CIS Top 20
#3
Secure Configuration of Hardware and Software

Lisa Niles – CISSP, Chief Solution Architect
CIS Top 20 Critical Security Controls

- Critical Governance and the CIS Critical Security Controls
CIS Top 20 Critical Security Controls

• How the CIS Critical Security Controls can help?
CIS Top 20 Critical Security Controls

• Sample:

• Governance item #1: Manage the known cyber vulnerabilities of your information and make sure the necessary security policies are in place to manage the risk.
  • At a minimum, you should be able to identify and manage the large volume of known flaws and vulnerabilities found in information technology and processes. The flowing CIS Critical Security Controls are the primary means to establish a baseline of responsible practices that can be measured, managed and reported.
  • CSC3: Secure Configurations of Hardware and Software
  • CSC#4: Continuous Vulnerability Assessment and Remediation
CIS Top 20 Critical Security Controls

• CIS CSC focus on various technical aspects of information security

• Outside of the technical realm, a comprehensive security program should also take into account:
  • Numerous additional areas of security
    • Policies
    • Procedures
    • Process
    • Organizational structure
    • Physical security.
CIS Top 20 Critical Security Controls

• What am I trying to protect?
• Where are my gaps?
• What are my priorities?
• Where can I automate?
CIS Top 20 Critical Security Controls

EXPANDING SECURITY CHALLENGE

PRIVATE CLOUD

IOT
INFRASTRUCTURE
LOCAL USERS

HEADQUARTERS

BRANCH

MOBILE

SaaS
PUBLIC CLOUD
CIS Top 20 Critical Security Controls

Confluence of Macro Trends Creating Visibility Challenges

Growth of Devices and Platform Diversity

- 280Bn IP-based devices by 2020

Cloud Adoption Creates New Challenges

- Multiple Device Locations and Access Points
- Heterogeneous Environment with Multiple Vendors
- De-centralized Management

IT and OT Convergence

- OT networks are no longer physically separated
- Threats moving between cyber and physical dimensions
- Assets are highly vulnerable and rarely can be patched
Implementing the Controls:

• Carefully plan

• Organizational structure

• “Governance, Risk, and Compliance (GRC)” program.

• Program managers
Basic Security Hygiene (Back to the Basics!)

- Know what you have (Inventory HW & SW)
- Limit what you don’t NEED (EOL, Services, Networks, Rights)
- Update your software
- Secure Default Configurations
- Employ Process Controls
CIS Top 20 Critical Security Controls

Who are you?
- Employee
- Partner
- Contractor
- Guest

Who owns your device?
- Corporate
- BYOD
- Rogue

What type of device?
- Windows, Mac
- iOS, Android
- VM
- Non-user devices, IoT

Where/how are you connecting?
- Switch/
- Port/PoE
- Wireless/Controller
- VPN
- IP, MAC
- VLAN

What is the device hygiene?
- Configuration
- Software
- Services
- Patches
- Security Agent
CIS Top 20 Critical Security Controls

First 5 CIS Controls
Eliminate the vast majority of your organization's vulnerabilities

Secure Your Organization

All 20 CIS Controls
Secure your entire organization against today's most pervasive threats

1: Inventory of Authorized and Unauthorized Devices
2: Inventory of Authorized and Unauthorized Software
3: Secure Configurations for Hardware and Software
4: Continuous Vulnerability Assessment and Remediation
5: Controlled Use of Administrative Privileges

6: Maintenance, Monitoring, and Analysis of Audit Logs
7: Email and Web Browser Protections
8: Malware Defenses
9: Limitation and Control of Network Ports
10: Data Recovery Capability
11: Secure Configurations for Network Devices
12: Boundary Defense
13: Data Protection
14: Controlled Access Based on the Need to Know
15: Wireless Access Control
16: Account Monitoring and Control
17: Security Skills Assessment and Appropriate Training to Fill Gaps
18: Application Software Security
19: Incident Response and Management
20: Penetration Tests and Red Team Exercises
CIS Top 20 Critical Security Controls

• Control #3

• Secure Configuration of Hardware and Software

• Key Principle Control:
  • Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, workstations, mobile devices using rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
CIS Top 20 Critical Security Controls

How to Get Started

Step 1. Gap Assessment.
Step 2. Implementation Roadmap
Step 3. Implement the First Phase of Controls
Step 4. Integrate Controls into Operations
Step 5. Report and Manage Progress
CIS Top 20 Critical Security Controls

Why is CIS Control 3 critical?

