



# Módulo 23: Avaliação de vulnerabilidade de endpoint



CyberOps Associate v1.0

Prof. Clemilson Oliveira

[clemilson.oliveira@edu.sc.senai.br](mailto:clemilson.oliveira@edu.sc.senai.br)



# Objetivos do módulo

**Título do módulo:** Avaliação de vulnerabilidade de endpoint

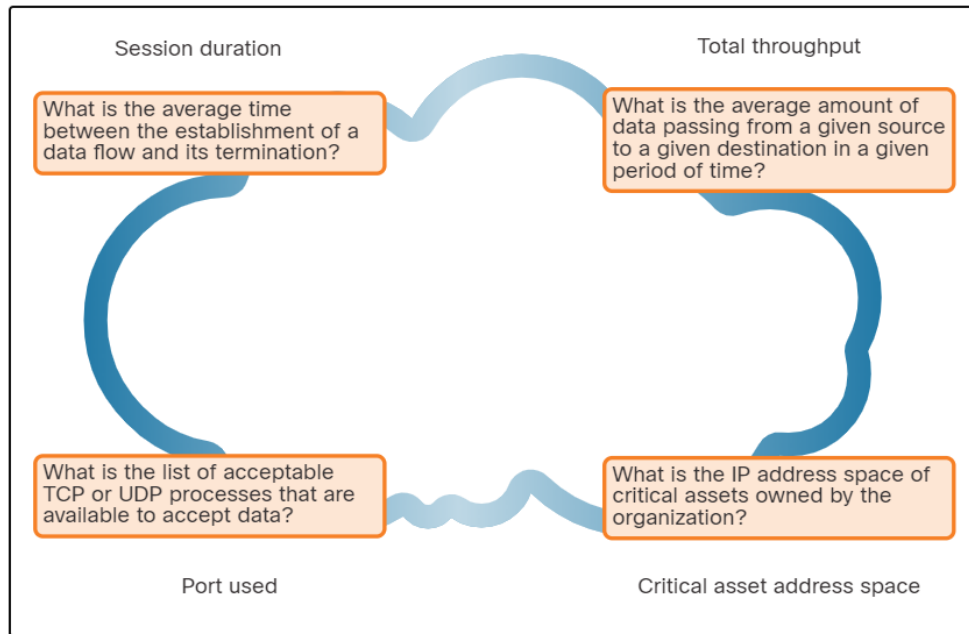
**Objetivo do módulo:** Explicar como as vulnerabilidades do endpoint são avaliadas e gerenciadas.

Título do Tópico	Objetivo do Tópico
Perfil de rede e servidor	Explicar o valor do perfil de rede e servidor.
Sistema de pontuação de vulnerabilidade comum (CVSS)	Explicar como os relatórios de CVSS são usados para descrever as vulnerabilidades de segurança.
Gerenciamento seguro de dispositivos	Explicar como as técnicas de gerenciamento de dispositivo seguro são usadas para proteger dados e ativos.
Sistemas de Gestão de Segurança da Informação	Explicar como os sistemas de gerenciamento de segurança da informação são usados para proteger os ativos.

# 23.1 Perfil de rede e servidor

## Criação de perfil de rede e servidor

- O perfil de rede e dispositivo fornece informações estatísticas de linha de base que podem servir como um ponto de referência para o desempenho normal da rede e do dispositivo.
- Elementos do perfil de rede:
  - Duração da sessão
  - Rendimento total
  - Espaço de endereço de ativo crítico
  - Tipo de tráfego típico



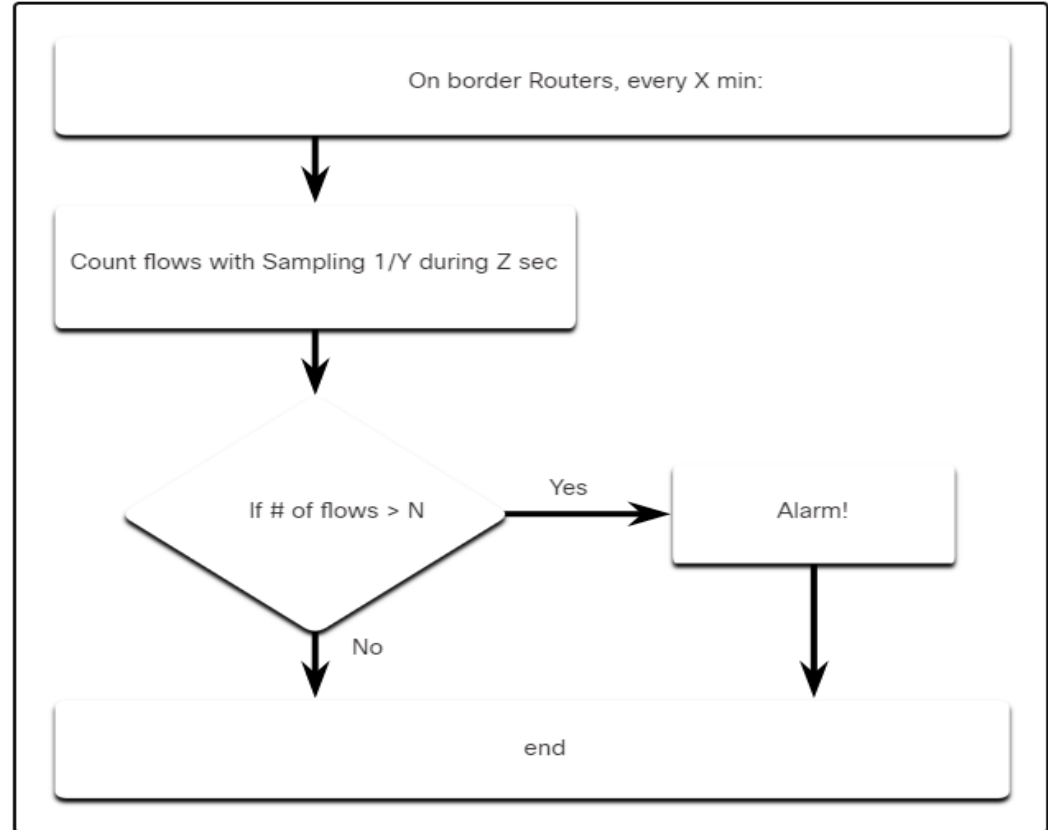
### Elementos de um Perfil de Rede

# Criação de perfil do servidor de criação de perfil de rede eservidor

- Um perfil de servidor é uma linha de base de segurança para um determinado servidor.
- A definição de perfil do servidor é usada para estabelecer o estado operacional aceito dos servidores.
- Os elementos de perfil do servidor são os seguintes:
  - Portas de escuta
  - Usuários e contas logadas
  - Contas de serviço
  - Ambiente de software

# Detecção de anomalias de rede e criação de perfis de rede

- O comportamento da rede é descrito por uma grande quantidade de dados diversos, como os recursos do fluxo de pacotes, os recursos dos próprios pacotes e a telemetria de várias fontes.
- As técnicas de análise de Big Data podem ser usadas para analisar esses dados e detectar variações a partir da linha de base.
- A detecção de anomalias pode identificar hosts infectados na rede que estão verificando outros hosts vulneráveis.
- A figura ilustra uma versão simplificada de um algoritmo projetado para detectar uma condição incomum nos roteadores de fronteira de uma empresa.



