2025 WTR WORKSHOP TECNOLOGIAS DE REDE PoPRN

Fortaleça Sua Segurança com Soluções Open-Source

Matheus Camargo

CAIS/RNP

RNP

$whoami

Matheus Camargo

- Analista de Segurança na Informação Sr no CAIS/RNP
- Formado em Redes de Computadores
- MBA em Cibersecurity
- 9 Anos de experiencia em TI e segurança, 4 em segurança ofensiva
- CVE-2024-3867 – XSS no Tainacan
- CVE-2024-55210
- SANS GCIH
- Futebol toda semana
- Warzone, Apex Legends, Chess.com nos momentos livres

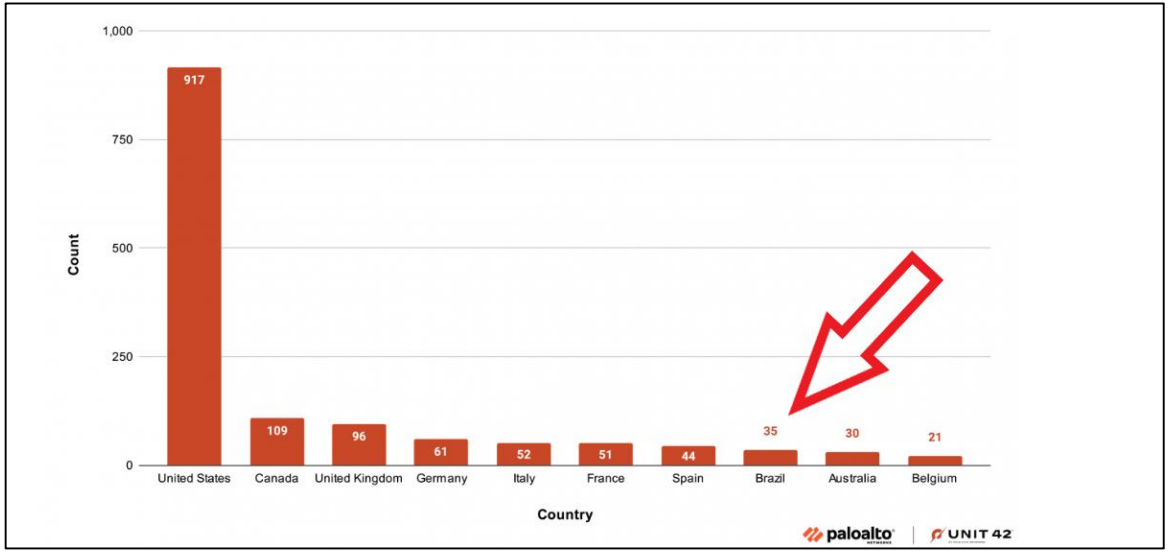
Agenda

- Cenário Atual
- Como Fortalecer sua Segurança com Soluções Open Source
- Soluções Open Source
- Conclusão

Cenário Atual: Ataques Cibernéticos em Alta

Em 2024, um ataque cibernético ocorreu a cada 39 segundos no mundo
(Clark School, University of Maryland https://keepnetlabs.com/blog/171-cyber-security-statistics-2024-s-updated-trends-and-data)

Brasil está entre os **10 países mais atacados**, com foco em vazamento de dados e ransomware
(Kaspersky, Fortinet https://br.cointelegraph.com/news/brazil-registers-1-379-cyber-attacks-per-minute-reveals-kaspersky-report https://www.fortinet.com/br/resources/reports/threat-landscape-report)



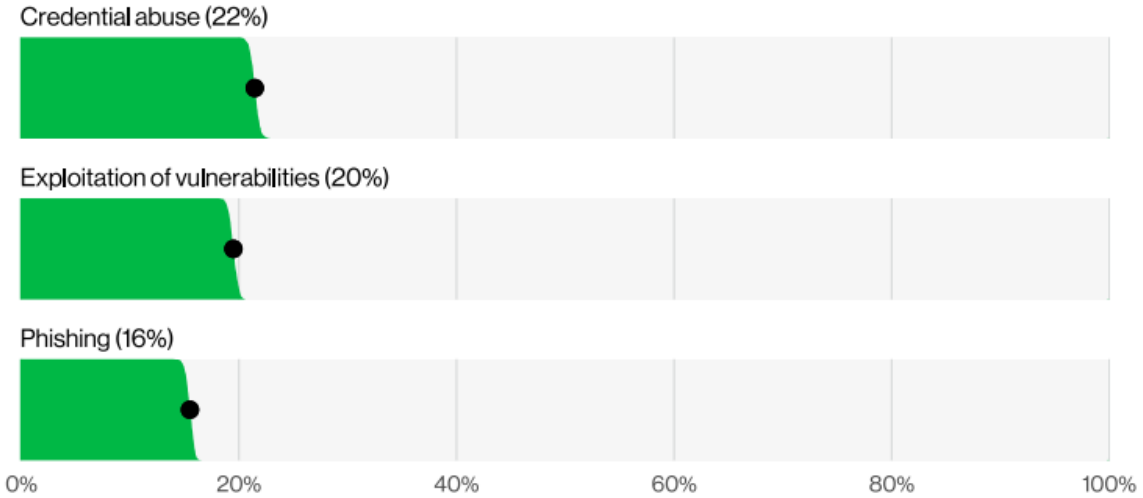
https://unit42.paloaltonetworks.com/unit-42-ransomware-leak-site-data-analysis/

Devemos se preocupar com vulnerabilidades?