• CSC #3 is all about preventing exposure due to misconfiguration.

Most Breaches are Preventable

97% of breaches are avoidable through standard controls*

› No visibility of the environment
› Lack of actionable intelligence
› Disjointed security tools and data
› Lack of cross-functional expertise

Organizations don’t understand their attack surface

*According to Verizon Data Breach Investigation Report
### CIS Top 20 Critical Security Controls

<table>
<thead>
<tr>
<th>System</th>
<th>3.1</th>
<th>Establish standard secure configurations of your operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>3.2</td>
<td>Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise. Any existing system that becomes compromised should be re-imaged with the secure build. Regular updates or exceptions to this image should be integrated into the organization’s change management processes. Images should be created for workstations, servers, and other system types used by the organization.</td>
</tr>
<tr>
<td>System</td>
<td>3.3</td>
<td>Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.</td>
</tr>
<tr>
<td>System</td>
<td>3.4</td>
<td>Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.</td>
</tr>
<tr>
<td>System</td>
<td>3.5</td>
<td>Use file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. The reporting system should: have the ability to account for routine and expected changes; highlight and alert on unusual or unexpected alterations; show the history of configuration changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command). These integrity checks should identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes).</td>
</tr>
<tr>
<td>System</td>
<td>3.6</td>
<td>Implement and test an automated configuration monitoring system that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur. This includes detecting new listening ports, new administrative users, changes to group and local policy objects (where applicable), and new services running on a system. Whenever possible use tools compliant with the Security Content Automation Protocol (SCAP) in order to streamline reporting and integration.</td>
</tr>
<tr>
<td>System</td>
<td>3.7</td>
<td>Deploy system configuration management tools, such as Active Directory Group Policy Objects for Microsoft Windows systems or Puppet for UNIX systems that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals. They should be capable of triggering redeployment of configuration settings on a scheduled, manual, or event-driven basis.</td>
</tr>
</tbody>
</table>
### CSC 3.1 Establish standard secure configurations of your operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.

#### CSC 3.1 Procedure: Standardize configuration of operating system.

**The organization:**

1. IT department to build hardened OS configuration data base.
2. IT department will update hardened configurations as high risk vulnerabilities are identified.
3. IT department will push confirmation updates out to active devices

#### Metrics:

1. The IT department will maintain a list hardened configurations
2. The IT department will audit configurations monthly.
CIS Top 20 Critical Security Controls

- CSC 3 Procedures and Tools
- Start with publicly developed, vetted, supported benchmarks, security guides or checklists:
  - CISecurity.org
  - NIST (checklists.nist.gov)
  - DISA STIG’s
- Many tools available to measure (agent or agentless)
CIS Top 20 Critical Security Controls

• How to start..
• Automated discovery tool (MBSA) for Windows
• Use you CSC #1 & #2 inventories
  • Network devices (Firewalls, switches, routers, wifi)
• Create system baselines (CISecurity.org)
CIS Top 20 Critical Security Controls
CIS Top 20 Critical Security Controls
CIS Top 20 Critical Security Controls

• 3-1 Establish and ensure the use of standard secure configurations of your operating systems.

• Free Tools
  • DISA STIGs - DoD recommended secure systems baselines including phones, applications, OSes, network devices, etc...
  • MBSA - assessing missing security updates and less-secure security settings within Microsoft Windows
  • Cisecurity.org Baselines, hardening guides and templates.

• Commercial Tools
  • Qualys - Policy Compliance – automatic tech control assessment across network ***Also available for cloud resources
  • skybox - Policy Compliance, firewall audit, network map and modeling
3-2 Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise.

Free Tools

- Cisecurity.org Baselines, hardening guides and templates.
- FOG - Free and Open Source imaging from a central server based on Linux.

Commercial Tools

- Deep Freeze - Build a clean image, revert to it easily with a reboot.
- ManageEngine OS Deployer
CIS Top 20 Critical Security Controls

• 3-3 Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible.

• Free Tools
  • FOG - Free and Open Source imaging from a central server based on Linux.

• Commercial Tools
  • Deep Freeze - Build a clean image, revert to it easily with a reboot.
  • ManageEngine OS Deployst: OS Deployer automates the disk imaging and deployment process
  • Avecto - Offers Privilege Management, Application Control, and Sandboxing
CIS Top 20 Critical Security Controls

• 3-4 *Do all remote administration of servers, workstation, network devices, and similar equipment over secure channels.*

• This is referring to protocols, such as RDP, SSH, etc...

