SYNERCOMM
SECURE • INTELLIGENT • NETWORKS

CIS Top 20 #12

Boundary Defense

Lisa Niles: CISSP, Director of Solutions Integration

CIS Top 20 Critical Security Controls

CSC # 12 - *Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data*

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

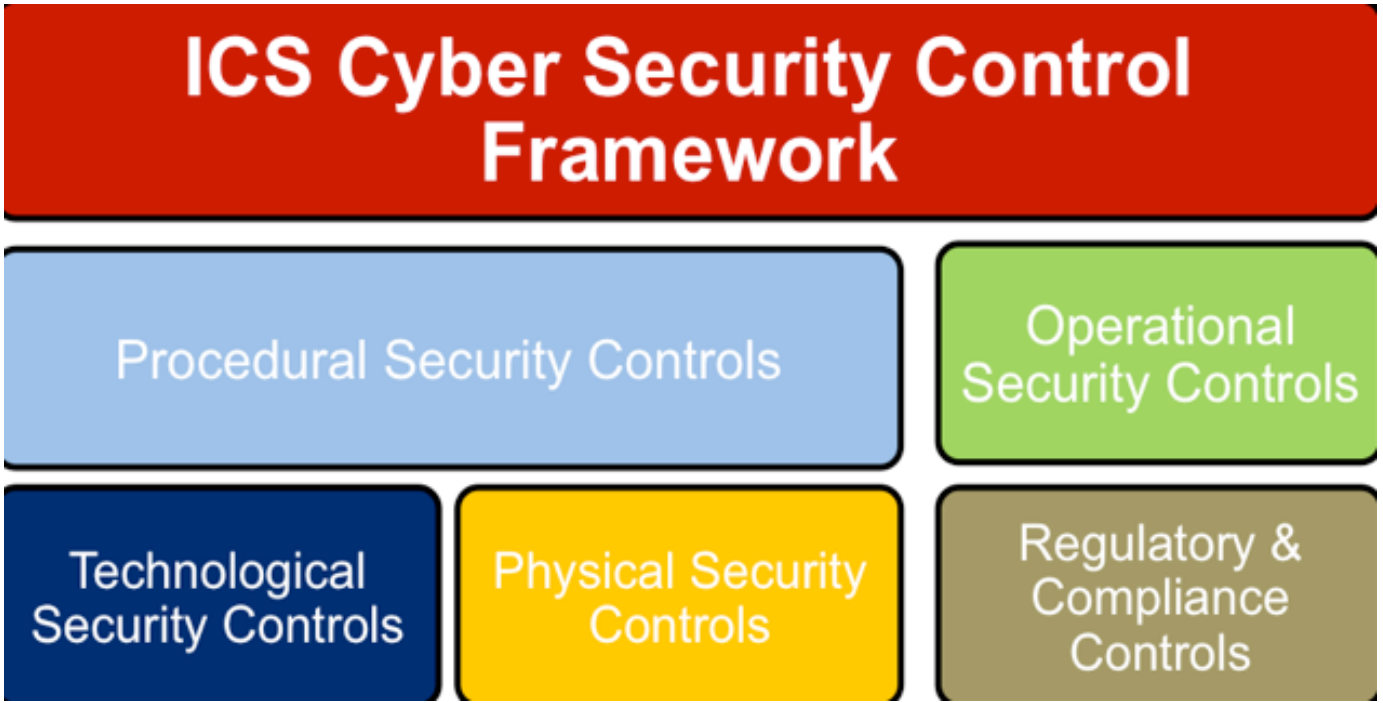
Foundational

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



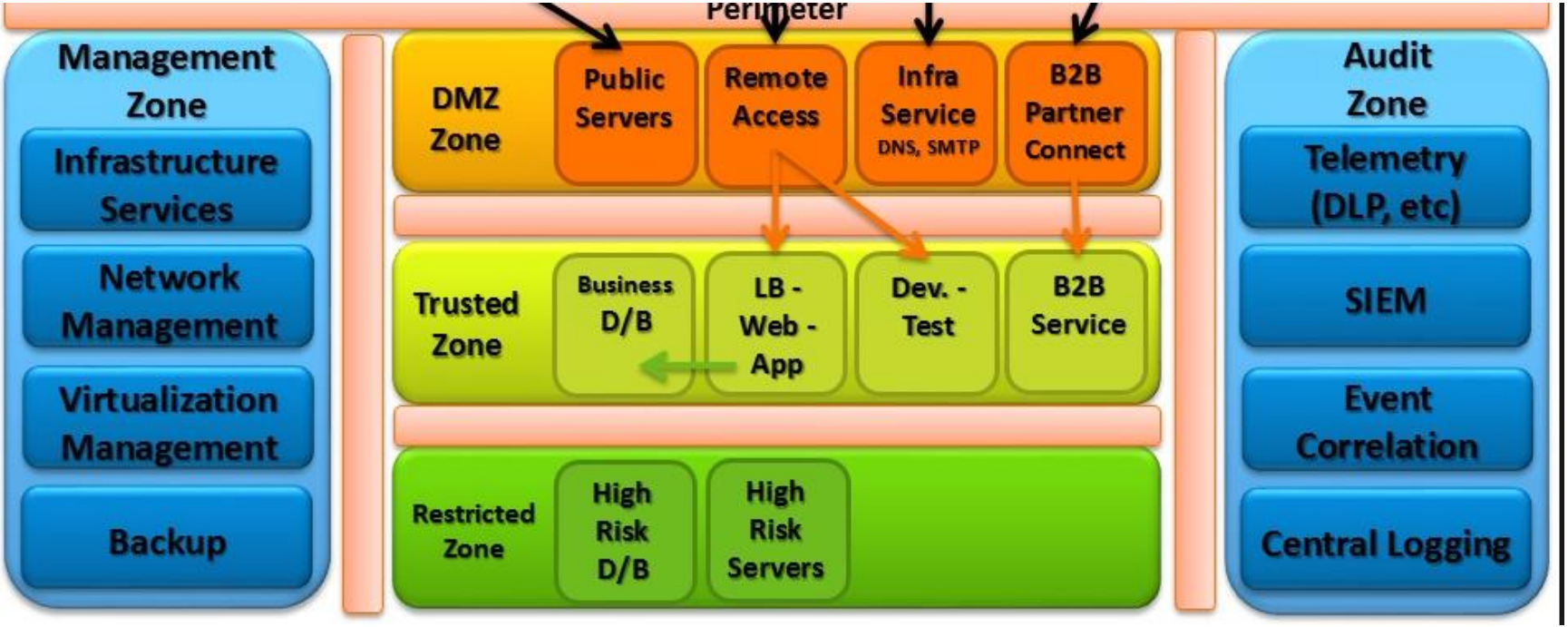
CIS Top 20 Critical Security Controls

- Boundary defenses are not just about keeping attackers out, but just as much about keeping sensitive information in.

CIS Top 20 Critical Security Controls

- Where should you place these controls?
  - Consider asking yourself these three questions:
