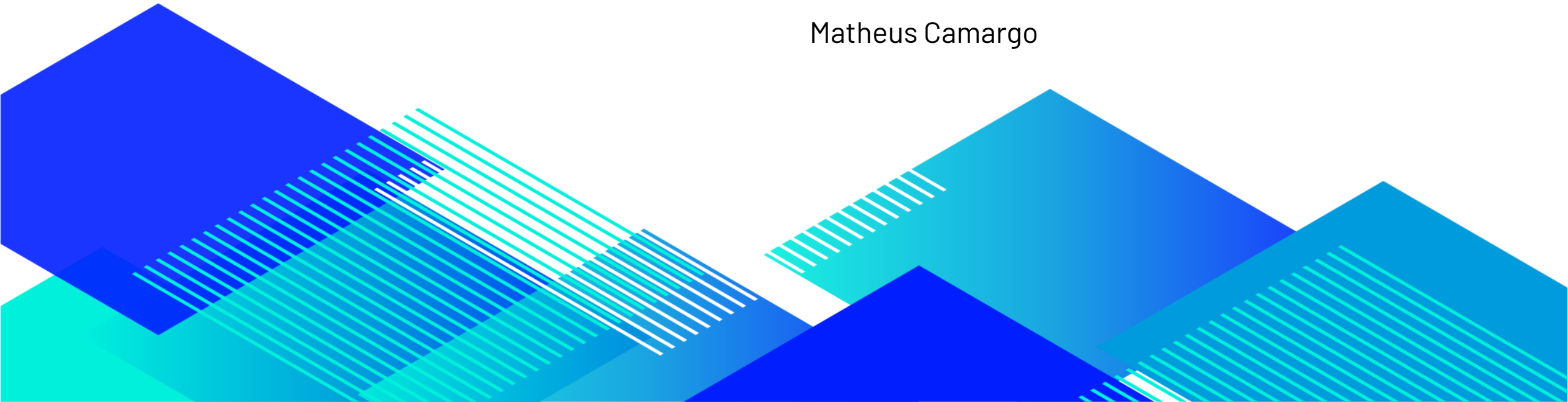
Preambulo

cais Inteligência em Cibersegurança

Gestão de Vulnerabilidades Técnicas com Ferramentas Abertas

Matheus Camargo



cais Inteligência em Cibersegurança

Sobre a Gestão de Vulnerabilidades Técnicas

02/10/24

Sobre a 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

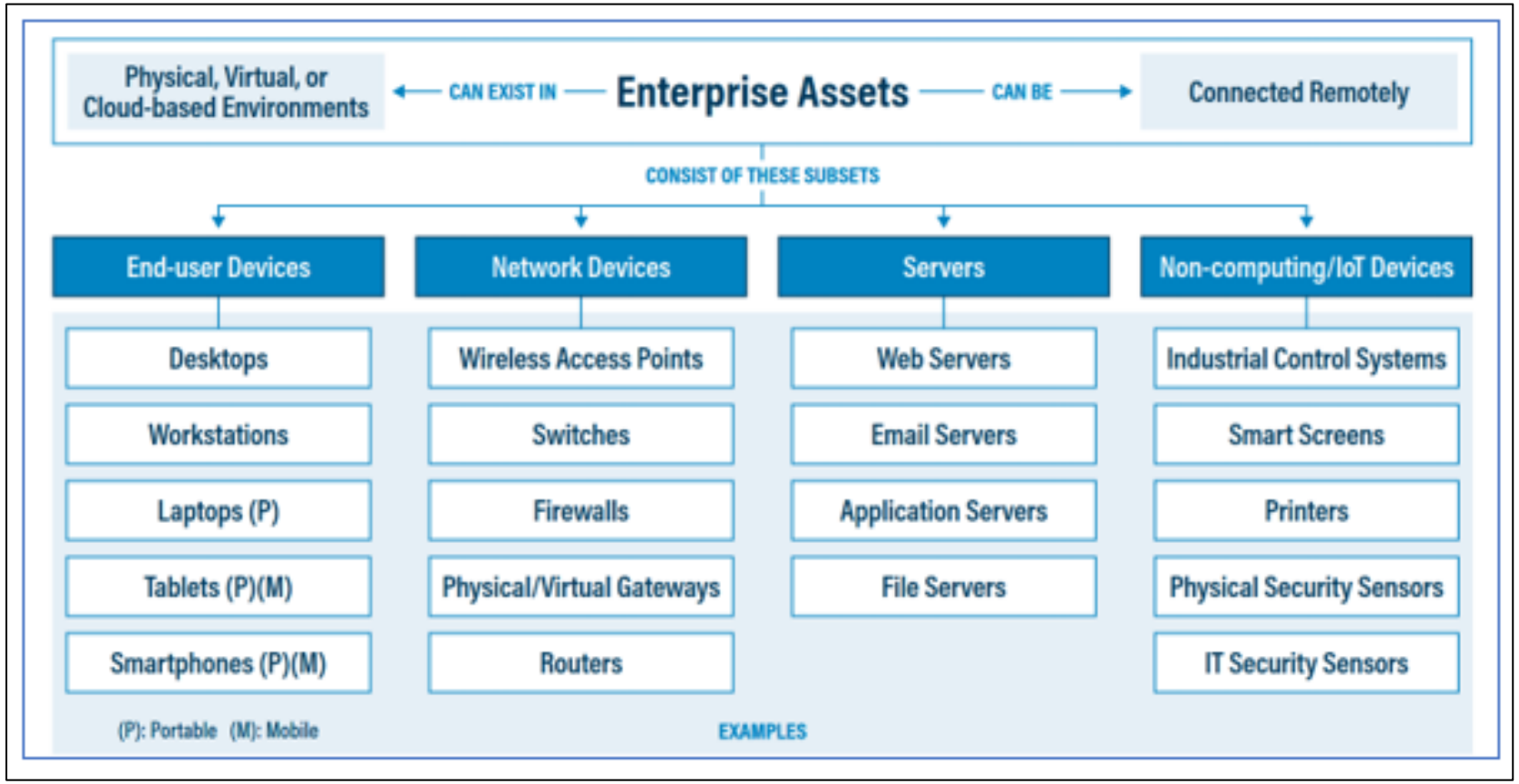