Vulnerabilidades ainda são porta de entrada para ataques!

- Em 2024, mais de 40.000 vulnerabilidades novas foram catalogadas (https://www.cvedetails.com/)

- Em 2025, há um aumento de 34% na ocorrência de ataques provenientes de exploração de vulnerabilidades (https://www.verizon.com/business/resources/reports/dbir/)



https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf

Ransomware: Como se Proteger

USAR AUTENTICAÇÃO MULTIFATOR (MFA)

Exigir a autenticação multifator, para acesso remoto à rede, serviços web, serviços em nuvem e usuários com privilégios de administrador.

CONSCIENTIZAR FUNCIONÁRIOS

Treinar funcionários e terceiros para reconhecer e reportar potenciais problemas de segurança.

FAZER E PROTEGER *BACKUPS*

Fazer *backups* regulares. Manter ao menos uma cópia *offline*. Proteger contra acesso indevido e testar regularmente se os dados estão íntegros e a restauração é eficaz.

GERENCIAR IDENTIDADES E ACESSOS

Conceder às contas apenas os acessos essenciais e pelo tempo necessário.

FAZER GESTÃO DE VULNERABILIDADES

Fazer gestão de vulnerabilidades usando estratégia de priorização baseada em risco.

USAR FERRAMENTAS DE PROTEÇÃO

Implementar ferramentas de proteção e de monitoração de rede.

REDUZIR A SUPERFÍCIE DE ATAQUE

Desativar serviços sem uso e não expor os demais desnecessariamente.

SEGMENTAR A REDE

Dividir a rede em segmentos menores e segregados.

https://cert.br/docs/ransomware/proteger/

Compreender **os princípios da gestão de vulnerabilidades:**

- ***Conjunto de atividades coordenadas que tem por objetivo a redução, a níveis aceitáveis, das vulnerabilidades de segurança encontradas durante o processo de "Análise de Segurança" ou "Análise de Vulnerabilidades" em um determinado ativo, conjunto de ativos ou ambiente.***

  Guia Gestão de Vulnerabilidades Técnicas - RNP

- **Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.**

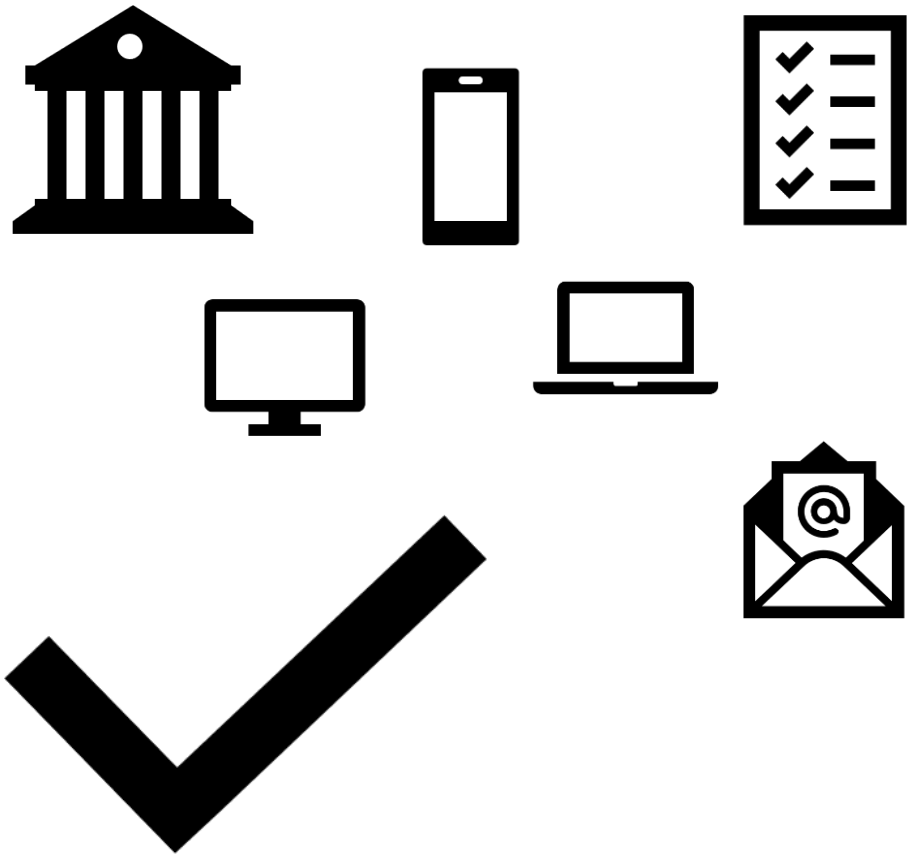
  CIS Controls v8, Safeguards 7.1

Definição de Escopo

A execução de um processo de Gestão de Vulnerabilidades é melhor realizada quando se tem um escopo bem definido

