SYNERCOMM
SECURE • INTELLIGENT • NETWORKS

CIS Top 20 #8

Malware Defenses

Lisa Niles: CISSP, Director of Solutions Integration

CIS Top 20 Critical Security Controls

CSC # 8 – Malware Defenses

- *Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.*

CIS Controls™

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

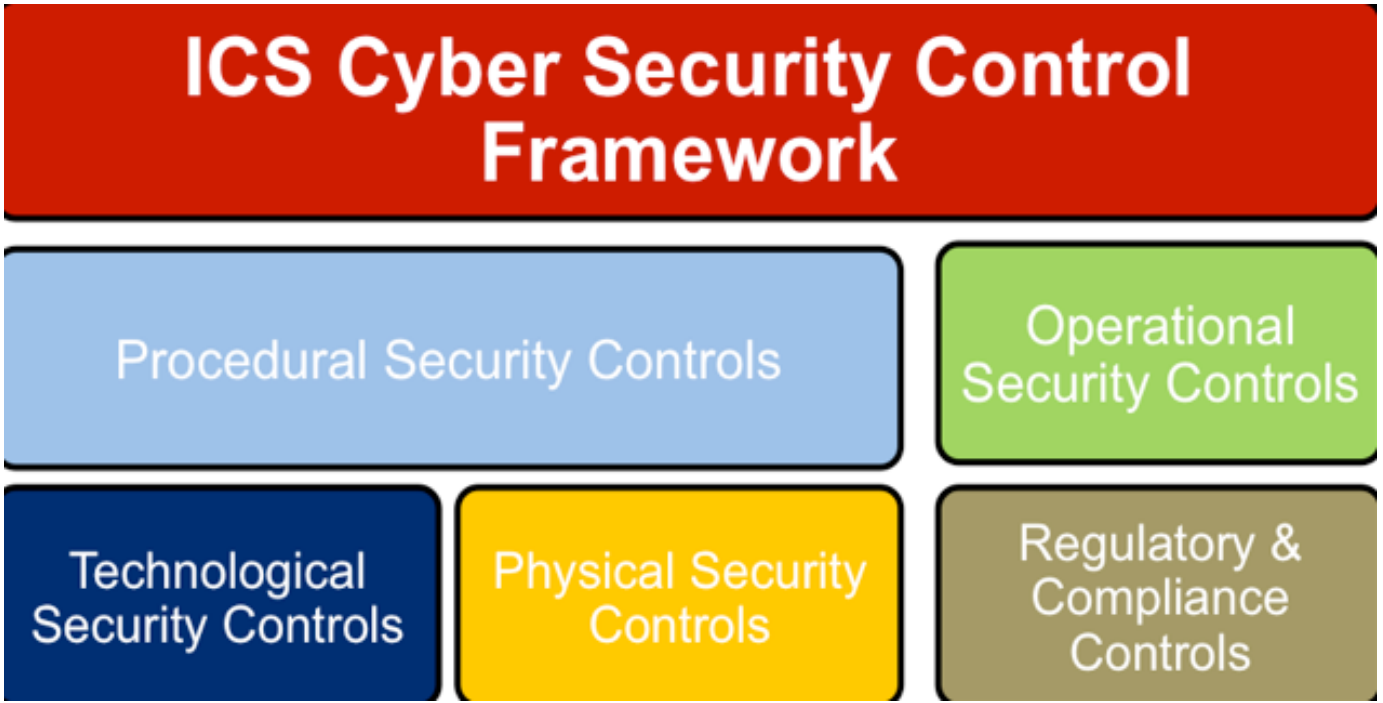
Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

