

Módulo 22: Proteção de endpoint



CyberOps Associate v1.0

Prof. Clemilson Oliveira

clemilson.oliveira@edu.sc.senai.br

Objetivos do módulo

Título do módulo: Proteção de endpoint

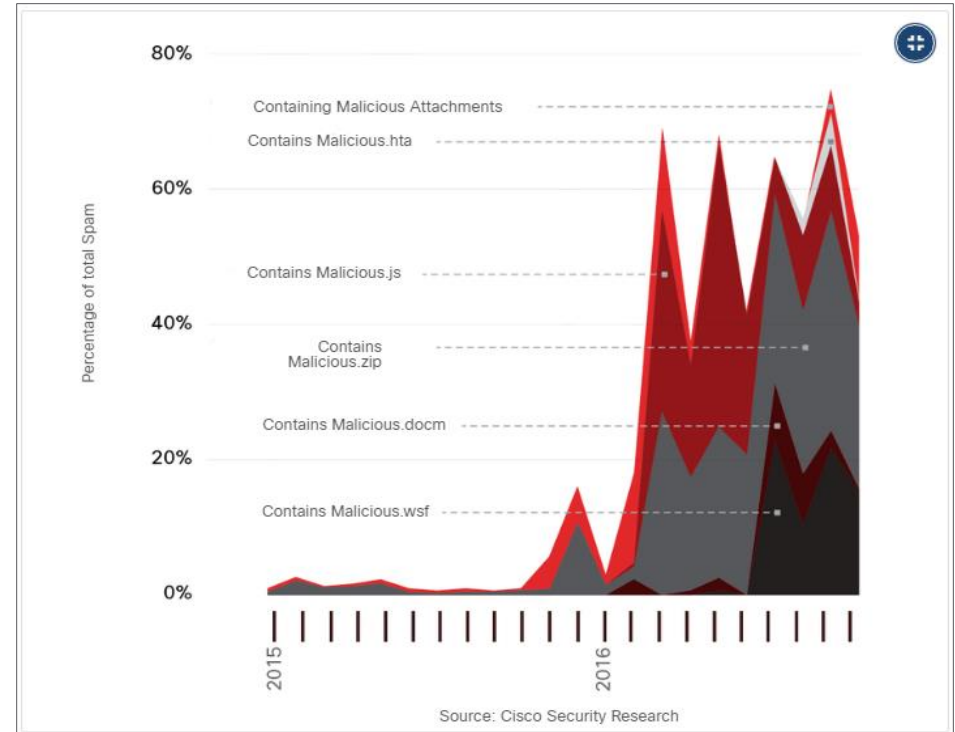
Objetivo do módulo: Explicar como um site de análise de malware gera um relatório de análise de malware.

Tópico	Objetivo do Tópico
Proteção Antimalware	Explicar os métodos de mitigação de malware.
Prevenção de intrusão baseada em host	Explicar entradas de log IPS / IDS baseadas em host
Segurança de aplicações	Explique como um sandbox é usado para analisar malware

22.1 Proteção antimalware

Ameaças de endpoints

- Os pontos de extremidade podem ser definidos como hosts na rede que podem acessar ou ser acessados por outros hosts na rede.
- Cada ponto de extremidade é potencialmente uma forma de software malicioso obter acesso a uma rede.
- Dispositivos que acessam redes remotamente através de VPNs também são pontos finais que podem injetar malware na rede VPN a partir da rede pública.
- Vários tipos comuns de malware foram encontrados para alterar significativamente os recursos em menos de 24 horas, a fim de evitar a detecção.