# Teste de Vulnerabilidade de Rede e Criação de Perfil de Servidor

- Os testes de vulnerabilidade de rede incluem análise de risco, avaliação de vulnerabilidades e testes de penetração.
- A tabela lista exemplos de atividades e ferramentas que são usadas em testes de vulnerabilidade:

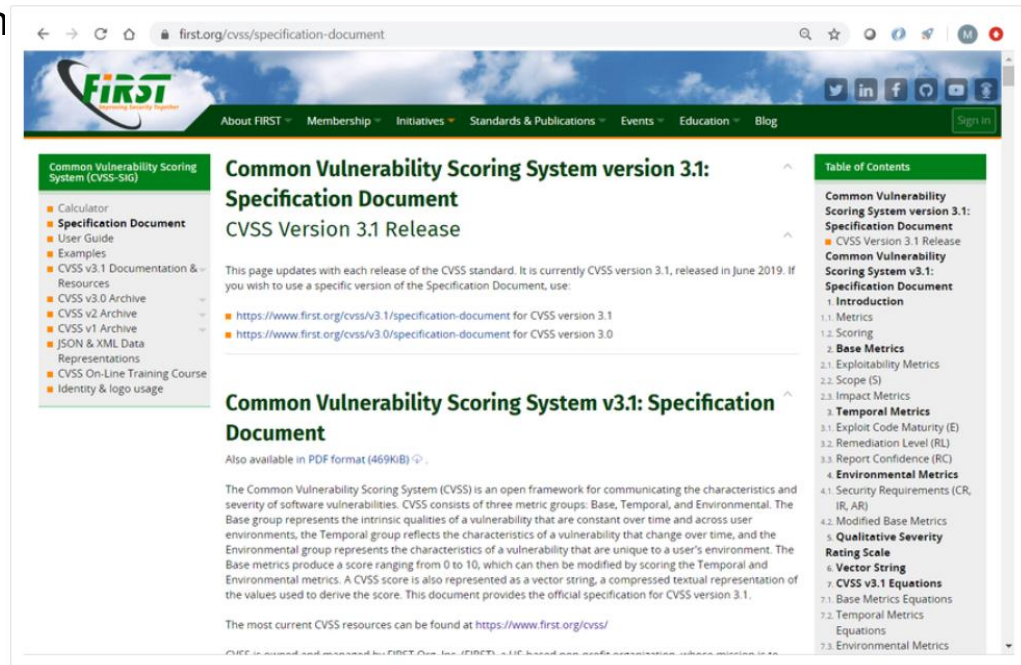
Atividade de	Descrição	Ferramentas
<b>Análise de risco</b>	Indivíduos realizam uma análise abrangente dos impactos dos ataques nos ativos principais da empresa e no funcionamento	Consultores internos ou externos, quadros de gestão de riscos
<b>Avaliação de vulnerabilidade</b>	Gerenciamento de patches, varreduras de host, varredura de portas, outras verificações de vulnerabilidade e serviços	OpenVAS, Analisador de Linha de Base da Microsoft, Nessus, Qualys, Nmap
<b>Teste de penetração</b>	Uso de técnicas e ferramentas de hacking para penetrar nas defesas da rede e identificar a profundidade de penetração potencial	Metasploit, CORE impact, hackers éticos

# 23.2 Common Vulnerability Scoring System (CVSS)



## Visão geral do CVSS

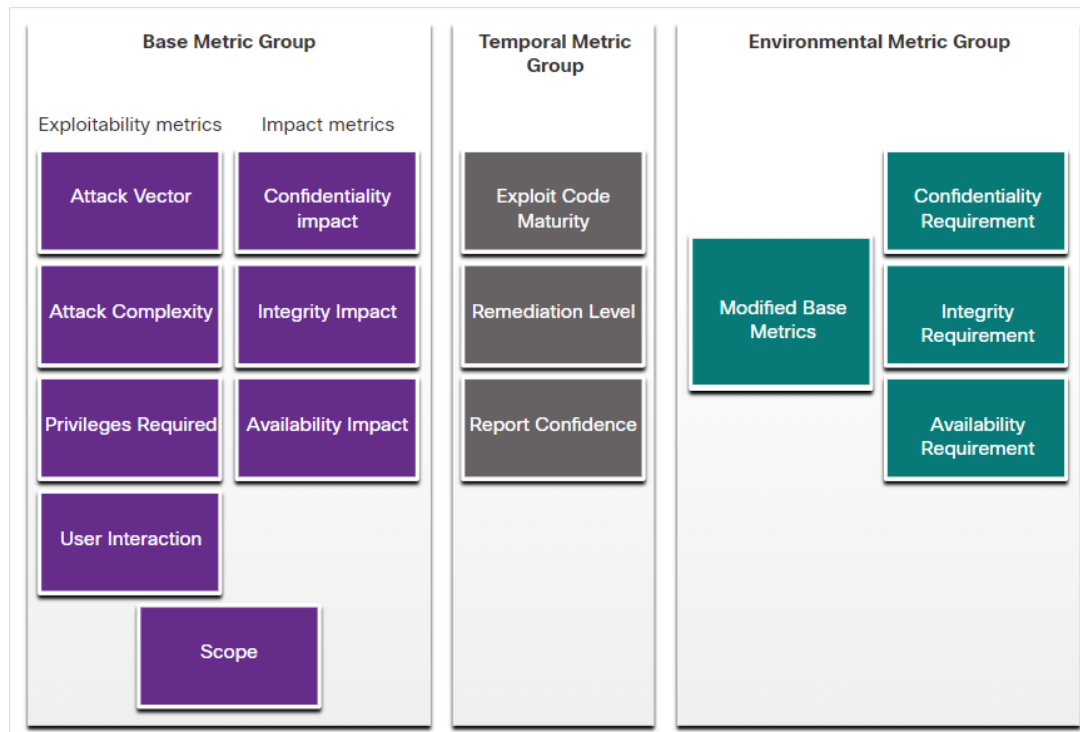
- O Common Vulnerability Scoring System (CVSS) é uma ferramenta de avaliação de risco projetada para transmitir os atributos comuns e a gravidade das vulnerabilidades em sistemas de hardware e software de computador.
- O CVSS fornece pontuações padronizadas de vulnerabilidade.
- Ele fornece uma estrutura aberta com métricas para todos os usuários.
- O CVSS ajuda a priorizar o risco.
- O Fórum de Equipes de Resposta a Incidentes e Segurança (FIRST) foi designado como guardião do CVSS para promover sua adoção globalmente.



