CIS Top 20 #4

Continuous Vulnerability Assessment & Remediation
CIS Top 20 Critical Security Controls

- Organizations must know at all times:
  - Which vulnerabilities are present in their IT assets
  - The level of risk each one carries
  - Remediation of affected IT assets
CIS Top 20 Critical Security Controls
This week, we’re focusing on CIS Control 4: Continuous Vulnerability Assessment and Remediation.

More specifically: “Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.”
CIS Top 20 Critical Security Controls

Get to know the CIS Controls
CIS Top 20 Critical Security Controls

**THE ISSUE**

- Credit card breaches, identity theft, ransomware & loss of privacy are now everyday news.
- Organizations lack effective cybersecurity practices & policies.
- The ‘Fog of More’ overwhelms organizations facing cybersecurity decisions.
CIS Top 20 Critical Security Controls

**A Community Solution**

- The CIS Critical Security Controls (CIS Controls) started as a grass-roots activity in 2008.
- Focused on the most critical actions organizations should take, informed by experts & real threat data.
- Embodies the Pareto Principle, an "80/20 Rule" to emphasize the most valuable security actions.
CIS Top 20 Critical Security Controls

HOW ARE THEY CREATED?

Expert volunteers from every part of the cyber ecosystem, including vendors & consultants, develop the CIS Controls.

The Center for Internet Security's CIS Controls have matured into an international movement of individuals & institutions.

More than "good things to do," the CIS Controls are a prioritized set of actions that bridge technical security & risk management.
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

CIS Controls

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 SecureSuite Membership
Become a member
CIS Top 20 Critical Security Controls

• Stay informed
• Putting it together
• Its all about reducing risk
Why is CIS Control 4 critical?

• Organizations that do not scan for vulnerabilities and proactively address discovered flaws face significant likelihood of having their computer systems compromised.
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

<table>
<thead>
<tr>
<th>Function</th>
<th>Management Perspective</th>
<th>Defined Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Management</td>
<td>How well do we detect, accurately identify, handle, and recover from security incidents?</td>
<td>• Cost of Incidents&lt;br&gt;• Mean Cost of Incidents&lt;br&gt;• Mean Incident Recovery Cost&lt;br&gt;• Mean-Time to Incident Discovery&lt;br&gt;• Number of Incidents&lt;br&gt;• Mean-Time Between Security Incidents&lt;br&gt;• Mean-Time to Incident Recovery</td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td>How well do we manage the exposure of the organization to vulnerabilities by identifying and mitigating known vulnerabilities?</td>
<td>• Vulnerability Scanning Coverage&lt;br&gt;• Percent of Systems with No Known Severe Vulnerabilities&lt;br&gt;• Mean-Time to Mitigate Vulnerabilities&lt;br&gt;• Number of Known Vulnerabilities&lt;br&gt;• Mean Cost to Mitigate Vulnerabilities</td>
</tr>
<tr>
<td>Patch Management</td>
<td>How well are we able to maintain the patch state of our systems?</td>
<td>• Patch Policy Compliance&lt;br&gt;• Patch Management Coverage&lt;br&gt;• Mean-Time to Patch&lt;br&gt;• Mean Cost to Patch</td>
</tr>
</tbody>
</table>
CIS Top 20 Critical Security Controls

• CSC 4.1 Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis
• CSC 4.1 Procedure: Scan entire network daily using SCAP (Security Content Automation Protocol) scanner
• The organization:
  – IT department to run SCAP scan weekly (Monday mornings)
  – IT department will review SCAN logs for completeness
  – Metrics:
    – IT department will report in new vulnerabilities
    – The IT department will audit SIEM logs daily
CIS Top 20 Critical Security Controls

• No one solution will prevent all attacks, vulnerability assessment is a matter of foundational security practice
CIS Top 20 Critical Security Controls

• Identified vulnerabilities or misconfigurations, patches (or updates) must be applied to all affected

• Where possible, automate patch management. Basic preventive hygiene practices that will significantly enhance your security posture.
CIS Top 20 Critical Security Controls

• Routinely check system logs to verify that vulnerabilities have been addressed and identify any scanning problems.

• By comparing logs over time, you can see look for patterns and ensure that any scanning activity taking place.

