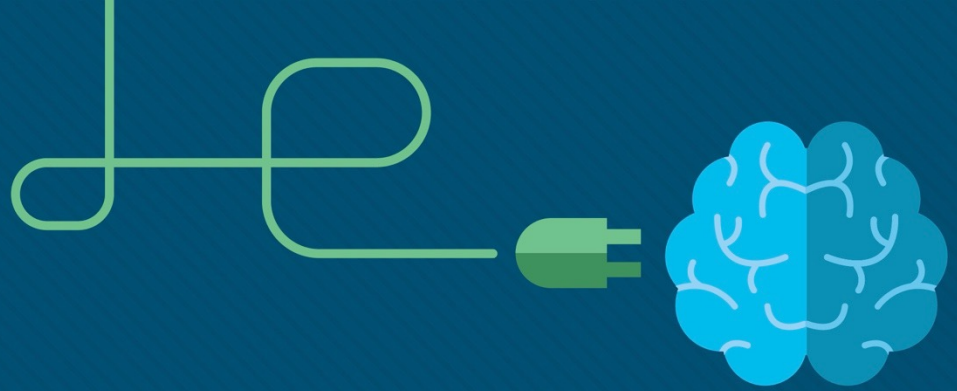


Chapter 11: Endpoint Security and Analysis

Information Security

Dr. Ayman Aljarbouh

11.1 Endpoint Protection

Module Objectives

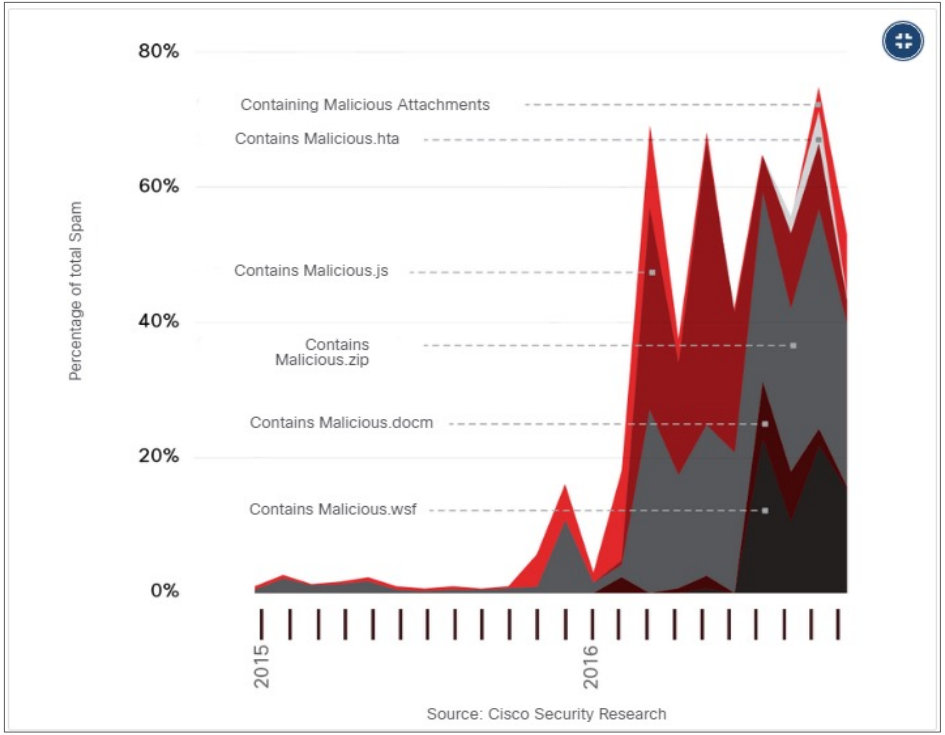
Module Title: Endpoint Protection

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

Endpoint Threats

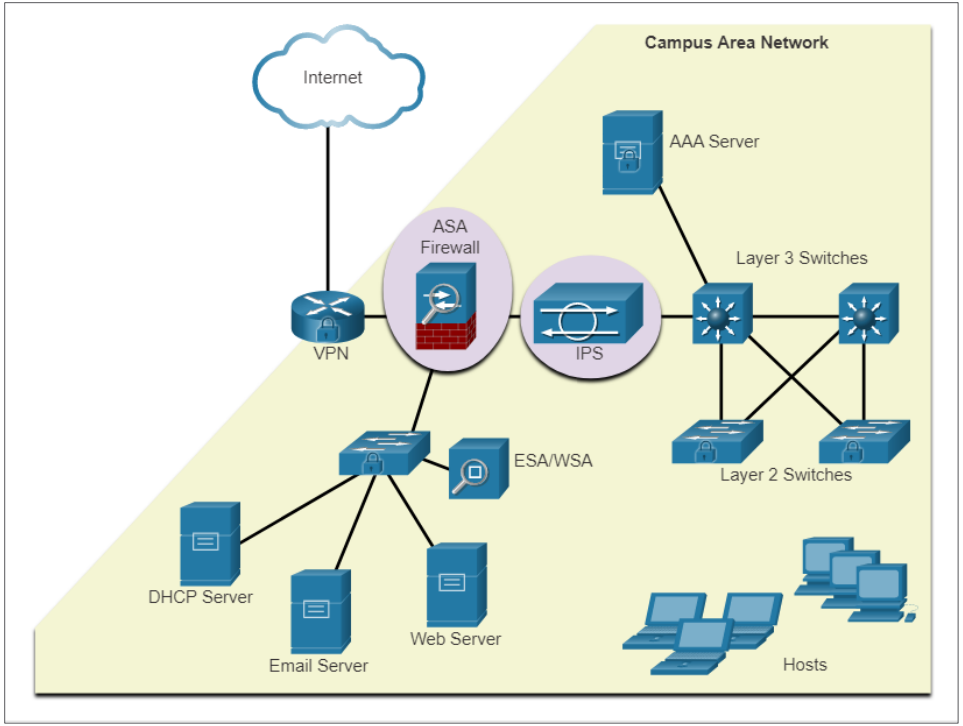
- Endpoints can be defined as hosts on the network that can access or be accessed by other hosts on the network.
- Each endpoint is potentially a way for malicious software to gain access to a network.
- Devices that remotely access networks through VPNs are also endpoints that could inject malware into 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