The screenshot shows the official website for the Common Vulnerability Scoring System (CVSS) version 3.1. The page is titled "Common Vulnerability Scoring System version 3.1: Specification Document" and "CVSS Version 3.1 Release". It includes a navigation menu with links to "About FIRST", "Membership", "Initiatives", "Standards & Publications", "Events", "Education", and "Blog". A sidebar on the left lists various resources like "Calculator", "Specification Document", "User Guide", "Examples", and "CVSS v3.1 Documentation & Resources". The main content area explains that the page updates with each release of the CVSS standard, currently version 3.1, released in June 2019. It provides links to the specification document for CVSS version 3.1 and CVSS version 3.0. A section titled "Common Vulnerability Scoring System v3.1: Specification Document" states that the CVSS is an open framework for communicating the characteristics and severity of software vulnerabilities, consisting of three metric groups: Base, Temporal, and Environmental. It also mentions that the CVSS score is represented as a vector string. A table of contents on the right lists the sections: Introduction, Metrics, Scoring, Base Metrics, Exploitability Metrics, Scope (S), Impact Metrics, Temporal Metrics, Exploit Code Maturity (E), Remediation Level (RL), Report Confidence (RC), Environmental Metrics, Security Requirements (CR, IR, AR), Modified Base Metrics, Qualitative Severity Rating Scale, Vector String, CVSS v3.1 Equations, Base Metrics Equations, Temporal Metrics Equations, and Environmental Metrics.

## Grupos métricos CVSS

- O CVSS utiliza três grupos de métricas para avaliar a vulnerabilidade.
- **Grupo de Métricas Base:** Representa as características de uma vulnerabilidade que são constantes ao longo do tempo e em contextos.
- **Grupo de métricas temporais:** mede as características de uma vulnerabilidade que pode mudar ao longo do tempo, mas não em ambientes de usuário.
- **Grupo de métricas ambientais:** mede os aspectos de uma vulnerabilidade que estão enraizados no ambiente de uma organização específica.



## Grupo Métrico Base CVSS

- As métricas de Exploração do Grupo de Métricas Base incluem os seguintes critérios:
  - Vetor de ataque
  - A complexidade do ataque
  - Privilégios necessários
  - Interação do usuário
  - Examinar
- Os componentes de métricas de Impacto do Grupo Métrico Base incluem os seguintes critérios:
  - Impacto de Confidencialidade
  - Impacto da integridade
  - Impacto da disponibilidade



## O Processo CVSS

- O processo CVSS usa uma ferramenta chamada Calculadora CVSS v3.1.
- A calculadora é como um questionário no qual são feitas as escolhas que descrevem a vulnerabilidade para cada grupo de métricas.
- Posteriormente, uma pontuação é gerada e a classificação de gravidade numérica é exibida.

The screenshot displays the CVSS v3.1 calculator interface. At the top right, a yellow box shows the **Base Score** as **3.8 (Low)**. Below this, the calculator is organized into two columns of metrics, each with a title and a set of buttons for selection.

**Left Column Metrics:**

- Attack Vector (AV):** Network (N) [selected], Adjacent (A), Local (L), Physical (P)
- Attack Complexity (AC):** Low (L) [selected], High (H)
- Privileges Required (PR):** None (N), Low (L), High (H) [selected]
- User Interaction (UI):** None (N) [selected], Required (R)

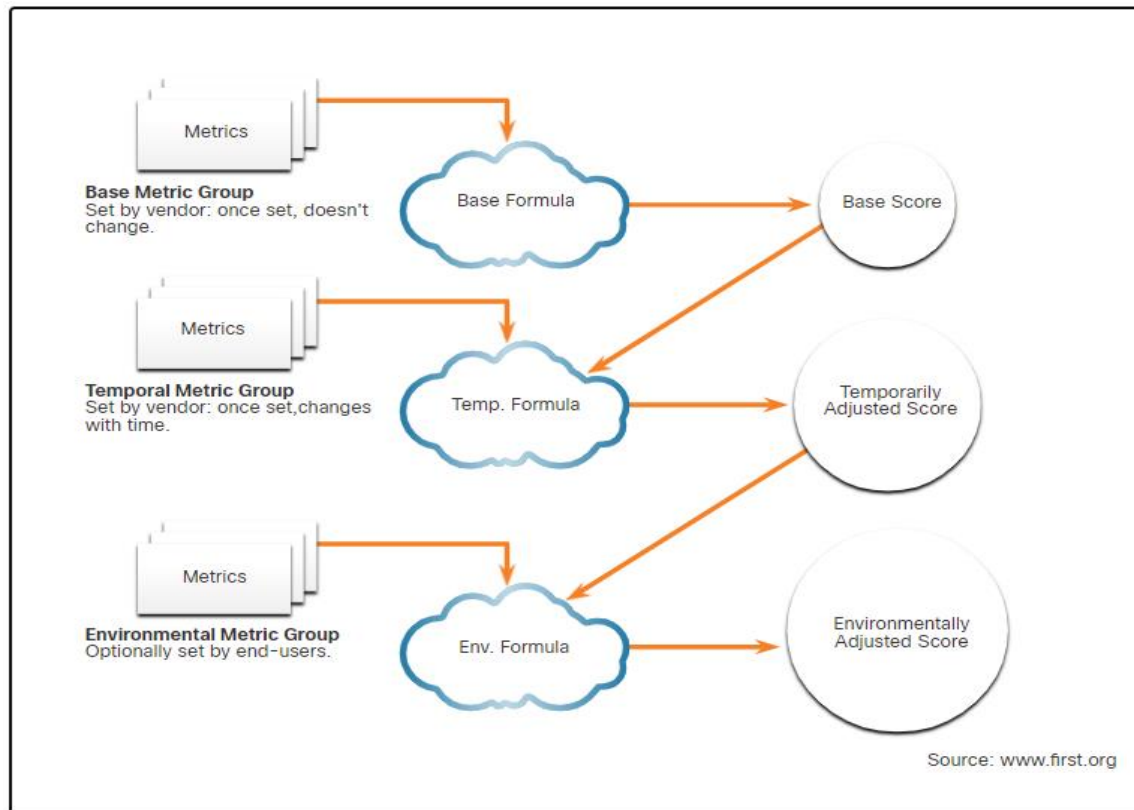
**Right Column Metrics:**

- Scope (S):** Unchanged (U) [selected], Changed (C)
- Confidentiality (C):** None (N), Low (L) [selected], High (H)
- Integrity (I):** None (N), Low (L) [selected], High (H)
- Availability (A):** None (N) [selected], Low (L), High (H)

At the bottom, a green bar displays the **Vector String**: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N

## Processo CVSS (Cond.)

- Após a conclusão do grupo Métrica Base, os valores de métrica Temporal e Ambiental modificam os resultados da Métrica Base para fornecer uma pontuação geral.