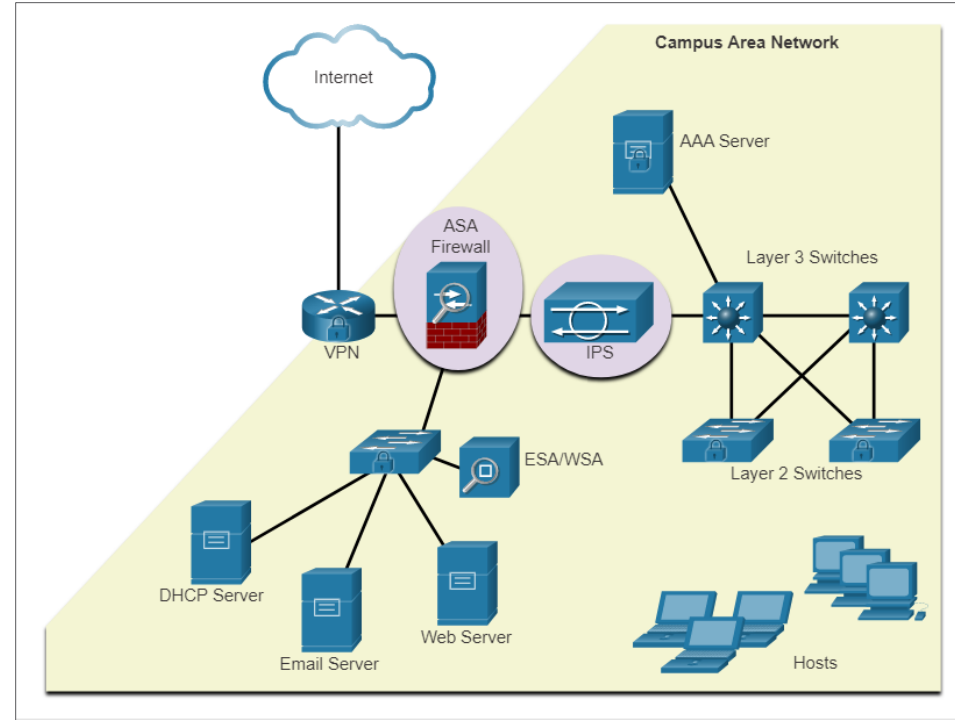


Porcentagem de Spam

© 2020 Cisco e/ou suas afiliadas. Todos os direitos reservados.
Confidencial da Cisco

Segurança de Endpoint

- Como muitos ataques se originam de dentro da rede, proteger uma LAN interna é quase tão importante quanto proteger o perímetro externo da rede.
- Depois que um host interno é infiltrado, ele pode se tornar um ponto de partida para um invasor obter acesso a dispositivos críticos do sistema, como servidores e informações confidenciais.
- Há dois elementos LAN internos para proteger:
 - **Endpoints** - Os hosts são suscetíveis a ataques relacionados a malware.
 - **Infraestrutura de rede** - Pontos de extremidade de interconexão de dispositivos de infraestrutura LAN



Proteção de Endpoint contra malware baseada em host

- Software antimalware/antivírus baseado em host e firewalls baseados em host são usados para proteger dispositivos móveis usando VPN.