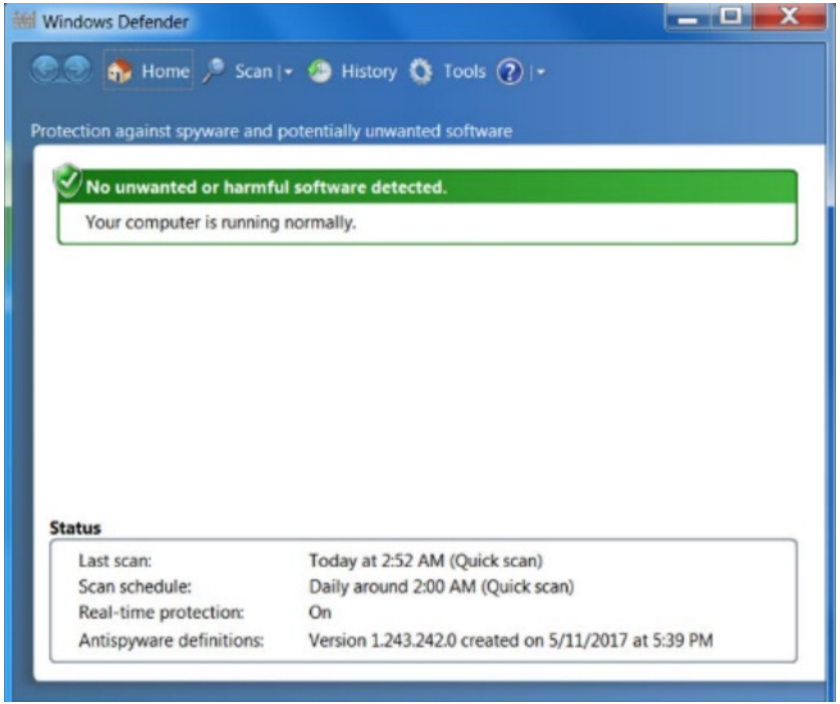
Endpoint Security

- 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



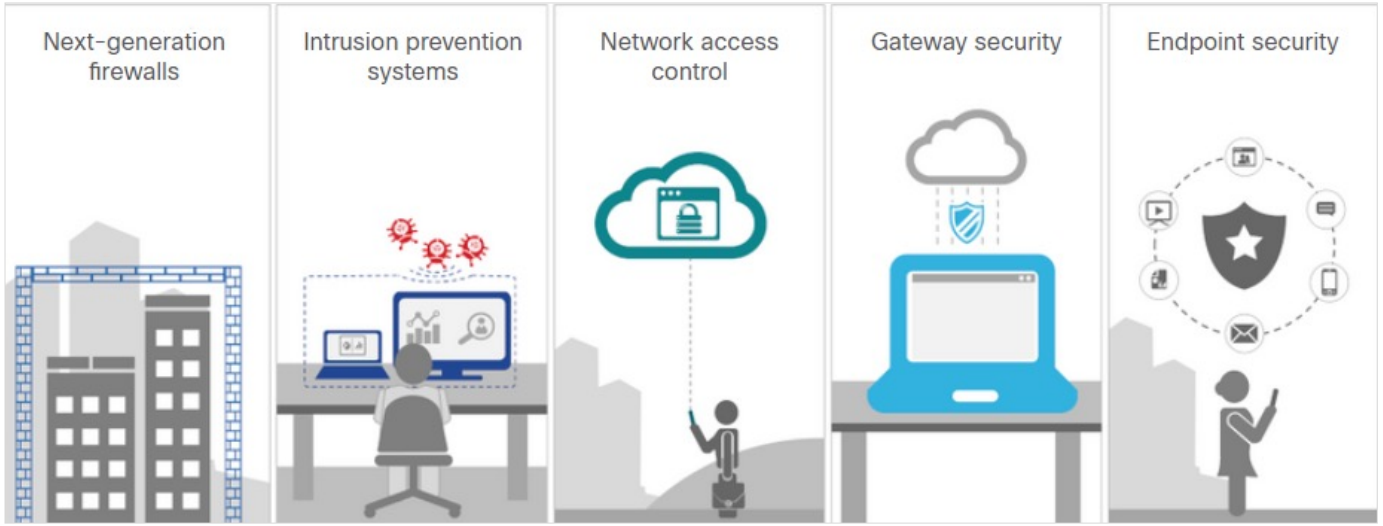
Host-Based Malware Protection

- Antimalware/antivirus software.
  - 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 Firewall - restricts incoming and outgoing connections.