# Relatórios CVSS

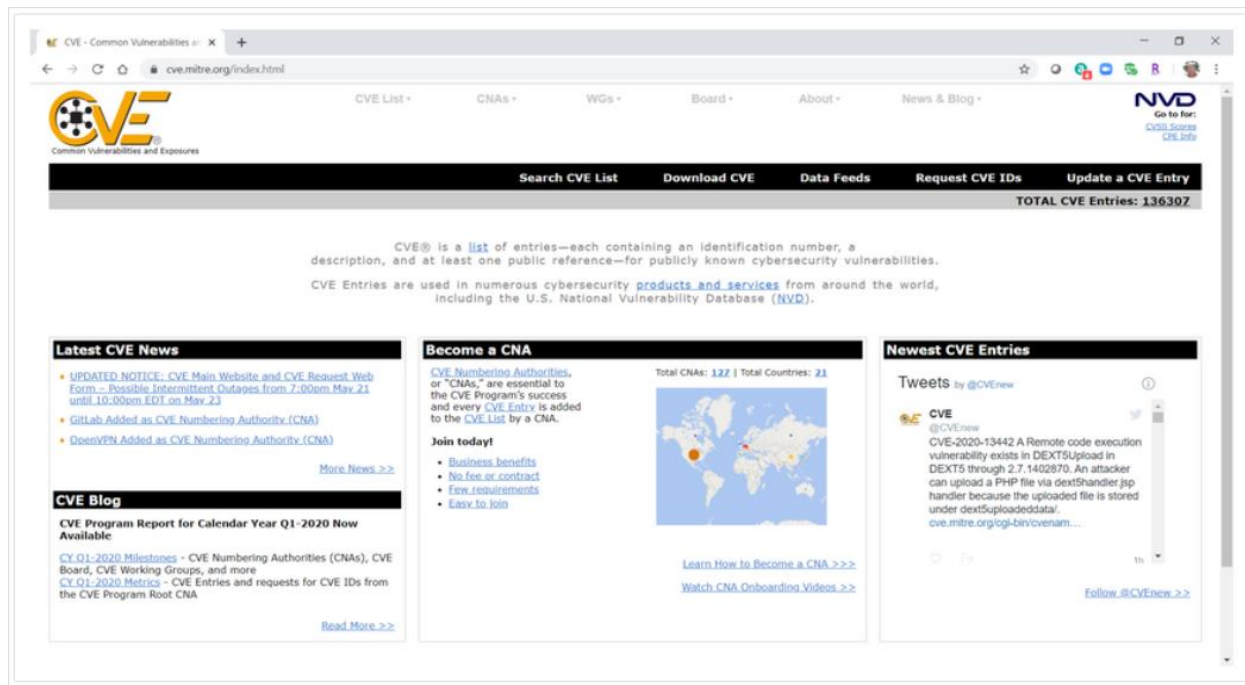
- Quanto maior a classificação de gravidade, maior o impacto potencial de uma exploração e maior a urgência em abordar a vulnerabilidade.
- Qualquer vulnerabilidade que exceda 3.9 deve ser resolvida.
- Os intervalos de escores e o significado qualitativo correspondente são mostrados na tabela:

Classificação	Pontuação CVSS
Nenhum	0
Baixa	0.1 – 3.9
Médio	4.0 – 6.9
Alto	7.0 – 8.9
Críticos	9.0 – 10.0

## Outras fontes de informações sobre vulnerabilidades

### Common Vulnerabilities and Exposures (CVE):

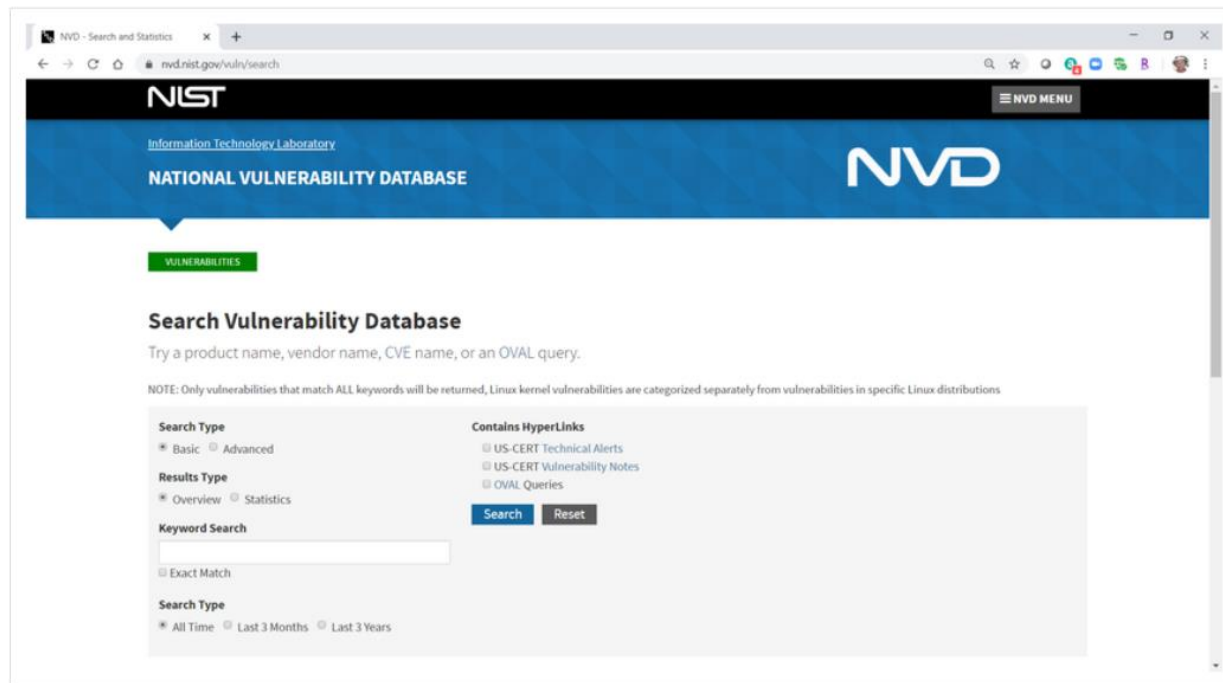
- O identificador CVE fornece uma maneira padrão de pesquisar uma referência a vulnerabilidades.
- Os serviços de inteligência contra ameaças usam identificadores CVE e aparecem em vários logs do sistema de segurança.
- O site CVE Details fornece uma ligação entre as pontuações do CVSS e as informações do CVE.



# Outras Fontes de Informações sobre Vulnerabilidade (Contd.)

## National Vulnerability Database (NVD):

- Isso utiliza identificadores CVE e fornece informações adicionais sobre vulnerabilidades, como pontuações de ameaças CVSS, detalhes técnicos, entidades afetadas e recursos para investigação adicional.
- O banco de dados foi criado e é mantido pela agência do National Institute of Standards and Technology (NIST) do governo dos EUA.

