CIS Top 20
#2
Inventory of Authorized and Unauthorized Software

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

• Introduction

• Many CISOs wonder where they should optimize processes and focus their resources to reduce security risk

• The CIS Critical Security Controls are 20 prioritized, vetted, and well supported security actions to assess and improve cyber security.

• Validating your security controls and processes against the CIS Top 20 can help secure your organization’s assets, infrastructure, and information

• CSC strengthen your security posture: continuous, automated protection and monitoring

• “Offense must inform defense” approach to select and prioritize CSC
CIS Top 20 Critical Security Controls

• While the CSCs are broken down into 20 separate controls, the authors recognize that organizations need a place to start.

• The control sequence reflects their impact, from one to 20.

• Within each control, sub-levels provide further guidance so that every organization can experience “quick wins,” gain “visibility and attribution” of assets in their infrastructure, and improve “configuration and hygiene” of assets to reduce exposure to threats.

• CSCs relevant to any organization, even if solely as a means to validate that existing efforts meet “due care” expectations for cybersecurity.
CIS Top 20 Critical Security Controls

• The Controls are specific guidelines that CISOs, CIOs, CTOs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses.

• They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical threat and highest payoff defenses, while providing a common baseline for action against risks that we all face.
CIS Top 20 Critical Security Controls

• The control areas in the CIS CSC focus on various technical aspects of information security

• Primary goal of supporting organizations in prioritizing their efforts in defending against today’s most common and damaging attacks.

• Outside of the technical realm, a comprehensive security program should also take into account:
  • Numerous additional areas of security, including overall policy, organizational structure, personnel issues (e.g., background checks, etc.), and physical security.

• To help maintain focus, the controls in this document do not deal with these important, but non-technical, aspects of information security.

• Organizations should build a comprehensive approach in these other aspects of security as well
Because IT controls are just one aspect of being compliant, you may ask why IT compliance is such an important topic.

The answer is, quite simply, that it’s because the vast majority of business and government today is done through or with information technology.
Most IT compliance requirements start at the top with laws and regulations.

They articulate the ‘policies’ governing their requirements.

Policies, in turn, have their own operating requirements for compliance.

These organizations use standards as guidance for operational policies used to comply with the laws.

Those same standards, combined with related methodologies, are the basis used by auditors to test policy controls and certify compliance.
CIS Top 20 Critical Security Controls

• Maintaining your perspective starts with understanding your organization’s policy control objectives.

• This is a fancy way of saying, ‘What are you trying to protect or control’

• Understand the types of controls that make up your compliance universe.

• Companies often focus only on controls for data security and overlook other key areas such as:
  
  • **Administrative controls**: policies, procedures, and processes associated with the control objectives.
  
  • **Physical and environmental controls**: the physical protection of electronic and non-electronic information or assets. Examples are door locks, camera monitoring, and fire suppression.
  
  • **Logical controls**: the control of access to specific networks and resources by an authorized user; generally managed by information technology.
What is an IT security framework?

- An information security framework is a series of documented processes that are used to define policies and procedures around the implementation and ongoing management of information security controls in an enterprise environment.

- These frameworks are basically a "blueprint" for building an information security program to manage risk and reduce vulnerabilities. Information security teams can utilize these frameworks to define and prioritize the tasks required to build security into an organization.

- NIST Cybersecurity Framework, NIST guidelines, and the ISO 27000 series or regulations such as PCI DSS, HIPAA, NERC CIP, FISMA
CIS Top 20 Critical Security Controls

CSC guiding principles:

• Defenses should focus on addressing the most common and damaging attacks

• Enterprise environments must ensure consistent controls across an enterprise to effectively negate attacks. (not 80%)

• Defenses should be automated where possible, and periodically or continuously measured using automated measurement techniques where feasible.
The five critical tenets of an effective cyber defense system as reflected in the CIS Critical Security Controls are:

- Offense informs defense
- Prioritization
- Metrics
- Continuous diagnostics and mitigation
- Automation
CIS Top 20 Critical Security Controls

- Prevent, detect, remediate, report
- Rinse and repeat
CIS Top 20 Critical Security Controls