- Host-based Security Suites - include antivirus, anti-phishing, safe browsing, Host-based intrusion prevention system, firewall capabilities and robust logging functionality.



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.

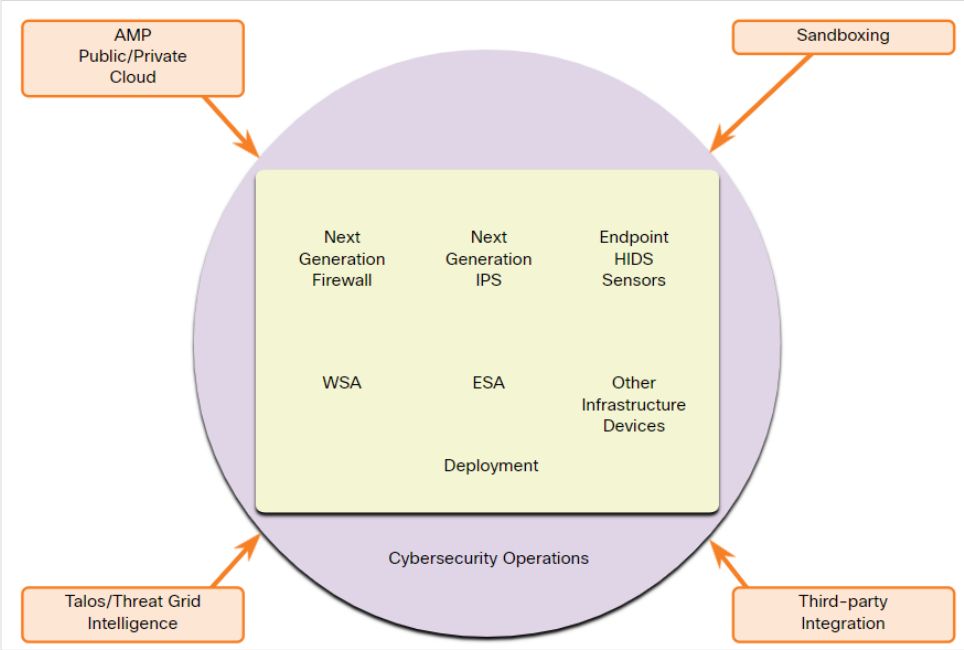


Advanced Malware Protection Everywhere

Network-Based Malware Protection (Contd.)