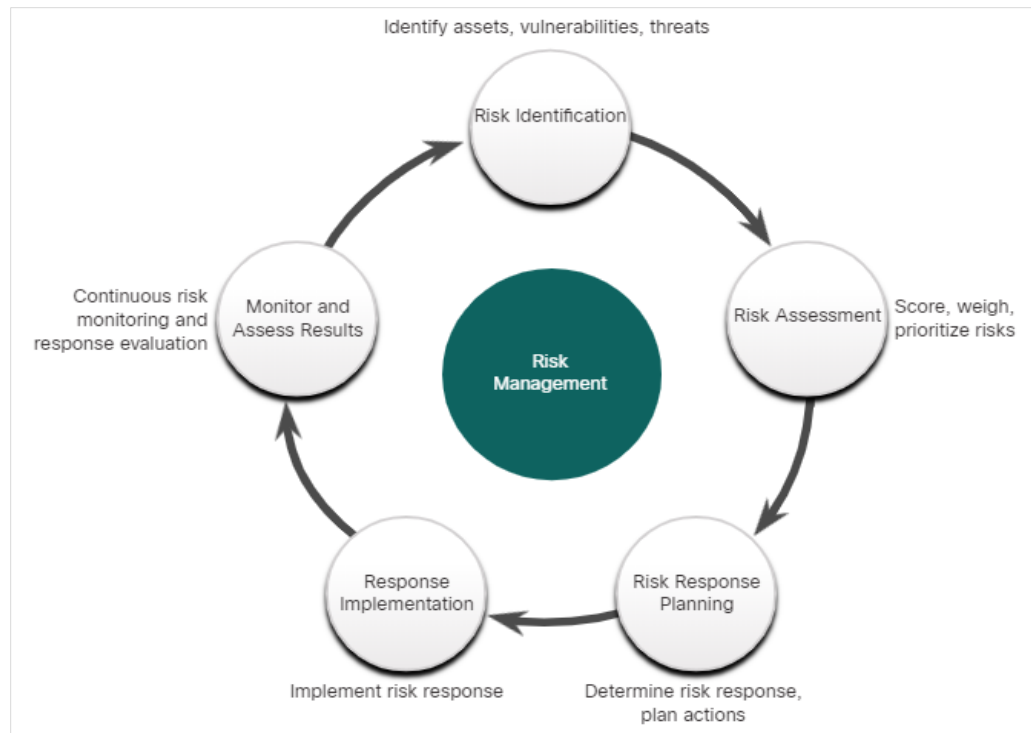




# 23.3 Gerenciamento de dispositivo seguro

# Gerenciamento de risco

- O gerenciamento de riscos envolve a seleção e especificação de controles de segurança para uma organização.
- Uma atividade obrigatória na avaliação de riscos é identificar ameaças e vulnerabilidades.
- Formas de responder aos riscos identificados:
  - **Prevenção de riscos** - Parar de realizar as atividades que criam risco.
  - **Redução de riscos** - Tomar medidas para reduzir a vulnerabilidade.
  - **Partilha de riscos** - Deslocar algum risco para outras partes.
  - **Retenção de riscos** - Aceite o risco e suas consequências.



# Gerenciamento de vulnerabilidades

- O gerenciamento de vulnerabilidades é uma prática de segurança projetada para impedir proativamente a exploração de vulnerabilidades de TI.
- As etapas do Ciclo de Vida do Gerenciamento de Vulnerabilidades:
  - **Descobrir** - Desenvolva uma linha de base de rede. Identifique vulnerabilidades de segurança em um agendamento automatizado regular.
  - **Priorizar ativos** - Categorize os ativos em grupos ou unidades de negócios e atribua um valor comercial com base na sua importância às operações de negócios.
  - **Avaliar** - Determinar um perfil de risco básico para eliminar riscos com base na importância, vulnerabilidade, ameaças e classificação de ativos.



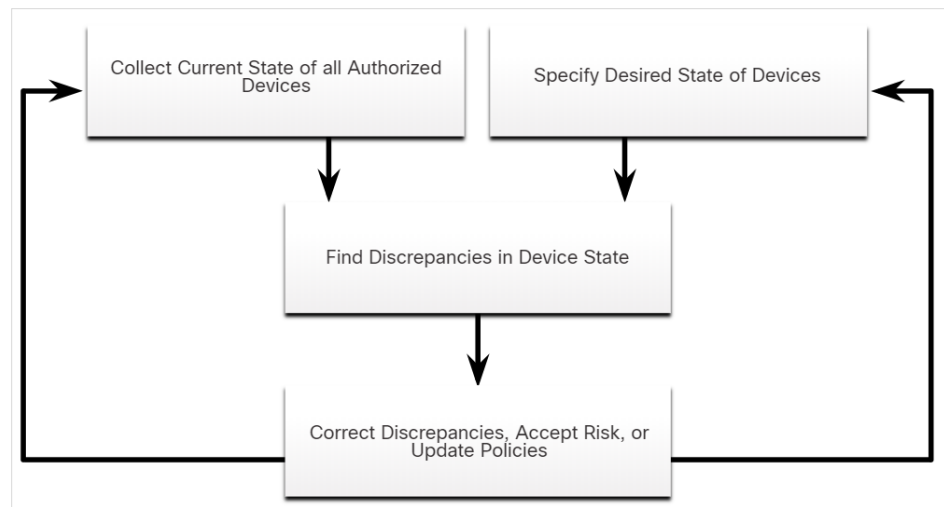
## Gestão de Vulnerabilidade (Cont.)

- **Relatório**- Meça o nível de risco comercial associado aos seus ativos de acordo com suas políticas de segurança. Documente um plano de segurança, monitore atividades suspeitas e descreva vulnerabilidades conhecidas.
- **Remediar** - Priorizar de acordo com o risco comercial e resolver vulnerabilidades em ordem de risco.
- **Verificar** - Verifique se as ameaças foram eliminadas por meio de auditorias de acompanhamento.



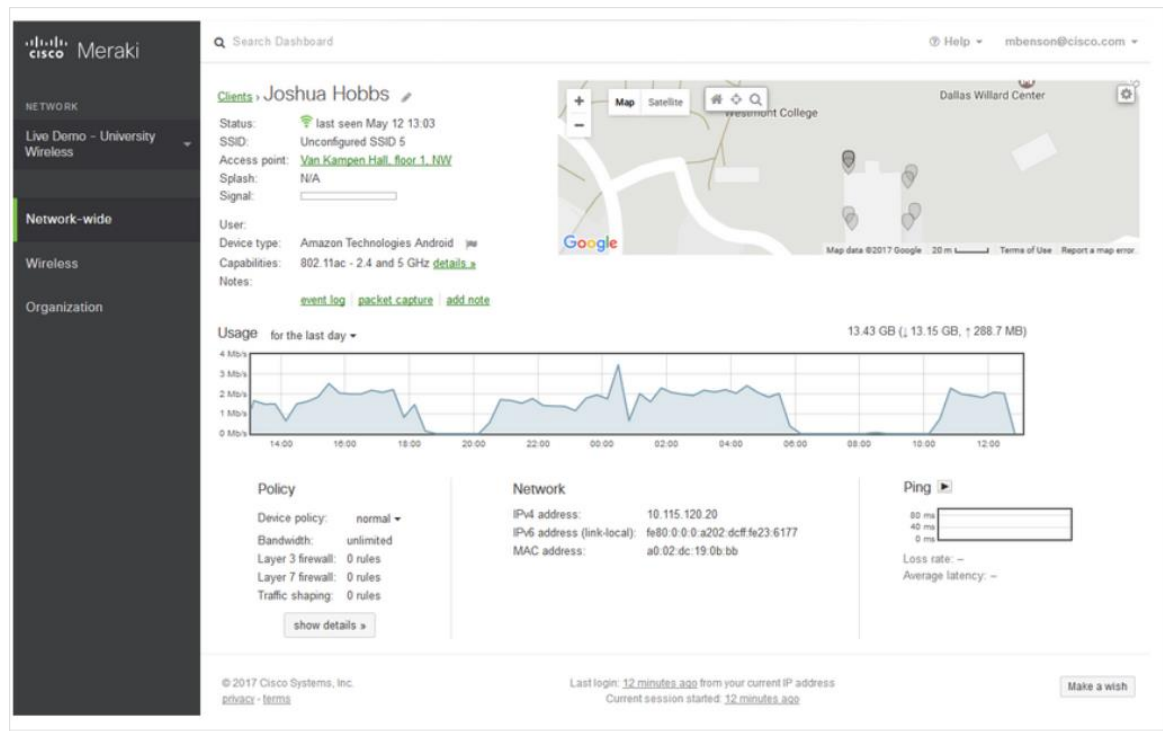
# Gerenciamento de ativos

- O gerenciamento de ativos envolve a implementação de sistemas que controlam a localização e a configuração de dispositivos e software em rede em uma empresa.
- **Ferramentas e técnicas para gerenciamento de ativos:**
  - Detecção automatizada e inventário do estado real dos dispositivos
  - Articulação do estado desejado para esses dispositivos usando políticas, planos e procedimentos no plano de segurança das informações da organização
  - Identificação de ativos autorizados não conformes
  - Remediação ou aceitação do estado do dispositivo, possível iteração da definição de estado desejado
  - Repita o processo em intervalos regulares ou contínuos