Normalmente, o escopo precisa ser o mais abrangente possível, contendo todos os ativos da instituição

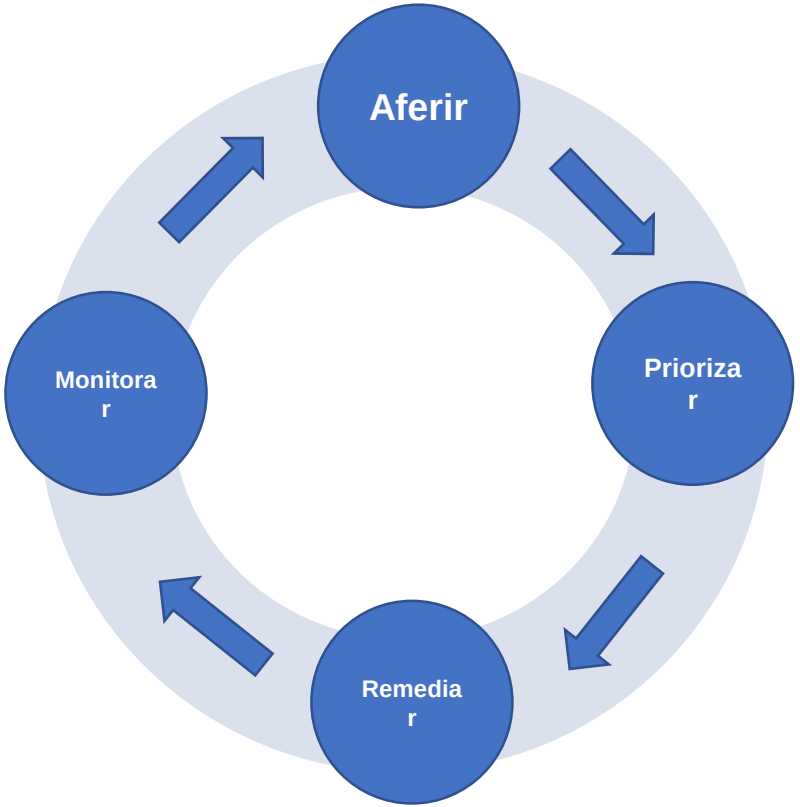
Dessa forma, a definição do escopo pode estar atrelada ao processo de inventariado. Se fizermos essa associação, garantiremos que todos os ativos, incluindo novos ativos no parque, estão incluídos no processo de Gestão de Vulnerabilidades



Como Fortalecer sua Segurança com Soluções Open-Source

Gestão de Vulnerabilidades: Ciclo de vida

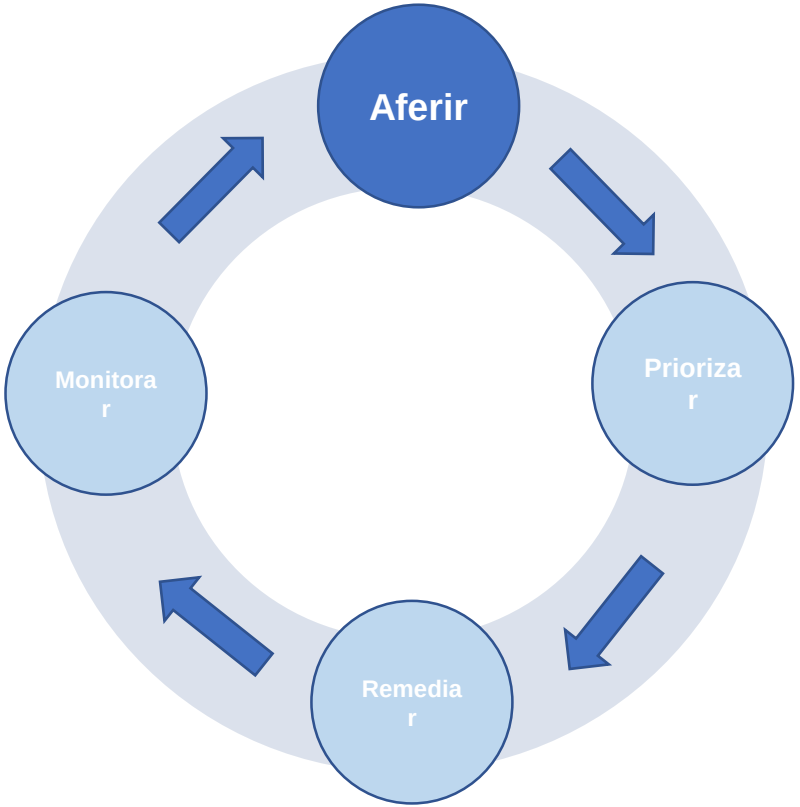
- Processo contínuo
- Foco em reduzir a superfície de ataque e mitigar riscos reais
- Envolve integração entre áreas (ex. times de infraestrutura, segurança e desenvolvimento)
- É uma prática organizacional para identificação, avaliação, priorização e correção de vulnerabilidades