Gestão de Vulnerabilidades: Ativos

The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes.

NISTIR 8286 - NIST

Gestão de Vulnerabilidades: Ativos

- Dispositivos de Usuário Final;
- Dispositivos de Rede;
- IoT;
- Servidores.



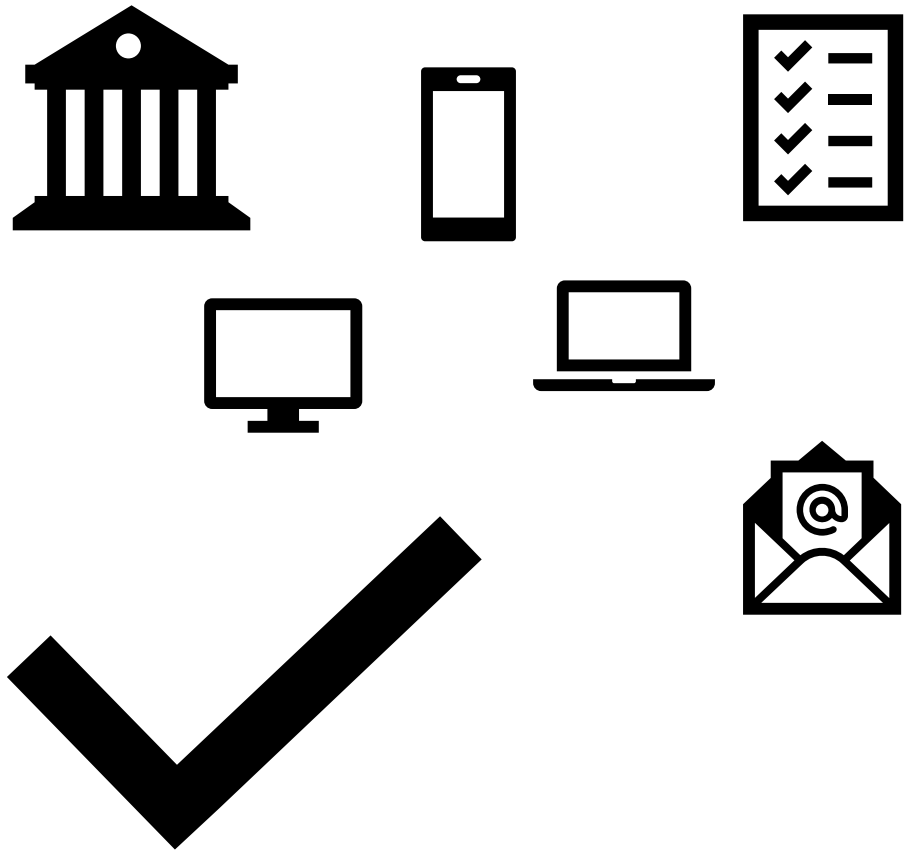
Disponível em: https://www.cisecurity.org/insights/white-papers/vulnerability-management-policy-template-for-cis-control-7

