SYNERCOMM
SECURE • INTELLIGENT • NETWORKS

CIS Top 20 #11

Secure Configuration of Network Devices

Lisa Niles: CISSP, Director of Solutions Integration

CIS Top 20 Critical Security Controls

CSC # 11 – Secure Configuration of Network Devices

Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices.

- *Using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.*

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

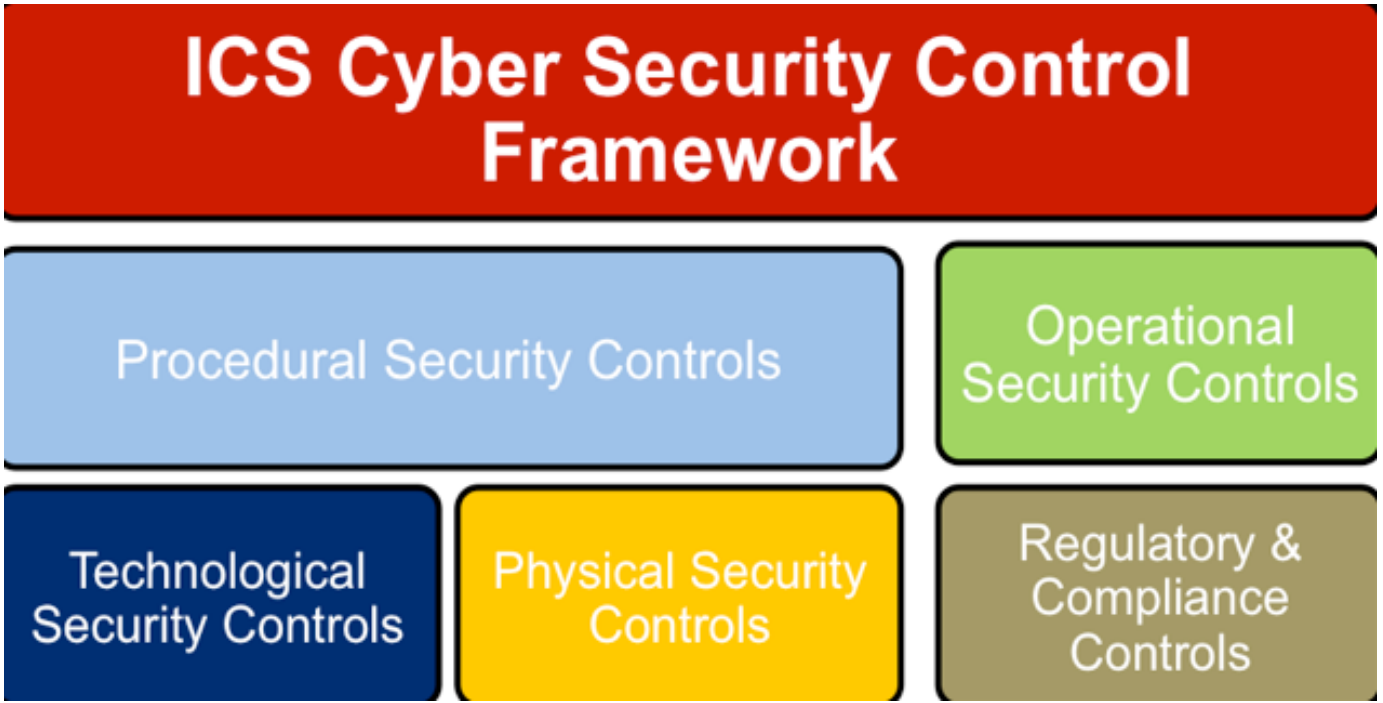
Foundational

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



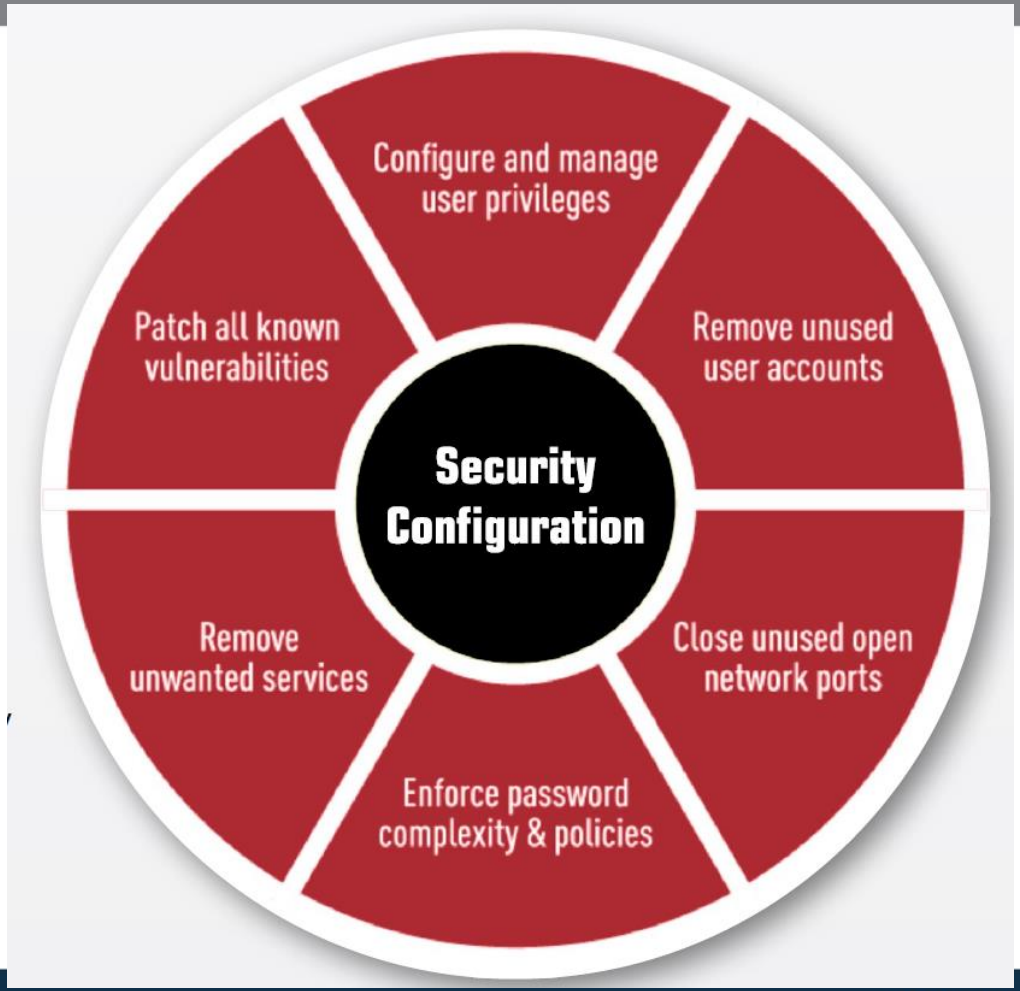
CIS Top 20 Critical Security Controls

The management of the secure configurations for networking devices is not a one-time event!

COMPLIANCE IS MORE
THAN A ONE-TIME EVENT

CIS Top 20 Critical Security Controls

Network Device Security and Configuration Assessment Approach


Configure and manage user privileges
Remove unused user accounts
Close unused open network ports
Enforce password complexity & policies
Remove unwanted services
Patch all known vulnerabilities
Security Configuration

CIS Top 20 Critical Security Controls

- Shift & drift…..

CIS Top 20 Critical Security Controls

- How to Implement This Security Control

CIS Top 20 Critical Security Controls

- Use authoritative hardening guides
- Always maintain and update network diagram
- Strong auth for all network devices
- Advanced scanning

CIS Top 20 Critical Security Controls

- Key Takeaways for Control 11
  - Leverage existing controls.
  - Network devices are computers too.