Como Fortalecer sua Segurança com Soluções Open-Source

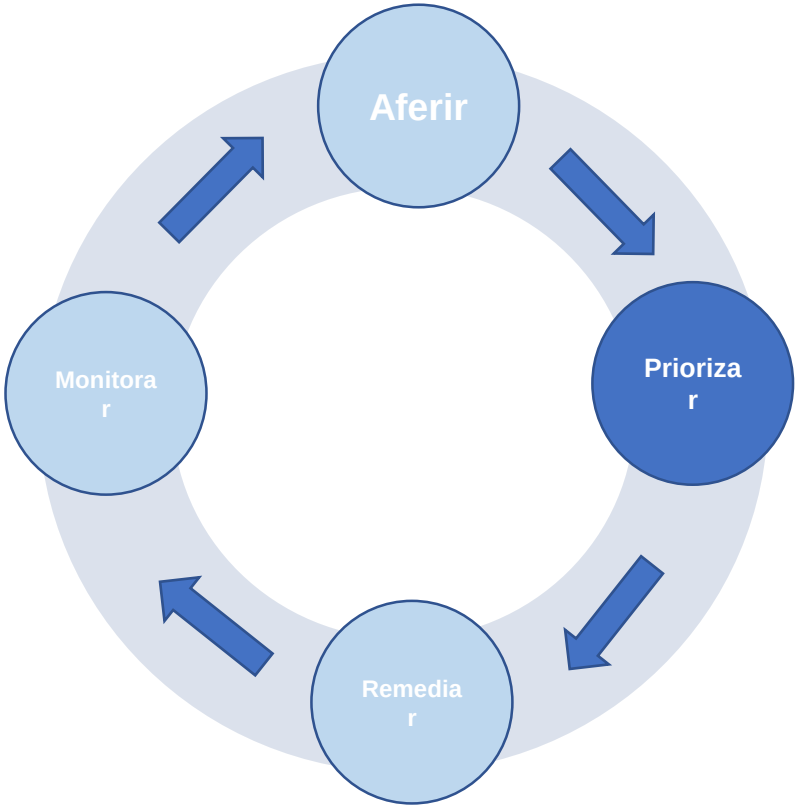
Gestão de Vulnerabilidades: Aferir

- Busca ativa por vulnerabilidades
- Ações automatizadas e/ou manuais
- Padrão de Severidade:
  - Crítica
  - Alta
  - Média
  - Baixa
  - Informativa
- Obtenção de listagem inicial