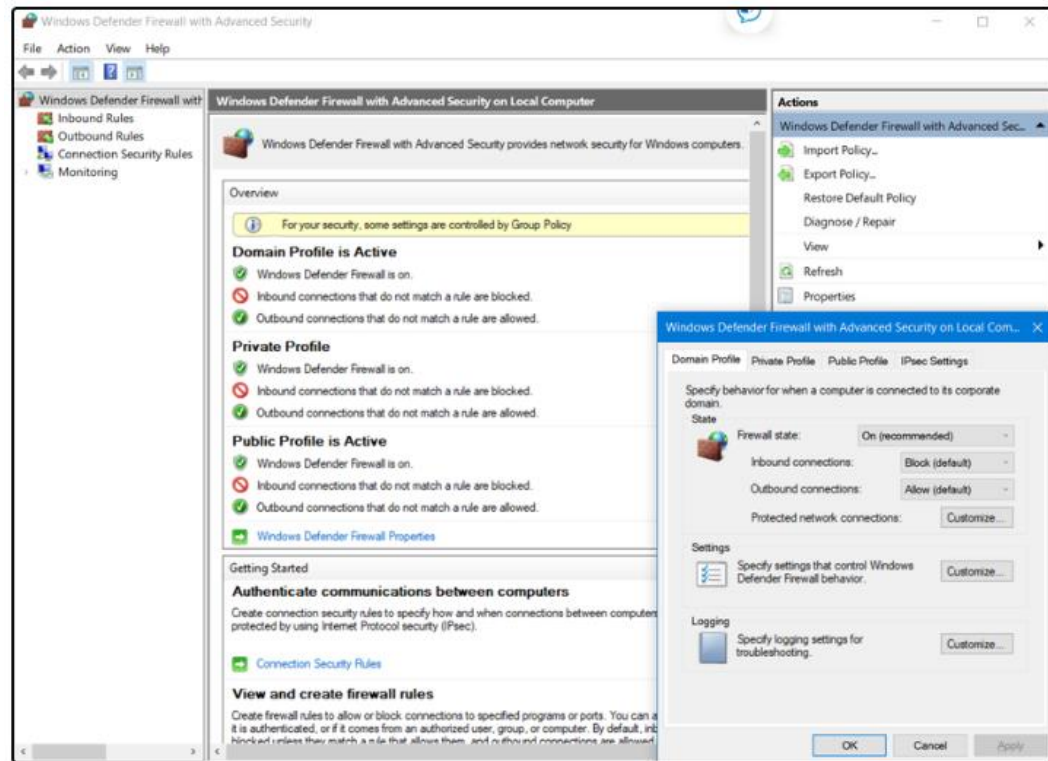
Software antivírus / antimalware

- É um software instalado em um host para detectar e mitigar vírus e malware. Por exemplo, proteção contra vírus e ameaças do Windows Defender, Cisco AMP for Endpoints, Norton Security, McAfee, Trend Micro e outros.
- Programas antimalware podem detectar vírus usando três abordagens diferentes:
 - **Baseado em assinatura:** reconhece várias características de arquivos de malware conhecidos
 - **Baseado em heurística:** reconhece recursos gerais compartilhados por vários tipos de malware
 - **Baseado em comportamento:** emprega análise de comportamento suspeito
- A proteção antivírus baseada em host, também conhecida como baseada em agentes, é executada em todas as máquinas protegidas.

Proteção contra malware baseada em host do Endpoint Protection (Condd.)

Firewall de host

- Este software está instalado em um host.
- Restringe conexões de entrada e saída a conexões iniciadas somente por esse host.
- Alguns softwares de firewall podem impedir que um host se infecte e impedir que hosts infectados espalhem malware para outros hosts. Esta função está incluída em alguns sistemas operacionais.
- Por exemplo, o Windows inclui o Firewall do Windows Defender com Segurança Avançada.



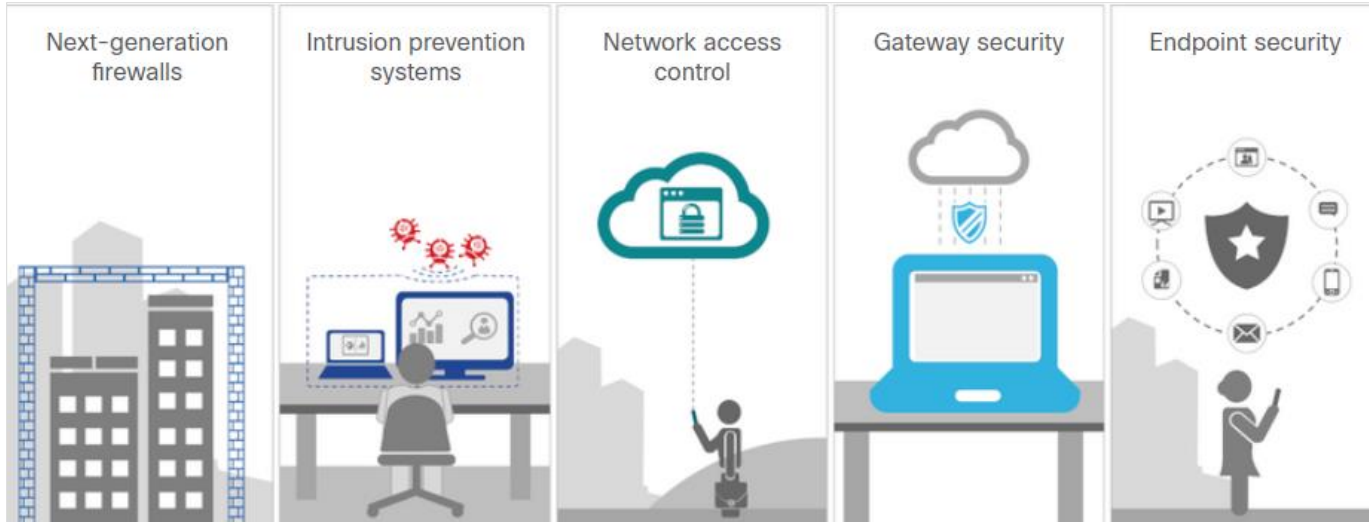
Proteção contra malware baseado em host do Endpoint Protection (cont.)

Suites de segurança baseadas em host

- Recomenda-se instalar um conjunto de produtos de segurança baseado em host em redes domésticas e empresariais para fornecer uma defesa em camadas que proteja contra as ameaças mais comuns.
- Estes incluem antivírus, anti-phishing, navegação segura, sistema de prevenção de intrusões baseado em host e recursos de firewall.
- Os produtos de segurança baseados em host também fornecem função de telemetria.
- A maioria dos softwares de segurança baseados em host inclui uma funcionalidade robusta de registro que é essencial para operações de segurança cibernética.
- O laboratório de testes independente AV-TEST fornece análises de alta qualidade de proteções baseadas em host, bem como informações sobre muitos outros produtos de segurança.

