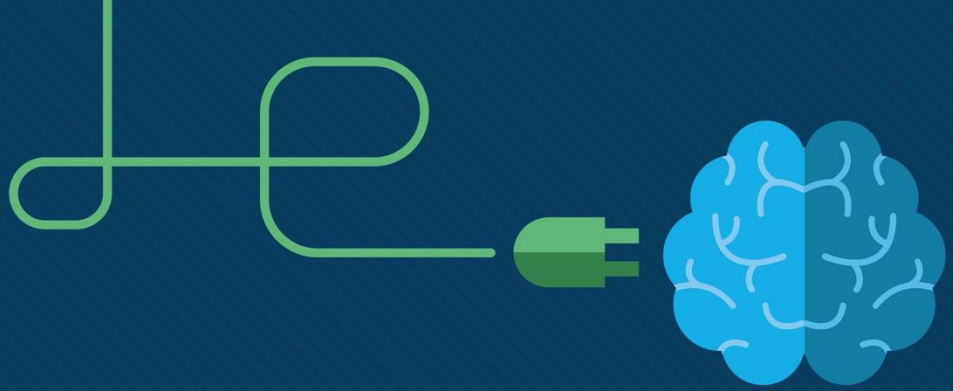


Module 22: Endpoint Protection

CyberOps Associate v1.0

Module Objectives

Module Title: Endpoint Protection

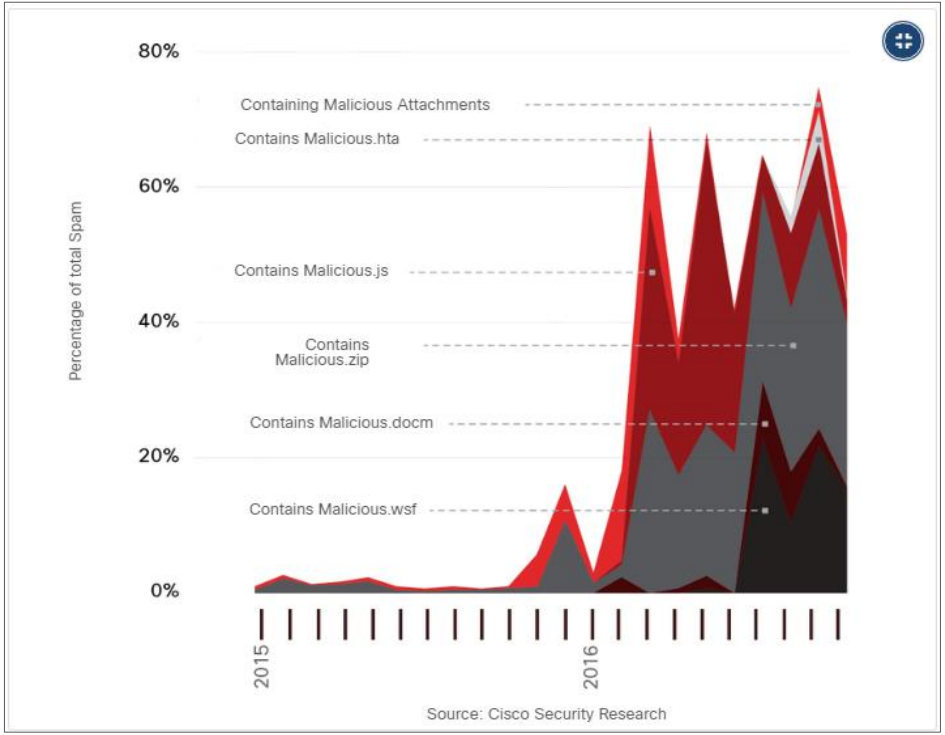
Module Objective: Explain how a malware analysis website generates a malware analysis report.