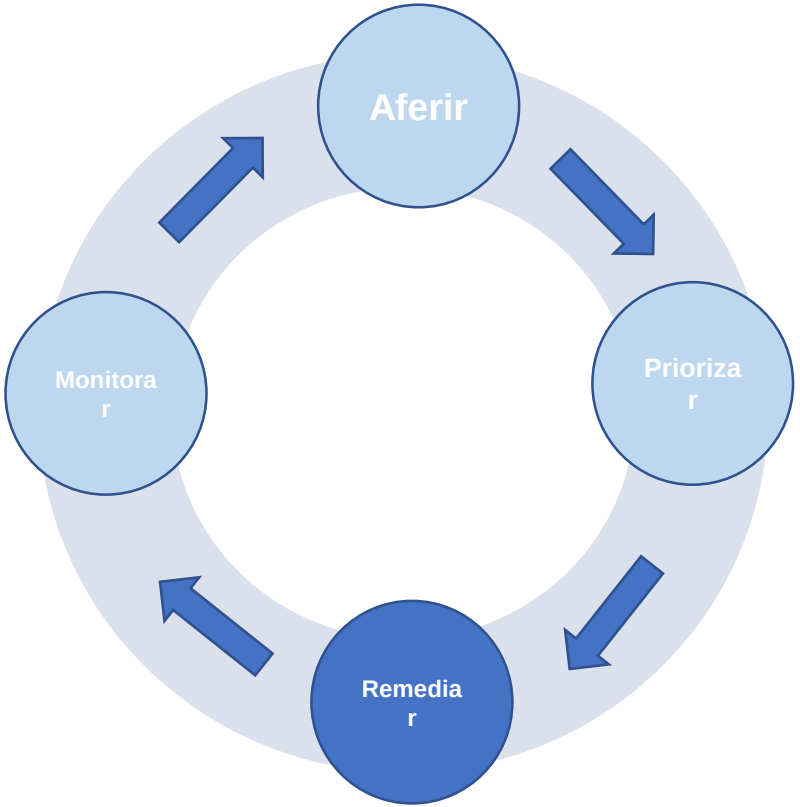
Gestão de Vulnerabilidades: Priorizar

- Atividade de classificação de vulnerabilidades
- CVSS, EPSS, KEV, SSVC
- Podem haver alterações em severidades
- Obtenção de uma lista pós priorização



Gestão de Vulnerabilidades: Remediar

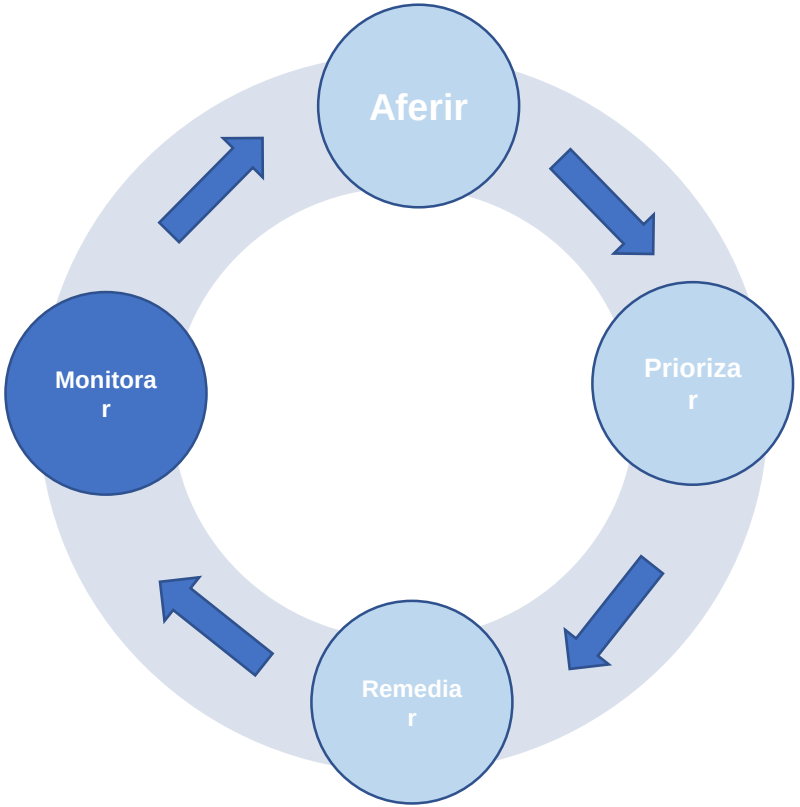
- Aplicação de correções e/ou mitigações
- Sempre tentar remover a vulnerabilidade
- Aplicar mitigações diferenciadas em casos específicos
- Falhas tratadas



Como Fortalecer sua Segurança com Soluções Open-Source

Gestão de Vulnerabilidades: Monitorar

- Verificar a eficácia das tratativas
- Tratar outros problemas que venham a aparecer
- Descobrir a raiz do problema
- Reaplicar controles ou aplicar novas mitigações



Soluções Open-Source Recomendadas

Defect Dojo

Fonte: https://defectdojo.github.io/django-DefectDojo/

- Plataforma para Gestão de Vulnerabilidades
- Código Aberto
- Boas Integrações com Ferramentas de Segurança
- API robusta e muito funcional
- Provê grande auxílio em SecDevOps
- Aceita diversos tipos de relatório, incluindo de ferramentas específicas para nuvem

Soluções Open-Source Recomendadas

Defect Dojo

DAST: Acunetix Scan / Acunetix360 Scan, AppSpider, ZAP Scan, Burp Scan / Burp Enterprise, IBM AppScan DAST, Netsparker Scan, Wapiti Scan, Nikto Scan, Arachni Scan, Wpscan, etc.

SAST / SCA / SBOM / Outros: Bandit Scan, Brakeman, Checkmarx Scan (incluindo a versão "detailed"), Dependency Check Scan, Dependency Track FPF, Retire.js Scan, NPM Audit Scan, Safety Scan, Trufflehog Scan, ESLint Scan, Gosec Scanner, Gitleaks Scan, Rubocop Scan, Rusty Hog Scan, Semgrep JSON Report, Snyk Scan, OWASP Dependency Check, etc.

Container / Infraestrutura / Image Scans: Anchore Engine Scan / Enterprise / Grype, Clair Scan, Twistlock Image Scan, Trivy Scan / Trivy Operator Scan, Harbor Vulnerability Scan, Aqua Scan, etc.