Proteção de ponto de extremidade contra malware baseada em rede

- Os dispositivos de prevenção de malware baseados em rede são capazes de compartilhar informações entre si para tomar decisões melhor informadas.
- A proteção de endpoints em uma rede sem fronteiras pode ser realizada usando técnicas baseadas em rede, bem como baseadas em host.

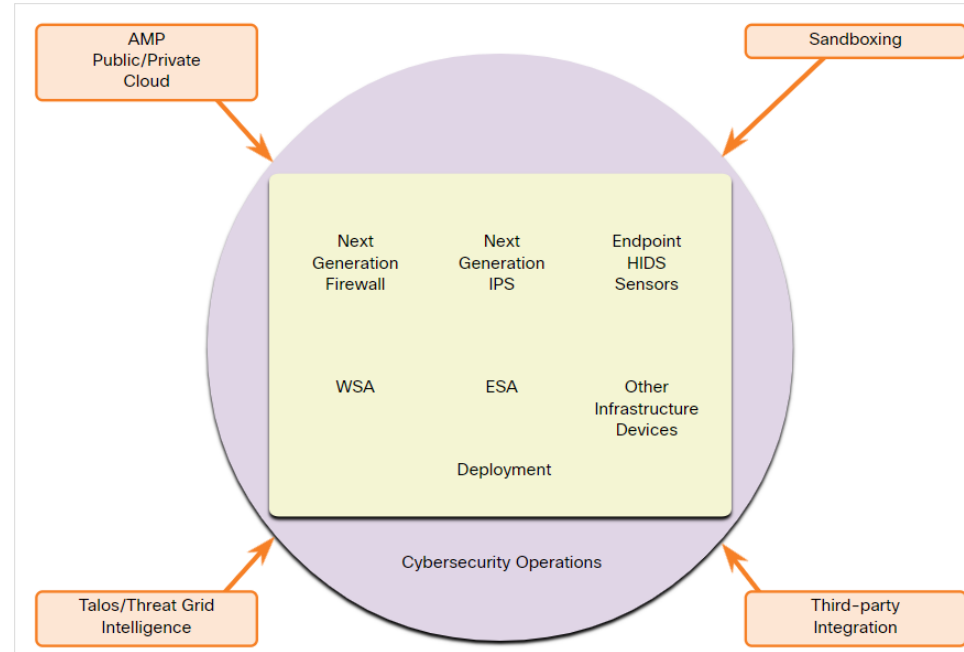


Proteção avançada contra malware em todos os lugares

Proteção contra malware com base em rede (cont.)

Alguns exemplos de dispositivos e técnicas que implementam proteções de host no nível da rede:

- **Proteção avançada contra malware (AMP)** - Fornece proteção de terminais contra vírus e malware.
- **Email Security Appliance (ESA)** - Fornece filtragem de SPAM e e-mails potencialmente maliciosos antes que eles cheguem ao endpoint.
- **Web Security Appliance (WSA)** - Fornece filtragem de sites e lista negra
- **Controle de Admissão de Rede (NAC)** - Permite que somente sistemas autorizados e compatíveis se conectem à rede.