• Getting Started: Key Questions
  • What am I trying to protect?
  • Where are my gaps?
  • What are my priorities?
  • Where can I automate?
  • How can my vendor partners help?
CIS Top 20 Critical Security Controls
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
- Secure Web Apps
General Guidance for Implementing the Controls:

- Carefully plan.
- Organizational structure for program’s success.
- Establish a “Governance, Risk, and Compliance (GRC)” program.
- Assigning program managers
CIS Top 20 Critical Security Controls

Defining a Strong Security Team/Program

- Basic security hygiene
- Security Operations Center processes and tools
- “Business Security Analysts”

- Integration into procurement, M&A, supply chain decisions
- Cross-industry participation
CIS Top 20 Critical Security Controls

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

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

Secure Your Organization

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

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 #2
• Inventory of Authorized and Unauthorized Software
• Key Principle Control:
  • Control #2 focuses on knowing all software that is installed on servers and workstations & devices throughout your organization
CIS Top 20 Critical Security Controls

Securing: IoT Security

- Explosion of varying types of IoT endpoints creates a **broad attack surface**

- IoT security-related technology disruptions can be broken down into the following:
  - Asset discovery, profiling and tracking
  - Authentication
  - Network-based protection
  - Secure software development
  - Visibility through monitoring, detection and response

- The **integration** of these IoT security technologies with traditional IT and operational technology (OT) security infrastructures and practices **remains a challenge**

- Latest disruptive trends and developments:
  - IoT endpoint threats
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

- Successful implementation of the Controls will require many organizations to shift their mindset on security and how they approach IT operations and defense.
- No longer can employees be allowed to install software at random or travel with sensitive data in their pockets.
- A BIG change in mindset on this control CSC#2 inventory of software deals with the change in mindset with allowing the “Local admin” credentials on devices.
CIS Top 20 Critical Security Controls

- Why is CIS Control 2 critical?
- An organization without the ability to inventory and control its computers' installed programs makes its systems more vulnerable to attack.
- The vast majority of attacks are leveraging vulnerabilities in software.
- Self contained .exe viruses are old school.
- In order to combat this potential threat, an organization should scan a network and identify known or responding hosts and applications to help prioritize patching, removal, blocking, quarantine, alerting
CIS Top 20 Critical Security Controls

<table>
<thead>
<tr>
<th>Inventory of Authorized and Unauthorized Software</th>
<th>2.1</th>
<th>Protect</th>
<th>Software Whitelisting System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment of application whitelisting technology that allows systems to run software only if it is included on the whitelist and protects execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Inventory of Authorized and Unauthorized Software</th>
<th>2.2</th>
<th>Protect</th>
<th>Software Whitelisting System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment of software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. The software inventory systems must be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Inventory of Authorized and Unauthorized Software</th>
<th>2.3</th>
<th>Identify</th>
<th>Software Application Inventory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual machines and/or air-gapped systems should be used to isolate and run applications that are required for business operations but based on higher risk should not be installed within a networked environment. Establish standard secure configurations of your operating systems and</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Inventory of Authorized and Unauthorized Software</th>
<th>2.4</th>
<th>Protect</th>
<th>OS Virtualization System</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## CIS Top 20 Critical Security Controls

<table>
<thead>
<tr>
<th>Sub-Control</th>
<th>Description</th>
<th>Control</th>
<th>Security Technology Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>File Integrity monitoring</td>
<td>This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.</td>
<td>Tenable, Qualys, Rapid 7, Tripwire, Solarwinds, LogRhythm, Alienvault</td>
</tr>
<tr>
<td>2.2</td>
<td>Whitelisting</td>
<td>Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software</td>
<td>Windows (app locker, config manager, Policy PAK) Tenable, Qualys, Rapid 7, Alienvault</td>
</tr>
<tr>
<td>2.3</td>
<td>Inventory of Authorized Software</td>
<td>Perform regular scanning for unauthorized software. A change-control process should also be implemented to control any changes or installation of (executable files, DLLs, other libraries, etc.) are found</td>
<td>Tenable, Qualys, Rapid7</td>
</tr>
<tr>
<td>2.4</td>
<td>Inventory of Authorized Software</td>
<td>Virtual Machines should be isolated/air gapped</td>
<td>Vmware NSX firewalls, Virtual Box, Comodo</td>
</tr>
</tbody>
</table>
CIS Top 20 Critical Security Controls