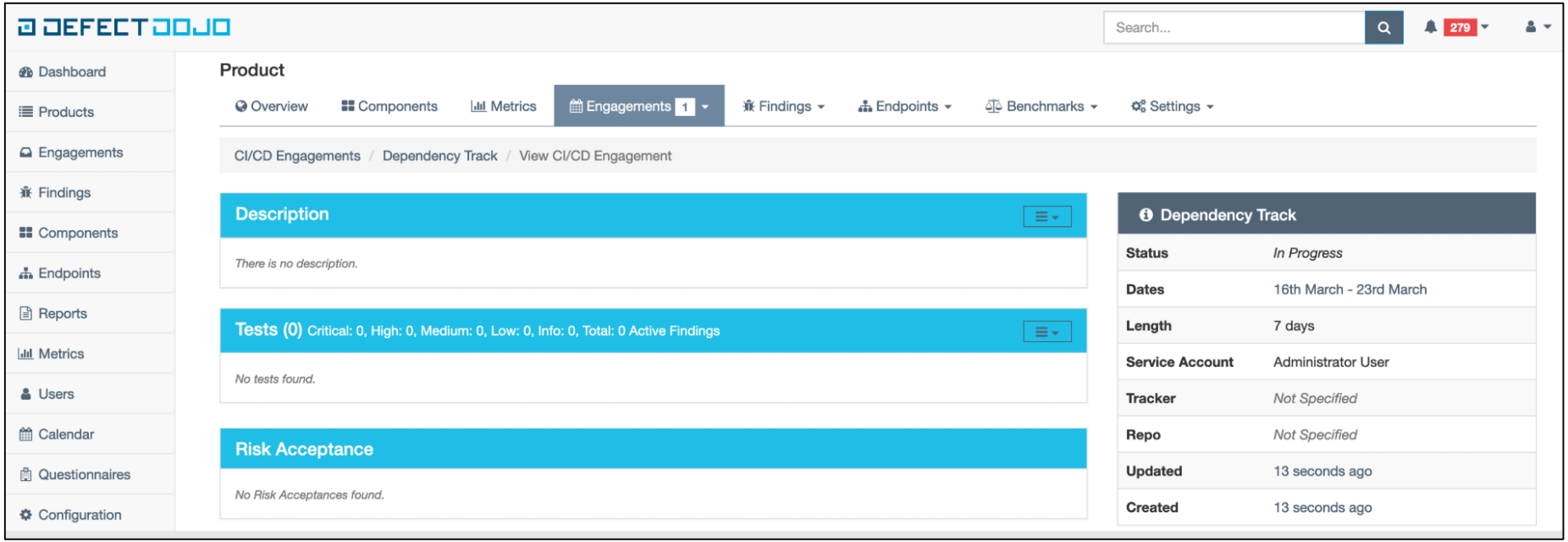
Cloud / Infraestrutura / Diverso: AWS Prowler Scan, AWS Scout2 Scan, AWS Security Hub Scan, Qualys Scan / Infrastructure / Webapp Scan, OpenVAS CSV, Nexpose Scan, Nmap Scan, Outpost24 Scan, etc.

Outros (API, integração, compliance, etc.): BugCrowd Scan, HackerOne Cases, Crowd-sourced APIs (GitHub Vulnerability Scan, GitLab SAST Report, etc.), CrashTest JSON/XML, CycloneDX, SARIF, Trelliscan, etc.

Ferramentas adicionais: Blackduck Hub / Component Risk, SonarQube Scan / detailed / API import, Sonatype Application Scan, Contrast Scan, Microfocus Webinspect Scan, Mozilla Observatory Scan, Whitesource Scan, SSL Labs Scan, SSLyze Scan (JSON), Sslscan, Testssl Scan, kube-bench, Codechecker, DSOP Scan, Trufflehog3, and muitos outros.

