SYNERCOMM
SECURE • INTELLIGENT • NETWORKS

CIS Top 20 #14

Controlled Access Based on Need to Know

Lisa Niles: CISSP, Director of Solutions Integration

CIS Top 20 Critical Security Controls

CSC # # 14

- *The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification*

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

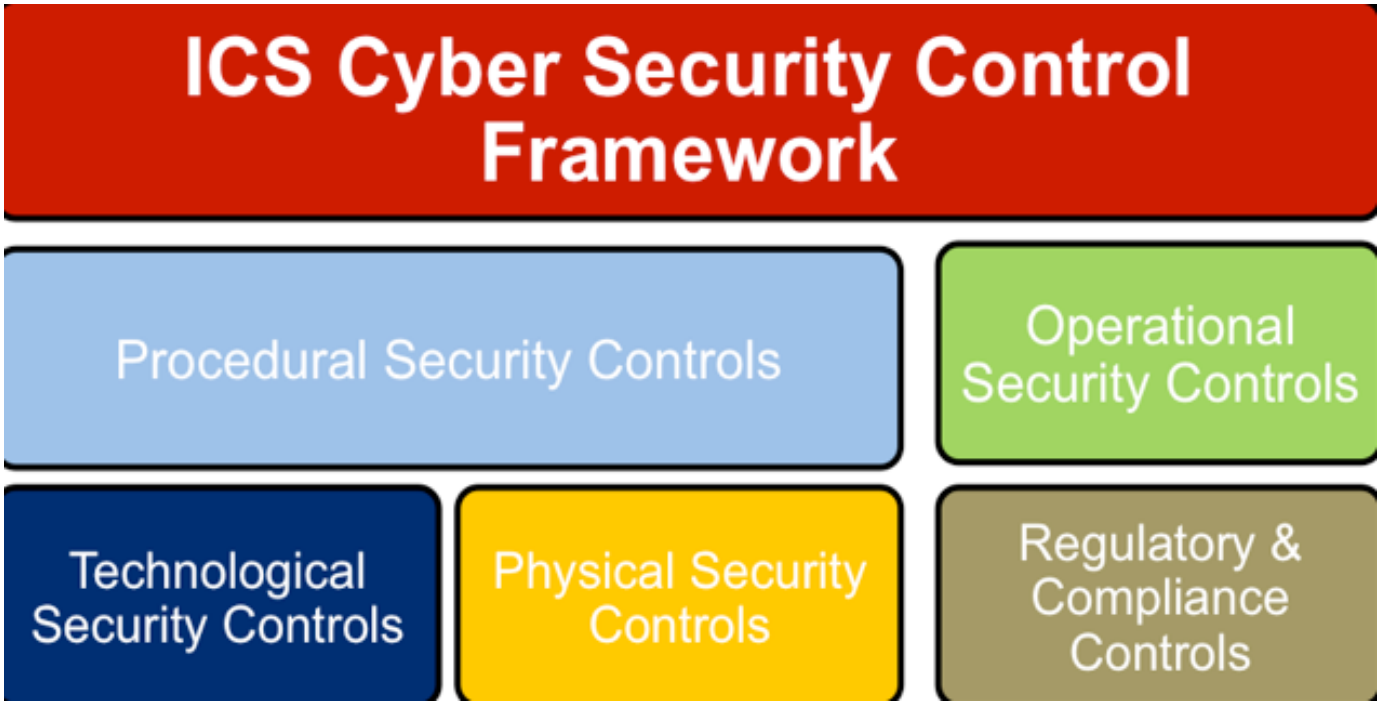
Foundational

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

- Let's start with some simple, yet often unasked questions….

- Do you know what critical assets—information and data….exist in your organization's network?
- Do you have a data classification policy?
- Who defines the criticality of systems and information?

CIS Top 20 Critical Security Controls

- It is important that an organization understand what its sensitive information is, where it resides, and who needs access to it.

CIS Top 20 Critical Security Controls

- **Information Security 101**.
  - There are a lot of foundational controls in here which should be adopted by even the smallest of organizations.
  - Network segmentation, permissions, and data encryption are basic security hygiene that are cheap and easy to implement.

CIS Top 20 Critical Security Controls

SEG/ME/NT

CIS Top 20 Critical Security Controls

- What further controls around sensitive data are a must?

CIS Top 20 Critical Security Controls

- Audit your ACLs and AD users and security groups regularly

CIS Top 20 Critical Security Controls

- If data are flowing over a network with a lower trust level, encryption should be used.

