University Cyber-security Program
Controls Book

Larry Wilson
Version 1.0
November, 2013

Cyber-security Controls Summary

Council on Cyber-security Critical Security Controls (CSC)

CSC-01 IT Asset Management	CSC-02 Software Asset Management	CSC-03 System Configuration	CSC-04 Vulnerability Management	CSC-05 Malware Defenses
CSC-06 Application Security	CSC-07 Wireless Devices	CSC-08 Data Recovery	CSC-09 Security Training	CSC-10 Network Configuration
CSC-11 Ports, Protocols, Services	CSC-12 Administrative Privileges	CSC-13 Boundary Defenses	CSC-14 Audit Logs	CSC-15 Controlled Access
CSC-16 Account Monitoring	CSC-17 Data Loss Prevention	CSC-18 Incident Response	CSC-19 Secure Network Engineering	CSC-20 Penetration Testing

Council on Cyber-security Critical Security Controls

Control Number	Control Description	Page	Control Objective	Control Assessment	Design Specification	Alerting & Reporting
CSC-01	Inventory of Authorized and Unauthorized Devices	4	✓	✓	✓	✓
CSC-02	Inventory of Authorized and Unauthorized Software	6	✓	✓	✓	✓
CSC-03	Secure Configurations for Hardware and Software	8	✓	✓	✓	✓
CSC-04	Continuous Vulnerability Assessment and Remediation	10	✓	✓	✓	✓
CSC-05	Malware Defenses	12	✓	✓	✓	✓
CSC-06	Application Software Security	14	✓	✓	✓	✓
CSC-07	Wireless Device Control	16	✓	✓	✓	✓
CSC-08	Data Recovery Capability	18	✓	✓	✓	✓
CSC-09	Security Skills Assessment and Appropriate Training	20	✓	✓	✓	✓
CSC-10	Secure Configurations for Network Devices	22	✓	✓	✓	✓
CSC-11	Limitation and Control of Ports, Protocols and Services	24	✓	✓	✓	✓
CSC-12	Controlled Use of Administrative Privileges	26	✓	✓	✓	✓
CSC-13	Boundary Defense	28	✓	✓	✓	✓
CSC-14	Maintenance, Monitoring and Analysis of Audit Logs	30	✓	✓	✓	✓
CSC-15	Controlled Access based on the Need to Know	32	✓	✓	✓	✓
CSC-16	Account Monitoring and Control	34	✓	✓	✓	✓
CSC-17	Data Loss Prevention	36	✓	✓	✓	✓
CSC-18	Incident Response and Management	38	✓	✓	✓	✓
CSC-19	Secure Network Engineering	40	✓	✓	✓	✓
CSC-20	Penetration Tests and Red Team Exercises	42	✓	✓	✓	✓

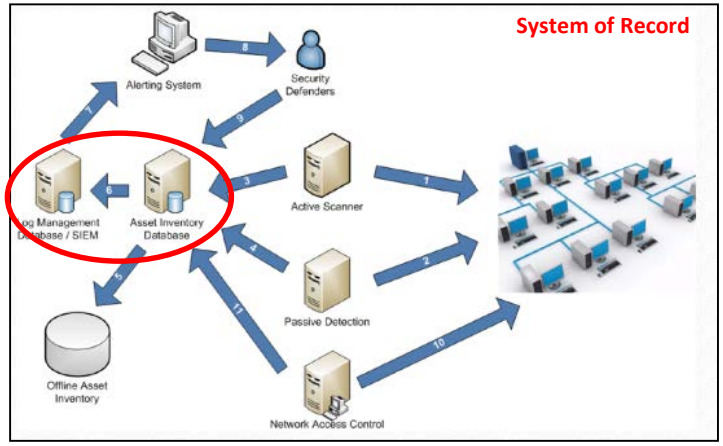
CSC-01: IT Asset Management Control Environment

Control Objective
Reduce the ability of attackers to find and exploit unauthorized and unprotected systems.

Control
Use active monitoring and configuration management to maintain an up-to-date inventory of devices connected to the network, including servers, workstations, laptops, remote devices.

Consequences of not Implementing this control
Criminal groups deploy systems that scan address spaces of target organizations, waiting for new and unprotected systems to be attached to the network. Attackers from anywhere in the world may quickly find and exploit such systems that are accessible via the Internet.

Control System Analysis
ITAM control systems identify new systems introduced into the environment that has not been authorized.



Step 1: Active device scanner scans network systems
Step 2: Passive device scanner captures system information
Step 3: Active scanner reports to inventory database
Step 4: Passive scanner reports to inventory database
Step 5: Inventory database stored offline
Step 6: Inventory database initiates alert system
Step 7: Alert system notifies security defenders
Step 8: Security defenders monitor and secure inventory database
Step 9: Security defenders update secure inventory database
Step 10: Network access control continuously monitors network
Step 11: Network access control checks and provides updates to the asset inventory database.

Control Assessment

Control 1.1 : Deploy an automated asset inventory discovery tool and use it to build a preliminary asset inventory of systems connected to the network. Both active tools that scan through network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.

Control 1.2 : Deploy DHCP Server logging, and utilize a system to improve the asset inventory and help detect unknown systems through this DHCP information.

Control 1.3: All equipment acquisitions should automatically update the inventory system as new, approved devices are connected to the network. A robust change control process can also be used to validate and approve all new devices.

Control 1.4: Maintain an asset inventory of all systems connected to the network and the network devices themselves. The inventory should include every system that has an IP address on the network, including desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), storage area networks, etc. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether or not they are attached to the network.

Control 1.5: Ensure the asset inventory database is properly protected and a copy stored in a secure location.

Control 1.6: In addition to an inventory of hardware, the organization should develop an inventory of information assets that identifies their critical information and maps critical information to the hardware assets (including servers, workstations, and laptops) on which it is located. A department and individual responsible for each information asset should be identified, recorded, and tracked.

Control 1.7: Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. 802.1x must be tied into the inventory data to determine authorized vs. unauthorized systems.

Control 1.8: Deploy network access control (NAC) to monitor authorized systems so if attacks occur, the impact can be remediated by moving the untrusted system to a virtual local area network that has minimal access.

Control 1.9: Create separate VLANs for BYOD systems or other untrusted devices.

Control 1.10: Implement client certificates to validate and authenticate systems prior to connecting to the private network.

CSC-01: IT Asset Management Technical Solution

Design Specification

START

Control Requirements: *Use active monitoring and configuration management to maintain an up-to-date inventory of devices connected to the organization network, including servers, workstations, laptops, and remote devices.*

Design Requirements:

1. Establish IT Asset Management (ITAM) system of record.
- Create initial baseline of known devices and information assets
- Include critical information mapping and information owners

2. Update ITAM with known assets
- Add / remove assets following standard approach
- Create systems build template for new systems
- Create asset deletion / destruction for devices removed from inventory

3. Scan network for unknown assets (active discovery)
- Establish network scanning process to detect unknown devices.
- Run network scan, compare results with inventory, reconcile differences

4. Monitor network for unknown assets (passive discovery)
- Establish traffic monitoring process to detect unknown devices.
- Configure Netflow, AppFlow, Full Packet Capture to ITAM data collectors
- Monitor DHCP scopes on server networks to discover unknown systems

5. Filter network access from unknown assets (Network Access Control)
- *802.1x* - Authentication for devices , users connecting to networks
- NAC - Visibility into network end points, and allows access based on policies
- Client certificates - Identify / authenticate via encrypted digital identification

6. Generate Real-time Alerts and Management Reports
- Alert Security Defenders when suspicious activity is detected.
- Produce management and operations reports (ad-hoc and pre-defined)

7. Update IIT Asset Management (ITAM) system of record.
- Update with known as well as unknown (discovered) devices

Compliance Assessment: *Implement, operate, alert and report using processes and tools to track/control/prevent/correct network access by devices (computers, network components, printers, anything with IP addresses) based on an asset inventory of which devices are allowed to connect to the network.*

END

Alerting & Reporting

START

Control Requirements: *Use active monitoring and configuration management to maintain an up-to-date inventory of devices connected to the organization network, including servers, workstations, laptops, and remote devices.*

Alerting & Reporting Requirements:

1. Establish IT Asset Management (ITAM) system of record.
- Current state network map of asset groupings by domain or network block.
- Monthly report of asset inventory by domain or network block.
- Trend report of changes in asset inventory over 12 months

2. Update ITAM with known assets
- Report of devices added, moved, deleted from asset inventory over previous month.
- Trend report of devices added or removed from asset inventory over past 12 months

3. Scan network for unknown assets (active discovery)
- Report of unknown / unauthorized assets discovered via network scan.
- Trend report of unknown / unauthorized assets via scan over past 12 months

4. Monitor network for unknown assets (passive discovery)
- Report of unknown / unauthorized assets discovered via network monitoring.
- Trend report of unknown / unauthorized assets via monitoring over past 12 months.

5. Filter network access from unknown assets (Network Access Control)
- Report of unknown / unauthorized assets discovered via network filtering.
- Trend report of unknown / unauthorized assets over past 12 months.

6. Generate Real-time Alerts and Management Reports
- Report of all ITAM alerts from previous month.
- Trend report of all ITAM alerts over past 12 months.

7. Update IT Asset Management (ITAM) system of record.
- See ITAM control system of record reports

Compliance Assessment: *Implement, operate, alert and report using processes and tools to track/control/prevent/correct network access by devices (computers, network components, printers, anything with IP addresses) based on an asset inventory of which devices are allowed to connect to the network.*

END

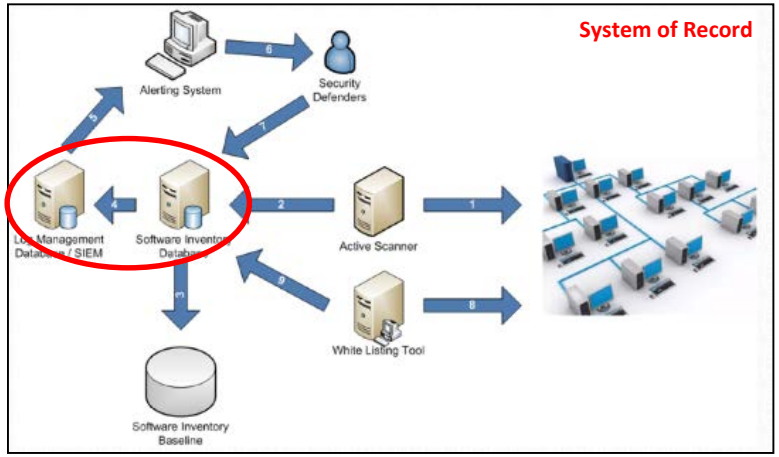
CSC-02: Software Asset Management Control Environment

Control Objective
Identify vulnerable or malicious software to mitigate or root out attacks

Control
Devise a list of authorized software for each type of system, and deploy tools to track software installed (including type, version, and patches) and monitor for unauthorized or unnecessary software.

Consequences of not Implementing this control
Computer attackers deploy systems that continuously scan address spaces of target organizations looking for vulnerable versions of software that can be remotely exploited. Without proper knowledge or control of the software deployed in an organization, defenders cannot properly secure their assets.

Control System Analysis
SAM Control Systems identify new software introduced to the environment that has not been authorized.



Step 1: Active device scanner
Step 2: Active scanner reports to inventory database
Step 3: Inventory database compares to inventory baseline
Step 4: Inventory database initiates alerting system
Step 5: Alert system notifies security defenders
Step 6: Security defenders monitor and secure inventory database
Step 7: Security defenders update software inventory database
Step 8: White listing tool continuously monitors all systems on the network
Step 9: White listing checks and updates to the software inventory database.

Control Assessment

Control 2.1: Deploy application white listing technology that allows systems to run software only if it is included on the white list and prevents execution of all other software on the system. When protecting systems with customized software difficult to white list, isolate the software in virtual operating system that does not retain infections.

Control 2.2: Devise a list of authorized software that is required for each type of system, including servers, workstations, laptops, etc. This list should be monitored by file integrity checking tools to validate authorized software has not been modified.

Control 2.3: Perform regular scanning for unauthorized software and generate alerts when discovered on a system. A strict change-control process should be implemented to control any changes or installation of software to any systems on the network.

Control 2.4: Deploy software inventory tools covering each of the operating system types in use, including servers, workstations, and laptops. Track the version of the underlying operating system as well as the applications installed on it. Record not only the type of software installed on each system, but also its version number and patch level. The software inventory should be tied to vulnerability reporting/threat intelligence services to fix vulnerable software proactively.

Control 2.5: The software inventory systems must be tied into the hardware asset inventory so that all devices and associated software are tracked from a single location.

Control 2.6: The software inventory tool should monitor for unauthorized software installed on each machine. This unauthorized software includes legitimate system administration software installed on inappropriate systems where there is no business need. Dangerous file types (e.g., exe, zip, msi, etc.) should be monitored and/or blocked.

Control 2.7: Software inventory and application white listing should also be deployed on all mobile devices that are utilized across the organization.

Control 2.8: Virtual machines or air-gapped systems used to isolate applications required based on higher risk and should not be installed within a networked environment.

Control 2.9: Configure client workstations with nonpersistent, virtualized operating environments that can be quickly and easily restored to a trusted snapshot on a periodic basis.

Control 2.10: Deploy software that only provides signed software ID tags. A software identification tag is an XML file that is installed alongside software and uniquely identifies the software, providing data for software inventory and asset management.

CSC-02: Software Asset Management Technical Solution

Design Specification

START

Control Requirements: *Devise a list of authorized software for each type of system, and deploy tools to track software installed (including type, version, and patches) and monitor for unauthorized or unnecessary software.*

Design Requirements:

1. Establish Software Asset Management (SAM) system of record.
- Establish SAM database including authorized software
- Include all software (desktops / laptops, servers, networks, mobile devices)

2. Update SAM with authorized software
- Establish process for approving / adding / removing authorized software.
- Establish software whitelist by device type of approved software
- Incorporate SWID tags into standard build process
- Isolate high risk applications on dedicated networks

3. Scan assets for unauthorized software (Active Discovery)
- Establish process for scanning devices to detect unauthorized software.
- Include development, test, prod environments

4. Monitor assets for unauthorized software (Passive Discovery)
- Establish process for monitoring devices to detect unauthorized software.
- Include software on servers, workstations, laptops, networks, etc**.**

5. Restrict assets from unauthorized software uploads (Whitelist / Blacklist)
- Block all software uploads unless on the approved whitelist
- Include development, test, production environments
- Include software on servers, workstations, laptops, networks, etc.

6. Real-time Alerts and Management Reports
- Alert Security Defenders when suspicious activity is detected.
- Produce management and operations reports (ad-hoc and pre-defined)

7. Update Software Asset Management (SAM) system of record.
- Update with known as well as unknown / authorized software

Compliance Assessment: *Implement, operate, alert and report using processes and tools to track/control/prevent/correct installation and execution of software on computers based on an asset inventory of approved software.*

END

Alerting & Reporting

START

Control Requirements: *Devise a list of authorized software for each type of system, and deploy tools to track software installed (including type, version, and patches) and monitor for unauthorized or unnecessary software.*

Alerting & Reporting Requirements:

1. Establish Software Asset Management (SAM) system of record.
- Current state inventory of authorized (whitelist) software programs by asset type
- Monthly inventory of authorized (whitelist) software programs by asset type

2. Update SAM with authorized software
- Report of authorized software added, removed by asset type from previous month.
- Trend report of authorized software added, removed by asset type over past 12 months.

3. Scan assets for unauthorized software (Active Discovery)
- Report of unauthorized (blacklisted) software discovered via device scan.
- Trend report of unauthorized (blacklisted) software via device scan over past 12 months.

4. Monitor assets for unauthorized software (Passive Discovery)
- Report of unauthorized software discovered via device monitoring.
- Trend report of unauthorized software via monitoring over past 12 months.

5. Restrict assets from unauthorized software uploads (Whitelist / Blacklist)
- Monthly report of unauthorized software discovered via device configuration auditing.
- Trend report of unauthorized software over past 12 months.

6. Real-time Alerts and Management Reports
- Report of all SAM alerts from previous month.
- Trend report of all SAM alerts over past 12 months.