22.2 Proteção contra intrusão baseada em host

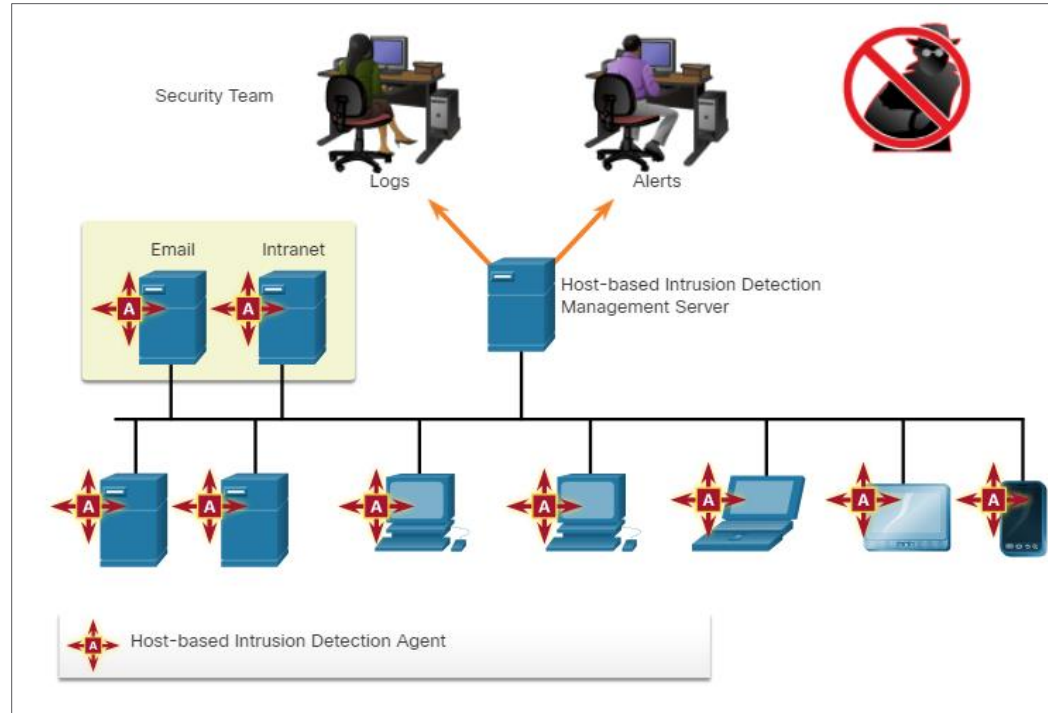
Proteção contra intrusões baseada em host Firewalls baseados em host

- Firewalls pessoais baseados em host são programas de software autônomos que controlam o tráfego que entra ou sai de um computador.
- Aplicativos de firewall baseados em host também podem ser configurados para emitir alertas aos usuários se um comportamento suspeito for detectado.
- Alguns exemplos de firewalls baseados em host:
 - **Firewall do Windows Defender**— Primeiro incluído no Windows XP, o Firewall do Windows (agora Firewall do Windows Defender) usa uma abordagem baseada em perfil para a funcionalidade do firewall.
 - **iptables**— Esta é uma aplicação que permite aos administradores de sistema Linux configurar regras de acesso à rede que fazem parte dos módulos Netfilter do kernel Linux.
 - **nftables**— O sucessor do iptables, nftables é um aplicativo de firewall do Linux que usa uma máquina virtual simples no kernel do Linux.
 - **TCP Wrappers**— Este é um sistema de registro e controle de acesso baseado em regras para Linux.

Proteção contra intrusões baseada em host

Detecção de intrusões baseada em host

- Um Sistema de Detecção de Intrusões baseado em Host (HIDS) foi projetado para proteger hosts contra malware conhecido e desconhecido.
- Um HIDS pode realizar monitoramento detalhado e relatórios sobre a configuração do sistema e a atividade do aplicativo.
- HIDS é um aplicativo de segurança abrangente que combina as funcionalidades de aplicativos antimalware com funcionalidade de firewall.
- Como o HIDS deve ser executado diretamente no host, ele é considerado um sistema baseado em agente.



Arquitetura de detecção de intrusões baseada em

Operação HIDS de proteção contra intrusões baseada em host

- Um HIDS pode impedir intrusões porque utiliza assinaturas para detectar malware conhecido e impedir que infecte um sistema.
- Algumas famílias de malware exibem polimorfismo.
- Um conjunto adicional de estratégias é usado para detectar a possibilidade de intrusões bem-sucedidas por malware que evade a detecção de assinaturas:
 - **Baseado em anomalias**- O comportamento do sistema host é comparado a um modelo de linha de base aprendido de comportamento normal. Se uma intrusão for detectada, o HIDS poderá registrar detalhes da intrusão, enviar alertas para sistemas de gerenciamento de segurança e tomar medidas para evitar o ataque.
 - **Baseado em políticas**- O comportamento normal do sistema é descrito por regras, ou a violação de regras, que são predefinidas. A violação dessas políticas resultará em ação do HIDS, como o encerramento de processos de software.