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

- Sample Gap questions

1. Does an access control baseline exist for all data sets that details the appropriate permissions for each user who needs access to the resource?
2. Does an access control baseline exist that documents the permissions necessary for each data set?
3. Have users only been assigned the appropriate permissions to the data sets necessary to complete their job requirements?
4. Do proper authorizations exist for each user granted rights to each of the organization's data sets?
5. Does an automated validation process exist to ensure that only proper users have the proper rights to each data set?

CIS Top 20 Critical Security Controls

14.1	Segment the network based on the label or classification level of the information stored on the servers. Locate all sensitive information on separated VLANS with firewall filtering to ensure that only authorized individuals are only able to communicate with systems necessary to fulfill their specific responsibilities.
14.2	All communication of sensitive information over less-trusted networks should be encrypted. Whenever information flows over a network with a lower trust level, the information should be encrypted.
14.3	All network switches will enable Private Virtual Local Area Networks (VLANs) for segmented workstation networks to limit the ability of devices on a network to directly communicate with other devices on the subnet and limit an attackers ability to laterally move to compromise neighboring systems.
14.4	All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principal that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.
14.5	Sensitive information stored on systems shall be encrypted at rest and require a secondary authentication mechanism, not integrated into the operating system, in order to access the information.
14.6	Enforce detailed audit logging for access to nonpublic data and special authentication for sensitive data.
14.7	Archived data sets or systems not regularly accessed by the organization shall be removed from the organization's network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.

CIS Top 20 Critical Security Controls

14-1 - Segment the network based on the label or classification level of the information stored on the servers. Locate all sensitive information on separated VLANS with firewall filtering to ensure that only authorized individuals are only able to communicate with systems necessary to fulfill their specific responsibilities.

Free Tools

- Domain Isolation - While not a single tool, it is a common best practice to separate your network into zones and define higher security standards for zones that contain sensitive data using IPsec.
- Netwrix Auditor - Change auditing and reporting for IT systems.

Commercial Tools

- Varonis - Shows where in file systems sensitive data resides, who has access to it, who should and shouldn't have access to it, who uses it, who owns it, and where is it over exposed.
- Forcepoint
- DigitalGuardian

CIS Top 20 Critical Security Controls

- 14-2 All communication of sensitive information over less-trusted networks should be encrypted. Whenever information flows over a network with a lower trust level, the information should be encrypted.

Free Tools

- Windows Bitlocker GPO

Commercial Tools

- NGFW VPN,, Digital Guardian, Forcepoint

CIS Top 20 Critical Security Controls

- 14-3 - All network switches will enable Private Virtual Local Area Networks (VLANs) for segmented workstation networks to limit the ability of devices on a network to directly communicate with other devices on the subnet and limit an attackers ability to laterally move to compromise neighboring systems.

CIS Top 20 Critical Security Controls

- 14-4 - All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principal that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. (FIP)

Free Tools

- OSSEC – Free HIPS

Commercial Tools

- Splunk, Rapid7, Digital Guardian, Tripwire, Solarwinds, Alienvault, Forcepoint

CIS Top 20 Critical Security Controls

- 14-5 Sensitive information stored on systems shall be encrypted at rest and require a secondary authentication mechanism, not integrated into the operating system, in order to access the information.

Free Tools

- Windows Server - Data Classification Infrastructure (DCI) allows you to classify data if it contains content you specify as a certain classification (SSN = high), then applies rules to certain levels of classification (do not copy/print, encrypt, etc..).

Commercial Tools

- Digital Guardian - Classify files as they are created and create rules on what to do with certain classifications.
- Forcepoint

CIS Top 20 Critical Security Controls

- *14-6* - Enforce detailed audit logging for access to nonpublic data and special authentication for sensitive data

Free Tools

- Windows system and security logs

Commercial Tools

- Tenable Log Correlation Engine - A leader in Security, Tenable makes a great tool that collect, normalizes, analyzes, and alerts for almost any log out there.
- EventLog Analyzer - Ties in with ManageEngines other wide array of IT tools. They do offer a free version for upto 5 devices
- AlienVault USM - With everything else that it does, it also has log correlation

CIS Top 20 Critical Security Controls

- *14-7* - Archived data sets or systems not regularly accessed by the organization shall be removed from the organization's network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.

CIS Top 20 Critical Security Controls

CIS Top 20 Critical Security Controls

Thank you for Attending.

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

Tuesday September 4th

CIC CSC # 17

Security Skills Assessment and Appropriate Training