SYNERCOMM
SECURE • INTELLIGENT • NETWORKS

CIS Top 20 #9

Limitation and Control of Network Ports

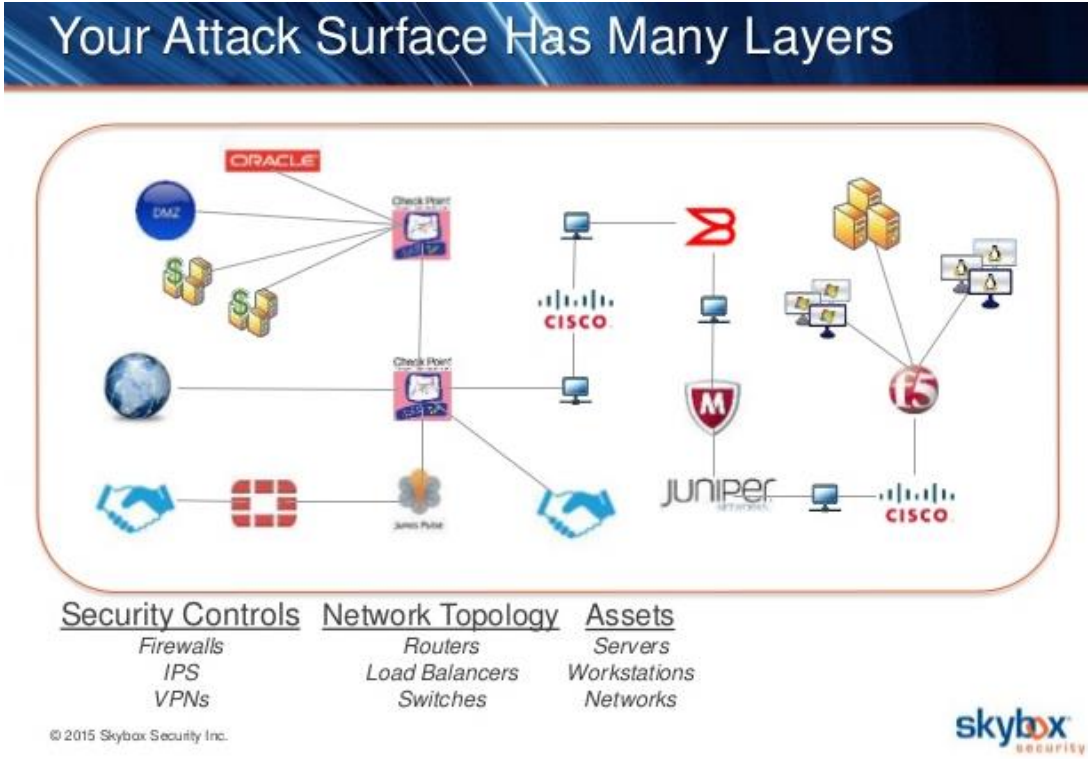
Lisa Niles: CISSP, Director of Solutions Integration

CIS Top 20 Critical Security Controls

CSC # 9 – Limitation and Control of Network Ports

"Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers"