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

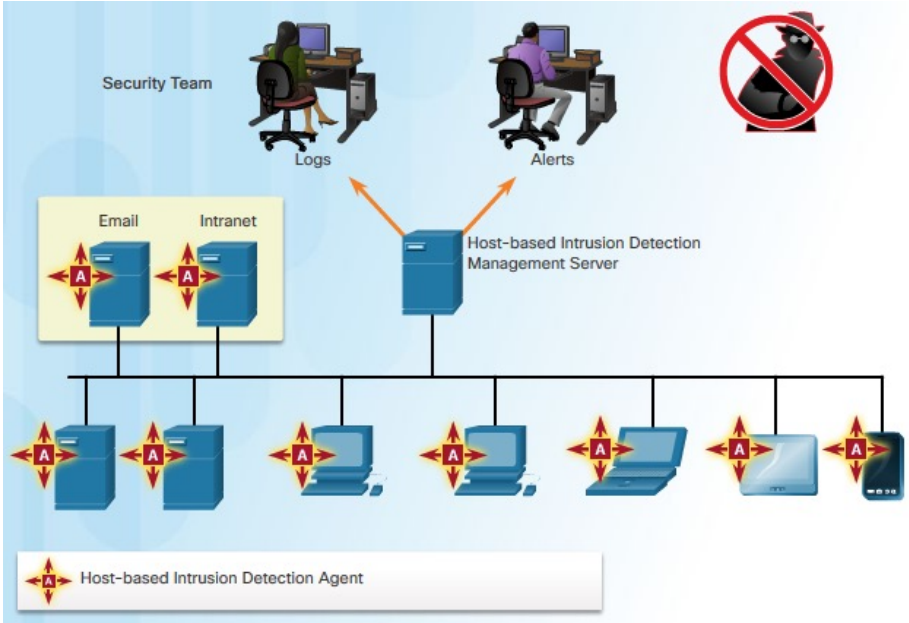
- **Advanced Malware Protection (AMP)** - Provides endpoint protection from viruses and malware.
- **Email Security Appliance (ESA)** - Provides filtering of SPAM and potentially malicious emails before they reach the endpoint.
- **Web Security Appliance (WSA)** - Provides filtering of websites and blacklisting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



Host-Based Firewalls

- Host-based personal firewalls are standalone software programs that control traffic entering or leaving a computer.
- Host-based firewalls include;
  - **Windows Firewall** - uses a profile-based approach to configuring firewall functionality.
  - **Iptables** - allows Linux system administrators to configure network access rules.
  - **Nftables** - successor to iptables, nftables is a Linux firewall application that uses a simple virtual machine in the Linux kernel.
  - **TCP Wrapper for Linux-based devices** - rule-based access control and logging system.

Host-Based Intrusion Detection



- Host-Based Intrusion Detection System (HIDS) protects hosts against malware and can perform the following:
  - monitoring and reporting
  - log analysis
  - event correlation
  - integrity checking
  - policy enforcement
  - rootkit detection
- HIDS software must run directly on the host, so it is considered an agent-based system.

HIDS Operation

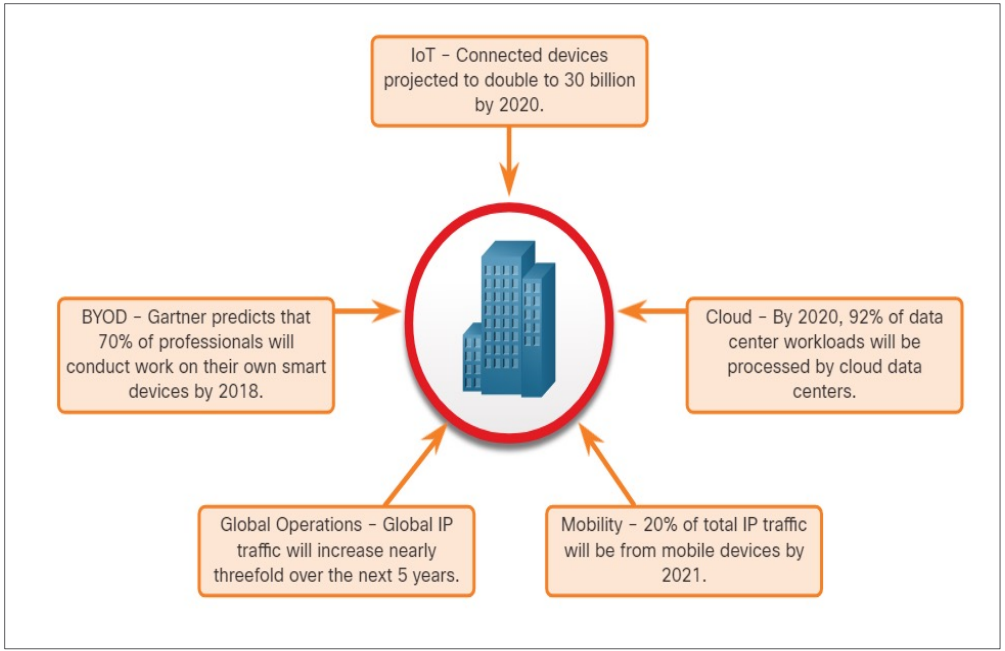
- A HIDS can prevent intrusion because it uses signatures to detect known malware and prevent it from infecting a system.
- An additional set of strategies are used to detect malware that evades signature detection:
  - **Anomaly-based** - host behavior is compared to a learned baseline model.
  - **Policy-based** – normal behavior is described by rules or by the violation of predefined rules.