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. Has the organization defined an information flow that baselines what network services are allowed to travel to which parts of the network?
2. Has the organization been segmented using access control lists to limit network access to only appropriate zones?
3. Is encryption used to protect sensitive data passing over all network segments (including internal)?
4. Are network monitoring tools in use to monitor for inappropriate/malicious traffic?
5. Are data loss prevention tools in place to monitor for inappropriate data sets entering or leaving the network?

CIS Top 20 Critical Security Controls

11.1	Compare firewall, router, and switch configuration against standard secure configurations defined for each type of network device in use in the organization. The security configuration of such devices should be documented, reviewed, and approved by an organization change control board. Any deviations from the standard configuration or updates to the standard configuration should be documented and approved in a change control system.
11.2	All new configuration rules beyond a baseline-hardened configuration that allow traffic to flow through network security devices, such as firewalls and network-based IPS, should be documented and recorded in a configuration management system, with a specific business reason for each change, a specific individual's name responsible for that business need, and an expected duration of the need.
11.3	Use automated tools to verify standard device configurations and detect changes. All alterations to such files should be logged and automatically reported to security personnel.
11.4	Manage network devices using two-factor authentication and encrypted sessions.
11.5	Install the latest stable version of any security-related updates on all network devices.
11.6	Network engineers shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.
11.7	Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

CIS Top 20 Critical Security Controls

- *11-1 - Compare firewall, router, and switch configuration against standard secure configurations defined for each type of network device in use in the organization. The security configuration of such devices should be documented, reviewed, and approved by an organization change control board. Any deviations from the standard configuration or updates to the standard configuration should be documented and approved in a change control system.*
- Free Tools
  - CIS Cis-Cat – again, another great tool from the CIS website!
- Commercial Tools
  - Nessus - Can scan an uploaded configuration of any (most) network device and alert you to insecure configurations.
  - Network Configuration Management - ManageEngine's
  - Tripwire - audit configurations of switches, firewalls, routers, OSs, Applications, and more.

CIS Top 20 Critical Security Controls

- 11-2 - *All new configuration rules beyond a baseline-hardened configuration that allow traffic to flow through network security devices, such as firewalls and network-based IPS, should be documented and recorded in a configuration management system, with a specific business reason for each change, a specific individual's name responsible for that business need, and an expected duration of the need.*
- *Tools:*
  - *Can include paper logs, Change Management systems or purpose built tools like RedSeal, Firemon, Skybox*

CIS Top 20 Critical Security Controls

- 11-3 - *Use automated tools to verify standard device configurations and detect changes. All alterations to such files should be automatically reported to security personnel.*
- *Free tools*
  - *Rapid7 IoT seeker for IoT default admin*
  - *CIS Cis-Cat*
- *Tools*
  - *Rapid7, Qualys, Tenable (CSC#1, 3)*

CIS Top 20 Critical Security Controls

- 11-4 - *Manage network devices using two-factor authentication and encrypted sessions.*
- *Tools*
  - *Use RADIUS at a minimum*
  - *Putty SSH only*
  - *Centrify, Beyond trust MFA*

CIS Top 20 Critical Security Controls

- *11-5 - Install the latest stable version of any security-related updates.*
- Tools
  - You can receive notifications from the vendor via RSS, email, or mailing list.

CIS Top 20 Critical Security Controls

- *11-6 -Network engineers shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.*
- *Tools:*
  - *Jump box on management Zone (Can build your own)*
  - *Prefer MFA to access jump box and session recording*
  - *Centrify*

CIS Top 20 Critical Security Controls

- *11-7 - Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.*
- *Tools*
  - *Network design and security zones*

CIS Top 20 Critical Security Controls

- Additional tips
  - Some vendors provide best practice hardening guides and tools for continued self assessment.
    - Example: PaloAlto PPA report

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 June 26th

CIC CSC # 12

Boundary Defenses