Topic	Topic Objective
Antimalware Protection	Explain methods of mitigating malware
Host-based Intrusion Prevention	Explain host-based IPS/IDS log entries
Application Security	Explain how a sandbox is used to analyze malware

22.1 Antimalware Protection

Endpoint Threats

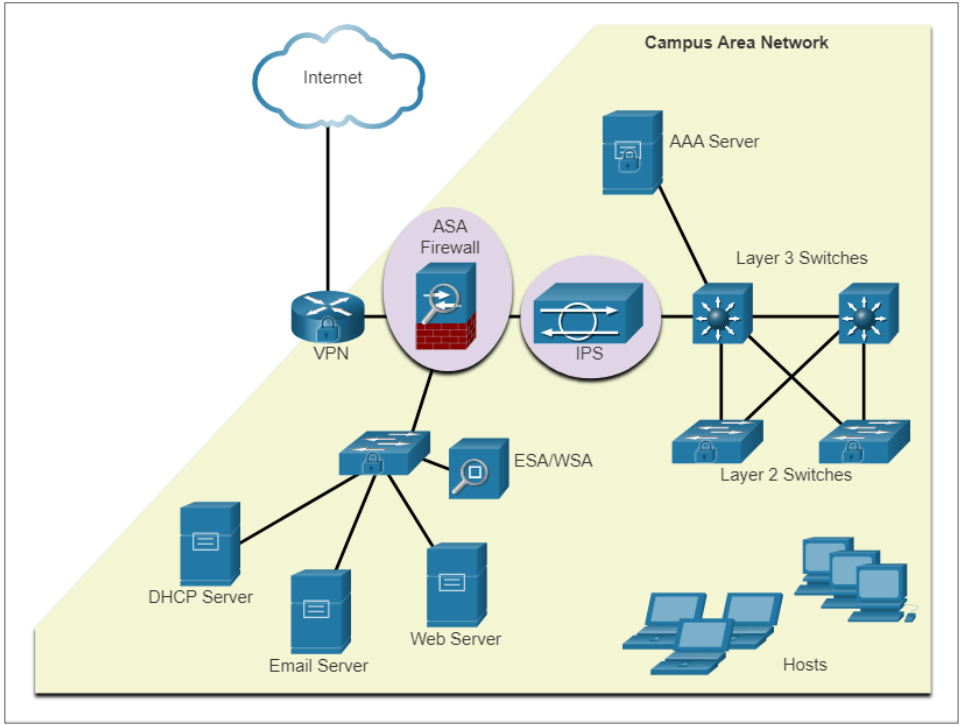
- Endpoints can be defined as hosts on the network that can access or be accessed by other hosts on the network.
- Each endpoint is potentially a way for malicious software to gain access to a network.
- Devices that remotely access networks through VPNs are also endpoints that could inject malware into the VPN network from the public network.
- Several common types of malware have been found to significantly change features in less than 24 hours in order to evade detection.



Malicious Spam Percentage

Endpoint Security

- As many attacks originate from inside the network, securing an internal LAN is nearly as important as securing the outside network perimeter.
- After an internal host is infiltrated, it can become a starting point for an attacker to gain access to critical system devices, such as servers and sensitive information.
- There are two internal LAN elements to secure:
  - **Endpoints** - Hosts are susceptible to malware-related attacks.
  - **Network infrastructure** - LAN infrastructure devices interconnect endpoints



Host-Based Malware Protection

- Host-based antimalware/antivirus software and host-based firewalls are used to protect mobile devices using VPN.