# Gerenciamento de dispositivos móveis (MDM)

- Os dispositivos móveis não podem ser controlados fisicamente nas instalações de uma organização.
- Os sistemas MDM, como o Cisco Meraki Systems Manager, permitem que o pessoal de segurança configure, monitore e atualize um conjunto muito diversificado de clientes móveis a partir da nuvem.



# Gerenciamento de configurações

- **Gerenciamento de configuração:** Conforme definido pelo NIST, gerenciamento de configuração:

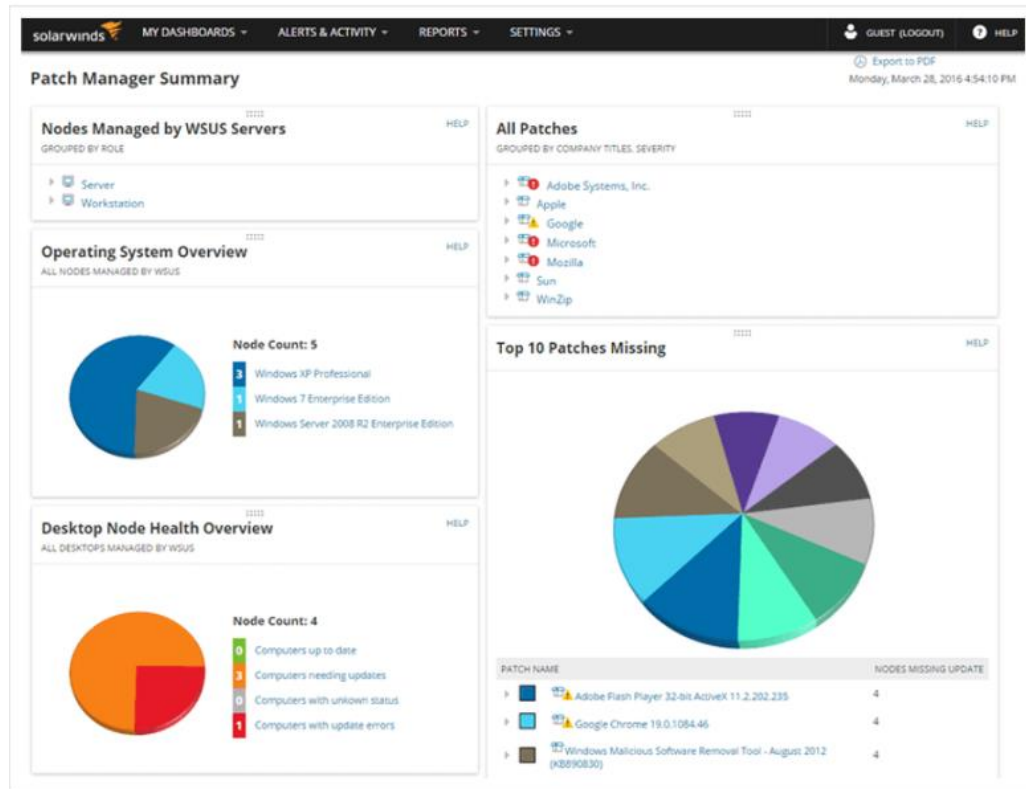
*Compreende uma coleção de atividades focadas no estabelecimento e manutenção da integridade de produtos e sistemas, através do controle dos processos de inicialização, mudança e monitoramento das configurações desses produtos e sistemas.*

- **Ferramentas de configuração :** Puppet, Chef, Ansible, and SaltStack

# Gerenciamento seguro de dispositivos

## Gerenciamento Corporativo de Patches

- O gerenciamento de patches envolve todos os aspectos da aplicação de patches de software, incluindo a identificação de patches necessários, aquisição, distribuição, instalação e verificação.
- O gerenciamento de patches é exigido por algumas regulamentações de conformidade, como Sarbanes Oxley (SOX) e a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA).