• Since automated patching tools may not detect or install all patches, you can compare system logs against patches listed on vendor websites to ensure you’ve got the latest security updates.
### CIS Top 20 Critical Security Controls

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).</td>
</tr>
<tr>
<td>4.2</td>
<td>Correlate event logs with information from vulnerability scans to fulfill two goals. First, personnel should verify that the activity of the regular vulnerability scanning tools is itself logged. Second, personnel should be able to correlate attack detection events with prior vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable.</td>
</tr>
<tr>
<td>4.3</td>
<td>Perform vulnerability scanning in authenticated mode either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested. Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses. Ensure that only authorized employees have access to the vulnerability management user interface and that roles are applied to each user.</td>
</tr>
<tr>
<td>4.4</td>
<td>Subscribe to vulnerability intelligence services in order to stay aware of emerging exposures, and use the information gained from this subscription to update the organization’s vulnerability scanning activities on at least a monthly basis. Alternatively, ensure that the vulnerability scanning tools you use are regularly updated with all relevant important security vulnerabilities.</td>
</tr>
<tr>
<td>4.5</td>
<td>Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.</td>
</tr>
<tr>
<td>4.6</td>
<td>Monitor logs associated with any scanning activity and associated administrator accounts to ensure that this activity is limited to the timeframes of legitimate scans.</td>
</tr>
<tr>
<td>4.7</td>
<td>Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk. Such acceptance of business risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed, increasing the risk.</td>
</tr>
<tr>
<td>4.8</td>
<td>Establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets (example, DMZ servers, internal network servers, desktops, laptops). Apply patches for the riskiest vulnerabilities first. A phased rollout can be used to minimize the impact to the organization. Establish expected patching timelines based on the risk rating level.</td>
</tr>
</tbody>
</table>
CIS Top 20 Critical Security Controls

• 4-1 Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk.

• Free Tools
  • CIS Cis-Cat - Our friends at CIS
  • AlienVault OSSIM - OpenSource fairly comprehensive
  • OpenVAS - Comes in AlienVault, but if you JUST need a vulnerability scanner, this is it.
  • Rapid 7 IoT Seeker seek IoT devices and check for default passwords

• Commercial Tools
  • Nessus - Industry known and trusted scanner.
  • Nexpose - Rapid7 Vulnerability scanner
CIS Top 20 Critical Security Controls
CIS Top 20 Critical Security Controls
CIS Top 20 Critical Security Controls
CIS Top 20 Critical Security Controls
CIS Top 20 Critical Security Controls
CIS Top 20 Critical Security Controls

• 4-2 Correlate event logs with information from vulnerability scans to fulfill two goals. First, personnel should verify that the activity of the regular vulnerability scanning tools themselves is logged. Second, personnel should be able to correlate attack detection events with earlier vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable.

• Free Tools
  • AlienVault OSSIM - again
  • OpenVAS - Comes in AlienVault, but if you JUST need a vulnerability scanner, this is it.

• Commercial Tools
  • Nessus - Industry known and trusted scanner.
  • Nexpose - Rapid7 Vulnerability scanner
  • Qualys - Qualys Vulnerability scanner
4-3 - Perform vulnerability scanning in authenticated mode either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested.

Free Tools
- AlienVault OSSIM - What can't it do???
- OpenVAS - Comes in AlienVault, but if you JUST need a vulnerability scanner, this is it.

Commercial Tools
- Nessus - Industry known and trusted scanner.
- Nexpose - Rapid7 Vulnerability scanner
- Qualys - Qualys Vulnerability scanner
CIS Top 20 Critical Security Controls

• 4-4 - Subscribe to vulnerability intelligence services in order to stay aware of emerging exposures, and use the information gained from this subscription to update the organization's vulnerability scanning activities on at least a monthly basis.

• Free Tools
  You must get these tools from each vendor you use. Usually these would be mailing lists, RSS feeds, etc. A few I subscribe to:
  • https://isc.sans.edu/newssummary.html
  • http://sectools.org/
  • CVE - Common Vulnerability and Exposures subject to National Vulnerability Database
  • OpenSSL - Stay up to date for the next Heart Bleed
  • https://www.us-cert.gov/ncas/current-activity, (Alerts & tips),
  • http://www2.mitre.org/work/sepo/toolkits/risk/
  • OWASP – Vulnerabilities. Rating and more
  • Vendors: Trendmicro, FireEye
CIS Top 20 Critical Security Controls

CVE Data Feeds
Please see below for the latest CVE updates.