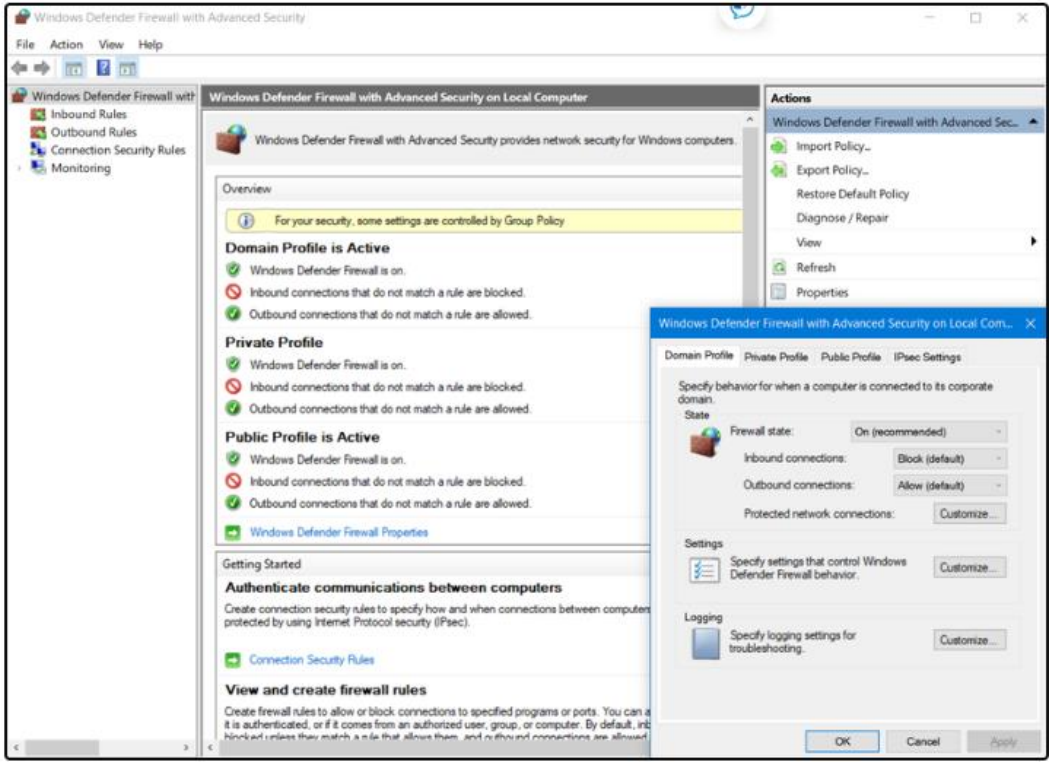
Antivirus/Antimalware Software

- It is a software that is installed on a host to detect and mitigate viruses and malware. For example, Windows Defender Virus & Threat Protection, Cisco AMP for Endpoints, Norton Security, McAfee, Trend Micro, and others.
- Antimalware programs may detect viruses using three different approaches:
  - **Signature-based:** Recognizes various characteristics of known malware files
  - **Heuristics-based:** Recognizes general features shared by various types of malware
  - **Behavior-based:** Employs analysis of suspicious behavior
- Host-based antivirus protection, also known as agent-based, runs on every protected machine.

Host-Based Malware Protection (Contd.)

Host-based Firewall

- This software is installed on a host.
- It restricts incoming and outgoing connections to connections initiated by that host only.
- Some firewall software can prevent a host from becoming infected and stop infected hosts from spreading malware to other hosts. This function is included in some operating systems.
- For example, Windows includes Windows Defender Firewall with Advanced Security.



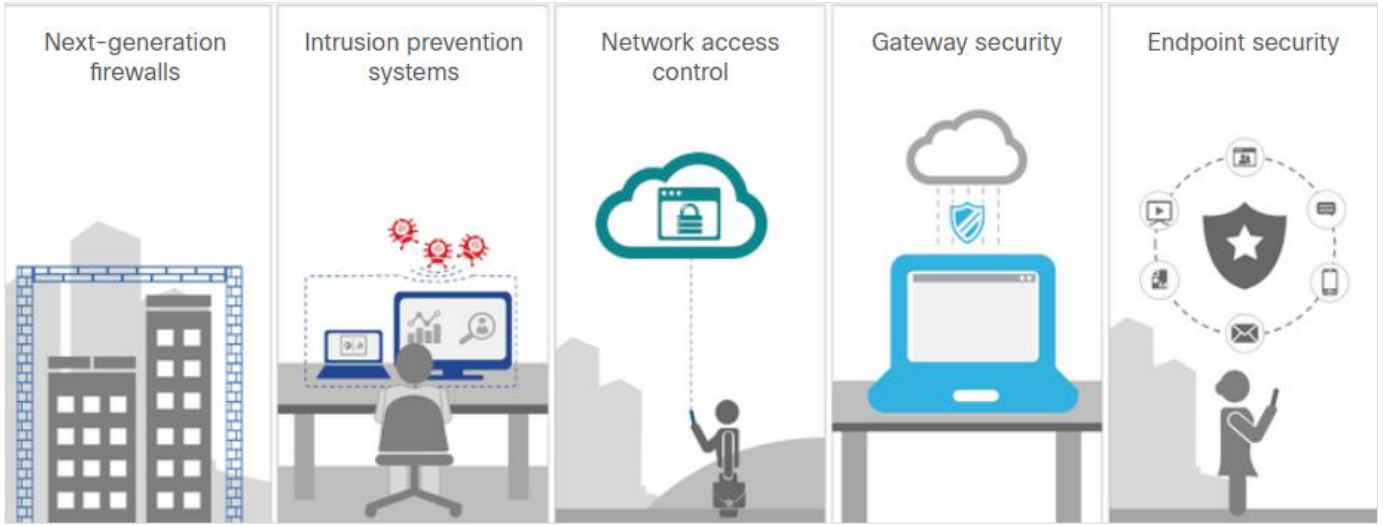
Host-Based Malware Protection (Contd.)