7. Update Software Asset Management (SAM) system of record.
- See SAM control system of record reports

Compliance Assessment: *Implement, operate, alert and report using processes and tools to track/control/prevent/correct installation and execution of software on computers based on an asset inventory of approved software.*

END

CSC-03: Server / Desktop Configuration Management Control Environment

Control Objective

Prevent attackers from exploiting services and settings that allow easy access through networks and browsers

Control

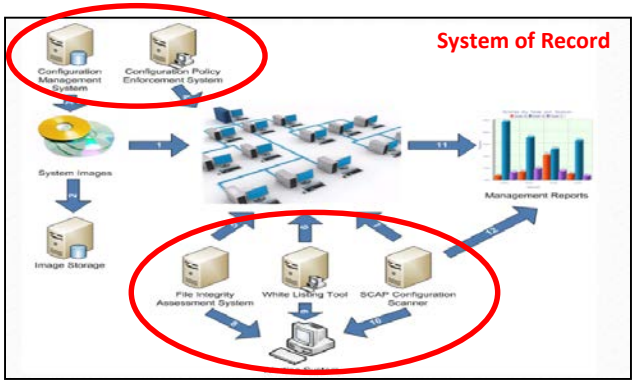
Establishing a secure configuration standard (based on industry best practices such as DISA STIGs, CIS Benchmarks, etc.) ensures the secure configurations are deployed on pre-configured hardened systems, the configurations are updated on a regular basis, and are tracked in a configuration management system

Consequences of not implementing this control

On both the Internet and internal networks that attackers have already compromised, automated computer attack programs constantly search target networks looking for systems that were configured with vulnerable software installed the way it was delivered from manufacturers and resellers, thereby making it immediately vulnerable to exploitation.

Control System Analysis

SDCM Control Systems manage and implement consistent configuration settings to workstations, laptops, servers on the network.



Step 1: Secured system images applied to computer systems
Step 2: Secured system images stored in a secure manner
Step 3:Configuration management system validates and checks system images
Step 4: Scan production systems for misconfigurations or deviations from baselines
Step 5: File integrity assessment systems monitor critical system binaries and data sets
Step 6: White listing tool monitors systems configurations and software
Step 7: SCAP configuration scanner validates configurations
Step 8: File integrity assessment system sends deviations to alerting system
Step 9: White listing tool sends deviations to alerting system
Step 10: SCAP configuration scanner sends deviations to alerting system
Step 11 and 12: Management reports document configuration status

Control Assessment

3.1: Establish and ensure the use of standard secure configurations of your operating systems. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system.

3.2: Implement automated patching tools and processes that ensure security patches are installed within 48 hours of their release (applications and for operating system software)

3.3: Limit administrative privileges to very few users who have the knowledge and a business need to modify the configuration of the underlying operating system

3.4: Follow strict configuration management, building a secure image that is used to build all new systems that are deployed. Any compromised system should be re-imaged.

3.5: Store master images on securely configured servers, with integrity checking tools and change management to ensure that only authorized changes to the images are possible.

3.6: Any deviations from the standard build or updates to the standard build should be approved by a change control board and documented in a change management system.

3.7: Negotiate contracts to buy systems configured securely out of the box using standardized images, which should be devised to avoid extraneous software that would increase their attack surface and susceptibility to vulnerabilities.

3.8: Utilize application white listing to control and manage any configuration changes to the software running on the system.

3.9: Remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, etc., should only be used if they are performed over a secondary encryption channel, such as SSL or IPSEC.

3.10: Utilize file integrity checking tools on a weekly basis to ensure critical system files have not been altered. All alterations to files should be reported to security personnel.

3.11: Implement and test an automated configuration monitoring system that measures all secure configuration elements that can be measured through remote testing.

3.12: Deploy system configuration management tools, such as Active Directory Group Policy Objects for Microsoft Windows systems or Puppet for Unix systems that will automatically enforce and redeploy configuration settings at regularly scheduled intervals.

3.13: Establish formal process and management approach for controlling mobile devices.

CSC-03: Server / Desktop Configuration Management Technical Solution

Design Specification

START

Control Requirements: *Establishing a secure configuration standard (based on industry best practices such as DISA STIGs, CIS Benchmarks, etc.) ensures the secure configurations are deployed on pre-configured hardened systems, the configurations are updated on a regular basis, and are tracked in a configuration management system*

Design Requirements:

1. Establish Server / Desktop Configuration Management (SDCM) system of record.
- Establish SDCM system of record based on known configurations
- Include all desktops, laptops, servers, mobile devices

2. Create approved server, desktop configuration standards
- Establish secure configuration standards for servers & desktops based on CIS baselines.
- Compare new server, desktop, laptop builds with standard configuration image

3. Scan desktops, servers for unauthorized configuration changes
- Establish change management process for authorized configuration changes
- Scan devices to detect unauthorized configuration changes
- Compare differences between current server, desktop and baseline configurations
- Determine whether configuration changes are authorized (change management)

4. Monitor desktops, servers for unauthorized configuration changes
- Establish change management process for authorized configuration changes
- Monitor devices to detect unauthorized configuration changes
- Compare differences between current server, desktop and baseline configurations
- Determine whether configuration changes are authorized (change management)

5. Restrict unauthorized server, desktop configuration changes
- Establish change management process for authorized configuration changes
- Detect and block unauthorized configuration changes

6. Real-time Alerts and Management Reports
- Alert Security Defenders when suspicious activity is detected.
- Produce management and operations reports (ad-hoc and pre-defined)

7. Update Server / Desktop Configuration Management (SDCM) system of record.
- Update with new / authorized configuration standards

Compliance Assessment: *Implement, operate, alert and report using processes and tools to track/control/prevent/correct security weaknesses in the configurations of the hardware and software of mobile devices, laptops, workstations, and servers based on a formal configuration management and change control process.*

END

Alerting & Reporting

START

Control Requirements: *Establishing a secure configuration standard (based on industry best practices such as DISA STIGs, CIS Benchmarks, etc.) ensures the secure configurations are deployed on pre-configured hardened systems, the configurations are updated on a regular basis, and are tracked in a configuration management system*

Alerting & Reporting Requirements:

1. Establish Server / Desktop Configuration Management (SDCM) system of record.
- Current state inventory of baseline device configurations by asset type
- Monthly inventory of baseline device configurations by asset type

2. Create approved server, desktop configuration standards
- Report of configurations added to baseline inventory
- Report of configurations removed from baseline inventory

3. Scan desktops, servers for unauthorized configuration changes
- Monthly report of unknown / unauthorized configurations discovered via device scan.
- Trend report of unknown / unauthorized configurations over past 12 months

4. Monitor desktops, servers for unauthorized configuration changes
- Report of unknown / unauthorized configurations discovered via device monitoring.
- Trend report of unknown / unauthorized configurations over past 12 months.

5. Restrict unauthorized server, desktop configuration changes
- Report of unknown / unauthorized configurations discovered via device configuration auditing.
- Trend report of unknown / unauthorized configurations over past 12 months.

6. Real-time Alerts and Management Reports
- Report of all SDCM alerts from previous month.
- Trend report of all SDCM alerts over past 12 months.

7. Update Server / Desktop Configuration Management (SDCM) system of record.
- See SDCM control system of record reports

Compliance Assessment: *Implement, operate, alert and report using processes and tools to track/control/prevent/correct security weaknesses in the configurations of the hardware and software of mobile devices, laptops, workstations, and servers based on a formal configuration management and change control process.*

END

CSC-04: Vulnerability Management Control Environment

Control Objective

Proactively identify and repair software vulnerabilities reported by security researchers or vendors

Control

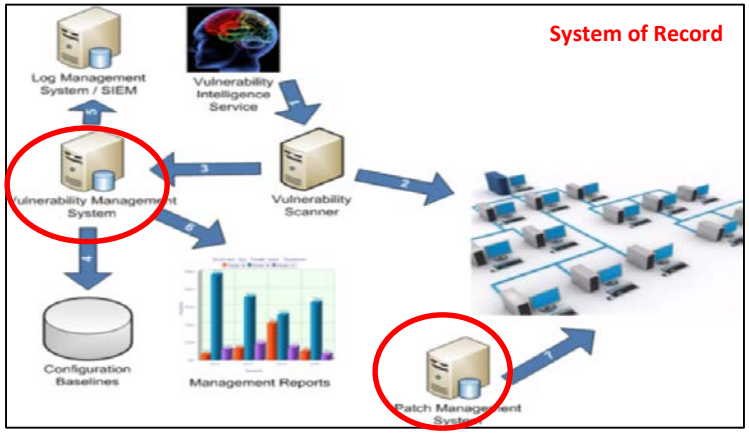
Regularly run automated vulnerability scanning tools against all systems and quickly remediate any vulnerabilities, with critical problems fixed within 48 hours.

Consequences of not implementing this control

Soon after new vulnerabilities are discovered and reported by security researchers or vendors, attackers engineer exploit code and then launch that code against targets of interest. Any significant delays in finding or fixing software with dangerous vulnerabilities provides ample opportunity for persistent attackers to break through, gaining control over the vulnerable machines and getting access to the sensitive data they contain

Control System Analysis

VM Control Systems include vulnerability scanners, management system, patch management systems, and configuration baselines that work together to address vulnerability management and remediation.



Step 1: Vulnerability intelligence service provides inputs to vulnerability scanner
Step 2: Vulnerability scanners scan production systems
Step 3: Scanners report detected vulnerabilities to Vulnerability Management System (VMS)
Step 4: The VMS compares production systems to configuration baselines
Step 5: The VMS sends information to log management correlation system
Step 6: The VMS produces reports for management
Step 7: A patch management system applies software updates to production systems.

Control Assessment

4.1: Run automated vulnerability scanning tools against all systems on their networks on a weekly or more frequent basis. Any vulnerability identified should be remediated in a timely manner, with critical vulnerabilities fixed within 48 hours.

4.2: Event logs should be correlated with information from vulnerability scans to verify activity of the regular vulnerability scanning tools is logged, and to correlate attack detection events with earlier vulnerability scanning results to determine whether the exploit was used against a known-vulnerable target.

4.3: Deploy automated patch management tools and software update tools for operating system and third-party software on all systems for which such tools are available and safe.

4.4: In order to overcome limitations of unauthenticated vulnerability scanning, ensure that all vulnerability scanning is performed 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.

4.5: 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.

4.6: Vulnerability scanning tools should be tuned to compare services that are listening on each machine against a list of authorized services.

4.7: Security personnel should chart the numbers of unmitigated, critical vulnerabilities for each department/division.

4.8: Security personnel should share vulnerability reports indicating critical issues with senior management to provide effective incentives for mitigation.

4.9: Measure the delay in patching new vulnerabilities and ensure that the delay is equal to or less than the benchmarks set forth by the organization.

4.10: Critical patches must be evaluated in a test environment before being pushed into production on organization systems

CSC-04: Vulnerability Management Technical Solution

Design Specification

START

Control Requirements: *Regularly run automated vulnerability scanning tools against all systems and quickly remediate any vulnerabilities, with critical problems fixed within 48 hours.*

Design Requirements:

1. Establish Vulnerability Management (VM) system of record.
- Align with Asset Management Inventory (hardware, OS , software applications, owner)

2. Create approved build standards
- Include vulnerability scanning and remediation as part of standard build process.
- Monitor industry sources (X-Force, vendors, etc.) for vulnerability announcements

3. Scan devices for known vulnerabilities
- Conduct regular internal, external vulnerability scans (including authenticated scans)
- Notify network and system administrators of discovered vulnerabilities
- Correlate vulnerabilities with event logs to detect attacks and compare to prior scans
- Test patches and deploy patches using patch management tools
- Monitor and report on vulnerability remediation activities
- Establish and publish Vulnerability Assessment Program metrics & report**s**

4. Monitor intelligence sources for zero-day vulnerability announcements.
- Monitor networks for new discovered vulnerabilities
- Monitor industry sources (X-Force, vendors, etc.) for vulnerability announcements
- Document results and assign to network and system administrators for remediation

5. Restrict access to devices with vulnerabilities
- Monitor systems connecting to the network for vulnerabilities
- Upgrade, patch or remove risky services from devices with known vulnerabilities
- Remove vulnerable devices from the network that have not been remediated

6. Real-time Alerts and Management Reports
- Alert Security Defenders when suspicious activity is detected.
- Produce management and operations reports (ad-hoc and pre-defined)

7. Update Vulnerability Management (VM) system of record
- Update with new / authorized configuration standards

Compliance Assessment: *Implement, operate, alert and report using processes and tools to detect/prevent/correct security vulnerabilities in the configurations of devices that are listed and approved in the asset inventory database.*

END

Alerting & Reporting

START

Control Requirements: *Regularly run automated vulnerability scanning tools against all systems and quickly remediate any vulnerabilities, with critical problems fixed within 48 hours.*

Alerting & Reporting Requirements:

1. Establish Vulnerability Management (VM) system of record.
- Current state inventory of vulnerabilities by asset type
- Monthly report of vulnerabilities by asset type

2. Create approved build standards
- Report of critical assets , internal & external vulnerabilities from previous month.
- Trend report of critical assets, internal & external vulnerabilities over 12 months.

3. Scan devices for known vulnerabilities
- Report of assets with vulnerabilities discovered via active network scan.
- Trend report of assets with vulnerabilities over past 12 months

4. Monitor intelligence sources for zero-day vulnerability announcements.
- Monthly report of assets with vulnerabilities discovered via passive network scan
- Trend report of assets with vulnerabilities discovered over past 12 months

5. Restrict access to devices with vulnerabilities
- Report of vulnerabilities discovered via threat / vulnerability intelligence
- Trend report of assets with vulnerabilities discovered over past 12 months.

6. Real-time Alerts and Management Reports
- Report of all VM alerts from previous month.
- Trend report of all VM alerts over past 12 months.

7. Update Vulnerability Management (VM) system of record
- See VM control system of record reports

Compliance Assessment: *Implement, operate, alert and report using processes and tools to detect/prevent/correct security vulnerabilities in the configurations of devices that are listed and approved in the asset inventory database.*

END

CSC-05: Malware Defenses Control Environment

Control Objective

The processes and tools used to detect/prevent/correct installation and execution of malicious software on all devices.

Control

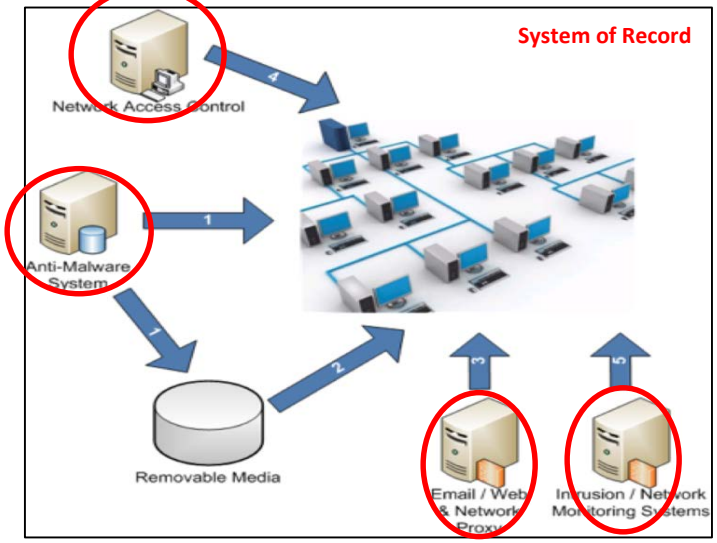
Use automated ant-virus and anti-spyware software to continuously monitor and protect workstations, servers, and mobile devices. Automatically update such anti-malware tools on all machines on a daily basis. Prevent network devices from using auto-run programs to access removable media.

Consequences of not Implementing this Control

Malicious software is an integral and dangerous aspect of Internet threats, targeting end-users and organizations via web browsing, e-mail attachments, mobile devices, the cloud, and other vectors. Malicious code may tamper with the system's contents, capture sensitive data, and spread to other systems.

Control System Analysis

The control system includes anti-malware systems and threat vectors such as removable media.



Step 1: Anti-malware systems analyze production systems and removable media
Step 2: Removable media is analyzed when connected to production systems
Step 3: Email/web and network proxy devices analyze incoming and outgoing traffic
Step 4: Network access control monitors all systems connected to the network
Step 5: Intrusion/network monitoring systems perform continuous monitoring looking for signs of malware.

Control Assessment

5.1: Employ automated tools to continuously monitor workstations, servers, and mobile devices for active, up-to-date anti-malware protection with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to anti-malware administration tools and event log servers.

5.2: Employ anti-malware software and signature auto update features or have administrators manually push updates to all machines on a daily basis. After applying an update, automated systems should verify that each system has received its signature update.

