Projeto de Gestão de Vulnerabilidades com DefectDojo

Este documento descreve um fluxo completo para a criação e operação de um processo de gestão de vulnerabilidades utilizando a plataforma DefectDojo. O objetivo é centralizar achados de scanners, pentests e análises manuais, priorizar riscos e garantir a correção eficiente de falhas de segurança.

1. Planejamento do Processo

- Definir fontes de vulnerabilidades (scanners, pentests, bug bounty). - Estabelecer classificação de risco (CVSS v3.1). - Definir responsáveis por cada etapa (analistas, gestores, dev/infra).

2. Configuração Inicial no DefectDojo

- Criar Produtos (ex.: Portal Web, Mobile, Cloud). - Criar Engagements (projetos, ciclos de scan, pentests). - Importar vulnerabilidades de scanners automáticos. - Criar templates de relatórios padronizados.

3. Triagem e Priorização

- Validar se a vulnerabilidade é real (eliminar falsos positivos). - Classificar severidade usando CVSS. - Priorização sugerida: * Críticas/Altas → correção imediata. * Médias → prazo intermediário. * Baixas → melhorias contínuas.

4. Atribuição e Acompanhamento

- Atribuir vulnerabilidades para responsáveis de correção. - Integrar com Jira/GitLab/GitHub Issues. - Definir SLAs de correção (ex.: Críticas em 7 dias, Altas em 15, Médias em 30, Baixas em 60).

5. Correção e Validação

- Após correção, realizar reteste no DefectDojo. - Atualizar status para Mitigated ou Accepted Risk (quando aplicável).

6. Relatórios e Métricas

- Gerar relatórios executivos e técnicos. - Métricas recomendadas: * Vulnerabilidades abertas por criticidade. * Tempo médio de correção (MTTR). * Conformidade com SLAs. * Vulnerabilidades reincidentes.

Template de Relatório de Vulnerabilidade

Campo	Descrição
Título	Nome da vulnerabilidade (ex.: SQL Injection no /login)

Descrição	Resumo da falha e contexto em que ocorre
Impacto	Impacto técnico e de negócio
Evidência	Provas: prints, requests, outputs de scanner
Reprodução	Passos para reproduzir a vulnerabilidade
Severidade	Classificação baseada em CVSS v3.1
Recomendação	Como corrigir a falha
Referências	Links OWASP, CVE, guias de mitigação

A adoção de um fluxo estruturado de gestão de vulnerabilidades com DefectDojo permite maior visibilidade, priorização eficiente e controle sobre os riscos de segurança. Além disso, a padronização de relatórios garante melhor comunicação com áreas técnicas e executivas, promovendo a maturidade da segurança da informação na organização.