Host-based Security Suites

- It is recommended to install a host-based suite of security products on home and business networks to provide a layered defense that will protect against most common threats.
- These include antivirus, anti-phishing, safe browsing, Host-based intrusion prevention system, and firewall capabilities.
- Host-based security products also provide telemetry function.
- Most host-based security software includes robust logging functionality that is essential to cyber security operations.
- The independent testing laboratory AV-TEST provides high-quality reviews of host-based protections, as well as information about many other security products.

Network-Based Malware Protection

- Network-based malware prevention devices are capable of sharing information among themselves to make better informed decisions.
- Protecting endpoints in a borderless network can be accomplished using network-based, as well as host-based techniques.

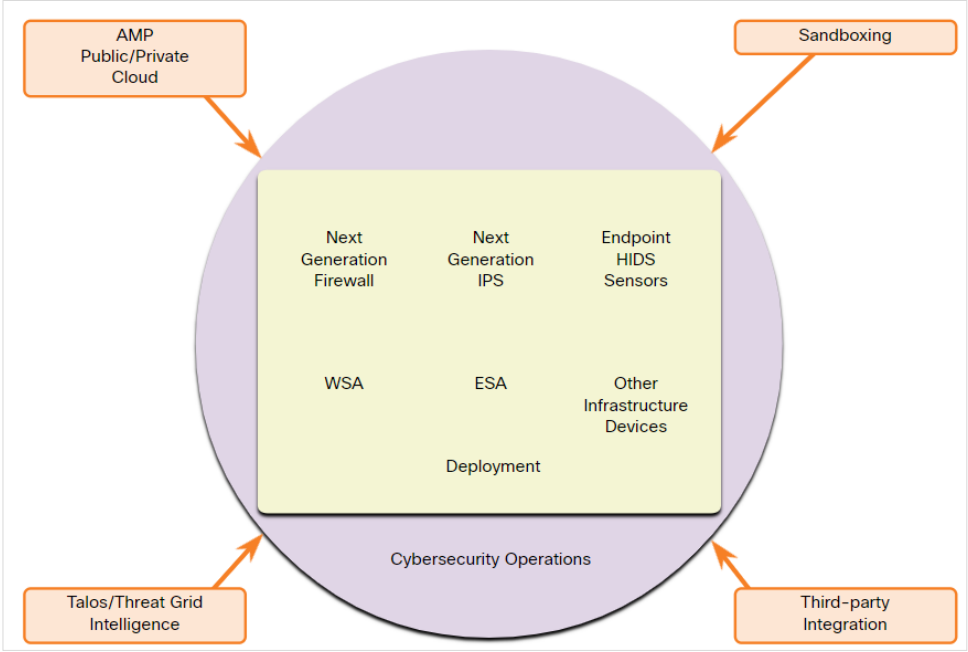


Advanced Malware Protection Everywhere

Network-Based Malware Protection (Contd.)

Some examples of devices and techniques that implement host protections at the network level:

- **Advanced Malware Protection (AMP)** - Provides endpoint protection from viruses and malware.
- **Email Security Appliance (ESA)** - Provides filtering of SPAM and potentially malicious emails before they reach the endpoint.
- **Web Security Appliance (WSA)** - Provides filtering of websites and blacklisting
- **Network Admission Control (NAC)** - Permits only authorized and compliant systems to connect to the network.