Newest CVE Entries Feed
CVE-2012-2830
Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service (incorrect pointer use) or possibly have unspecified other impact via an HTML document with a crafted URL.

CVE-2012-2831
Use-after-free vulnerability in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web page served over HTTP.

CVE-2012-2832
The image-codec implementation in the PDF functionality in Google Chrome before 20.0.1132.43 does not initialize an unspecified pointer, which allows remote attackers to cause a denial of service (inaccurate pointer use) or possibly have unspecified other impact.

CVE-2012-2833
Buffer overflow in the JS API in the PDF functionality in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted PDF documents.

CVE-2012-2834
Integer overflow in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted PDF documents.

Latest CVE News Feed
CVE Announcements
CVE Adds 2 New CVE Numbering Authorities (CNA's): Facebook & Twitter.

Other Updates and Feeds
U.S. National Vulnerability Database (NVD)
NVD, which is fully synchronized with the CVE List, so any updates to CVE appear immediately in NVD, offers these CVE content feeds:
- JSON Vulnerability Feed
- XML Vulnerability Feed
CIS Top 20 Critical Security Controls
CIS Top 20 Critical Security Controls
CIS Top 20 Critical Security Controls

• 4-5 - Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe.

• Free Tools
  • Ninite - While not free, it is DIRT CHEEP. But only patches 3rd party applications listed on its website.
  • Microsoft System Center Configuration Manager - SCCM patch management capabilities have been a de facto standard for enterprise IT shops for many years.

• Commercial Tools
  • Solarwinds - SolarWinds Patch Management Suite for scanning, patching, management, LEM
  • Tenable - suite of course with VM, inventory, configuration settings
  • LanGuard - most platforms
CIS Top 20 Critical Security Controls
CIS Top 20 Critical Security Controls
CIS Top 20 Critical Security Controls

### Outstanding Remediation Tracking

<table>
<thead>
<tr>
<th>Time Since Patch Publication</th>
<th>Assets</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
<th>Critical</th>
<th>Exploitable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 45 days</td>
<td>12</td>
<td>9</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>46 - 90 days</td>
<td>18</td>
<td>5</td>
<td>40</td>
<td>25</td>
<td>20</td>
<td>12</td>
</tr>
<tr>
<td>91 - 180 days</td>
<td>16</td>
<td>3</td>
<td>39</td>
<td>16</td>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td>More than 180 days</td>
<td>17</td>
<td>3</td>
<td>19</td>
<td>19</td>
<td>10</td>
<td>2</td>
</tr>
</tbody>
</table>

### Outstanding Microsoft Remediations - Time Since Patch Publication

<table>
<thead>
<tr>
<th>Time Since Patch Publication</th>
<th>Assets</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
<th>Critical</th>
<th>Exploitable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 45 days</td>
<td>12</td>
<td>9</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>46 - 90 days</td>
<td>18</td>
<td>5</td>
<td>40</td>
<td>25</td>
<td>20</td>
<td>12</td>
</tr>
<tr>
<td>91 - 180 days</td>
<td>16</td>
<td>3</td>
<td>39</td>
<td>16</td>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td>More than 180 days</td>
<td>17</td>
<td>3</td>
<td>19</td>
<td>19</td>
<td>10</td>
<td>2</td>
</tr>
</tbody>
</table>

### Outstanding Remediations by Device Type

<table>
<thead>
<tr>
<th>Device</th>
<th>Assets</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
<th>Critical</th>
<th>Exploitable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>7</td>
<td>7</td>
<td>16</td>
<td>31</td>
<td>44</td>
<td>64</td>
</tr>
<tr>
<td>Unix</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Apple</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>18</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Network</td>
<td>1</td>
<td>0</td>
<td>5</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