• **Free Tools**
  • [MRemoteNG](#) - All-in-one for remote access. does NOT support encrypted VNC.
  • [UltraVNC](#) - Offers a server and client which can provide encrypted VNC

• **Commercial Tools**
  • [RealVNC](#) - Feature rich VNC server/client
  • [RemoteDesktopManager](#) - Feature rich RDP client
  • [Centrify](#) - Secure and manage super user, service, and application accounts on servers and network devices, both on-premises and in the cloud.
CIS Top 20 Critical Security Controls

• 3-5 Utilize file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered...

• This is basically referring to a HIDS.

• Free Tools

  • AlienVault OSSIM - HIDS, SEIM, Inventory, Service Monitor, and more.
  • OSSEC - used in OSSIM, it is just the HIDS portion.
  • OpenHIDS - Windows only

• Commercial Tools

  • Tripwire - heterogeneous server monitoring across Windows, Linux, Solaris, AIX and HP-UX platforms.
CIS Top 20 Critical Security Controls

- Implement and test an automated configuration monitoring system that measures all secure configuration elements that can be measured through remote testing using features such as those included with tools compliant with Security Content Automation Protocol (SCAP), and alerts when unauthorized changes occur.

- **Free Tools**
  - **AlienVault OSSIM** - HIDS, SEIM, Inventory, Service Monitor, and more.
  - **OSSEC** - used in OSSIM, it is just the HIDS portion.
  - **OpenHIDS** - Windows only
  - **SCM** – Microsoft’s Security Compliance manager
  - **nmap** – Security Scanner, Port Scanner, & Network Exploration Tool.

- **Commercial Tools**
  - **ForeScout** - see devices, control them and orchestrate system-wide wired and wireless campus, data center, cloud and operational technology deployments without agents.
  - **Qualys** – Unparalleled visibility and control of all your assets
  - Skybox – as mentioned earlier
CIS Top 20 Critical Security Controls

• 3-7 Deploy system configuration management tools, such as Active Directory Group Policy Objects for Microsoft Windows systems or Puppet for UNIX systems that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.

• Free Tools
  • Salt - Meant for deploying change management to ANY scale. Great for cloud deployments with OpenStack.
  • Puppet - GPMC for Linux. Kind of.

• Commercial Tools
  • Chef - The Chef client is installed on each server, virtual machine, container, or networking device you manage. The client periodically polls Chef server latest policy and state of your network. If anything on the node is out of date, the client brings it up to date.
  • Ansible - Deploy apps. Manage systems. Centrally managed.
CIS Top 20 Critical Security Controls

**NOTIFY**
- Open trouble ticket
- Send email notification
- SNMP Traps
- Start application
- Run script to install application
- Auditable end-user acknowledgement
- HTTP browser hijack
- Trigger endpoint management system

**COMPLY**
- Deploy a virtual firewall
- Reassign the device to a VLAN
- Update access lists
- DNS hijack (captive portal)
- Move device to a guest network

**RESTRICT**
- Move device to quarantine VLAN
- Block access with 802.1x
- Alter login credentials to block access
- Block access with device authentication
- Turn off switch port (802.1x, SNMP)
- Wi-Fi port block
- Terminate applications
- Disable peripheral device
CIS Top 20 Critical Security Controls
CIS Top 20 Critical Security Controls

Skybox - Vulnerability Control

Vulnerability Occurrence Analysis - Exposed Vulnerabilities

<table>
<thead>
<tr>
<th>Exposure</th>
<th>TID</th>
<th>Stack</th>
<th>ID</th>
<th>OS</th>
<th>Assult</th>
<th>DB</th>
<th>Service Ports</th>
<th>Content Header</th>
<th>Original</th>
<th>Risk</th>
<th>Credibility</th>
<th>Host Tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>TID</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Vulnerability Occurrence Analysis - Internal Memory Disclosure Vulnerability

<table>
<thead>
<tr>
<th>Title</th>
<th>Exposure</th>
<th>Description</th>
<th>Risk</th>
<th>Credibility</th>
<th>Host Tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>RDP Internal Memory Disclosure Vulnerability</td>
<td>Direct</td>
<td>BID 4, BID 5 show remote access to sensitive information such as environment variables.</td>
<td>Direct</td>
<td>Host Tags</td>
<td></td>
</tr>
</tbody>
</table>
CIS Top 20 Critical Security Controls