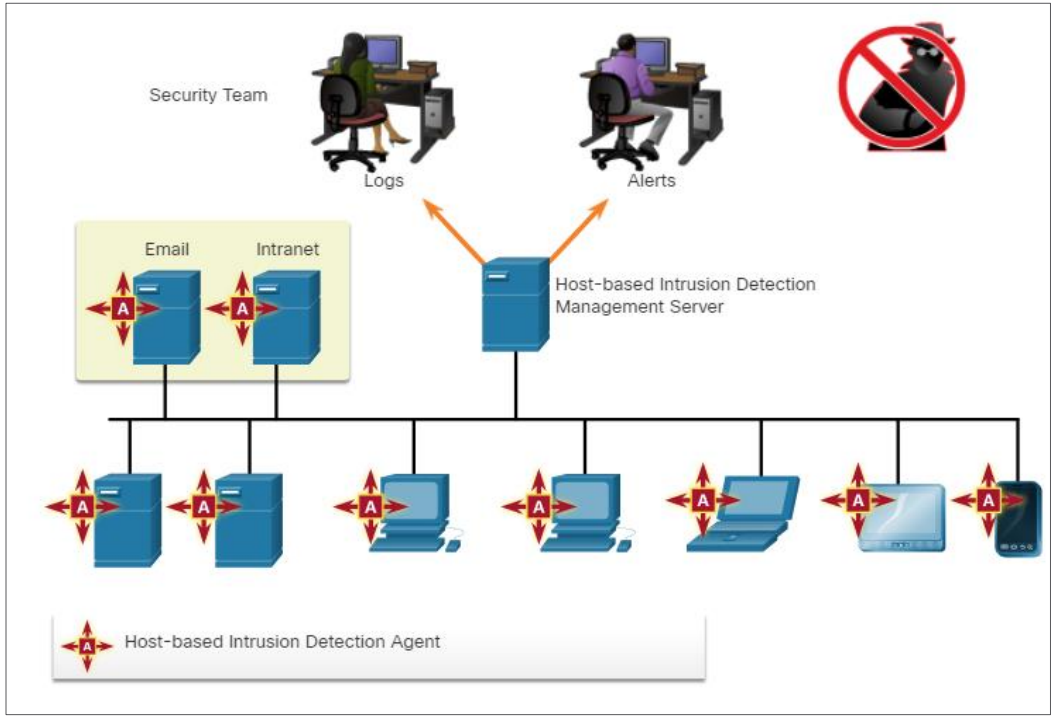
22.2 Host-Based Intrusion Protection

Host-Based Firewalls

- Host-based personal firewalls are standalone software programs that control traffic entering or leaving a computer.
- Host-based firewall applications can also be configured to issue alerts to users if suspicious behavior is detected.
- Some examples of host-based firewalls:
  - **Windows Defender Firewall** – First included with Windows XP, Windows Firewall (now Windows Defender Firewall) uses a profile-based approach to firewall functionality.
  - **iptables** – This is an application that allows Linux system administrators to configure network access rules that are part of the Linux kernel Netfilter modules.
  - **nftables** – The successor to iptables, nftables is a Linux firewall application that uses a simple virtual machine in the Linux kernel.
  - **TCP Wrappers** – This is a rule-based access control and logging system for Linux.

Host-Based Intrusion Detection

- A Host-based Intrusion Detection System (HIDS) is designed to protect hosts against known and unknown malware.
- A HIDS can perform detailed monitoring and reporting on the system configuration and application activity.
- HIDS is a comprehensive security application that combines the functionalities of antimalware applications with firewall functionality.
- As HIDS must run directly on the host, it is considered as an agent-based system.



Host-based Intrusion Detection Architecture

HIDS Operation

- A HIDS can prevent intrusion because it uses signatures to detect known malware and prevent it from infecting a system.
- Some malware families exhibit polymorphism.
- An additional set of strategies are used to detect the possibility of successful intrusions by malware that evades signature detection:
  - **Anomaly based** - Host system behavior is compared to a learned baseline model of normal behavior. If an intrusion is detected, the HIDS can log details of the intrusion, send alerts to security management systems, and take action to prevent the attack.
  - **Policy based** - Normal system behavior is described by rules, or the violation of rules, that are predefined. Violation of these policies will result in action by the HIDS, such as shut down of software processes.