Soluções Open-Source Recomendadas

Defect Dojo: Interface



Soluções Open-Source Recomendadas

OpenVAS

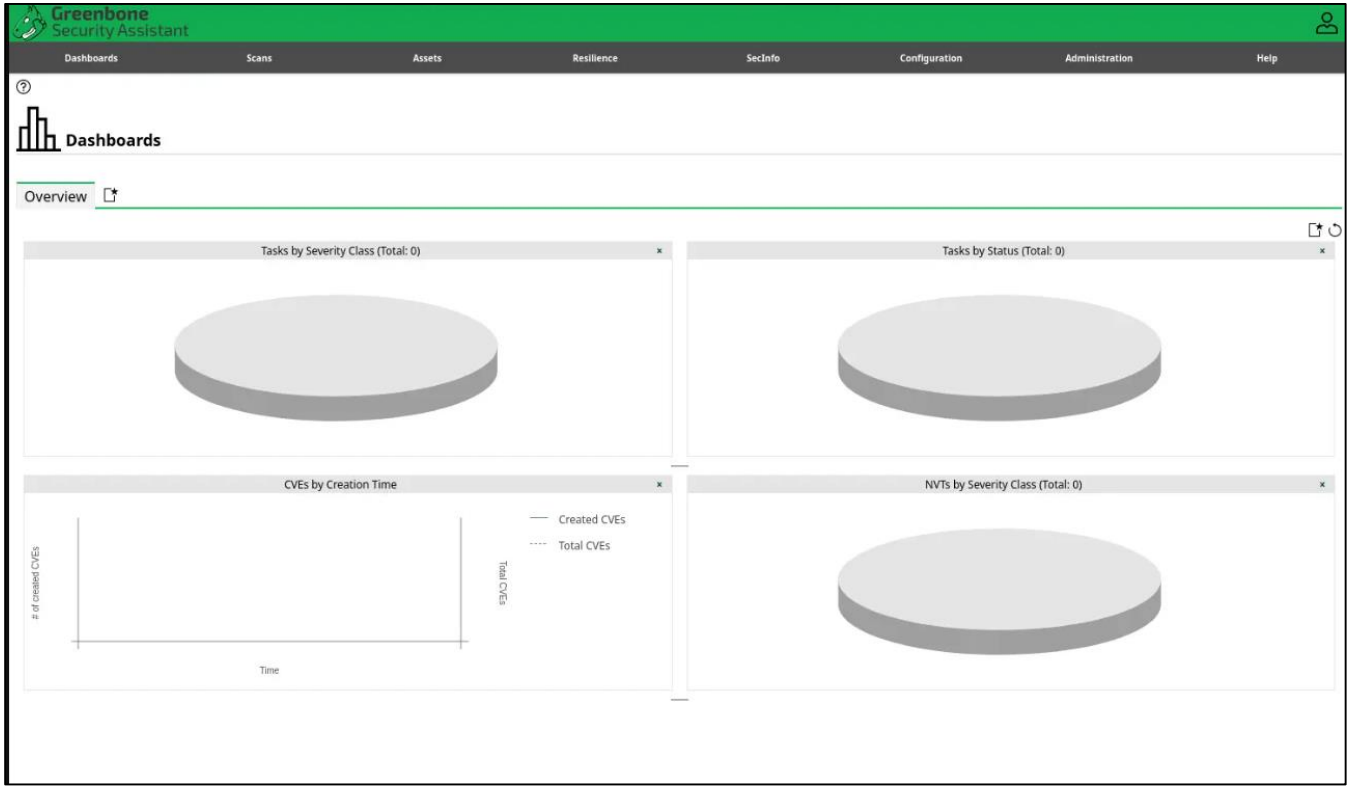
Greenbone

Sustainable Resilience

Fonte: https://greenbone.github.io/docs/latest/index.html

- Open Vulnerability Assessment System
- OpenVAS = Greenbone Community Edition
- Interface Web
- Scan de Vulnerabilidades
- Muito bom para varreduras em Servidores e Desktops
- Atualizações em Feeds de Vulnerabilidades são frequentes
- Gera relatórios em formatos diferentes