### End of Life Software Detection

<table>
<thead>
<tr>
<th>Plugin ID</th>
<th>Name</th>
<th>Severity</th>
<th>Host Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>43951</td>
<td>Mozilla Foundation Unsupported Javascript</td>
<td>Critical</td>
<td>3</td>
</tr>
<tr>
<td>323113</td>
<td>Microsoft Exchange Server Unsupported Version Detection</td>
<td>Critical</td>
<td>2</td>
</tr>
<tr>
<td>32860</td>
<td>Low Operating System Unsupported Version Detection</td>
<td>Critical</td>
<td>2</td>
</tr>
<tr>
<td>88710</td>
<td>Whisker, Unfiltered Unsupported Version Detection</td>
<td>Critical</td>
<td>2</td>
</tr>
<tr>
<td>34460</td>
<td>Unsupported Web Server Detection</td>
<td>High</td>
<td>1</td>
</tr>
<tr>
<td>69967</td>
<td>Adobe AIR Unsupported Version Detection</td>
<td>Critical</td>
<td>1</td>
</tr>
<tr>
<td>62255</td>
<td>Microsoft IIS Remote (IISAU) and IIS Core Service Unsupported</td>
<td>Critical</td>
<td>1</td>
</tr>
<tr>
<td>78699</td>
<td>OpenSSL Unassisted</td>
<td>Critical</td>
<td>1</td>
</tr>
</tbody>
</table>
CIS Top 20 Critical Security Controls

• 4-6 - Carefully monitor logs associated with any scanning activity and associated administrator accounts to ensure that all scanning activity and associated access via the privileged account is limited to the timeframes of legitimate scans.

Free Tools
• Netwrix - AD Change Reporter Free
• Scripted - on github
• GPO - Only enables logging, you still need to alert

Commercial Tools
• Solarwinds - Part of LEM suite
• Splunk also offers commercial versions of their free tool above.
• Rapid7 part of complete suite.
CIS Top 20 Critical Security Controls
CIS Top 20 Critical Security Controls
CIS Top 20 Critical Security Controls
CIS Top 20 Critical Security Controls

• 4-7 - Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk.
  – This is more of a process than a tool.

• 4-8 - Establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets (example, DMZ servers, internal network servers, desktops, laptops).
## CIS Top 20 Critical Security Controls

### Strategic Cyber Resiliency Design Principles
- Focus on common critical assets.
- Support agility and architect for adaptability.
- Reduce attack surfaces.
- Assume compromised resources.
- Expect adversaries to evolve.

### Structural Cyber Resiliency Design Principles
- Limit the need for trust.
- Control visibility and use.
- Contain and exclude behaviors.
- Layer and partition defenses.
- Plan and manage diversity.
- Maintain redundancy.
- Make resources location-versatile.
- Leverage health and status data.
- Maintain situational awareness.
- Manage resources (risk-) adaptively.
- Maximize transience; minimize persistence.
- Determine ongoing trustworthiness.
- Change or disrupt the attack surface.
- Make unpredictability and deception user-transparent.

### Key to Aligned Disciplines:
- Security
- Resilience Engineering & Survivability
- Evolvability
- Unique to Consideration of Advanced Cyber Threats

---

**Warning:** For any given mission, system, or program, only a subset of these principles will be relevant – selection must be based on a variety of considerations, including lifecycle stage, type of system, and relevant design principles from other disciplines. In addition, more specific restatements may prove more useful in guiding analysis and assessment.
# CIS Top 20 Critical Security Controls

