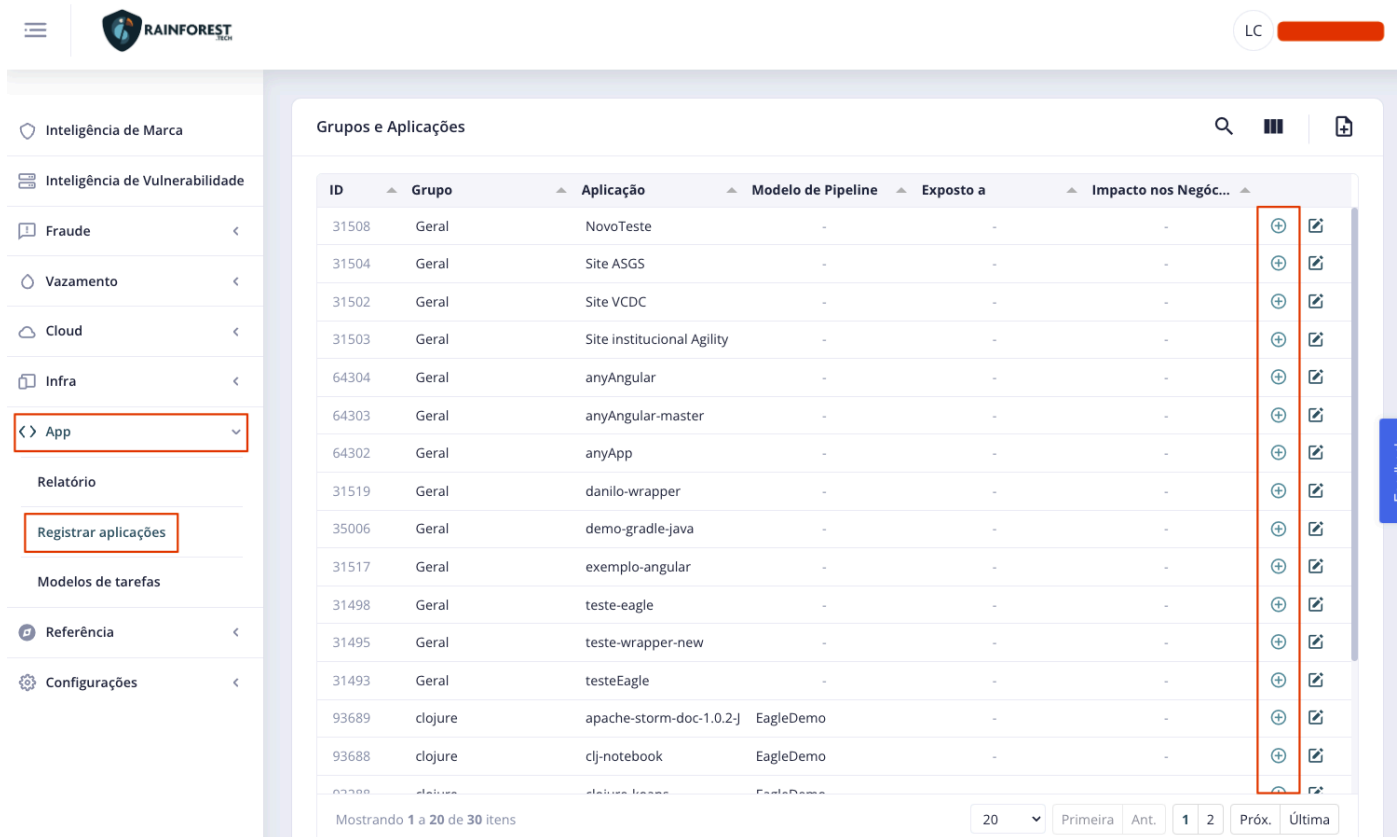
# Registrar Vulnerabilidades em Aplicações

 support.rainforest.tech/pt-br/kb/registrar-vulnerabilidades-aplicacoes

## Veja como realizar o registro de uma vulnerabilidade manualmente em aplicações cadastradas na plataforma Rainforest.

Além das vulnerabilidades que a plataforma Rainforest encontra automaticamente através das análises que ela realiza, temos a possibilidade de cadastrar de forma manual o registro de vulnerabilidades encontradas, como por exemplo em casos de PENTESTs realizados, onde podemos subir no Rainforest seus resultados e termos um histórico dos testes feitos em cada aplicação.

Para isso acesse o menu **App > Registrar Aplicações > Editar aplicação (+)** .



The screenshot shows the Rainforest web interface. On the left, a sidebar menu is visible with the following items: Inteligência de Marca, Inteligência de Vulnerabilidade, Fraude, Vazamento, Cloud, Infra, App (selected), Relatório, Registrar aplicações (highlighted), Modelos de tarefas, Referência, and Configurações. The main content area is titled 'Grupos e Aplicações' and contains a table with the following columns: ID, Grupo, Aplicação, Modelo de Pipeline, Exposto a, and Impacto nos Negócios. The table lists various applications, including 'NovoTeste', 'Site ASGS', 'Site VCDC', 'Site Institucional Agility', 'anyAngular', 'anyAngular-master', 'anyApp', 'danilo-wrapper', 'demo-gradle-java', 'exemplo-angular', 'teste-eagle', 'teste-wrapper-new', 'testeEagle', 'apache-storm-doc-1.0.2-J', 'EagleDemo', and 'clj-notebook'. A red box highlights the '+' icon in the rightmost column of the table, indicating the action to edit an application. At the bottom of the table, it says 'Mostrando 1 a 20 de 30 itens' and there are pagination controls for '20', 'Primeira', 'Ant.', '1', '2', 'Próx.', and 'Última'.

Posteriormente o formulário de registro será apresentado para realizar o preenchimento. Informe os campos e clique em **Salvar**.

## Registrar Vulnerabilidade



Nome

Test 1

Título

Test 1

Severidade

Muito Baixa

Categoria

Test 1

CVSS

Test 1

Descrição

Test 1

Localização

Test 1

URL da localização

Test 1

Localização do módulo

Test 1

Localização do arquivo

Test 1

Localização da linha

Test 1

Localização da posição

Test 1

Localização do recurso

Test 1

Última alteração por usuário

Test 1

Contexto

Test 1

Status da correção

Test 1

Esforço de correção

Test 1

Recomendações para Solucionar

Test 1

Branch

Test 1

Branch de Produção

Test 1

Data de Importação

Test 1

Conformidade (separado por vírgulas)

Test 1

CANCELAR

SALVAR

Após salvar o registro, a vulnerabilidade estará visível para, se for o caso, início das tratativas de resolução e/ou acompanhamento. Em **App > Relatório**, filtre por exemplo pela aplicação que acabou de realizar o registro da vulnerabilidade.

**Filtros** ×

**Grupo**

Geral ×

**Aplicação**

NovoTeste ×

**Branch**

Test 1 ×

**Categoria**

Selecione uma opção ×

**Compliance**

Selecione uma opção ×

**Status**

Selecione uma opção ▼

**Severidade**

Muito Baixa

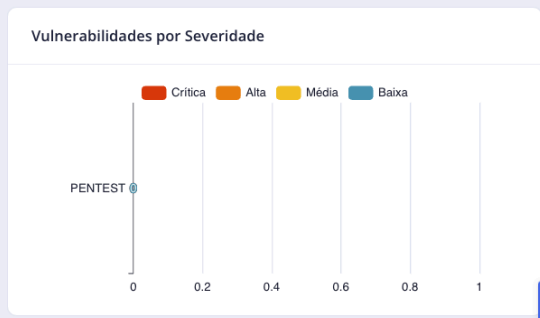
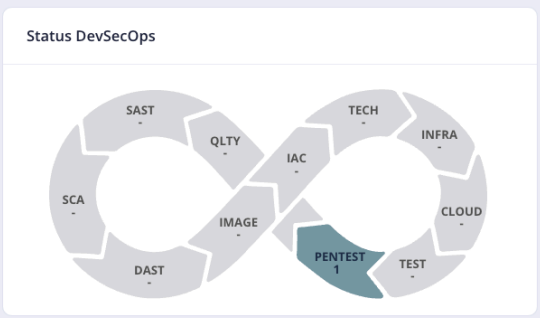
**LIMPAR**

**Feedback**

Ela será apresentada na lista de vulnerabilidades da aplicação ao qual foi cadastrada.

- Inteligência de Marca
- Inteligência de Vulnerabilidade
- Fraude
- Vazamento
- Cloud
- Infra
- App
- Relatório
- Registrar aplicações
- Modelos de tarefas
- Referência
- Configurações

1 App   0 Infra   0 Cloud   0 Mitigado   0 Priorizado



### Informações sobre Políticas e Pipeline

Progresso: 1 2

Política <b>Sim</b>	Pipeline <b>Não</b>	Pronto <b>Não</b>	Grupo <b>Geral</b>
App: <b>NovoTeste</b>	Nome da branch atual: <b>Test 1</b>	Nome da última branch: <b>Não encontrado</b>	URL do repositório:
URL: <a href="https://api.rainforest.tech/pages/application/report?group=Geral&amp;app=NovoTeste&amp;branch=Test 1&amp;tenant=19">https://api.rainforest.tech/pages/application/report?group=Geral&amp;app=NovoTeste&amp;branch=Test 1&amp;tenant=19</a> <span>COPIAR</span>			

### Vulnerabilidades por Aplicações e Branch

ID	Severidade	Categoria	Nome	Título
82139492	very-low	PENTEST	Test 1 [Very Low]	Test 1

Feedback



# Classificação dos Itens Encontrados

 support.rainforest.tech/pt-br/kb/classificacao-itens

## Como é realizada a classificação dos itens encontrados na plataforma da Rainforest

Os itens encontrados são classificados e exibidos dentro dos respectivos módulos da plataforma, as categorias podem variar dependendo do módulo da plataforma

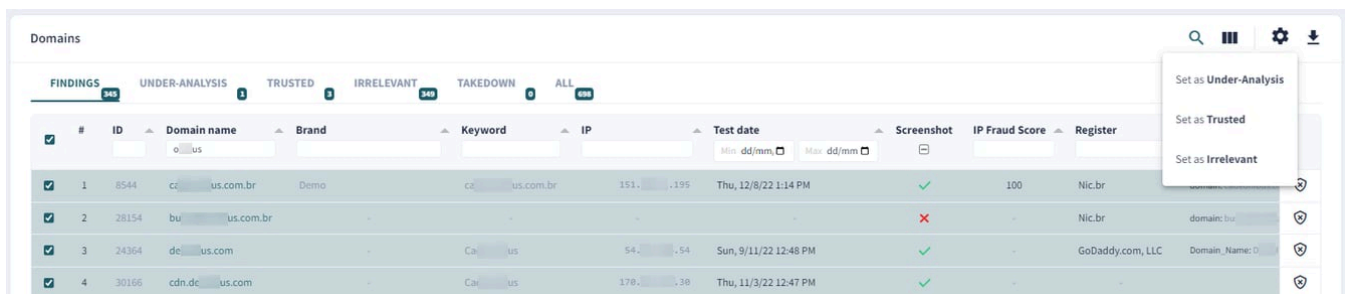
## Inteligência de Marca



A classificação dos itens dentro dos módulos do pilar de inteligência de marca pode ser realizada nos seguintes módulos e menus::

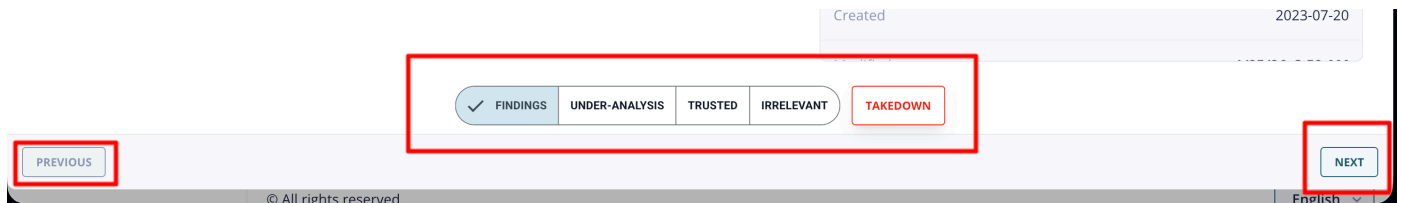
- **Descobertas:** Itens novos aguardando classificação.
- **Sob Análises:** Itens classificados como suspeitos e que foram separados automaticamente ou por ações manuais dos usuários para uma análise mais detalhada. Normalmente utilizado para itens que estão sob análise manual ou aguardando aprovação interna antes da solicitação de takedown.
- **Confiável:** Itens que foram classificados como confiáveis.
- **Irrelevante:** Itens que foram classificados como irrelevantes ou falso-positivos.
- **Takedown:** Itens que são considerados fraude ou vazamentos e estão em processo de takedown para serem retirados do ar.
- **Todos:** agrupamento de todos os registros das categorias anteriores.

Além das classificações automáticas, os itens também podem ser classificados manualmente ou em grupos a partir da tabela onde todos os itens são listados.



#	ID	Domain name	Brand	Keyword	IP	Test date	Screenshot	IP Fraud Score	Register
1	8544	ca[redacted].us.com.br	Demo	ca[redacted].us.com.br	151.[redacted].195	Thu, 12/8/22 1:14 PM	✓	100	Nic.br
2	28154	bu[redacted].us.com.br	-	-	-	-	✗	-	Nic.br domain: bu[redacted].us.com.br
3	24364	dc[redacted].us.com	-	Ca[redacted].us	54.[redacted].54	Sun, 9/11/22 12:48 PM	✓	-	GoDaddy.com, LLC Domain_Name: 0
4	30186	cdn.dc[redacted].us.com	-	Ca[redacted].us	178.[redacted].38	Thu, 11/3/22 12:47 PM	✓	-	-

Acessando um item, navegar entre os registros e categoriza-los, bem como abrir uma solicitação de takedown. Isso facilita no momento da análise registros quando estão em grande quantidade.



## Inteligência de Vulnerabilidade

Dentro de pilar de inteligencia de vulnerabilidade, a plataforma categorizar os itens em:

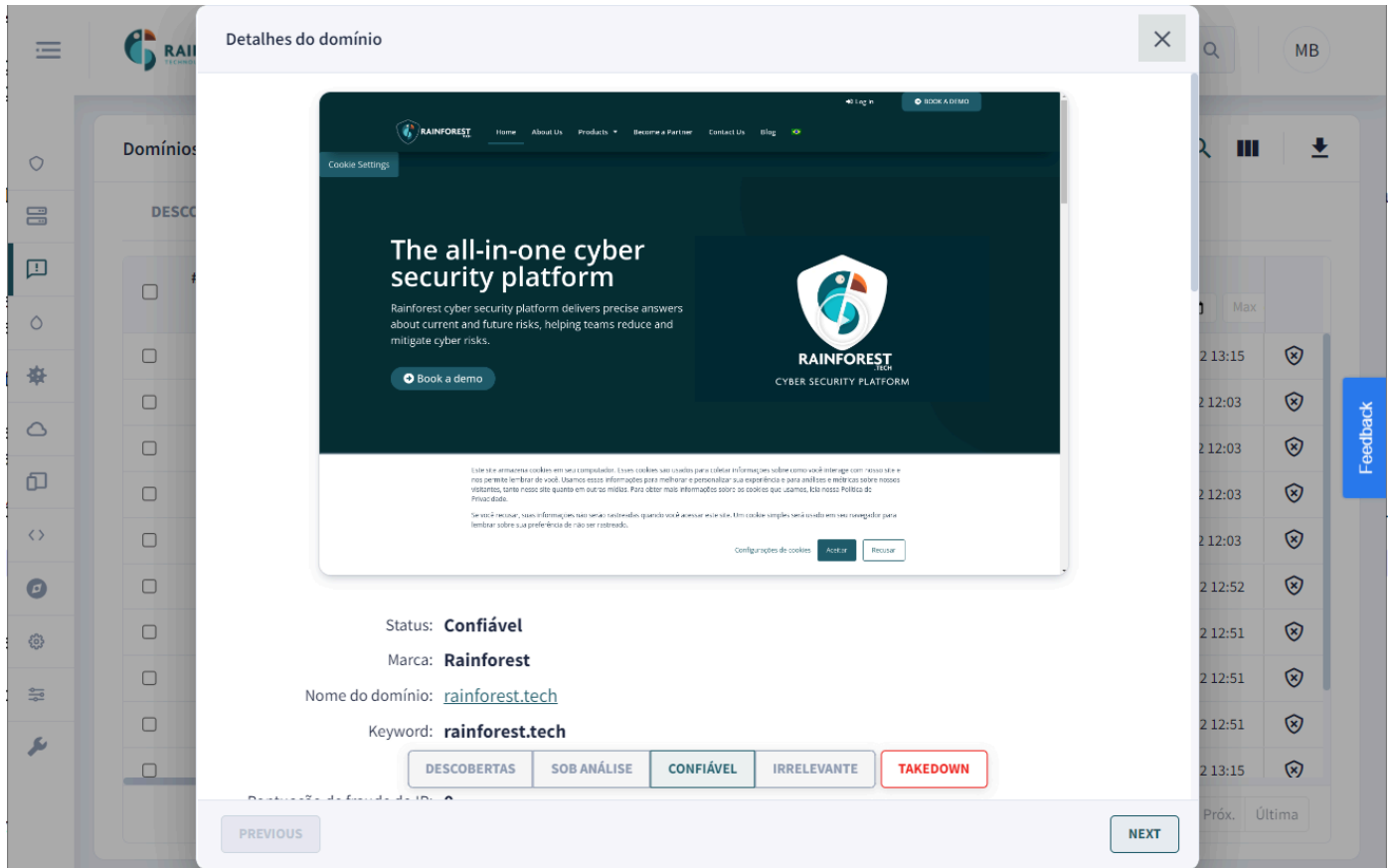
- Aberto
- Mitigado
- Transferido
- Fechado
- Falso Positivo
- Decommission
- Todos

### FINDINGS

OPEN	MITIGATED	TRANSFERRED	CLOSED	FALSE POSITIVE	DECOMMISSION	ALL <span>0</span>	
ID ↑↓	Severity ↑↓	Category ↑↓	Status ↑↓	Name ↑↓	Details ↑↓	Location ↑↓	First Find ↑↓
<input type="checkbox"/>	<input type="text" value="Filter..."/>	<input type="text" value="Filter..."/>	<input type="text" value="Filter..."/>	<input type="text" value="Filter..."/>	<input type="text" value="Filter..."/>	<input type="text" value="Filter..."/>	<input type="text" value="Filter..."/>
<input type="checkbox"/>	98676610	CLIFFFACE	Open	Shadow Consolidation for IP 40.20.63.2	Item not found	url: 40.20.63.201	6/6/23 1:35 PM

Dentro de uma janela de scan, se um achado de qualidade ou segurança, descoberto em análises anteriores, foi corrigido, ele é removido automaticamente de **Aberto** para **Fechado**.

Ao clicar em algum item, também é possível visualizar os detalhes desse e quando possível também a imagem do sistema na hora que foi realizada a detecção.



Para o vazamento de credenciais, a plataforma oferece uma classificação chamada **Resolvido**, para as descobertas que foram solucionadas.



## Ações em Lote

A plataforma possibilita a execução de ações em lote nos registros identificados, as ações podem variar dependendo do módulo, dentre elas temos:


- Alteração de severidade
- Adição de comentário
- Marcar como sob análise
- Marcar como confiável
- Marcar como irrelevante
- Exportação de dados

## Domains

FINDINGS 453 UNDER-ANALYSIS 5 TRUSTED 319 IRRELEVANT 1,127 TAKEDOWN 1 ALL 1,905

Actions:

MARK AS UNDER-ANALYSIS MARK AS TRUSTED MARK AS IRRELEVANT CHANGE SEVERITY ADD COMMENT REPROCESS URL

<input checked="" type="checkbox"/>	#	ID	Thumbnail	Status ↑↓	Severity ↑↓	Domain name ↑↓	Brand ↑↓
		<input type="text" value="Filtre"/>		<input type="text" value="Filtre"/>	<input type="text" value="v"/>	<input type="text" value="Filter..."/>	<input type="text" value="v"/>
							

- Abrir
- Mitigar
- Transferido
- Fechado
- Falso positivo

## FINDINGS

OPEN 56 MITIGATED 0 TRANSFERRED 0 CLOSED 1,833 FALSE POSITIVE 63 DECOMMISSION 45 ALL 1,997

Actions:

OPEN MITIGATED TRANSFERRED CLOSED FALSE POSITIVE

<input checked="" type="checkbox"/>	ID ↑↓	Severity ↑↓	Category ↑↓	Status ↑↓	Name ↑↓	Details ↑↓
	<input type="text" value="Fil"/>	<input type="text" value="Filter.."/>	<input type="text" value="Filter.."/>	<input type="text" value="Filtre"/>	<input type="text" value="Filter..."/>	<input type="text" value="Filter..."/>
<input checked="" type="checkbox"/>	67891391	Critical	SAST	Open	Hard-coded password	(1/1) * Possible vulnerability detected: Hard-cc
<input checked="" type="checkbox"/>	41430858	Critical	SAST	Open	Hard-coded password	(1/1) * Possible vulnerability detected: Hard-cc
<input checked="" type="checkbox"/>	41430855	Critical	SAST	Open	Hard-coded password	(1/1) * Possible vulnerability detected: Hard-cc

# Habilitar autenticação de dois fatores (2FA)

---

 [support.rainforest.tech/pt-br/kb/habilitar-autenticacao-dois-fatores](https://support.rainforest.tech/pt-br/kb/habilitar-autenticacao-dois-fatores)

## Aumente a segurança ao logar-se na plataforma Rainforest

---

A **Rainforest** oferece para os usuários da plataforma a autenticação de dois fatores (2FA), fortalecendo a segurança de acesso exigindo dois métodos (também chamados de fatores) para verificar sua identidade. Essa forma de autenticação protege contra phishing, engenharia social e força bruta de senha, além de proteger seus logins de invasores que exploram credenciais fracas ou roubadas.

O recurso pode ser habilitado tanto em nível geral, obrigatoriamente para todos os usuários do cliente, como em nível individual, veremos em seguida como realizar a configuração para esses dois níveis.

### Habilitando Autenticação em Nível Organizacional

---

Para que a autenticação de dois fatores (2FA) seja habilitado para todos os usuários, acesse o menu **Configurações > Organizações**.

**0/100**  
Nota da Empresa

**Vulnerabilidades**

**Crítica**

**158** Ativos      **308** Vulns

**Probabilidade por CVE**

Planeje corrigir

Após acessar o menu você terá disponível a listagem de organizações cadastradas na plataforma.

**Organizações**

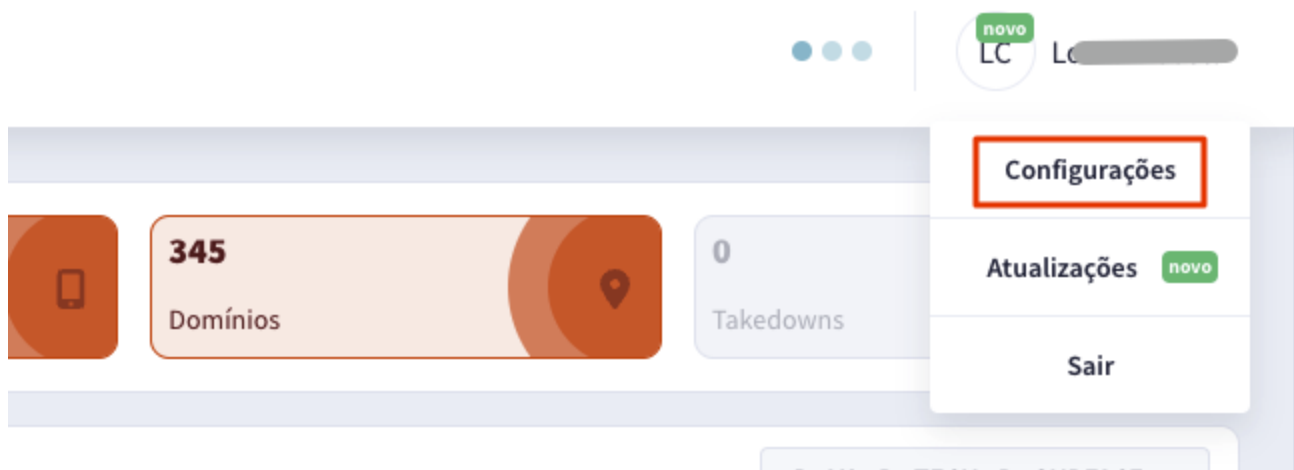
ID	Nome	Gerente	Licenças									Criado em
filtra	filtrar...	filtrar...	THREATINTEL	TEST	REPUTATION	LEAK	GPD	FRAUD	CLOUD	INFRA	APPLICATION	filtrar...
19	Demo	-	0	1	1	1	0	1	1	1	1	12/3/20, 7:36 PM
92	Teste criar tenant	Demo	-	-	-	-	-	-	-	-	-	12/21/22, 4:12 PM

Clique sobre a organização desejada e habilite a opção **Autenticação 2FA - Obrigatório para todos os usuários**. Desta forma, para todos os usuários será habilitado e obrigatório.



### Habilitando Autenticação em Nível Individual

Para habilitar esse recurso, logue na plataforma Rainforest e acesse as configurações de usuário no canto superior direito, **Seu Nome de Usuário > Configurações**.



Selecione a aba **autenticação de dois fatores** e clique em **habilitar autenticação de dois fatores**.

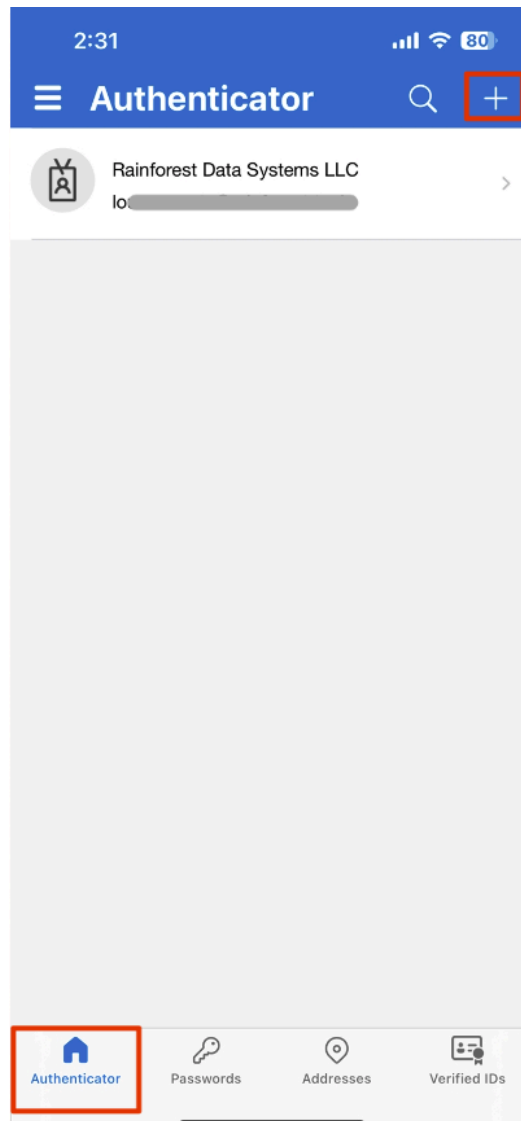


Será necessário realizar o download e instalação de um aplicativo autenticador.

**Observação:** neste exemplo, demonstraremos como realizar o processo em um dispositivo utilizando iOS, usando o aplicativo autenticador da Microsoft.

## Configurando o aplicativo em seu smartphone

Faça o download do aplicativo desejado e logue-se nele. Caso não tenha login, será necessário primeiro criar uma conta. Após logado, clique em **Authenticator > Adicionar (+)**



Se for a primeira vez que estiver utilizando o aplicativo de autenticação, será solicitada permissão para utilizar a camera do aparelho, clique em **Permitir**, em seguida volte no Rainforest e com o smartphone leia o QRCode gerado.

