GVT - GERENCIAMENTO DE VULNERABILIDADE TÉCNICA

LGPD

v.2.0 | *Revisão* 2025

A.S
ALMEIDA SANTOS
ADVOGADOS

POP – Procedimento Operacional Padrão					
Equipe: 17 TECNOLOGIA DA INFORMAÇÃO					
Atividade: GVT - Gerenciamento de Vulnerabilidade Técnica					
Elaborado por:	**Aprovado por:**	**Publicado em:**	**Prox. revisão:**	**Ciclo:**	**ID:**
SJV	JR	21/08/2021	21/08/2025	Anual	17.03
Nome do arquivo: 17.03_GVT - Gerenciamento De Vulnerabilidades Técnicas.Docx					

Sumário

POP – Procedimento Operacional Padrão					
Equipe: 17 TECNOLOGIA DA INFORMAÇÃO					
Atividade: GVT - Gerenciamento de Vulnerabilidade Técnica					
Elaborado por:	**Aprovado por:**	**Publicado em:**	**Prox. revisão:**	**Ciclo:**	**ID:**
SJV	JR	21/08/2021	21/08/2025	Anual	17.03
Nome do arquivo: 17.03_GVT - Gerenciamento De Vulnerabilidades Técnicas.Docx					

Objetivo

O Processo de Gerenciamento de Vulnerabilidades Técnicas (PGVT) tem por finalidade identificar e remediar, periodicamente e sistematicamente, as vulnerabilidades técnicas em redes e sistemas de informações da Almeida Santos Advogados.

Campo de Aplicação

Segurança da Tecnologia da Informação

Definições

Scan: Processo de execução de varredura em busca por vulnerabilidade

Rescan: repetição de um Scan com as mesmas características e configurações de varredura de um Scan

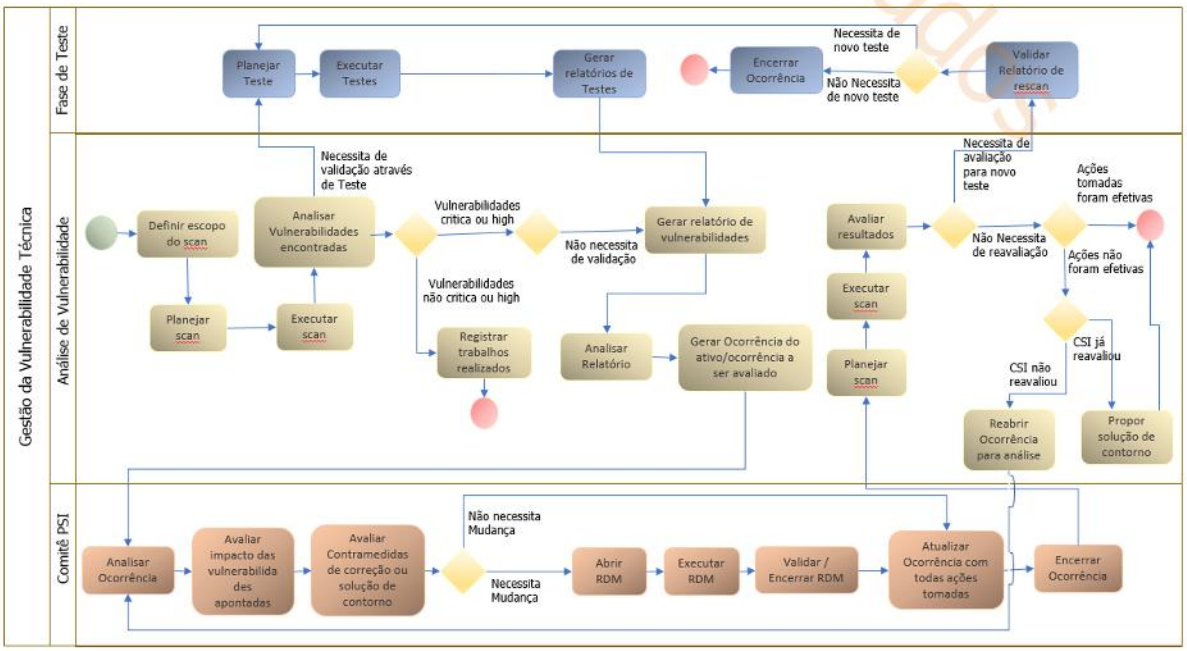
Ciclos de Scans: ciclo de averiguação por vulnerabilidades que tem início com um SCAN e finaliza, após execução de um ou mais RESCANS, com a validação de mitigação de riscos associados a vulnerabilidades do tipo Alto, Médio ou Baixo e sua quantidade para cada categoria.