HIDS Products

- Most 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.
  - Examples: 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.

Attack Surface

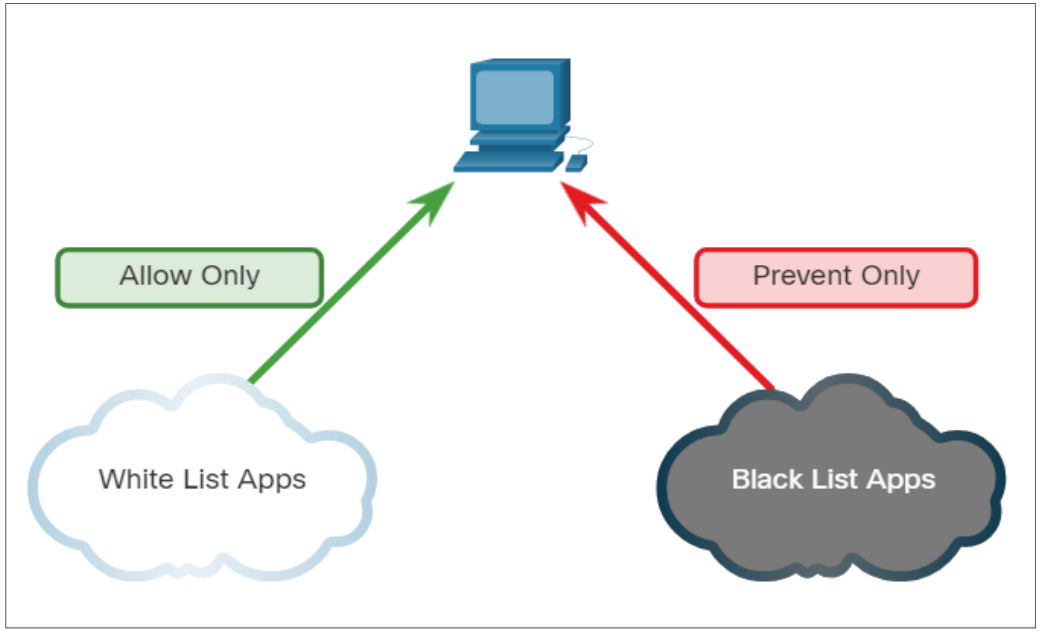
- An attack surface is the total sum of the vulnerabilities in a given system that is accessible to an attacker.
- It can consist of open ports on servers or hosts, software running on internet-facing servers, wireless network protocols, and users.
- Components of the Attack Surface:
  - **Network Attack 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