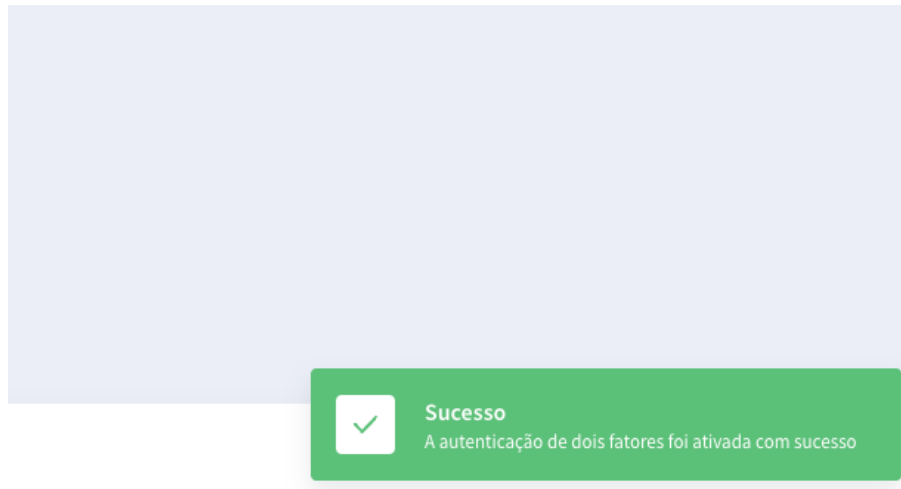


Após realizar a leitura, no aplicativo será apresentando um código para você inserir na etapa 3. Insira o código e clique em **Verificar**.

No aplicativo cada código tem validade de 30 segundos, após esse período um novo código será gerado, certifique-se de que o código que está usando ainda está dentro do período de validade fornecido pelo aplicativo.



Após verificado, você receberá um alerta no Rainforest e será habilitado um botão para desabilitar a autenticação de dois fatores quando necessário.



Na próxima vez que o usuário for realizar o login no Rainforest será solicitado o código de autenticação fornecido pelo aplicativo autenticador escolhido, digite o código e caso esteja correto, o Rainforest o encaminhará para a tela inicial automaticamente.



### Two-factor authentication

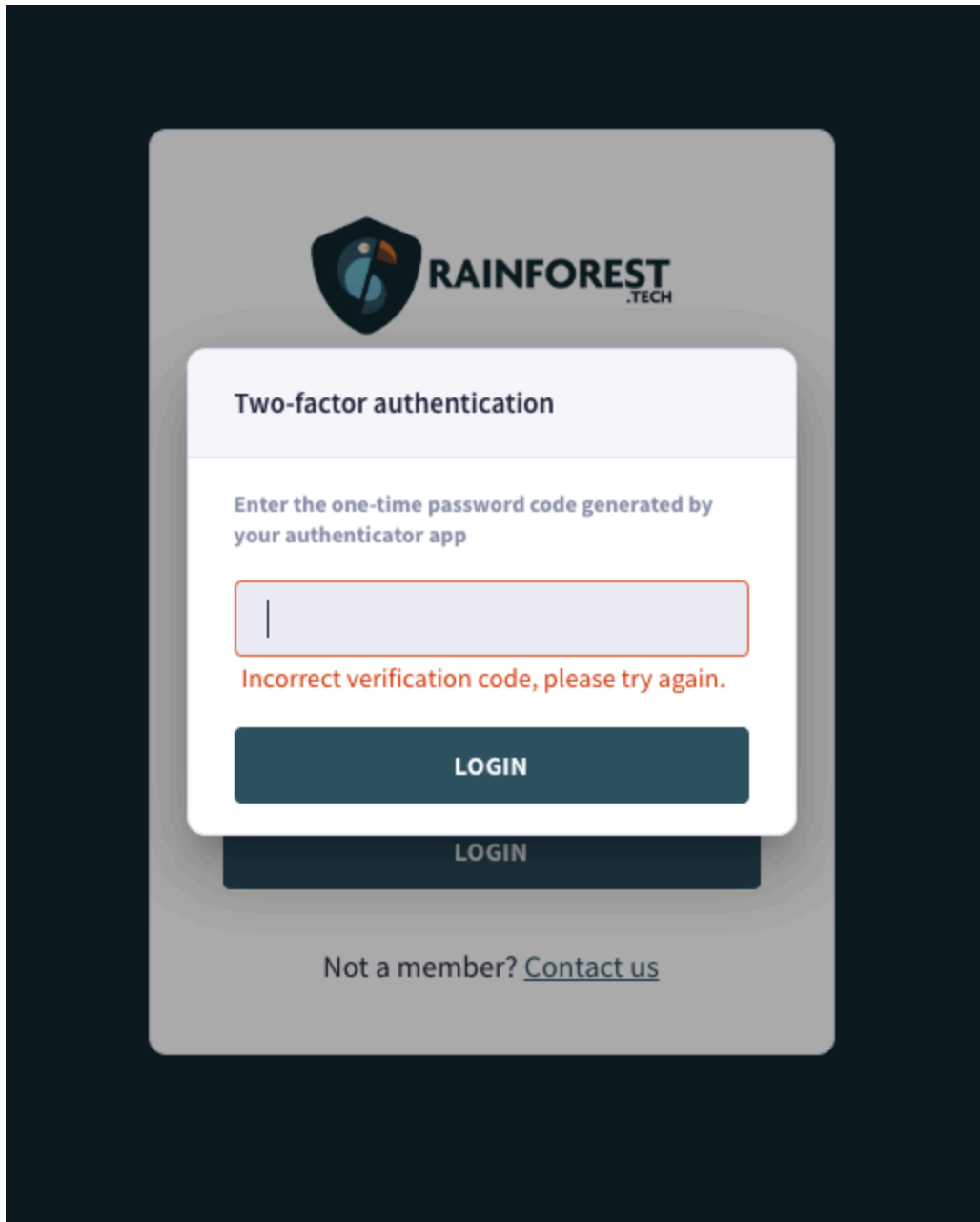
Enter the one-time password code generated by your authenticator app

LOGIN

LOGIN

Not a member? [Contact us](#)

Caso digite o código errado, será apresentado na tela um alerta.



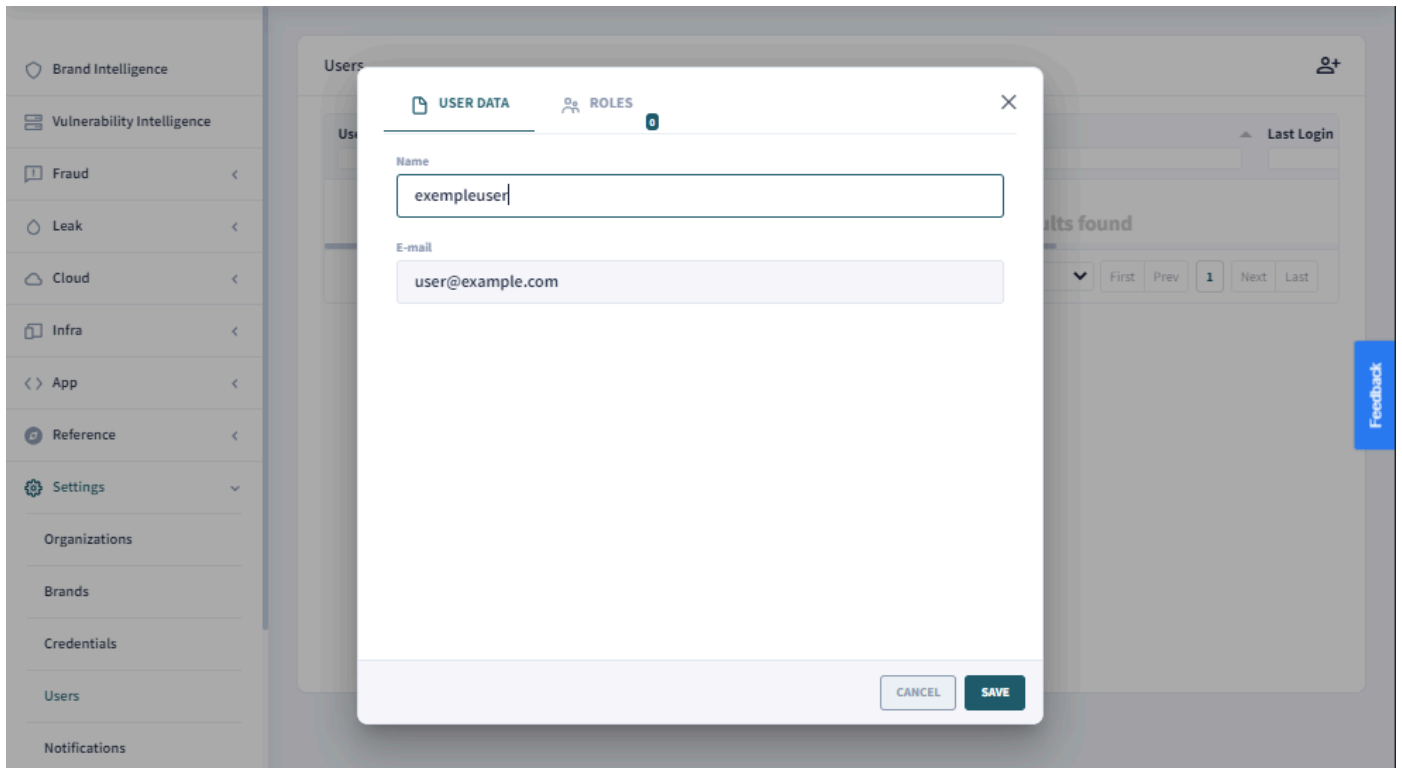
Para configuração da funcionalidade de dois fatores de autenticação (2FA) para todos os usuários simultaneamente, entre em contato com a equipe de suporte da Rainforest.

# Configurar usuários e permissões

 [support.rainforest.tech/pt-br/kb/configurar-usuarios-e-permissoes](https://support.rainforest.tech/pt-br/kb/configurar-usuarios-e-permissoes)

## Veja como gerenciar usuários e as permissões de acesso.

Usuários que tenham a permissão de "*Administrator*" podem gerenciar os usuários e editar as permissões através do menu **Configurações > Usuários**.



Ao criar um novo usuário é necessário informar o email de acesso e as permissões (*roles*) que acesso, seguem abaixo os tipos de permissões e acessos que estas liberaram.

### **ADMINISTRATOR:**

- Gerenciar usuários e suas permissões;
- Configurar marcas a serem monitoradas;
- Configurar os conectores.

### **ADMIN do Módulo:**

- Gerenciar os itens encontrados;
- Configurar domains e keywords a serem monitoradas;
- Solicitar Takedown nos menus que tem essa opção;
- Receber notificações dos itens encontrados;
- Se for módulo de Application, também pode cadastrar os applications.

- **OPERATOR do Módulo:**

- Pode gerenciar os itens encontrados dentro do módulo;
- Visualizar os status dos Takedown solicitados;
- Receber notificações dos itens encontrados.

- **VIEW do Módulo:**

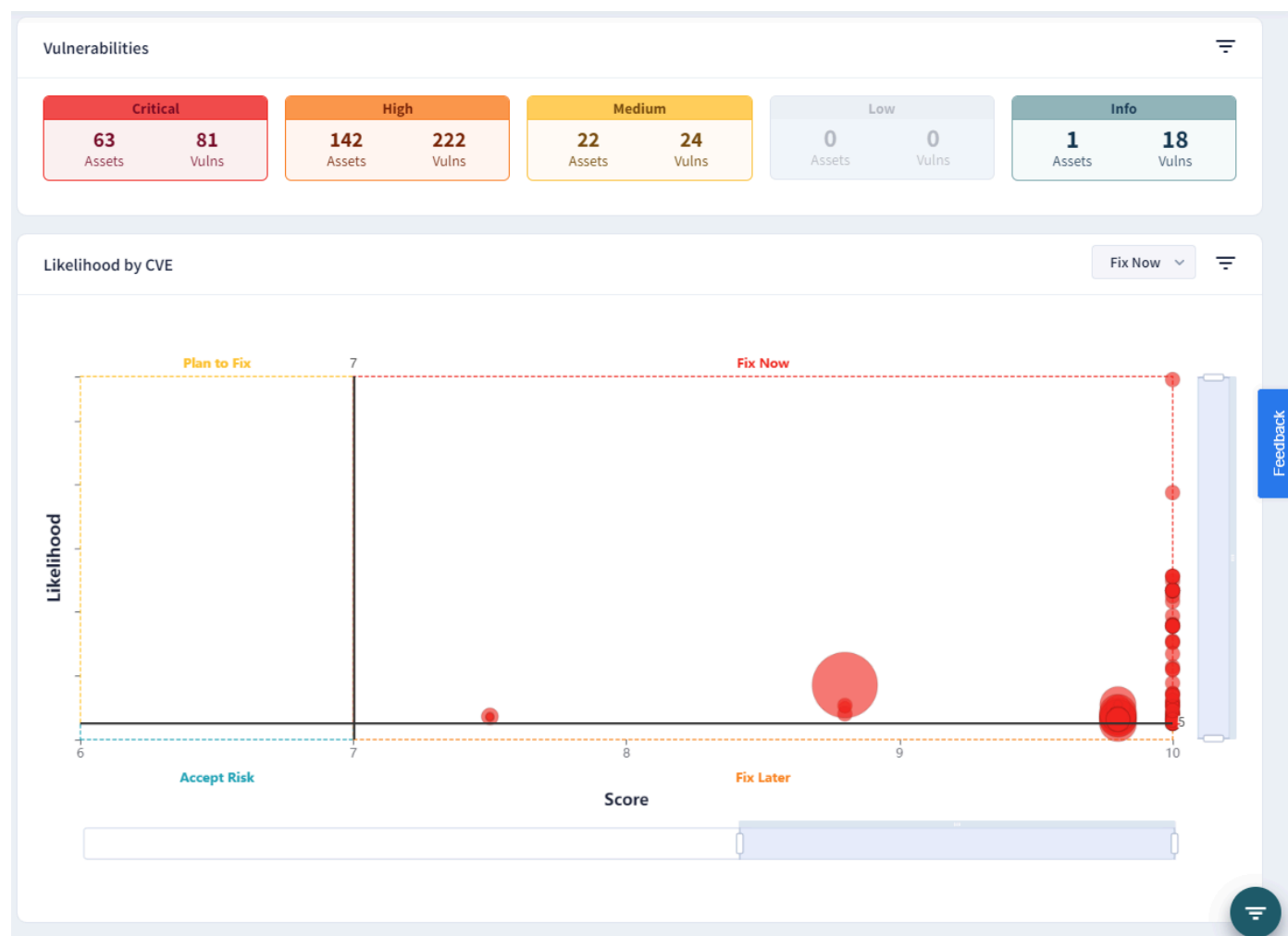
- Pode visualizar os itens encontrados dentro do módulo;
- Visualizar os status dos Takedown solicitados;
- Receber notificações dos itens encontrados.

# Visualização das Vulnerabilidades

 support.rainforest.tech/pt-br/kb/visualizacao-vulnerabilidades

## Gráficos, Filtros, Relatórios e Exportar Vulnerabilidades

A plataforma disponibiliza gráficos por quantidades, por probabilidade de exploração, por top vulnerabilidades e histórico de correções, entre outros.



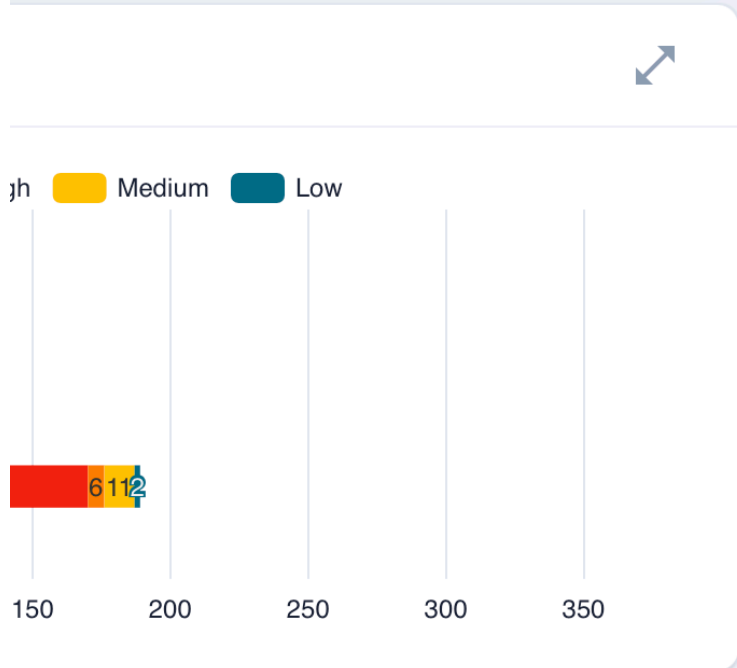
Sempre que uma nova varredura é realizada, a plataforma da Rainforest atualiza a lista de vulnerabilidades ativas. Desta forma o usuário da sempre terá o status real das vulnerabilidades ativas que estão impactando seu ambiente.

A plataforma também permite realizar diversos filtros, dentre eles temos:

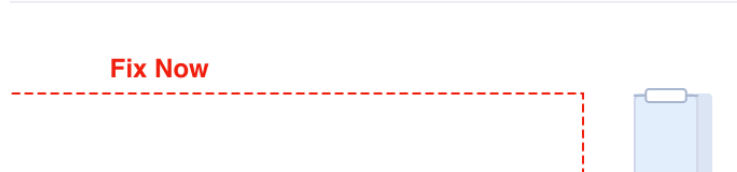
- Severidade
- Categoria
- Tipos de categoria
- Tecnologia

- Status dos achados
- Nome
- Tipos de achados
- Tipos de itens
- Status do item
- Labels
- Datas
- Desenvolvedor

EXPORT



Fix Now



### Filters



#### Severity

- All
- Critical
- High
- Medium
- Low
- Info

#### Category

- All
- QLTY
- SAST
- SCA
- DAST
- IMAGE
- IAC
- TECH

See more

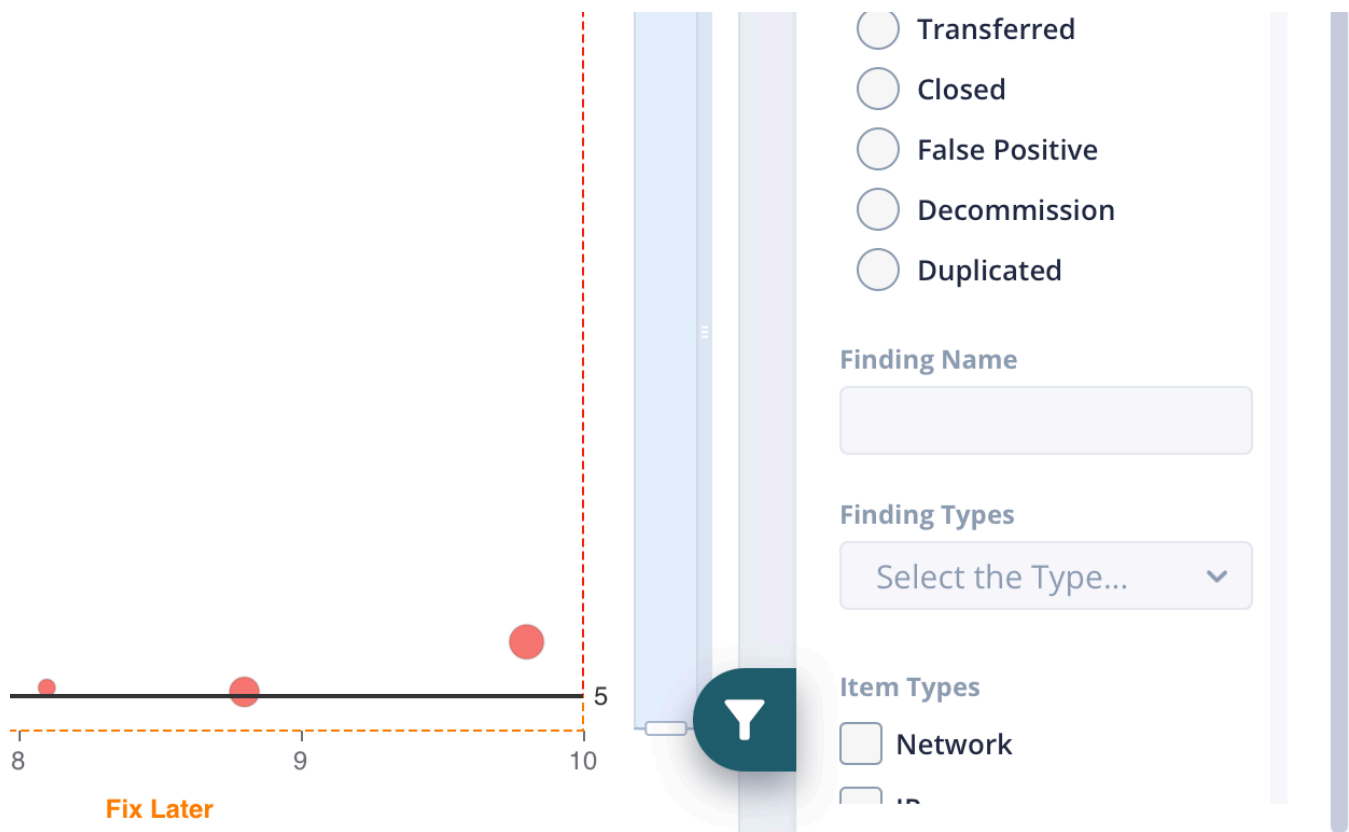
#### Category Types

- All
- quality
- vulnerability
- test

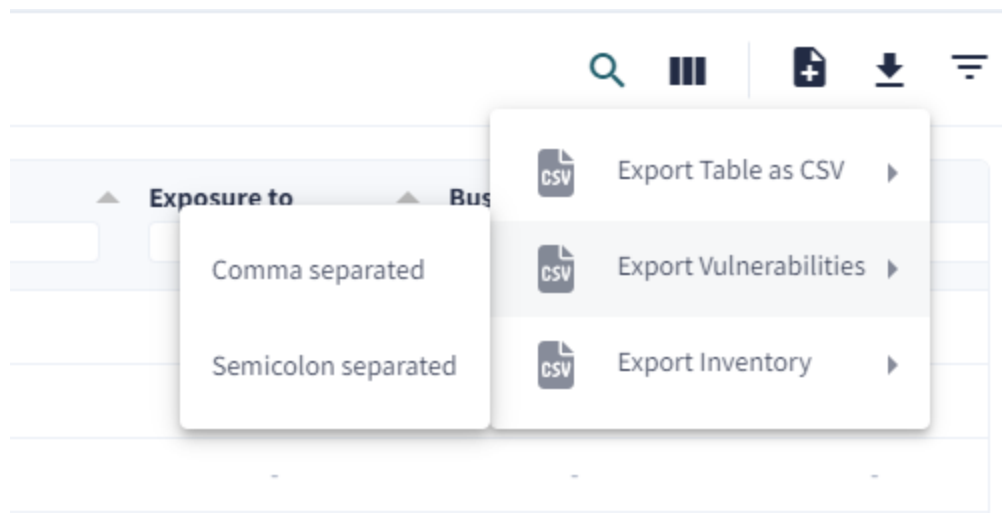
#### Technology

#### Findings Status

- All
- Open
- Mitigated



Também é possível exportar as informações para CSV com o objetivo de visualizar essas informações em outros sistemas.



## Exemplos de Gráficos Disponíveis

### Vulnerabilidades por Ativo

A plataforma permite os usuários visualizarem a quantidade de vulnerabilidades por ativo, para isso acesse o menu **Infra > Ativos**, acesse a lista de ativos e em sequencia o ativo desejado.

Mostrando 6 de 6 itens 20 Primeira An

**Ativos**

#	ID	Tipo	Nome	IP	Network	Exposto a	Impacto nos B
1	16	Ativo único	10.1.203.3	10.1.203.3	-	internal	medium
2	17	Ativo único	10.1.203.5	10.1.203.5	-	internal	medium
3	18	Ativo único	10.1.203.4	10.1.203.4	-	internal	medium
4	19	Ativo único	10.1.203.8	10.1.203.8	-	internal	medium
5	20	Ativo único	10.1.203.9	10.1.203.9	-	internal	medium
6	21	Ativo único	10.1.203.11	10.1.203.11	-	internal	medium
7	22	Ativo único	10.1.203.14	10.1.203.14	-	internal	medium
8	23	Ativo único	10.1.203.18	10.1.203.18	-	internal	medium
9	24	Ativo único	10.1.203.20	10.1.203.20	-	internal	medium
10	25	Ativo único	10.1.203.19	10.1.203.19	-	internal	medium
11	26	Ativo único	10.1.203.17	10.1.203.17	-	internal	medium
12	27	Ativo único	10.1.203.21	10.1.203.21	-	internal	medium
13	28	Ativo único	10.1.203.22	10.1.203.22	-	internal	medium

Mostrando 206 de 206 itens 250 Primeira Ant. 1 Próx. Última

Feedback

Ao acessar o ativo você visualizará a quantidade de vulnerabilidades no ativo categorizadas nas respectivas abas.

**DADOS DO ATIVO**

TECNOLOGIAS **5** VULNS POR TECH **3** VULNS POR VA **19** VULNS POR SURFACE VULNS POR XDR

Nome do Ativo: [Redacted] Fonte: system Tipo de Ativo: Ativo único Endereço de IP: [Redacted]

Departamento: [Redacted] Coordenadas: Latitude, longitude Network: Selecione uma rede


Exposto a: Internal Impacto nos Negócios: Média Ambiente: [Redacted]

Ex.: 38.12024, -122.039998

Descrição: [Redacted]

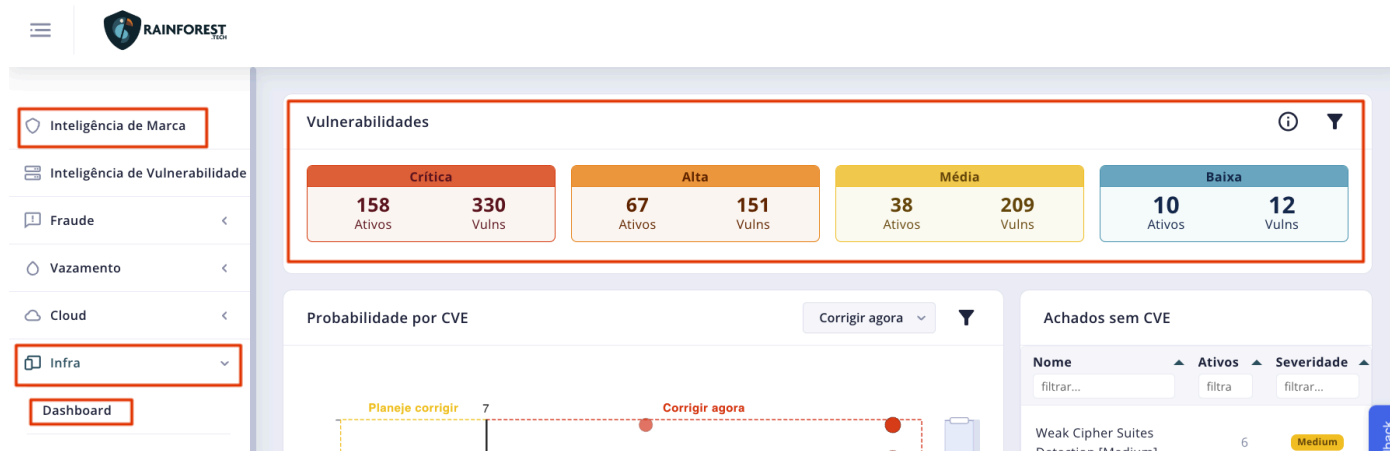
Technologies Discovery

Labels GERENCIAR RÓTULOS

 Nenhum rótulo foi atribuído a este recurso ainda. Clique no botão acima para gerenciar rótulos.

## Quantidade de Vulnerabilidades por Criticidade

Acesse o menu **Infra > Dashboard** ou **Inteligência de Marca** e visualize a quantidade de vulnerabilidades categorizadas por criticidade junto com a quantidade de ativos.



The screenshot shows the RAINFOREST dashboard with the 'Infra' menu selected. The 'Vulnerabilidades' section displays a summary of vulnerabilities categorized by severity:

Criticidade	Ativos	Vulns
Crítica	158	330
Alta	67	151
Média	38	209
Baixa	10	12

Below this, there is a 'Probabilidade por CVE' chart and a table of 'Achados sem CVE' (e.g., Weak Cipher Suites Detection with 6 Medium severity findings).