CSC 2.1 Requirement: Inventory of Authorized and Unauthorized Software

CSC 2.1 Procedure: Software Inventory

<table>
<thead>
<tr>
<th>The organization:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Departments will document and clearly define what authorized and unauthorized software are in their respective areas.</td>
</tr>
<tr>
<td>2. Departments will update the Assets inventory reports and auditors of inventory software.</td>
</tr>
<tr>
<td>3. Departments will spot check devices monthly to ensure that they are authorized</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Metrics:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The IT department will maintain a list of whitelist &amp; blacklisted software</td>
</tr>
<tr>
<td>2. The IT department spot check each department every 6-months</td>
</tr>
</tbody>
</table>
CSC 2 Procedures and Tools

The Control requires both technical and procedural actions;

• In order to combat this potential threat, an organization should scan a network and identify known or responding applications

• Commercial software and Free inventory tools are widely available.

• The best tools provide an inventory check of hundreds of common applications, pulling information about the patch level of each installed program.

• This ensures that it is the latest version and that it leverages standardized application names, like those found in the Common Platform Enumeration (CPE) specification
CIS Top 20 Critical Security Controls

• How to start..

• Automated asset/application inventory discovery tool

• Create a list of authorized software/version (IoT)

• File integrity checking tools to validate that the authorized software has not been modified.

• Application whitelisting that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system.

• Vulnerability prevention tools to protect against Zeroday and unpatchables

• Segmentation-- IoT and other “unpatchables”
CIS Top 20 Critical Security Controls

• 2-1 - *Deploy application whitelisting technology*

• **Free Tools**
  
  • [RunAsSPC](#) - While not an application whitelist, it can allow users to run applications which require elevation

• **Commercial Tools**
  
  • If you have Enterprise Edition of Windows, you can use [Software Restriction Policies](#) with [AppLocker](#).
  
  • If you have Windows 8, You can use [application whitelisting for child accounts](#).
  
  • [PowerBroker](#) - Powerful tool to escalate privileges and take care of pesky UNC. Solution for Windows and Linux.
  
  • [PolicyPak](#) - Integrates with Group Policy
  
  • [Dell Authority Management Suite](#) - Centralized, secure and consistent desktop management software for Windows environments.
  
  • [Avecto](#) - Offers Privilege Management, Application Control, and Sandboxing
  
  • [Centrify Server Suite](#) - Windows and Linux application and Privilege control.
CIS Top 20 Critical Security Controls

• 2-2 - Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.

• This item goes hand-in-hand with control 2-1. Your whitelist of software will be your list of authorized software.

• Free Tools
  • Spiceworks - Scans for software (Inventory > Software) but not for whitelisting or application control. Can be configured to alert you if it detects potentially unwanted software.
  • AlienVault OSSIM - Can monitor file system changes and alert you when something is accessed, changed, or tampered with.

• Commercial Tools
  • AlienVault USM - Commercial version of OSSIM, provides persistent logging for SIEM.
  • Tripwire - Develop secure system baselines and monitor changes to file systems.
CIS Top 20 Critical Security Controls

• 2-3 - Perform regular scanning for unauthorized software and generate alerts when it is discovered on a system. A strict change-control process should also be implemented to control any changes or installation of software to any systems on the network.

• Free Tools
  • May be able to leverage existing tools (AV, etc)

• Commercial Software
  • **Nessus** - This dashboard tracks assets that have unauthorized software installed on them. It also lists the most common types of software, services and the frequency of software installations.
CIS Top 20 Critical Security Controls

• 2-4 - Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. Furthermore, the tool should record not only the type of software installed on each system, but also its version number and patch level.

• Free Tools
  • Spiceworks - does this pretty well.

• Commercial Tools
  • LAN Sweeper - Audit and find software, but also centrally deploy software.
CIS Top 20 Critical Security Controls

• 2-5 - The software inventory systems must be integrated with the hardware asset inventory so that all devices and associated software are tracked from a single location.
  • Many of the tools listed above can do this.