<table>
<thead>
<tr>
<th>Generally Accepted Design Principle</th>
<th>Corresponding Cyber Resiliency Design Principle(s) from Table 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design to reduce exposure to attack</td>
<td>Reduce attack surfaces.</td>
</tr>
<tr>
<td>Design to reduce persistence of access by the adversary</td>
<td>Maximize transient; minimize persistence.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Generally Accepted Design Principle</th>
<th>Corresponding Cyber Resiliency Design Principle(s) from Table 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design to reduce adversary’s ability to act</td>
<td>Control visibility and use.</td>
</tr>
<tr>
<td></td>
<td>Contain and exclude behaviors.</td>
</tr>
<tr>
<td>Design to limit the consequences of attack</td>
<td>Manage resources (risk-) adaptively.</td>
</tr>
<tr>
<td>Design to minimize common cause failure</td>
<td>Focus on common critical assets.</td>
</tr>
<tr>
<td></td>
<td>Maintain redundancy.</td>
</tr>
<tr>
<td>Design to tolerate compromise</td>
<td>Assume compromised resources.</td>
</tr>
<tr>
<td></td>
<td>Limit the need for trust.</td>
</tr>
<tr>
<td>Design to degrade gracefully</td>
<td>Manage resources (risk-) adaptively.</td>
</tr>
<tr>
<td>Design to crash early and recover quickly</td>
<td>Manage resources (risk-) adaptively.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Additional Design Principle</th>
<th>Corresponding Cyber Resiliency Design Principle(s) from Table 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design for integrity and availability</td>
<td>Determine ongoing trustworthiness.</td>
</tr>
<tr>
<td>Design to be threat independent</td>
<td>Expect adversaries to evolve.</td>
</tr>
<tr>
<td>Design to be vulnerability independent</td>
<td>Expect adversaries to evolve.</td>
</tr>
<tr>
<td>Design such that users will not seek to circumvent security and resilience features</td>
<td>Make unpredictability and deception user-transparent.</td>
</tr>
<tr>
<td>Design with distributed and localized decision support</td>
<td>Make resources location-creative.</td>
</tr>
<tr>
<td>Integrate horizontally for resilience of the whole system / mission</td>
<td>Control visibility and use.</td>
</tr>
<tr>
<td></td>
<td>Layer and partition defenses.</td>
</tr>
<tr>
<td>Design components with computational plasticity (alternative functional paths to achieve the computing results)</td>
<td>Support agility and architect for adaptability.</td>
</tr>
<tr>
<td>Design for simplicity and modularity to change easily / frequently</td>
<td>Support agility and architect for adaptability.</td>
</tr>
</tbody>
</table>
## CIS Top 20 Critical Security Controls

<table>
<thead>
<tr>
<th>Operational Principle</th>
<th>Corresponding Cyber Resiliency Design Principle(s) from Table 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actively look for bad guys in the system</td>
<td>Assume compromised resources. Expect adversaries to evolve.</td>
</tr>
<tr>
<td>Leverage cyber intelligence to inform operations</td>
<td>Assume compromised resources. Expect adversaries to evolve.</td>
</tr>
<tr>
<td>Operate to reduce adversary’s ability to act</td>
<td>Control visibility and use. Contain and exclude behaviors. Layer and partition defenses.</td>
</tr>
<tr>
<td>Operate to contain vulnerabilities</td>
<td>Control visibility and use. Contain and exclude behaviors. Layer and partition defenses.</td>
</tr>
<tr>
<td>Operate to reconstitute and recover quickly to an acceptable level of trust</td>
<td>Determine ongoing trustworthiness.</td>
</tr>
<tr>
<td>Prioritize operational TTPs based on mission assurance needs</td>
<td>Maintain situational awareness.</td>
</tr>
<tr>
<td>Balance / coordinate local defense with global defense</td>
<td>Control visibility and use. Contain and exclude behaviors. Layer and partition defenses.</td>
</tr>
<tr>
<td>Operate to control / limit the damage / consequences of attack</td>
<td>Manage resources (risk-) adaptively.</td>
</tr>
<tr>
<td>Operate with agility and alternative operational contingencies</td>
<td>Manage resources (risk-) adaptively.</td>
</tr>
<tr>
<td>Operate to confuse, deceive, and impede the adversary (but not the mission operators)</td>
<td>Make unpredictability and deception user-transparent.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operational Principle</th>
<th>Corresponding Cyber Resiliency Design Principle(s) from Table 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor integrity and availability, and respond accordingly</td>
<td>Maintain situational awareness.</td>
</tr>
<tr>
<td>Train operators to understand cyber impact to mission operations to operate in ways that ensure mission execution success</td>
<td>Manage resources (risk-) adaptively.</td>
</tr>
</tbody>
</table>
CIS Top 20 Critical Security Controls

- **Vulnerability Factors:**
  Goal is to estimate the likelihood of the particular vulnerability being discovered and exploited.

- **Ease of discovery**
  How easy is it for this group of threat agents to discover this vulnerability?

- **Ease of exploit**
  How easy is it for this group of threat agents to actually exploit this vulnerability?

- **Awareness**
  How well known is this vulnerability to this group of threat agents?