## Probabilidade por CVE

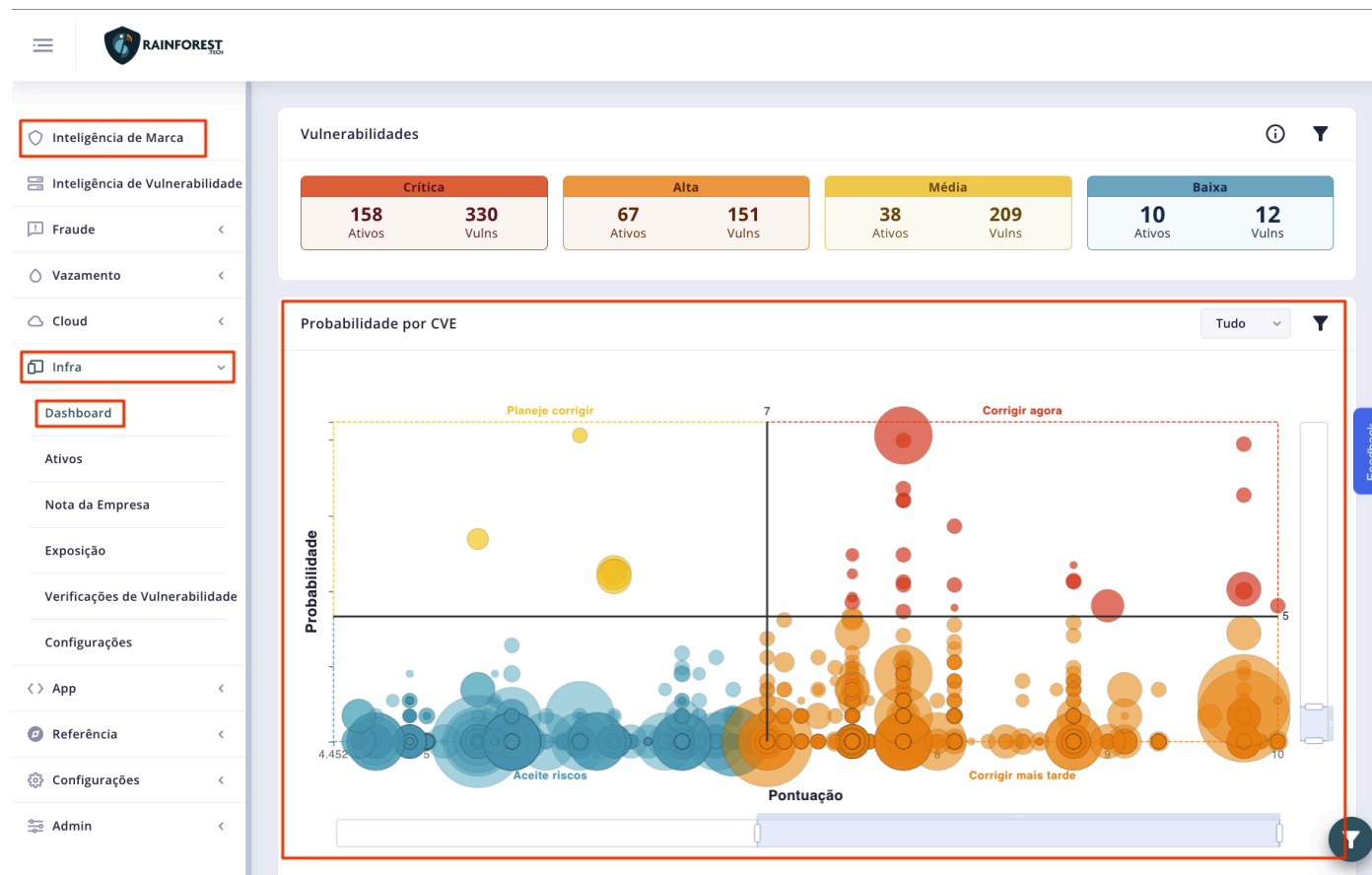
Disponibilizamos para os usuários o gráfico Probabilidade por CVE, aonde a plataforma correlaciona a pontuação (*score*) das vulnerabilidades divulgadas (eixo X) com o quanto ela está sendo falada em fóruns, portais, comunidades ou seja, sua probabilidade de utilização por atacantes (eixo Y).

Dividimos cada vulnerabilidade em 4 quadrantes principais, são eles:

- Corrigir agora
- Corrigir mais tarde
- Planeja corrigir
- Aceite riscos

Desta forma a plataforma aloca as vulnerabilidades em um dos quadrantes, possibilitando que a empresa consiga analisar e definir quais vulnerabilidades estão tendo um maior impacto ao negócio para a partir desse momento tomar as medidas cabíveis para solucioná-las.

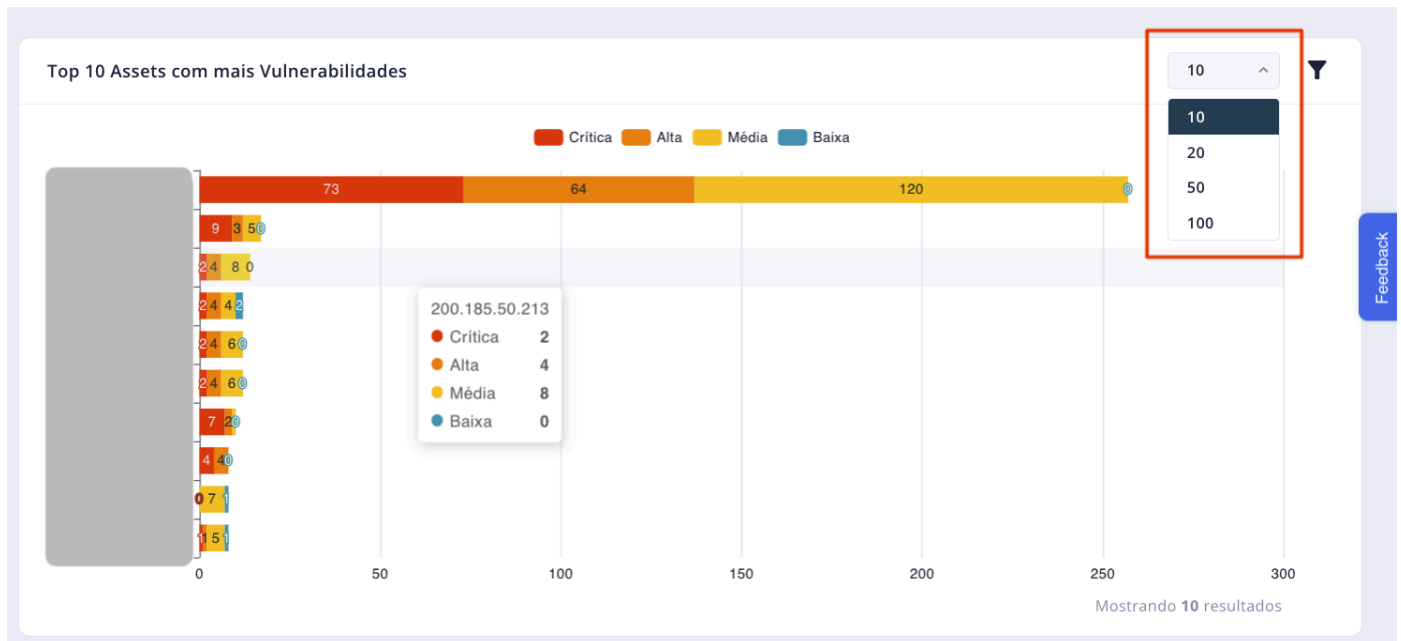
O gráfico está disponível nos menus **Inteligência de Marca e Infra > Dashboard**.



Passando o cursor do mouse pelos círculos no gráfico, a plataforma mostra a CVE, junto com a sua pontuação, quantidade de ativos impactados e suas probabilidades. Clicando sobre o círculo a plataforma realiza o filtro automaticamente, retornando a listagem dos ativos impactados.

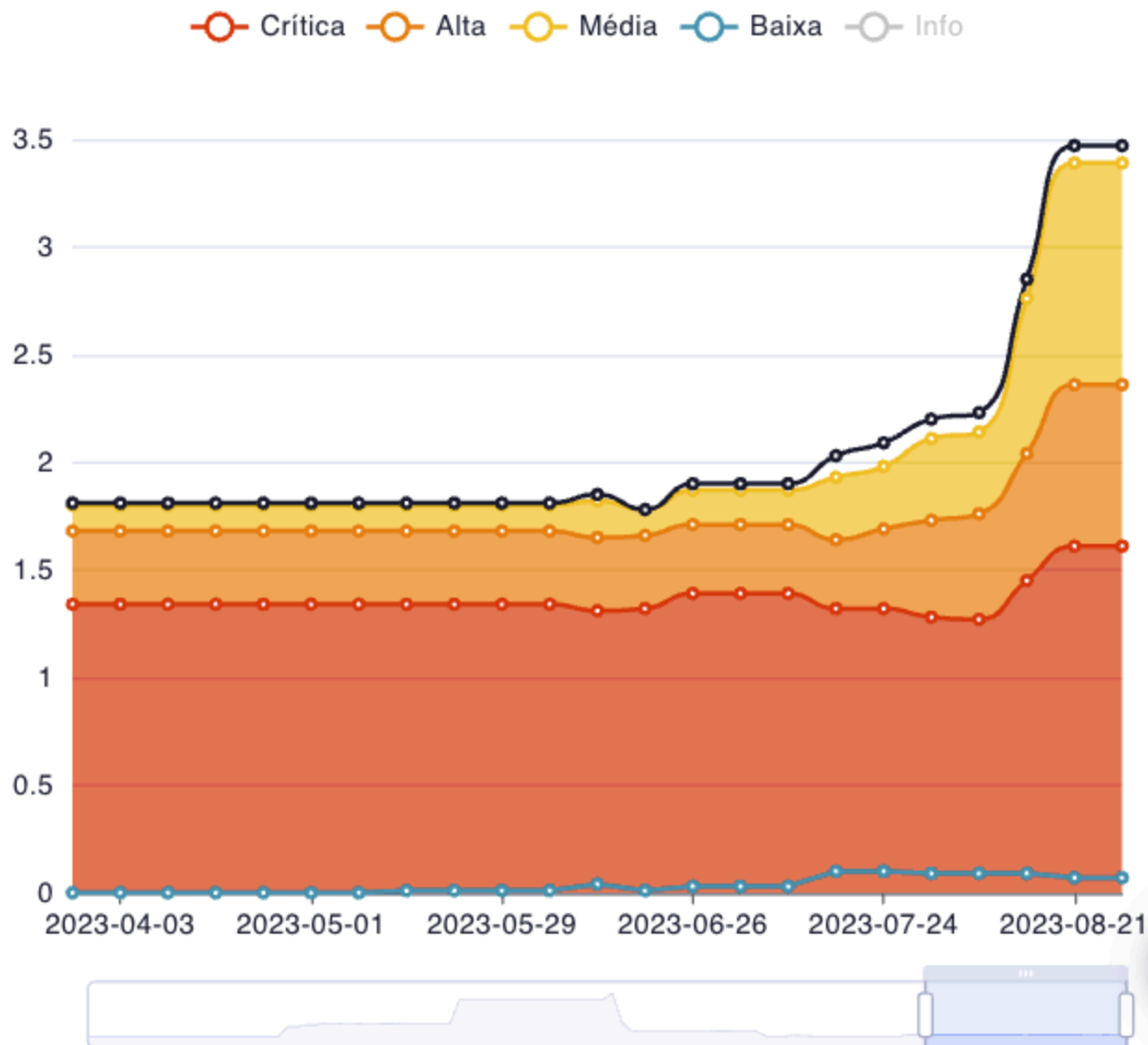
### Ativos com mais Vulnerabilidades

Clicando sobre a barra do respectivo asset, a plataforma realiza o filtro automaticamente, abrindo o pop-up com maiores detalhes. O usuário pode selecionar a quantidade de ativos que gostaria de visualizar, podendo selecionar entre as opções 10, 20, 50, 100.



### Histórico de Vulnerabilidades (Média por Ativo)

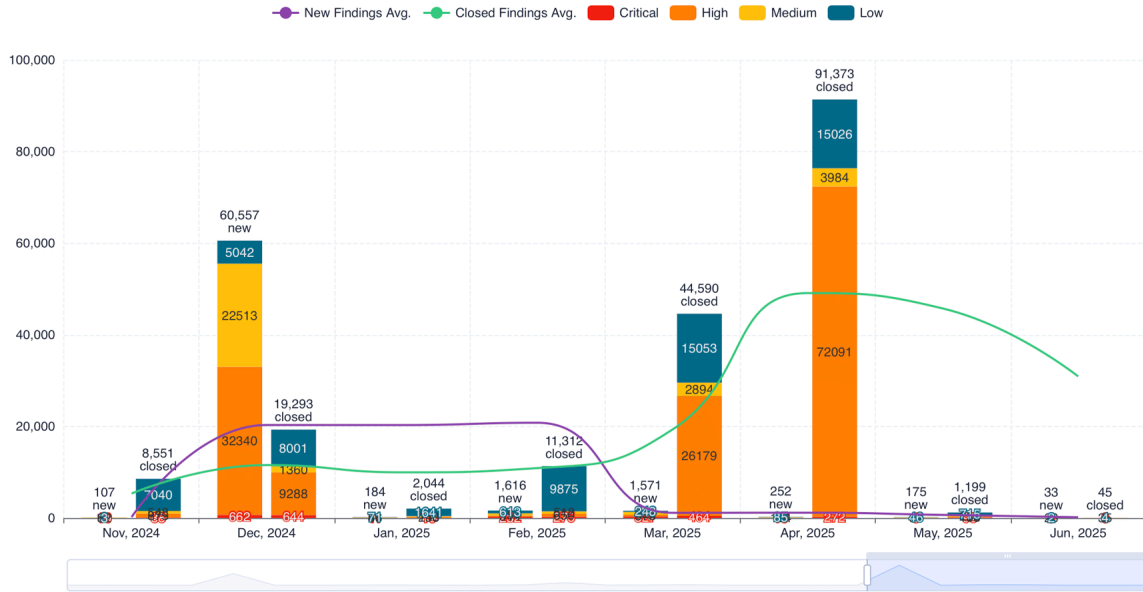
Acompanhe a média de vulnerabilidades por ativo na plataforma da Rainforest, para visualizar esse relatório acesse o menu **Infra > Dashboard**.



### Vulnerabilidades Novas e Fechadas por Período

Nesse gráfico você consegue ter uma visão histórica do número de vulnerabilidades encontradas por período, onde temos uma segmentação por severidade.

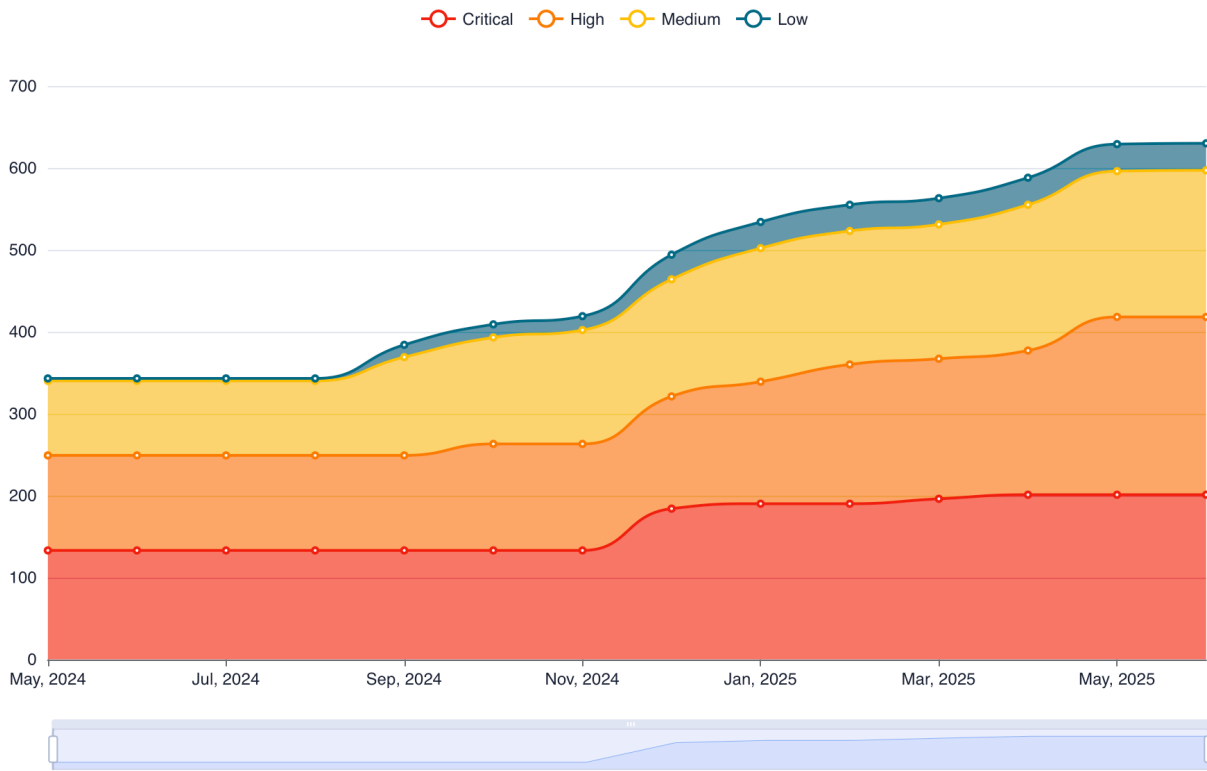
New and Closed by Period



### Evolução de Descobertas

Acompanhe o histórico de vulnerabilidades descobertas dentro de um período, para visualizar esse relatório acesse o menu **Inteligência de Vulnerabilidade**.

Findings Evolution

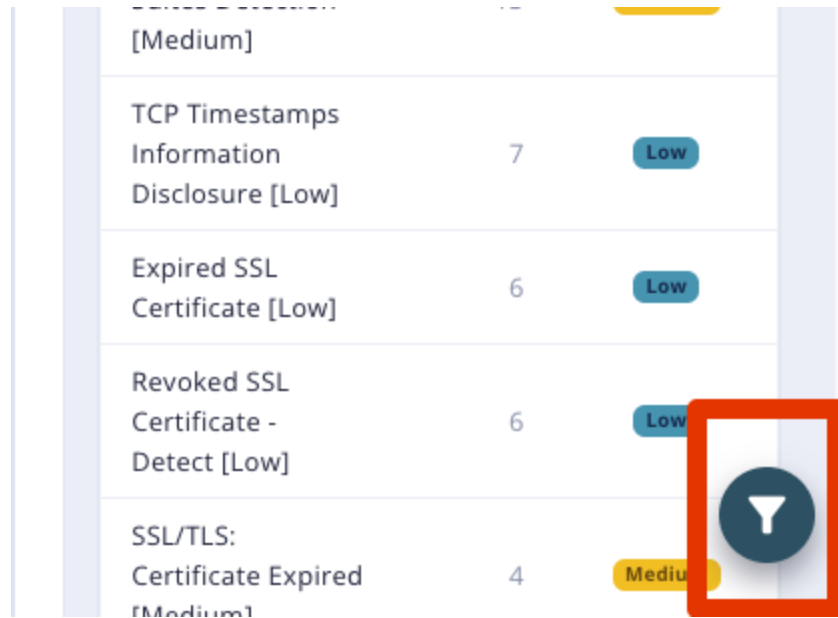


## Filtro em Vulnerabilidades

---

Caso não consiga ter a informação desejada através dos gráficos disponíveis atualmente, você pode utilizar a funcionalidade de **Filtro** para obter algo mais personalizado.

Clique no ícone de filtro presente no canto inferior direito da plataforma.



The image shows a table of vulnerabilities. The table has three columns: the name of the vulnerability, the count of occurrences, and the severity level. A filter icon (a funnel) is highlighted with a red square in the bottom right corner of the table area.

[Medium]		
TCP Timestamps Information Disclosure [Low]	7	Low
Expired SSL Certificate [Low]	6	Low
Revoked SSL Certificate - Detect [Low]	6	Low
SSL/TLS: Certificate Expired [Medium]	4	Medium

Depois faça o filtro conforme a sua necessidade, a medida que você for preenchendo os campos de filtro com a informação desejada, a plataforma realizará a atualização das informações na tela, retornando os dados que correspondem ao filtro.

# Entendendo Descobertas

---

 [support.rainforest.tech/pt-br/kb/entendendo-descobertas](https://support.rainforest.tech/pt-br/kb/entendendo-descobertas)

## **Entenda cada informação das descobertas realizadas pela Rainforest nas aplicações, ativos e cloud configuradas na plataforma.**

---

Ao realizarmos as parametrizações necessárias para que a plataforma da Rainforest comece a realizar suas análises, em pouco tempo ela começará a retornar para os usuários as descobertas de vulnerabilidades e/ou melhorias de código em aplicações, ativos e ambientes cloud.

É importante que o usuário entenda cada informação fornecida, desta forma, detalharemos cada sessão das informações fornecidas, vejamos abaixo.

1

No Default Hash [High]

2

SAST
High
8.9
×

3

**Details**

Discovery: 5/15/23 2:31 PM

(1/1) \* Possible vulnerability detected: No Default Hash  
 This App uses Hash Code. It's a weak hash function and should never be used in Secure Crypto Implementation. For more information checkout the CWE-327 (<https://cwe.mitre.org/data/definitions/327.html>) advisory.

4

**Fix Recommendations**

```
public int hashCode() {
```

5

**AI Recommendations (Beta Feature)**

Show AI Recommendations

Technical Recommendation:  
 The best practice to secure the code is to use a stronger cryptographic hashing algorithm such as SHA-256 or the bcrypt algorithm. These algorithms are more resistant to brute force attacks and provide stronger security for the application.

Example 1:  

```
public int hashCode() {
  return SHA256.hash(user);
}
```

Example 2:  

```
public int hashCode() {
  return BCrypt.hash(user);
}
```

6

**Application Details**

Group: **webgoat**  
 App: **webgoat**  
 Application URL: **webgoat**  
 Branch: **main**  
 Production Branch: **No**  
 Registry URL (Container Image): **webgoat/webgoat**  
 Repository URL: <https://github.com/WebGoat/WebGoat>

7

**Location**

File: `src/main/java/org/owasp/webgoat/container/users/WebGoatUser.java`  
 Line: 87  
 Position: 12

8

**Context**

```
public int hashCode() {
  return user.hashCode();
}
```

9

**References**

CWE (governance) <https://cwe.mitre.org/data/definitions/327.html>

10

**Compliance**

Sorry, no results found

11

**Actions**

	Description
<input type="checkbox"/> False Positive	<div style="border: 1px solid #ccc; padding: 5px; min-height: 40px;">Describe the reasons for this change</div>
<input type="checkbox"/> Prioritize	
<input type="checkbox"/> Mitigated	

SAVE

PREVIOUS

NEXT

1. **Título da Vulnerabilidade:** nome da vulnerabilidade encontrada.
2. **Classificação:** definidas pela plataforma com base no tipo de análise, severidade, e nota associadas a referencia da vulnerabilidade.
3. **Detalhes:** explicação mais detalhada da vulnerabilidade.
4. **Recomendações para Solucionar:** sugestão de recomendação de solução da vulnerabilidade fornecida pela plataforma caso já esteja disponível ou indicação do ponto mais crítico a ser corrigido.

2/3

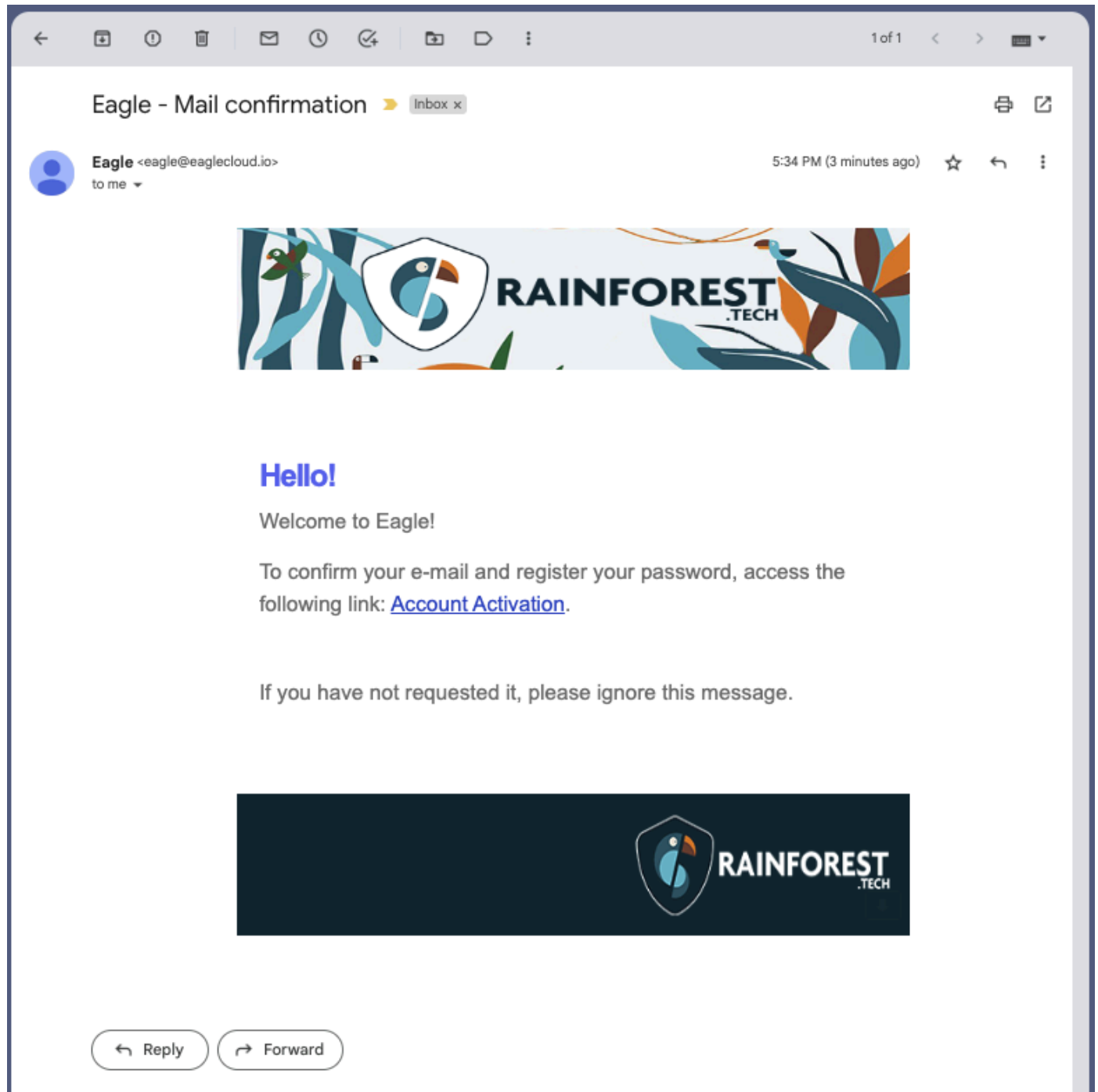
5. **Recomendações pela IA (Inteligência Artificial):** atualmente, para os casos de análises SAST que não haja recomendação pré-definida, a plataforma oferece a possibilidade do usuário ter uma recomendação de solução fornecida através de inteligência artificial. Neste caso, é importante estar ciente que os dados poderão ser submetidos a serviços externos à plataforma com o objetivo de identificar a melhor recomendação indicada.
6. **Detalhes da Aplicação:** maiores informações do item associado a vulnerabilidade como seu grupo, app, url, *branch*, se é uma branch de produção, registry url e url do repositório onde encontra-se hospedado.
7. **Localização:** informações de referência onde encontram-se a vulnerabilidade, por exemplo, em casos de descobertas relacionada a código: arquivo, linha e posição da vulnerabilidade.
8. **Contexto:** caso permitido pelo cliente, pequenos trechos de código podem ser coletados para que um contexto da vulnerabilidade seja oferecido aos desenvolvedores, a fim de permiti-los que identifiquem rapidamente a vulnerabilidade.
9. **Referências:** referências como artigos ou CVE(s) associadas a vulnerabilidade encontrada.
10. **Compliance:** caso a plataforma identifique algum padrão de conformidade conhecido associado, será indicado nesse espaço.
11. **Ações:** categorização manual das vulnerabilidades, podendo ser definida como falso positivo, priorizada ou mitigada. Vale ressaltar que a plataforma utiliza de mecanismos, entre eles Inteligência Artificial, para realizar classificações de forma automatizada e que caso a correção seja realizada em uma nova atualização do código (*commit* do desenvolvedor) a aplicação será analisada novamente.