5.3: Configure laptops, workstations, and servers so that they will not auto-run content from USB tokens (i.e., "thumb drives"), USB hard drives, CDs/DVDs, Firewire devices, external serial advanced technology attachment devices, mounted network shares, or other removable media.

5.4: Configure systems so that they conduct an automated anti-malware scan of removable media when it is inserted.

5.5: All attachments entering the organization's e-mail gateway should be scanned and blocked if they contain malicious code or file types unneeded for the organization's business. This scanning should be done before the e-mail is placed in the user's inbox. This includes email content filtering and web content filtering.

5.6: Automated monitoring tools should use behavior-based anomaly detection to complement and enhance traditional signature-based detection.

5.7: Deploy network access control tools to verify security configuration and patch-level compliance before granting access to a network.

5.8: Continuous monitoring should be performed on outbound traffic. Any large transfers of data or unauthorized encrypted traffic should be flagged and, if validated as malicious, the computer should be moved to an isolated VLAN.

5.9: Implement an Incident Response process which allows their IT Support organization to supply their Security Team with samples of malware running undetected on corporate systems. Samples should be provided to the Anti-Virus vendor for 'out-of-band' signature creation and deployed to the organization by system administrators.

CSC-05: Malware Defenses Technical Solution

Design Specification

START

Control Requirements: *Use automated ant-virus and anti-spyware software to continuously monitor and protect workstations, servers, and mobile devices. Automatically update such anti-malware tools on all machines on a daily basis. Prevent network devices from using auto-run programs to access removable media.*

Design Requirements:

1. Establish Malware Defenses (MD) system of record
- Align with Asset Management system of record

2. Incorporate anti-malware into standard builds
- Implement desktop, laptop, server anti-malware software

3. Scan devices for known malware indicators
- Desktops, servers are scanned daily for known malware
- Anti-malware systems analyze production systems and removable media
- Removable media is analyzed when connected to production systems

4. Monitor intelligence sources for known malware and zero-day threats
- Email devices analyze incoming and outgoing traffic for malware
- Web proxy devices analyze incoming and outgoing traffic for malware
- Network malware defenses monitor for BotNet command and control
- Monitor industry sources (X-Force, vendors, etc.) for zero-day malware indicators

5. Filter network access from devices with suspected malware
- Monitor systems that attempt to connect to the network for instances of malware
- Perform continuous monitoring looking for signs of malware

6. Real-time Alerts and Management Reports
- Alert Security Defenders when suspicious activity is detected.
- Produce management and operations reports (ad-hoc and pre-defined)

7. Update Malware Defenses (MD) system of record
- Update malware inventory through build, scan, monitor, filter processes above
- Advise asset owners of changes and receive approval of updated inventory

Compliance Assessment: *Implement, operate, alert and report using processes and tools to detect/prevent/correct installation and execution of malicious software on all devices.*

END

Alerting & Reporting

START

Control Requirements: *Use automated ant-virus and anti-spyware software to continuously monitor and protect workstations, servers, and mobile devices. Automatically update such anti-malware tools on all machines on a daily basis. Prevent network devices from using auto-run programs to access removable media.*

Alerting & Reporting Requirements:

1. Establish Malware Defenses (MD) system of record
- Current state inventory of malware by asset type
- Monthly report of malware by asset type

2. Incorporate anti-malware into standard builds
- Report of critical assets and associated malware from previous month.
- Trend report of critical assets and associated malware over 12 months.

3. Scan devices for known malware indicators
- Report of assets with unknown malware via active device scan from previous month.
- Trend report of assets with unknown malware via active device scan over 12 months

4. Monitor intelligence sources for known malware and zero-day threats
- Report of assets with unknown malware via passive device scan from previous month.
- Trend report of assets with unknown malware over past 12 months

5. Filter network access from devices with suspected malware
- Report of assets with unknown malware via event correlation from previous month.
- Trend report of assets with unknown malware over 12 months.

6. Real-time Alerts and Management Reports
- Report of all unknown malware alerts from previous month.
- Trend report of unknown malware alerts over past 12 months.

7. Update Malware Defenses (MD) system of record
- See MD control system of record reports

Compliance Assessment: *Implement, operate, alert and report using processes and tools to detect/prevent/correct installation and execution of malicious software on all devices.*

END

CSC-06: Application Security Control Environment

Control Objective

The processes and tools organizations use to detect/prevent/correct security weaknesses in the development and acquisition of software applications

Control

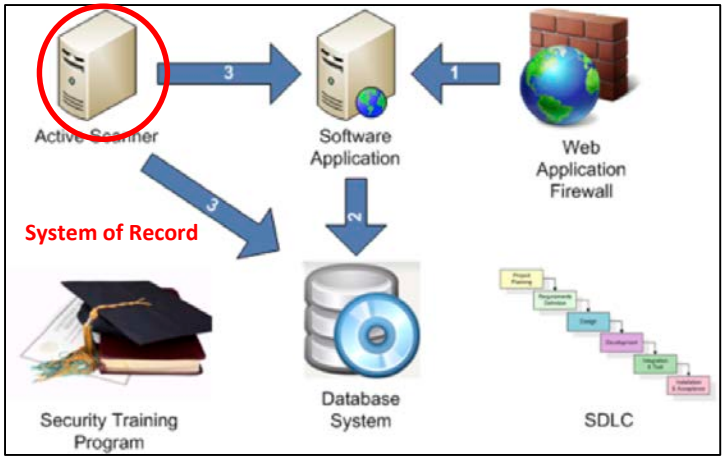
Carefully test internally developed and third-party application software for security flaws, including coding errors and malware. Deploy web application firewalls that inspect traffic, and explicitly check for errors in all user input (including by size and data type).

Consequences of not implementing this control

Attacks against vulnerabilities in web-based and other application software have been a top priority for criminal organizations in recent years. Application software that does not properly check the size of user input, fails to CSCitize user input by filtering out unneeded but potentially malicious character sequences, or does not initialize and clear variables properly could be vulnerable to remote compromise. Attackers can inject specific exploits, including buffer overflows, SQL injection attacks, cross-site scripting, cross-site request forgery, and clickjacking of code to gain control over vulnerable machines.

Control System Analysis

The process of monitoring applications and using tools that enforce a security style when developing applications.



Step 1: Web application firewalls protect connections to internal web applications
Step 2: Software applications securely connect to database systems
Step 3: Code analysis and vulnerability scanning tools scan application systems and database systems.

Control Assessment

6.1: Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks, including but not limited to cross-site scripting, SQL injection, command injection, and directory traversal attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.

6.2: At a minimum, explicit error checking should be done for all input. Whenever a variable is created in source code, the size and type should be determined. When input is provided by the user it should be verified that it does not exceed the size or the data type of the memory location in which it is stored or moved in the future.

6.3: Test in-house-developed and third-party-procured web applications for common security weaknesses using automated remote web application scanners prior to deployment, whenever updates are made to the application, and on a regular recurring basis.

6.4: Do not display system error messages to end-users (output CSCitization).

6.5: Maintain separate environments for production and nonproduction systems. Developers should not typically have unmonitored access to production environments.

6.6: Test in-house-developed and third-party-procured web and other application software for coding errors and malware insertion, including backdoors, prior to deployment using automated static code analysis software. If source code is not available, test compiled code using static binary analysis tools. In particular, input validation and output encoding routines of application software should be carefully reviewed and tested.

6.7: For applications that rely on a database, conduct a configuration review of both the operating system housing the database and the database software itself, checking settings to ensure that the database system has been hardened using standard hardening templates. All of the organization's systems that are part of critical business processes should also be tested.

6.8: Ensure that all software development personnel receive training in writing secure code for their specific development environment.

6.9: Uninstall or remove from the system sample scripts, libraries, components, compilers, or any other unnecessary code that is not being used by an application.

CSC-06: Application Security Technical Solution

Design Specification

START

Control Requirements: *Carefully test internally developed and third-party application software for security flaws, including coding errors and malware. Deploy web application firewalls that inspect traffic, and explicitly check for errors in all user input (including by size and data type).*

Design Requirements:

1. Establish Application Security (AS) system of record
- Establish inventory of critical applications
- Document security controls for all critical applications

2. Incorporate Application Security into Application Development / Procurement process
- Establish SDLC process for application development
- Incorporate static & dynamic code testing into application development process
- Ensure purchased software applications incorporate secure code development practices

3. Scan applications for application level vulnerabilities
- Conduct monthly web application scans for vulnerabilities (OWASP top 10) and errors

4. Monitor applications for unknown threats & vulnerabilities
- Implement Web Application Firewalls (WAFs) to detect application level threats
- Monitor industry sources (X-Force, vendors, etc.) for zero-day application-level threat indicators

5. Restrict access to applications based on unknown / suspicious behavior
- Configure IPS, Firewalls, BotNet monitoring systems to block known application attacks

6. Real-time Alerts and Management Reports
- Alert Security Defenders when suspicious activity is detected.
- Produce management and operations reports (ad-hoc and pre-defined)

7. Update Application Security system of record
- Update with new / authorized malware signatures

Compliance Assessment: *Implement, operate, alert and report using processes and tools to detect/prevent/correct security weaknesses in the development and acquisition of software applications*

END

Alerting & Reporting

START

Control Requirements: *Carefully test internally developed and third-party application software for security flaws, including coding errors and malware. Deploy web application firewalls that inspect traffic, and explicitly check for errors in all user input (including by size and data type).*

Alerting & Reporting Requirements:

1. Establish Application Security (AS) system of record
- Application inventory by business criticality / location for dev, test, prod environments
- Monthly report of applications added to inventory for all environments (dev, test, prod).

2. Incorporate Application Security into Application Development / Procurement process
- Report of known vulnerabilities for applications (dev, test, and prod environments).
- Trend report of known vulnerabilities for all applications over past 12 months.

3. Scan applications for application level vulnerabilities
- Report of unknown vulnerabilities discovered through active application scanning for all environments (dev, test, prod)
- Trend report of unknown vulnerabilities discovered through active application scanning for all environments over past 12 months

4. Monitor applications for unknown threats & vulnerabilities
- Report of unknown vulnerabilities discovered through passive application scanning for all environments (dev, test, prod)
- Trend report of unknown vulnerabilities discovered through passive application scanning for all environments (dev, test, prod) over past 12 months

5. Restrict access to applications based on unknown / suspicious behavior
- Monthly report of applications with unknown malware and attack probes via web and database logs for all environments.
- Trend report of applications with unknown malware and attack probes via web and database logs for all environments. over past 12 months.

6. Real-time Alerts and Management Reports
- Report of all application alerts from previous month.
- Trend report of all application alerts over past 12 months.

7. Update Application Security system of record
- See AS control system of record reports

Compliance Assessment: *Implement, operate, alert and report using processes and tools to detect/prevent/correct security weaknesses in the development and acquisition of software applications*

END

CSC-07: Wireless Devices Control Environment

Control Objective

The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.

Control

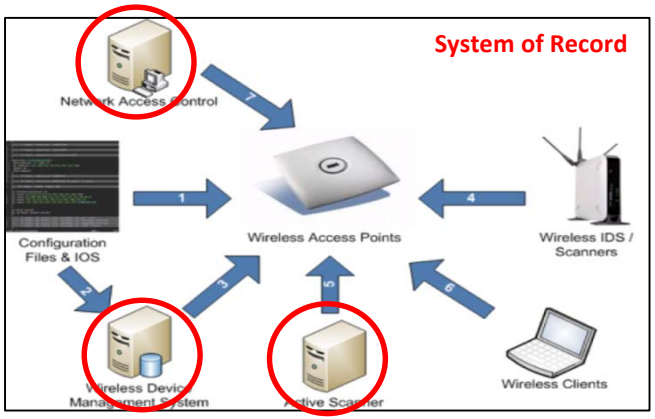
Allow wireless devices to connect to the network only if they match an authorized configuration and security profile and have a documented owner and defined business need. Ensure that all wireless access points are manageable using enterprise management tools. Configure scanning tools to detect wireless access points.

Consequences of not implementing this control

Major thefts of data have been initiated by attackers who have gained wireless access to organizations from outside the physical building, bypassing organizations' security perimeters by connecting wirelessly to access points inside the organization. Wireless clients accompanying traveling officials are infected on a regular basis through remote exploitation during air travel or in cyber cafes. Such exploited systems are then used as back doors when they are reconnected to the network of a target organization

Control System Analysis

The configuration and management of wireless devices, wireless IDS/scanners, wireless device management systems, and vulnerability scanners



Step 1: Hardened configurations applied to wireless devices
Step 2: Hardened configurations managed by a configuration management system
Step 3: Configuration management system manages the configurations on wireless devices
Step 4: Wireless IDS monitor usage of wireless communications
Step 5: Vulnerability scanners scan wireless devices for potential vulnerabilities
Step 6: Wireless clients utilize wireless infrastructure systems in a secure manner.

Control Assessment

7.1: Ensure each wireless device connected to the network matches an authorized configuration and security profile, with documented owner and business need.

7.2: All wireless access points are manageable using organization management tools.

7.3: Network vulnerability scanning tools are configured to detect wireless access points connected to the wired network. Unauthorized (rogue) access points are deactivated.

7.4: Use wireless intrusion detection systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromises.

7.5: 802.1x is used to control devices allowed to connect to the wireless network.

7.6: A site survey is performed to determine what areas that need coverage.

7.7: Where a specific business need for wireless access has been identified, configure wireless access on client machines to allow access only to authorized wireless networks.

7.8: For devices that do not have an essential wireless business purpose, disable wireless access in the hardware configuration**.**

7.9: Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least WiFi Protected Access 2 (WPA2) protection**.**

7.10: Wireless networks use authentication (Extensible Authentication Protocol-Transport Layer Security EAP/TLS), with credential protection and mutual authentication**.**

7.11: Ensure that wireless clients use strong, multi-factor authentication credentials to mitigate the risk of unauthorized access from compromised credentials.

7.12: Disable peer-to-peer wireless network capabilities on wireless clients, unless such functionality meets a documented business need.

7.13: Disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need.

7.14: Wireless access points are not directly connected to the private network. They are either placed behind a firewall or a separate VLAN with traffic examined and filtered.

7.15: All mobile devices must be registered prior to connecting to the wireless network.

7.16: Configure all wireless clients used to access private networks or handle the organization's data in a manner so that they cannot be used to connect to public wireless networks.

CSC-07: Wireless Devices Technical Solution

Design Specification

START

Control Requirements: *Allow wireless devices to connect to the network only if they match an authorized configuration and security profile and have a documented owner and defined business need. Ensure that all wireless access points are manageable using enterprise management tools. Configure scanning tools to detect wireless access points.*

Design Requirements:

1. Establish Wireless LAN (WLAN) system of record
- Includes both IT supported WLANS and Rogue WLANS
- Maintain inventory of Wireless Networks
- Physically secure access points

2. Establish WLAN build and configuration standards
- Includes CIS Benchmark for Wireless Network Device
- Includes Wireless Vendor recommended configuration
- Incorporate WPA-2 encryption capability

3. Scan wireless networks for unknown devices
- Detect and report instances of unknown device discovery including rogue devices

4. Monitor wireless networks for unknown devices
- Identify / disable rogue wireless networks
- Incorporate Wireless Intrusion Protection Services (WIPS) to block wireless attacks
- Monitor threat intelligence sources for zero-day wireless threats

5. Filter wireless access based on known devices
- Detect / block WLAN threats and attacks

6. Real-time Alerts and Management Reports
- Alert Security Defenders when suspicious activity is detected.
- Produce management and operations reports (ad-hoc and pre-defined)

7. Update Wireless LAN (WLAN) system of record
- Advise asset owners of changes and receive approval of updated inventory

Compliance Assessment: *Implement, operate, alert and report using processes and tools to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.*

END

Alerting & Reporting

START

Control Requirements: *Allow wireless devices to connect to the network only if they match an authorized configuration and security profile and have a documented owner and defined business need. Ensure that all wireless access points are manageable using enterprise management tools. Configure scanning tools to detect wireless access points.*

Alerting & Reporting Requirements:

1. Establish Wireless LAN (WLAN) system of record
- Inventory of WLANs by organization, location, configuration (public vs. private)
- Monthly report of WLANs by organization, location, configuration (public vs. private)

2. Establish WLAN build and configuration standards
- Report of WLANs added / removed by organization, location, configuration
- Trend report of WLANs added /removed over past 12 months

3. Scan wireless networks for unknown devices
- Report of unknown wireless access points and SSIDs discovered via active WLAN scan.
- Trend report of unknown wireless access points and SSIDs discovered through active WLAN scan over past 12 months

4. Monitor wireless networks for unknown devices
- Report of unknown wireless devices that perform NAT services discovered through passive WLAN scan.
- Trend report of unknown devices that perform NAT services discovered through passive WLAN scan over past 12 months

5. Filter wireless access based on known devices
- Report of unknown wireless devices discovered through monitoring and analysis of activity logs
- Trend report of unknown wireless devices discovered through monitoring and analysis of activity logs over past 12 months.