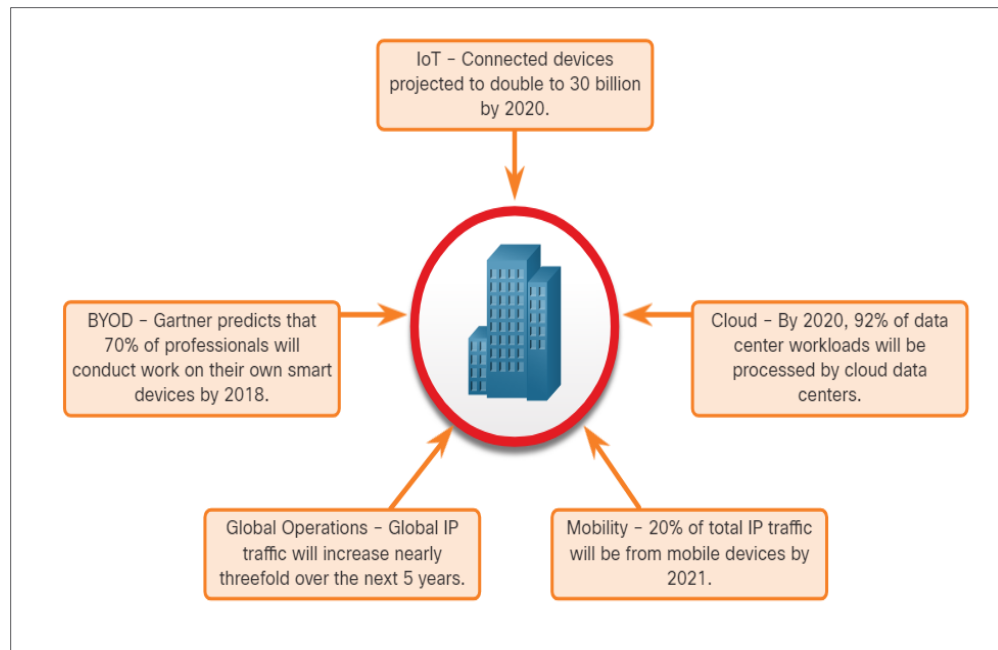
Produtos HIDS de proteção contra intrusões baseados em host

- A maioria dos HIDS utiliza software no host e algum tipo de funcionalidade centralizada de gerenciamento de segurança que permite a integração com serviços de monitoramento de segurança de rede e inteligência contra ameaças.
- Alguns exemplos são Cisco AMP, AlienVault USM, Tripwire e Open Source HIDS Security (OSSEC).
- O OSSEC usa um servidor de gerenciador central e agentes instalados em hosts individuais.
- O servidor OSSEC, ou Manager, também pode receber e analisar alertas de uma variedade de dispositivos de rede e firewalls através de syslog.
- O OSSEC monitora os logs do sistema nos hosts e também realiza a verificação da integridade do arquivo.

22.3 Segurança de aplicativos

Superfície de ataque de segurança

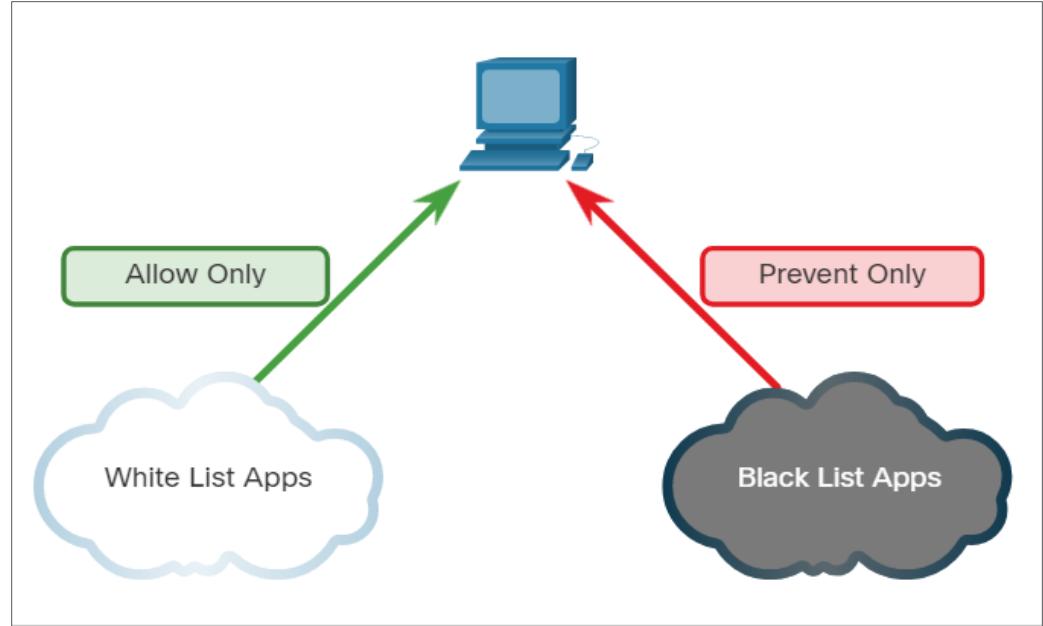
- Uma superfície de ataque é a soma total das vulnerabilidades em um determinado sistema que é acessível a um invasor.
- Ele pode consistir em portas abertas em servidores ou hosts, software executado em servidores voltados para a Internet, protocolos de rede sem fio e usuários.
- Componentes da superfície de ataque:
 - **Superfície de ataque de rede:** explora vulnerabilidades em redes.
 - **Superfície de ataque de software:** fornecido por meio da exploração de vulnerabilidades em aplicativos de software baseados na Web, na nuvem ou em host.
 - **Superfície de ataque humano:** explora fraquezas no comportamento do usuário.