  - What is my risk?
  - What am I trying to monitor and protect?
  - How does the traffic flow in my environment?

CIS Top 20 Critical Security Controls

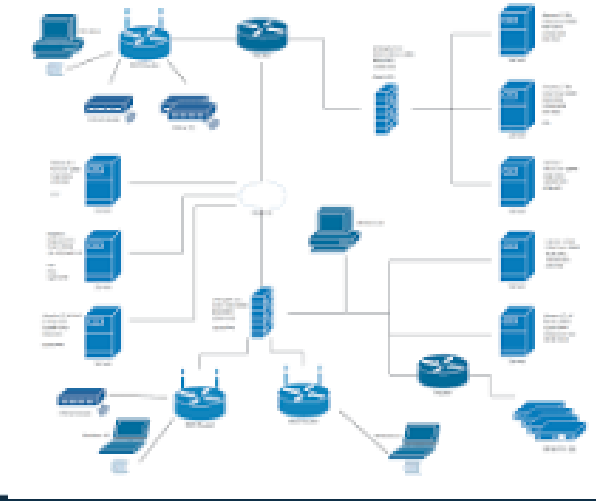


CIS Top 20 Critical Security Controls

- To Zone or not Zone, that is the question I ask…
  - Internet Zone - No Trust
  - External DMZ - Low Trust
  - Enterprise Zone - Medium Trust
  - Extranet Zone - Medium Trust
  - Internal DMZ - High Trust
  - Management Zone - Highest Trust
  - Restricted Zone - Highest Trust

CIS Top 20 Critical Security Controls

- MAINTAIN AN INVENTORY OF NETWORK BOUNDARIES
  - **Description**: Maintain an up-to-date inventory of all of the organization's network boundaries.