# Primeiro acesso

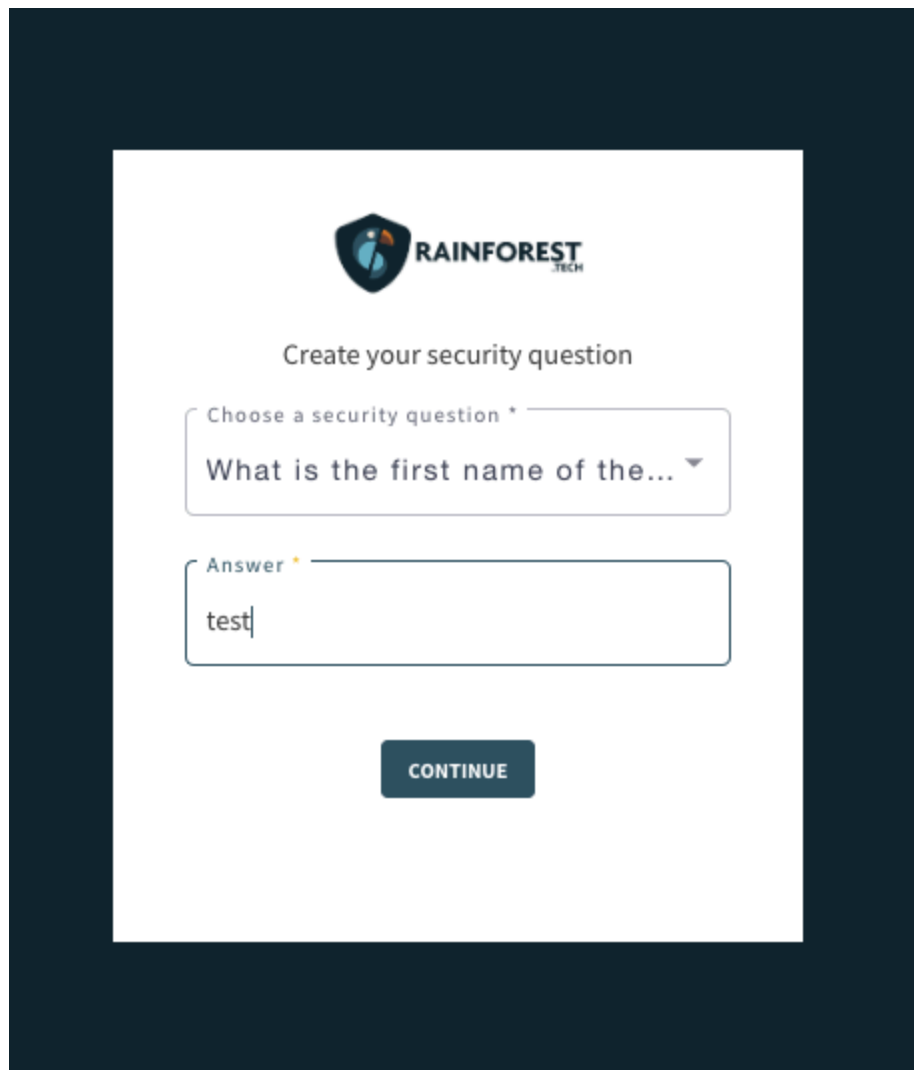
 support.rainforest.tech/pt-br/kb/primeiro-acesso

## Como realizar o primeiro acesso

Para se cadastrar no Rainforest você precisará receber um convite por e-mail de nosso time ou do time de uma empresa parceira Rainforest. Cada usuário do Rainforest App receberá esse e-mail de convite com um link para se registrar na plataforma, como no exemplo abaixo:



Ao receber o e-mail clique em **Account Activation**, abrirá uma nova aba em seu navegador o direcionando para a tela de registro. Nessa tela será solicitado que você escolha uma pergunta de segurança e digite uma resposta, feito isso clique em **Continuar**.



RAINFOREST  
TECH

Create your security question

Choose a security question \*

What is the first name of the... ▼

Answer \*

test

CONTINUE

Em seguida, digite e confirme a senha que será utilizada para logar no Rainforest. É exigido um nível mínimo de força/complexidade da senha para manter o padrão de segurança, devendo contar pelo menos:

- Uma letra minúscula
- Uma letra maiúscula
- Um número
- Um caractere especial
- No mínimo 8 caracteres



Choose your new password

New Password \*

.....



Your password must contain:

- A lowercase letter
- An uppercase letter
- A number
- A special character
- Minimum 8 characters

Confirm Password \*

.....|



CONTINUE

[← Back](#)

Clicando em **Continuar** você será direcionado para a tela de login, realize o login com seu e-mail e senha cadastrada anteriormente. Pronto, você estará logado na plataforma Rainforest.

RAINFOREST

0/100 Company Grade **F** 781 Credentials 9 Mobile Apps 345 Domains 0 Takedowns

Vulnerabilities By VA, By TECH, By SURFACE

Critical	High	Medium	Low	Info
63 Assets 81 Vulns	142 Assets 222 Vulns	22 Assets 24 Vulns	0 Assets 0 Vulns	1 Assets 18 Vulns

Likelihood by CVE Fix Now By VA, By TECH, By SURFACE

Related Info

Title	Source	Date

Latest Critical Vulnerabilities

Name	Severity	Affected Assets	Last Update (GM...)
CVE-2022-41074	MEDIUM	3	12/15/22, 8:30 PM
CVE-2022-41077	MEDIUM	2	12/15/22, 8:30 PM

A partir desse ponto você terá acesso a todas as funcionalidades adquiridas. [Conheça a plataforma](#), como ela é distribuída, navegação, funcionalidades gerais.

# Opções no Cadastro de uma Aplicação

---

 [support.rainforest.tech/pt-br/kb/opcoes-cadastro-aplicacao](https://support.rainforest.tech/pt-br/kb/opcoes-cadastro-aplicacao)

## Entenda cada parâmetro disponível e como utiliza-lo no cadastro de uma aplicação.

---

Ao abrir a tela de cadastro de aplicação você terá disponível 3 abas principais, **Aplicação**, **DockerFile** e **Owaspzap-contextfile**.

Este artigo descreve a principal delas onde são configurados os parâmetros para análise de aplicação (Aplicação).

As demais são utilizadas em casos específicos para:

- Realizar o *build* (caso DockerFile) em integrações específicas; e
- Possibilitar diferentes opções de autenticação (Owaspzap-contextfile).

**Em caso onde sejam necessárias configuração de tais parâmetros, o parceiro ou time Rainforest poderá auxiliar.**

## Aplicação

---

Na aba Application há parâmetros para o cadastro da aplicação na plataforma Rainforest.

Aplicação*	Grupo*		
Aplicação	Grupo		
Modelo de Pipeline*	Branch de Produção	Filtro de Branch	
Selecione um modelo	Nome da branch de produç	main master production	
URL do repositório Git (para SAST, SCA e QLT Scan)	Tipo	Caminho do Subprojeto	Credencial
Repositório Git	GIT	Caminho do Subprojeto	Selecione uma credenc...
URL do artefato (para baixar a dependência da compilação)	Tipo	Credencial	
URL de Artefato	Selecione u...	Selecione u...	
URL da imagem do contêiner no registro (para verificação de imagem)	Tipo	Credencial	
URL de Registro da Aplicação	Docker Regist...	Selecione u...	
URL UAT do aplicativo (para DAST)	Type of SCAN	Tipo	
Aplicação	Basic	Selecione u...	
Exposto a	Impacto nos Negócios		
Selecione uma exposiç...	Selecione o impacto no...		

SALVAR

- **Grupo:** grupo no qual a aplicação que está sendo cadastrada fará parte, pode ser um sistema, squad ou outra forma de agrupar que faça sentido para a empresa ou negócio.
- **Aplicação:** nome da aplicação que está sendo cadastrada
- **Modelo de Pipeline:** permite configurar quais serão as análises realizadas na plataforma Rainforest, por exemplo, SAST, SCA, DAST etc; caso não haja uma configuração disponível na sua tela, o parceiro ou time Rainforest poderá auxiliar com tal configuração.
- **Branch de Produção:** nome da *branch* de produção; tal informação será utilizada para permitir a comparação de evolução do código em análises da plataforma, por exemplo, o código analisado na última análise está igual ou superior (em termo de achados) com o código em produção?
- **Filtro de Branch:** permite especificar quais *branches* (ramificações do desenvolvimento) serão analisadas pela plataforma, por exemplo, *main*, *master*, *production* ou outras que façam sentido à esteira de desenvolvimento (*pipeline*) em questão; quando houver um *commit* em uma das *branches* especificadas a plataforma iniciará automaticamente as análises com base nas informações que estão definidas nos próximos parâmetros.

- **URL do repositório Git (para SAST, SCA e QLTy Scan):** trata-se do endereço do repositório que será utilizado para análise; tal endereço deve ser especificado na forma que o repositório permite que seja clonado o código usando o protocolo git, por exemplo, se HTTPS (<https://gitlab.internal/>) ou se SSH (<ssh://gitlab.internal/path>).
  - **Tipo:** atualmente, a plataforma da Rainforest suporta GIT como protocolo para clonar um projeto e analisar o código; caso utilize alguma outra solução entrar em contato com parceiro ou time Rainforest para analisar possibilidade de realizar um *proxy* entre tecnologias.
  - **Caminho do Subprojeto:** tal campo pode ser usado para especificar o subprojeto que será analisado dentro de um repositório.
  - **Credencial:** deve ser configurada no menu Configurações > Credenciais indicando user/pass (se HTTPS) ou user/privatekey (se SSH); uma forma de verificar se está funcionando corretamente é realizar um *git clone* com os parâmetros especificados diretamente máquina onde rodam os processos de análise Rainforest dentro do ambiente.
- **URL do artefato (para baixar a dependência da compilação):** endereço do repositório de artefatos para *build* (compilação) do código; se o repositório / endereço for interno, especificar o caminho (<https://npm.internal/> ou <https://atf.internal:443>), caso o endereço não seja interno a plataforma irá buscar o endereço externamente e, para tanto, necessitará ter acesso à Internet.
 

**Tipo:** especifica a forma de acesso a URL do artefato:

  - **OPEN\_URL:** acesso direto via http ou https.
  - **AWS\_S3:** repositório de arquivos na nuvem pública da AWS.
  - **MAVEN:** ferramenta de automação de *build* (compilação).
  - **GOOGLE\_PLAY:** busca direta do artefato .APK na Google Play; se o arquivo APK já estiver no repositório GIT, este já será analisado.
  - **NEXUS:** gerenciador de repositório que provê uma plataforma centralizada para armazenar artefatos.
- **Credencial:** deve ser configurada no menu **Configurações > Credenciais** indicando usuário, senha e o tipo (GIT).
- **URL do repositório (registry) de imagens (container docker):** endereço do repositório onde tem os modelos imagens que são utilizados para rodar a aplicação, por exemplo, <example.com:443/nexus3/repository/docker-hosted/some/custom/image> ou <nexus.internal:18442/company/image:1.3.1-RELEASE>.
  - **Tipo:** atualmente, a plataforma da Rainforest suporta Docker Registry.
  - **Credencial:** deve ser configurada no menu Configurações > Credenciais indicando usuário, senha e o tipo (REGISTRY).

- **URL UAT do aplicativo (para DAST):** endereço da aplicação para realização das análises dinâmicas, por exemplo `http://example.com/application` ou `https://example.internal/application`.
    - **Tipo de SCAN:** diferentes tipos de varredura podem ser selecionados de acordo com o ambiente, profundidade e análise que será realizada
      - **Basic:** conjunto de testes básicos no endereço que evitam gerar indisponibilidade da URL testada; tal teste é recomendado para ser aplicado inicialmente em ambiente de produção.
      - **Advanced (can stop services):** conjunto avançado de testes no endereço especificado que podem parar ou degradar o serviço; tal análise é recomendada apenas em ambiente de homologação ou ambientes controlados onde sejam conhecidos os impactados na parada de um serviço.
      - **API:** análise de API (*Application Programming Interface*) utilizando diferentes tipos de especificação: API-OpenAPI, API-SOAP e API-GraphQL.
    - **Tipo:** tal parâmetro está relacionado a autenticação, ou seja, se os testes que serão executados serão feitos após autenticação na página indicada;
      - **Not Authenticated:** nesta opção não haverá autenticação e os achados de vulnerabilidade serão identificados, por exemplo, com base em retornos do servidor ou ataques aos campos de formulário da aplicação.
      - **WebForm:** nesta opção é possível indicar qual a página inicial que permite a autenticação na aplicação para que - na sequencia - sejam realizados testes.
        - **Application UAT URL Login:** endereço específico da página que permite a autenticação na aplicação.
        - **Credential:** credenciais de autenticação que devem ser configuradas no menu Configurações > Credenciais indicando usuário e senha.
        - **ID campo user:** identificador do campo do formulário que deve receber a informação de usuário no momento da autenticação durante a análise.
        - **ID campo pass:** identificador do campo do formulário que deve receber a informação de password no momento da autenticação durante a análise.
        - **ID campo submit:** identificador do campo que submete as informações e consequentemente dispara o processo de autenticação na aplicação.
- Havendo necessidade de autenticações mais complexas, poderá ser usado a configuração do **Owaspzap-contextfile**, conforme indicado no início deste artigo. Para tanto, o parceiro ou time Rainforest poderá auxiliar no processo.
- **Exposto a:** este parâmetro permite classificar qual o nível de exposição da aplicação para facilitar a filtragem, ou seja, se está exposta na Internet (Web), apenas interna (Internal) ou se não deve considerar tal informação (None).
  - **Impacto nos Negócios:** de forma análoga, este parâmetro permite classificar qual o nível de impacto que a aplicação tem no negócio da empresa: baixo, médio, alto ou crítico; pode ser usado, também, como um parâmetro para filtrar as informações que são exibidas nos painéis da plataforma.

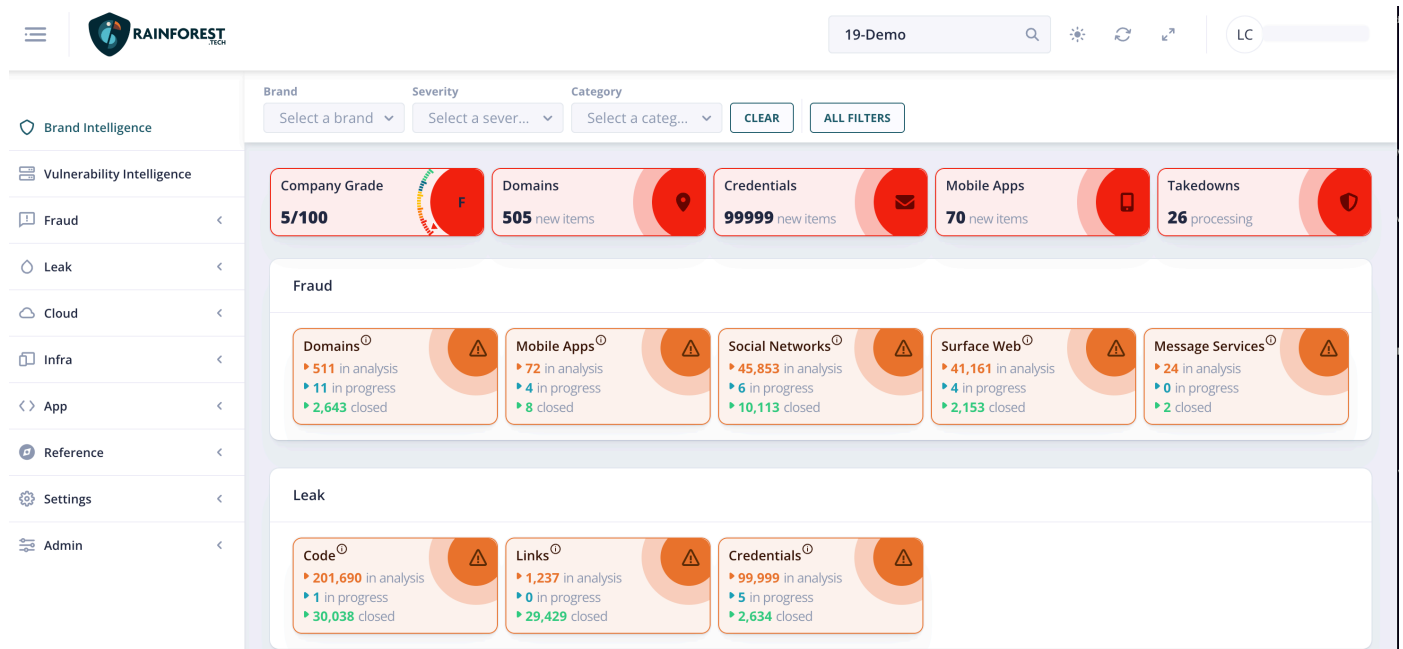
# Quais módulos compõem a solução de Inteligência de Marca?

 [support.rainforest.tech/pt-br/kb/modulos-inteligencia-de-marca](https://support.rainforest.tech/pt-br/kb/modulos-inteligencia-de-marca)

A solução de Inteligência de Marca da Rainforest é composta por dois módulos:

- **[Fraude](#)**  
Obtenha dados em tempo real sobre domínios fraudulentos, URLs, perfis e páginas em redes sociais se passando por sua empresa na tentativa de fraudar.
- **[Vazamento](#)**  
Monitore se dados, credenciais e outras informações de sua empresa foram vazadas e estão à venda na surface, deep e dark web.

Através de um dashboard, computamos e centralizamos os principais índices para ajudar nas visões macros e tomadas de decisões.



# Fontes, Resultados e Integrações da Plataforma

---

 [support.rainforest.tech/pt-br/kb/rf-fontes-resultados-integracoes](https://support.rainforest.tech/pt-br/kb/rf-fontes-resultados-integracoes)

## Conheça algumas fontes, resultados e integrações da plataforma

---

A plataforma Rainforest tem sua própria base de conhecimento, consulta diversas bases externas e também tem integrações para disponibilizar informações para outras soluções. As informações obtidas são processadas pelos algoritmos internos, os resultados são classificados e, quando relevantes, exibidos nos respectivos menus de interesse dentro da plataforma.

**Atualizações:** a lista a seguir é atualizada constantemente e por questões de segurança, sigilo de contrato e/ou estratégia de negócio nem todas essas informações são citadas neste documento.

**Confidencial:** apenas para uso de clientes Rainforest, não deve ser compartilhado em parte ou no todo.

A lista a seguir contem exemplos de algumas das principais fontes, resultados e integrações da plataforma:

- Apkfun
- Apkmirror
- Appbrain
- Apple Store
- Aptoide
- AWS (*Amazon Web Services*)
- Bing
- Bitbucket
- Bug Bounty
- Certificados (crt.sh)
- CVEs (NIST)
- CWE (MITRE)
- CyberArk
- DuckDuckGo
- Exploit-db
- Facebook
- Fóruns públicos e privados (quando adquirido serviços gerenciados dos parceiros)
- GCP (*Google Cloud Platform*)
- GitHub
- GitLab

- Google
- Google Play
- Hashcorp Vault
- IBM Security Verify Privilege Vault
- Instagram
- Jira
- LinkedIn
- Mercado Livre
- Microsoft Azure
- Mozilla Observatory
- Nessus Pro
- OCI (*Oracle Cloud Infrastructure*)
- OLX
- ONION
- OpenVAS
- Outros serviços de mensageiria (quando adquirido serviços gerenciados dos parceiros)
- OWASP (*Open Web Application Security Project*)
- Pastebin
- Phishtank
- Postman
- RSS
- Senhasegura
- Service Now
- Shodan
- Slack
- Sonarqube
- Swagger
- Teams
- Telegram
- TikTok
- Trend Micro Vision One
- TTP (MITRE)
- Twitter
- Veracode
- Virus Total
- Wazuh
- Yahoo

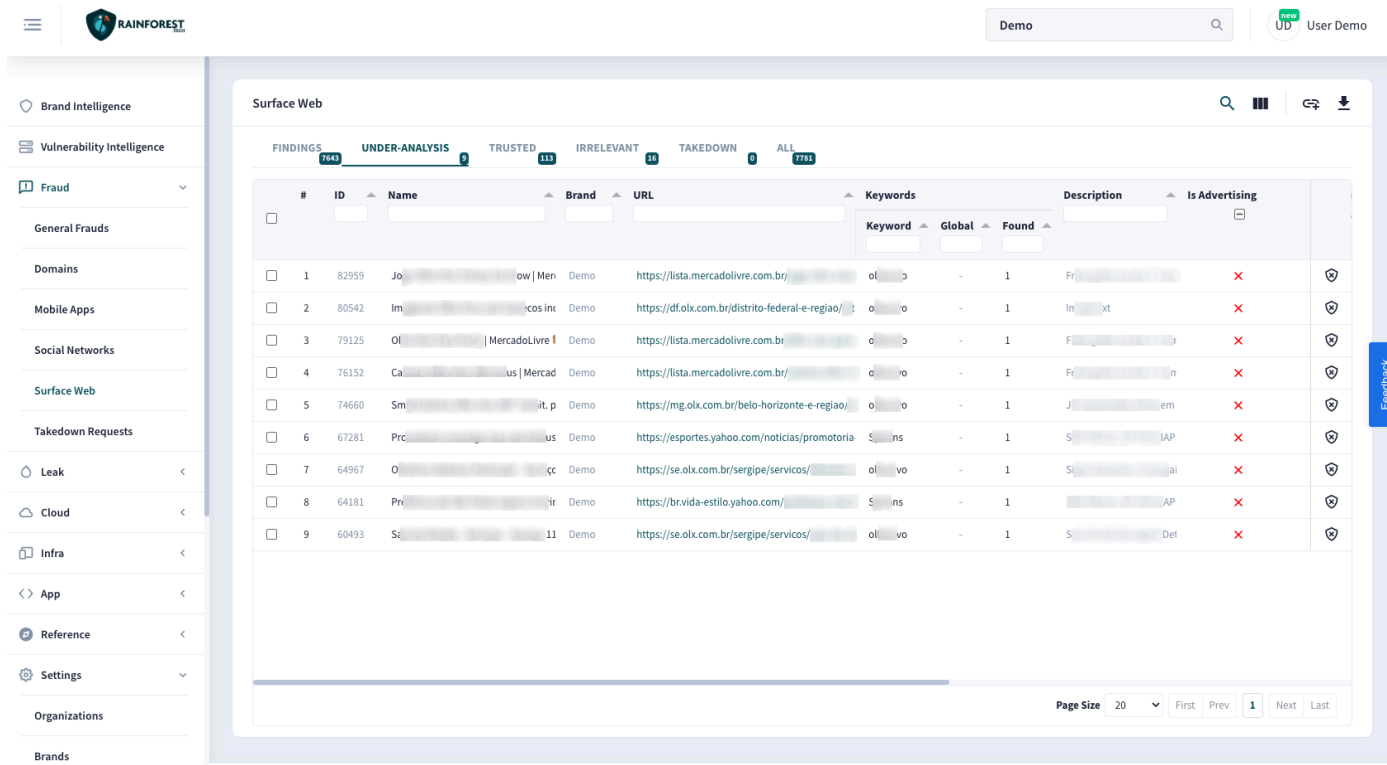
# Fraude na Surface Web

 support.rainforest.tech/pt-br/kb/fraude-surface-web

## Entenda como a plataforma Rainforest monitora a Surface Web em busca de fraudes

Além de fraudes específicas em domínios, aplicativos móveis e redes sociais, é de conhecimento que os golpistas podem publicar conteúdos em outros locais na web visando que a vítima seja direcionada para, por exemplo, uma venda de produto falsa em nome da empresa (marca). Para endereçar tal situação, a plataforma da Rainforest faz a busca de informações na Surface Web através de indexadores de conteúdo e buscas diretas na web. Tal busca permite monitorar e obter informações que vão além daquelas indexadas em outras funcionalidades da plataforma trazendo uma cobertura ainda maior. Com isso, podemos identificar outras redes sociais (além daquelas que estão em Redes Sociais), sites de venda de produtos, gestão de projetos, fóruns e muitos outros.

Tal funcionalidade está inclusa no módulo de **Fraude** e pode ser acessada em **Fraude > Surface Web**.



The screenshot displays the Rainforest platform interface. On the left is a navigation sidebar with categories like Brand Intelligence, Vulnerability Intelligence, Fraud, Domains, Mobile Apps, Social Networks, Surface Web, Takedown Requests, Leak, Cloud, Infra, App, Reference, Settings, Organizations, and Brands. The main content area is titled 'Surface Web' and shows a table of search results. The table has columns for #, ID, Name, Brand, URL, Keywords, Description, and Is Advertising. The results list various fraudulent listings on platforms like MercadoLivre and OLX. At the bottom right, there is a 'Page Size' dropdown set to 20 and navigation buttons for 'First', 'Prev', '1', 'Next', and 'Last'.

#	ID	Name	Brand	URL	Keywords	Description	Is Advertising
1	82959	Jo...ow   Men	Demo	https://lista.mercadolivre.com.br/...	ol	Fr...	×
2	80542	Im...cos Inv	Demo	https://df.olx.com.br/distributo-federal-e-regiao/...	ol	ln...xt	×
3	79125	Ol...   MercadoLivre	Demo	https://lista.mercadolivre.com.br/...	ol	Fr...	×
4	76152	Ca...us   Mercad	Demo	https://lista.mercadolivre.com.br/...	ol	Fr...n	×
5	74660	Sm...it.p	Demo	https://mg.olx.com.br/belo-horizonte-e-regiao/...	ol	J...em	×
6	67281	Prc...us	Demo	https://esportes.yahoo.com/noticias/promotoria...	S...ns	S...IAP	×
7	64967	O...çç	Demo	https://se.olx.com.br/sergipe/servicos/...	ol	S...ai	×
8	64181	Pr...ir	Demo	https://br.vida-estilo.yahoo.com/...	S...ns	...AP	×
9	60493	Sc...	Demo	https://se.olx.com.br/sergipe/servicos/...	ol	S...Det	×

Para redes sociais e outros itens que não tenham uma categoria específica na plataforma, serão listados no menu **Surface Web** da plataforma, um exemplo desse cenário é a rede social empresarial **LinkedIn**.