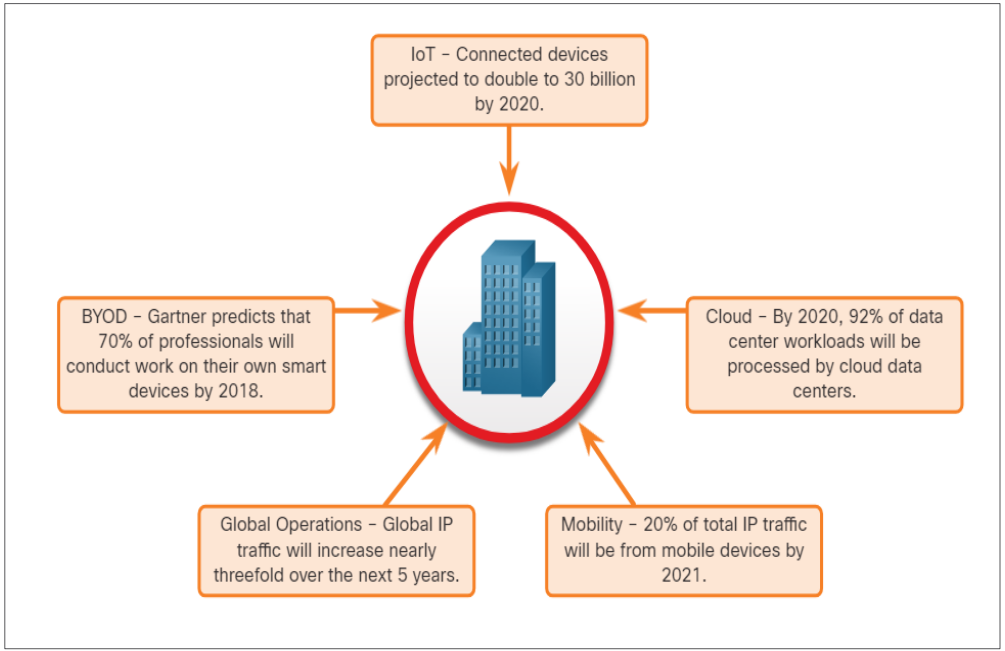
HIDS Products

- Most of the HIDS utilize software on the host and some sort of centralized security management functionality that allows integration with network security monitoring services and threat intelligence.
- Some examples are Cisco AMP, AlienVault USM, Tripwire, and Open Source HIDS SECurity (OSSEC).
- OSSEC uses a central manager server and agents that are installed on individual hosts.
- The OSSEC server, or Manager, can also receive and analyze alerts from a variety of network devices and firewalls over syslog.
- OSSEC monitors system logs on hosts and also conducts file integrity checking.

22.3 Application Security

Attack Surface

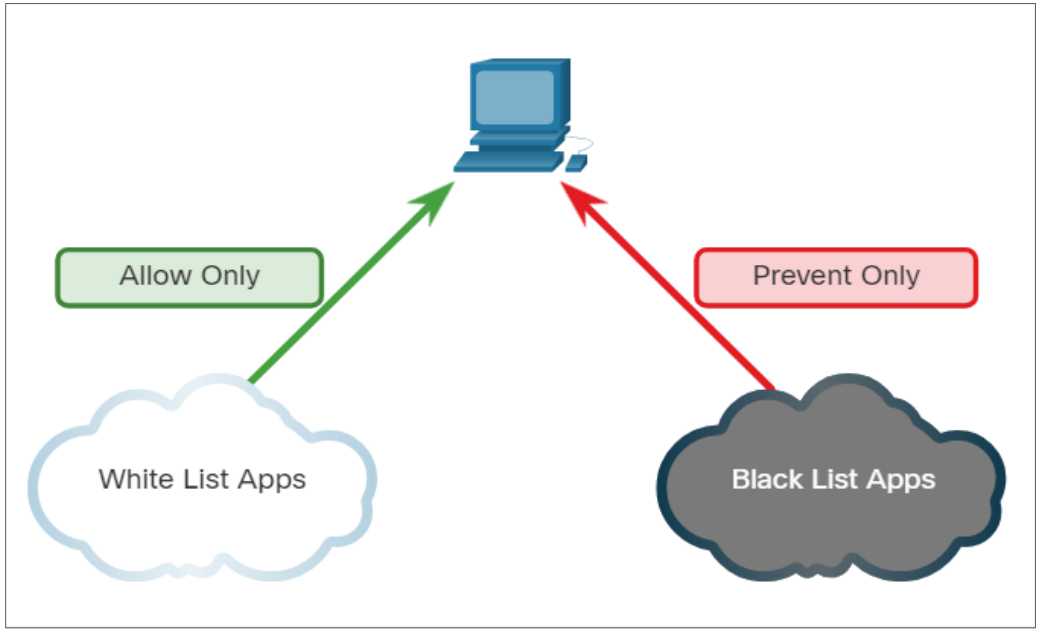
- An attack surface is the total sum of the vulnerabilities in a given system that is accessible to an attacker.
- It can consist of open ports on servers or hosts, software running on internet-facing servers, wireless network protocols, and users.
- Components of the Attack Surface:
  - **Network Attack Surface:** Exploits vulnerabilities in networks.
  - **Software Attack Surface:** Delivered through exploitation of vulnerabilities in web, cloud, or host-based software applications.
  - **Human Attack Surface:** Exploits weaknesses in user behavior.