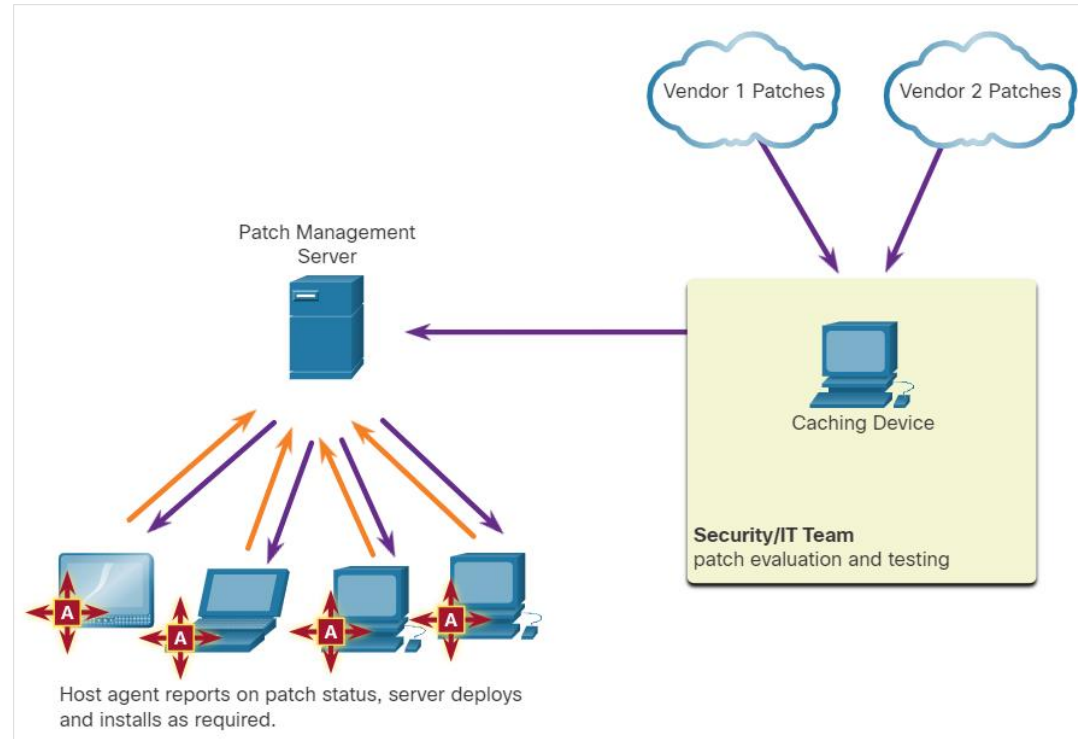




# Técnicas de gerenciamento de dispositivos

## Baseado em agente:

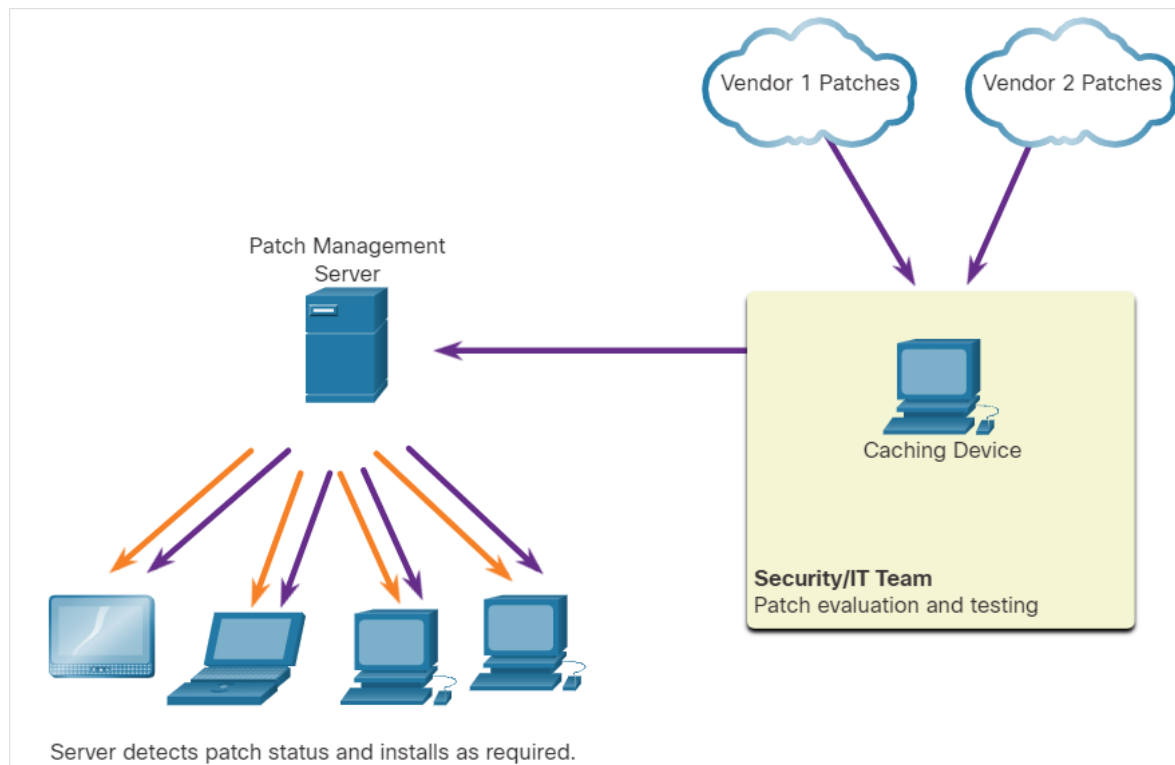
- Isso requer que um agente de software esteja sendo executado em cada host a ser corrigido.
- O agente informa se o software vulnerável está instalado no host.
- O agente se comunica com o servidor de gerenciamento de patches e determina se existem patches que exigem instalação e instala os patches.
- As abordagens baseadas em agentes são os meios preferidos para a aplicação de patches em dispositivos móveis.



# Técnicas de gerenciamento de patch

## Varredura sem agente:

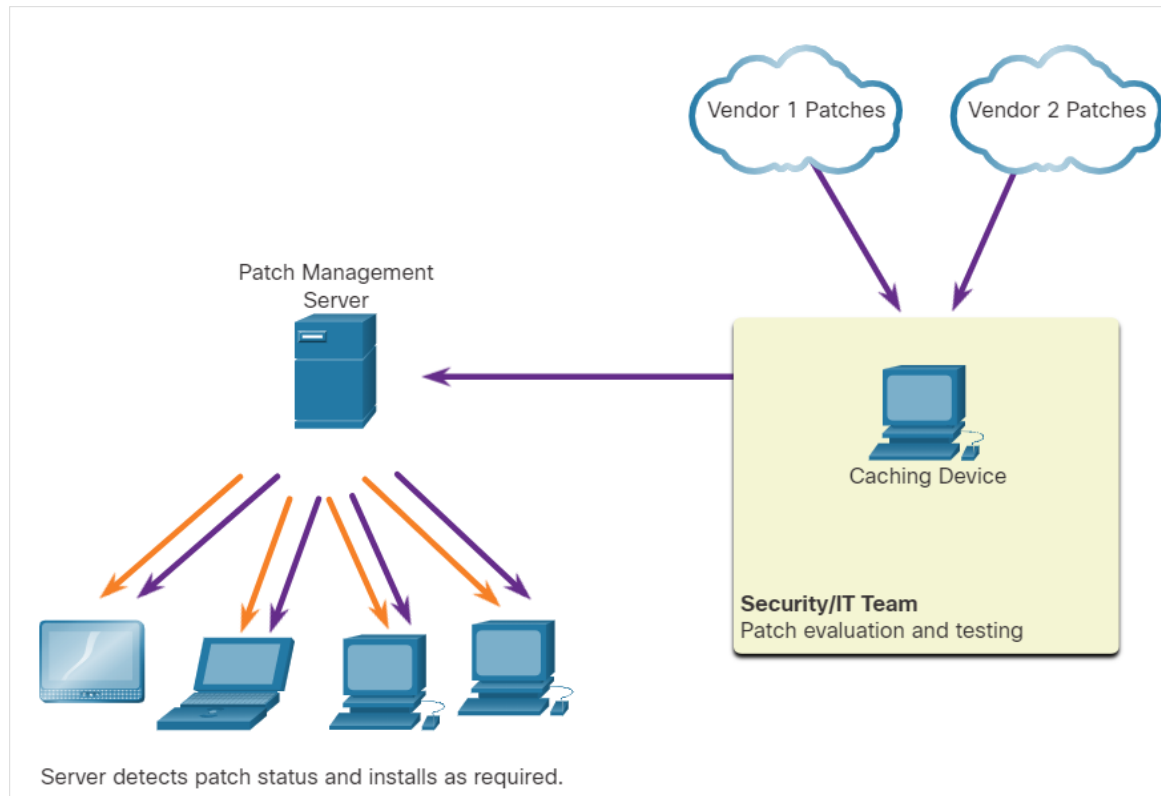
- Os servidores de gerenciamento de patches verificam a rede em busca de dispositivos que exigem patches.
- O servidor determina quais patches são necessários e instala esses patches nos clientes.
- Somente os dispositivos que estão em segmentos de rede digitalizados podem ser corrigidos, o que pode ser um problema para dispositivos móveis.