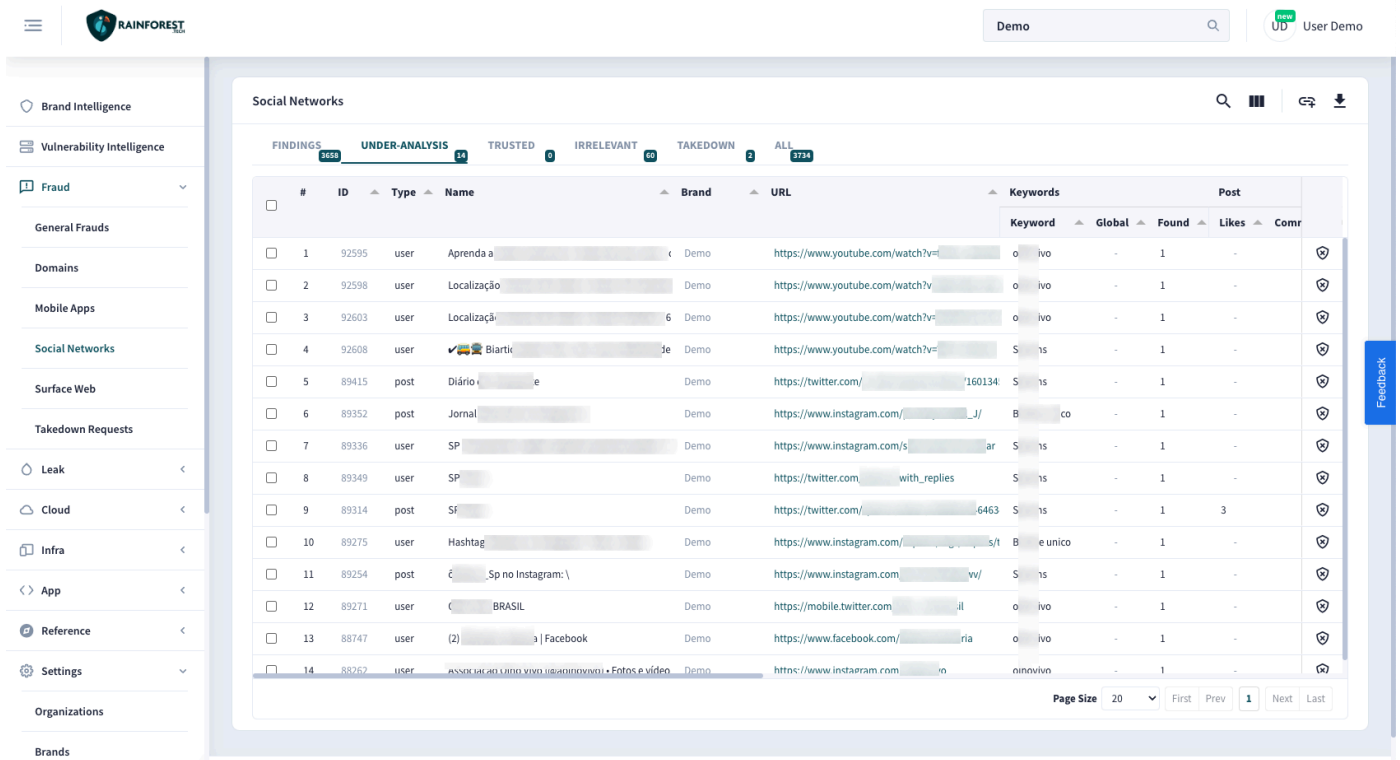
# Fraude em Redes Sociais

 support.rainforest.tech/pt-br/kb/fraude-redes-sociais

## Entenda como a plataforma Rainforest monitora fraudes de Redes Sociais

Certamente, você já ouviu falar de golpes relacionados às redes sociais. Não é incomum ouvir que uma empresa teve sua página copiada e que seus clientes estão sendo prejudicados com tal fraude. Golpistas tem copiado páginas para se passar por empresas a fim de aplicar golpes que geram prejuízos financeiros e de imagem para a marca (reputação). Quanto antes tal evento for detectado mais rápido a possibilidade de validar se, de fato, trata-se de um incidente e tomar as ações necessárias em resposta ao incidente. A plataforma da Rainforest monitora de forma automática e periodicamente usuários (users), páginas (pages) e postagens (posts) que façam menção as palavras-chaves (keywords) da empresa que são monitorados com o objetivo de identificar possíveis fraudes. Nesta funcionalidade, a plataforma considera itens que são aplicados ao contexto de redes sociais como curtidas (*likes*), comentários, compartilhamentos, seguidores etc. A plataforma monitora redes sociais como Facebook, Instagram, X (Twitter), Youtube e TikTok através desta funcionalidade. Além dessas redes sociais, outras também são monitoradas dentro de Surface Web. Como exemplo temos LinkedIn, entre outras.

Tais funcionalidades estão inclusas no módulo de Fraude (*Fraud*) e podem ser acessadas em **Fraude > Redes Sociais** e **Fraude > Surface Web**.



The screenshot displays the Rainforest platform interface for monitoring social media fraud. The main content area is titled "Social Networks" and shows a list of findings. The interface includes a sidebar with navigation options and a top navigation bar with a search bar and user information.

#	ID	Type	Name	Brand	URL	Keywords			Post	
						Keyword	Global	Found	Likes	Comr
1	92595	user	Aprenda a	Demo	https://www.youtube.com/watch?v=	o	ivo	-	1	-
2	92598	user	Localização	Demo	https://www.youtube.com/watch?v=	o	ivo	-	1	-
3	92603	user	Localizaçã	Demo	https://www.youtube.com/watch?v=	o	ivo	-	1	-
4	92608	user	Biartico	Demo	https://www.youtube.com/watch?v=	S	1s	-	1	-
5	89415	post	Diário	Demo	https://twitter.com/	S	1s	-	1	-
6	89352	post	Jornal	Demo	https://www.instagram.com/	B	co	-	1	-
7	89336	user	SP	Demo	https://www.instagram.com/s	S	1s	-	1	-
8	89349	user	SP	Demo	https://twitter.com/	S	1s	-	1	-
9	89314	post	Sf	Demo	https://twitter.com/	S	1s	-	1	3
10	89275	user	Hashtag	Demo	https://www.instagram.com/	B	e unico	-	1	-
11	89254	post	Sp no Instagram	Demo	https://www.instagram.com/	S	1s	-	1	-
12	89271	user	BRASIL	Demo	https://mobile.twitter.com/	o	ivo	-	1	-
13	88747	user	(2) Facebook	Demo	https://www.facebook.com/	o	ivo	-	1	-
14	88752	user	ASSISTIR AO LIVE	Demo	https://www.instagram.com/	n	n	-	1	-

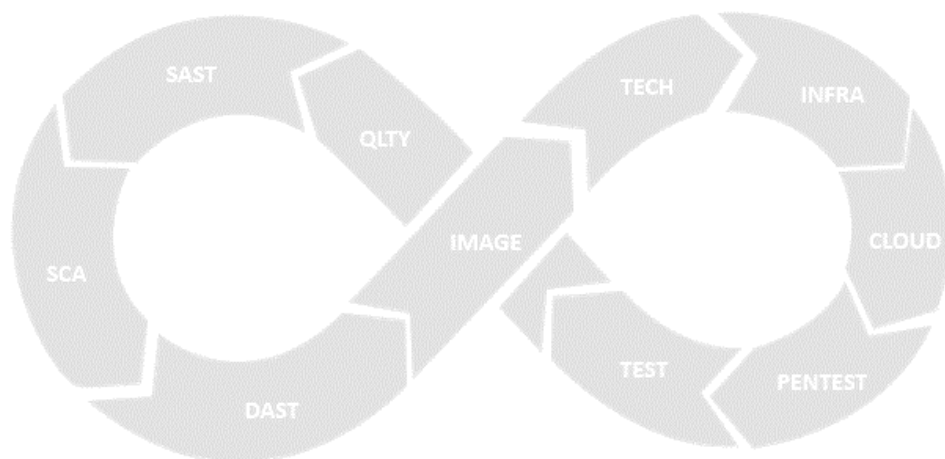
# Visão Geral App

 [support.rainforest.tech/pt-br/kb/visao-geral-app](https://support.rainforest.tech/pt-br/kb/visao-geral-app)

## Descubra todos os benefícios que o módulo de App do Rainforest pode trazer para seu processo de desenvolvimento.

Olhar para vulnerabilidades e melhorias de código em aplicação no tempo de desenvolvimento pode ser um desafio para as equipes que constroem soluções. Nesse sentido a plataforma da Rainforest auxilia equipes a terem uma visão clara através de suas análises.

A Rainforest fornece um panorama de todo o ciclo **DevSecOps**, quando falamos de aplicações, de forma clara e objetiva os usuários tem acesso as descobertas feitas pelas análises que auxiliam no desenvolvimento seguro das aplicações, são elas:



ADD SEC TO YOUR DEVOPS

- **QLTY**: descobertas das análises relacionadas a qualidade de código das aplicações
- **SAST**: descobertas das análises relacionadas a código fonte das aplicações
- **SCA**: descobertas das análises relacionadas a código de terceiros, por exemplo, bibliotecas, frameworks que a aplicação utilize.
- **DAST**: descobertas relacionadas a análise dinâmicas que a plataforma realiza, por exemplo, submissão de conteúdo (tentativa de SQL Injection) em campos de formulário.
- **IMAGE**: descobertas relacionadas a imagens Docker cadastradas da plataforma
- **MAST**: descobertas relacionadas a aplicações mobile cadastradas na plataforma
- **IAC**: descobertas vinculadas as análise referentes a infraestrutura como código

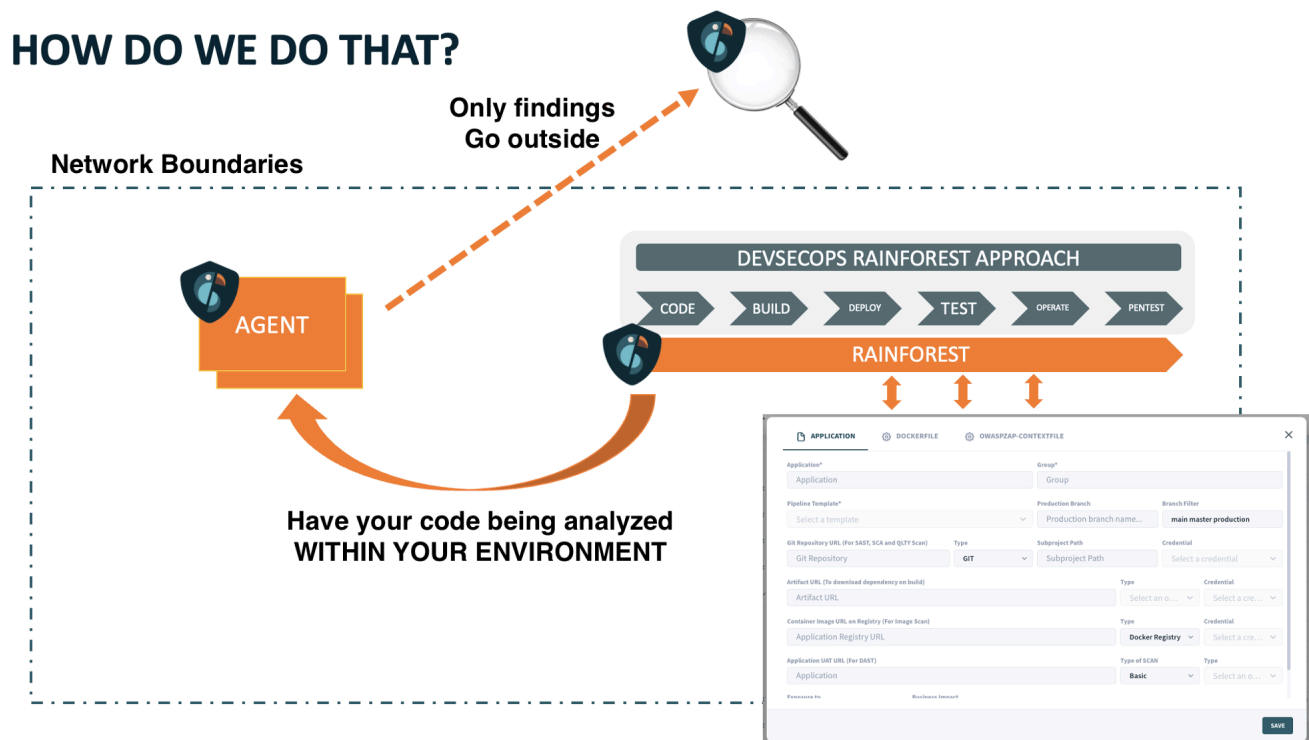
Desta forma a equipe de desenvolvimento tem de forma centralizada uma visão de todas as vulnerabilidades e melhorias de código que devem ser tratadas antes do código da aplicação ir para produção. As análises de código realizadas pela plataforma acontecem a cada commit enviado pelo desenvolvedor, trazendo para aplicação praticamente em tempo real se o código criado possui alguma vulnerabilidade ou melhoria a ser feita.

Veja em [Gráficos e Filtros em Aplicações](#) como utilizar os dashboards e analisar cada descoberta feita pelo Rainforest.

## Seu Ambiente, Seu Código

Sabemos que para a maioria das empresas atuais, a privacidade é um ponto crucial do negócio, principalmente relacionado a código, visto que o código na maioria dos cenários atuais está diretamente ligado ao produto e/ou serviço que a empresa oferece.

Desta forma, a Rainforest tem a preocupação para que tanto as análises quanto os códigos fontes permaneçam na infraestrutura do cliente, ou seja, não seja levado para ambientes externos.



Como representado na imagem acima, a instalação dos analisadores (agentes) e as análises são realizadas dentro da infraestrutura do cliente, sendo encaminhado para a nuvem da Rainforest apenas as descobertas dessas análises.

Para os casos de análises de códigos fonte, a Rainforest possibilidade que apenas o trecho do código onde foi diagnosticado a vulnerabilidade ou melhoria seja levado para a nuvem da Rainforest, para que um contextualização sobre a descoberta seja oferecida para o desenvolvedor dentro da plataforma.

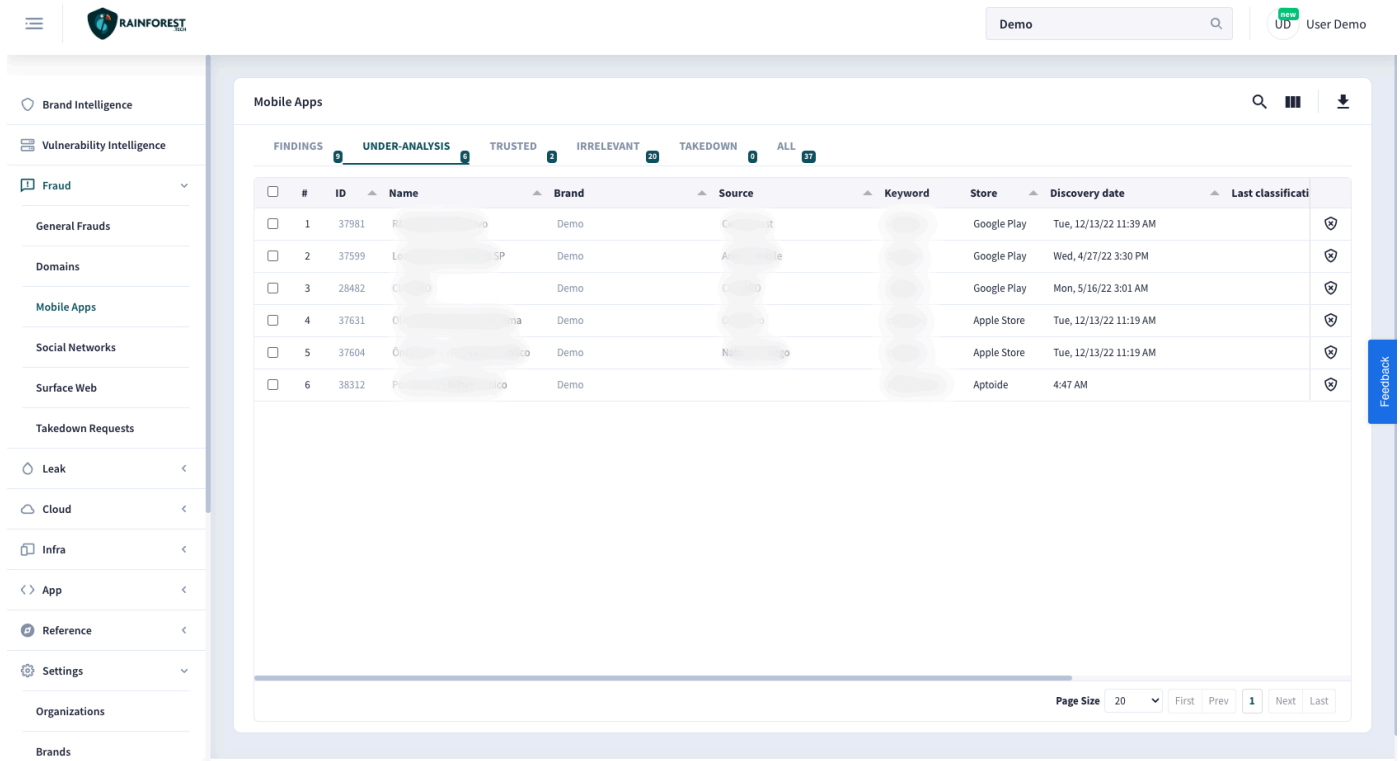
# Fraude em Aplicativos Móveis (App)

 support.rainforest.tech/pt-br/kb/fraude-aplicativos-moveis

## Entenda como a plataforma Rainforest monitora fraudes de Aplicativos Móveis (App)

Uma das formas que os golpistas utilizam para obter informações pessoais ou mesmo pagamentos indevidos é através dos aplicativos (apps) de dispositivos móveis como celulares, tablets etc. Para tanto, um desenvolvedor que não está devidamente credenciado ou autorizado a desenvolver uma aplicação em nome de uma determinada empresa (marca), pode criar uma aplicação e publica-la em lojas de aplicativos oficiais ou mesmo repositórios públicos na web. Em lojas de aplicativos oficiais, como Apple Store, Google Play e Aptoide, a dificuldade de encontrar tais aplicativos falsos é maior, pois existem processos de publicação que dificultam a ação de atacantes mal-intencionados. Mesmo assim, é possível identificar aplicativos de desenvolvedores independentes que citam termos, palavras-chave (*keywords*), que fazem referência ou alusão à marca da empresa. A plataforma Rainforest monitora lojas de aplicativos oficiais bem como sites de referência (que listam arquivos APKs, por exemplo) que disponibilizam aplicativos na web.

Tal funcionalidade está inclusa no módulo de Fraude (*Fraud*) e pode ser acessada em **Fraude > Aplicativos Móveis**.



The screenshot shows the Rainforest platform interface. The main content area displays a table of mobile apps under analysis. The table has the following columns: #, ID, Name, Brand, Source, Keyword, Store, Discovery date, and Last classified. The data is as follows:

#	ID	Name	Brand	Source	Keyword	Store	Discovery date	Last classified
1	37981	...	Demo	...	...	Google Play	Tue, 12/13/22 11:39 AM	OK
2	37599	...	Demo	...	...	Google Play	Wed, 4/27/22 3:30 PM	OK
3	28482	...	Demo	...	...	Google Play	Mon, 5/16/22 3:01 AM	OK
4	37631	...	Demo	...	...	Apple Store	Tue, 12/13/22 11:19 AM	OK
5	37604	...	Demo	...	...	Apple Store	Tue, 12/13/22 11:19 AM	OK
6	38312	...	Demo	...	...	Aptoide	4:47 AM	OK

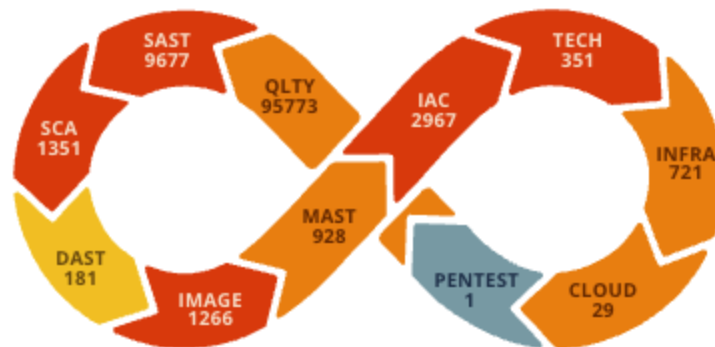
# O que é Inteligência de Vulnerabilidade?

 support.rainforest.tech/pt-br/kb/definicao-inteligencia-de-vulnerabilidade

**Todo ativo ou desenvolvimento está sujeito a vulnerabilidades e encontrá-las o quanto antes é fundamental para evitar problemas mais graves.**

Seja você um profissional de infraestrutura, nuvem ou desenvolvimento, uma coisa é fato: em algum momento vai se deparar com vulnerabilidades, sejam elas de gravidade mais leve ou mais alta. Inteligência de vulnerabilidade é o processo de coletar, analisar e disseminar informações sobre vulnerabilidades potenciais em sistemas, redes e ambientes. Esta informação pode incluir detalhes sobre falhas de segurança ou outros tipos de vulnerabilidades que podem ser exploradas por atacantes para comprometer a segurança de um sistema. A inteligência de vulnerabilidade é importante porque ajuda a identificar e mitigar vulnerabilidades antes que elas sejam inseridas no ambiente de produção e exploradas por atacantes. Isso pode ajudar a proteger sistemas e redes de ataques cibernéticos e outras ameaças à segurança proativamente. Além disso, a inteligência de vulnerabilidade também pode ser usada para avaliar a exposição de uma organização a ameaças cibernéticas e para tomar medidas para minimizar essa exposição.

## Status DevSecOps



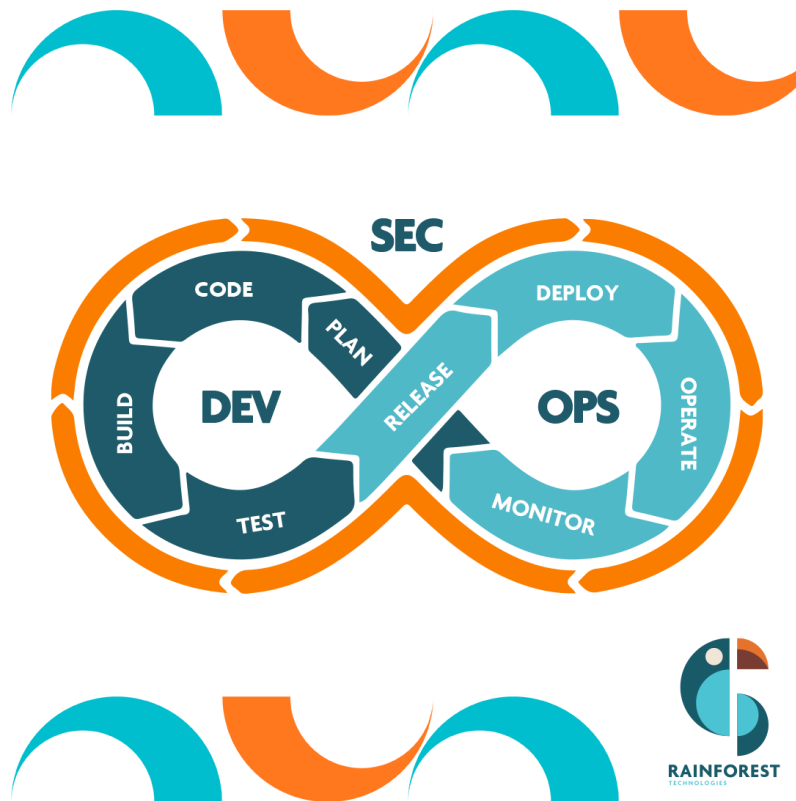
A comunicação entre a plataforma da Rainforest e a estrutura do cliente para realização das análises é feita de forma segura com criptografia e através de chaves de API, mantendo assim a segurança e sigilo dos dados e vulnerabilidades encontradas no ambiente.

# DevSecOps com Rainforest

 [support.rainforest.tech/pt-br/kb/devsecops-rainforest](https://support.rainforest.tech/pt-br/kb/devsecops-rainforest)

## Adicionando segurança em esteiras de desenvolvimento DevOps, transformando-as em DevSecOps com Rainforest

DevSecOps é a conduta de integrar testes de segurança a todos os estágios do processo de desenvolvimento de software. Adiciona ferramentas e processos que promovem a colaboração entre desenvolvedores, especialistas em segurança e equipes de operação para desenvolver softwares eficientes e seguros. O DevSecOps incentiva uma transformação cultural que faz o tema segurança uma responsabilidade compartilhada por todos que estão desenvolvendo o software.



DevSecOps significa desenvolvimento, segurança e operações. Diz respeito sobre uma ampliação da prática de DevOps. Cada termo se refere a diferentes funções e responsabilidades dos times de desenvolvimento de software durante a criação de aplicações.

- **Desenvolvimento:** processo de planejamento, codificação, construção e test da aplicação.
- **Segurança:** adição de forma antecipada no ciclo de desenvolvimento de software de testes de segurança realizados pelos profissionais que testam o software antes que a empresa o libere.

- **Operations:** liberação, monitoração e adequação de quaisquer problemas que apareçam no software.

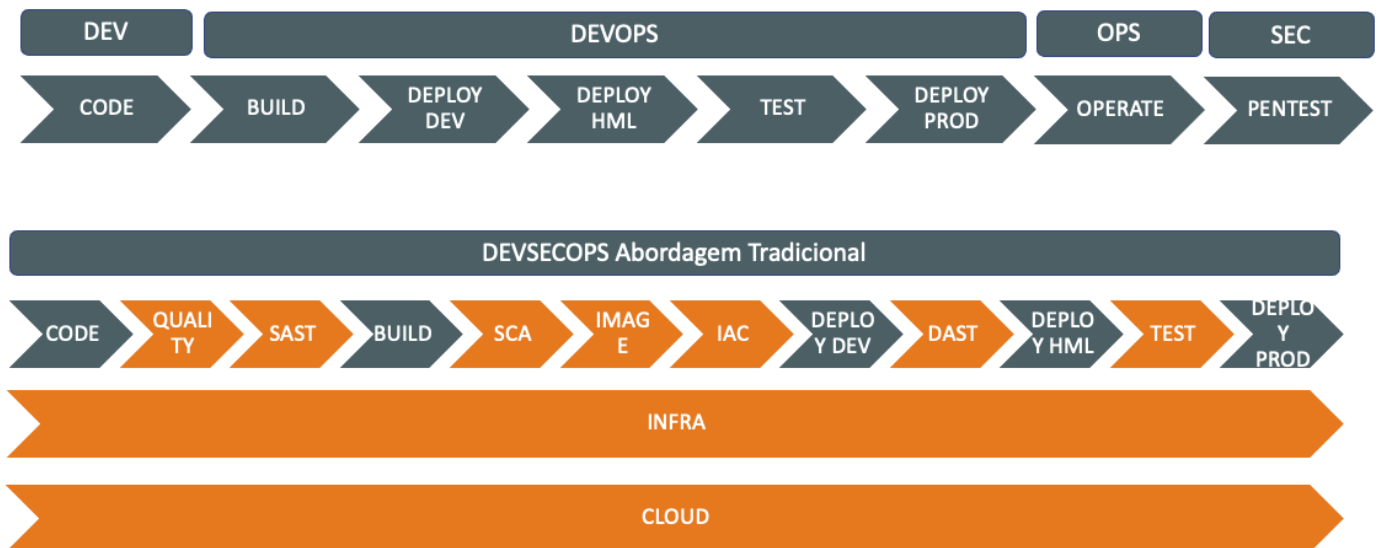
A cultura DevSecOps promove o trabalho conjunto e flexível entre as equipes de desenvolvimento, operações e segurança. Essas equipes compartilham o mesmo entendimento a respeito de segurança de software e utilizam ferramentas para automatizar a avaliação e geração de resultados.

A Rainforest se posiciona como uma plataforma que ajuda nesse processo de integração de processos e equipes durante o ciclo de desenvolvimento de software.

## Abordagem Comum

A abordagem tradicional sobre a inclusão de segurança no fluxo de DevOps consiste em adicionar etapas no processo CI/CD atual. As equipes de desenvolvimento trabalham juntas para diagnosticar vulnerabilidades no software.

## Abordagem tradicional DEVOPS → DEVSECOPS

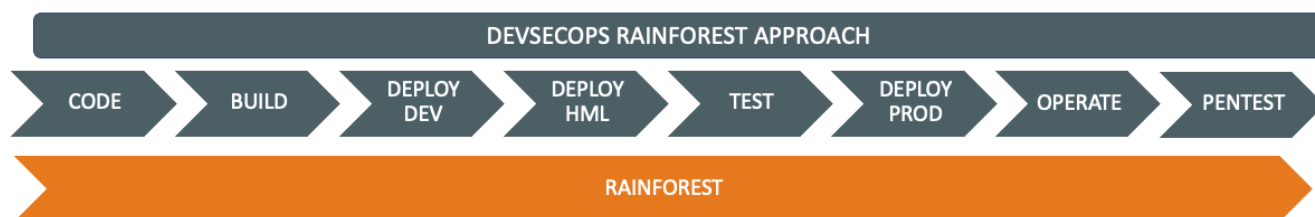


Essa abordagem, por consequência, gera impactos que muitas vezes prejudicam o processo de desenvolvimento de software, entre eles podemos citar:

- Tempo de implementação longo
- O código é levado para ambientes de terceiros para que as análises possam ser realizadas
- Diferentes times
- Análises distorcidas
- Pipelines separados

## Abordagem Rainforest

A Rainforest tem uma abordagem diferente, nos propomos a não interferir diretamente na esteira de desenvolvimento. Desta forma, as análises realizadas pela plataforma para cada teste são executadas em paralelo a esteira atual do cliente.