Uma superfície de ataque em expansão

Lista negra e lista branca de aplicativos

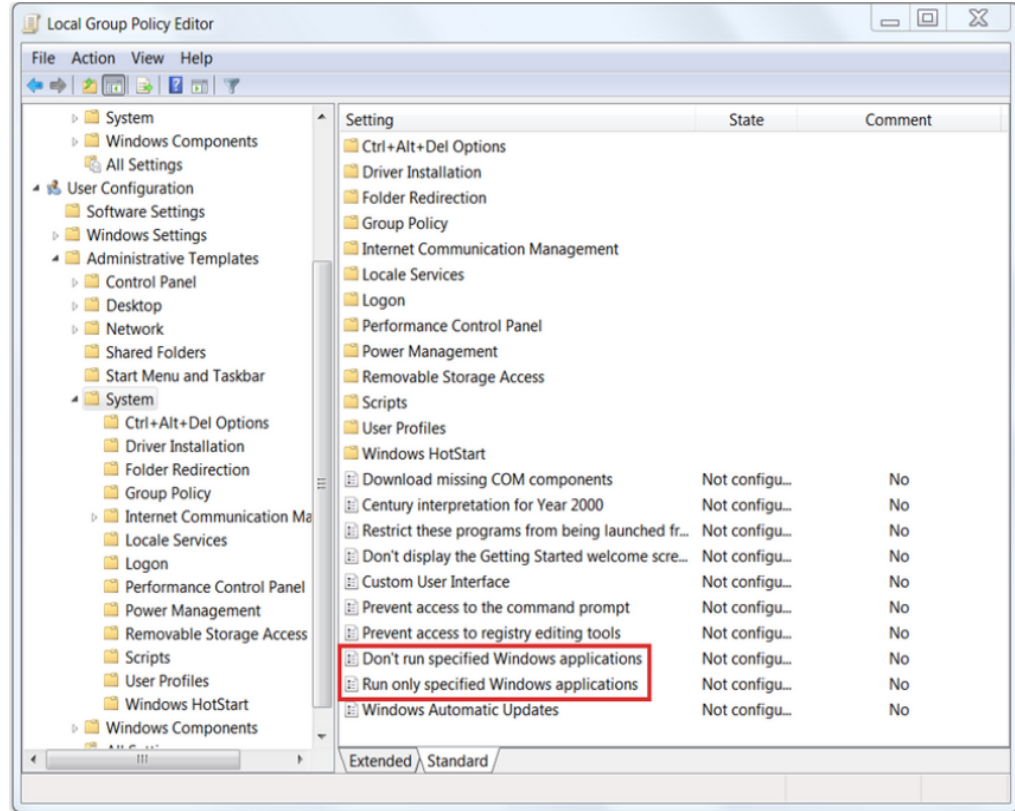
- Limitar o acesso a ameaças potenciais criando listas de aplicativos proibidos é conhecido como lista negra.
- As listas negras de aplicativos podem ditar quais aplicativos de usuário não têm permissão para serem executados em um computador.
- As listas brancas especificam quais programas podem ser executados.
- Dessa forma, aplicativos vulneráveis conhecidos podem ser impedidos de criar vulnerabilidades em hosts de rede.



Lista negra e lista branca de aplicativos

Lista negra e lista branca de aplicativos (cont.)

- Os sites também podem ser incluídos na lista branca e na lista negra.
- Essas listas negras podem ser criadas manualmente ou podem ser obtidas de vários serviços de segurança.
- As listas negras podem ser continuamente atualizadas pelos serviços de segurança e distribuídas para firewalls e outros sistemas de segurança que as utilizam.
- O sistema de gerenciamento de segurança Firepower da Cisco é um exemplo de um sistema que pode acessar o serviço de inteligência de segurança Cisco Talos para obter listas negras.