6. Real-time Alerts and Management Reports
- Report of all WLAN alerts over previous month.
- Trend report of all WLAN alerts over past 12 months.

7. Update Wireless LAN (WLAN) system of record
- See WLAN control system of record reports

Compliance Assessment: *Implement, operate, alert and report using processes and tools to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.*

END

CSC-08: Backup and Recovery Control Environment

Control Objective

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

Control

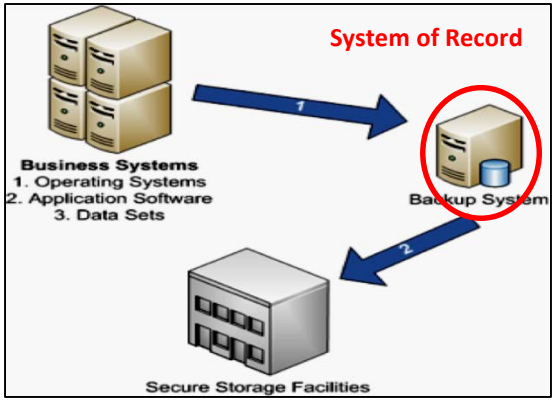
Implement trustworthy plan for removing all traces of an attack. Automatically back up all information required to fully restore each system, including the operating system, application software, and data. Back up all systems at least weekly; back up sensitive systems more often. Regularly test the restoration process.

Consequences of not Implementing this control

When attackers compromise machines, they often make significant changes to configurations and software. Sometimes attackers also make subtle alterations of data stored on compromised machines, potentially jeopardizing organizational effectiveness with polluted information. When the attackers are discovered, it can be extremely difficult for organizations without a trustworthy data recovery capability to remove all aspects of the attacker's presence on the machine..

Control System Analysis

The capability to restore systems in the event that data need to be restored because of a data loss or breach of a system. While backups are certainly an important part of this process, the ability to restore data is the critical component.



Step 1: Production business systems backed up on a regular basis to authorized backup systems
Step 2: Backups created are stored offline at secure storage facilities

Control Assessment

8.1: Each system should be automatically backed up on at least a weekly basis, and more often for systems storing sensitive information.

8.2: Operating systems, application software, and organization data should be included in the overall backup procedure.

8.3: Data on backup media should be tested on a regular basis by performing a data restoration process.

8.4: Key personnel should be trained on both the backup and restoration processes.

8.5: Alternative personnel should be trained on the restoration process in case the primary point of contact is not available.

8.6: Backups should be properly protected via physical security or encryption when stored locally, or transmitted across the network.

8.7: Backup media, such as hard drives and tapes, should be stored in physically secure, locked facilities

CSC-08: Backup and Recovery Technical Solution

Design Specification

START

Control Requirements: Automatically back up all information required to fully restore each system, including the operating system, application software, and data. Back up all systems at least weekly; back up sensitive systems more often. Regularly test the restoration process.

Design Requirements:

1. Establish Back-up and Recovery (BAR) system of record
- Inventory all systems with back-up enabled

2. Create approved Back-up, Recovery, Retention Standards
- Include operating systems, application software, and information in backup procedure.
- Test data on backup media on a regular basis by performing a data restoration process.
- Train on both the backup and restoration processes.
- Ensure backups are protected via physical security, storage or transmission encryption.
- Ensure backup media such as tape drives are protected via physical security

3. Incorporate back-up software / schedule in standard build
- Establish a schedule for incremental and full system backups
- Ensure systems (databases, file systems, network devices, applications, etc.) are included in back-up schedule.

4. Monitor production systems to ensure successful back-ups
- Monitor backups to identify instances of incremental and full backups are successful

5. Identify and remediate instances of back-up errors and failures
- Notify back-up administrators of failed back-ups

6. Real-time Alerts and Management Reports
- Alert Security Defenders when suspicious activity is detected.
- Produce management and operations reports (ad-hoc and pre-defined)

7. Update Back-up and Recovery (BAR) system of record
- Advise asset owners of changes and receive approval of updated inventory

Compliance Assessment: *Implement, operate, alert and report using processes and tools to properly back up critical information with a proven methodology for timely recovery of it.*

END

Alerting & Reporting

START

Control Requirements: Automatically back up all information required to fully restore each system, including the operating system, application software, and data. Back up all systems at least weekly; back up sensitive systems more often. Regularly test the restoration process.

Alerting & Reporting Requirements:

1. Establish Back-up and Recovery (BAR) system of record
- Inventory of systems, applications, information that have back-up configured and are backed-up on a regular basis.
- Monthly report of systems, applications, information that have back-up configured and are backed-up on a regular basis.

2. Create approved Back-up, Recovery, Retention Standards
- Organizational standards that include back-up intervals and procedures, recovery procedures and data retention standards.
- Trend reports that include implementation results based on back-up intervals and procedures, recovery procedures and data retention standards over past 12 months.

3. Incorporate back-up software / schedule in standard build
- Analysis of systems, applications and information to ensure backups are performed in accordance with standards.

4. Monitor production systems to ensure successful back-ups
- Report indicating successful backups for systems, applications, information.
- Trend report indicating successful backups for systems, applications, information over past 12 months

5. Identify and remediate instances of back-up errors and failures
- Report indicating unsuccessful backups for systems, applications, information.
- Trend report indicating unsuccessful backups for systems, applications, information over past 12 months

6. Real-time Alerts and Management Reports
- Report of all BAR alerts over previous month.
- Trend report of all BAR alerts over past 12 months.

7. Update Back-up and Recovery (BAR) system of record
- See BAR control system of record reports

Compliance Assessment: *Implement, operate, alert and report using processes and tools to properly back up critical information with a proven methodology for timely recovery of it.*

END

CSC-09: Security Skills Assessment Control Environment

Control Objective

The process and tools to make sure an organization understands the technical skill gaps within its workforce, including an integrated plan to fill the gaps through policy, training, and awareness.

Control

Develop a security skills assessment program, map training against the skills required for each job, and use the results to allocate resources effectively to improve security practices.

Consequences of not Implementing this Control

A constantly updated security awareness and education program for all users is important, but it will not stop determined attackers. Most determined adversaries will be stopped by effective implementation of the other Critical Controls, but some will slip through fissures in the security program. Skilled employees are essential for implementing and monitoring those Controls, for finding those attackers that get through the defenses, and for developing systems that are much harder to exploit.

Control System Analysis

CSCS Securing the Human (STH) - The organization Security Awareness Training is based on CSCS Securing The Human (STH) CSCS Securing The Human provides the materials for an engaging, high-impact security awareness program. The training addresses the most common risks using a proven framework based on the Critical Security Controls.

Security Skills Assessment Use Cases

- **Use Case 1:** Perform gap analysis to see which skills employees need and which behaviors employees are not adhering to, using this information to build a training and awareness roadmap.
- **Use Case 2:** Deliver training to fill the skills gap. Use more senior staff or outside instructors to train employees.
- **Use Case 3:** Implement an online security awareness program such as CSCS Securing the Human tat is mandated for completion by all employees at least annually.
- **Use Case 4:** Validate and improve awareness levels through tests such as PhishMe.com. PhishMe is a spear phishing simulator that raises awareness of the strategies and sophisticated tactics utilized today by hackers looking to compromise your organization's data and systems.
- **Use Case 5:** Use security skills assessments for each of the mission-critical skills to identify skills gaps.

Control Assessment

9.1: Perform gap analysis to see which skills employees need and which behaviors employees are not adhering to, using this information to build a training and awareness roadmap.

9.2: Deliver training to fill the skills gap. If possible, use more senior staff to deliver the training. A second option is to have outside teachers provide training onsite so the examples used will be directly relevant. If you have small numbers of people to train, use training conferences or online training to fill the gaps.

9.3: Implement an online security awareness program that:
(1) focuses on methods used in intrusions blocked through individual action
(2) is delivered in short online modules convenient for employees
(3) is updated frequently (at least annually) to represent the latest attack techniques
(4) is mandated for completion by all employees at least annually
(5) is reliably monitored for employee completion

9.4: Validate and improve awareness levels through periodic tests to see whether employees will click on a link from suspicious e-mail or provide sensitive information on the telephone without following appropriate procedures for authenticating a caller; targeted training should be provided to those who fall victim to the exercise.

9.5: Use security skills assessments for each of the mission-critical skills to identify skills gaps. Use hands-on, real-world examples to measure mastery. If you do not have such assessments, use one of the available online competitions that simulate real-world scenarios for each of the identified jobs in order to measure skills mastery

CSC-09: Security Skills Assessment Technical Solution

Design Specification

START

Control Requirements: Develop a security skills assessment program, map training against the skills required for each job, and use the results to allocate resources effectively to improve security practices.

Design Requirements: Building an Effective Security Awareness Program

1. Establish Security Policy, Program, Communications
- Document security program goals, objectives and requirements in a security policy.

2. Identify Current Training Needs
- The next step is to identify the current training needs of your organization.
- Obtain support from senior management, officers , others in positions of influence.

3. Establish Security Awareness System of Record
- CSCS Securing the Human – Security Awareness Training

4. Determine Audiences and Key Messages
- Present information that is relevant to the particular audience.
- Establish a single core message or mission statement.
- All other key messages should support and map back to this mission statement.

5. Implement Training and Communications
- Develop a framework for consistent and effective delivery of your messages.
- Define available communication vehicles.
- Establish scoring system and measure results.

6. Establish Management Reporting Approach
- Produce management and operations reports (ad-hoc and pre-defined)

7. Update Policy, Program Communications on an annual basis
- Update the program based on changes in the environment and improved practices

Compliance Assessment: *Implement, operate, alert and report using process and tools to ensure an organization understands the technical skill gaps within its workforce, including an integrated plan to fill the gaps through policy, training, and awareness*

END

Alerting & Reporting

CSCS Securing the Human Awareness Roadmap - This roadmap will enable the university to build, maintain and measure a high-impact security awareness program that goes beyond just compliance and ultimately reduces risk by changing human behavior.
- Identify the maturity level of the existing Security Awareness Program. Then select which maturity level you would like bring the program to.
- Follow the steps detailed in "How to Get There", which also identifies the Deliverables
- Each stage includes templates and checklists to help plan and document your program.
- Download all documents as part of the Security Awareness Program Planning Package

Stage 1: No Awareness Program - Program does not exist. Employees have no idea that they are a target, do not know or understand organizational security policies, and easily fall victim to cyber or human-based attacks.

Stage 2: Compliance Focused - Program designed primarily to meet specific compliance or audit requirements. Training is limited to annual or ad-hoc basis. Employees are unsure of organizational policies, their role in protecting their organization's information assets, and how to prevent, identify, or report a security incident.

Stage 3: Promotes Awareness & Change - Program identifies the training topics that have the greatest impact in supporting the organization's mission and focuses on those key topics. Program goes beyond just annual training and includes continual reinforcement throughout the year. Content is communicated in an engaging and positive manner that encourages behavior change at work, home, and while traveling. As a result, employees, contractors and staff understand and follow organizational policies and actively recognize, prevent and report incidents.

Stage 4: Long Term Sustainment - Program has processes and resources in place for a long-term life cycle, including at a minimum an annual review and update of both training content and communication methods. As a result, the program is an established part of the organization's culture and is current and engaging.

Stage 5: Metrics Framework - Program has a robust metrics framework to track progress and measure impact. As a result, the program is continuously improving and able to demonstrate return on investment. In addition, some set of metrics will be used in previous stages.

CSC-10: Secure Configuration for Network Devices Control Environment

Control Objective

The processes and tools used to track/control/prevent/correct security weaknesses in the configurations in network devices such as firewalls, routers, and switches based on formal configuration management and change control processes.

Control

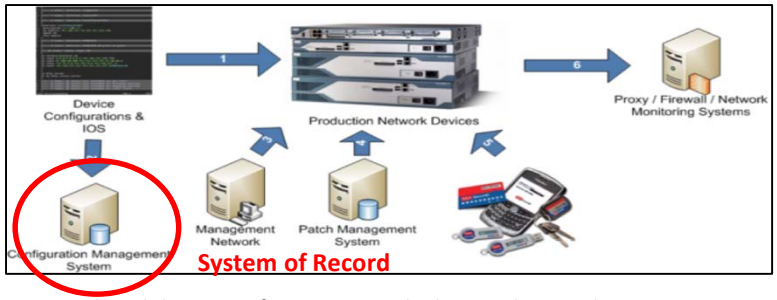
Compare firewall, router, switch configurations against standards for each type of network device. Ensure that any deviations from the standard configurations are documented and approved and that any temporary deviations are undone when the business need abates.

Consequences of not Implementing this control

Attackers take advantage of the fact that network devices may become less securely configured over time as users demand exceptions for specific and temporary business needs, as the exceptions are deployed, and as those exceptions are not undone when the business need is no longer applicable. Attackers search for electronic holes in firewalls, routers, and switches and use those to penetrate defenses. Attackers have exploited flaws in these network devices to gain access to target networks, redirect traffic on a network (to a malicious system masquerading as a trusted system), and intercept and alter information while in transmission.

Control System Analysis

NCM control systems examine network devices, test lab network devices, configuration systems, and configuration management devices.



Step 1: Hardened device configurations applied to production devices
Step 2: Hardened device configuration stored in a secure configuration management system
Step 3: Management network system validates configurations on production network devices
Step 4: Patch management system applies tested software updates to production network devices
Step 5:Two-factor authentication system required for administrative access to production devices
Step 6: Proxy/firewall/network monitoring systems analyze all connections to production network devices.

Control Assessment

10.1: 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.

10.2: At network interconnection points-such as Internet gateways, inter-organization connections, and internal network segments with different security controls--implement ingress and egress filtering to allow only those ports and protocols with an explicit and documented business need. All other ports and protocols should be blocked with default-deny rules by firewalls, network-based IPS, and/or routers.

10.3: 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.

10.4: Network filtering technologies employed between networks with different security levels (firewalls, network-based IPS tools, and routers with access controls lists) should be deployed with capabilities to filter Internet Protocol version 6 (IPv6) traffic. However, if IPv6 is not currently being used it should be disabled. Since many operating systems today ship with IPv6 support activated, filtering technologies need to take it into account.

10.5: Manage network devices using two-factor authentication and encrypted sessions.

10.6: Install the latest stable version of any security-related updates within 30 days of the update being released from the device vendor.

10.7: 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.

CSC-10: Secure Configuration for Network Devices Technical Solution

Design Specification

START

Control Requirements: Compare firewall, router, switch configurations against standards for each type of network device. Ensure that any deviations from the standard configurations are documented and approved and that any temporary deviations are undone when the business need abates

Design Requirements:

1. Establish Secure Network Configuration system of record.
- Establish network configuration system of record based on known configurations
- Include all network devices

2. Create approved network configuration standards
- Establish secure configuration standards for networks based on CIS baselines.
- Compare new network device builds with standard configuration image

3. Scan network devices for unauthorized configuration changes
- Establish change management process for authorized configuration changes
- Scan devices to detect unauthorized configuration changes
- Compare differences between current network device configs and baseline configs
- Determine whether configuration changes are authorized (change management)

4. Monitor network devices for unauthorized configuration changes
- Establish change management process for authorized configuration changes
- Monitor devices to detect unauthorized configuration changes
- Compare differences between current network device configs and baseline configs
- Determine whether configuration changes are authorized (change management)

5. Filter unauthorized network device configuration changes
- Establish change management process for authorized configuration changes
- Detect and block unauthorized configuration changes

6. Real-time Alerts and Management Reports
- Alert Security Defenders when suspicious activity is detected.
- Produce management and operations reports (ad-hoc and pre-defined)

7. Update Secure Network Configuration system of record
- Update configuration inventory through build, scan, monitor, filter processes above
- Advise asset owners of changes and receive approval of updated inventory

Compliance Assessment: *Implement, operate, alert and report using processes and tools to track/control/prevent/correct security weaknesses in the configurations in network devices such as firewalls, routers, and switches based on formal configuration management and change control processes.*

END

Alerting & Reporting

START

Control Requirements: Compare firewall, router, switch configurations against standards for each type of network device. Ensure that any deviations from the standard configurations are documented and approved and that any temporary deviations are undone when the business need abates

Alerting & Reporting Requirements:

1. Establish Secure Network Configuration system of record.
- Current state inventory of baseline device configurations by asset type
- Monthly inventory of baseline device configurations by asset type

2. Create approved network configuration standards
- Report of configurations added to baseline inventory
- Report of configurations removed from baseline inventory

3. Scan network devices for unauthorized configuration changes
- Monthly report of unknown / unauthorized configurations via device scan.
- Trend report of unknown / unauthorized configurations over past 12 months

4. Monitor network devices for unauthorized configuration changes
- Report of unknown / unauthorized configurations via device monitoring.
- Trend report of unknown / unauthorized configurations over past 12 months

5. Filter unauthorized network device configuration changes
- Report of unknown / unauthorized configurations via device configuration auditing.
- Trend report of unknown / unauthorized configurations over past 12 months.