Gestão de Vulnerabilidades: Escopo

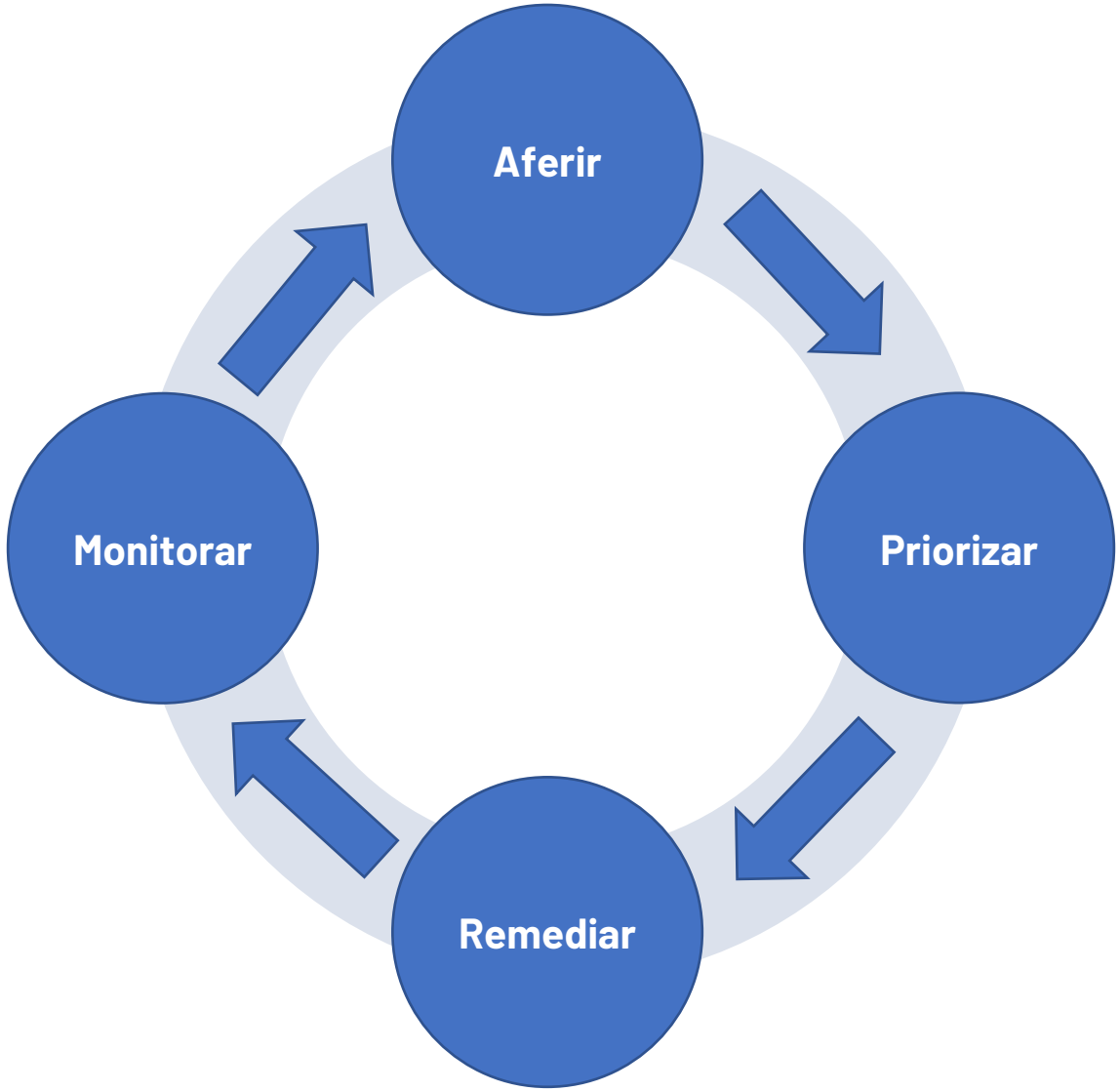
A execução de um processo de Gestão de Vulnerabilidades é melhor realizada quando se tem um escopo bem definido