• 2-6 - Dangerous file types (e.g., .exe, .zip, .msi) should be closely monitored and/or blocked.
  • Many of the tools listed above can do this.
CIS Top 20 Critical Security Controls

• 2-7 - Virtual machines and/or air-gapped systems should be used to isolate and run applications that are required for business operations but based on higher risk should not be installed within a networked environment.

• Free Tools
  • VirtualBox
  • Comodo Internet Security - Allows you to run applications within a virtual desktop and sandbox environment. [How to configure.](#)
  • Comodo Dragon - Chrome based browser, has a virtual sandbox mode.
  • Comodo Ice Dragon - Firefox based browser, has a virtual sandbox mode.
2-8 - Configure client workstations with non-persistent, virtualized operating environments that can be quickly and easily restored to a trusted snapshot on a periodic basis.

This control specifically states "virtual environments". While we cannot all jump to VDI, nor see the need to, these are alternatives that I believe can meet the core requirements of the control.

Free Tools
- **FOG** - while not exactly what the control specifies, it can offer a clean slate in the need of a restore. Centralized server, based on PXE booting.

Commercial Tools
- **ShadowProtect** - Backup software that has the ability to revert to previous snapshots/save points across any hardware/VM platform.
- **DeepFreeze** - protects endpoints by Freezing a snapshot of a workstation’s desired configuration and settings set by the IT Admin. With an instant reboot, any unwelcome or unwanted changes are removed from the system, restoring it to its pristine frozen state.
CIS Top 20 Critical Security Controls

• 2-9 - **Deploy software that only provides signed software ID tags.** A software identification tag is an XML file that is installed alongside software and uniquely identifies the software, providing data for software inventory and asset management.

• **Tools**
  - Windows, Apple, Symantec
CIS Top 20 Critical Security Controls

• CSC 2 Procedures and Tools

• Start with an initial assessment from these tools to begin the process of realizing what software is installed and leverage them
  • Free or low-cost
    • Spiceworks
    • PDQ Inventory
    • Microsoft Intune
  • Enterprise
    • McAfee, Trend Micro, Symantec Endpoint Security
    • Microsoft System Center Configuration Manager (SCCM)
    • Tenable.io, Rapid7 Nexpose/InsightVM, Qualys
CIS Top 20 Critical Security Controls

• More tools:
  • WMIC – Windows Management Instrumentation Command-line lists software on given systems (Command line Kung Fu blog)
  • Psexec tool from Microsoft can perform software inventory that do not use standard Windows installer
    • @echo off
    • Psexec dir *.exe>%computername%_ExeFound.txt
    • Attack.mitre.org  Great site to see, use published attack vectors for validation testing
Application Whitelisting Techniques

- Probably already available in your environment
  - Software Restriction Policies
  - Microsoft AppLocker Policies
  - AppArmor/SeLinux
- Endpoint Security Products
  - Symantec, Trend, Carbon Black, etc.
CIS Top 20 Critical Security Controls

- Now for some Enterprise type solutions..
CIS Top 20 Critical Security Controls

<table>
<thead>
<tr>
<th>Title</th>
<th>Impact</th>
<th>Severity</th>
<th>Published</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analysis of ROK exploit kit weaponizing CVE-2019-1130</td>
<td>5</td>
<td>40 days ago</td>
<td></td>
</tr>
<tr>
<td>Avast AVA vulnerabilities</td>
<td>1</td>
<td>3/0/2016</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows under active attack</td>
<td>3</td>
<td>2/12/2019</td>
<td></td>
</tr>
<tr>
<td>Adobe Flash Player under new 0-day attack</td>
<td>15</td>
<td>4/6/2016</td>
<td></td>
</tr>
<tr>
<td>Adobe Flash partial 0-day patched in DBS mode</td>
<td>15</td>
<td>4/4/2016</td>
<td></td>
</tr>
<tr>
<td>Assets with easily exploitable vulnerabilities</td>
<td>168</td>
<td>0.2%</td>
<td></td>
</tr>
<tr>
<td>Assets with public exploit available</td>
<td>344</td>
<td>12.7%</td>
<td></td>
</tr>
<tr>
<td>Assets with potentially high impact</td>
<td>262</td>
<td>5.6%</td>
<td></td>
</tr>
<tr>
<td>Assets with high lateral movement vulnerabilities</td>
<td>304</td>
<td>0.1%</td>
<td></td>
</tr>
<tr>
<td>Assets vulnerable to active DOS</td>
<td>180</td>
<td>4.4%</td>
<td></td>
</tr>
<tr>
<td>Assets with patchable vulnerabilities aged 30 days</td>
<td>336</td>
<td>1.0%</td>
<td></td>
</tr>
<tr>
<td>Assets with unpatchable vulnerabilities</td>
<td>15</td>
<td>8.3%</td>
<td></td>
</tr>
</tbody>
</table>
CIS Top 20 Critical Security Controls