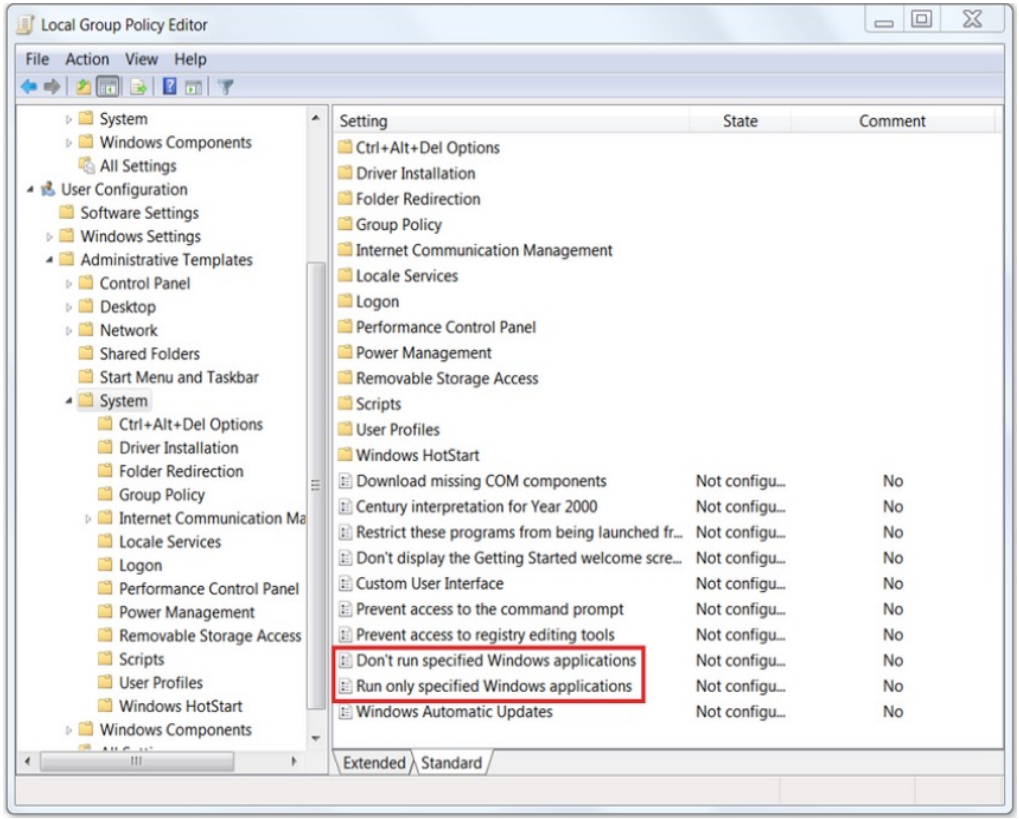
- Limiting access to potential threats by creating lists of prohibited applications is known as blacklisting.
- Application blacklists can dictate which user applications are not permitted to run on a computer.
- Whitelists specify which programs are allowed to run.
- In this way, known vulnerable applications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



Application Blacklisting and Whitelisting

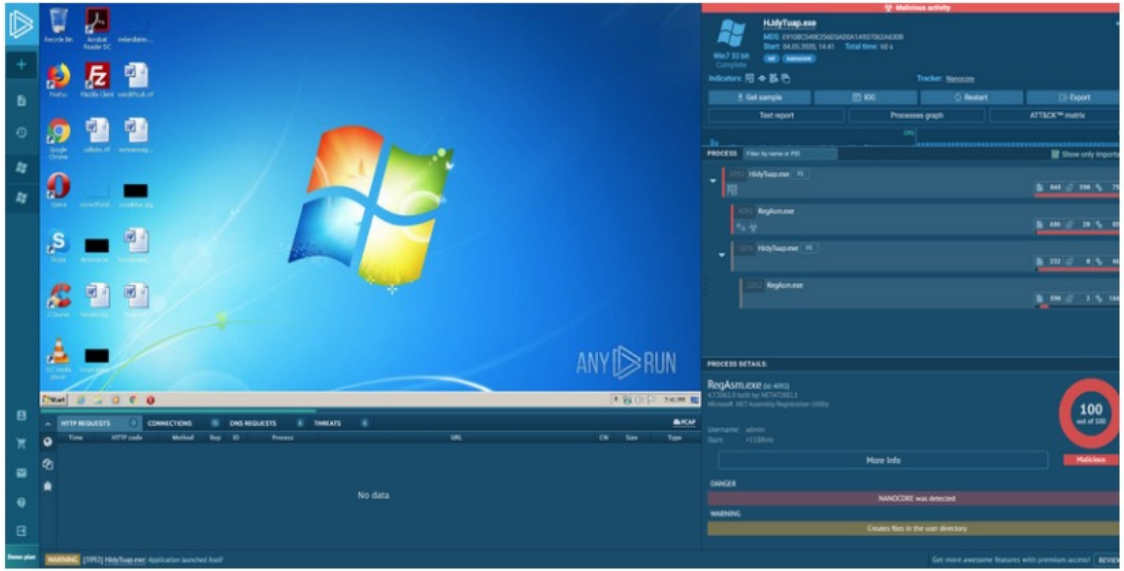
Application Blacklisting and Whitelisting (Contd.)

- 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.



New Terms and Commands

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

Lab 38 - Interpret HTTP and DNS Data to Isolate Threat Actor

In this lab, you will complete the following objective:

- Investigate SQL injection and DNS exfiltration exploits using Security Onion tools.