6. Real-time Alerts and Management Reports
- Report of all network configuration alerts from previous month.
- Trend report of all network configuration alerts over past 12 months.

7. Update Secure Network Configuration system of record
- See network configuration control system of record reports

Compliance Assessment: *Implement, operate, alert and report using processes and tools to track/control/prevent/correct security weaknesses in the configurations in network devices such as firewalls, routers, and switches based on formal configuration management and change control processes.*

END

CSC-11: Limitation and Control of Ports, Protocols and Services Control Environment

Control Objective

The processes and tools used to track/control/prevent/correct use of ports, protocols, and services on networked devices.

Control

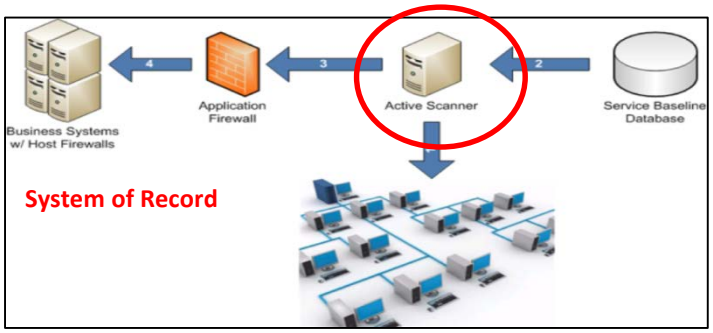
Apply host-based firewalls and port-filtering and scanning tools to block traffic that is not explicitly allowed. Properly configure web servers, mail servers, file servers, print servers and domain name servers (DNS) to limit remote access. Disable automatic installation of unnecessary software components. Move servers inside the firewall unless remote access is required for business purposes.

Consequences of not Implementing this Control

Attackers search for remotely accessible network services that are vulnerable to exploitation. Common examples include poorly configured web servers, mail servers, file and print services, and domain name system (DNS) servers installed by default on a variety of different device types, often without a business need for the given service. Many software packages automatically install services and turn them on as part of the installation of the main software package without informing a user or administrator that the services have been enabled. Attackers scan for such issues and attempt to exploit these services, often attempting default user IDs and passwords or widely available exploitation code.

Control System Analysis

Examine how active scanning systems gather information on network devices and evaluate that data against the authorized service baseline database.



Step 1: Active scanner analyzes production systems for unauthorized ports, protocols, and services
Step 2: System baselines regularly updated based on necessary/required services
Step 3: Active scanner validates which ports, protocols, and services are blocked or allowed by the application firewall
Step 4: Active scanner validates which ports, protocols, and services are accessible on business systems protected with host-based firewalls.

Control Assessment

11.1: Host-based firewalls or port filtering tools should be applied on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

11.2: Automated port scans should be performed on a regular basis against all key servers and compared to a known effective baseline. If a new port is found open, an alert should be generated and reviewed.

11.3: Any server that is visible from the Internet or an untrusted network should be verified, and if it is not required for business purposes it should be moved to an internal VLAN and given a private address.

11.4: Services needed for business use across the internal network should be reviewed quarterly via a change control group, and business units should re-justify the business use. Sometimes services are turned on for projects or limited engagements, and should be turned off when they are no longer needed.

11.5: Operate critical services on separate physical host machines, such as DNS, file, mail, web, and database servers**.**

11.6: Application firewalls should be placed 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

CSC-11: Limitation and Control of Ports, Protocols and Services Technical Solution

Design Specification

START

Control Requirement: Apply host-based firewalls and port-filtering and scanning tools to block traffic that is not explicitly allowed. Properly configure web servers, mail servers, file servers, print servers and domain name servers (DNS) to limit remote access. Disable automatic installation of unnecessary software components. Move servers inside the firewall unless remote access is required for business purposes.

Design Requirements:

1. Establish Ports, Protocols, Services (PPS) system of record.
- Establish PPS system of record

2. Create device specific configuration baseline including allowable PPS
- Determine allowable ports, protocols, services for networks, servers, desktops
- Quarterly review and business validation of services needed for business use
- Ensure critical services operate on separate physical host machines, such as DNS, file, mail, web, and database servers**.**

3. Scan devices to detect unauthorized ports, protocols, services
- Perform automated port scans on a regular basis against all key servers
- Compare scan results to a known effective baseline.

4. Monitor devices to detect unauthorized ports, protocols, services
- Monitor network device configurations for unauthorized ports, protocols, services
- If a new port is found open, an alert should be generated and reviewed
- Identify and justify any server visible from the Internet or an untrusted network.

5. ***Configure network devices to restrict unauthorized ports, protocols, services***
- Implement host-based firewalls or port filtering tools on end systems
- Establish default-deny rule to drop all traffic except services, ports explicitly allowed.
- Implement application firewalls in front of any critical servers

6. Real-time Alerts and Management Reports
- Alert Security Defenders when suspicious activity is detected.
- Produce management and operations reports (ad-hoc and pre-defined)

7. Update Ports, Protocols, Services (PPS) system of record.
- Advise asset owners of changes and receive approval of updated configuration

Compliance Assessment: *Implement, operate, alert and report using processes and tools to track/control/prevent/correct use of ports, protocols, and services on networked devices.*

END

Alerting & Reporting

START

Control Requirement: Apply host-based firewalls and port-filtering and scanning tools to block traffic that is not explicitly allowed. Properly configure web servers, mail servers, file servers, print servers and domain name servers (DNS) to limit remote access. Disable automatic installation of unnecessary software components. Move servers inside the firewall unless remote access is required for business purposes.

Alerting & Reporting Requirements:

1. Establish Ports, Protocols, Services (PPS) system of record.
- Current state inventory and criticality assessment of servers or network devices
- Monthly inventory and criticality assessment of servers or network devices

2. Create device specific configuration baseline including allowable PPS
- Report of PPS added, removed from baseline inventory from previous month.
- Trend report of PPS added, removed from baseline inventory over past 12 months

3. Scan devices to detect unauthorized ports, protocols, services
- Monthly report of unknown / unauthorized PPS discovered via device scan.
- Trend report of unknown / unauthorized PPS discovered via device scan over past 12 months

4. Monitor devices to detect unauthorized ports, protocols, services
- Monthly report of unknown / unauthorized PPS discovered via device monitoring.
- Trend report of unknown / unauthorized PPS discovered via device monitoring over past 12 months..

5. ***Configure network devices to restrict unauthorized ports, protocols, services***
- Monthly report of unknown / unauthorized PPS discovered via device configuration auditing.
- Trend report of unknown / unauthorized PPS discovered over past 12 months.

6. Real-time Alerts and Management Reports
- Report of all PPS alerts from previous month.
- Trend report of all PPS alerts over past 12 months.

7. Update Ports, Protocols, Services (PPS) system of record.
- See PPS control system of record reports

Compliance Assessment: *Implement, operate, alert and report using processes and tools to track/control/prevent/correct use of ports, protocols, and services on networked devices.*

END

CSC-12: Controlled Use of Administrative Privileges Control Environment

Control Objective

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

Control

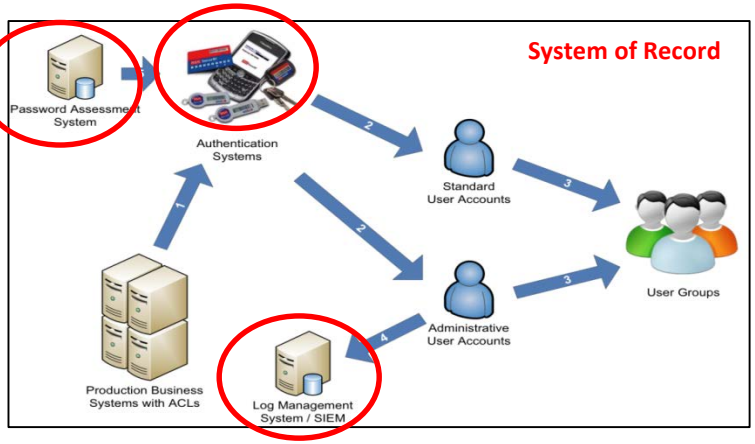
Protect and validate administrative accounts on desktops, laptops, and servers to prevent two common types of attack: (1) enticing users to open malicious e-mail, attachment, or file, or to visit a malicious website; and (2) cracking an administrative password and thereby gaining access to a target machine. Use robust passwords that follow Federal Desktop Core Configuration (FDCC) standards.

Consequences of not implementing this control

The misuse of administrative privileges is a primary method for attackers to spread inside a target enterprise.

Control System Analysis

Examine the components of user account provisioning and user authentication.



Step 1: Production systems use proper authentication systems
Step 2: Standard and administrative user accounts use proper authentication systems
Step 3: Standard and administrative user accounts properly managed via group memberships
Step 4: Administrative access to systems properly logged via log management systems
Step 5: Password assessment system validates the strength of the authentication systems.

Control Assessment

12.1: Minimize admin privileges and only use admin accounts when required. Implement auditing on administrative privileged functions and monitor for anomalous behavior.

12.2: Use automated tools to inventory admin accounts and validate individuals with admin privileges on desktops, laptops, and servers is authorized by a senior executive.

12.3: Configure all admin passwords to be complex and contain letters, numbers, and special characters intermixed, with no dictionary words present in the password. Passwords should be of a sufficient length to increase the difficultly it takes to crack the password.

12.4: Configure all administrative-level accounts to require regular password changes on a frequent interval tied to the complexity of the password.

12.5: Before deploying new devices, change default passwords for applications, operating systems, routers, firewalls, access points, etc., to a difficult-to-guess value.

12.6: Ensure all service accounts have long and difficult-to-guess passwords that are changed on a periodic basis of no longer than 90 days.

12.7: Store passwords in a well-hashed or encrypted format. Files containing these hashed passwords required for systems to authenticate readable only with super-user privileges.

12.8: Utilize access control lists to ensure that admin accounts are used only for system admin activities, and not for reading e-mail, composing documents, or surfing the Internet. Web browsers and e-mail clients must be configured to never run as administrator.

12.9: Require administrators establish different passwords for admin and non-admin accounts. Admin accounts should never be shared. Domain admin accounts should be used when required for system administration instead of local administrative accounts.

12.10: Configure operating systems so that passwords cannot be re-used within six months.

12.11: Configure systems to alert when an account is added /removed from a domain.

12.12: Use two-factor authentication for admin access, including domain admin access.

12.13: Block access to a machine for admin-level accounts. Instead, access a system using a fully logged and non-admin account. Once logged on to the machine without admin privileges, the administrator should transition to admin privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems.

12.14: If services are outsourced to third parties, include language in the contracts to ensure that they properly protect and control administrative access.

CSC-12: Controlled Use of Administrative Privileges Technical Solution

Design Specification

START

Control Requirements: Protect and validate administrative accounts on desktops, laptops, and servers to prevent two common types of attack: (1) enticing users to open malicious e-mail, attachment, or file, or to visit a malicious website; and (2) cracking an administrative password and thereby gaining access to a target machine. Use robust passwords that follow Federal Desktop Core Configuration (FDCC) standards.

Design Requirements:

1. Establish Administrative Privileges (AP) system of record.
- Establish AP system of record based on known configurations
- Include all devices with administrative accounts

2. Create baseline image of approved administrative accounts
- Establish secure configuration standards based on CIS baselines.
- Compare new network device builds with standard configuration image
- Ensure administrative align with baseline configuration

3. Scan network devices for unauthorized configuration changes
- Establish change management process for authorized administrative accounts
- Scan devices to detect unauthorized administrative accounts
- Compare differences between current admin privileges vs. approved admin accounts
- Determine whether administrative accounts are authorized

4. Monitor for creation of unauthorized administrative accounts
- Establish change management process for authorized administrative accounts
- Monitor devices to detect unauthorized configuration changes
- Compare differences between current admin privileges vs. approved admin accounts
- Determine whether administrative accounts are authorized

5. Restrict creation of unauthorized administrative accounts
- Establish change management process for authorized administrative accounts
- Compare differences between current admin privileges vs. approved admin accounts
- Detect and block unauthorized administrative accounts
- Determine whether administrative accounts are authorized

6. Real-time Alerts and Management Reports
- Alert Security Defenders when suspicious activity is detected.
- Produce management and operations reports (ad-hoc and pre-defined)

7. Update Administrative Privileges system of record
- Update AP system of record based on known / approved administrative accounts
- Advise asset owners of changes and receive approval of updated privileged accounts

Compliance Assessment: *Implement, operate, alert and report using processes and tools to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.*

END

Alerting & Reporting

START

Control Requirements: *Protect and validate administrative accounts on desktops, laptops, and servers to prevent two common types of attack: (1) enticing users to open malicious e-mail, attachment, or file, or to visit a malicious website; and (2) cracking an administrative password and thereby gaining access to a target machine. Use robust passwords that follow Federal Desktop Core Configuration (FDCC) standards.*

Alerting & Reporting Requirements:

1. Establish Administrative Privileges system of record.
- Establish database that inventories all administrative users based on role
- Monthly report of users with administrative privileges

2. Create baseline image of approved administrative accounts
- Report of administrative accounts added / removed from previous month.
- Trend report of administrative accounts added / removed from past 12 months

3. Scan network devices for unauthorized administrative accounts
- Report of unauthorized administrative accounts discovered via device scan.
- Trend report of unauthorized administrative accounts over past 12 months

4. Monitor for creation of unauthorized administrative accounts
- Report of unauthorized administrative accounts discovered via device monitoring.
- Trend report of unauthorized administrative accounts over past 12 months.

5. Restrict creation of unauthorized administrative accounts
- Report of unauthorized administrative accounts discovered via configuration auditing.
- Trend report of unauthorized administrative accounts over past 12 months.

6. Real-time Alerts and Management Reports
- Report of all administrative account alerts from previous month.
- Trend report of all administrative account alerts over past 12 months.

7. Update Administrative Privileges system of record
- See AP control system of record reports

Compliance Assessment: *Implement, operate, alert and report using processes and tools to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.*

END

CSC-13: Boundary Defenses Control Environment

Control Objective

The processes and tools used to detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

Control

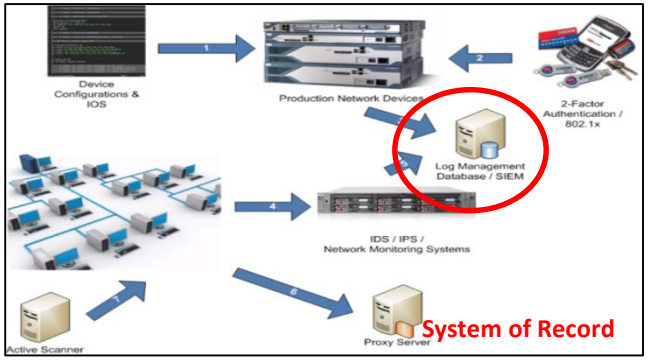
Establish multi-layer boundary defenses by relying on firewalls, proxies, demilitarized zone (DMZ) perimeter networks, and other network-based tools. Filter inbound and outbound traffic, including through business partner networks (extranets)

Consequences of not Implementing this Control

Attackers focus on exploiting systems that they can reach across the Internet, including not only DMZ systems but also workstation and laptop computers that pull content from the Internet through network boundaries. Threats such as organized crime groups and nation-states use configuration and architectural weaknesses found on perimeter systems, network devices, and Internet-accessing client machines to gain initial access into an organization. Then, with a base of operations on these machines, attackers often pivot to get deeper inside the boundary to steal or change information or to set up a persistent presence for later attacks against internal hosts.