### Critical Security Controls Initial Assessment Tool (v6.0a)

<table>
<thead>
<tr>
<th>Maturity level:</th>
<th>Description:</th>
<th>Score:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level One</td>
<td>Policies Complete</td>
<td>0.25</td>
</tr>
<tr>
<td>Level Two</td>
<td>Controls 1-5 Implemented</td>
<td>0.40</td>
</tr>
<tr>
<td>Level Three</td>
<td>All Controls Implemented</td>
<td>0.31</td>
</tr>
<tr>
<td>Level Four</td>
<td>All Controls Automated</td>
<td>0.22</td>
</tr>
<tr>
<td>Level Five</td>
<td>All Controls Reported</td>
<td>0.06</td>
</tr>
</tbody>
</table>

**Maturity Rating**: 1.239

*Rating is on a 0-5 scale.

### Maturity Level Aggregate Scores

<table>
<thead>
<tr>
<th>Category</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies Complete</td>
<td>0.25</td>
</tr>
<tr>
<td>Controls 1-5 Implemented</td>
<td>0.40</td>
</tr>
<tr>
<td>All Controls Implemented</td>
<td>0.31</td>
</tr>
<tr>
<td>All Controls Automated</td>
<td>0.22</td>
</tr>
<tr>
<td>All Controls Reported</td>
<td>0.06</td>
</tr>
</tbody>
</table>

### Total Completion (by CSC)

- Policies Complete: 47%
- Controls 1-5 Implemented: 41%
- All Controls Reported: 22%
- All Controls Automated: 19%
- All Controls Implemented: 28%
- All Controls Reported: 25%
- Policies Complete: 18%
- Controls 1-5 Implemented: 25%
- All Controls Reported: 26%
- All Controls Automated: 28%
- All Controls Implemented: 19%
- Policies Complete: 0%
- Controls 1-5 Implemented: 0%
- All Controls Reported: 0%
- All Controls Automated: 0%
CIS Top 20 Critical Security Controls

- Center for Internet Security (CIS): https://www.cisecurity.org/
- Auditscripts resources (provided by James Tarala, CSC Editor): https://www.auditscripts.com/free-resources/critical-security-controls/
- STIG https://iase.disa.mil/stigs/Pages/index.aspx
# CIS Top 20 Critical Security Controls

The SANS Best of Awards are not driven by vendors, but by the people actually using these products. The Awards are an extension of the SANS WhatWorks Program which creates awareness of security programs and solutions that are actually being used to stop bad guys and improve security. The 2016 winners can be found below.

## The Best of 2016 Award winners and Honorable Mentions

<table>
<thead>
<tr>
<th>Category</th>
<th>Winner</th>
<th>Honorable Mention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Assessment</td>
<td><strong>Winner:</strong> Tenable Nessus</td>
<td><strong>Honorable Mention:</strong> Rapid7, Qualys</td>
</tr>
<tr>
<td>End Point Protection</td>
<td><strong>Winner:</strong> Cylance Protect</td>
<td><strong>Honorable Mention:</strong> Symantec, Trend Micro</td>
</tr>
<tr>
<td>Threat Intelligence</td>
<td><strong>Winner:</strong> CrowdStrike Falcon Intelligence</td>
<td><strong>Honorable Mention:</strong> FireEye Threat Intelligence, Cisco ThreatGrid</td>
</tr>
<tr>
<td>Next Generation Firewall</td>
<td><strong>Winner:</strong> Palo Alto Networks PA Series</td>
<td><strong>Honorable Mention:</strong> CheckPoint Software, Fortinet</td>
</tr>
<tr>
<td>Application Security</td>
<td><strong>Winner:</strong> Qualys WAS</td>
<td><strong>Honorable Mention:</strong> Rapid7, Checkmarx (tie), Veracode (tie)</td>
</tr>
<tr>
<td>Advanced Threat Detection</td>
<td><strong>Winner:</strong> FireEye Intrusion NX</td>
<td><strong>Honorable Mention:</strong> Snort, Cisco</td>
</tr>
<tr>
<td>SIEM</td>
<td><strong>Winner:</strong> LogRhythm Security Intelligence Platform</td>
<td><strong>Honorable Mention:</strong> Splunk, IBM</td>
</tr>
<tr>
<td>Endpoint Detection/Response</td>
<td><strong>Winner:</strong> Carbon Black Platform</td>
<td></td>
</tr>
</tbody>
</table>
Thank you for Attending.

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

Tuesday March 6th
CIC CSC #4 – Continuous Vulnerability & Remediation