Regras e Diretrizes

- O processo deverá seguir as normas e padrões estabelecidas, testadas e documentadas.
- O processo será baseado na Documentação de Boas Práticas de Gerenciamento e Riscos.
- Modelo de Maturidade a ser utilizado: Gestão de Vulnerabilidade

Processo: Averiguação e Tratamento de Vulnerabilidades

Fluxo do Processo



POP – Procedimento Operacional Padrão					
Equipe: 17 TECNOLOGIA DA INFORMAÇÃO					
Atividade: GVT - Gerenciamento de Vulnerabilidade Técnica					
Elaborado por:	**Aprovado por:**	**Publicado em:**	**Prox. revisão:**	**Ciclo:**	**ID:**
SJV	JR	21/08/2021	21/08/2025	Anual	17.03
Nome do arquivo: 17.03_GVT - Gerenciamento De Vulnerabilidades Técnicas.Docx					

Descrição do Processo

Atividade	Descrição da Atividade
Definir escopo da análise	O escopo estabelece quais ativos de TI entrarão no Ciclo de Scan. Atualmente, utilizamos como escopo dos ativos um range de ips ativos agrupado por grupo de máquinas (Servidores, Desktop, Notebook).
Planejar SCAN Greenbone Security Assistant OPENVAS	Uma vez definido o escopo de ativos de TI a serem varridos, o Scan é programado no OpenVAS, para iniciar o ciclo de Scan. O Scan é configurado da seguinte forma: • Nome do SCAN: Composto por "SCAN-" + "IP Público"; • Política de SCAN (Scan Polícy): A política a ser utilizada para Scan baseado em ciclo será o "Scan básico de rede"; • Alvos: IP ou conjunto de IPS de acordo com seu grau de importância e riscos.
Agendar SCAN	A janela de manutenção definida para execução de Scan é a 3ª quarta-feira de cada mês e já fica agendado para execução automática pelo OpenVAS.
Executar SCAN	Ao chegar o dia de execução do Scan, o OpenVAS executa a varredura conforme os parâmetros definidos.
Analisar vulnerabilidades descobertas	Após a execução de um scan (ou rescan), uma análise prévia deve ser feita pelo técnico responsável pela varredura com o propósito de identificar o nível de risco associado às vulnerabilidades encontradas. Nessa análise de risco deve-se considerar o seguinte critério: • Deve ser tratado todas as vulnerabilidades marcadas como "Crítica" e/ou "High"; • Poderá ser avaliado outros requisitos para considerar um nível menor para certos riscos categorizados como "Crítica" e/ou "High", como falso-positivo ou falso-negativo.
Abrir ocorrência para o grupo CSI	Para cada ciclo de SCAN deve ser criado uma (e somente uma) ocorrência no sistema Help Desk da empresa para sua tratativa. Nessa ocorrência deve constar o relatório (em PDF) constando somente as vulnerabilidades de nível CríticaL, High e Medium, onde só serão tratadas as duas primeiras.
Atender ocorrência	A ocorrência é atendida inicialmente pelos Técnicos de TI que reportará ao Comitê CSI para que juntos apliquem a solução de mitigação apontada no relatório (campo "solution").
Avaliar impacto da vulnerabilidade	O Técnico que iniciou a tratativa da ocorrência, deve: • Avaliar a prioridade de correção ou aplicação de solução da vulnerabilidade com base no impacto que a mesma poderá causar se for explorada por uma ameaça; • Avaliar se a vulnerabilidade encontrada é falso-positivo onde, neste caso, deverá notificar (via e-mail o Comitê CSI) e registrar as medidas tomadas.