Control System Analysis

Examine network boundary devices and supporting systems such as authentication servers, two-factor authentication systems, network monitoring systems, network proxy devices.



Step 1: Hardened device configurations applied to production devices
Step 2:Two-factor authentication systems for administrative access to production devices
Step 3: Production network devices send events to log management and correlation system
Step 4: Network monitoring system analyzes network traffic
Step 5: Network monitoring system sends events to log management and correlation system
Step 6: Outbound traffic passes through and is examined by network proxy devices
Step 7: Network systems scanned for potential weaknesses

Control Assessment

13.1: Deny communications with known malicious IP addresses (black lists), or limit access only to trusted sites (white lists).

13.2: Configure monitoring systems on DMZs to record packet header and payloads of the traffic destined for or passing through the network border. Send traffic to SEIM so that events can be correlated from all devices on the network.

13.3: To mitigate spoofed e-mail messages, implement the Sender Policy Framework (SPF) by deploying SPF records in DNS and enabling receiver-side verification in mail servers.

13.4: Deploy network-based IDS sensors on Internet and extranet DMZs that look for unusual attack mechanisms and detect compromise of these systems.

13.5: Use **n**etwork IPS devices to compliment IDS by blocking known bad signature or behavior of attacks.

13.6: Implement network perimeters for outgoing web, FTP, and SSH traffic to the Internet passes through a DMZ proxy. The proxy should support logging individual TCP sessions; blocking specific URLs, domain names, IP addresses to implement blacklist / white list.

13.7: 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.

13.8: All devices remotely logging into the internal network should be managed by the organization, with remote control of their configuration, installed software, and patch levels.

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

13.10: To limit access by an insider or malware spreading on an internal network, the organization should devise internal network segmentation schemes to limit traffic to only those services needed for business use across the internal network.

13.11: Rapidly deploy internal network filters to stop spread of malware or intruder.

13.12: Only allow DMZ systems to communicate with private network systems via application proxies or application-aware firewalls over approved channels.

13.13: To identify covert channels exfiltrating data through a firewall, configure firewall session tracking mechanisms to identify TCP sessions that last an unusually long time.

13.14: Deploy NetFlow collection and analysis to DMZ network flows to detect anomalous activity.

CSC-13: Boundary Defenses Technical Solution

Design Specification

START

Control Requirements: *Establish multi-layer boundary defenses by relying on firewalls, proxies, demilitarized zone (DMZ) perimeter networks, and other network-based tools. Filter inbound and outbound traffic, including through business partner networks (extranets).*

Design Requirements:

1. Establish Boundary Defenses (BD) system of record.
- Establish BD system of record based inclusive of all perimeter technologies

2. Configure perimeter defenses based to allow only trusted connections
- Configure firewalls to deny all except connections that are explicitly allowed
- Configure IPS to allow all except connections that are explicitly denied
- Configure outbound e-mail, web proxy, ftp to allow connections to only trusted sites
- Configure inbound e-mail to allow connections from only trusted e-mail servers

3. Scan network to detect vulnerable (mis-configured or unpatched) systems
- Detect / remediate mis-configured internal servers that are not Internet accessible
- Detect / remediate misconfigured or un-pactched servers that are Internet accessible
- Detect / remediate misconfigured firewall rule sets

4. Monitor inbound traffic for suspicious activity
- Configure IPS, Firewalls to detect / block untrusted connections (port, IP, signature)
- Log all denies to a central log server (BD system of record)

5. Filter outbound connections (ftp, web, e-mail)
- Restrict connections to trusted sites only

6. Real-time Alerts and Management Reports
- Alert Security Defenders when suspicious activity is detected.
- Produce management and operations reports (ad-hoc and pre-defined)

7. Update Boundary Defenses system of record
- Update AP system of record based on known / approved administrative accounts
- Advise asset owners of changes and receive approval of updated privileged accounts

Compliance Assessment: *Implement, operate, alert and report using processes and tools to detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.*

END

Alerting & Reporting

START

Control Requirements: *Establish multi-layer boundary defenses by relying on firewalls, proxies, demilitarized zone (DMZ) perimeter networks, and other network-based tools. Filter inbound and outbound traffic, including through business partner networks (extranets).*

Alerting & Reporting Requirements:

1. Establish Boundary Defenses system of record.
- Establish BD systems of record based inclusive of all perimeter technologies

2. Configure perimeter defenses based to allow only trusted connections
- Report of firewall and IDS rules review
- Report of blocked connection attempts via firewall / IDS
- Report of e-mail, web proxy, ftp configuration reviews

3. Scan network to detect vulnerable (mis-configured or unpatched) systems
- Monthly external scan report

4. Monitor inbound traffic for suspicious activity
- Monthly anti-malware (Botnet) report

5. Filter outbound connections (ftp, web, e-mail)
- Report of blocked outbound connection attempts (ftp, web, e-mail)

6. Real-time Alerts and Management Reports
- Report of all system event alerts from previous month.
- Trend report of all system event alerts over past 12 months.

7. Update Boundary Defenses system of record
- See BD control system of record reports

Compliance Assessment: *Implement, operate, alert and report using processes and tools to detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.*

END

CSC-14: Maintenance, Monitoring, and Analysis of Audit Logs Control Environment

Control Objective

The processes and tools used to detect/prevent/correct the use of systems and information based on audit logs of events that are considered significant or could impact the security of an organization

Control

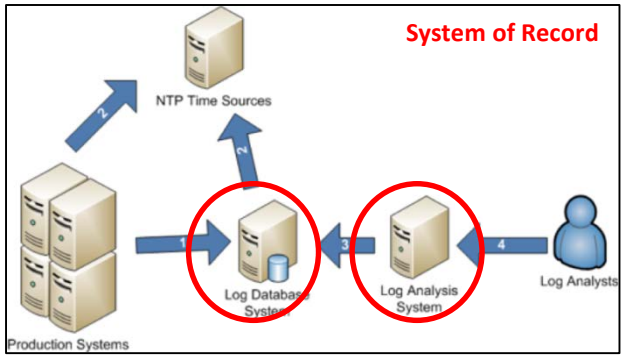
Generate standardized logs for each hardware device and the software installed on it, including date, time stamp, source addresses, destination addresses, and other information about each packet and/or transaction. Store logs on dedicated servers, and run bi-weekly reports to identify and document anomalies.

Consequences of not Implementing this Control

Deficiencies in security logging and analysis allow attackers to hide their location, malicious software used for remote control, and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records they are blind to the details of the attack and to subsequent actions taken by the attackers. Without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible.

Control System Analysis

Examine audit logs, the central log database system, the central time system, and log analysts.



Step 1:Production systems generate logs and send them to a centrally managed log database system
Step 2: Production systems and log database system pulls synchronize time with central time management systems
Step 3: Logs analyzed by a log analysis system
Step 4: Log analysts examine data generated by log analysis system

Control Assessment

14.1: Include at least two synchronized time sources (NTP) so that timestamps in logs are consistent.

14.2: Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Record logs in a standardized format such as syslog.

14.3: Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

14.4: Develop a log retention policy to make sure that the logs are kept for a sufficient period of time. As APT (advanced persistent threat) continues to stealthily break into systems, organizations are often compromised for several months without detection. The logs must be kept for a longer period of time than it takes an organization to detect an attack.

14.5: Verbosely log all remote access to a network, whether to the DMZ or the internal network (i.e., VPN, dial-up, or other mechanism).

14.6: Configure operating systems to log access control events associated with a user attempting to access a resource (e.g., a file or directory) without the appropriate permissions. Failed logon attempts must also be logged.

14.7: Have security personnel and/or system administrators run biweekly reports that identify anomalies in logs. They should then actively review the anomalies, documenting their findings.

14.8: Configure network boundary devices, including firewalls, network-based IPS, and inbound and outbound proxies, to verbosely log all traffic (both allowed and blocked) arriving at the device.

14.9: For all servers, ensure that logs are written to write-only devices or to dedicated logging servers running on separate machines from hosts generating the event logs, lowering the chance that an attacker can manipulate logs stored locally on compromised machines.

14.10: Deploy a SEIM for log aggregation and consolidation from multiple machines and for log correlation and analysis. Using the SEIM, system administrators and security personnel should devise profiles of common events so that they can tune detection to focus on unusual activity, avoid false positives, rapidly identify anomalies, and prevent insignificant alerts.

14.11: Carefully monitor for service creation events. On Windows systems, many attackers use psexec functionality to spread from system to system. Creation of a service is an unusual event and should be monitored closely.

CSC-14: Maintenance, Monitoring, and Analysis of Audit Logs Technical Solution

Design Specification

START

Control Requirements: *Generate standardized logs for each hardware device and the software installed on it, including date, time stamp, source addresses, destination addresses, and other information about each packet and/or transaction. Store logs on dedicated servers, and run bi-weekly reports to identify and document anomalies.*

Design Requirements:

1. Establish Log management (LM) system of record.
- Establish LM system of record

2. Create device specific hardened configuration baseline
- Quarterly review and business validation of services needed for business use

3. Scan devices to detect unauthorized configurations or connections
- Perform automated port scans on a regular basis against all key servers
- Compare scan results to a known effective baseline.

4. Monitor devices to detect unauthorized configurations or connections
- Monitor network device configurations for unauthorized ports, protocols, services
- If a new port is found open, an alert should be generated and reviewed
- Identify and justify any server visible from the Internet or an untrusted network.

5. ***Configure network devices to restrict unauthorized configurations or connections***
- Implement host-based firewalls or port filtering tools on end systems
- Establish default-deny rule that drops all traffic except services and ports explicitly allowed.

6. Real-time Alerts and Management Reports
- Alert Security Defenders when suspicious activity is detected.
- Produce management and operations reports (ad-hoc and pre-defined)

7. Update Log management (LM) system of record.
- Advise asset owners of changes and receive approval of updated configuration

Compliance Assessment: *Implement, operate, alert and report using processes and tools to detect/prevent/correct the use of systems and information based on audit logs of events that are considered significant or could impact the security of an organization*

END

Alerting & Reporting

START

Control Requirements: *Generate standardized logs for each hardware device and the software installed on it, including date, time stamp, source addresses, destination addresses, and other information about each packet and/or transaction. Store logs on dedicated servers, and run bi-weekly reports to identify and document anomalies.*

Alerting & Reporting Requirements:

1. Establish Log management (LM) system of record.
- Establish LM system of record
- Monthly report of all log sources added or deleted

2. Create device specific hardened configuration baseline
- Report of device configurations added, removed from baseline over previous month.
- Trend report of device configurations added, removed over past 12 months

3. Scan devices to detect unauthorized configurations or connections
- Report of unauthorized device configurations discovered via device scan.
- Trend report of unauthorized device configurations over past 12 months

4. Monitor devices to detect unauthorized configurations or connections
- Report of unauthorized device configurations discovered via device monitoring
- Trend report of unauthorized device configurations over past 12 months

5. ***Filter devices to restrict unauthorized configurations or connections***
- Report of unauthorized device configurations discovered via device filtering
- Trend report of unauthorized device configurations over past 12 months

6. Real-time Alerts and Management Reports
- Report of all system event alerts from previous month.
- Trend report of all system event alerts over past 12 months.

7. Update Log management (LM) system of record.
- See LM control system of record reports

Compliance Assessment: *Implement, operate, alert and report using processes and tools to detect/prevent/correct the use of systems and information based on audit logs of events that are considered significant or could impact the security of an organization*

END

CSC-15: Controlled Access Based on the Need to Know Control Environment

Control Objective

The processes and tools used to track/control/prevent/correct secure access to information according to the formal determination of which persons, computers, and applications have a need and right to access information based on an approved classification.

Control

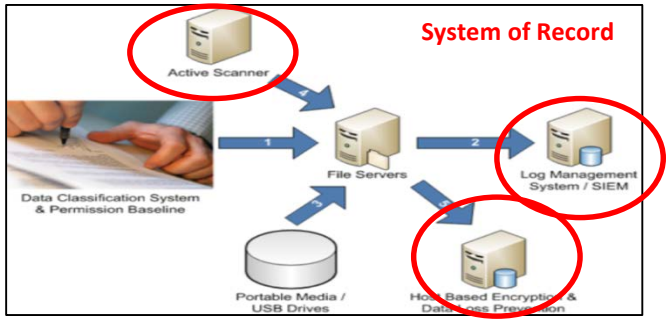
Carefully identify and separate critical data from information that is readily available to internal network users. Establish a multilevel data classification scheme based on the impact of any data exposure, and ensure that only authenticated users have access to nonpublic data and files.

Consequences of not Implementing this Control

Some organizations do not carefully identify and separate their most sensitive data from less sensitive, publicly available information on their internal networks. In many environments, internal users have access to all or most of the information on the network. Once attackers have penetrated such a network, they can easily find and exfiltrate important information with little resistance.

Control System Analysis

The data classification system and permission baseline is the blueprint for how authentication and access of data is controlled.



Step 1: An appropriate data classification system and permissions baseline applied to production data systems
Step 2: Access appropriately logged to a log management system
Step 3: Proper access control applied to portable media/USB drives
Step 4: Active scanner validates, checks access, and checks data classification
Step 5: Host-based encryption and data-loss prevention validates and checks all access requests.

Control Assessment

15.1: Locate any sensitive information on separated VLANS with proper firewall filtering. All communication of sensitive information over less-trusted networks needs to be encrypted.

15.2: Establish a multi-level data identification/classification scheme (e.g., a three- or four-tiered scheme with data separated into categories based on the impact of exposure of the data).

15.3: Enforce detailed audit logging for access to nonpublic data and special authentication for sensitive data.

15.4: Segment the network based on the trust levels of the information stored on the servers. Whenever information flows over a network with a lower trust level, the information should be encrypted.

15.5: Use host-based data loss prevention (DLP) to enforce ACLs even when data is copied off a server. In most organizations, access to the data is controlled by ACLs that are implemented on the server. Once the data have been copied to a desktop system, the ACLs are no longer enforced and the users can send the data to whomever they want

CSC-15: Controlled Access Based on the Need to Know Technical Solution

Design Specification

START

Control Requirements: *Carefully identify and separate critical data from information that is readily available to internal network users. Establish a multilevel data classification scheme based on the impact of any data exposure, and ensure that only authenticated users have access to nonpublic data and files.*

Design Requirements:

1. Establish Controlled Access (CA) system of record.
- Establish CA system of record based on known configurations
- Include all users with administrative accounts

2. Create baseline image of approved administrative accounts and sensitive data
- Establish RBAC model for roles based access
- Establish data classification practice to Identify systems with critical data
- Establish process to update authorized admin accounts and sensitive data

3. Scan for unauthorized administrative accounts and sensitive data
- Scan devices to detect unauthorized users, roles, permissions
- Scan devices to detect critical data
- Compare authorized admin accounts and sensitive data with authorized devices

4. Monitor for unauthorized administrative accounts and sensitive data
- Monitor devices to detect unauthorized users, roles, permissions
- Monitor devices to detect sensitive data
- Compare authorized admin accounts and sensitive data with authorized devices

5. Restrict creation of unauthorized administrative accounts and sensitive data
- Restrict access from unauthorized users, roles, permissions
- Restrict storage of sensitive data except where explicitly allowed
- Compare authorized admin accounts and sensitive data with authorized devices

6. Real-time Alerts and Management Reports
- Alert Security Defenders when suspicious accounts or data are detected.
- Produce management and operations reports (ad-hoc and pre-defined)

7. Update Controlled Access (CA) system of record
- Update CA system of record based on approved users, roles, data
- Advise asset owners of changes and receive approval of users, roles, data

Compliance Assessment: *Implement, operate, alert and report using processes and tools to track/control/prevent/correct secure access to information according to the formal determination of which persons, computers, and applications have a need and right to access information based on an approved classification.*

END

Alerting & Reporting

START

Control Requirements: *Carefully identify and separate critical data from information that is readily available to internal network users. Establish a multilevel data classification scheme based on the impact of any data exposure, ensure only authenticated users have access to nonpublic data and files.*

Alerting & Reporting Requirements:

1. Establish Controlled Access (CA) system of record.
- Establish database that inventories all administrative users based on role
- Establish inventory of all critical data based on a data classification scheme
- Monthly report of users with administrative privileges
- Monthly report of systems that contain sensitive data based on data classification

2. Create baseline image of approved administrative accounts and sensitive data
- Report of administrative accounts added / removed from previous month.
- Report of systems with critical data added / removed from previous month.
- Trend report of administrative accounts added / removed from past 12 months
- Trend report of systems with sensitive data added / removed from past 12 months

3. Scan network devices for unauthorized administrative accounts and sensitive data
- Report of unauthorized administrative accounts discovered via device scan.
- Report of unauthorized systems with critical data discovered via device scan.
- Trend report of unauthorized administrative accounts over past 12 months
- Trend report of systems with critical data over past 12 months

4. Monitor for creation of unauthorized administrative accounts and sensitive data
- Report of unauthorized administrative accounts discovered via device monitoring
- Report of unauthorized systems with critical data discovered via device monitoring
- Trend report of unauthorized administrative accounts over past 12 months
- Trend report of systems with critical data over past 12 months

5. Restrict creation of unauthorized administrative accounts and sensitive data
- Report of unauthorized administrative accounts discovered via configuration auditing
- Report of unauthorized systems with critical data discovered via configuration auditing
- Trend report of unauthorized administrative accounts over past 12 months
- Trend report of systems with critical data over past 12 months

6. Real-time Alerts and Management Reports
- Alert Security Defenders when suspicious accounts or data are detected.
- Produce management and operations reports (ad-hoc and pre-defined)

7. Update Controlled Access (CA) system of record
- See CA control system of record reports

Compliance Assessment: *Implement, operate, alert and report using processes and tools to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.*

END

CSC-16: Account Monitoring Control Environment

Control Objective

The processes and tools used to track/control/prevent/correct the use of system and application accounts.