- Now for a few Enterprise packages:
Even AWS is recommending the CIS

**COMPLIANCE REPORTING FOR AWS**

- Actively report on security compliance of cloud accounts
  - Evaluates 50+ security best practices for AWS
  - On-demand report generation from the console
  - Designed for the CIO/CISO and compliance teams
- Interactive dashboard for SecOps & SOC team
CIS Top 20 Critical Security Controls

AuditScripts

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

Maturity level: Description: Score:
Level One: Policies Complete: 0.25
Level Two: Controls 1-5 Implemented: 0.40
Level Three: All Controls Implemented: 0.31
Level Four: All Controls Automated: 0.22
Level Five: All Controls Reported: 0.06

Maturity Rating*: 1.239
*Rating is on a 0-5 scale.

Maturity Level Aggregate Scores

Total Completion (by CSC)

Policies Complete: 0.25
Controls 1-5 Implemented: 0.40
All Controls Implemented: 0.31
All Controls Automated: 0.22
All Controls Reported: 0.06

22% 19% 25% 25% 18% 25% 19% 28% 27% 26% 47% 41% 0% 14% 28% 16% 0% 8% 19% 0%
CIS Top 20 Critical Security Controls

ATT&CK Matrix for Enterprise

The full ATT&CK Matrix below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the threat models.

<table>
<thead>
<tr>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Execution</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Command and Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>bash_profile and bash</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>AppleScript</td>
<td>AppleScript</td>
<td>Audio Capture</td>
<td>Automated Exfiltration</td>
<td>Commonly Used Port</td>
</tr>
<tr>
<td>Accessibility Features</td>
<td>Accessibility Features</td>
<td>Binary Padding</td>
<td>Bash History</td>
<td>Application Window Discovery</td>
<td>Application Deployment Software</td>
<td>Command-Line Interface</td>
<td>Automated Collection Data Compressed</td>
<td>Communication Through Removable Media</td>
<td></td>
</tr>
<tr>
<td>AppCert DLLs</td>
<td>AppCert DLLs</td>
<td>Bypass User Account Control</td>
<td>Brute Force</td>
<td>File and Directory Discovery</td>
<td>Distributed Component Object Model</td>
<td>Dynamic Data Exchange</td>
<td>Browser Extensions Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>AppInit DLLs</td>
<td>AppInit DLLs</td>
<td>Clear Command History</td>
<td>Credential Dumping</td>
<td>Network Service Scanning</td>
<td>Exploitation of Vulnerability</td>
<td>Execution through API</td>
<td>Clipboard Data</td>
<td>Data Transfer Size Limits Custom Command and Control Protocol</td>
<td></td>
</tr>
<tr>
<td>Application Shimming</td>
<td>Application Shimming</td>
<td>Code Signing</td>
<td>Credentials in Files</td>
<td>Network Share Discovery</td>
<td>Logon Scripts</td>
<td>Execution through Module Load</td>
<td>Data Staged</td>
<td>Exfiltration Over Alternative Protocol Custom Cryptographic Protocol</td>
<td></td>
</tr>
<tr>
<td>Authentication Package</td>
<td>Bypass User Account Control</td>
<td>Component Firmware</td>
<td>Exploitation of Vulnerability</td>
<td>Peripheral Device Discovery</td>
<td>Pass the Hash</td>
<td>Graphical User Interface</td>
<td>Data from Local System</td>
<td>Exfiltration Over Command and Control Channel Data Encoding</td>
<td></td>
</tr>
<tr>
<td>Bootkit</td>
<td>DLL Search Order Hijacking</td>
<td>Component Object Model Hijacking</td>
<td>Forced Authentication</td>
<td>Permission Groups Discovery</td>
<td>Pass the Ticket</td>
<td>InstallUtil</td>
<td>Data from Network Shared Drive</td>
<td>Exfiltration Over Other Network Medium Data Obfuscation</td>
<td></td>
</tr>
</tbody>
</table>