CIS Top 20 Critical Security Controls



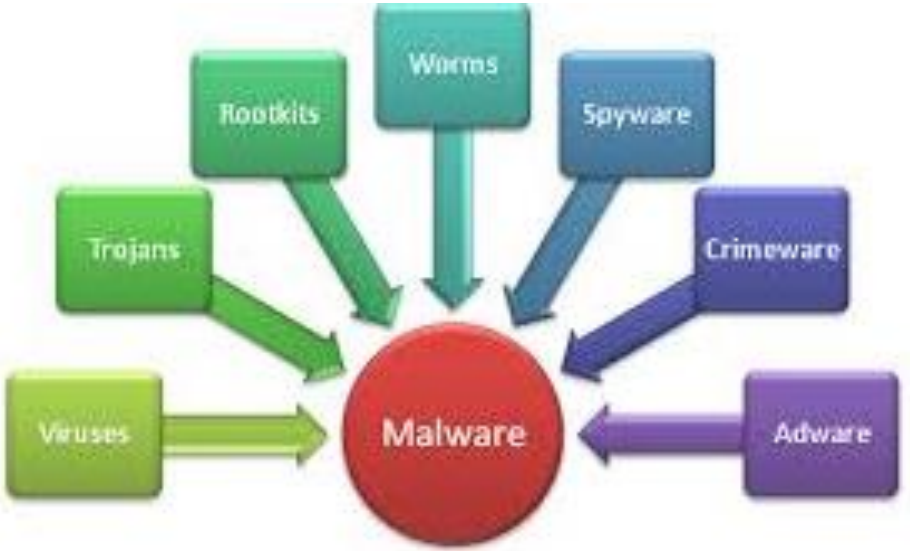
CIS Top 20 Critical Security Controls

- Before we jump into the waves of controls;
  - AV
  - Antimalware
  - EDR (Endpoint Detection and Response)
  - NGAV (Next Gen AV)
  - NGES (Next Gen Endpoint Solution)

- Lets define the difference between virus and malware?

CIS Top 20 Critical Security Controls

The term “malware” can be a little misleading



CIS Top 20 Critical Security Controls

- It leads to the conclusion that:
- **Virus is malware, but not all malware is a virus.**

CIS Top 20 Critical Security Controls

- How do EPP (Endpoint Protection Platforms)differ?
  - AV (antivirus)
  - Antimalware
  - NGAV (Next Gen AV)
  - EDR (Endpoint Detection and Response)
  - AEP (Advanced Endpoint Protection)

Cyber Kill Chain Case Study

CIS Top 20 Critical Security Controls

- **Antivirus software** is a piece of software originally designed to offer protection against computer viruses.

CIS Top 20 Critical Security Controls

- In this method, antivirus software are able to identify malicious files based on their structure, profile, or through certain string patterns encoded in them.

CIS Top 20 Critical Security Controls

Main features to look for in an antivirus program:

- Virus scanning,
- Blocks malicious script files and prevent them from running,
- Heuristic analysis
- Automatic updates
- Malware removal
- Database of known malware
- Ransomware protection Antivirus might also be packed with phishing protection, vulnerability scan, browser protection, system optimization.

CIS Top 20 Critical Security Controls

- Antimalware software protects against infections caused by many types of malware, including all types of viruses, as well as rootkits, ransomware and spyware

CIS Top 20 Critical Security Controls

- Antimalware software use three strategies to protect systems from malicious software;
  - Signature-based malware detection
  - Behavior-based malware detection
  - Sandboxing.

CIS Top 20 Critical Security Controls

- The main features to look for in antimalware software:
  - Scan, detect and remove known Trojans, adware, spyware, and other advanced malware
  - Acts like a shield and offers second generation malware protection
  - Is a malware removal tool
  - Automatic software updates to easily identify new online threats
  - Traffic filtering for your Internet activity to secure your PC against cyber threats and blocking access to infected servers, PCs.
  - Anti phishing protection is a feature that is focused on detecting and blocking scam and phishing websites.
  - Offer security against advanced exploit kits.
  - Protect against website involved in malware distribution
  - Provides a specialized malware database.

CIS Top 20 Critical Security Controls

- Why antivirus and antimalware (why you need both)
  - Multiple layers of protection
  - AV programs are more efficient and effective on the classic types (worms, virus, trojan, keyloggers)
  - Anti malware can detect and remove new and sophisticated malware strains and strengthen security.

CIS Top 20 Critical Security Controls

- NGAV is the natural (and much needed) evolution of traditional AV.
  - Protects computers from the full spectrum of modern cyber attacks
  - Prevents commodity malware better than traditional AV
  - Prevents unknown malware and sophisticated attacks by evaluating the *context of an entire attack* resulting in better prevention
  - Provides visibility and context to get to the root cause of a cyber attack and provide further attack context and insight
  - Remediates attacks (traditional AV simply stops mass malware)

CIS Top 20 Critical Security Controls

- Endpoint Detection and Response (**EDR**) is an emerging technology.
  - Category of solutions that focus on detecting, investigating, and mitigating suspicious activities and issues on hosts and endpoints.