Control

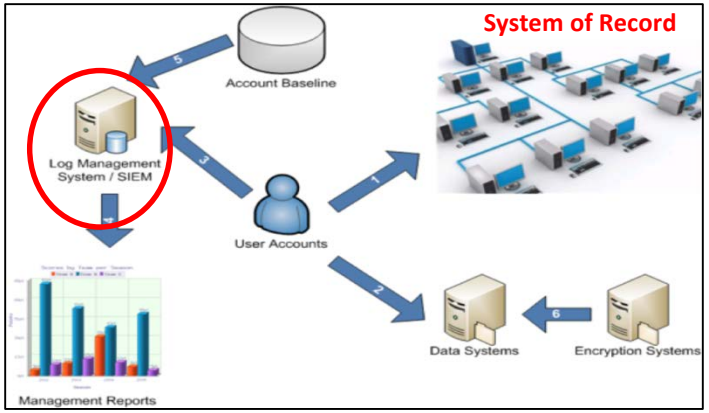
Review all system accounts and disable any that are not associated with a business process and owner. Immediately revoke system access for terminated employees and contractors. Disable dormant accounts and encrypt and isolate any files associated with such accounts. Use robust passwords that conform to FDCC standards.

Consequences of not Implementing this Control

Attackers frequently discover and exploit legitimate but inactive user accounts to impersonate legitimate users, thereby making discovery of attacker behavior difficult for network watchers. Accounts of contractors and employees who have been terminated have often been misused in this way. Additionally, some malicious insiders or former employees have accessed accounts left behind in a system long after contract expiration, maintaining their access to an organization's computing system and sensitive data for unauthorized and sometimes malicious purposes.

Control System Analysis

Examine user accounts and how they interact with the data systems and the log management systems



Step 1: User accounts are properly managed on production systems
Step 2: User accounts are assigned proper permissions to production data sets
Step 3: User account access is logged to log management system
Step 4: Log management systems generate user account and access reports for management
Step 5: Account baseline information is sent to log management system
Step 6: Critical information is properly protected and encrypted for each user account.

Control Assessment

16.1: Review all system accounts and disable any account that cannot be associated with a business process and owner.

16.2: Ensure that all accounts have an expiration date associated with the account.

16.3: Ensure systems automatically create a report that includes a list of locked-out accounts, disabled accounts, accounts with passwords that exceed maximum password age, and accounts with passwords that never expire.

16.4: Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor.

16.5: Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

16.6: Monitor account usage to determine dormant accounts that have not been used for a given period, such as 45 days, notifying the user or user's manager of the dormancy. After a longer period, such as 60 days, the account should be disabled.

16.7: When a dormant account is disabled, any files associated with that account should be encrypted and moved to a secure file server for analysis by security or management personnel.

16.8: Require that all non administrator accounts have strong passwords that contain letters, numbers, and special characters, be changed at least every 90 days, have a minimal age of one day, and not be allowed to use the previous 15 passwords as a new password. These values can be adjusted based on the specific business needs of the organization.

16.9: Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time.

16.10: On a periodic basis, such as quarterly or at least annually, require that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators should then disable accounts that are not assigned to active employees or contractors.

16.11: Monitor attempts to access deactivated accounts through audit logging.

16.12: Profile each user's typical account usage by determining normal time-of-day access and access duration. Daily reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration by 150 percent. This includes flagging the use of the user's credentials from a computer other than computers on which the user generally works.

CSC-16: Account Monitoring Technical Solution

Design Specification

START

Control Requirements: *Review all system accounts and disable any that are not associated with a business process and owner. Immediately revoke system access for terminated employees and contractors. Disable dormant accounts and encrypt and isolate any files associated with such accounts. Use robust passwords that conform to FDCC standards.*

Design Requirements:

1. Establish Account Monitoring (AM) system of record.
- Establish AM system of record based on known configurations
- Include all devices with admin accounts

2. Create baseline image of approved administrative accounts
- Establish secure configuration standards based on CIS baselines.
- Compare new network device builds with standard configuration image
- Ensure administrative align with baseline configuration

3. Scan network devices for unauthorized configuration changes
- Scan devices to detect unauthorized administrative accounts
- Compare differences between current admin privileges vs. approved admin accounts

4. Monitor for creation of unauthorized administrative accounts
- Monitor devices to detect unauthorized configuration changes
- Compare differences between current admin privileges vs. approved admin accounts

5. Restrict creation of unauthorized administrative accounts
- Compare differences between current admin privileges vs. approved admin accounts
- Detect and block unauthorized admin account**s**

6. Real-time Alerts and Management Reports
- Alert Security Defenders when suspicious activity is detected.
- Produce management and operations reports (ad-hoc and pre-defined)

7. Update Account Monitoring (AM) system of record
- Update AM system of record based on known / approved admin accounts
- Advise asset owners of changes and receive approval of updated privileged accounts

Compliance Assessment: *Implement, operate, alert and report using processes and tools to track/control/prevent/correct the use of system and application accounts.*

END

Alerting & Reporting

START

Control Requirements: *Review all system accounts and disable any that are not associated with a business process and owner. Immediately revoke system access for terminated employees and contractors. Disable dormant accounts and encrypt and isolate any files associated with such accounts. Use robust passwords that conform to FDCC standards.*

Alerting & Reporting Requirements:

1. Establish Account Monitoring (AM) system of record.
- Establish database that inventories all devices with administrative accounts
- Monthly report of privileged user account activity

2. Create baseline image of approved administrative accounts
- Report of administrative accounts added / removed from previous month.
- Report of systems with critical data added / removed from previous month.
- Trend report of administrative accounts added / removed from past 12 months
- Trend report of systems with sensitive data added / removed from past 12 months

3. Scan network devices for unauthorized configuration changes
- Monthly report of changed configurations via device scan.
- Trend report of changed configurations over past 12 months

4. Monitor for creation of unauthorized administrative accounts
- Monitor devices to detect unauthorized configuration changes
- Compare differences between current admin privileges vs. approved admin accounts

5. Restrict creation of unauthorized administrative accounts
- Compare differences between current admin privileges vs. approved admin accounts
- Detect and block unauthorized admin account**s**

6. Real-time Alerts and Management Reports
- Alert Security Defenders when suspicious activity is detected.
- Produce management and operations reports (ad-hoc and pre-defined)

7. Update Account Monitoring (AM) system of record
- Update AM system of record based on known / approved admin accounts
- Advise asset owners of changes and receive approval of updated privileged accounts

Compliance Assessment: *Implement, operate, alert and report using processes and tools to track/control/prevent/correct the use of system and application accounts.*

END

CSC-17: Data Loss Prevention Control Environment

Control Objective

The processes and tools used to track/control/prevent/correct data transmission and storage, based on the data's content and associated classification

Control

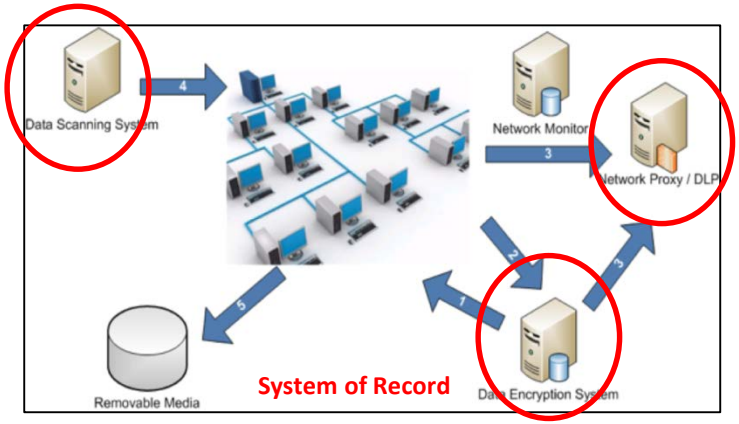
Scrutinize the movement of data across network boundaries, both electronically and physically, to minimize the exposure to attackers. Monitor people, processes, and systems, using a centralized management framework.

Consequences of not Implementing this Control

In recent years, attackers have exfiltrated significant amounts of often-sensitive data from organizations of all shapes and sizes. Many attacks occurred across the network, while others involved physical theft of laptops and other equipment holding sensitive information. Yet in most cases, the victims were not aware that the sensitive data were leaving their systems because they were not monitoring data outflows. The movement of data across network boundaries both electronically and physically must be carefully scrutinized to minimize its exposure to attackers.

Control System Analysis

Examine the flow of information in and out of the organization in an attempt to limit potential data loss via network or removable media sources.



Step 1: Data encryption system ensures that appropriate hard disks are encrypted
Step 2: Sensitive network traffic encrypted
Step 3: Data connections monitored at the network's perimeter by monitoring systems
Step 4: Stored data scanned to identify where sensitive information is stored
Step 5: Offline media encrypted.

Control Assessment

17.1: Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.

17.2: Deploy an automated tool on network perimeters that monitors for certain sensitive information (i.e., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel.

17.3: Conduct periodic scans of server machines using automated tools to determine whether sensitive data (i.e., personally identifiable information, health, credit card, and classified information) is present on the system in clear text. These tools, which search for patterns that indicate the presence of sensitive information, can help identify if a business or technical process is leaving behind or otherwise leaking sensitive information.

17.4: Data should be moved between networks using secure, authenticated, and encrypted mechanisms.

17.5: If there is no business need for supporting such devices, the organization should configure systems so that they will not write data to USB tokens or USB hard drives. If such devices are required, organization software should be used that can configure systems to allow only specific USB devices (based on serial number or other unique property) to be accessed, and that can automatically encrypt all data placed on such devices. An inventory of all authorized devices must be maintained.

17.6: Use network-based DLP solutions to monitor and control the flow of data within the network. Any anomalies that exceed the normal traffic patterns should be noted and appropriate action taken to address them.

17.7: Monitor all traffic leaving the organization and detect any unauthorized use of encryption. Attackers often use an encrypted channel to bypass network security devices. Therefore it is essential that the organization detect rogue connections, terminate the connection, and remediate the infected system.

17.8: Block access to known file transfer and e-mail exfiltration websites.

CSC-17: Data Loss Prevention Technical Solution

Design Specification

START

Control Requirements: Scrutinize the movement of data across network boundaries, both electronically and physically, to minimize the exposure to attackers. Monitor people, processes, and systems, using a centralized management framework.

Design Requirements:

1. Establish Data Loss Prevention (DLP) system of record.
- Establish DLP system of record
- Classify all data types based on sensitivity

2. Create baseline of known sensitive data
- Establish inventory to track instances of sensitive data

3. Scan network devices for unknown sensitive data
- Scan devices to detect sensitive data at rest
- Compare differences between sensitive data inventory and data discovered via scan

4. Monitor for creation of unknown sensitive data
- Monitor devices to detect sensitive data in motion
- Compare differences between sensitive data inventory and data discovered via monitoring

5. Restrict creation of unknown sensitive data
- Establish rules to filter / block sensitive data leaving the organization
- Compare differences between sensitive data inventory and data blocked via filtering

6. Real-time Alerts and Management Reports
- Alert Security Defenders when suspicious activity is detected.
- Produce management and operations reports (ad-hoc and pre-defined)

7. Update Data Loss Prevention (DLP) system of record
- Update DLP system of record based on discovered sensitive data
- Advise asset owners of changes and receive approval of instances of sensitive data

Compliance Assessment: *Implement, operate, alert and report using processes and tools to track/control/prevent/correct data transmission and storage, based on the data's content and associated classification*

END

Alerting & Reporting

START

Control Requirements: Scrutinize the movement of data across network boundaries, both electronically and physically, to minimize the exposure to attackers. Monitor people, processes, and systems, using a centralized management framework.

Alerting & Reporting Requirements:

1. Establish Data Loss Prevention (DLP) system of record.
- Establish database that inventories all devices with administrative accounts
- Monthly report of sensitive data added / removed from inventory
- Trend report of sensitive data added / removed over past 12 months

2. Create baseline of known sensitive data
- Report of sensitive data added / removed from previous month.
- Report of systems with sensitive data added / removed from previous month.
- Trend report of sensitive data added / removed from past 12 months
- Trend report of systems with sensitive data added / removed from past 12 months

3. Scan network devices for unknown sensitive data
- Monthly report of sensitive data discovered via monthly scan
- Trend report of sensitive data discovered via scan over past 12 months

4. Monitor for creation of unknown sensitive data
- Monthly report of sensitive data discovered via monitoring
- Trend report of sensitive data discovered via monitoring over past 12 months

5. Restrict creation of unknown sensitive data
- Monthly report of sensitive data discovered via filtering
- Trend report of sensitive data discovered via filtering over past 12 months

6. Real-time Alerts and Management Reports
- Alert Security Defenders when unknown sensitive data is detected.
- Produce management and operations reports (ad-hoc and pre-defined)

7. Update Data Loss Prevention (DLP) system of record
- Update DLP system of record based on discovered sensitive data
- Advise asset owners of changes and receive approval of instances of sensitive data

Compliance Assessment: *Implement, operate, alert and report using processes and tools to track/control/prevent/correct data transmission and storage, based on the data's content and associated classification*

END

CSC-18: Incident Response and Management Control Environment

Control Objective

The process and tools to make sure an organization has a properly tested plan with appropriate trained resources for dealing with any adverse events or threats of adverse events

Control

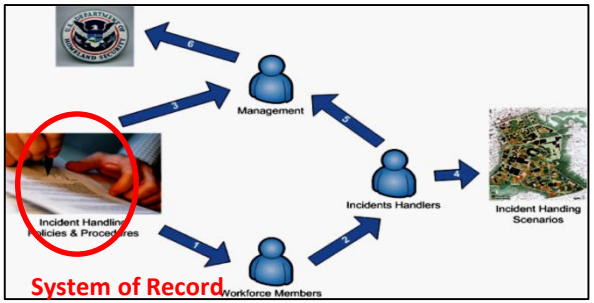
Develop an incident response plan with clearly delineated roles and responsibilities for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of network and systems.

Consequences of not Implementing this Control

Considerable damage has been done to organizational reputations and a great deal of information has been lost in organizations that do not have fully effective incident response plans in place. Without an incident response plan, an organization may not discover an attack in the first place, or, if the attack is detected, the organization may not follow proper procedures to contain damage, eradicate the attacker's presence, and recover in a secure fashion. Thus, the attacker may have a far greater impact, causing more damage, infecting more systems, and possibly exfiltrating more sensitive data than would otherwise be possible were an effective incident response plan in place.

Control System Analysis

Examine the incident handling process and how prepared the organization is in the event that an incident occurs.



Step 1: Incident handling policies and procedures educate workforce members as to their responsibilities during an incident
Step 2: Some workforce members designated as incident handlers
Step 3: Incident handling policies and procedures educate management as to their responsibilities during an incident
Step 4: Incident handlers participate in incident handling scenario tests
Step 5: Incident handlers report incidents to management
Step 6: The organization's management reports incidents to outside law enforcement and the appropriate computer emergency response team, if necessary.