Os testes são executados a cada commit realizado pelos desenvolvedores, por consequência, o cliente tem quase que simultaneamente o resultado das análises para checagem das vulnerabilidades, informações sensíveis como senhas, tokens e/ou melhorias de código que a plataforma Rainforest identifica. Além dessa vantagem a abordagem adotada pela Rainforest traz outros benefícios, como:

- Implantação PLUG and PLAY, levando pouquíssimo tempo para ter os primeiros resultados
- Código permanece em sua infraestrutura, não levamos seu código para ambientes da Rainforest
- Times integrados usando a mesma plataforma, tendo acesso aos mesmos resultados
- Análises centralizadas em um único lugar
- Rodamos em paralelo, não impactando no pipeline atual do cliente

A solução Rainforest fornece informações para bloqueio da esteira com objetivo de evitar que uma aplicação siga em frente para produção em determinadas condições. A solução permite que isto seja feito em diferentes estágios de maturidade. Como exemplos:

1. inicialmente sem o bloqueio
2. em seguida bloqueando quando o código atual não esteja igual ou melhor ao código que esteja rodando em produção, e
3. bloqueando se a aplicação tiver alguma vulnerabilidade alta ou crítica.

Esses são exemplos de bloqueio, mas é possível - utilizando API - usar outras informações para tomada de decisão.

# Fraude em Domínios

---

 support.rainforest.tech/pt-br/kb/fraude-dominios

## Entenda como a plataforma Rainforest protege contra fraude em domínios

---

Uma das formas que os golpistas utilizam para fraudar usuários é direcionar as vítimas para domínios similares ao real. Tais nomes de domínios parecem com o legítimo, contudo não são escritos de forma semelhante a fim de enganar até mesmo olhos atentos. Esse ataque é conhecido como *typosquatting* e são alguns exemplos: google.com ao invés de google.com ou betsbuy.com ao invés de bestbuy.com.

As pessoas que procuram um site legítimo acabam sendo direcionadas para um site falso que pode conter *malware* ou solicitar informações pessoais.

Os golpistas também trocam frequentemente certas letras e números que são difíceis de diferenciar, como a letra minúscula “L” versus o numeral “1” (um). Isso torna difícil ver a diferença entre hotmail.com e hotmai1.com. Somado a isso o atacante pode caracteres internacionais e marcações para dificultar ainda mais a identificação de tal tipo de golpe.

Além disso, o golpista pode usar, em parte do nome do domínio, a marca com o objetivo de confundir as pessoas e direciona-las para sites falsos. Por exemplo, pode existir uma empresa que faz financiamento de crédito pessoal que tem como nome fictício Example e tem o site cadastrado como example.com. É comum encontrar registro de domínios que utilizam parte do nome em uma ação como, por exemplo, Financie Na Example registrado com o domínio financienaexample.com.

A Rainforest através de múltiplas inteligências, algoritmos e buscas em diversas fontes possui mecanismos de identificação de domínios similares ao real ou mesmo nome de domínios que utilizam parte da marca no nome.

Com base na configuração de uma marca (*brand*), onde deve-se incluir os domínios reais, a plataforma Rainforest realiza tal busca e apresenta os domínios que podem representar fraude.

Tal funcionalidade está inclusa no módulo de Fraude (*Fraud*) e pode ser acessada em **Fraude > Domínios**.

RAINFOREST

Demo

User Demo

Brand Intelligence

Vulnerability Intelligence

Fraud

General Frauds

Domains

Mobile Apps

Social Networks

Surface Web

Takedown Requests

Leak

Cloud

Infra

App

Reference

Settings

Organizations

Brands

Domains

FINDINGS 345 UNDER-ANALYSIS 1 TRUSTED 3 IRRELEVANT 140 TAKEDOWN 0 ALL 698

#	ID	Domain name	Keyword	IP	Test date	Screenshot	IP Fraud Score	Register
1	35468	u...rg.info	-	155.94.149.226	Tue, 12/13/22 12:05 PM	✓	-	Web Commerce Communications Limite
2	32954	u...rg.info	-	198.55.122.234	Sun, 12/11/22 12:05 PM	✓	-	Web Commerce Communications Limite
3	35467	u...na.info	-	204.44.75.53	Tue, 12/13/22 12:05 PM	✓	-	Web Commerce Communications Limite
4	30654	js...llc.com	-	34.102.136.180	Wed, 11/16/22 12:47 PM	✓	-	GoDaddy.com, LLC
5	30287	s...ov.com	-	104.240.54.63	Sun, 11/6/22 12:47 PM	✓	-	NameCheap, Inc.
6	30299	s...llc.org	-	66.96.162.134	Sun, 11/6/22 12:47 PM	✓	-	Domain.com, LLC
7	30300	tr...s.com	-	66.70.188.182	Sun, 11/6/22 12:47 PM	✓	-	NameSilo, LLC
8	29601	o...eb.com	-	45.224.128.33	Fri, 10/21/22 12:47 PM	✓	-	GoDaddy.com, LLC
9	29622	ra...o.com.br	-	159.89.247.36	Sun, 11/27/22 12:59 PM	✓	-	Nic.br
10	29250	m...ne.com	-	34.102.136.180	Mon, 10/17/22 2:46 PM	✓	-	GoDaddy.com, LLC
11	28604	...al.com.br	-	187.1.137.73	Sun, 10/9/22 12:47 PM	✓	-	Nic.br
12	27013	...ct.com	-	20.124.180.190	Fri, 9/30/22 12:47 PM	✓	-	GoDaddy.com, LLC
13	24368	is...er.com	-	78.142.211.222	Tue, 9/13/22 12:47 PM	✓	-	Google LLC
14	28127	u...u.com	-	155.94.177.137	12:44 AM	✗	-	ALIBABA.COM SINGAPORE E-COMMERCE
15	23257	o...e.com	-	162.215.226.3	Tue, 10/4/22 1:10 PM	✓	-	PNP Ltd. d/b/a PublicDomainRegistry

Page Size 20 First Prev 1 2 3 4 5 Next Last

Feedback

Ao abrir um registro na plataforma, ela trará maiores detalhes do domínio encontrado,, por exemplo:

- Informações de cadastro
- Informações de IP
- Score da probabilidade de fraude
- Informações de contato
- Localização
- Whois
- Entre outros dados

OVERVIEW

SCREENSHOT HISTORY 27

**Buy now** **\$2,895 USD**

**Make an offer**

**Buy now →**

Status	<b>Findings</b>
Severity	Medium
Brand	Demo
Domain name	.....a.com
IP	.....172
IP Fraud Score	0
IP City	San Jose
IP Region	California
IP Country	United States
ISP	om, Inc.
Organization	west-1)
Longitude	.895
Latitude	37.4
Test date	<b>12/11/25, 7:05 PM</b> (2 months ago)
SSL Expiration Date	<b>3/10/26, 6:30 PM</b> (in 1 month)

Activity

- Discovered** almost 2 years ago
  - System** almost 2 years ago  
Status changed to New - Found additional keywords
  - System** 4 months ago  
Status changed from Irrelevant to New - Severity level increased
- Write a comment here...
- COMMENT

- FINDINGS
- UNDER-ANALYSIS
- TRUSTED
- IRRELEVANT
- TAKEDOWN

PREVIOUS

NEXT

SSL Expiration Date

**3/10/26, 6:30 PM**

(in 1 month)

Register

Dynadot LLC

Contact

support@dynadot.com

Details

```
"Domain_Name": "K[REDACTED].COM",
"Registry_Domain_ID": "284[REDACTED].COM-
VRSN",
"Registrar_WHOIS_Server": "whoi[REDACTED].n",
"Registrar_URL": "http://w[REDACTED].om",
"Updated_Date": "20[REDACTED] 5Z",
"Creation_Date": "2[REDACTED] 29Z",
"Registry_Expiry_Date": "20[REDACTED] Z",
"Registrar": "D[REDACTED].c",
"Registrar_IANA_ID": "[REDACTED]",
"Registrar_Abuse_Contact_Email": "at[REDACTED]@
n[REDACTED].om",
"Registrar_Abuse_Contact_Phone": "1[REDACTED]",
"Domain_Status": "cl[REDACTED] d
ht[REDACTED]ted",
"Name_Server": "[REDACTED]",
"DNSSEC": "[REDACTED] d",
"URL_Abuse_Contact_Form": "https://[REDACTED]/"
```

[Show less](#)

Created

2023-12-25

Modified

**1/27/26, 3:54 AM**

(11 hours ago)

Discovery date

**4/25/24, 3:48 AM**

(2 years ago)

## SSL - Data de Expiração

Adicionalmente, a plataforma da Rainforest da visibilidade e proporciona o controle e gerenciamento dos certificados SSL dos domínios que o possuem.

The screenshot displays the Rainforest Tech interface. At the top, there is a search bar with '19-Demo' and a user profile 'LC'. The left sidebar contains navigation options: Brand Intelligence, Vulnerability Intelligence, Fraud, Domains, Mobile Apps, Social Networks, Surface Web, Message Services, RF Tags, Takedown Requests, Leak, Cloud, Infra, App, Reference, Settings, and Admin. The main content area shows a table of findings for the 'Demo' brand. A notification at the top states: 'This module has a trial license that may show a limited amount of information and will expire in 2 years'. The table has columns for Brand, Keyword, IP, Test date, SSL Expiration Date, IP Fraud Score, and Register. The 'SSL Expiration Date' column is highlighted with a red box. The table contains 7 rows of data.

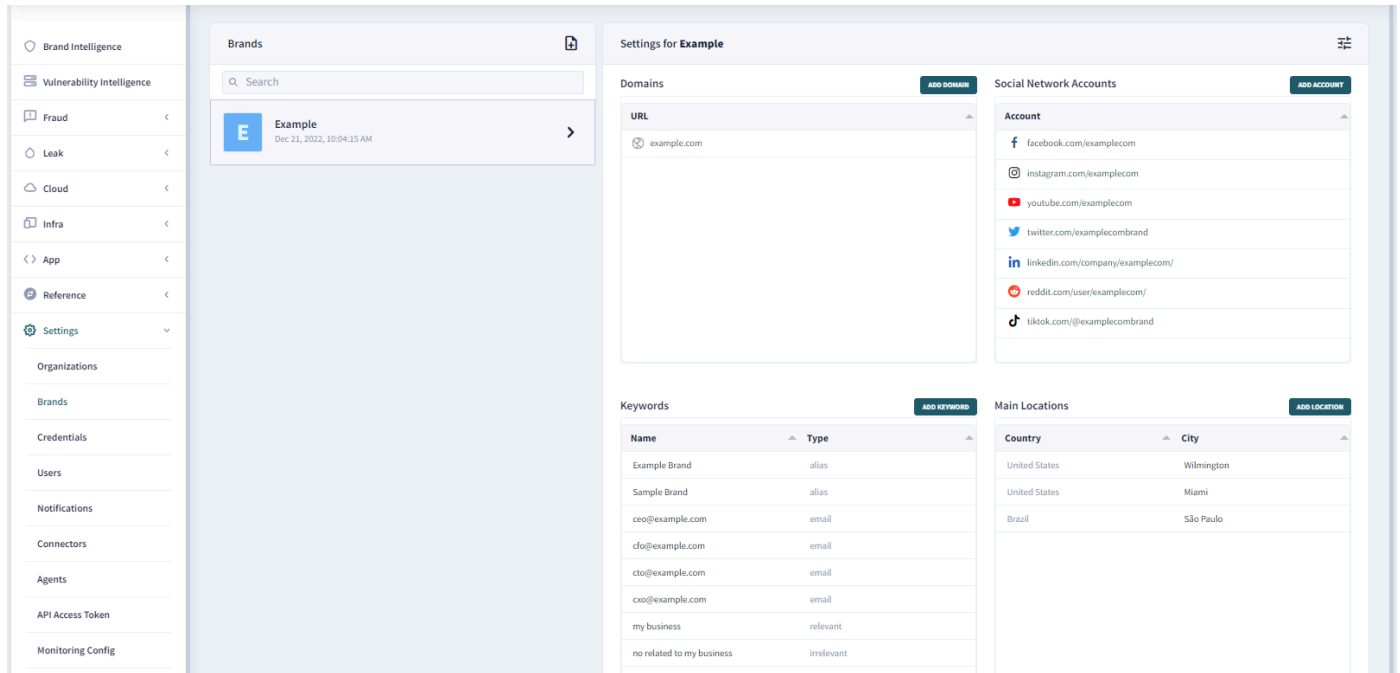
Brand	Keyword	IP	Test date	SSL Expiration Date	IP Fraud Score	Register
Demo	-	3.33.165.172	Thu, 12/11/25 7:05 PM	3/10/26, 6:30 PM - in 1 month	-	...
Demo	-	178.63.150.246	Wed, 12/31/25 6:52 PM	3/26/26, 6:22 PM - in 2 months	-	...
Demo	-	104.21.19.113	Mon, 12/8/25 6:44 PM	3/8/26, 1:58 AM - in 1 month	-	...
Demo	-	54.76.177.85	Sun, 7/27/25 8:11 AM	7/25/26, 1:42 PM - in 6 months	-	...
Demo	-	13.203.149.144	Thu, 1/15/26 6:42 PM	4/7/26, 9:45 PM - in 2 months	-	...
Demo	-	13.203.149.144	Thu, 1/15/26 6:43 PM	4/7/26, 9:45 PM - in 2 months	-	...

# Configurar a Monitoração de uma Marca

 support.rainforest.tech/pt-br/kb/configuracao-marca

## Entenda como configurar os principais itens que definem uma marca na plataforma da Rainforest.

A Plataforma Rainforest realiza a monitoração de Fraudes e Vazamentos baseada em marcas que são definidas no menu **Configurações > Marcas**.



The screenshot shows the 'Settings for Example' configuration page. The left sidebar contains navigation options: Brand Intelligence, Vulnerability Intelligence, Fraud, Leak, Cloud, Infra, App, Reference, Settings, Organizations, Brands, Credentials, Users, Notifications, Connectors, Agents, API Access Token, and Monitoring Config. The main content area is divided into several sections:

- Brands:** A search bar and a card for 'Example' with a date 'Dec 21, 2022, 10:04:15 AM'.
- Domains:** A table with one entry: 'example.com'.
- Social Network Accounts:** A list of accounts for Facebook, Instagram, YouTube, Twitter, LinkedIn, Reddit, and TikTok.
- Keywords:** A table with columns 'Name' and 'Type'.
- Main Locations:** A table with columns 'Country' and 'City'.

Name	Type
Example Brand	alias
Sample Brand	alias
ceo@example.com	email
cfo@example.com	email
cto@example.com	email
ceo@example.com	email
my business	relevant
no related to my business	irrelevant

Country	City
United States	Wilmington
United States	Miami
Brazil	São Paulo

Após a configuração das marcas, domínios e palavras-chave, a plataforma iniciará o processo de monitoramento periódico e automatizado, possibilitando que o usuário inicie as análises e categorização dos registros encontrados. Abaixo temos os principais itens que podem ser configurados para cada marca, nem todos esses itens são obrigatórios, mas ajudam em diferentes níveis aos algoritmos da plataforma a identificarem melhor os itens descobertos (*findings*) e a pré-classificar esses itens em níveis de relevância:

- **Domínios:** são os domínios (endereços eletrônicos) que foram registrados para a marca e são utilizados principalmente em sites e emails. Não é necessário adicionar os subdomains, somente o domínio base. Recomenda-se que tenha no mínimo um domínio configurado para cada marca.
- **Redes Sociais:** caso a marca tenha alguma rede social, é indicado o cadastro dessas os usuários e páginas dessas redes.

- **Palavras Chaves:** são palavras que identificam a marca, essas palavras podem ser dos seguintes tipos.
  - **Pseudônimo (Alias):** são palavras e apelidos de como a marca é conhecida e referenciada. Aqui pode ser definido também um conjunto de palavras separadas por espaço que juntos definem o nome da marca.
  - **Relevante:** são palavras importantes que quando associadas ao nome da empresa indicam que devem ser consideradas com um nível de importância maior. Podem ser atividades relacionadas ao ramo de negócio, nomes de produtos, etc.
  - **Irrelevante:** são palavras que quando associadas ao nome da empresa indicam que essa referência a empresa provavelmente não é muito importante e deve ser considerada com um nível menor de importância.
  - **Email:** são emails adicionais que também devem ser monitorados e não estão abaixo dos domínios oficiais da marca já cadastrados no outro item. Esse campo normalmente é utilizado quando a marca possui algum email em domínios como o gmail.com ou hotmail.com.
- **Principais Localizações:** algumas buscas são sensíveis a localização da marca ou ao local de acesso dos clientes. Um exemplo disso são os anúncios pagos que são exibidos em sites de buscas e redes sociais. A definição dessas localizações não restringe as buscas, mas indicam localizações que devem ser priorizadas ou nos ajudam a regionalizar o formato da busca para encontrar mais informações relevantes.

## Configuração de Usuários Permitidos (whitelisted)

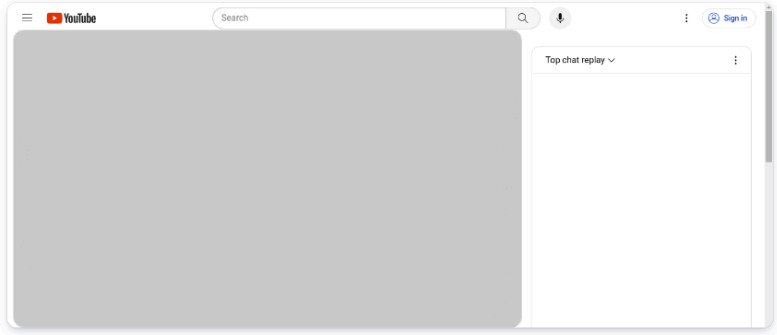
Para casos de redes sociais, você pode se deparar com o cenário em que precisará adicionar exceções no mecanismo de análise da plataforma, ou seja, precisará adicionar usuários na lista de usuários permitidos, fazendo com que a plataforma Rainforest automaticamente classifique achados dos usuários presente na *White List*. Para fazer essa parametrização, acesse **Fraude > Redes Sociais**, acesse o registro do usuário desejado.

The screenshot shows the Rainforest Security dashboard. On the left, there is a sidebar with navigation items: Inteligência de Marca, Inteligência de Vulnerabilidade, Fraude (expanded), Domínios, Aplicativos Móveis, Redes Sociais, and Surface Web. The main content area is titled 'Redes Sociais' and features a filter bar with categories: DESCOBERTAS (11591), SOB ANÁLISE (11), CONFIÁVEL (0), IRRELEVANTE (51), TAKEDOWN (2), and TODOS (11655). Below the filter bar is a table with the following columns: #, ID, Severi..., Tipo, Nome, Marca, URL, Keywords, and Posta. The first row of the table is highlighted with a red border and contains the following data: # 1, ID I5007, Severi... Alta, Tipo user, Nome [redacted], Marca [redacted], URL https://www.youtube, Keywords [redacted], and Posta [redacted]. The second row contains: # 2, ID I5006, Severi... Alta, Tipo user, Nome [redacted], Marca [redacted], URL https://www.youtube, Keywords [redacted], and Posta [redacted]. The third row contains: # 3, ID I5155, Severi... Crítica, Tipo post, Nome São Paulc, Marca -, URL https://www.instagram, Keywords [redacted], and Posta [redacted]. The fourth row contains: # 4, ID I5170, Severi... Crítica, Tipo post, Nome São Paulc, Marca -, URL https://www.instagram, Keywords [redacted], and Posta [redacted].

Em seguida, clique no botão **Adicionar usuário à lista de permissões**, localizado no canto inferior direito do pop-up.

Detalhes - Redes Sociais

VISÃO GERAL ATIVIDADE SCREENSHOT HISTORY



Status: **Descobertas**

Severidade: **Alta**

Marca: [REDACTED]

ID: [REDACTED]

ID do Crawler: [REDACTED]

ID da Keyword: [REDACTED]

URL: [REDACTED]

Nome: [REDACTED]

Tipo: **user**

Nome do usuário: [REDACTED]

Keyword: [REDACTED]

Total de Keywords: [REDACTED]

Data da descoberta: **August 24, 2023 - 02:54 AM - há aproximadamente 13 horas**

Modificado: **August 24, 2023 - 06:20 AM - há aproximadamente 9 horas**

DESCOBERTAS SOB ANÁLISE CONFIÁVEL IRRELEVANTE **TAKEDOWN**

ANTERIOR **ADICIONAR USUÁRIO À LISTA DE PERMISSÕES** PRÓXIMO

A funcionalidade de **Adicionar usuário à lista de permissões** é apresentada apenas para descobertas do tipo **User**.

# Sobre a Rainforest Technologies

---

 [support.rainforest.tech/pt-br/kb/sobre-a-rainforest](https://support.rainforest.tech/pt-br/kb/sobre-a-rainforest)

**Conheça mais sobre nós, nossos valores, nossa solução.**

---



## Sobre nós

---

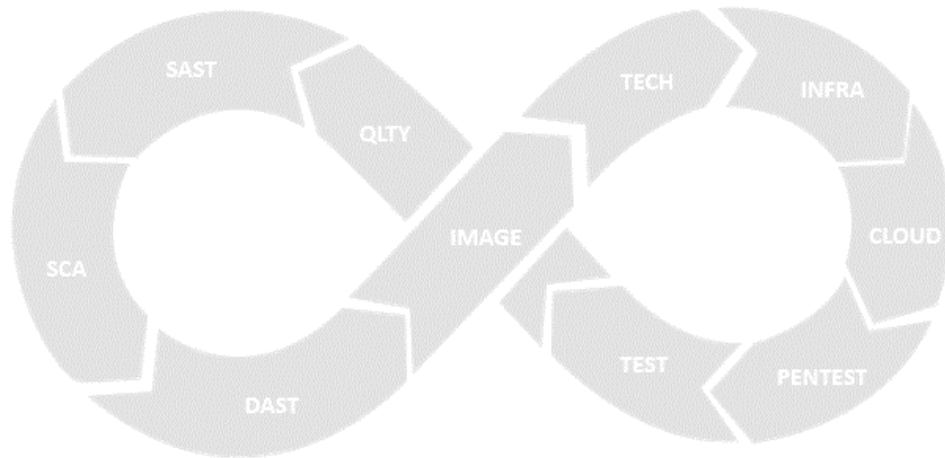
O mundo do crime cibernético vem crescendo, se organizando e se estruturando com o passar dos anos, causando bilhões em prejuízos com ataques cada vez mais sofisticados.

Do outro lado, produtos de cibersegurança tem sobrecarregado as equipes internas com milhares de alertas.

Todos alertas são importantes, mas quais são críticos? Quais realmente mostram quais vulnerabilidades devem ser corrigidas agora ao invés de outras?

A Rainforest ajuda equipes de cibersegurança a serem mais eficientes e eficazes detectando perfis falsos, vazamentos, aplicações fraudulentas e vulnerabilidades que demandam remediação imediata, reduzindo a escassez de profissionais, sobrecarga de equipes e atrasos em detectar e corrigir problemas críticos.

A integração de qualquer esteira de desenvolvimento aproximamos o mundo da segurança cibernética para o DevOps, criando uma visão que as equipes não tinham antes.



ADD SEC TO YOUR DEVOPS

---

## Manter nossos clientes confiáveis

---

Isto é o que define nossa missão, entregando mais do que produtos e serviços.

## Simplificar a proteção da reputação corporativa

---

A Rainforest mitiga riscos relacionados a vulnerabilidades em aplicações e ameaças a marcas, oferecendo um ecossistema de cibersegurança para simplificar a proteção da reputação de empresas usando múltiplas inteligências e observabilidade pró-ativa.

## Nossos Valores

---

### Centrado no Cliente

---

Tudo que fazemos é pensando em entregar soluções melhores e mais rapidamente para prover segurança.

### Padrões Altos

---

Todo e cada um de nós é o melhor no que faz, não aceitamos desculpas: o trabalho DEVE ser feito.

### Mergulhamos Fundo

---

Não somos superficiais. Para estar no topo, mergulhamos fundo.

## Foco no Resultado

---

Não é sobre "o que jogamos" ou "como jogamos", o que importa mais é "Como Vencemos".

## A Plataforma de Cibersegurança que sua Empresa Precisa

---

Com a plataforma **SaaS** de cibersegurança da Rainforest, você integra uma empresa inteira com segurança, dos desenvolvedores à governança e risco – sem gerar atrito entre os times. Com um único login, o usuário é capaz de com segurança ter visualização em um painel centralizado de todas as vulnerabilidades presentes em seu ambiente.

Por conta de sua modularização, é possível definir perfis de usuários com responsabilidades em módulos diferentes, mantendo segurança e privacidade.

Uma plataforma híbridas, onde as análises acontecem parte no ambiente do cliente e parte em ambiente cloud.

## Inteligência de Vulnerabilidades

---

**Rainforest Vulnerability Intelligence** é uma plataforma poderosa projetada para fornecer informações abrangentes sobre vulnerabilidades de segurança. Ele utiliza algoritmos e metodologias avançadas para escanear e analisar sistemas, identificando possíveis vulnerabilidades e fraquezas.

A solução oferece uma compreensão aprofundada das ameaças de segurança e fornece inteligência acionável, permitindo que as organizações tratem e reduzam os riscos de segurança de forma proativa, permitindo operações mais seguras e resilientes.

## Inteligência de Marca

---

**Rainforest Brand Intelligence** é uma solução inovadora que monitora ativamente a marca de uma empresa contra ameaças potenciais como fraudes ou vazamentos empregando tecnologia avançada para identificar atividades fraudulentas e vazamentos que possam prejudicar a reputação da empresa e resultar em prejuízos financeiros.

Com abordagem data-driven, fornece insights acionáveis que permitem que as empresas respondam prontamente e estrategicamente para mitigar os riscos relacionados à marca. Com Rainforest Brand Intelligence, as empresas podem proteger a integridade de sua marca e manter sua posição no mercado.

# Notificações na Plataforma Rainforest

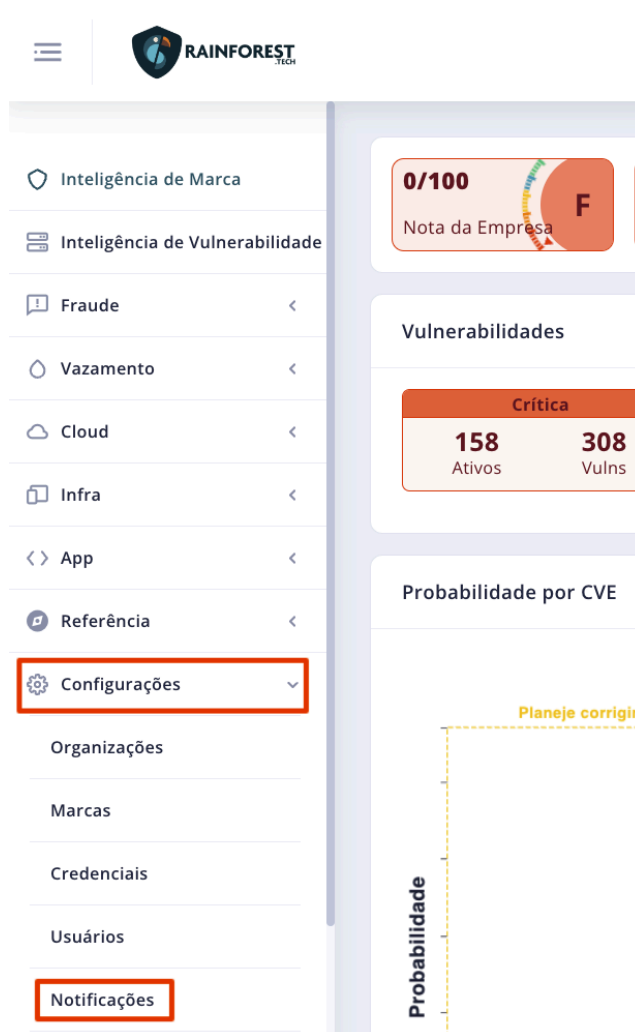
 [support.rainforest.tech/pt-br/kb/notificacoes-rainforest](https://support.rainforest.tech/pt-br/kb/notificacoes-rainforest)

## Veja como você pode configurar para receber notificações da plataforma Rainforest.

Sabemos que cada segundo importa na atuação contra **fraudes e vulnerabilidades** que possam ou serem descobertas contra a empresa e o quanto antes for tomadas as devidas ações, como por exemplo a solicitação de **takedown**, menor será o impacto causado.

Partindo desse pressuposto, a plataforma da Rainforest possibilita a configuração de notificações para determinados seções, possibilitando assim os usuários serem alertados no mesmo instante em que, a plataforma identificar uma vulnerabilidade ou fraude por exemplo.