	• Avaliar o custo-benefício da aplicação da solução para a vulnerabilidade encontrada, apontando, se for o caso, uma justificativa para a inviabilidade técnica ou de custo.
Abrir RDM – Requisição de Mudança	Independente do tipo da solução (correção, atualização de SO, aplicação de patch, etc), uma RDM deverá ser associado e o processo de mudança deverá ser formalmente seguido.
Executar RDM	De acordo com os requisitos definido na mudança, a solução apontada no relatório de vulnerabilidades deve ser aplicada, com as regras de roll back em caso de falhas.
Validar/Encerrar RDM	A solução aplicada é testada e validada.
Atualizar informações de tratativa na ocorrência	Após encerrar a mudança, o técnico responsável pelo atendimento da ocorrência juntamente a um mebro da equipe do Comitê de CSI, registra na demanda as ações tomadas para aplicação da solução.
Planejar RESCAN	A Equipe de TI é notificada das correções e/ou aplicação da solução. Com isso, é executado novo Scan (rescan) com as mesmas características configuradas para o Scan inicial.
Executar RESCAN	O Rescan é executado.
Validar Ocorrência	A ocorrência só será validada e finalizada, e o ciclo de Scan considerado encerrado, quando: • O Rescan apontar redução ou mitigação do nível de risco das vulnerabilidades do tipo Crítica e/ou High; • Ser informado que as vulnerabilidades Crítica e/ou High são falsos-positivos onde, neste caso, deverá ser validado pela equipe de TI; • Ser informado que a aplicação de solução nas vulnerabilidades Crítica e/ou High são inviáveis tecnicamente ou financeiramente, tornando mais custoso tratar a vulnerabilidade que encontrar outras ações de mitigação apontadas no relatório ou aceite do risco. Tal situação só será validada pelos membros do Comitê CSI. Obs.: Um ciclo de Scan não termina com um Rescan, necessariamente. Enquanto houver vulnerabilidades do tipo Crítica e/ou High, um rescan deverá ser executado até não as encontrar mais.
Reabrir ocorrência	Uma ocorrência deve ser devolvida para o Comitê CSI, quando: • Forem encontradas vulnerabilidades Crítica e/ou High não tratadas após execução do Rescan; • Forem encontradas vulnerabilidades Crítica e/ou High que embora tratadas, não foram mitigadas pela solução proposta, após execução do Rescan; • Forem negadas as solicitações de recategorização do risco; • Forem negadas as justificativas de aceite de risco.

Avaliar relatório de RESCAN	O grupo do Comitê CSI deverá avaliar o relatório de Rescan comparando com o relatório de Scan com o objetivo de identificar alternativas de solução para mitigação do risco inerente às vulnerabilidades e/ou identificar àquelas soluções aplicadas que não surtiram efeito.

Matriz Raci

Atividades	Gestor TI	Analista	Comitê CSI
Definir escopo da análise	A	R	C
Planejar SCAN	A	R	C
Agendar SCAN	A	R	I
Executar SCAN	A	R	I
Analisar vulnerabilidades descobertas	A	R	C
Abrir ocorrência para Comitê CSI	R	I	C
Atender ocorrência	A	R	I
Avaliar impacto da vulnerabilidade	R	R	R
Abrir RDM	R	R	I
Executar RDM	R	R	I
Validar/Encerrar RDM	R	R	I
Atualizar informações de tratativa no ocorrência	R	R	I
Planejar RESCAN	A	R	I
Executar RESCAN	A	R	I
Validar ocorrência	A	R	I
Reabrir ocorrência para Comitê CSI	R	R	R
Avaliar relatório de RESCAN	R	R	I

LEGENDA: (*Responsible* | *Accountable* | *Consulted* | *Informed* = R - Responsável | A - Prestador de Contas | C - Consultado | I - Informado)

Scan Report – (OpenVas)

June 26, 2023

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Pentest - Mensal". The scan started at Sat Jun 24 21:01:28 2023 UTC and ended at Sat Jun 24 21:03:40 2023 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
Total: 0	0	0	0	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

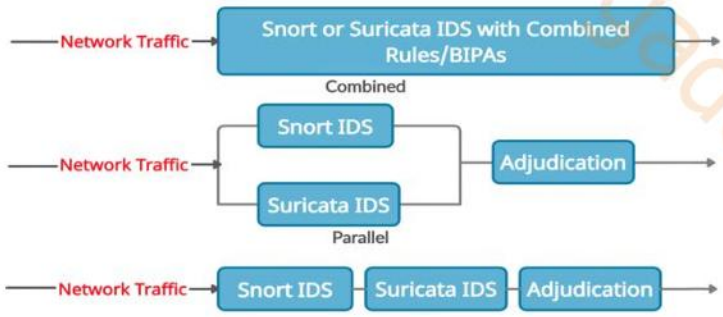
This report contains 0 results. Before filtering there were 0 results.

2 Results per Host

This file was automatically generated.

PFSense - Suricata (snort)

Arquivos de LOGS SIEM armazenados



Controle de Atualização

Versão	Data	Alterações
01	21/08/2021	Versão Inicial
02	21/08/2025	Versão Final