- **Intrusion detection**
  How likely is an exploit to be detected?
CIS Top 20 Critical Security Controls

WHAT’S MOST IMPORTANT

WHAT ARE THE RISKS

HOW TO MITIGATE THE RISKS

Crown Jewels Analysis (CJA)

CONOPS Use Cases End-to-End Flows

Mission Impact Analysis

Establish Mission Priorities

Identify Mission Dependencies

Cyber Threat Susceptibility Assessment

Cyber Risk Remediation Analysis

Mitigation Techniques

Threat Assessment & Remediation Analysis (TARA)
# CIS Top 20 Critical Security Controls

<table>
<thead>
<tr>
<th>Factor Range</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Proximity:</strong> What proximity would an adversary need in order to apply this TTP?</td>
<td>no physical or network access required</td>
<td>protocol access through DMZ and firewall</td>
<td>user account to target system (no admin access)</td>
<td>admin access to target system</td>
<td>physical access to target system</td>
</tr>
<tr>
<td><strong>Locality:</strong> How localized are the effects posed by this TTP?</td>
<td>isolated to single unit</td>
<td>single unit and supporting network</td>
<td>external networks potentially impacted</td>
<td>all units in theater or region</td>
<td>all units globally and associated infrastructure</td>
</tr>
<tr>
<td><strong>Recovery Time:</strong> How long would it take to recover from this TTP once the attack was detected?</td>
<td>&lt; 10 hours</td>
<td>20 hours</td>
<td>30 hours</td>
<td>40 hours</td>
<td>&gt; 50 hours</td>
</tr>
<tr>
<td><strong>Restoration Costs:</strong> What is the estimated cost to restore or replace affected cyber asset?</td>
<td>&lt;$10K</td>
<td>$25K</td>
<td>$50K</td>
<td>$75K</td>
<td>&gt;$100K</td>
</tr>
<tr>
<td><strong>Impact:</strong> How serious an impact is loss of data confidentiality resulting from successful application of this TTP?</td>
<td>no impact from TTP</td>
<td>minimal impact</td>
<td>limited impact requiring some remediation</td>
<td>remediation activities detailed in CDOP</td>
<td>COOP remediation activities routinely exercised</td>
</tr>
<tr>
<td><strong>Impact:</strong> How serious an impact is loss of data integrity resulting from successful application of this TTP?</td>
<td>no impact from TTP</td>
<td>minimal impact</td>
<td>limited impact requiring some remediation</td>
<td>remediation activities detailed in CDOP</td>
<td>COOP remediation activities routinely exercised</td>
</tr>
<tr>
<td><strong>Impact:</strong> How serious an impact is loss of system availability resulting from successful application of this TTP?</td>
<td>no impact from TTP</td>
<td>minimal impact</td>
<td>limited impact requiring some remediation</td>
<td>remediation activities detailed in CDOP</td>
<td>COOP remediation activities routinely exercised</td>
</tr>
<tr>
<td><strong>Prior Use:</strong> Is there evidence of this TTP in the MITRE Threat DB?</td>
<td>no evidence of TTP use in MITDB</td>
<td>evidence of TTP use possible</td>
<td>confirmed evidence of TTP use in MITDB</td>
<td>frequent use of TTP reported in MITDB</td>
<td>widespread use of TTP reported in MITDB</td>
</tr>
<tr>
<td><strong>Required Skills:</strong> What level of skill or specific knowledge is required by the adversary to apply this TTP?</td>
<td>no specific skills required</td>
<td>generic technical skills</td>
<td>some knowledge of targeted system</td>
<td>detailed knowledge of targeted system</td>
<td>knowledge of both mission and targeted system</td>
</tr>
<tr>
<td><strong>Required Resources:</strong> Would resources be required or consumed in order to apply this TTP?</td>
<td>no resources required</td>
<td>minimal resources required</td>
<td>some resources required</td>
<td>significant resources required</td>
<td>resources required and consumed</td>
</tr>
</tbody>
</table>
CIS Top 20 Critical Security Controls

### Maturity Level

<table>
<thead>
<tr>
<th>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

- **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

### Total Completion (by CSC)

- Policies Complete: 22%
- Controls 1-5 Implemented: 19%
- All Controls Implemented: 25%
- All Controls Automated: 28%
- All Controls Reported: 19%
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

• SynerComm’s IT Summit
• April 9-10\textsuperscript{th}
• Lambeau Field, Green Bay, WI
• Validate Your IT Strategy
• FREE!!
• Register:  [www.events.synercomm.com](http://www.events.synercomm.com)
CIS Top 20 Critical Security Controls

Thank you for Attending.

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

Tuesday March 20th
CIC CSC #5
Controlled Use of Administrative Privileges