Follow @MITREattack
Last 5 Pages Viewed
Adversarial Tactics, Techniques & Common Knowledge
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Inventory of Authorized and Unauthorized Devices</td>
<td></td>
<td></td>
<td>Tenable, Qualys, Infoblox, Forescout</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Inventory of Authorized and Unauthorized Software</td>
<td></td>
<td></td>
<td>Tenable, Qualys, Infoblox, Carbonblack</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Secure Configuration of end-user devices</td>
<td></td>
<td></td>
<td>Tenable, Rapid7</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Continuous Vulnerability &amp; remediation</td>
<td></td>
<td></td>
<td>Qualys, Tenable, Rapid7</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Controlled Use of Administrative privileges</td>
<td></td>
<td></td>
<td>Centrify, CyberArk, BeyondTrust, Okta</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Maintenance, Monitoring and Analysis of Audit Logs</td>
<td></td>
<td></td>
<td>SolarWinds, Log Rhythm</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Email and Web Browser Protection</td>
<td></td>
<td></td>
<td>Barracuda, Proofpoint, zScaler, Fireeye (Web - Palo, Checkpoint, Forcepoint)</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Malware Defense</td>
<td></td>
<td></td>
<td>Bitdefender, carbonblack, PaloAlto TRAPS, Sophos, TrendMicro</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Limitation &amp; Control of network Ports, protocols, and Service</td>
<td></td>
<td></td>
<td>PaloAlto, Juniper, Checkpoint, Fortinet</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Data Recovery Capability</td>
<td></td>
<td></td>
<td>Barracuda</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Boundry Defense</td>
<td></td>
<td></td>
<td>PaloAlto, Juniper, Checkpoint, Fortinet</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Data Protection</td>
<td></td>
<td></td>
<td>Rapid7, tenable, Imperva, Infoblox, PaloAlto</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Controlled Access Based on Need to Know</td>
<td></td>
<td></td>
<td>Centrify, OKTA</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Wireless Access Control</td>
<td></td>
<td></td>
<td>Aerohive with 802.1x &amp; WIPS/PFW</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Account Monitoring and Control</td>
<td></td>
<td></td>
<td>Centrify, Beyond Trust, OKTA, A&amp;A training</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Security Skills Assessment and Appropriate Training</td>
<td></td>
<td></td>
<td>A&amp;A training</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Application Software Security</td>
<td></td>
<td></td>
<td>Rapid7, Splunk</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Incident Response and Management</td>
<td></td>
<td></td>
<td>Rapid7, redseal, A&amp;A</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Penetration Tests and Red Team Exercises</td>
<td></td>
<td></td>
<td>A&amp;A</td>
<td></td>
</tr>
</tbody>
</table>
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/
CIS Top 20 Critical Security Controls

- CISsecurity.org JOIN!!
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>Tenable Nessus</td>
<td>Rapid7</td>
</tr>
<tr>
<td>End Point Protection</td>
<td>Cylance Protect</td>
<td>Symantec</td>
</tr>
<tr>
<td>Threat Intelligence</td>
<td>Crowdstrike Falcon Intelligence</td>
<td>FireEye Threat Intelligence</td>
</tr>
<tr>
<td>Next Generation Firewall</td>
<td>Palo Alto Networks PA Series</td>
<td>CheckPoint Software</td>
</tr>
<tr>
<td>Application Security</td>
<td>Quayls WAS</td>
<td>Rapid7</td>
</tr>
<tr>
<td>Advanced Threat Detection</td>
<td>FireEye Intrusion NX</td>
<td>Snort</td>
</tr>
<tr>
<td>SIEM</td>
<td>LogRhythm Security Intelligence Platform</td>
<td>Splunk</td>
</tr>
<tr>
<td>Endpoint Detection/Response</td>
<td>Carbon Black Platform</td>
<td>Palo Alto Network Traps</td>
</tr>
</tbody>
</table>


CIS Top 20 Critical Security Controls

Thank you for Attending.

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