CIS Top 20 Critical Security Controls

- SCAN FOR UNAUTHORIZED CONNECTIONS ACROSS TRUSTED NETWORK BOUNDARIES
  - **Description**: Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.

CIS Top 20 Critical Security Controls

- DENY COMMUNICATION OVER UNAUTHORIZED PORTS
  - **Description**: Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.

CIS Top 20 Critical Security Controls

- Key Takeaways for Control 12
  - Leverage existing controls.
  - Know your network and data boundaries
  - Segment, segment, segment.

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. Are clear business requirements defined each time custom business applications are developed or implemented?
2. Is appropriate security always defined as a business requirement for business application systems?
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

12.1	Deny communications with (or limit data flow to) known malicious IP addresses (black lists), or limit access only to trusted sites (whitelists). Tests can be periodically carried out by sending packets from bogon source IP addresses (non-routable or otherwise unused IP addresses) into the network to verify that they are not transmitted through network perimeters. Lists of bogon addresses are publicly available on the Internet from various sources, and indicate a series of IP addresses that should not be used for legitimate traffic traversing the Internet.
12.2	On DMZ networks, configure monitoring systems (which may be built in to the IDS sensors or deployed as a separate technology) to record at least packet header information, and preferably full packet header and payloads of the traffic destined for or passing through the network border. This traffic should be sent to a properly configured Security Information Event Management (SIEM) or log analytics system so that events can be correlated from all devices on the network.
12.3	Deploy network-based IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These network-based IDS sensors may detect attacks through the use of signatures, network behavior analysis, or other mechanisms to analyze traffic.
12.4	Network-based IPS devices should be deployed to complement IDS by blocking known bad signatures or the behavior of potential attacks. As attacks become automated, methods such as IDS typically delay the amount of time it takes for someone to react to an attack. A properly configured network-based IPS can provide automation to block bad traffic. When evaluating network-based IPS products, include those using techniques other than signature-based detection (such as virtual machine or sandbox-based approaches) for consideration.
12.5	Design and implement network perimeters so that all outgoing network traffic to the Internet must pass through at least one application layer filtering proxy server. The proxy should support decrypting network traffic, logging individual TCP sessions, blocking specific URLs, domain names, and IP addresses to implement a black list, and applying whitelists of allowed sites that can be accessed through the proxy while blocking all other sites. Organizations should force outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter.
12.6	Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication.
12.7	All enterprise devices remotely logging into the internal network should be managed by the enterprise, with remote control of their configuration, installed software, and patch levels. For third-party devices (e.g., subcontractors/vendors), publish minimum security standards for access to the enterprise network and perform a security scan before allowing access.
12.8	Periodically scan for back-channel connections to the Internet that bypass the DMZ, including unauthorized VPN connections and dual-homed hosts connected to the enterprise network and to other networks via wireless, dial-up modems, or other mechanisms.
12.9	Deploy NetFlow collection and analysis to DMZ network flows to detect anomalous activity.
12.10	To help identify covert channels exfiltrating data through a firewall, configure the built-in firewall session tracking mechanisms included in many commercial firewalls to identify TCP sessions that last an unusually long time for the given organization and firewall device, alerting personnel about the source and destination addresses associated with these long sessions.

CIS Top 20 Critical Security Controls

12-1 - Deny communications with (or limit data flow to) known malicious IP addresses (black lists), or limit access only to trusted sites (whitelists).