# Técnicas de gerenciamento de patch

## Monitoramento passivo de rede:

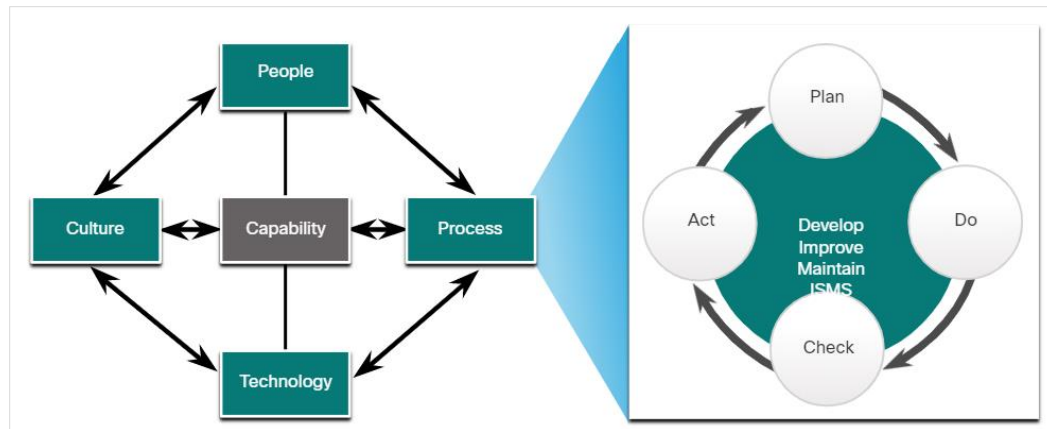
- Os dispositivos que requerem aplicação de patches são identificados através do monitoramento do tráfego na rede.
- Essa abordagem só é eficaz para software que inclui informações de versão em seu tráfego de rede.



# 23.4 Sistemas de gerenciamento de segurança da informação

# Sistemas de gestão de segurança

- Um Sistema de Gerenciamento de Segurança da Informação (ISMS) consiste em uma estrutura de gerenciamento para identificar, analisar e lidar com riscos de segurança da informação.
- Os ISMSS fornecem modelos conceituais que orientam as organizações no planejamento, implementação, controle e avaliação de programas de segurança da informação.
- Ele incorpora o quadro PDCA (“plan-do-check-act”, Planejar, Fazer, Verificar, Agir), conhecido como o ciclo Deming.
- O ISM é visto como uma elaboração sobre o modelo de capacidade organizacional de Povo-Process-Tecnologia-Cultura

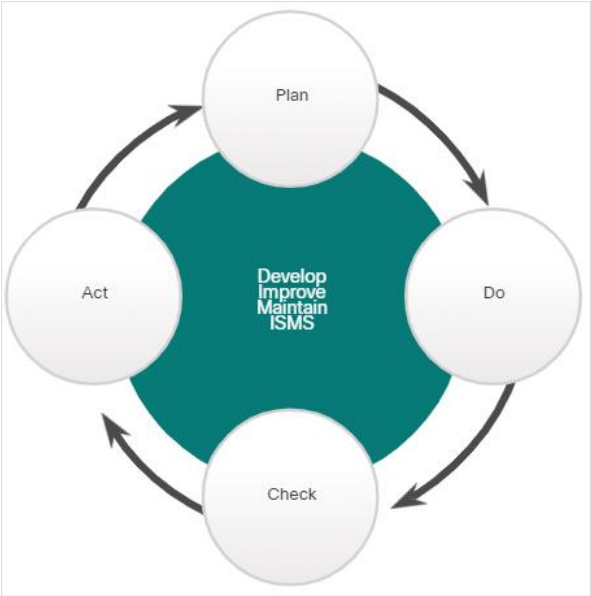


Um Modelo Geral para Capacidade Organizacional

# ISO-27001

- ISO/IEC 27000 família de padrões — padrões internacionalmente aceitos que facilitam negócios realizados entre países. A ISO 27001 - especificação global, em toda a indústria para um ISMS.

Planejar	Certo	Verificar	Aja
<ul style="list-style-type: none"><li>• Entenda os objetivos de negócios</li><li>• Definir escopode atividades</li><li>• Acesse e gerencie o suporte</li><li>• Avaliar e definir o risco</li><li>• Realizar gerenciamento de ativos e avaliação de vulnerabilidades</li></ul>	<ul style="list-style-type: none"><li>• Criar e implementar um plano de gestão de riscos</li><li>• Estabelecer e aplicar políticas e procedimentos de gestão de riscos</li><li>• Treinar pessoal, alocar recursos</li></ul>	<ul style="list-style-type: none"><li>• Monitorar a execução</li><li>• Compilar relatórios</li><li>• Suporte a auditoria externa de certificação</li></ul>	<ul style="list-style-type: none"><li>• Auditoria contínua de processos</li><li>• Melhorar continuamente os processos</li><li>• Tomar medidas corretivas</li><li>• Tomar medidas preventivas</li></ul>



# NIST Cybersecurity Framework

- **NIST Cybersecurity Framework** — é um conjunto de padrões projetados para integrar padrões, diretrizes e práticas existentes para ajudar a gerenciar e reduzir melhor o risco de segurança cibernética.
- A tabela abaixo descreve as principais funções no NIST Cybersecurity Framework:

Função principal	Descrição
IDENTIFIQUE	Desenvolva um entendimento organizacional para gerenciar o risco de segurança cibernética para sistemas, ativos, dados e recursos.
PROTEJA	Desenvolver e implementar as salvaguardas adequadas para garantir a prestação de serviços de infraestrutura crítica.
DETECTE	Desenvolver e implementar as atividades apropriadas para identificar a ocorrência de um evento de segurança cibernética.
RESPONDA	Desenvolver e implementar as atividades apropriadas para agir em um evento de segurança cibernética detectado.
RECUPERE	Desenvolver e implementar as atividades apropriadas para manter planos de resiliência e restaurar quaisquer capacidades ou serviços que tenham sido prejudicados devido a um evento de segurança cibernética.

# 23.5 Resumo da avaliação das vulnerabilidades de endpoint



# Resumo da avaliação de vulnerabilidade de endpoint

- O perfil de rede e dispositivo fornece informações de linha de base estatísticas que podem servir como um ponto de referência para o desempenho normal da rede e do dispositivo.
- A segurança de rede pode ser avaliada usando uma variedade de ferramentas e serviços.
- A avaliação de vulnerabilidades usa software para verificar servidores voltados para a Internet e redes internas em busca de vários tipos de vulnerabilidades.
- O Common Vulnerability Scoring System (CVSS) é uma estrutura aberta de padrão do setor neutro para classificar os riscos de uma determinada vulnerabilidade usando uma variedade de métricas para calcular uma pontuação composta.
- As vulnerabilidades são classificadas de acordo com o vetor de ataque, a complexidade do ataque, os privilégios necessários, a interação do usuário e o escopo.
- O gerenciamento de riscos envolve a seleção e especificação de controles de segurança para uma organização.

## Resumo da avaliação de vulnerabilidade de endpoint (Cont.)

- O gerenciamento de vulnerabilidades é uma prática de segurança projetada para impedir proativamente a exploração de vulnerabilidades de TI existentes em uma organização.
- As organizações podem usar um Sistema de Gerenciamento de Segurança da Informação (ISM) para identificar, analisar e lidar com os riscos de segurança das informações.
- Os padrões para gerenciamento de riscos de segurança cibernética estão disponíveis na ISO e no NIST.
- O NIST também desenvolveu o Cybersecurity Framework, que é semelhante aos padrões ISO/IEC 27000.