Control Assessment

18.1: The organization should ensure that they have written incident response procedures that include a definition of personnel roles for handling incidents. The procedures should define the phases of incident handling consistent with the NIST guidelines cited above.

18.2: The organization should assign job titles and duties for handling computer and network incidents to specific individuals.

18.3: The organization should define management personnel who will support the incident handling process by acting in key decision-making roles.

18.4: The organization should devise organization-wide standards for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.

18.5: The organization should publish information for all personnel, including employees and contractors, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities.

18.6: The organization should conduct periodic incident scenario sessions for personnel associated with the incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the incident handling team.

CSC-18: Incident Response and Management Technical Solution

Design Specification

START

Control Requirements: *Develop an incident response plan with clearly delineated roles and responsibilities for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of network and systems.*

Design Requirements:

1. Establish Incident Reporting (IR) system of record
- Track and manage all Security Incidents

2. Create CSIRT to manage incidents
- Assign individuals from appropriate organizations / departments
- Conduct periodic table top exercises to prepare for an incident

3. Establish process for detecting incidents (precursors and indicators)
- Precursor: an incident may occur in the future
- Indicator: an incident may have occurred or may be occurring now

4. Establish process for managing incidents
- Detect: Receive and review event information, reports and alerts.
- Triage: Determine what happened, impact, recovery and mitigation
- Respond: Resolve or mitigate an incident, implement follow-up strategies

5. Establish set of incident handling use cases and actions
- Use Case 1: Malware Detection and Analysis
- Use Case 2: Compromised Credentials
- Use Case 3: DDoS Attack
- Use Case 4: Zero Day Threat or Vulnerability
- Use Case 5: Lost or stolen laptop / desktop
- Use Case 6: Lost or stolen tape drive
- Use Case 7: Unauthorized data disclosure (via e-mail, website posting)
- Use Case 8: Compromised System

6. Real-time Alerts and Management Reports
- Alert Security Defenders when suspicious activity is detected.
- Produce management and operations reports (ad-hoc and pre-defined)

7. Update Incident Reporting (IR) system of record
- Update IR system of record based on detected incidents
- Advise management of incidents

Compliance Assessment: *Implement, operate, alert and report using process and tools to make sure an organization has a properly tested plan with appropriate trained resources for dealing with any adverse events or threats of adverse events*

END

Alerting & Reporting

START

Control Requirements: *Develop an incident response plan with clearly delineated roles and responsibilities for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of network and systems.*

Alerting & Reporting Requirements:

1. Establish Incident Reporting (IR) system of record
- Establish database that inventories all security incidents
- Create monthly report of new security incidents
- Create trend report of security incidents over past 12 months

2. Create CSIRT to manage incidents
- Report of individuals added / removed from CSIRT

3. Establish process for detecting incidents (precursors and indicators)
- Monthly report of precursor: an incident may occur in the future
- Monthly report of indicator: an incident may have occurred or may be occurring now

4. Establish process for managing incidents
- Report of incidents including detection, triage steps, response

5. Establish set of incident handling use cases and actions
- Use Case 1 Report : Malware Detection and Analysis
- Use Case 2 Report: Compromised Credentials
- Use Case 3 Report: DDoS Attack
- Use Case 4 Report: Zero Day Threat or Vulnerability
- Use Case 5 Report: Lost or stolen laptop / desktop
- Use Case 6 Report: Lost or stolen tape drive
- Use Case 7 Report: Unauthorized data disclosure (via e-mail, website posting)
- Use Case 8 Report: Compromised System

6. Real-time Alerts and Management Reports
- Alert Security Defenders when suspicious activity is detected.
- Produce management and operations reports (ad-hoc and pre-defined)

7. Update Incident Reporting (IR) system of record
- Update IR system of record based on detected incidents
- Advise management of incidents

Compliance Assessment: *Implement, operate, alert and report using process and tools to make sure an organization has a properly tested plan with appropriate trained resources for dealing with any adverse events or threats of adverse events*

END

CSC-19: Secure Network Engineering Control Environment

Control Objective

The process and tools used to build, update, and validate a network infrastructure that can properly withstand attacks from advanced threats.

Control

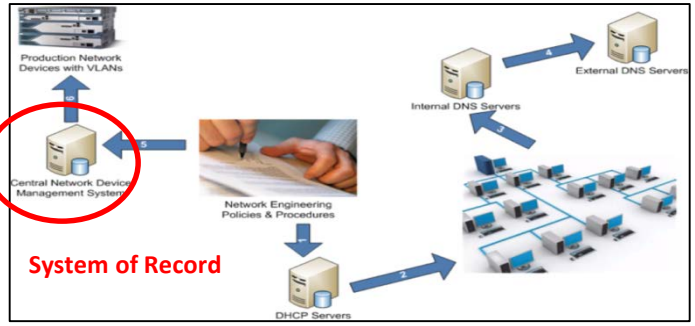
Use a robust, secure network engineering process to prevent security controls from being circumvented. Deploy a network architecture with at least three tiers; DMZ, middleware, private network. Allow rapid deployment of new access controls to quickly deflect attacks.

Consequences of not Implementing this Control

Many controls in this document are effective but can be circumvented in networks that are poorly designed. Without a carefully planned and properly implemented network architecture, attackers can bypass security controls on certain systems, pivoting through the network to gain access to target machines. Attackers frequently map networks looking for unneeded connections between systems, weak filtering, and a lack of network separation. Therefore, a robust, secure network engineering process must be employed to complement the detailed controls being measured in other sections of this document.

Control System Analysis

Examine the network engineering process and evaluating the controls that work together in order to create a secure and robust network architecture.



Step 1: Network engineering policies and procedures dictate how network systems function to include dynamic host configuration protocol (DHCP) servers
Step 2: DHCP servers provide IP addresses to systems on the network
Step 3: Network devices perform DNS lookups to internal DNS servers
Step 4: Internal DNS servers perform DNS lookups to external DNS servers
Step 5: Network engineering policies and procedures dictate how a central network management system functions
Step 6: Central network management systems configure network devices.

Control Assessment

19.1: Design the network using a minimum of a three-tier architecture (DMZ, middleware, and private network). Any system accessible from the Internet should be on the DMZ, but DMZ systems should never contain sensitive data. Any system with sensitive data should reside on the private network and never be directly accessible from the Internet. DMZ systems should communicate with private network systems through an application proxy residing on the middleware tier.

19.2: To support rapid response and shunning of detected attacks, engineer the network architecture and its corresponding systems for rapid deployment of new access control lists, rules, signatures, blocks, black holes, and other defensive measures.

19.3: Deploy domain name systems (DNS) in a hierarchical, structured fashion, with all internal network client machines configured to send requests to intranet DNS servers, not to DNS servers located on the Internet. These internal DNS servers should be configured to forward requests they cannot resolve to DNS servers located on a protected DMZ. These DMZ servers, in turn, should be the only DNS servers allowed to send requests to the Internet.

19.4: Segment the enterprise network into multiple, separate trust zones to provide more granular control of system access and additional intranet boundary defenses

CSC-19: Secure Network Engineering Technical Solution

Design Specification

START

Control Requirements: *Use a robust, secure network engineering process to prevent security controls from being circumvented. Deploy a network architecture with at least three tiers; DMZ, middleware, private network. Allow rapid deployment of new access controls to quickly deflect attacks.*

Design Requirements:

1. Establish Secure Network Engineering system of record.
- Establish DMZ, middleware, private network system of record

2. Create secure network architecture configuration baseline
- Quarterly review and business validation of DMZ, middleware, private network configurations

3. Scan devices to detect mis-configured network components
- Perform automated scans on a regular basis against DMZ, middleware, private network configurations
- Compare scan results to a known effective baseline.

4. Monitor devices to detect mis-configured network components
- Monitor DMZ, middleware, private network configurations
- Compare monitor results to a known effective baseline.

5*. Configure network devices to block mis-configurations*
- Filter unauthorized connections to DMZ, middleware, private networks
- Compare monitor results to a known effective baseline.

6. Real-time Alerts and Management Reports
- Alert Security Defenders when suspicious activity is detected.
- Produce management and operations reports (ad-hoc and pre-defined)

7. Update Secure Network Engineering system of record.
- Advise asset owners of changes and receive approval of updated configuration

Compliance Assessment: *Implement, operate, alert and report using process and tools to build, update, and validate a network infrastructure that can properly withstand attacks from advanced threats.*

END

Alerting & Reporting

START

Control Requirements: *Use a robust, secure network engineering process to prevent security controls from being circumvented. Deploy a network architecture with at least three tiers; DMZ, middleware, private network. Allow rapid deployment of new access controls to quickly deflect attacks.*

Design Requirements:

1. Establish Secure Network Engineering system of record.
- Create monthly report of DMZ, middleware, private network configuration changes
- Create trend report of DMZ, middleware, private network configuration changes over past 12 months

2. Create secure network architecture configuration baseline
- Report of quarterly review and business validation of DMZ, middleware, private network configurations

3. Scan devices to detect mis-configured network components
- Report of DMZ, middleware, private network configuration changes discovered via monthly scan
- Trend report of DMZ, middleware, private network configuration changes discovered via monthly scan over past 12 months

4. Monitor devices to detect mis-configured network components
- Report of DMZ, middleware, private network configuration changes discovered via monitoring
- Trend report of DMZ, middleware, private network configuration changes discovered via monitoring over past 12 months

5*. Configure network devices to block mis-configurations*
- Report of blocked / allowed DMZ, middleware, private network configuration changes
- Trend report of blocked / allowed DMZ, middleware, private network configuration changes over past 12 months.

6. Real-time Alerts and Management Reports
- Alert Security Defenders when suspicious activity is detected.
- Produce management and operations reports (ad-hoc and pre-defined)

7. Update Secure Network Engineering system of record.
- Advise asset owners of changes and receive approval of updated configuration

Compliance Assessment: *Implement, operate, alert and report using process and tools to build, update, and validate a network infrastructure that can properly withstand attacks from advanced threats.*

END

CSC-20: Penetration Testing and Red Team Exercises Control Environment

Control Objective

The process and tools used to simulate attacks against a network to validate the overall security of an organization.

Control

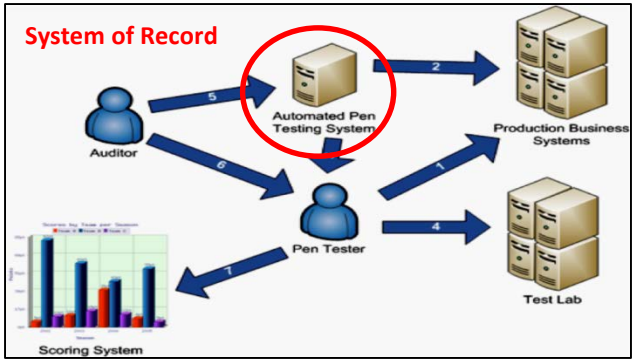
Conduct regular internal and external penetration tests that mimic an attack to identify vulnerabilities and gauge the potential damage. Use periodic red team exercises – all-out attempts to gain access to critical data and systems to test existing defenses and response capabilities.

Consequences of not Implementing this Control

Attackers penetrate networks and systems through social engineering and by exploiting vulnerable software and hardware. Once they get access, they often burrow deep into target systems and broadly expand the number of machines over which they have control. Most organizations do not exercise their defenses, so they are uncertain about their capabilities and unprepared for identifying and responding to attack.

Control System Analysis

Examine red team and penetration exercises and how those efforts can be valuable to organization personnel when identifying which vulnerabilities are present in the organization.



Step 1: Penetration testers perform penetration tests of production systems
Step 2: Automated pen-testing tools perform penetration tests of production systems
Step 3: Automated pen-testing tools inform penetration tester of vulnerabilities discovered
Step 4: Penetration testers perform more extensive penetration tests of test lab systems
Step 5: Auditors evaluate and inspect the work performed by automated pen-testing tools
Step 6: Auditors evaluate and inspect the work performed by penetration testers
Step 7:Penetration testers generate reports and statistics about the vulnerabilities that have been discovered.

Control Assessment

20.1: Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems. Penetration testing should occur from outside the network perimeter as well as from within its boundaries to simulate both outsider and insider attacks.

20.2: If any user or system accounts are used to perform penetration testing, control and monitor those accounts to make sure they are only being used for legitimate purposes.

20.3: Perform periodic red team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.

20.4: Ensure that systemic problems discovered in penetration tests and red team exercises are fully tracked and mitigated.

Control 20.5: Measure how well the organization has reduced the significant enablers for attackers by setting up automated processes to find:

- Cleartext e-mails and documents with "password" in the filename or body
- Critical network diagrams stored online and in cleartext
- Critical configuration files stored online and in cleartext
- Vulnerability assessment, penetration test reports, and red team finding documents stored online and in cleartext
- Other sensitive information identified by management personnel as critical to the operation of the enterprise

20.6: Include social engineering within a penetration test. The human element is often the weakest link in an organization and one that attackers often target.

20.7: Plan clear goals of the penetration test itself with blended attacks in mind, identifying the goal machine or target asset. Many APT-style attacks deploy multiple vectors--often social engineering combined with web or network exploitation. Red team manual or automated testing that captures pivoted and multi-vector attacks offers a more realistic assessment of security posture and risk to critical assets.

20.8: Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.

20.9: Devise a scoring method for determining the results of red team exercises so that results can be compared over time.

20.10: A test bed that mimics a production environment for specific penetration tests and red team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.

CSC-20: Penetration Testing and Red Team Exercises Technical Solution

Design Specification

START

Control Requirements: *Conduct regular internal and external penetration tests that mimic an attack to identify vulnerabilities and gauge the potential damage. Use periodic red team exercises – all-out attempts to gain access to critical data and systems to test existing defenses and response capabilities.*

Design Requirements:

Adopt best practices for frequency and approach for security penetration testing

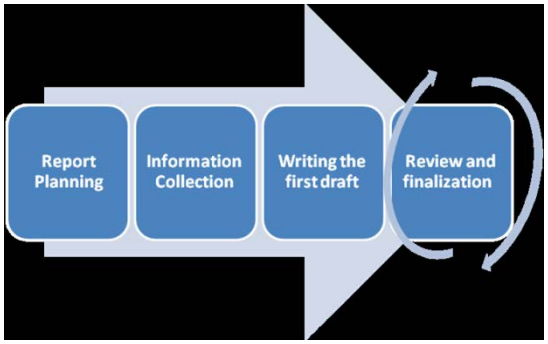
- Match Testing Frequency to Real-World Needs and Regulations - The PCI DDS advises that "penetration testing should be performed at least annually".
- Identify Potential Threats - test against internal and external threats. Internal system threats include those initiated by employees, clients and partners, while external threats are almost always Internet-based.
- Protect The System Before Testing - Conducting penetration testing presents a risk to the stability of a system. Creating a secure system-wide backup should be part of any penetration test.
- Create A Persona of Attackers - Penetration testers are hired to think and act like actual attackers, so the more information they have about who might want to hack into a security system, the better.
- Conduct Both Black Box and White Box Testing - Black box penetration testing assumes that the attacker has no knowledge of your specific system or network. These hackers look for weaknesses and information leaks that are commonly found within networks. White box testing works on the assumption that the would-be attacker has extensive prior knowledge of the network, such as an employee or former employee might have. This testing provides detailed data about how a network functions, providing valuable insight as to both the security of a system as well as the system design quality.

Compliance Assessment: *Implement, operate, alert and report using process and tools to simulate attacks against a network to validate the overall security of an organization.*

END

Alerting & Reporting

Pen Test Reporting Process (recommendation from CSCS)



Report Planning:
- Includes objectives, timeframe, target audiences, scope, classification, distribution

Information Collection:
- Collecting the information during the penetration testing stages/steps is an important step to be able to write the report. This includes scanning results, vulnerability assessment, snap shots of the findings and exploits (if any), etc.

Writing the First Draft:
- Start writing a rough draft report using all relevant information gathered using the relevant notes. At this stage, it is highly recommended not to be concerned about proofreading and editing. Typically, 60% of report writing time will be in writing the draft.

Review and Finalization:
- Draft needs to be reviewed to enhance it, peer review is highly recommended to have a second opinion. In case the penetration testing has been conducted by a team, all team members need to review and/or edit it. Peer review depends on the type of penetration testing conducted, if it is a black box penetration testing, one of the penetration testing team needs to review the report. If the test is white penetration testing, someone with knowledge of the target system will review the report collaboratively. This will lead to much better results.