An Expanding Attack Surface

Application Blacklisting and Whitelisting

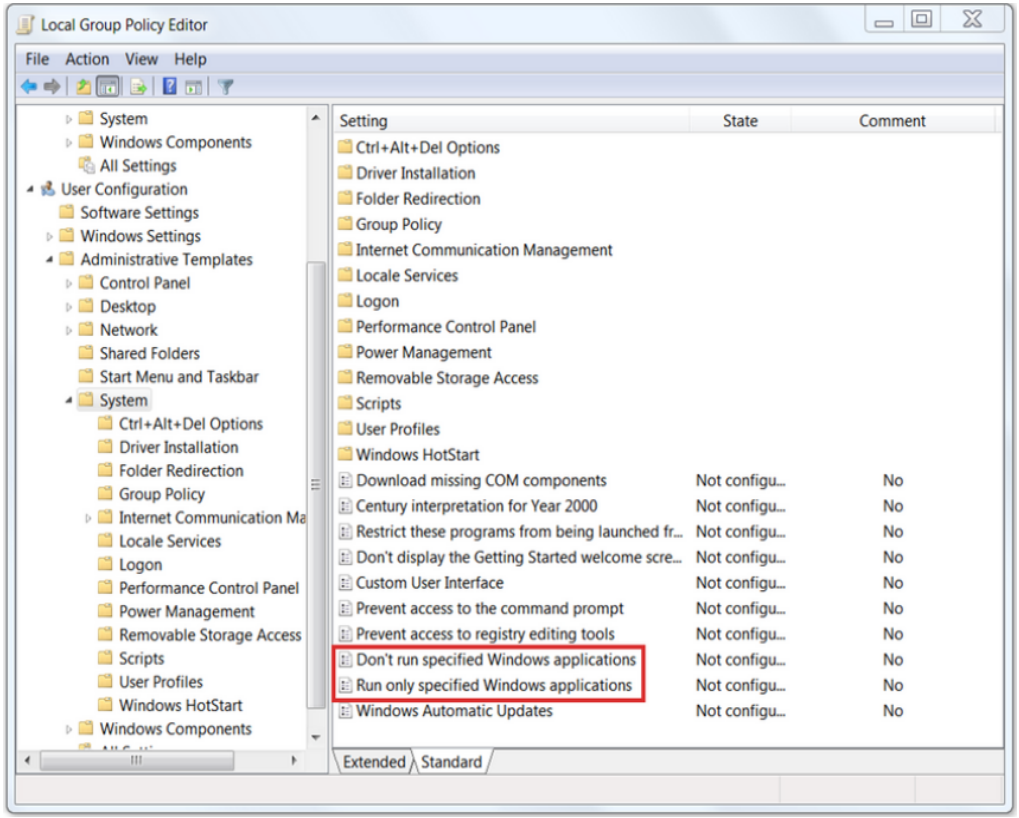
- Limiting access to potential threats by creating lists of prohibited applications is known as blacklisting.
- Application blacklists can dictate which user applications are not permitted to run on a computer.
- Whitelists specify which programs are allowed to run.
- In this way, known vulnerable applications can be prevented from creating vulnerabilities on network hosts.



Application Blacklisting and Whitelisting

Application Blacklisting and Whitelisting (Contd.)