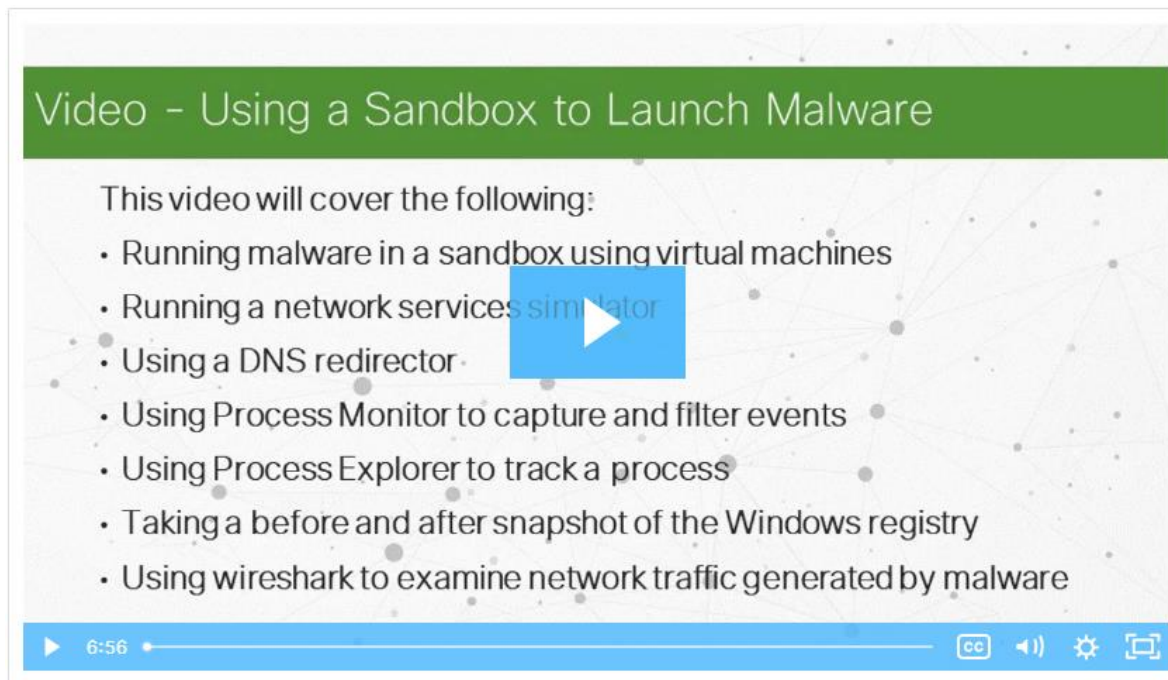
Sandboxing baseado em sistema de segurança de aplicativos

- Sandboxing é uma técnica que permite que arquivos suspeitos sejam executados e analisados em um ambiente seguro.
- Cuckoo Sandbox é um sandbox popular sistema de análise de malware livre. Ele pode ser executado localmente e ter amostras de malware enviadas a ele para análise.
- ANY.RUN é uma ferramenta online que oferece a capacidade de carregar uma amostra de malware para análise como qualquer sandbox online.



Vídeo de segurança de aplicativos - Usando uma sandbox para iniciar malware

- Reproduza o vídeo para ver uma demonstração do uso do ambiente sandbox para iniciar e analisar um ataque de malware.



22.4 Resumo da proteção do endpoint

O que aprendi neste módulo?

- Os pontos de extremidade são definidos como hosts na rede que podem acessar ou ser acessados por outros hosts na rede.
- Há dois elementos de LAN internos para proteger: endpoints e infra-estrutura de rede.
- O Software Antivírus/Antimalware é instalado em um host para detectar e mitigar vírus e malware.
- Firewalls baseados em host podem usar um conjunto de políticas predefinidas, ou perfis, para controlar pacotes que entram e saem de um computador.
- Alguns exemplos de firewalls baseados em host incluem Firewall do Windows Defender, iptables, nftables e TCP Wrappers.
- O HIDS protege os hosts contra malware conhecido e desconhecido.
- Uma superfície de ataque é a soma total das vulnerabilidades em um determinado sistema que pode ser acessado por um invasor.
- As listas negras de aplicativos ditam quais aplicativos de usuário não têm permissão para serem executados em um computador e as listas brancas especificam quais programas podem ser executados.

Novos termos e comandos

<ul style="list-style-type: none">• Antivirus/Antimalware• Endpoint	<ul style="list-style-type: none">• Firewall baseado em host• Sandboxing	<ul style="list-style-type: none">• Sistema de detecção de intrusão baseado em host (HIDS)• Superfície de ataque
--	---	---