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



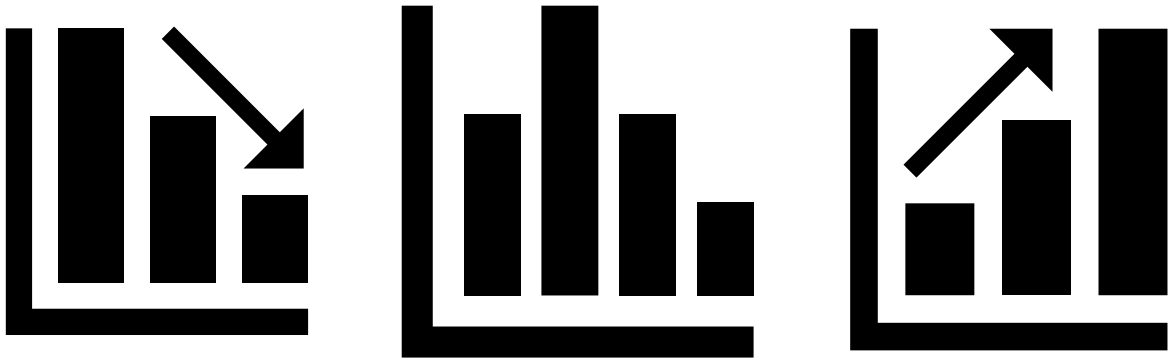
Gestão de Vulnerabilidades: Ciclo de Vida



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
- 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