- Websites can also be whitelisted and blacklisted.
- These blacklists can be manually created, or they can be obtained from various security services.
- Blacklists can be continuously updated by security services and distributed to firewalls and other security systems that use them.
- Cisco's Firepower security management system is an example of a system that can access the Cisco Talos security intelligence service to obtain blacklists.

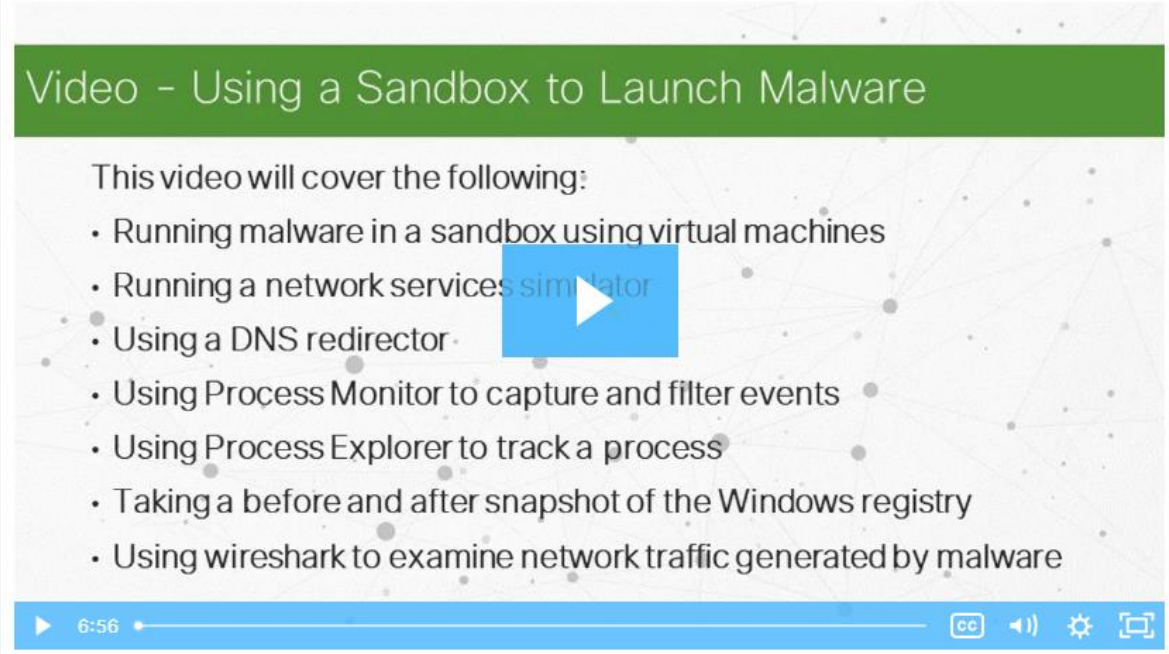


System-Based Sandboxing

- Sandboxing is a technique that allows suspicious files to be executed and analyzed in a safe environment.
- Cuckoo Sandbox is a popular free malware analysis system sandbox. It can be run locally and have malware samples submitted to it for analysis.
- ANY.RUN is an online tool that offers the ability to upload a malware sample for analysis like any online sandbox.

Video - Using a Sandbox to Launch Malware

- Play the video to view a demonstration of using sandbox environment to launch and analyze a malware attack.



22.4 Endpoint Protection Summary

What Did I Learn in this Module?

- Endpoints are defined as hosts on the network that can access or be accessed by other hosts on the network.
- There are two internal LAN elements to secure: Endpoints and Network Infrastructure.
- Antivirus/Antimalware Software is installed on a host to detect and mitigate viruses and malware.
- Host-based firewalls may use a set of predefined policies, or profiles, to control packets entering and leaving a computer.
- Some examples of host-based firewalls include Windows Defender Firewall, iptables, nftables, and TCP Wrappers.
- HIDS protects hosts against known and unknown malware.
- An attack surface is the total sum of the vulnerabilities in a given system that is accessible to an attacker.
- Application blacklists dictate which user applications are not permitted to run on a computer and whitelists specify which programs are allowed to run.

New Terms and Commands

• Antivirus/Antimalware • Endpoint	• Host-based firewall • Sandboxing	• Host-based Intrusion Detection System (HIDS) • Attack Surface


CISCO