Reduce your attach surface



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

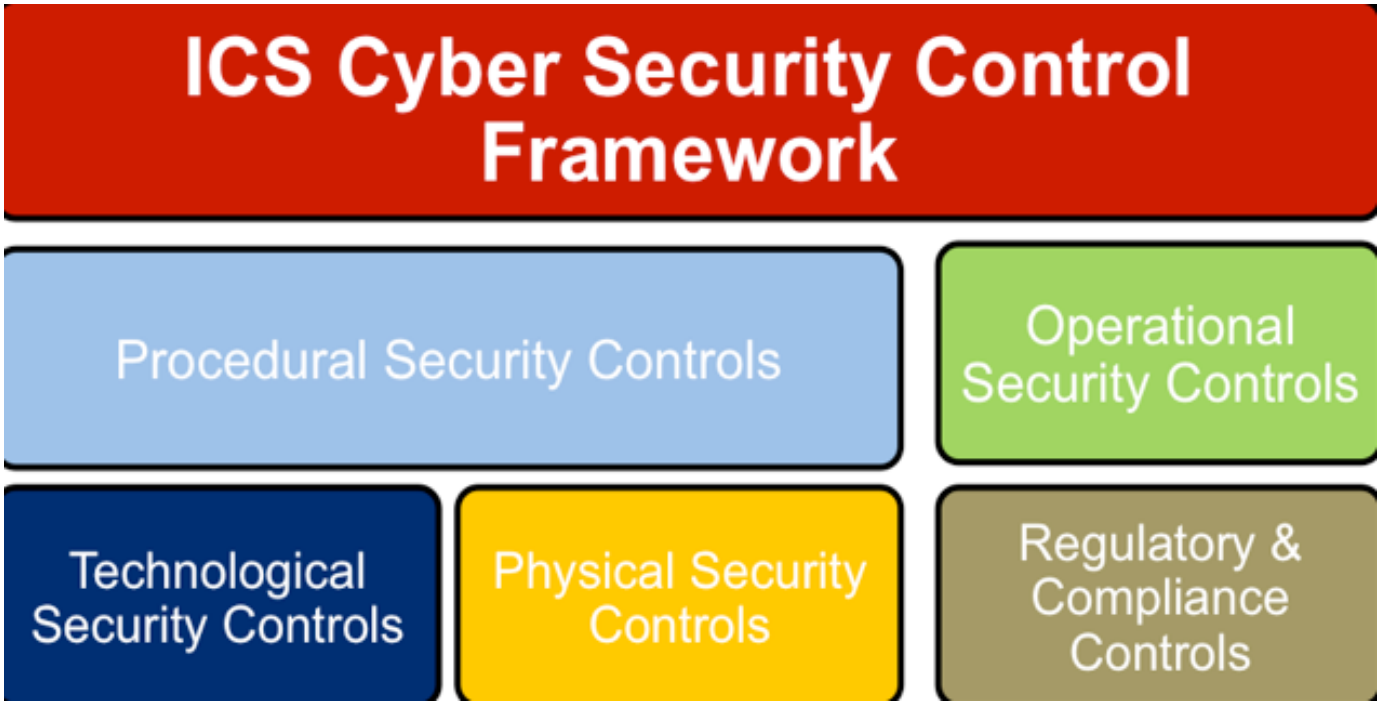
Foundational

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

- Limitation PPS comes down to knowing your environment.
  - Remember CSC #1, #2, #3, #4, #6
  - You get the point…

CIS Top 20 Critical Security Controls

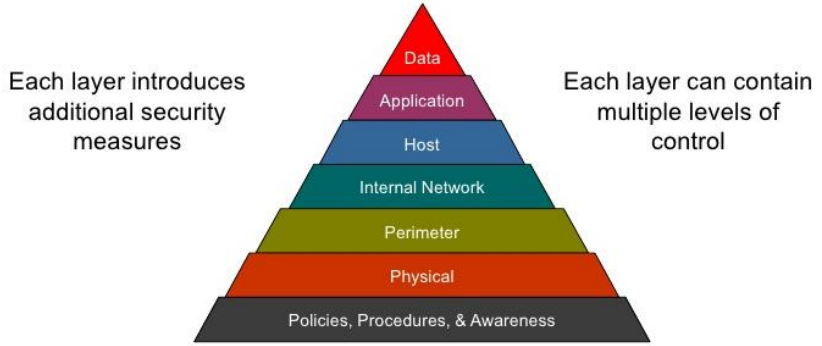
- Key Takeaways for Control 9 (and most CSCs)
  - ”One of the most effective means of mitigating risk exposure is through minimization of the available attack surface”

CIS Top 20 Critical Security Controls

- **Why Is This Control Critical?**
  - Attackers search for remotely accessible network services that are vulnerable to exploitation.

CIS Top 20 Critical Security Controls

- Defense-in-depth
  - Use layered perimeter defenses such as:
    - Application-aware firewalls
    - NAC
    - IDS/IPS
    - HIPS
    - Secure Configs



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

9.1	Ensure that only ports, protocols, and services with validated business needs are running on each system.
9.2	Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
9.3	Perform automated port scans on a regular basis against all key servers and compared to a known effective baseline. If a change that is not listed on the organization's approved baseline is discovered, an alert should be generated and reviewed.
9.4	Verify any server that is visible from the Internet or an untrusted network, and if it is not required for business purposes, move it to an internal VLAN and give it a private address.
9.5	Operate critical services on separate physical or logical host machines, such as DNS, file, mail, web, and database servers.
9.6	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized services or traffic should be blocked and an alert generated.

CIS Top 20 Critical Security Controls

- *9-1* - Ensure that only ports, protocols, and services with validated business needs are running on each system.

- Free Tools
  - Nmap - Well known port scanner available for Windows, Linux, Mac
- Commercial Tools
  - Forescout
  - Qualys
  - Rapid7
  - Tripwire
  - Tenable

CIS Top 20 Critical Security Controls

- *9-2* - Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

- Free Tools
  - The Windows firewall, and GPOs work just great for this.
  - Windows Firewall with Advanced Security has a STIG!
- Commercial Tools
  - Forescout or Adv Endpoint TrendMicro, Kaspersky, Symantec, Sophos, Cylance, CarbonBlack, BitDefender

CIS Top 20 Critical Security Controls

- *9-3* - Perform automated port scans on a regular basis against all key servers and compared to a known effective baseline. If a change that is not listed on the organization's approved baseline is discovered, an alert should be generated and reviewed.

- Free Tools
  - AlienVault OSSIM - HIDS, SEIM, Inventory, Service Monitor
  - Netflow, SNMP, proxy, syslog to SIEM
  - OpenHIDS - Windows only

- Commercial Tools
  - Qualys
  - Rapid7
  - Tenable

CIS Top 20 Critical Security Controls

- *9-4* - Verify any server that is visible from the Internet or an untrusted network, and if it is not required for business purposes, move it to an internal VLAN and give it a private address.
- Tools:
  - WAP –protect direct server interactions
  - Reverse proxy
  - NGFW
  - Micro segmentation

CIS Top 20 Critical Security Controls

- *9-5* - Operate critical services on separate physical or logical host machines, such as DNS, file, mail, web, and database servers.
- Tools:
  - Again, micro segmentation with NGFW

CIS Top 20 Critical Security Controls

- *9-6* Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized services or traffic should be blocked and an alert generated.

- Free Tools
  - ModSecurity - Probably the most well-known open source Layer 7 firewall.
  - AQTronix - Open source WAF, used for Apache and IIS web apps.
- Commercial Tools
  - PaloAlto NGFW, Fortinet, Checkpoint, F5, Netscaler, Barracuda

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 May 15th

CIC CSC # 10

Data Recovery Capability