Para realizar a configuração de notificações acesse o menu **Configurações > Notificações**:



The screenshot displays the Rainforest Tech dashboard interface. On the left, a navigation menu lists various sections: Inteligência de Marca, Inteligência de Vulnerabilidade, Fraude, Vazamento, Cloud, Infra, App, Referência, Configurações (highlighted with a red box), Organizações, Marcas, Credenciais, Usuários, and Notificações (also highlighted with a red box). The main content area on the right shows a 'Nota da Empresa' (0/100), a 'Vulnerabilidades' section with 'Crítica' status, 158 Ativos, and 308 Vulns, and a 'Probabilidade por CVE' section with a 'Planeje corrigir' label and a graph showing 'Probabilidade' on the y-axis.

Ao acessar o menu, você terá acesso as seções da plataforma na qual podem receber notificações, dentre elas temos:

- Exposure
- Social Monitoring
- Leaks
- Apps
- CVEs
- Domains
- Request
- Affected Assest
- Email Leaks
- Fraud

Notificações

Módulo	Seção	Severidade Mín...	E-mail	Slack	Telegram	Critério
Threat Intelligence	Exposure		desativado	desativado	desativado	
Threat Intelligence	Social Monitoring		desativado	desativado	desativado	
Threat Intelligence	Leaks		desativado	desativado	desativado	
Threat Intelligence	Apps		desativado	desativado	desativado	
Threat Intelligence	CVEs		desativado	desativado	desativado	
Threat Intelligence	Domains		desativado	desativado	desativado	
Threat Intelligence	Requests		desativado	desativado	desativado	
Threat Intelligence	Affected Assets		desativado	desativado	desativado	
Threat Intelligence	Email Leaks		desativado	desativado	desativado	
Threat Intelligence	Fraud		desativado	desativado	desativado	

Mostrando 10 de 10 itens

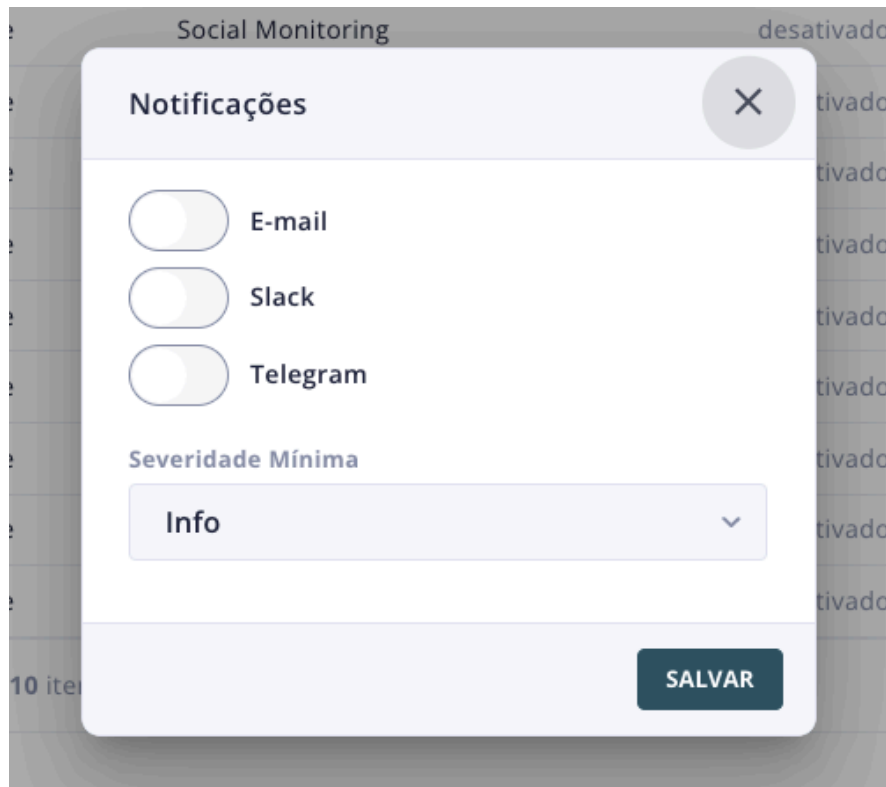
20 Primeira Ant. 1 Próx. Última

Atualmente a plataforma possui integrações que possibilitam o envio de notificações para as seguintes ferramentas:

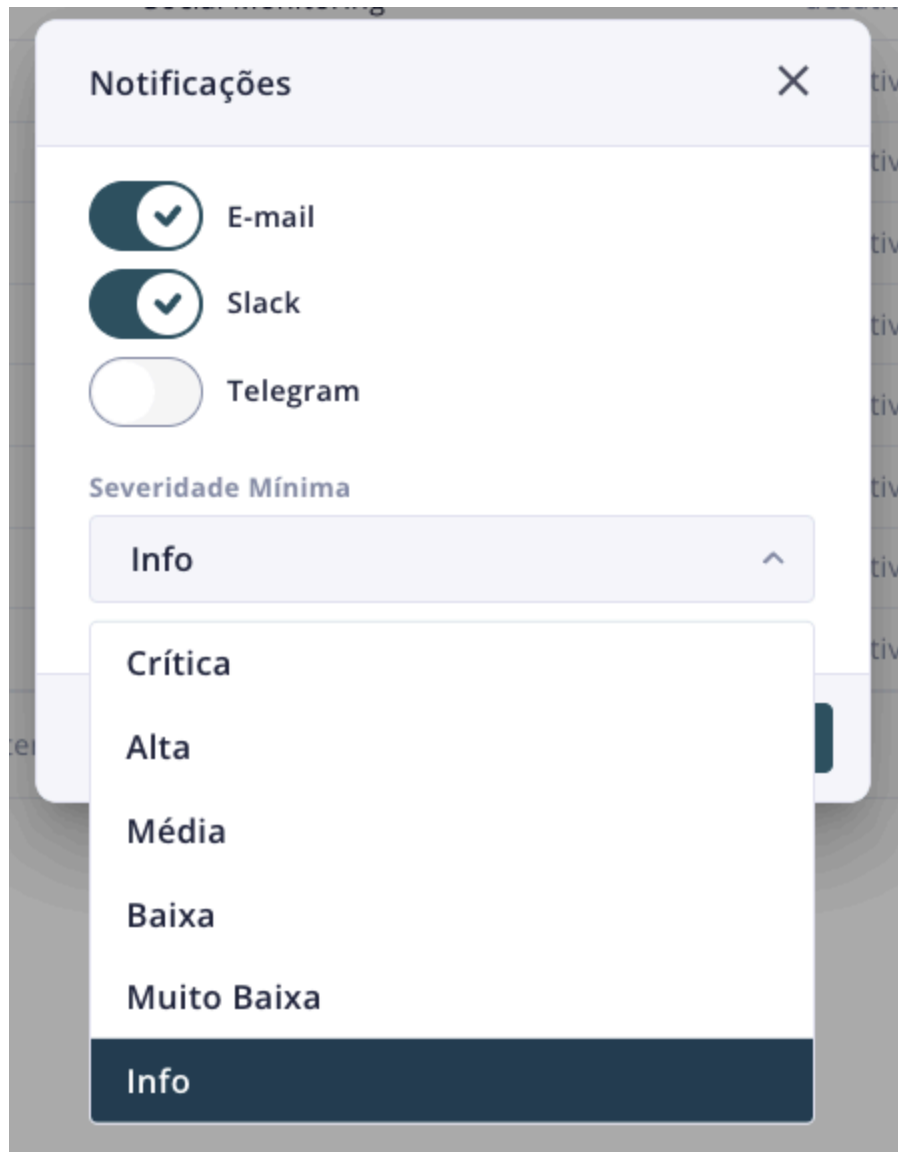
- E-mail
- Slack
- Telegram

## Configurando Notificações

Visto as possibilidades de notificações que a plataforma da Rainforest pode enviar aos usuários e as ferramentas de destino, para iniciar a configuração da(s) seção(ões) desejada(s), passe o cursor do mouse sobre a seção desejada e clique. Será apresentado a tela de configuração.



Na tela temos os canais, mencionados anteriormente, em que a plataforma fará o envio, habilite os canais desejadas e defina a severidade mínima da qual gostaria de receber as notificações.



Se desejar receber todas as notificações independente da severidade, selecione a opção **Info**.

Se optar por receber notificações apenas **Alta** e **Crítica**, selecione a opção **Alta**.

Realizada a configuração, clique em **Salvar**, o painel de opções de notificações será atualizado.

Módulo	Seção	Severidade Mín...	E-mail	Slack	Telegram	Critério
Threat Intelligence	Exposure		desativado	desativado	desativado	
Threat Intelligence	Social Monitoring		desativado	desativado	desativado	
Threat Intelligence	Leaks		ativado	ativado	desativado	
Threat Intelligence	Apps		desativado	desativado	desativado	
Threat Intelligence	CVEs		desativado	desativado	desativado	

Repita o processo para todas as seções desejadas.

É obrigatório primeiramente configurar os respectivos conectores para que a notificação comece a ser enviada. Para maiores informações acesse o artigo:

[Conectores Rainforest](#)

# Gráficos e Filtros em Aplicações

 [support.rainforest.tech/pt-br/kb/grafico-filtro-vulnerabilidades-app](https://support.rainforest.tech/pt-br/kb/grafico-filtro-vulnerabilidades-app)

## Tenha rapidamente a visão de todas as descobertas encontradas pela plataforma Rainforest.

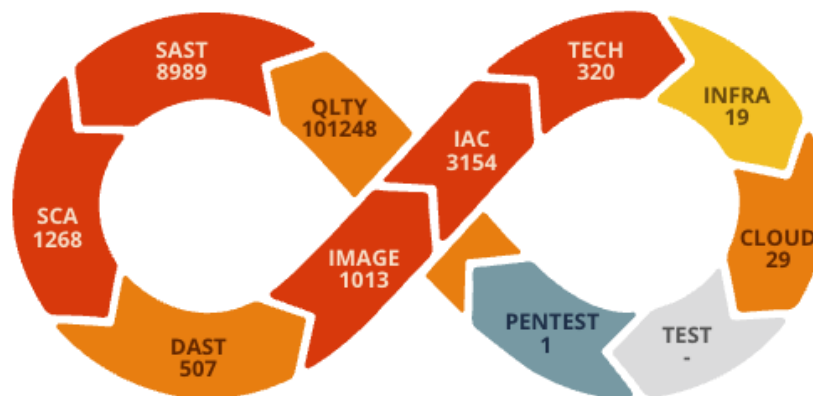
Em App, quando cadastramos as aplicações e a plataforma Rainforest começa a realizar as suas análises, conseqüentemente teremos como resultado os "Findings", ou seja, as descobertas de vulnerabilidades ou melhorias no código que a plataforma identificou. Desta forma, a plataforma também já começa a computar as informações nos dashboards disponíveis, organizando-as e ajudando os usuários na tomada de decisão.

Para o módulo de App, temos disponíveis o gráfico de **Status DevSecOps**, **Vulnerabilidades por Severidade** e a listagem de **Vulnerabilidades por Grupo e Aplicações**. Vejamos abaixo como utiliza-las.

### Status DevSecOps

O gráfico de **Status DevSecOps** (infinito), traz para os usuários da plataforma Rainforest um panorama segmentado por etapas que estão relacionadas diretamente com as análises que a plataforma realiza nas aplicações cadastradas. Ao passar por todas as etapas, temos na prática o ciclo DevSecOps se realizando na plataforma.

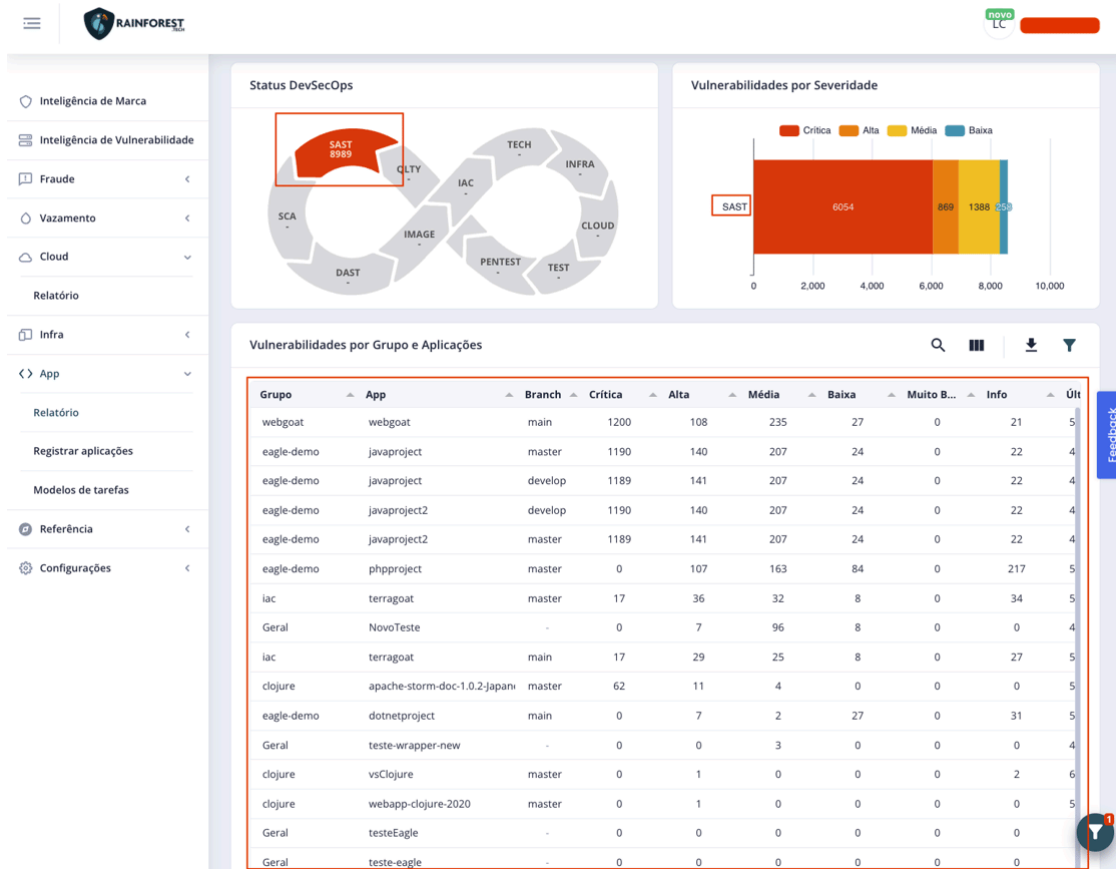
Status DevSecOps



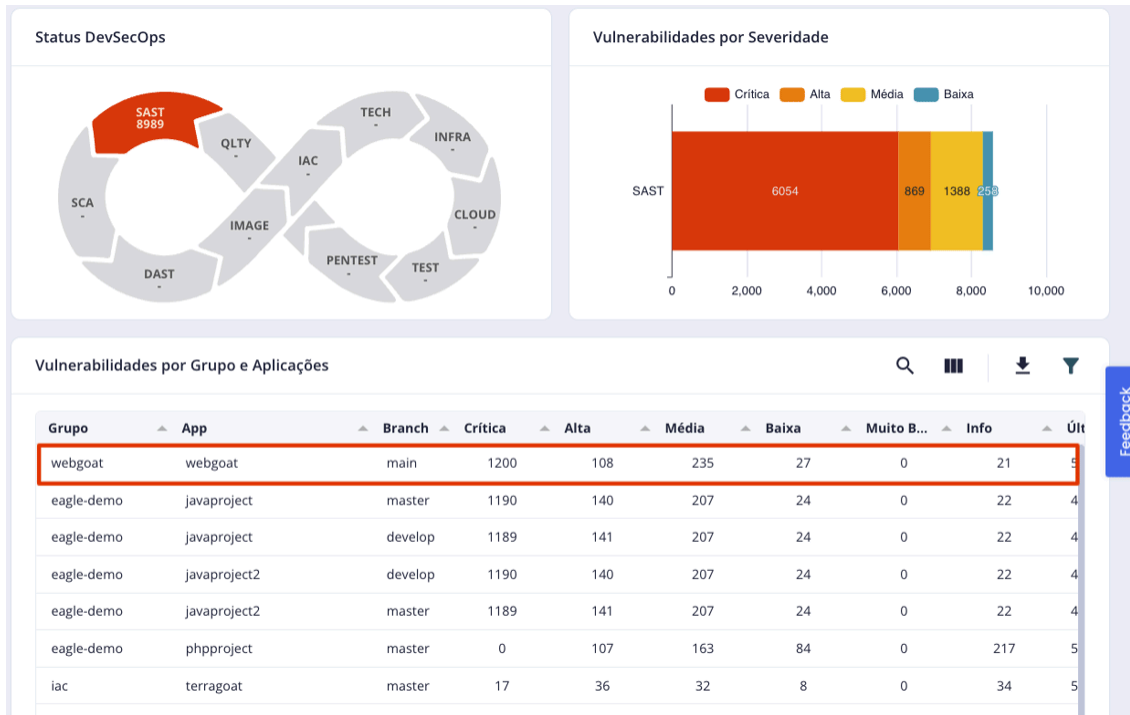
Para entender melhor cada tipo de análise realizada nas aplicações cadastradas no Rainforest, veja o artigo [Visão Geral App](#)

Podemos interagir com cada etapa do gráfico, onde ao clicarmos em alguma específica, a plataforma identificará isso e realizará o filtro, aplicando-o na listagem de **Vulnerabilidades por Grupo e Aplicações**.

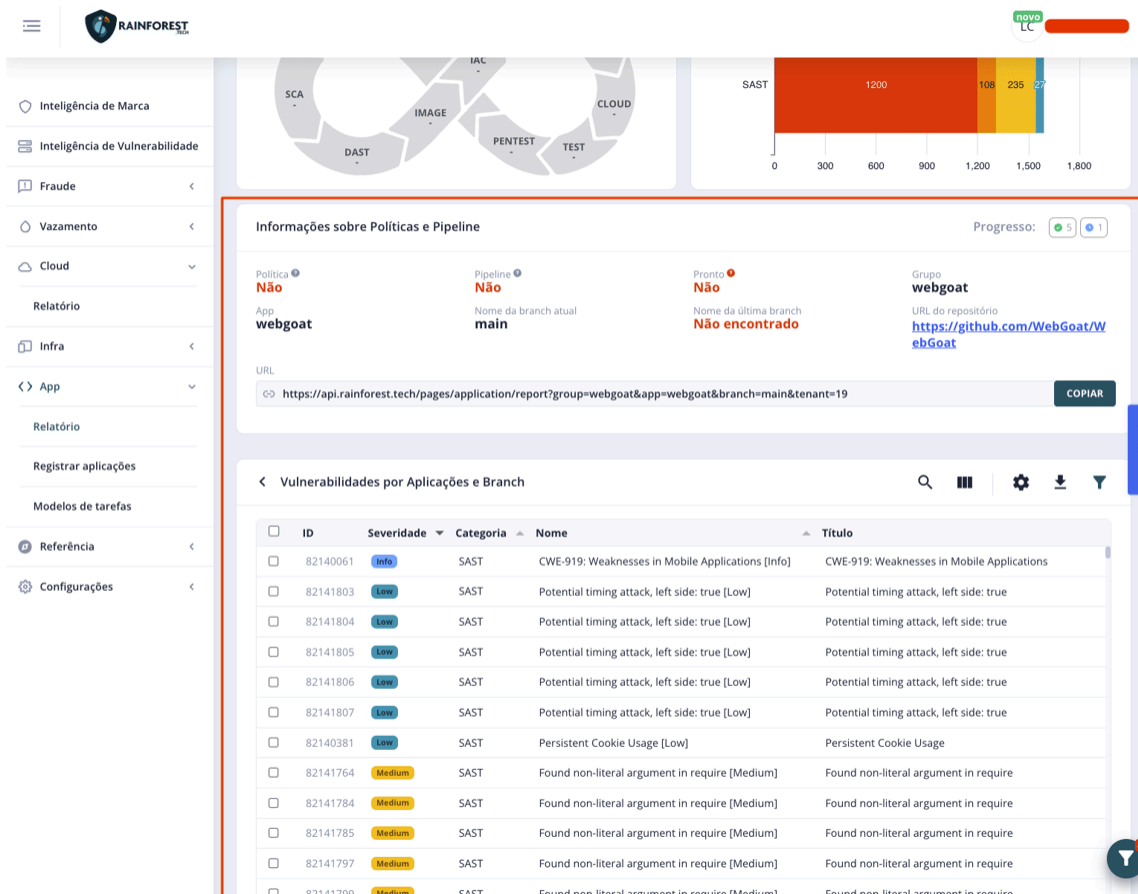
Por exemplo, se clicarmos na etapa **SAST** teremos o resultado abaixo, onde a plataforma sinaliza nos gráficos **Status DevSecOps** e **Vulnerabilidades por Severidade** a etapa do ciclo selecionada, além de alterar a listagem retornando apenas as descobertas relacionadas a etapa **SAST**.



Em seguida podemos nos aprofundar na análise selecionando uma aplicação da listagem disponível para visualizar as vulnerabilidades/melhorias descobertas para ela especificamente.



Ao clicarmos em uma aplicação da listagem a plataforma realiza o **drill down** e nos fornece uma nova listagem informações mais detalhadas das descobertas referente a aplicação selecionada, denominada **Vulnerabilidade por Aplicações e Branch**.



Indo um pouco mais além, se clicarmos em uma das vulnerabilidades da nova listagem, a plataforma nos trará maiores detalhes desse registro.

Potential timing attack, left side: true [Low] SAST Low 3.9

Potential timing attack, left side: true

**Detalhes**

Descoberta: 5/15/23 2:33 PM

Insecure comparisons (==, !=, !== and ===), which check input sequentially. This could lead to timing attacks on your application.

**Localização**

Arquivo: src/main/resources/webgoat/static/js/libs/ace.js  
Linha: 11047  
Desculpe, nenhum resultado encontrado

**Referências**

CWE (governance) <https://cwe.mitre.org/data/definitions/208.html>

**Compliance**

Desculpe, nenhum resultado encontrado

**Recomendações para Solucionar**

Desculpe, nenhum resultado encontrado

**Recomendações de IA (Beta Feature)**

Mostrar recomendações de IA

**Detalhes da Aplicação**

Grupo: webgoat  
App: webgoat  
URL da Aplicação: webgoat  
Branch: main  
Branch de Produção: Não  
URL do registro (imagem do contêiner): webgoat/webgoat  
URL do Repositório: <https://github.com/WebGoat/WebGoat>

**Contexto**

```
indentation += tabSize;           else if (token ==  
TAB_SPACE)                       continue;
```

**Ações**

Ações	Descrição
<input type="checkbox"/> Falso Positivo	
<input type="checkbox"/> Priorizar	
<input type="checkbox"/> Mitigado	

Descreva os motivos dessa mudança

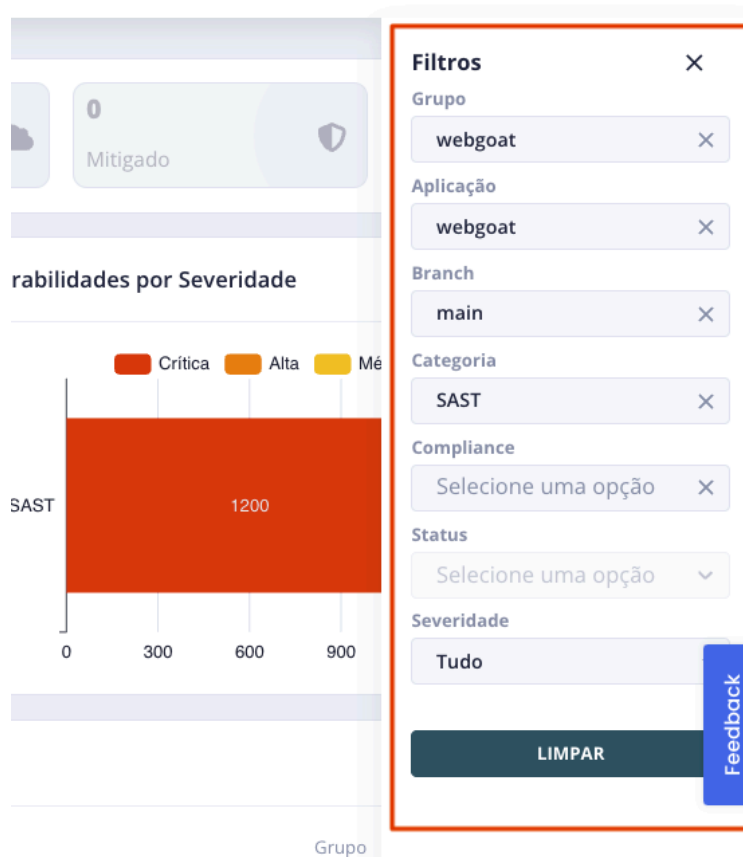
SAVE

ANTERIOR PRÓXIMO

Entenda cada informação da vulnerabilidade ou melhoria de código descoberta pela plataforma da Rainforest no artigo [Entendendo Descobertas](#)

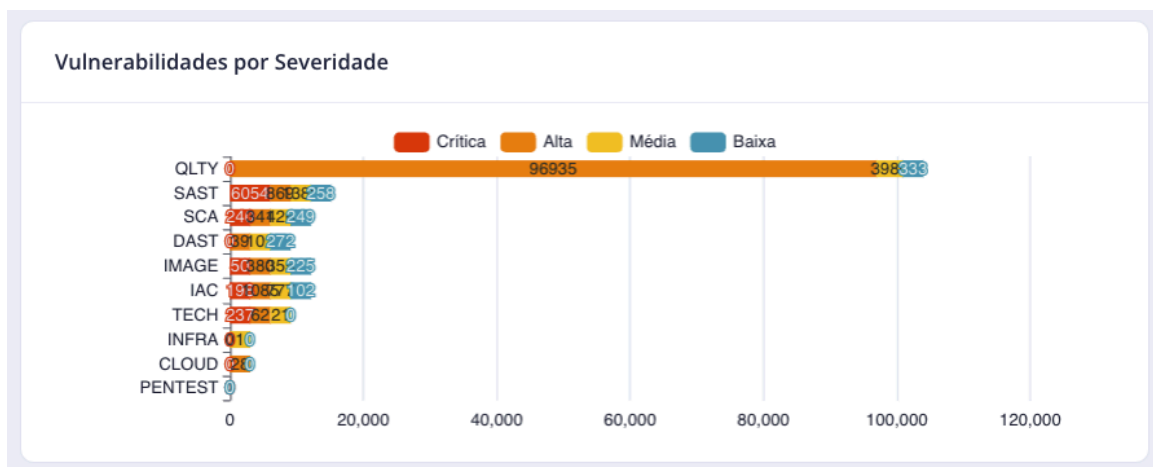
Repare que conforme o usuário vai evoluindo na seleção, a plataforma ao mesmo tempo atualiza os filtros, deixando claro quais critérios foram realizados para as ações e mostrando para o usuário uma segunda forma de chegar ao mesmo resultado.





## Vulnerabilidade por Severidade

A plataforma da Rainforest também fornece o gráfico de vulnerabilidades por severidade, onde o usuário ter uma visão das vulnerabilidades pela categoria desejada, por exemplo, obtendo as informações do número de vulnerabilidades críticas descobertas por tipo de análise.



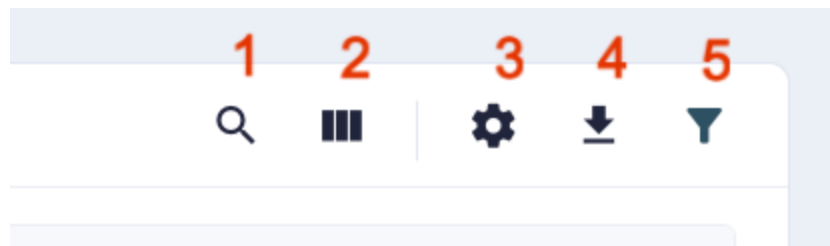
Podemos manter selecionado apenas a categoria **Crítica** do gráfico e selecionar uma análise, a partir desse momento o comportamento da plataforma é o mesmo no gráfico **Status DevSecOps**.

Neste exemplo, selecionaremos a etapa **IAC**, desta forma a plataforma trará as respectivas informações.



## Vulnerabilidade por Grupo e Aplicações

Conforme vamos interagindo com os gráficos e/ou filtros, a plataforma da Rainforest atualiza a listagem de aplicações/vulnerabilidades. Além de termos a listagem sempre atualizada de acordo com as opções selecionadas pelo usuário, podemos buscar por uma aplicação/vulnerabilidade específica (1), ajustar visualização/ordenação das colunas presentes na listagem (2 - exclusivo para vulnerabilidades), realizar a definição de registros em massa (3 - exclusivo para vulnerabilidades), exportação da listagem de aplicações/vulnerabilidades visíveis em tela (4), visualizar/atualizar os filtros (5).