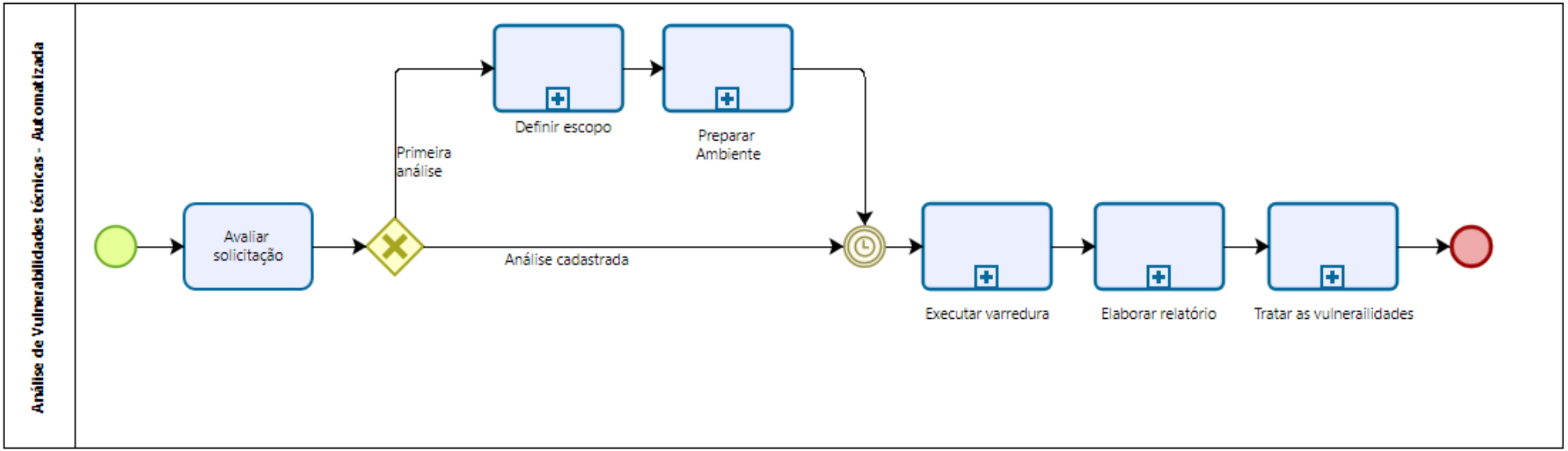
Gestão de Vulnerabilidades: Monitorar

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

Alguns Benefícios do Processo de Gestão de Vulnerabilidades

- Conhecimento do ambiente;
- Apoio no processo de Inventário de software e hardware (responsabilidade por ativos);
- Transparência;
- Informações claras sobre cada ativo e o que é necessário implementar;
- Auxílio para tomada de decisão;
- Priorização de ações;
- **Ambiente mais seguro.**

Gestão de Vulnerabilidades – Análise de Vulnerabilidades Técnicas



cais Inteligência em Cibersegurança

OpenVAS e Defect Dojo

02/10/24

OpenVAS

- Open Vulnerability Assessment System
- OpenVAS = Greenbone Community Edition
- Código Aberto
- 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

Greenbone

Sustainable Resilience

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

OpenVAS Instalação

Greenbone

Sustainable Resilience

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

- Informações em:
  - https://greenbone.github.io/docs/latest/
- Algumas formas de instalação incluem:
  - Build from Source;
  - Utilizando Conteineres;
  - Instalação de pacotes.

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

Defect Dojo - Instalação

- Informações em:
  - https://defectdojo.github.io/django-DefectDojo/getting_started/installation/
- Instalação baseada em Docker:
  - https://hub.docker.com/r/defectdojo/defectdojo-django

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

cais Inteligência em Cibersegurança

Utilizando OpenVAS

02/10/24

OpenVAS - Configurando Novas Credenciais

Greenbone

Sustainable Resilience

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

- Credenciais são usadas para autenticação em sistemas alvo durante os scans
- São associadas aos alvos

OpenVAS - Configurando Novas Listagens de Portas

Greenbone

Sustainable Resilience

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

- Criar uma listagem de portas que serão escaneadas
- São associadas aos alvos

OpenVAS - Configurando Novos Agendamentos

Greenbone

Sustainable Resilience

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

- Criar novos agendamentos que serão associados a tarefas

OpenVAS - Configurando Novas Modalidades de Alertas

Greenbone

Sustainable Resilience

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

- Criar modalidades para envio de alertas, como por exemplo encaminhar informações via email