CIS Top 20 Critical Security Controls

The main features that most EDR solutions have include:

- Detect and prevent hidden exploit processes that are more complex than a simple signature or pattern and evade traditional AV
- Threat intelligence
- Visibility throughout endpoints, including applications, processes and communications, to detect malicious activities and simplify incident response
- Automation of alerts, as well as defensive responses such as turning off specific processes when an attack is detected
- Forensic capabilities, deep dive into their activities so you can understand their movements and minimize the impact of the breach
- Data collection to build a repository used for analytics

CIS Top 20 Critical Security Controls

- AEP
  - Advanced Endpoint Protection is next-generation cyber security that blocks bad files and automatically contains unknown files
  - An AEP product must be able to detect, prevent, continuously monitor, and take action against threats while providing end-to-end visibility through event logs generated by the endpoint product.

CIS Top 20 Critical Security Controls

- Example attack lifecycle
- Banking Trojan Attacks
- The attack lifecycle – typical of banking Trojan:
- Stage 1: A spambot sends emails with Word attachments that contain malicious macros.
- Stage 2: Social engineering & embedded in the message with macros.
- Stage 3: The malicious VBScripts begin with “safety checks” to ensure they’ve landed on a suitable target.
- Stage 4: The malicious VBScripts download the malware payload, put it in the local file system and trigger its execution.

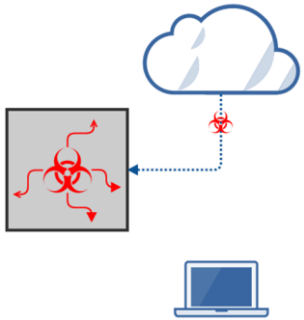
CIS Top 20 Critical Security Controls

Sandboxing and Behavior (Heuristic)

- In this type of scanning, the solution looks for certain behaviors or even commands that might be indicative of malicious actions.

CIS Top 20 Critical Security Controls

- Sandboxing
  - A sandbox is a secure virtual environment where executable files are sent for analysis.



CIS Top 20 Critical Security Controls

- Additional things to consider….

CIS Top 20 Critical Security Controls

- Log detection and responses
  - Enterprise-level antivirus and antimalware solutions have granular logging ability.

CIS Top 20 Critical Security Controls

- Scan removable media before it's allowed on anything, and limit who can install software.
- Removing local admin/root privileges

CIS Top 20 Critical Security Controls

- Watch your edges
  - Network-level scanning (CnC, malicious DNS and URLs)
  - IDS/IPS and logging (log session lengths, DNS requests, and traffic patterns to look for access)
  - Looking at inbound and outbound network traffic from unusual IP addresses,

CIS Top 20 Critical Security Controls

How to Get Started

Step 1. Gap Assessment.

2. Implementation Roadmap
3. Implement the First Phase of Controls
4. Integrate Controls into Operations
5. Report and Manage Progress

CIS Top 20 Critical Security Controls

8.1	Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers.
8.2	Employ anti-malware software that offers a centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying an update, automated systems should verify that each system has received its signature update.
8.3	Limit use of external devices to those with an approved, documented business need. Monitor for use and attempted use of external devices. Configure laptops, workstations, and servers so that they will not auto-run content from removable media, like USB tokens (i.e., “thumb drives”), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares. Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted.
8.4	Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased protection, deploy capabilities such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executables.
8.5	Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.
8.6	Enable domain name system (DNS) query logging to detect hostname lookup for known malicious C2 domains.

CIS Top 20 Critical Security Controls

- *8-1* - Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers.

- Tools:
  - TrendMicro, Kaspersky, Symantec, Sophos, Cylance, CarbonBlack, BitDefender, PaloAlto TRAPS

CIS Top 20 Critical Security Controls

- *8-2* - Employ anti-malware software that offers a centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying an update, automated systems should verify that each system has received its signature update.

- Free Tools
  - Notes: Any enterprise class AV/NGAV software will have this capability.
  - Tools to test AV are: AV-Test, AV-Comparatives, or Virus Bulletin.

CIS Top 20 Critical Security Controls

- *8-3* - Limit use of external devices to those with an approved, documented business need. Monitor for use and attempted use of external devices. Configure laptops, workstations, and servers so that they will not auto-run content from removable media, like USB tokens (i.e., “thumb drives”), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares. Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted.