Além disso, podemos ordenar os dados pelas informações presentes no grid clicando na coluna da informação que deseja visualizar de forma ordenada.



Ao  
TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS  
Av. André Araújo, S/N - Bairro Aleixo - CEP 69060-000 - Manaus - AM - www.tjam.jus.br

**Ref.: EDITAL DE LICITAÇÃO - PE - SECOP/SEAC - EDITAL DO PREGÃO ELETRÔNICO/SRP N.º  
006/2026 - TJAM**

**Objeto:** Registro de preços para eventual aquisição de solução de análise de vulnerabilidade, desenvolvimento seguro, que contemple mecanismos antifraude, conforme condições e exigências estabelecidas neste instrumento e seus anexos.

### **COMPROVAÇÕES COMPLEMENTARES - DADOS TÉCNICOS**

Para fins de comprovações técnicas do Objeto de contratação do Pregão 006/2025, apresentamos abaixo, no ANEXO I – DESCRIÇÃO PONTO A PONTO, a descrição detalhada das especificações dos produtos e serviços ofertados, incluindo documentação técnica pertinente, certificados de conformidade, relatórios de testes realizados e demais informações exigidas pelo edital.

Declaramos, para os devidos fins, que todas as informações técnicas prestadas são verdadeiras e correspondem às características reais dos produtos/serviços ofertados.

Atenciosamente,

Amir Velho  
Diretor de Operações – Rainforest

**ANEXO I – DESCRIÇÃO PONTO A PONTO**

<b>Código</b>	<b>Descrição</b>	<b>Página do Manual PDF de Comprovação</b>
<b>Descrição Geral da Contratação</b>		
1.2.3.1	Fortalecimento da Postura de Segurança Cibernética: o TJAM passará a contar com um nível elevado de maturidade em segurança da informação, sustentado por uma solução integrada que permitirá a análise contínua de vulnerabilidades em aplicações, infraestrutura e ambientes de desenvolvimento, proporcionando visão centralizada e resposta proativa a incidentes	163
1.2.3.2	Integração com Práticas DevSecOps: os pipelines de desenvolvimento (CI/CD) estarão plenamente integrados a controles automatizados de segurança, permitindo que vulnerabilidades sejam identificadas e tratadas antes da publicação de novos sistemas ou atualizações, reduzindo significativamente o risco de exposição a ataques cibernéticos.	152
1.2.3.3	Mitigação de Riscos de Vazamento de Dados e Fraudes Digitais: o Tribunal contará com mecanismos permanentes de monitoramento de credenciais, detecção de domínios fraudulentos e proteção de marca em ambientes como surface, deep e dark web, prevenindo fraudes, clonagem de domínios e uso indevido da identidade institucional.	139
1.2.3.4	Automação na Gestão de Vulnerabilidades: a gestão de vulnerabilidades será marcada por alta automação, permitindo a priorização de riscos, a classificação de vulnerabilidades e a geração de recomendações de correção com maior agilidade e eficiência das equipes técnicas.	149
1.3.1	A justifica para o quantitativo a ser adquirido encontra-se no Estudo Técnico Preliminar, anexo a este termo.	
<b>1.3.2</b>	<b>GRUPO 01 - Detecção e Mitigação de Vulnerabilidades em Aplicações</b>	
1.3.2.1	A solução deve permitir análise de até 10 aplicações em desenvolvimento e/ou já existentes no ambiente de produção do TJAM.	145
1.3.2.2	Toda a análise de códigos fonte deverá ocorrer dentro do perímetro de segurança do TJAM e/ou fábrica de software onde a aplicação esteja sendo desenvolvida, de acordo com as políticas de segurança definidas pelo TJAM,	146
1.3.2.3	Para fins de análise do código-fonte, não deverá ser realizado envio (upload) para a nuvem da CONTRATADA ou de terceiros.	146
1.3.2.4	Deve ser compatível com protocolo Git com o objetivo de se conectar no repositório de código-fonte do TJAM.	137
1.3.2.5	A solução deverá ser apta e ter opção de contexto, e permitir que a CONTRATADA clique e armazene pequenos trechos de código-fonte a fim de permitir ao desenvolvedor que identifique rapidamente o contexto em que a vulnerabilidade foi detectada.	130
1.3.2.6	A solução deve permitir a integração direta (plug and play) com repositório de código-fonte (Git) e repositório de imagens (Docker) interdependente da esteira DevOps de desenvolvimento (Jenkins, Gitlab, Azure DevOps	137

1.3.2.7	A solução deve permitir, quando necessário, bloqueio de esteira para que a aplicação não siga em frente para produção (funcionalidade conhecida como gatekeeper), no mínimo nos seguintes cenários:	152
1.3.2.7	Bloquear a esteira caso seja detectado que a aplicação ou imagem foi gerada a partir de um código que não atendeu as etapas obrigatórias do processo de análise de segurança, garantindo a conformidade com as políticas de governança estabelecidas	152
1.3.2.7.2	Quando houver alguma vulnerabilidade considerada alta ou crítica não tratada.	152
1.3.2.7.3	Quando houver código sensível identificado na análise de código-fonte com objetivo de detectar e alertar sobre melhorias de qualidade de código.	152
1.3.2.8	A solução deve possuir funcionalidade para análise de código e detectar e alertar sobre vulnerabilidades de segurança (SAST – Static Application Security Testing).	145
1.3.2.9	A solução deve possuir funcionalidade para análise de segurança de terceiros (SCA – Software Composition Analysis).	145
1.3.2.10	A solução deve possuir funcionalidade para varredura de vulnerabilidades dinâmicas na aplicação (DAST – Dynamic Application Security Testing).	145
1.3.2.11	A solução deve possuir funcionalidade para varredura em containers, Docker, para detectar vulnerabilidades de segurança.	145
1.3.2.12	A solução deve possuir funcionalidade para análise de vulnerabilidades em aplicações móveis (MAST – Mobile Application Security Testing).	145
1.3.2.13	A solução deve possuir funcionalidade para análise de segurança em infraestrutura como código (IaC – Infrastructure as Code), por exemplo, Ansible e Terraform.	145
1.3.2.14	A solução deve ter capacidade de identificação de vulnerabilidades do OWASP TOP10.	141
1.3.2.15	A solução deve possuir funcionalidades para análise de código com recomendações de melhoria de qualidade.	145
1.3.2.16	A solução deverá fornecer recomendações para correções (utilizando a base de conhecimentos da própria plataforma ou implementando funcionalidades de inteligência artificial para apresentar tais recomendações).	129 / 130
1.3.2.17	A solução deve gerar alertas de vulnerabilidades via plataforma: e-mail, Telegram e/ou Slack.	165
1.3.2.18	A solução deve possuir painel (dashboard) que apresente o nível de risco de código-fonte e infraestrutura por criticidade.	117
1.3.2.19	Deve apresentar painel (dashboard) do ciclo DevSecOps com painel de vulnerabilidades por etapa, com no mínimo as etapas “Quality”, “SAST”, “SCA”, “DAST”, “Image”, “MAST” e “IaC”.	169
1.3.2.20	A solução deve possuir funcionalidade para classificar as vulnerabilidades como falso-positivo, a priorizar ou mitigado em outro ambiente.	102
1.3.2.21	A solução deve permitir análise contínua, bastante a atualização do código pelo desenvolvedor, para que a plataforma inicie a análise de código.	152
1.3.2.22	A solução deve permitir o cadastro manual de vulnerabilidades.	97

1.3.2.23	A solução deve disponibilizar uma extensão (plugin) que permita acompanhar os achados de vulnerabilidade em ambiente de desenvolvimento integrado (Integrated Development Environment – IDE) suportando soluções como Microsoft Visual Studio Code.	85
<b>1.3.3</b>	<b>GRUPO 02 Detecção e Mitigação de Vulnerabilidades em Infraestrutura</b>	
1.3.3.1	A Solução deve analisar até 500 dispositivos da infraestrutura do TJAM a serem definidos pela SETIC.	74
1.3.3.2	Deve possibilitar o cadastro manual de redes e ativos de redes individuais, com cadastro do endereço IP, departamento, localização geográfica, nome e descrição do ativo.	62
1.3.3.3	Deve conter um cadastro manual de tecnologias instaladas em um ativo no inventário, com no mínimo informações como: fabricante, produto e versão.	59
1.3.3.4	Deve contar com funcionalidade própria de inventário automatizado dos ativos do ambiente, com suporte a inventário usando credenciais de acesso aos ativos.	50
1.3.3.5	Deve ser capaz de identificar ativos existentes em uma faixa (range) de rede e cadastrá-los na plataforma aos poucos.	51
1.3.3.6	Deve ser capaz de autenticar nos ativos encontrados e realizar o inventário automatizado de todas as tecnologias instaladas em cada um dos equipamentos servidores e estações de trabalho do escopo.	55
1.3.3.7	Deve reconhecer e inventariar tecnologias, como Java, Bancos de dados (SQL Server, MySQL, MariaDB, Oracle), Sistemas operacionais (Windows, Linux, MacOS, IOS, Android), Ferramentas de usuários (Pacotes Office, VSCode, Adobe Acrobat e Acrobat Reader).	59
1.3.3.8	Deve ser capaz de realizar varreduras de vulnerabilidades dos ativos identificados através do inventário, em períodos definidos no próprio sistema.	39
1.3.3.9	Deve possuir opção para iniciar varredura de vulnerabilidades via agendamento.	39 / 40
1.3.3.10	Deve permitir que sejam definidos janelas para execução das varreduras com o objetivo de limitar a data e horário de início e final das análises que serão realizadas no ativo.	39
1.3.3.11	Todas as vulnerabilidades detectadas pela análise de vulnerabilidades devem ser armazenadas pela plataforma para gestão.	55
1.3.3.12	Armazenar, também, todas as vulnerabilidades vinculadas a uma determinada tecnologia já lida.	55
1.3.3.13	Deve ser capaz de identificar novas vulnerabilidades nos ativos inventariados, sem execução de varreduras e sem geração de tráfego baseando-se nas tecnologias do ativo.	74
1.3.3.14	A solução deve gerar alertas de vulnerabilidades via plataforma: e-mail, Telegram e/ou Slack.	165
1.3.3.15	Deve contar com opções de notificação, para que o gestor possa selecionar quais as suas preferências para recebimento de alertas.	165 / 166
1.3.3.16	Deve ser capaz de integrar com ferramentas de Endpoint Detection and Response (EDR).	36
1.3.3.17	Deve permitir a configuração do período, em dias, que um dispositivo será automaticamente descomissionado se permanecer inativo (sem análise de	32

	vulnerabilidade ou descoberta), ou seja, removido do inventário de dispositivos da plataforma a fim de sanitizá-la.	
1.3.3.18	Deve permitir que este seja a quantidade de dias seja configurada especificamente por técnica de descoberta do ativo, por exemplo, aqueles que foram identificados por análise de vulnerabilidade (X dias) ou através da integração com EDR (Y dias).	33
1.3.3.19	Possibilitar a configuração de janelas (períodos) onde a análise de infraestrutura poderá ser executada. Caso a análise de vulnerabilidade ultrapasse a janela configurada, a plataforma deverá pausar a análise e retomá-la assim que possível (próxima janela de execução).	40
1.3.4	<b>ITEM 03 – Análise de Exposição Dados e Credenciais</b>	
1.3.4.1	A Solução deve detectar vazamentos de informações sensíveis do TJAM com base em definições de um domínio e até 05 palavras-chave a serem definidas pelo TJAM;	26
1.3.4.2	Detectar vazamento de credenciais com base nos domínios e palavras-chave a serem definidas em conjunto pelo TJAM e CONTRATADA.	13 / 23
1.3.4.3	Deve realizar busca em múltiplas fontes que monitorem surface, deep e/ou dark web.	23 / 26
1.3.4.4	Deve realizar a classificação das credenciais que foram descobertas, incluindo aquelas que são diretamente de servidores do TJAM, mas também aquelas que são de clientes/usuários do TRIBUNAL, ou seja, usuários que utilizam serviços do TJAM.	24
1.3.4.5	Deve implementar formas automatizadas para a classificação dos itens que foram identificados reduzindo, sempre que possível, o esforço da análise / categorização manual.	101
1.3.4.6	Deve permitir, de forma macro, visualizar e correlacionar as credenciais das listas de registros encontradas a fim de evitar que os mesmos registros que foram identificados sejam expostos.	24
1.3.4.7	Deve implementar monitoramento de grupos de Telegram, onde são divulgadas informações dessa natureza.	15
1.3.4.8	As credenciais identificadas devem sempre que possível conter as seguintes informações: Classificação do vazamento, usuário (e-mail vazado), senha (password), alvo do acesso (site, URL, etc), descrição, data de vazamento e data da descoberta do vazamento.	25
1.3.4.9	Detectar vazamento de códigos-fonte de aplicações de desenvolvimento interno, com base em palavras-chave a serem definidas em conjunto pelo TJAM e CONTRATADA.	13
1.3.4.10	Deve verificar repositórios de códigos-fonte públicos como, por exemplo, GitHub, Gitlab, Postman e endereços de armazenamento de texto como, por exemplo, o site Pastebin com o objetivo de detectar compartilhamento indevido de informações corporativas.	140 / 141
1.3.4.11	Detectar referências (links) para os domínios e/ou palavras-chave que sinalizem uma possibilidade de vazamentos de documentos ou serviços do TJAM.	12
1.3.4.12	A solução deve possuir painéis que apresentem de forma consolidada um resumo do status atual da análise com base em classificações, indicando a	139

	evolução da análise dos achados, ou seja, quantos estão em análise e quantos foram fechados ou resolvidos.	
1.3.4.13	Para as funcionalidades de monitoramento de fraude e vazamento de informação que permitam a classificação das informações identificadas pelo sistema, deve possibilitar a classificação de um item identificado, pelo menos, como:	101
1.3.4.13.1	sob análise, para itens que foram encontrados e precisam ser verificados;	101
1.3.4.13.2	confiável ou resolvido, para itens que foram encontrados, mas são confiáveis ou já foram resolvidos;	101
1.3.4.13.3	irrelevante, para itens que foram encontrados e não representam risco ou fraude.	101
1.3.4.14	Possibilidade de personalizar quais colunas serão exibidas e em qual ordem serão exibidas.	9
1.3.4.15	Possibilidade de exportar as informações da tabela que são apresentadas na tela para valores separados por vírgulas ou ponto e vírgula (CSV – comma separated values).	9
<b>1.3.5</b>	<b>GRUPO 04 – Detecção de Domínios Fraudulentos</b>	
1.3.5.1	A Solução deverá realizar as análises de Fraudes Web com base em definições de um domínio e até 05 palavras-chave a serem definidas pelo TJAM;	158
1.3.5.2	Deve realizar monitoramento de nomes de domínio cadastrados na Internet, para identificar nomes semelhantes aos domínios monitorados (tipo de ataque também conhecido como cybersquatting).	158
1.3.5.3	Deve detectar possíveis domínios fraudulentos e permitir a notificação através da própria plataforma, e-mail, Telegram e/ou Slack.	165
1.3.5.4	Deve, sempre que possível, fornecer uma foto (screenshot) da tela (homepage) do possível domínio fraudulento.	155
1.3.5.5	Deve, sempre que possível, fornecer informações de cadastro do domínio (whois).	154
1.3.5.6	Utilizar de múltiplas inteligências (por exemplo: algoritmos de registro) para descoberta de possíveis domínios fraudulentos.	153
1.3.5.7	Consultar, no ato do registro, a legitimidade do domínio.	153
1.3.5.8	Apresentar uma pontuação (score) indicando a probabilidade de o IP para qual o domínio aponta ser utilizado para fraude, com o objetivo de possibilitar a priorização de ações.	154
1.3.5.9	Deve apresentar se o site em questão tiver selo seguro (HTTPS), qual a data de expiração do certificado SSL.	157
1.3.5.10	A funcionalidade de proteção de aplicações móveis deve ser capaz de permitir o cadastro de palavras-chave e nomes de aplicativos móveis (apps) que o TJAM tenha atualmente ou venha a ter para monitoramento.	158 / 159
1.3.5.11	Deve monitorar lojas de aplicativos (marketplaces) oficiais e não-oficiais, como Google Play, Apple Store e Aptoide, para detectar aplicativos que possam utilizar o nome do TJAM com objetivo de realizar fraudes.	148
1.3.5.12	Deve detectar possíveis aplicativos móveis falsos com o nome do TJAM, através da plataforma: e-mail, Telegram e/ou Slack.	148 / 165
1.3.5.13	A plataforma deverá executar o monitoramento periódico de tais informações de forma automatizada.	158

1.3.5.14	A funcionalidade de redes sociais (social networks) deve possibilitar o monitoramento de redes sociais com objetivo de identificar usuários, páginas e postagens (posts) que façam referência às palavras-chave que são monitoradas.	144
1.3.5.15	A solução deve realizar buscas, no mínimo nas seguintes redes sociais: Facebook, Instagram, TikTok, X (Twitter) e YouTube, trazendo informações que estejam disponíveis como “likes”, “comments”, “shares”, “posts”, “followers”, “following”.	144
1.3.5.16	Possibilidade de adicionar o usuário na lista de usuários permitidos (“add user to whitelist”) com o objetivo que todas as publicações do usuário já sejam automaticamente classificadas como permitidas (whitelisted).	159
1.3.5.17	A plataforma deverá executar o monitoramento periódico de redes sociais de forma automatizada.	158
1.3.5.18	A funcionalidade de web de superfície ou conteúdo indexado (surface web) deve possibilitar o monitoramento de conteúdos que estejam indexados em buscadores como, por exemplo, Google, repositórios de objetos ou arquivos (buckets AWS S3, por exemplo) e blogs.	12 / 142
1.3.5.19	Tal funcionalidade tem como objetivo identificar itens que não em categorias referenciadas anteriormente, contudo mesmo assim representem potencial risco de fraude ao TJAM.	142
1.3.5.20	Deve possibilitar a criação de marcação ou posicionamento específico, no momento da análise de páginas de fraudes que copie o conteúdo do TJAM ou conduta de redirecionamento da página e/ou que fazem referência a ela.	101 / 102
1.3.5.21	Tal funcionalidade tem como objetivo reduzir o tempo de identificação de páginas falsas que são utilizadas pelos fraudadores.	101 / 102
1.3.5.22	A solução deve possuir dashboards que apresentem de forma consolidada um resumo do status atual da análise dos achados, ou seja, quantos estão em análise e quantos foram fechados ou resolvidos.	139
1.3.5.23	Para as funcionalidades de monitoramento de fraude e vazamento de informação que permitam a classificação das informações identificadas pelo sistema, deve possibilitar a classificação de um item identificado, pelo menos, como:	101
1.3.5.23.1	sob análise (under analysis), para itens que foram encontrados e precisam ser verificados;	101
1.3.5.23.2	confiável (trusted) ou resolvido (solved), para itens que foram encontrados, mas são confiáveis ou já foram resolvidos;	101
1.3.5.23.3	irrelevante (irrelevant), para itens que foram encontrados e não representam risco ou fraude.	101
1.3.5.24	Possibilidade de personalizar quais colunas serão exibidas e em qual ordem serão exibidas.	9
1.3.5.25	Possibilidade de exportar as informações da tabela que são apresentadas na tela para valores separados por vírgulas ou ponto e vírgula (CSV – comma separated values).	9 / 10
1.3.6	Especificação técnica comum aos GRUPOS 01, 02, 03 e 04	

1.3.6.1	Contratação de solução de segurança no modelo híbrido (parte SaaS (Software as a Service) e parte on-premise capaz de realizar análise, monitoramento e acompanhamento de parâmetros de segurança no processo de gestão de vulnerabilidade desde o desenvolvimento de software até a proteção da marca (reputação) do TJAM.	161 - 163
1.3.6.2	A solução contratada deverá atender, diretamente ou em composição, aos seguintes requisitos desta contratação:	
1.3.6.2.1	No caso de composição de soluções e necessidade de integração, a CONTRATADA fornecerá ao TJAM um painel único, seguro, com uma única autenticação que mostre as informações de vulnerabilidades e proteção de reputação centralizadas.	163
1.3.6.2.2	A solução deverá mostrar e possibilitar a integração de funcionalidades de vulnerabilidade incluindo infraestrutura, desenvolvimento seguro (DevSecOps) e proteção de reputação.	163
1.3.6.3	A solução deve contar com uma interface web intuitiva para acesso às funcionalidades.	5 - 10 / 131 - 134
1.3.6.3.1	A plataforma deverá atender os módulos dos GRUPOS 01, 02, 03 e 04.	4
1.3.6.4	Implementar controle de acesso baseado em permissões de usuários para as funcionalidades da solução.	115
1.3.6.5	Deverá conter, pelo menos, três papéis (funções) de usuário pré-definidas: administrador, operador e visualizador. Cada nível restringirá as configurações e ações que o usuário poderá realizar em cada um dos módulos da solução.	115 - 116
1.3.6.6	Possibilidade de configurar um segundo fator de autenticação (2FA) com base em códigos baseados em chaves digitais (soft tokens) através de aplicativos como: Microsoft Authenticator e Google Authenticator.	105
1.3.6.7	Possibilidade de configurar o segundo fator de autenticação (2FA) como obrigatório para todos os usuários que utilizam a plataforma; ou	105
1.3.6.7.1	Possibilidade de configurar o segundo fator de autenticação como não obrigatório, podendo individual ape-nas para alguns usuários que utilizam a plataforma.	107
1.3.6.8	Possibilidade de configurar Single Sign On (SSO) para autenticação através de identidade federada com, no mínimo, as seguintes soluções:	4
1.3.6.8.1	Microsoft Active Directory Federation Services (ADFS)	87
1.3.6.8.2	Okta	76
1.3.6.9	Possibilidade de escolher o idioma de interface suportando, no mínimo, 2 idiomas: português e inglês.	72
1.3.6.9.1	Deve permitir que o usuário selecione um idioma padrão que já esteja salvo toda vez que ele abrir a solução.	72
1.3.6.10	Deve possuir uma área de consulta (referência rápida) onde o usuário realizará uma busca que inclua, no mínimo, as seguintes informações:	4
1.3.6.10.1	Sobre CVE (Common Vulnerabilities and Exposures): apresentar informações gerais sobre a vulnerabilidade como, por exemplo, pontuação (score), vetor de ataque (attack vector), referências externas, deverá manter-se atualizada sobre tendências, dispositivos e aplicações que são afetadas, além de exploits que já estejam disponíveis para explorar tal vulnerabilidade.	65

1.3.6.10.2	Sobre TTP (Tactics, Techniques and Procedures): referência geral à estrutura (framework) do MITRE ATT&CK sobre técnicas, táticas e procedimentos de atacantes para facilitar a consulta na solução sem que seja necessário visitar site externo.	56
1.3.6.11	Deve disponibilizar API (Application Programming Interface) para permitir integração com outras soluções do ambiente do TJAM podendo consumir os dados gerados pela plataforma.	47
1.3.6.12	Deve permitir a realização de ações em lote para a classificação dos achados da plataforma, possibilitando:	101
1.3.6.12.1	Seleção de múltiplos itens para classificação.	103
1.3.6.12.2	Seleção de múltiplos itens para edição de severidade, que se estenda para uma ação possível da plataforma.	103
1.3.6.12.3	Incluir comentários em achados, sempre que possível.	11
1.3.6.12.4	Seleção de múltiplos itens para ações, sempre que se tratar de uma ação possível da plataforma.	103
1.3.6.13	Deve possibilitar a adição e visualização de comentários de atividade nos achados para que seja possível rastreabilidade e trabalho colaborativo entre os usuários da plataforma.	11
1.3.7	<b>Especificação técnica comum aos GRUPOS 01 e 02.</b>	
1.3.7.1	A solução deve implementar tecnologia para análise dos códigos-fonte, através de concentradores de análise que deverão ser instalados dentro da infraestrutura (on-premises ou cloud) do TJAM de forma centralizada utilizando recursos de máquinas virtuais do próprio TJAM.	41
1.3.7.2	Entende-se por forma centralizada, não ser necessária a instalação em cada equipamento do desenvolvedor e/ou servidor de repositório de código-fonte.	35
1.3.7.3	Os concentradores de análise deverão ser compatíveis, no mínimo, com as seguintes versões de Sistema Operacional:	
1.3.7.3.1	Ubuntu 18.04.6 LTS (Bionic), 20.04.2 LTS (Focal) e 22.04.5 (Jammy Jellyfish).	34
1.3.7.4	Todas as credenciais que forem cadastradas na plataforma para acesso aos serviços do TJAM deverão ser armazenadas de forma segura garantindo que, uma vez cadastradas pelo TJAM, não sejam exibidas novamente na interface web em texto claro.	29
1.3.7.5	Todo tráfego de informação como credenciais, descobertas de vulnerabilidades ou outros tipos de comunicação entre a plataforma e os concentradores de análise deverá ser realizado através de protocolo seguro usando criptografia.	35
1.3.7.6	Sempre que houver uma nova varredura de vulnerabilidades, deverá ser atualizada a lista de vulnerabilidades ativas aquelas que não forem mais detectadas, mantendo assim as informações atualizadas.	117
1.3.7.7	Permitir a classificação dos itens de vulnerabilidade como redes, ativos, aplicações, etc através do uso de marcações conhecidas como tags ou labels a fim de organizar e agrupá-los, devendo permitir a criação e customização de novas marcações.	17
1.3.7.8	Para cada conjunto de análise que a plataforma executar, deverá fornecer painel (dashboard) com visão geral do cenário atual de vulnerabilidades, bem	117

	como sua evolução e priorização. Tal painel deverá apresentar, no mínimo, as seguintes informações:	
1.3.7.8.1	Achados por categoria (possibilitando filtrar: baixas, médias, altas e críticas).	117 - 127
1.3.7.8.2	Total de dispositivos ou achados.	117 - 127
1.3.7.8.3	Total de vulnerabilidades.	117 - 127
1.3.7.8.4	Classificação dos achados por família.	117 - 127
1.3.7.8.5	Priorização com base na criticidade da vulnerabilidade, na probabilidade (likelihood) e ativos do ambiente do TJAM através de um gráfico que agrupe: urgente (corrigir agora), alta (corrigir depois), média (planeje corrigir) e baixa (corrigir depois de todas as outras).	117 - 127
1.3.7.8.6	Vulnerabilidades ou achados novos ou resolvidos por período.	117 - 127
1.3.7.8.7	Evolução dos achados ao longo do tempo.	117 - 127
1.3.7.8.8	Lista configurável com, por exemplo, os 10, 15, 20, 50 ou 100 ativos com mais vulnerabilidades no ambiente.	117 - 127
1.3.7.9	Para cada conjunto de análise que a plataforma executar, deverá fornecer uma visualização em lista de itens que ao clicar permite entender quais vulnerabilidades estão associadas com aquele dispositivo ou aplicação.	66 - 67
1.3.7.10	Tais vulnerabilidades ou achados deverão ser agrupados, no mínimo, pelos seguintes critérios: abertos, mitigados, transferidos, fechados, não aplicáveis ao ambiente do TJAM (falso-positivos) ou removidos por automação da plataforma (descomissionados).	102
1.3.7.11	Deve permitir filtrar as informações das vulnerabilidades com base nas seguintes informações:	117 - 120
1.3.7.11.1	Severidade (crítica, alta, média e baixa).	117 - 120
1.3.7.11.2	Família.	117 - 120
1.3.7.11.3	Tecnologia.	117 - 120
1.3.7.11.4	Status do achado (aberto, mitigado, transferido, fechado, falso-positivo e descomissionados).	117 - 120
1.3.7.11.5	Nome do achado/vulnerabilidade.	117 - 120
1.3.7.11.6	CVSS (pontuação da família ou conformidade).	117 - 120
1.3.7.11.7	Marcações (Tags ou Labels).	117 - 120
1.3.7.11.8	Datas: item criado, item em reanálise e/ou reintervenção e/ou intervenção e data que foi fechado.	117 - 120
1.3.7.12	Deve possibilitar a exportação das informações apresentadas na plataforma (com base nos filtros aplicados) para valores separados por vírgulas ou ponto e vírgula (CSV – comma separated values).	9 - 10