OpenVAS - Configurando Novos Alvos

Greenbone

Sustainable Resilience

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

- Configurar o ativo que será efetivamente escaneado

OpenVAS – Configurando Novas Tarefas

Greenbone

Sustainable Resilience

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

- Configurar o scan em si, associando alvos e agendamentos

OpenVAS – Executando Scans e Gerando Relatórios

Greenbone

Sustainable Resilience

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

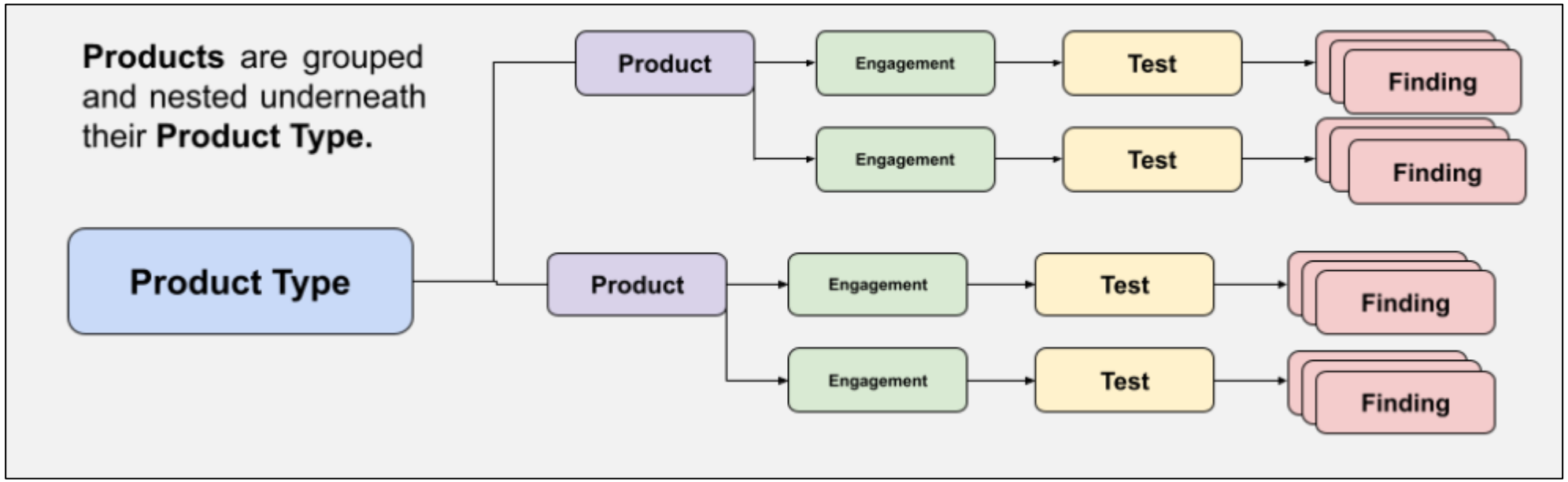
- Gerar relatórios em:
  - CSV;
  - PDF;
  - TXT

cais Inteligência em Cibersegurança

Utilizando Defect Dojo

02/10/24

DefectDojo – Entendendo sua Estrutura



Fonte: https://support.defectdojo.com/en/articles/8545273-core-data-classes-overview

DefectDojo – Configurando Tipos de Produto

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

- Tipos de Produtos ou Product Types;
- Agrupamento macro para Products
- Podem ser marcados como:
  - Critical product
  - Key product
- Podem ter controles de acesso baseados em Roles.

DefectDojo – Configurando Novos Produtos

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

- Podem ser:
  - Programas;
  - Projetos;
  - Servidores;
  - Aplicações Web;
- Precisam:
  - Ter um nome único;
  - Ter uma descrição;
  - Estar associados a um ProductType;
  - Estar associados a um SLA.
- É possível configurar controles de acesso baseados em Roles.

DefectDojo – Importando Relatórios do OpenVAS via Interface Web

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

- Regras para criação de novo Engagement:
  - Nome único;
  - Data de início e Fim;
  - Status;
  - Responsável pelo testes;
  - Um produto associado.
- Ao importar um scan, um engagement AD-HOC será criado;

DefectDojo – Importando Relatórios do OpenVAS via API

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

- Necessário token de acesso à API
  - Disponível em: /api/key-v2
- documentation.defectdojo.com/integrations/api-v2-docs/
- /api/v2/oa3/swagger-ui

DefectDojo – Obtendo Métricas e Estatísticas

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

Thanks !