- **Tools**
  - GPO
  - EPP solution

CIS Top 20 Critical Security Controls

- *8-4* - Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased protection, deploy capabilities such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executables.
- Tools:
  - Notes: This sounds like it can be complex, but it's really not. The DISA hardening guides provide step-by-step instructions on enabling these settings and so much more. If you implemented the hardening guidelines as outlined in Control 5, you're already ahead of the game.

CIS Top 20 Critical Security Controls

- *8-5* - Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.

CIS Top 20 Critical Security Controls

- *8-6* Enable domain name system (DNS) query logging to detect hostname lookup for known malicious C2 domains.

- **Notes**: This is a great passive way to monitor for malware in an environment. Sensors can log all of these queries without having to pull them off of the endpoint.
- Looking for new DNS queries and those that look to be computer-generated will be quick wins in terms of hunting out malware infections.

CIS Top 20 Critical Security Controls

- *Extra note:*
- Enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash.
- **Notes**: On high interaction systems, this can be quite noisy. From a forensics standpoint, it will be quite valuable. PowerShell and Bash are popular among malware families, but don't limit it to just those languages.

CIS Top 20 Critical Security Controls

- **Procedures and tools for implementing this control:**
  - Ensure anti-virus signatures are up to date
  - Verify that anti-virus, anti-spyware, and host-based IDS features are active on every device
  - Logging enabled for various command line tools, such as Windows PowerShell and Bash
  - Remove local admin or use MFA

CIS Top 20 Critical Security Controls

- **The Solution (tips):**
  1. Begin with the end in mind
  2. Know your audience (who is using the tool)
  3. Know what you mean by endpoint
  4. Start with a foundation of all the time visibility
  5. Keep track of your visibility data
  6. Know where you are exposed
  7. Continuous detection & response
  8. Consider forensics data
  9. Tear down the walls

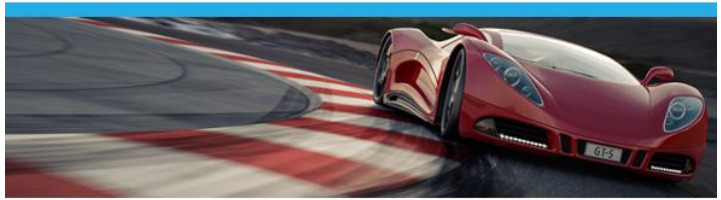
CIS Top 20 Critical Security Controls

Ask your vendor – how they handle:

1. False positives (detection accuracy)
2. Malware (known & unknown)
3. Viruses (Known & unknown)
4. HTTP
5. Email
6. Docs & Scripts
7. Offline threats
8. Unknown Threats
9. Exploits
10. Blended Threats
11. Evasive
12. Cleaning tool

ForeScout

SYNERCOMM



Experience the Difference of Agentless Visibility and Control

Put ForeScout CounterACT® through its paces in a real-time lab environment as you experience the difference of using agentless visibility and control in your IT, OT and IoT security efforts. During this three-hour, hands-on test drive, you'll see the before-and-after impact of using the ForeScout platform to automate:

1. **Asset Management.** Gain visibility of hardware/software you didn't know you had for an annual software audit.
2. **Device Compliance.** Streamline a security audit to determine if networked devices are running up-to-date security software. Create and apply a policy that notifies employees that they are out of compliance and confirms that systems are restored to company standards.
3. **Incident Response.** Respond to a WannaCry outbreak with an automated policy that quickly locates vulnerable hosts and determines which require patches and which are infected.
4. **Network Access Control.** Assess devices and restrict, block or quarantine non-compliant systems.
5. **Network Segmentation.** Tag non-compliant systems and use a Palo Alto Networks' NGFW to segment devices.

Experience the difference. Sign up today!

Register

When:

May 10th, 2018

8:30 a.m. - 11:30 a.m.

Where:

SynerComm Office

3265 Gateway Rd., Suite 650

Brookfield, WI 53045

(ISC)²®

CPE Credits Available

(ISC)² members who attend ForeScout's Test Drive Experience qualify for up to three continuing professional education credits. Please provide your (ISC)² membership number when you register.

SYNERCOMM

CIS Top 20 Critical Security Controls

Thank you for Attending.

Hope you can join us for the Complete CIS Top 20 CSC

Tuesday May 15th

CIC CSC # 9

Limitation and Control of Network Ports