- Free Tools
  - Sans storm center feed
  - IEEExplore feed
  - Global List
- Commercial Tools
  - Advanced endpoint, NextGen Firewalls (PaloAlto, etc)

CIS Top 20 Critical Security Controls

- 12-2 - On DMZ networks, configure monitoring systems to record at least packet header information, and preferably full packet header and payloads of the traffic destined for or passing through the network border.
  - This traffic should be sent to a properly configured Security Information Event Management (SIEM) or log analytics system so that events can be correlated from all devices on the network.
- **Tools:**
  - This is typically your NGFW, Proxy, IPS logs

CIS Top 20 Critical Security Controls

- 12-3 - Deploy network-based IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These network-based IDS sensors may detect attacks through the use of signatures, network behavior analysis, or other mechanisms to analyze traffic.
  - Free Tools
    - AlienVault OSSIM - contains behavioral monitoring. And a lot of other stuff.
    - Security Onion
    - Suricata – snort beater
    - OSSEC – Host IDS
  - Commercial Tools
    - AlienVault USM - Commercial release of OSSIM
    - NGFWs – PaloAlto, etc
    - SourceFire - Cisco

CIS Top 20 Critical Security Controls

- 12-4 Network-based IPS devices should be deployed to complement IDS by blocking known bad signatures or the behavior of potential attacks. As attacks become automated, methods such as IDS typically delay the amount of time it takes for someone to react to an attack. A properly configured network-based IPS can provide automation to block bad traffic. When evaluating network-based IPS products, include those using techniques other than signature-based detection (such as virtual machine or sandbox-based approaches) for consideration.
- Free Tools
  - Snort - Probably the most used open source IPS
- Commercial Tools
  - Most Firewall devices offer network IPS.

CIS Top 20 Critical Security Controls

- 12-5 - Design and implement network perimeters so that all outgoing network traffic to the Internet must pass through at least one application layer filtering proxy server.
- Free Tools
  - Most modern firewalls provide transparent and non-transparent proxy servers. However, this can severely degrade total throughput. Consider:
  - Squid - Standalone proxy server.
  - IP Fire - open source firewall/proxy that uses squid.
  - Endian - One of my personal favorites. It also uses squid. Very friendly interface.
  - PFSense - Well supported; with frequent updates fixing vulnerabilities as they are detected. Also uses squid, and several others through means of a 3rd party package manager.
- Commercial Tools
  - All of the above tools have paid for enterprise features.

CIS Top 20 Critical Security Controls

- 12-6 -Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication.
- **Free Tools**
  - FreeRADIUS - This is the poor-man's RSA token. But, it works.
  - Authy - 2 factor authentication
- **Commercial Tools**
  - Duo Security Easily the most feature rich and well documented implementations of 2FA.
  - Centrify - The only full function (SSO, Federation, MFA, Privilege acct mgmt

CIS Top 20 Critical Security Controls

- *12-7 - All enterprise devices remotely logging into the internal network should be managed by the enterprise, with remote control of their configuration, installed software, and patch levels. For third-party devices (e.g., subcontractors/vendors), publish minimum security standards for access to the enterprise network and perform a security scan before allowing access.*

  The security scan comes from Network health checks and NPS as outlined in section 1-6.
- *Free Tools*
  - *Spiceworks with MaaS360 - Features are lacking for a free solution, but better than nothing.*
  - *Miradore - Free, unlimited devices, no time limit.*
- *Commercial Tools*
  - *Gets back to CSC 1, 2, 3, Vulnerability scanners*

CIS Top 20 Critical Security Controls

- 12-8 Periodically scan for back-channel connections to the Internet that bypass the DMZ, including unauthorized VPN connections and dual-homed hosts connected to the enterprise network and to other networks via wireless, dial-up modems, or other mechanisms.
- **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

- 12-9 Deploy NetFlow collection and analysis to DMZ network flows to detect anomalous activity.
- **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**
  - Solarwinds
  - ManageEngine
  - Tripwire - heterogeneous server monitoring across Windows, Linux, Solaris, AIX and HP-UX platforms.

CIS Top 20 Critical Security Controls

- 12-10 To help identify covert channels exfiltrating data through a firewall, configure the built-in firewall session tracking mechanisms included in many commercial firewalls to identify TCP sessions that last an unusually long time for the given organization and firewall device, alerting personnel about the source and destination addresses associated with these long sessions.
- **Tools:**
  - This is really only something you can do, if your firewall allows you to do it.

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 July 10th

CIC CSC # 13

Data Protection