OpenVAS: Interface



Soluções Open-Source Recomendadas

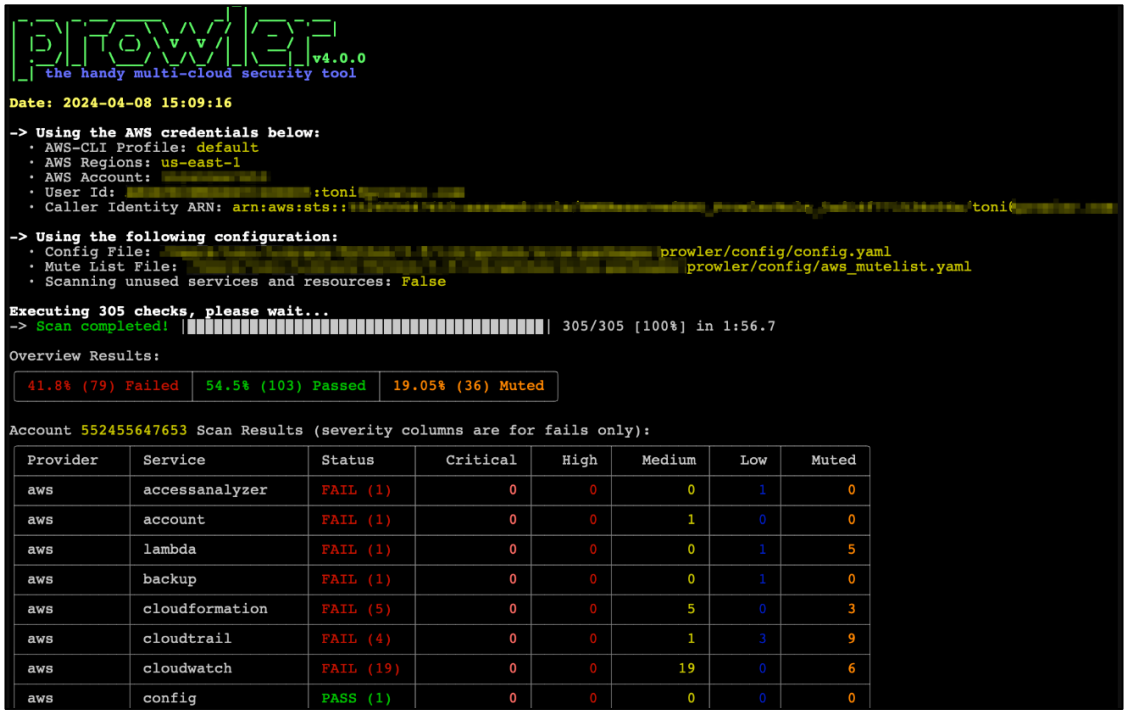
Prowler

https://github.com/prowler-cloud/prowler

- Ferramenta CLI para auditoria de contas AWS
- Avalia conformidade com benchmarks como **CIS AWS** e **HIPAA**
- Detecta permissões excessivas, falhas de configuração, recursos expostos
- Gera relatórios JSON/HTML integráveis com Defect Dojo

Soluções Open-Source Recomendadas

Prowler: interface



https://docs.prowler.com/projects/prowler-open-source/en/latest/img/short-display.png

Soluções Open-Source Recomendadas

Trivy

https://trivy.dev/latest/

- Trivy = Ferramenta Open Source da Aqua Security
- Interface CLI (linha de comando) e API REST (modo servidor)
- Scan de vulnerabilidades em Containers, Código, IaC e Secrets
- Ideal para pipelines CI/CD, containers, Kubernetes e projetos em desenvolvimento
- Atualizações frequentes do banco de dados de vulnerabilidades (via feeds como NVD, GitHub Advisory)
- Gera relatórios em múltiplos formatos (JSON, SARIF, tabela, etc.)

Soluções Open-Source Recomendadas

Trivy: Interface

```
~   trivy k8s --report summary
179 / 179 [-------------------------------------------------------------------------------------------------------------] 100.00% 12 p/s

Summary Report for k3d-first-cluster
```

Namespace	Resource	Vulnerabilities					Misconfigurations					Secrets				
		C	H	M	L	U	C	H	M	L	U	C	H	M	L	U
kube-system	Deployment/local-path-provisioner	2	5	2		1			8	11						
kube-system	Deployment/metrics-server		2	1		1			6	8						
kube-system	Deployment/traefik	3	5	1		3			7	7						
kube-system	DaemonSet/svclb-traefik	2	21	2				4	16	20						
kube-system	DaemonSet/svclb-traefik	2	21	2				4	16	20						
kube-system	Job/helm-install-traefik	10	54	20	1	14			8	11						
kube-system	Job/helm-install-traefik-crd	10	54	20	1	14			8	11						
kube-system	Deployment/coredns		1			1			8	5						
kube-system	Service/kube-dns								2	2						
kube-system	Service/metrics-server								2	2						
kube-system	Service/traefik								2	2						
default	Service/mysql								1	2						
default	Service/mysql-headless								1	2						
default	StatefulSet/mysql	12	36	26	113				7	12						
default	Pod/thisisfine	43	217	196	514	2			9	11						
default	Pod/nginx	6	18	24	92				9	11						
default	Service/kubernetes								1	2						

```
Severities: C=CRITICAL H=HIGH M=MEDIUM L=LOW U=UNKNOWN
```

https://trivy.dev/v0.28.1/docs/kubernetes/cli/scanning/

Conclusão

- Use Open Source para prototipar, testar e aprender
- Escale conforme a maturidade crescer e adquira soluções comerciais após isso
- Foque em processo, cultura, conhecimento e repetição
- Open source oferece liberdade e aprendizado; soluções comerciais oferecem escala e eficiência.

https://docs.defectdojo.com/en/about_defectdojo/about_docs/

OBRIGADO!

Matheus Nascimento de Camargo

matheus.camargo@rnp.br

PATROCÍNIO

ARPSIST FORTINET scansource Funpec GRUPO INTERJATO

APOIO

metrópole DIGITAL UFRN

REALIZAÇÃO

NÚCLEO DE REDES AVANÇADAS - UFRN

ESCOLA SUPERIOR DE REDES cais PoPRN RNP MINISTÉRIO DA CULTURA MINISTÉRIO DA DEFESA MINISTÉRIO DA SAÚDE MINISTÉRIO DAS COMUNICAÇÕES MINISTÉRIO DA EDUCAÇÃO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO