Creating a System Security Plan

with the 18 CIS Critical Security Controls

Duane Dunston

Table Of Contents

What is a System Security Plan?

The System Security Plan (SSP) is **“living” document.** It has to be reviewed often and updated as necessary. Even though a security control may be in place, it still has to be continually assessed to ensure it remains in place and performs as expected. Software patches, version changes, security patches, or other day-to-day system maintenance may change a control. An administrator may disable a control to determine if it is impacting a production process or service and forget to put it back in place. The SSP requires continuous review, updates as necessary, and testing the control. How the control is tested can be included in the SSP.

Due to the amount of sensitive information in it, the SSP has to be protected. It may reside encrypted at rest, in a tightly controlled wiki or Office365 or Google Drive. If keeping it in a cloud-based environment, it is important to use 2FA and to ensure the sharing controls do not change which could potentially lead to leakage of its existence and location or a breach.

How often the controls should be reviewed is organization-dependent. The risk tolerance of each organization depends on its mission and the information it manages. **Minimum, all controls should be tested every six months.** That provides **continuous monitoring** and may require updating and reviewing multiple controls, especially where there are overlaps. For example, penetration testing may require a review of audit logs due to events not triggering alerts. However, a control test can occur whenever an incident or security event occurs. For example, if there is a control in place to trigger an alert when login failures exceed an organization-defined threshold, then that is a control test. If the anti-malware software triggers an alert, that is a control test. Receiving an alert when a threshold for an alert is received is a control test because you have evidence it is working as expected. Another reason to test all controls is that an alert may not be triggering based on a given event so the control review allows testing to determine if the monitoring is still working. An application upgrade may have changed the location of logs and the alert is not working because it is monitoring non-existent files, for instance.

The SSP is the documentation for the security program. It provides a centralized location to keep track of all the requirements for the security of the organization. The SSP controls based on the CIS Top 18 controls include the technical controls. Those controls, when implemented properly, can help reduce the impact of many types of malware attacks, even phishing with routine security awareness training that is supplemented with phishing tests. Managerial and operational controls also have to be implemented and continuously assessed. If you are having a slow day, test some controls from the SSP and update as necessary. Make use of your calendar to test controls on a systematic basis. Ensure you keep the SSP protected, test often, and update as needed.

CIS Critical Security Control 1: Inventory and Control of Enterprise Assets

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate. -https://www.cisecurity.org/controls/inventory-and-control-of-enterprise-assets/

You **must** identify all of the organization's devices and assets to have a comprehensive security program. This helps to define the scope of what you have to protect. Distributed organizations add a layer of complexity, but not impossibility, to maintain an accurate inventory system.

Set up a plan to update the inventory at least on a monthly basis. More if you are in a large organization because purchases may occur more frequently. It is also recommended to use a passive asset discovery tool or other commercial product in an organization with hundreds or thousands of assets.

It cannot be overstated that you must know every device in your organization. There is no way to have a comprehensive security program unless you know what you have to protect. Some organizations may have a network-capable fire alarm or other service provided by a third-party organization. Those should be isolated on a VLAN separate from other internal resources. Breaches have occurred through third-party vendor assets. It is on your network so you must know it exists and apply controls where possible and network segmentation is a good start.

All other controls and recommendations follow this control.

All assets with an IP, or can obtain an IP (like a fluke that is not always connected to a network) or connected to a device (like a printer or fax machine) with an IP must be accounted for in order to create a comprehensive security program.

What to document

State of this control [Implemented, Planned, Not in Place]

Does your organization have an updated asset inventory management system, spreadsheet, or process? **If it is not in place, document a plan and date to begin the process.**

IP assets and assets connected (usb drives, printer, etc.) Use a spreadsheet, commercial, or open-source tool like a wiki.

Minimum documentation: Hostname, OS Name, OS Version, mac address, location, IP, function, primary contact(s)

-Use a tab in the spreadsheet for each OS or device type or group by org functions. Be consistent.

In your SSP, provide a link to the inventory or explain where it is located.

The specific tools and methods used to identify assets.

Some methods to collect an inventory of assets are to review, DHCP logs, DNS records, switch logs (**ideal since any device with an IP must traverse a switch, within virtually any network**), IDS/IPS logs, or if you use a scanner, use an arp sweep but connect the scanner to each VLAN/LAN segment. Remember the networking principle that the packet header replaces its mac address with the router it is traversing so plugging directly into each LAN segment is necessary.

- Inject a process into IT-related purchases to prepare for new assets and add to the inventory when it arrives or add an entry with a unique code so you know it is planning to be purchased. When you review your inventory, you can follow up to determine if it was purchased and edit the inventory accordingly
- If the budget allows, use a commercial tool for asset discovery. Those are usually advertised as passive asset discovery tools.

In the SSP, explain the procedures for checking and updating the inventory asset.

Example:

Download the DHCP server logs, switch logs, and IDS logs. Run the custom script XXX to parse the results and compare them to the asset inventory.

If a new device is found, contact the system and network administrators to identify the device. If the device cannot be located, check the switch logs to determine where it would be located and begin the incident response procedures.

If a device is in the inventory but doesn't show up during the comparison analysis, contact the POC and determine the status. If decommissioned, check the firewall (or ask XXX) to ensure no rules are in place for it.

First few days as an infosec professional and determining where assets are located

Inquire about remote workers, part-time and contractors and the devices they use.

Inquire about field offices and their locations and how assets are managed in those locations.

Interview system and network administrators - determine if mobile devices are personal or company-owned, determine if portable media is allowed, if users can plug in their cell phones into PCs, if cell phones are company-owned and what technology is used to manage those devices if company-owned. Network administrators can provide insight into assets by using switch logs or other network-based tools.

Inquire with the head of IT - they may know of devices that have been unaccounted for or will help create a process to inject IT insight into purchases

Identify people who perform support for their department (larger organizations may designate someone as a power user to perform basic tasks) - They may know of devices that have been purchased and bypassed standard procedures.

CIS Critical Security Control 2: Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.
https://www.cisecurity.org/controls/inventory-and-control-of-software-assets/

The control is to ensure your organization is actively keeping track of all software applications. In addition to an inventory, controlling which applications and associated libraries are allowed to execute on systems is recommended. Both of these require continuous monitoring, though, together, perform a highly effective method to mitigate the known and unknown threats. Application control does not stop all attacks, but can block common attacks and provide an early warning system before or immediately after a breach.

One method of learning what software is being used is to employ the auditing mode with AppLocker, Software Restriction Policies, or Sysmon. Linux has auditd which can log applications executing. These tools can help identify the software used on systems, but necessarily the version. Let those applications audit for a week or more and then use aggregation tools and methods to determine what software is being used in the organization. In large enterprises, these tools could prove to be invaluable to determine what is running and if legacy versions of software could be running or software that should have been deleted.

This is not an easy task and one that will take a fairly significant amount of time without automated tools in enterprise organizations. The effort is worth it to better understand processes within the organization.

What to document

State of this control [Implemented, Planned, Not in Place]

Does your organization have a software inventory and/or implement application control? **If it is not in place, document a plan and date to begin the process.**

Method(s) used to maintain software inventory

Explain the process for scanning hosts for software on each OS or the manual methods for hosts where automated scanning may not feasible (e.g. printers, faxes, scanners, etc.)

Use an enterprise tool to help maintain an inventory of installed software some vulnerability scanners have the capability to check for installed software. A policy can be put in place to also restrict installing software that is not provided by the OSes vendor.

Document any OSes that have policies regarding software installation. It can include who is allowed to install the software and if the software has to only be provided by the OSes vendor.

Hosts that contain legacy software or soon to be replaced outdated software with the plan and date for removal

The complexity of many organizations may necessitate running legacy software or the system may be high impact where downtime could put people's lives at risk. For example, systems where life and property are at stake, are highly sensitive and may require running legacy software. While it may seem counterintuitive to not have such critical systems patched, the downtime that can occur due to a patch or major system upgrade may be unacceptable (network segmentation could help protect those systems).

Document hosts and software programs containing legacy software along with their respective mitigating controls.

Response to unauthorized software

Document the procedure for responding to unauthorized software including whom to contact for a specific OS, management involvement, notifications to the user, or plans to remove or replace the software.

Document links to any organizational policies which explicitly state that unauthorized software has to be removed. Management involvement is needed because removing software could impact someone's productivity so a plan should be suggested to manage the unauthorized software.

Application control methods for authorized software, libraries, and scripts

Application control provides a powerful method of restricting software program execution. It includes the executables, and with some application control programs, their associated libraries (e.g. windows DLLs).

Microsoft Windows has AppLocker and on systems below Windows 10 Premium, it uses Software Restriction Policies (SRP). Active Directory can be used to control AppLocker and SRP policies so that the management is centralized. It also allows for creating test groups of PCs that can be used to push policies and determine how it impacts production processes. **To reiterate this point, application control policies must be pushed out systematically because of the complex nature of the organization's networks and to limit the impact on production processes.** However, when a conflict is found or a production process is impacted, centralizing allows for quickly rolling back the change and documenting the process that broke. Application controls require a detailed understanding of organizational processes which is an ***incidental*** benefit of its deployment - **understanding the complex processes within organizations**.

Document the name of the policy implemented for each OS version, group of users, or server function.

Document any planned application controls to the respective policy so those can be revisited at a later time.

Document the group of test users and the respective test policy. Explain the process used to alert the test group and how they should report any problems associated with the policy implementation.

Explain the process of how controls will be rolled back in case of significant impacts to production processes.

Document where the logs are stored for monitoring alerts from the application control software. If there are specific scripts, dashboards, or processes used to audit those alerts, document the location and methods for monitoring and responding.

CIS Critical Security Control 3: Data Protection

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data. https://www.cisecurity.org/controls/data-protection/

The control has to do with identifying the various types of stored, processed, and transmitted data within an organization. In many respects, the control has to do with Information Governance. It is the process within an organization of managing data across its entire 'lifecycle' (i.e. data provenance). Just like knowing the assets and what software is on each asset, it is essential to know the type of data stored and where it is stored in order to apply the appropriate controls to protect it. Accordingly, **this is a hard control**. *The value received from identifying data, locating it, and determining where it should reside is invaluable.* **It provides a tremendous amount of information about an organization, its processes, and if it is managing data that aligns with its mission.**

Keeping track of data can be a daunting task due to the data silos and the voluminous amounts of data that may exist within organizations. Sometimes data leakage or breaches occur as a result of data being stored unprotected. **Software needs to be properly configured, as well, to help further protect the data.**

Azure's Rights Management has many features to help with managing and protecting data. It includes tagging, automatic classification, encrypting Office documents, setting retention policies on data, and determining if it should be deleted or moved to a restricted area for review before deleting it, among other features. Commercial tools can also tag data to classify it and automatically move it to a specific location.

For all public facing servers and public servers that link to databases, it is good to ensure only the necessary data needed on those public systems are accessible. It may require having a separate database that is populated with data from the primary database. Ensure the public-facing database can not initiate connections to the primary database.

When a server is restored from backup, it should be scanned to determine if data that should be deleted or stored on another system exists on it.

What to document

State of this control [Implemented, Planned, Not in Place]

Has the organization identified the various types of data stored within its security boundary?

Does the organization have mechanisms in place to protect data based on the level of risk identified if the CIA (Confidentiality, Integrity, & Availability) is/are impacted?

Has the organization determined how long all the data types it manages need to reside within the organization and are their policies and procedures for destroying data when it is no longer needed?

If it is not in place, document a plan and date to begin the process.

Create a policy on how data is managed

The documentation for the data types is best kept in a database, spreadsheet, etc.

Document the location of the policy and procedures for managing the data. This could be a link to an existing policy and/or procedures.

Document the process the organization uses to scan for data and locate it on all assets.

Document the frequency in which scans are performed to search for data.

Document the types of data and which hosts it **should** be located.

Document the most sensitive data and who should have access to it.

Document the labels or tags applied to specific types of data.

Configure appropriate access controls

Encrypt data on End-user Devices and sensitive data at rest

When encrypting data on end-user devices, it needs to be determined in what state is the user's device in when the data is encrypted. Whole disk encryption is effective when the device is turned off. Once the system is booted, the data is available to any application or process. Highly sensitive data should be encrypted even when the computer is turned on. Even though the data may not be actively used, it should be encrypted until it is used. Software programs are available that can encrypt entire folders or individual files or volumes created to store the data at rest, while the device is turned on.

Document the software and process for encrypting data at rest in the various states of the device.

Document which types of data require being encrypted while the device is turned on, the software used, and the configuration requirements for the device.

Document data flows

Documenting data flows is a hard process. However, once the organization has gone through the process, it is invaluable because it helps to uncover redundancies, data siloes, outdated processes, and, sometimes, inefficient processes. It can help make sense of the many complexities within organizations and understand how it all interrelates.

Document how data is transmitted within an organization. The creation could be data coming into the organization from another source.

Encrypt data on removable devices

Document what types of data are allowed to be stored on removable devices.

Document the types of removable devices that are allowed for data to be stored. This may be a USB device that has built-in encryption only. It is also recommended to document how much data can be stored on removable devices (ie. does someone need 10 million customer records or a small sample?)

Encrypt sensitive data in transit

Document the processes for transmitting data and the encryption methods required for it to be transmitted. Keep in mind that communication between computers and network printers may not be encrypted, so it should be determined if highly sensitive data can be transmitted across the network to printers, faxes, scanners, etc.

Segment data processing and storage based on the sensitivity

Document the network segmentation requirements for highly sensitive data. This type of data may be sensitive intellectual property or employee information.

Document the procedures necessary for the data to be transmitted out of the segmented network and how it should be managed.

Document how often users receive training on proper management of data on secure LANs and what type of training they receive.

Deploy a data loss prevention (DLP) solution

Document the controls used for data loss prevention. The documentation should include where the DLP solutions are deployed, how it is configured, which users, and types of data it applies to.

Document the types of alerts that are generated and how often the logs are reviewed.

Document the response process for an alert that requires an investigation. It should include the data owner, system administrator, and procedures for the investigation.

Log sensitive data access

Most OSes have a native kernel feature to allow auditing access to specific files and folders. Commercial solutions could also provide this type of functionality.

Document the types of data that have to be monitored. This is typically the high-value data.

Document any regulatory compliance requirements and which data types have to be monitored.

Document the types of alerts that should be generated and how often the control is tested to ensure it is working as expected. A control test can be when an alert is received and may not need to be explicitly tested unless you have documented types of alerts that should be received, but are not received on a routine basis or at all.

Data Retention Policies

Document how long the data types identified by the organization have to be retained for regulatory or legal requirements. This will require the assistance of legal personnel to ensure the policy would not conflict with any e-discovery requirements.

Some commercial or native products such as Azure Rights Management allow classifying data and applying policies that will delete data or move it to a location to allow data owners the opportunity to determine if it is still necessary to keep in production.

CIS Critical Security Control 4: Secure Configuration of Enterprise Assets and Software

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications). -https://www.cisecurity.org/controls/secure-configuration-of-enterprise-assets-and-software/

This control deals with ensuring there is a process in place for secure configuration of assets and software which includes mobile devices.

In an existing enterprise, security configurations must be deployed systematically in order to minimize the impact on organizational processes. Organizations are complex regardless of how large or small. At some point in time, someone could have created a solution to fix an immediate need without documentation and it becomes a mission-critical process. A single change such as session lockout or implementing password lockouts could break a process that used to run automatically.

Remember that if the software isn't needed, the recommendation is to remove it because even though it may not be exposed due to users not authenticating to the system, it could potentially lead to a vulnerability, such as a local privilege escalation if an adversary does gain access to the system.

Secure configurations include software applications such as Microsoft Office. Malicious code can be executed using macros, for example, so there should be settings in place to mitigate the execution of macros unless it is signed by the organization or an organization-trusted third-party. Accordingly, both network-accessible services and local software applications must have secure configurations in place.

There are many organizations that provide hardening recommendations (e.g. NIST checklist, DISA STIGs, CIS hardening guides, PCI security recommendations). Those **must** be configured based on each organization's needs. It is not recommended to download a security hardening Group Policy, for example, and enable it because it is highly likely to disrupt production processes. The hardening recommendations **must** be **read carefully, understood, and tested carefully on each OS based on its function**. **Always** implement security hardening configuration **systematically and** after there is assurance the roles, processes, and other functions of the device or software is well-understood to **minimize impact** to production.

What to document

State of this control [Implemented, Planned, Not in Place]

The organization applies security configurations to all devices and software applications.

Firewalls are deployed on end-point devices and centrally managed.

Unnecessary services are uninstalled.

Mobile devices have centrally managed configuration policies and a separate workspace for personal and organizational data.

Secure remote management is implemented when remotely or locally configuring devices.

Establish and Maintain a Secure Configuration Process

If security policies such as those provided by the CIS organization are used, then a link to a spreadsheet or procedure hardening documents can be linked here. The security configurations should be outlined for each network and software service and each OS version and OS function. Any deviations **must** be documented along with the mitigating controls.

Document the security configurations for each OS and device on the network.

Document the security configurations for each software application.

Develop a test plan to verify security configurations are in place and working as expected

Scripts and automated tools can be employed to check that many security settings are in place and some may require manual testing.

Document the procedures for testing that all secure configuration settings are in place.

Document procedures for testing the security configurations and ensure each is working as expected. This will require understanding what each security configuration is supposed to achieve and creating a testing plan to see if an audit log is generated, if applicable.

Implement and Manage a Firewall on Servers and end-user devices

It is recommended to use a centralized management tool to configure firewall policies on servers and end-user devices. A good practice is to prevent all servers from accessing the Internet if those are used only for internal access. Many organizations ignore firewalls on servers to prevent breaking production processes.

Document the specific firewall policy applied to each server based on its role (e.g. DNS server, mail server, web server). The central firewall name and policy name can be documented here.

Document the specific firewall policy for end-user desktops.

Document any specific firewall policies for specific applications. Some firewall applications such as Windows Advanced Firewall and IPTables have capabilities to apply a rule to a specific service, application, or user.

Document the process for how often firewall rules should be audited.

Securely Manage Enterprise Assets and Software

Document the methods used for securely managing all assets. This can be the use of SSH for devices, or TLS based remote access (e.g. stunnel or HTTPS), or other secure methods including the use of which devices require two-factor authentication

Document the use of remote methods to see the GUI of a remote device such as RDP or end-user remote desktop support software.

Manage Default Accounts on Enterprise Assets and Software

Document the procedures for managing default accounts **before** a new device, software, or network service is brought online whether internal or externally accessible. It is recommended to have a VLAN that isolates new devices prior to being put on the production network.

Document the procedures for testing to ensure all devices, software, or network services have all default accounts disabled, changed, or password reset to organizationally defined policy **before** and **after** being put into production.

Document the tools or methods used to scan and test for default accounts being enabled.

Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Devices

Document which services or applications must be uninstalled or disabled on each OS and network device based on its role. OSes come installed with many applications and network services that may not be needed.

Configure Trusted DNS Servers on Enterprise Assets

Document which DNS servers all assets use for host and IP resolution to include internal and external servers. It is a good practice to have internal servers use only internal accessible DNS servers. DNS servers for resolution from hosts on the internet access should be segmented from the internal LAN and no connections from those DNS server should be initiated to the internal network.

Enforce Automatic Device Lockout on Portable End-User Devices

Document the procedures for configuring lockout on portable devices.

Document the settings enabled for each type of device.

Document where logs are sent to show devices are locked out after a given period of time.

Enforce Remote Wipe Capability on Portable End-User Devices

Document when a portable device can be remotely wiped.

Document the procedures for remote wiping.

Separate Enterprise Workspaces on Mobile End-User Devices

Document the software used to create workspaces (or profiles separating personal and enterprise apps) on mobile devices for users.

Document the process and settings that create the remote workspaces.

CIS Critical Security Control 5: Account Management

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software. - https://www.cisecurity.org/controls/account-management/

This control deals with managing user accounts and authorizations on all devices and software applications. It is highly recommended to inject a process into the hiring and termination of employees for account management. There are far too many case studies of employees who were fired and their account was not disabled and they caused harm to the organization or surrounding community (in cases of industrial control systems). The other issue is the delay in getting new employees on board due to miscommunications or there not being a process in place for administrators to add the users prior to their arrival.

When a new person is authorized to the system, an early warning is ideal because the admins can communicate with the employee's supervisor to determine their roles and responsibilities and ensure they are provided the minimal amount of access necessary. Every user should not be automatically provided an account for remote access, for example, but granted on an as-needed basis.

Another recommendation is to make use of native controls that automatically disable dormant accounts or lock an account after a given time period. The automation can help to mitigate forgetting to disable accounts for temporary employees or when the termination process doesn't occur as scheduled.

It is also recommended to not allow system administrators to log in to systems as an administrative user. Instead, they should log in with a normal user account and elevate it to admin.

There are many automated tools that can help to find service accounts that may have default credentials set and many online resources with default credentials for numerous devices which can be fed into those tools.

When assigning permissions to files, folders, and other resources, it is best to use a centralized management system and assign users to groups. By assigning users to a group, it is easier to disable one account and the group permissions prevent access to information. In an enterprise, it could be a daunting task to locate each resource an individual user has access to and disable it.

What to document

State of this control [Implemented, Planned, Not in Place]

The organization maintains an inventory of users and accounts.

Accounts use unique passwords

Processes are in place to disable dormant accounts

Administrative access to systems is restricted only to administrative users.

User account management is centralized.

Establish and Maintain an Inventory of Accounts

Document the roles in an organization and the user accounts that have those permissions.

Document the servers and the users that are allowed to authenticate to the server. This is for accounts that have interactive logins, not a file server for example.

Document all service accounts and what roles those play. This control can be used to monitor for unauthorized activity or a compromised system if it is well documented. The service account should have a note on which systems it resides. If there is an alert for access to remote systems using the account or a new account is created that is not in the list, then it must be investigated.

Use Unique Passwords

Document the process of determining if users are using unique passwords. In organizations with centralized user account management and Single Sign-On, just document the application used to manage the account passwords and password policies.

Document the policy stating passwords must be unique on all devices and software applications. It may be a link to the respective policy.

Disable Dormant Accounts

Document the process for disabling dormant accounts.

Document the process for auditing accounts and methods used to verify that the user account should still be active. If it is found that a user was terminated or resigned and the account is still active, a review of activity for that account should be performed and any activity investigated.

Document automated tools that can check to see if an account has not been used for the organization's defined period of time. A user's account may be active and they may be still employed. However, their roles or job position may have changed and they still have access to systems, which they no longer need to have access. Communicate with the user and their supervisor to determine if access is still needed and, if not, disable access to the respective systems. It is recommended to inject a process into HR for job position changes so the account access can be removed as soon as the user's role changes.

Restrict Administrator Privileges to Dedicated Administrator Accounts

Document which users have Administrative access.

Document the script or automated tool that checks logs for attempts to elevate to admin that are not in the allowed Administrator list.

Document the alerts that are generated if someone besides authorized users attempt to elevate to admin. A former administrator may have changed their job position and no longer need admin access so it should be removed as soon as possible. Be sure to update the user list who should have admin access.

Document the process for verifying if a user elevated or attempted to elevate to admin access who is not authorized.

Centralize Account Management

Even in an office of 20 people, it is best to use centralized account management. Ensure the system is very secure and has increased auditing capabilities and alerts for unusual activity or repeated login failures.

Document the centralized management system and how accounts are added, disabled, audited, and removed.

Document who is allowed to log in and manage accounts.

Document the process for investigating attempts to log in to the central management system that are not on the allowed list.

CIS Critical Security Control 6: Access Control Management

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software. - https://www.cisecurity.org/controls/access-control-management/

This control deals with having mechanisms in place that can manage the access and privileges that a user has on systems. Organizations should have policies and processes which inject system administrators into the hiring and terminating processes. It is needed so that users are not held up from accessing IT resources when they come on board, but also to ensure they have only the required permissions needed to perform their day-to-day tasks. Large enterprises may have people that come and go quickly or many organizations have contractors that perform work on their systems. Centralized management greatly reduces the overhead of managing those types of dynamic environments.

Access controls are essential to be managed so that users who are terminated, especially those who are fired, cannot gain access to organizational resources to cause damage, leak data, or try to cover their tracks. It is recommended that when the person is taken into the office to be fired, their account access is locked. If someone is resigning or retiring, then automated mechanisms can be employed to disable their account on a given day. The same is true for contractors where their accounts should be locked until their access is needed.

Another common issue is that contractors are often given very high-level privileges such as domain access. That type of access should be handed out sparingly. Organizations may have policies in place to ensure contractors have the appropriate background checks. Some contractors may perform tasks that the IT personnel do not know how to do or what they are doing. It is recommended to require contractors to document what they did and how they did it. In a Windows environment, Group Policies can be applied that allow restricted access for the contractor based on their access needs. Sudo can be used in Unix environments.

Multifactor authentication (MFA) is a powerful mechanism to help mitigate attacks when credentials are harvested via other means. The adversary would have to figure out the MFA used and then get access to the device or out-band communication channel in order to gain access to organizational resources and assets.

Role-based Access Control is a powerful method of implementing the fundamental principle of infosec - least privilege. However, it **requires a thorough understanding of the organizational processes and how someone's role interacts** with those processes.

Related control(s): Account Management

What to document

State of this control [Implemented, Planned, Not in Place]

Does the organization have a process in place to alert administrators before a new user is brought onboard or terminated?

Are there multifactor authentication mechanisms in place for remote access or access to highly sensitive organizational data?

Is access control centralized?

Establish an Access Revoking Process

Document the process for revoking access. A helpdesk system or other automated form-based system can be used to expedite the process.

Document the alerts that should be triggered when the user accounts are created. This can become a continuous monitoring and routine control test that new user, group, or deleted user and group accounts are monitored and alerts triggered. In organizations where users don't change often, then this control alerting should be manually tested.

Require MFA for Externally-Exposed Applications

Document the MFA used for remote access to external applications. This could be remote access to email or an intranet server, for example.

Document how access is granted including who must approve the access and in what form. The approval could be an email or helpdesk system.

Document the alerts to look for when MFA fails, especially the second or third factor.

Document the process for investigating alerts on MFA. Investigate multiple failure alerts when MFA is used, especially if the second or third factor attempts routinely fail.

Require MFA for Remote Network Access

This control is different from Externally-Exposed Applications because access to email or documents located on a web server could use MFA, but not require a full VPN connection to access those resources.

Document the MFA used to access the organizational network. This is usually a VPN or SSH gateway, etc.

Document how access is granted including who must approve the access and in what form. The approval could be an email or helpdesk system.

Document the alerts to look for when MFA fails, especially the second or third factor.

Document the process for investigating alerts on MFA. Investigate multiple failure alerts when MFA is used, especially if the second or third factor attempts routinely fail.

Require MFA for Administrative Access

Document the MFA used to grant administrative access.

Document which devices and applications require MFA access when administrative access is needed.

Establish and Maintain an Inventory of Authentication and Authorization Systems

Document the process for investigating alerts on MFA. Investigate multiple failure alerts when MFA is used, especially if the second or third factor attempts routinely fail.

Centralize Access Control

Document the system used for centrally managing access controls

Document the users allows to grant and revoke access

Document the process that must be followed for granting and revoking access

Define and Maintain Role-Based Access Control

Document the roles within the organization. A spreadsheet or other system may be used for the role granting and can be linked here in the SSP.

Document the permissions and privileges for each role

Document how to add users to their specific role

Document how often the users in roles are audited and whether they still belong. If users were terminated or changed roles, then investigate the cause for not receiving a notification about their dismissal or role change and fix the process errors.

CIS Critical Security Control 7: Continuous Vulnerability Management

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information. -https://www.cisecurity.org/controls/continuous-vulnerability-management/

This control has to do with creating a program to stay up-to-date with software and firmware on a routine basis. Keeping up with software updates can be made much easier when the organization has a comprehensive asset and software inventory. The inventories provide a baseline to ensure all assets are included in vulnerability management.

Legacy systems may be excluded from being scanned for vulnerabilities, though mitigating controls should be in place to reduce the chances of an adversary discovering them. Legacy systems must have compensating controls in place or put on a segmented LAN with access only from or to devices it has to communicate.

One major complication with vulnerability management is products that bundle their libraries instead of using the native OS system libraries or third-party libraries (e.g. OpenSSL, image libraries) installed on the OS. The problem is exacerbated when it is publicly accessible, there is a known vulnerability, it cannot be patched until the vendor provides an update (if they ever do), and the application is mission-critical. Organizations should understand the products they are purchasing to determine how soon a vendor will provide patches for all bundled software that is included and **ensure there is verbiage in the contract regarding how quickly security patches will be provided**.

Keeping up with patches is an ongoing process, especially in organizations with hundreds or thousands of end-user devices. Devices such as printers, scanners, and other devices need to be included in the vulnerability management program.

Understanding how scanners work and how those detect vulnerabilities is critical. Some scanners may look for a specific folder or version of a file to be present to detect if the software is updated. Patches or uninstalling software may leave behind latent files so the scanner will detect an old version present even though it has the latest version. Knowing what the scanner is looking for can allow removing the unneeded files and folders in order for the scan to come back clean. This process can be made simpler with vulnerability scanners that provide reports explaining why an application was flagged as needing to be updated.

Agent-based scans have a continuously running program in the background that waits for the central server to initiate the scan. It is recommended to restrict access to the port used only to the central server that can initiate the scan. Agent-less scanning requires credentials to be used in order to perform scans. Both have benefits. With the agent-based scan, the continuously running program could potentially cause performance problems if there is a bug in the agent process. However, those types of issues are generally rare.

Emergency scanning may be needed for a specific software application for a product or native to an OS. The documentation should include whom to contact and a plan to fix the vulnerability or mitigating controls to put in place until a patch is made available. The plan should include whom to alert to the vulnerability and must include management because they may have to make a risk-based decision if a production product is potentially vulnerable to an attack. If compensating controls can mitigate the attack, then ensure management knows whether or not the organization can put those in place. Otherwise, management will have to decide whether to continue running the vulnerable service or application based on the risk it presents to the organization's mission.

What to document

State of this control [Implemented, Planned, Not in Place]

Does the organization have a vulnerability management plan?

Are all devices covered in the vulnerability scan?

Does the organization use a central vulnerability management program?

Establish and Maintain a Vulnerability Management Process

Document the tools and processes used to perform vulnerability scanning

Document how often scans are performed

Document assets that require manual checks and how those checks must be performed. These types of devices may be printers, scanners, fax machines, or HVAC systems.

Establish and Maintain a Remediation Process

Document the process for remediating vulnerabilities. This could include which groups of users are included in testing updates

Document whom to contact when updates need to be performed on specific devices

Document how the organizational users are notified of system updates

Document the process of how to ensure users reboot the system if required for updates

Document how users are contacted for updates that may impact network connectivity to internal resources or to the internet

Perform Automated Operating System & Application Patch Management

Document which devices and applications, if any, receive automatic updates.

In an enterprise, this may not be desirable especially on production systems. If automatic updates are not allowed, that should be documented and control put in place to ensure automatic updating is turned off

Document how operating systems and applications are updated. The automation in this documentation could include the names and processes for using WSUS or the vendor's package management system or internal mirrors of vendor package management.

Document the schedule for applying updates

Perform Automated Vulnerability Scans of Internal Enterprise Assets and Externally-Exposed Enterprise Assets

Document the process for performing scans. The documentation could include whether or not users are made aware of scans or system administrators. Scanning on a schedule is ideal, though emergency scans may be needed in cases where a known vulnerability has been discovered.

Document the process for performing emergency scanning.

CIS Critical Security Control 8: Audit Log Management

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack. -https://www.cisecurity.org/controls/audit-log-management/

The control ensures the organization has a program in place to collect, analyze, and respond to alerts that are generated in their logs. A log is a record of an event that occurred at a given period of time on an OS, device, or within an application. The Verizon Data Breach Report consistently reports that there was evidence of a breach in the logs prior to the breach occurring.

Log analysis is a skill that may not be taught well in infosec training programs. Logs can provide a significant amount of information to not only support after-the-fact investigations but alert to a potential attack. Organizations can produce a tremendous number of logs based on the number of devices and software applications they have. Without the aid of a Security Information and Event Management (SIEM), it is impossible to review all logs to try and detect anomalies. There are many patterns of behaviors that are known which can alert to someone performing tasks leading up to and after an attack. However, it requires someone who is trained in analyzing logs to determine whether an alert requires further investigation or response. Analysis requires having an understanding of what software, services, and processes are within the organization, correlating logs, and learning to put together all of that information to understand, what happened, what is happening or is about to happen. Learning to analyze logs is a critical skill that must be taught and practiced. An organization is always generating logs so there are plenty of opportunities to practice.

A SIEM is necessary so that the noise can be filtered out and the well-known patterns of behavior can stand out. A good SIEM will have the option to create dashboards so that events can be separated out based on the OS, type (web, mail, login failures), have thresholds that allow alerting after a specified number of events are triggered within a given period of time, and indexing to allow for fast result retrieval.

Syslog is the standard for logging and sending logs to remote systems. However, other applications have been developed to allow for the use of TCP, encrypted log transfer, and buffering in case the central logging server goes down and logs aren't missed when the central logging server comes back online.

What to document

State of this control [Implemented, Planned, Not in Place]

Does the organization centralize log collection?

Are tools in place to review logs?

Does the organization employ alerting and have a response plan?

Does the organization know of any regulatory compliances for what events need to be logged and archived and for how long?

What training is provided or required for system, network, and security administrators?

Establish and Maintain an Audit Log Management Process

Document the process for audit log management.

Document how each OS version must be configured for logging.

Document the location of the application logs for all network services.

Collect Audit Logs

Document which applications send logs to a central server.

Document how logs are sent to a central server if there are no remote logging capabilities. The organization may have to use SNMP traps, FTP or write a script to send logs to a remote server on devices such as scanners, network printers, etc. if those don't support centralized logging.

Ensure Adequate Audit Log Storage

Document the process for monitoring the centralized logging server to alert when disk space starts to become low.

Document the process for managing low storage space on log servers.

Standardize Time Synchronization

Document the server the log servers synchronize their time on.

Document how timestamps are normalized if the organization collects logs from distributed servers in different timezones.

Document what time format logs will be used within the organization. Timezome of organization or UTC.

Collect Detailed Audit Logs

Document the levels of logs that will be collected with the organization.

Collect DNS Query Audit Logs

Document the DNS servers and the location of the query logs which shows the client that queried for a domain and how those are sent to the central logging server. It may be different if the logs are stored in a non-standard location.

Collect URL Request Audit Logs

Document the web servers or proxies and the location of logs and how those are sent to the central logging server.

Collect Command-Line Audit Logs

Document the logging for the execution of commands. Organizations may need this for regulatory compliance. Sysmon for Windows can collect commands executed and the native Linux audited can perform similar functions.

Centralize Audit Logs

Document the centralized logging servers and the methods in which logs are sent to those servers.

Document how to access the servers and who has access to the dashboards and is able to log in. Organizations should categorize their assets by OS and software. Some SIEMs provide the capability to allow users to search specific categories of systems. System administrators can benefit from having a central console to check system logs instead of having to log into each system they maintain.

Retain Audit Logs

Document how long logs are kept based on where they originate. In some organizations, regulatory compliance may require log retention for a given period of time for specific sets of events.

Conduct Audit Log Reviews

Document the process for auditing logs.

Document the types of alerts in which an email or some type of notification will be sent for review.

Document the process for thresholds for specific alerts.

CIS Critical Security Control 9: Email and Web Browser Protections

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement. - https://www.cisecurity.org/controls/email-and-web-browser-protections/

This control deals with managing the security threats presented by email and web browsers. Web browser and email continue to be common methods for adversaries to use as a vector to compromise systems. Web browsers and email provide the opportunity for compromising end-user systems because virtually every organization uses those products.

Web browsers provide multiple vectors of attack when the use of plugins and other add-ons are allowed. The functionality helps make browser experiences easier but those can be used as an attack vector if it is written without secure coding practices and not kept up-to-date if a vulnerability is found. If the plugin management is abandoned there may be no way for the user to know it is out-of-date. Some may not care because it is providing them some convenience. Water-hole attacks can impact organizations when an adversary compromises a website the target organization frequents and abuses that 'trust' relationship to compromise their computers.

Email is a vector for malware, phishing, and spearphishing attacks. When the email contains a malicious attachment and is executed, it could lead to an enterprise being compromised. Some plugins are available for email clients and suffer similar vulnerabilities as web browser plugins. Nation-state actors use email as a vector because it is likely to work and they only need one person to open an attachment or access a website that compromises their machine. If there are no other mitigating controls in place to prevent the attack, then the adversaries could move laterally through the organization, persist in multiple computers, and steal data or carry out their objective.

What to document

State of this control [Implemented, Planned, Not in Place]

Does the organization allow any plugins for web browsers?

Does the organization have a process to keep browsers and any plugins installed up-to-date and remove unsupported plugins?

Does the organization filter email and attachments?

Is there a proxy where malicious domains and URLs are filtered that are known to host malicious files?

Is anti-malware employed for scanning emails?

Ensure Use of Only Fully Supported Browsers and Email Clients

Document the process for scanning to determine the current versions of web browsers and email clients installed on devices.

Document the remediation process including whom to talk to and how the user is alerted to the need to update the browser.

Use DNS Filtering Services

Document the services or methods used to filter DNS queries.

Document how often the DNS access control list is updated.

Document the types of alerts and when a response is necessary.

Maintain and Enforce Network-Based URL Filters

Document the services employed to filter URLs. These types of applications are virtually required due to so many sites using HTTPS, by default, and bypassing enterprise border protections. If there is no central SSL proxy then an agent that resides on end-user desktops to filter URLs should be used within the organization.

Document the types of alerts and when a response is necessary.

Restrict Unnecessary or Unauthorized Browser and Email Client Extensions

Document the process for scanning to determine what plugins are installed on end-user systems or any device that uses a web browser to communicate with the internet.

Implement DMARC

Document if the organization employs the use of DMARC (a specification for authenticating email messages).

Document the servers where it is deployed - even if it is used on an outsourced email provider.

Block Unnecessary File Types

Document what file types the organization blocks.

Document the process for alerting users when files they attempt to send to customers or clients are blocked and methods to ensure safe delivery of the data.

Document the types of alerts and when a response is necessary.

Deploy and Maintain Email Server Anti-Malware Protections

Document the anti-malware solutions employed.

CIS Critical Security Control 10: Malware Defenses

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets. -https://www.cisecurity.org/controls/malware-defenses/

This control deals with ensuring there are defenses in place to mitigate the threat of malware. An organization needs to have more than just antivirus in place in order to effectively mitigate this threat. Malware can come in many forms and has several well-known vectors of attack, particularly email and web browsers, or being introduced as a result of an exploit that takes advantage of unpatched software or a zero-day (an actively exploited vulnerability before a patch is available).

Malware defenses must be layered. Along with antivirus, there should be controls that can proxy web traffic and block known malicious URLs, IPs, and domains. Additionally, host-based controls such as application control can restrict applications and scripts from executing if not in an allowed list or executes outside of an allowed folder (use folder-based allow lists sparingly). Applications can also be restricted if it matches a specific hash or are signed by a certificate. Even though those methods may seem cumbersome, they can be centralized with Active Directory or a third-party tool. Some vendors have restrictions that allow controlling the specific kernel functions each script and application can access and execute. These methods require a detailed understanding of the organization and require a careful implementation plan to prevent impact to production systems.

Antivirus products, domain, URL, and IP restrictions require routine updates because the threats are persistent. Ensure there are procedures in place to monitor host computers so that their definitions are updated consistently and at least daily checks for updates from the vendor. Immediately remediate and fix any system that does not have the most update to date definitions for access control restrictions and antivirus definitions.

If possible within the organization, develop an emergency application control plan that can restrict the use of a specific browser if there is an active exploit targeting browsers or other software that directly accesses the internet. An alternative browser could be used until a patch is deployed to all systems.

Sandboxing is another technology that executes applications in a restricted environment so a malware infection is contained within that environment. These are not perfect solutions but can provide protection against many types of malware attacks or control the spread of infection. If there is an infection, the sandbox can be deleted, the system scanned with the latest antivirus definitions and analyzed to determine if it is safe to put back online.

Ensure there is a plan in place to quickly and properly respond to a malware infection.

What to document

State of this control [Implemented, Planned, Not in Place]

Does the organization have a centralized anti-malware solution in place with the ability to see the current version of definitions and any system out of compliance?

Does the organization prevent autoruns and have a policy on removal media use?

Does the organization employ layers of defenses against malware?

Deploy and Maintain Anti-Malware Software

Document the anti-malware solution used within the organization.

Document all devices that must have anti-malware installed.

Document any devices that don’t have anti-malware and the compensating controls in place.

Document how the product is monitored and how alerts are generated.

Document the process for responding to organizational-defined anomalies.

Configure Automatic Anti-Malware Signature Updates

Document the procedure for ensuring anti-malware signatures are up-to-date on all devices.

Document alerting mechanisms in place when a device is found to be out of compliance.

Disable Autorun and Autoplay for Removable Media

Document if the organization does or doesn't allow autoruns of removable media. If the organization does not, then document any controls in place such as whether the anti-malware solution automatically scans removable media.

Document procedures or controls in place to prevent removable media from being used if employed within the organization.

Enable Anti-Exploitation Feature

Document if native features in the OS are enabled to prevent well-known attacks such as buffer overflow protection.

Many OSes have these features and some are enabled by default. However, those settings should be checked and any deviations documented. Some types of low-level controls such as DEP could break applications. **It would behoove the organization to contact the vendor of the product to fix the problem instead of disabling the protection on the entire OS due to one or two applications.**

Centrally Manage Anti-Malware Software

Document the device where the anti-malware solution is hosted.

Document how often checks are performed to determine if devices within the organization are checking in and receiving updates.

Document if technologies such as Network Access Controls are enabled which will allow a connection from a VPN or other remote system only after ensuring it has the latest anti-malware solution in place.

Use Behavior-Based Anti-Malware Software

Behavior-based anti-malware must be deployed systematically. Additionally, a thorough analysis of each system where it is deployed must be performed. If a system is already infected then the malicious software will appear to be normal behavior and may go undetected.

CIS Critical Security Control 11: Data Recovery

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state. -https://www.cisecurity.org/controls/data-recovery/

This control ensures the organization is able to recover mission-critical data in a reasonable amount of time. Organizations, regardless of size, must have backups of their data and critical services. The control requires the organization to document what their critical assets and services are and what is an acceptable amount of downtime. It may include the downtime associated with a cloud service that becomes unavailable and having a plan to temporarily host the most essential data and information for customers to continue to have access to prevent significant financial loss.

There is nothing more important when it comes to having a robust backup plan than to routinely test to ensure:

1. What is expected to be backed up is backed up.
2. restore a sample of data to ensure data integrity (disks or tapes, where data are stored, could become corrupted and render the backup useless or very expensive to recover)
3. check with the data owner to ensure the latest versions are backed up and restored
4. restoring a critical service and document how long it takes to restore to full operation

The organization has to determine what are the most critical services and data to have available and how much time to get it back online? During the testing of data recovery, those steps can be better determined.

Organizations should add in procedures to store data offsite either physically or digitally (such as to a cloud provider). Organizations should understand the ramifications of syncing data because a ransomware attack could cause encrypted data to propagate to their backup systems. Versioning could certainly help mitigate overwriting the original data so it is something to keep in mind as plans are being developed for offsite restoration. **Be sure to test to see how long it takes to restore data and full systems from a backup when using a cloud provider and determine if it is acceptable based on the organization's context**.

Test your data backups.

What to document

State of this control [Implemented, Planned, Not in Place]

The organization has a data backup and recovery process

Automated backups are performed and tests are performed to ensure what should be backed up is backed up.

Establish and Maintain a Data Recovery Process

Document the data backup and recovery process.

Document which hosts are backed up and the frequency.

Document how often the backup processes are reviewed to ensure all devices have up-to-date backups.

Perform Automated Backups

Document the schedule for data backups. The timing should be properly planned to ensure multiple systems **do not saturate bandwidth** sending data to the backup system and impact internal processes.

Protect Recovery Data

This aspect of the control also includes versioning which vendors may build into their data products and some cloud providers offer this feature.

Document the protection mechanisms in place to protect the data. This may include information about the off-site location whether physical or in the cloud.

Document if encryption is required on specific data types.

Document the procedures for protecting the encryption keys.

Document emergency procedures in case malicious attacks impact the backup system or data being sent to the backup system. An example is real-time syncing or disabling the backup system in the case of a ransomware attack.

Establish and Maintain an Isolated Instance of Recovery Data

Document how the backup system(s) are protected. This may include time-based access from systems such as in the evenings during little impact on internal processes. During business hours access to the backup system may be restricted by firewall rules since systems may not backup during the day.

Test Data Recovery

Document the process for data recovery. This should include the how, how much data, and whom to contact to ensure the data is the latest version.

CIS Critical Security Control 12: Network Infrastructure Management

Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points. - https://www.cisecurity.org/controls/network-infrastructure-management/

This control deals with maintaining the security of network devices such as routers and switches, and the design of the network segments. Network devices are particularly vulnerable because some continue to use insecure protocol versions, are designed for easy configuration so default accounts may exist, use cleartext protocols for management of devices, and do not restrict access to management ports or to the device.

Network devices should be configured to use the most appropriate versions of management protocols such as SNMPv3. Access for managing those devices should be restricted only to the administrators that need access by IP or 2FA when using cloud-based management. Secure communication programs like SSH or using TLS for remote access must be used.

It is imperative that the organization set up a schedule to routinely update network infrastructure devices, as well. Border routers, for example, are exposed directly to the internet. Vulnerabilities in how it handles network traffic could lead to availability issues for the entire organization (and impact distributed enterprise networks).

The design of networks with devices like switches is essential. VLANs should be configured to separate devices based on their role. Network segmentation is very difficult to implement in enterprise organizations due to how complex they are and how network and system administrators may not know the processes and interconnections that exist between devices on different LANs. It is not impossible but requires monitoring the traffic flows between devices and determining how to configure ACLs and putting those in place before the shift to segmented LANs. The segmentation must occur systematically to minimize the impact on production processes. If there are back-end servers used such as databases that do not require access by any user on the LAN, consider adding those to a segmented LAN with access only from the front-end servers it needs to communicate. Employees on separate VLANs should be restricted from communicating with each other using ACLs if there is no need for host-to-host communication between employee devices. Software developers and engineers may need to install new software on a more frequent basis than most employees so they should be on their own LAN. A separate thin-client PC can be set up for them to access LAN resources.

Network infrastructure should extend to devices such as fire alarms, HVAC, and any other devices managed by third parties. Those can present a threat because administrators in an organization normally do not have access to those devices or keep up with their software updates. Those should be put on a separate VLAN that is not accessible to internal resources.

What to document

State of this control [Implemented, Planned, Not in Place]

The organization routinely updates all networking devices.

The organization employs network segmentation.

The organization documents the security protocols used and when they must be employed when managing devices.

The organization has controls in place to limit access to networking devices.

Ensure Network Infrastructure is Up-to-Date

Document the process for ensuring network infrastructure devices are patched

Document the process for ensuring that network devices that are only physically accessible are being patched

Establish and Maintain a Secure Network Architecture

Document the segmented networks and the functions of devices that reside on the LAN.

Securely Manage Network Infrastructure

Document the software used to manage network devices.

Document any devices that do not support secure authentication. It is recommended to ensure the latest OS is installed since SSH is usually available on most network devices.

Document the process for ensuring all network devices have their default username and password either removed or the password changed. This should include changing the community string for SNMP.

Establish and Maintain Architecture Diagram(s)

Document the location of network diagrams.

Document the process for reviewing the diagrams and updating them as needed.

Document the process for showing who last reviewed the diagrams and updated them and when.

Centralize Network Authentication, Authorization, and Auditing (AAA)

Document if AAA is used and the name of the device.

Document the roles that are assigned for the respective users that are managed with AAA.

Document the authentication methods which should require 2FA for cloud-based network management access.

Use of Secure Network Management and Communication Protocols

Document the secure network protocols used within the organization and when it must be employed. This may include HTTPS or TLS for access to web resources, SMB encryption for AD and file shares, SNMPv3, WPA2 for wifi, etc.

Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure

Document when users are allowed to use remote access services.

Document the approval process when a user is allowed to use remote access services.

Document which alerts requires an investigation on remote access devices.

Document the authentication that is used for remote access services.

Establish and Maintain Dedicated Computing Resources for All Administrative Work

Document the methods used to connect to network devices.

This part of the controls suggests IT staff such as network admins use a separate device when managing a network device is required. It may be a thin-client PC next to their desk or a LiveCD PC with access controls that only allow the PC with that IP address to connect to it.

CIS Critical Security Control 13: Network Monitoring and Defense

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base. - https://www.cisecurity.org/controls/network-monitoring-and-defense/

This control deals with ensuring the organization is continuously monitoring the network and have layers of defenses. In order to effectively detect and respond to security events, **organizations need more than just tools**. It requires **security professionals who are able to interpret the data that it collects** to identify an imminent attack or an attack that has already occurred as quickly as possible. Networking monitoring solutions can help provide that insight if properly implemented. An intrusion detection system (IDS) that monitors traffic that passes through the firewall into the organization's network segment is needed. However, traffic needs to be monitored between the network segments in the organization, as well. Malicious traffic may have been delivered to a host undetected by the IDS, but filtering between segments may uncover its activity to infect other computers or perform recon on the network from hosts that should not be performing that activity.

Organizations need to have defenses at the host level because the majority of traffic will be web-based and many websites are using HTTPS. If a malicious site uses HTTPS then malicious code could potentially bypass the IDS. Host-based monitoring must be in place so that suspicious activity on a PC can be quickly investigated. The monitoring between network segments could detect unusual activity such as a user PC scanning all network segments that do not usually perform network scans. Network intrusion detection systems are still needed because those can be used to monitor devices that don't traditionally have host-based monitoring capabilities such as printers and IP phones.

A Network Access Control (NAC) solution may be deployed to restrict new devices on a network segment. A NAC can isolate a host to a segmented VLAN with no access to internal resources. The VLAN may allow access to the internet temporarily to receive OS or anti-malware definition updates prior to being allowed on other VLANs. The VLAN may also isolate the device until an admin finds the device or allows it on the network. Some solutions may allow access to a restricted VLAN only after the user authenticates to a proxy server. Organization-owned mobile devices may have an agent and the central server detects it when it connects to a VLAN and applies the appropriate updates before allowing it access to internal resources.

Additionally, all of the logs generated need to be sent to a central server where they can be aggregated, monitored on a routine basis, and alerts generated for suspicious activity. The Security Information Event Manager (SIEM) has to be tuned to be useful in detecting threats. Otherwise, it just collects logs but provides no value. Many have the option to create dashboards so categories of threats can be created to make viewing the logs easier. Some also contain algorithms that can detect well-known threat patterns and generate alerts. It will require someone taking time to enable those features and test periodically to ensure it is performing that task as intended so a real threat can be detected and a response provided.

What to document

State of this control [Implemented, Planned, Not in Place]

Does the organization use a SIEM for alerting?

Does the organization have a network/host-based intrusion/prevention system?

Does the organization have a system in place to alert on new devices plugged into the network?

Does the organization capture network flow for analysis?

Centralize Security Event Alerting

Document the types of alerts that are generated and the response required. The documentation should include whom to contact for the response.

Document how often rules are tested that do not produce many alerts. It is important to test alerts that do not produce many or any alerts at all especially if it is a high risk. Threat emulation tasks could be used to simulate an attack and see if it triggers the alert in case of a real incident.

Deploy a Host-Based Intrusion Detection Solution

Document any host-based intrusion services or applications in place for the respective devices in the organization. Those can be file integrity monitors, port monitors, or application control solutions. A table can be generated if different solutions are on the various devices.

Document what the solution is monitoring. For example, with file integrity, the function of the OS device may determine what files and directories are monitored. The specific settings for each OS should be documented here. If the specific settings are maintained in a separate system then document the location of the system here.

Document how often rules are to be tested that do not generate any alerts on a frequent basis.

Document the specific process for testing the alerts.

Deploy a Network Intrusion Detection Solution

Document the Network Intrusion detection system (NIDS) services or application in place. The documentation should include the location of the sensors, IPs, and the segments each one monitor.

Document what the solution is monitoring. For example, with file integrity, the function of the OS device may determine what files and directories are monitored. The specific settings for each NIDS may be kept in a centralized repository so the location and method used to collect the settings should be here.

Document how to respond if an alert is generated.

Document how to respond if an alert is generated.

Manage Access Control for Remote Assets

Document the controls in place for remote access devices. Some remote access solutions will ensure the remote device has updated anti-malware definitions, OS updates, and that specific security controls are in place to allow access to organization resources.

Document the level of access allowed for the different roles. The access may be different for an IT staff user versus a non-IT staff user.

Collect Network Traffic Flow Logs

Document the network devices that are generating network flow logs.

Document the method in which the network flow logs are collected and archived on those devices.

Document how often the logs are reviews and the types of alerts that get generated.

Deploy a Host-Based Intrusion Prevention Solution

Document any HIPS products deployed.

Document the types of rules which will automatically prevent the execution of organization-defined threats or prevent opening specific files.

Document how to respond when an alert is generated.

Deploy a Network Intrusion Prevention Solution

Document any NIPS products deployed.

Document the types of rules which will automatically prevent the execution of organization-defined threats or prevent opening specific files.

Document how to respond when an alert is generated.

Document the methods used to test NIPS alerting.

Deploy Port-Level Access Control

Document the configurations used for port-level access. This should include if access to the network is performed using certificates or manual intervention (in the case of mac-address filtering). Some organizations may use a Network Access Control (NAC) solution to manage unauthorized hosts.

Document the alert that is generated when an unauthorized device connects to the network.

Document the response process if a device does not pass the requisite security checks.

Perform application layer filtering

Document application proxies used in the organization.

Document how devices are authenticated to the proxy or if it is transparent.

Document the types of alerts that are generated and the response process.

Tune Security Event Alerting Threshold

Document the process for determining when alerts need to have a threshold.

Document how often the thresholds are reviewed. Thresholds may need to be adjusted depending on threat intell provided to the organization which may require removing or lowering the configurations that are in place.

CIS Critical Security Control 14: Security Awareness and Skills Training

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise. - https://www.cisecurity.org/controls/security-awareness-and-skills-training/

This control deals with ensuring the organization has an ongoing security and awareness training program. The employees in an organization are one of the first lines of defense and the ones likely to notice something amiss. Infosec professionals like to make fun of users for clicking links and downloading files and attachments, though until they've worked in incident response and see the work that went into a well-crafted spearphishing email, it can quickly change someone's mind and state "I would have clicked that too." Infosec professionals need to work on creating a relationship with employees in an organization so they feel comfortable approaching you when they suspect something is not quite right or they downloaded a file and quickly realize that it may have been a mistake. Part of that relationship building is being accessible.

Security awareness training is where that relationship and trust-building can occur. Even if the security awareness training is outsourced, the infosec professional should send reminders about being vigilant and a reminder they are there to assist and to forward messages they feel are suspicious. Those email messages should be followed up with a thank you, even if the message is benign and safe to open. It shows that they are being listened to and their efforts are appreciated. Security awareness training is even more essential when someone can see how they can be impacted or how their actions can impact the organization.

Sharing success stories and some examples of how adversaries are targeting the organization goes a long way to folks understanding how the threat is real and the infosec professional is helping to mitigate the risk WITH their assistance. A good practice is to send out a reminder once a month on where to submit suspicious computer activity or if a suspicious email is received. One person alerting IT to the problem can potentially prevent a mass compromise. Social engineering and phishing training are essential because of the ubiquity of those types of attacks and for being a common initial access point into an organization.

It would also behoove the organization to invest the time, financial, and people resources into providing security training that is specific to the roles of their employees. It may be difficult for someone in finance to understand the types of attacks faced by application developers and vice versa because they may not understand each other roles or the terminology being used. That may lead to people tuning out because they don't understand the language and context being discussed in the awareness training.

Creating a culture of risk comes from senior leadership. It is recommended that any required annual security awareness training be sent by senior executives. The middle managers have to listen and trickle down to the employees they lead. Senior leadership should also support sanctions for those that do not complete training such as disable their access until it is completed. They may even choose to go through the training first and let the organization know of their experience and the amount of time it took to go through it.

[Security awareness training programs should allow users to save their session and return later so that they are not inundated with a lot of information all at once.]

Organizations must budget for IT professionals to improve their skills on an annual basis. It could be a subscription to a training provider or a budget set aside for specialized training. IT training can be quite expensive depending on the provider. Though, the training in tasks related to their role-specific job or on detecting and responding to security incidents can prove to be quite beneficial. The training can provide benefits to the organization by having them attend training that improves business processes by increasing efficiency and potentially lowering costs when they learn about new technologies. Subscribing to a specific company may be helpful if the company provides training relevant to their role. However, that may not be the case so IT professionals should be provided a budget to find training that can benefit them and the organization.

What to document

State of this control [Implemented, Planned, Not in Place]

Does the organization have security awareness training at least annually?

Does the organization require employees to take the training?

Does the organization take action if employees don't complete the training?

Does the organization have role-based security awareness training?

Establish and Maintain a Security Awareness Program

Document the organization's security awareness training program. The training may be outsourced to a third-party organization and that should be documented. The documentation should include how often it occurs.

Document the actions taken if someone doesn't complete the training within a given period of time.

Documenting what is in the security awareness training program could be a screenshot or copy and paste of the various modules.

Minimum, the training should include:

- Recognizing Social Engineering Attacks
- Authentication Best Practices
- Data Handling Best Practices
- Causes of Unintentional Data Exposure
- Recognizing and Reporting Security Incidents
- How to Identify and Report if Their Enterprise Assets are Missing Security Updates
- Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks
- Learning to identify phishing email messages

Document what parts of the training are organization-specific or if the third party allows customizations.

Document how and who updates the training material.

Document who is involved to review the training to ensure it still pertains to the organization or needs to be updated.

Conduct Role-Specific Security Awareness and Skills Training

Document if there is role-specific training. The documentation should include the roles and the type of training they receive. If it is outsourced then document the links and types of training provided.

CIS Critical Security Control 15: Service Provider Management

Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately. -https://www.cisecurity.org/controls/service-provider-management/

This control deals with managing the security of organizational data, processes, and systems that are managed by third parties. When an organization chooses to outsource the risk involved with a service to a third party, the organization that outsourced the service is still responsible for the security of their data. The cloud provider has their own contractual agreements but the organization that uses the data for their business purposes could still be held liable for breaches or data leakages. Another tradeoff is what happens if the third-party systems become unavailable and the organization is unable to fulfill its mission. Before using third-party organizations to outsource the management of data and other services, it has to be determined what are acceptable downtime for the sake of business continuity to appease customer demand and to keep them updated on the status of gaining access to the resources they need.

Email is one service that many organizations are moving to third-party party hosting. Email is a primary method of communication, order delivery, order fulfillment, customer support, etc. The organization should carefully investigate whom they decide to outsource their email hosting to and ensure they have a reasonable record of uptime. Anything below 99% can call into question whether the organization is competent to host email services. Low prices for host services should not be the primary consideration. It can be worth paying a premium for high availability if the organizational mission depends on high uptime.

Another concern is when third-party companies outsource their services to other third parties or use plugins that may allow access to organizational data. There are many questions that need to be asked and documented to understand:

- *how data and services are being managed*
- *the security of the data,*
- *whether or not third parties have access to the data*
- *are backups stored offsite and is the data encrypted*
- *is data stored on foreign computers where encryption may not be allowed*
- *what are the security requirements the primary third-party has with other third parties that have access to the organizational data*
- *how soon will the organization be contacted if there is a data breach or data leakage is discovered*

The location of organizational data can become complicated and assurances cannot be determined without knowing what to look for and questions to ask third-party hosting providers. The security of data and services also applies when an organization hosts its own services but has it managed by third parties. A third party managing the security of an organization can become very complicated when they are allowed to make changes such as applying patches or changing configurations. If those are not planned with the organization they are managing, it can create significant productivity problems.

What to document

State of this control [Implemented, Planned, Not in Place]

Does the organization have a list of all service providers that manage organizational data and services?

Are there service level agreements in place on how data is managed by the service providers' third-party organizations?

Is data categorized and the appropriate controls applied to it by the third party?

Establish and Maintain an Inventory of Service Providers

Document all service providers and contractors and the role each one provides for the organization. The document should include the type of service provided, any points of contact within the organization, and a point of contact at the service provider's location. It also includes any supply chain organizations and **any organizational data they manage**. Effectively, any organization that interacts with the data, services, and day-to-day operations of the organization, including outsourced environmental control services.

Document how often the list of service providers and contact information for internal contacts and the external contacts have to be updated.

Establish and Maintain a Service Provider Management Policy

Document the location of all policies related to the service providers identified above. "Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. (https://www.cisecurity.org/controls/cis-controls-navigator/)"

Document the procedures to ensure any data the service provider has is securely destroyed and no longer accessible including their backups.

Document how often the policies should be reviewed and updated or the procedures carried out that decommissioned the service provider.

Classify Service Providers

Document the risk assessment methods used to classify the impact of any data or services that are made unavailable. Note that this will require the **existence** and review of a business impact analysis and business continuity plan.

Ensure Service Provider Contracts Include Security Requirements

Document the types of data that are managed by the services providers.

Document the requisite security requirements the service provider agrees to implement.

Document the process for how the provider outlined the organization will be contacted in case of a breach or leakage of organizational data they manage.

Document any third parties the service provider uses that interact with organizational data. The service provider should explain how the data is processed, stored, or transmitted to other third parties.

Assess Service Providers

Document the security guidelines that each service provider must adhere to based on the organizational data and services provided.

Document how often the service provider must present evidence they have undergone security reviews or audits to demonstrate they are adhering to the requirements. This will require knowing the various regulatory bodies and standards they have to meet and how often they have to re-certify compliance.

Document the contact at the organization to inquire about any security certifications or audits they should have undergone.

Monitor Service Providers

Document processes for monitoring service providers and any public information about their company. This may include monitoring for security incidents that are publicly reported or other threat intelligence sources that report data breaches and leakages.

Securely Decommission Service Providers

Document the process for ensuring that the removal of all organizational data is destroyed by the service provider when the services are no longer needed. This will require contractual agreements where the service provider attests they have procedures in place to destroy data of customers when it is no longer needed or face legal action if a breach uncovers latent or data from the organization that remained after the service was terminated.

Some service providers have policies that keep data for a given period of time in case their customer decides to re-active the service for convenience. A contractual agreement should be created before the signing of a contract that outlines whether or not the organization wants data deleted immediately after the termination of service.

CIS Critical Security Control 16: Application Software Security

Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise. - https://www.cisecurity.org/controls/application-software-security/

This control deals with managing the lifecycle of software used and developed by the organization. The control is differentiated from vulnerability management because it delves into the level of the “lifecycle” of the software. In other words, it goes beyond vulnerability scans. A vulnerability scanner may not be able to detect vulnerabilities with a custom application, though it could detect vulnerabilities with its installed dependencies (e.g. libraries) and this control pertains to the software development lifecycle.

Application security is essential because that is what is being targeted with attacks. Before an application is developed, the security implications must be considered during the planning all the way through to its production deployment and routinely tested while in development.

Far too often, an application is about to be released in production or has already been released and security vulnerabilities are discovered. Deployment can be delayed or a new application that is already being used for production could be taken offline or expose the organization to numerous threats.

When developing applications, it is best practice to use native functions within the language as much as possible. The most commonly used languages have extensive documentation and many provide sample code or user-contributed comments and suggestions. One issue that could lead to vulnerabilities is using a specific version of libraries and bundling those into the application instead of using the latest version provided by the vendor. That can lead to vulnerabilities with the application if the developer or organization no longer supports the application used in production. It can include an increased cost to the organization by purchasing a new program and the costs involved with its testing and deployment or having to hire a third party to update the software.

Another problem is when custom functions are created to perform tasks that the native language supports. For example, a custom function that uses a system call to perform a task such as a hostname lookup. That is particularly dangerous when the application takes in data from untrusted sources and passes it to the commandline. Aside from that, it can create performance problems in the application because the native programming language functions are typically faster and use lower-level library functions to perform tasks that are much faster and safer.

Despite how well-known many vulnerabilities there are, the same ones continue to be a vector for exploitation due to either a lack of awareness, lack of training, negligence but there is still the fact that programs are created by people and mistakes can be made. There are many free and commercial tools available that can be used to test software to find common vulnerabilities. Microsoft has an open software development lifecycle process that can be used by teams to help mitigate common vulnerabilities. Organizations such as OWASP are a great resource for learning how to create a software development lifecycle that includes security. It also provides a wealth of information about how to:

- test software
- secure code samples in a variety of languages
- applications with software vulnerabilities so developers and security professionals can learn secure coding
- the top ten most common web application vulnerabilities and how to protect against each one

OWASP also has application architecture frameworks that an organization can adopt for a maturity model. Along with OWASP and secure coding training programs such as those offered by We Hack Purple - https://wehackpurple.com - application developers have many resources to help mitigate the vulnerabilities that plague software programs.

What to document:

State of this control [Implemented, Planned, Not in Place, Not Applicable]

Does the organization have a software development process?

Do programmers receive training in secure coding?

Are developers separated from the production systems?

Establish and Maintain a Secure Application Development Process

Document the secure application development process.

The process should involve injecting someone from infosec into the planning meetings within an organization where new ideas are being presented. It can help catch new initiatives early so that security is implemented in the planning stages and throughout the project's lifecycle.

The process should include:

A Process to Accept and Address Software Vulnerabilities

Document the process for how software vulnerabilities are addressed. This includes determining whom to contact and who makes the final decision on whether the application stays in production or taken offline. This applies to having a business continuity plan that documents critical applications and services and their acceptable downtime.

The process for addressing the vulnerabilities must include a root cause analysis. The analysis may uncover a process that needs to be injected that was overlooked, or fix communication problems that may have led to the vulnerability being present in the application. The goal is to prevent any processes or procedures from occurring again that could introduce vulnerabilities. It is recommended to determine if other production applications were impacted by the process that led to the vulnerability exposure especially in organizations that have a software development process.

An inventory of Third-Party Software Components

Document all third-party software applications. This is similar to the software inventory and includes third-party custom-developed applications. Developers may want to try new frameworks, libraries, or a new version of a programming language for the respective applications.

Document all the libraries or third-party components that are used for particular applications that have been vetted by other team members.

Requiring the use of up-to-date and Trusted Third-Party Software Components

This part of the process requires management support because if a software program that is dependent on a production application will no longer be supported, it may require developing a new product or purchasing a replacement, or using an open-source equivalent.

Include a Severity Rating System and Process for Application Vulnerabilities

The severity rating system would be organization-defined to determine when a software application should be taken offline (namely for public exposed applications), how long is required to update the application, and should be based on the type of data that the application accesses within the organization.

Defining the standard Hardening Configuration Templates for Application Infrastructure

This involves documenting the hardening configurations and the process for determining if the applications have the settings in place. It should be based on the type of application used within the organization.

Secure Design Principles in Application Architectures

Document the secure application architectures used by the organization. OWASP, for example, has an architecture called SAMM.

Document the process for verifying application developers are using the organization-defined secure application architecture.

Implement Code-Level Security Checks

Document the process and applications used to perform security checks of applications to verify it includes all organization-defined safeguards.

Conduct Application Penetration Testing

Document the process and application used to perform application pen-tests.

Document how often the pen-tests are performed.

Document who is authorized to perform pen-tests on applications.

Document the process for security checks prior to deploying the application in production.

Document who has to sign off and verify that pen-tests were performed. It is recommended to require reports to be included along with who performed the test.

Conduct Threat Modeling

Document the process for performing thread modeling. This may include who is involved and at what stage of the software development lifecycle the threat modeling is performed.

Document any frameworks used during the threat modeling process.

Document who has to sign off and verify that threat modeling was performed.

Separate Production and Non-Production Systems

Document how development and production systems are separated. This should include the specific VLAN segment names, firewall rules in place, host-based security systems in place, and methods in which those on the developer network access resources on the production network.

Train Developers in Application Security Concepts and Secure Coding

Document the training that is required for application security developers.

Document how often the training is performed.

Document who is responsible for ensuring application developers attend the requisite security training. It is recommended to require reports to be included along with who performed the test.

CIS Critical Security Control 17: Incident Response and Management

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack. -https://www.cisecurity.org/controls/incident-response-management/

This control deals with ensuring the organization has a process in place to respond to an incident. Incident response (IR) management is virtually required for every organization. A well-developed IR management program goes a long way to mitigating the impact of an incident and that extends to public perception of the incident. It seems that if an organization is offline for any period of time, the first response is that there was a cyber attack. The problem is exacerbated when misinformation begins to spread and the media reports may be difficult for an organization to recover from what really happened because the real extent of the incident may not receive any follow-up press coverage.

Incident response management is required for any organization so that the appropriate processes are in place in case there is an incident that impacts the organization. Some incidents may simply be garden-variety fake AV. Today's headliner is ransomware attack. Regardless of the incident, the appropriate people and processes need to be in place to manage it effectively.

Managing an incident requires training on the IR process. Some organizations may have an IR team, though system administrators may be trained as first responders. They are the ones who may run an IR toolkit to gather initial information and send it to the IR team. They are the ones on call to gather evidence from a system(s) that were impacted. Network administrators are needed to collect evidence from devices such as switches, routers, or network flows. System administrators, however, are essential to understand the process so they are aware of what the IR team will need from them. They are particularly valuable when a third-party IR team comes into the organization to help them understand the IT environment. Helpdesk employees are also valuable because they typically have a lot of institutional knowledge about processes that could aid the investigation. They may have received a call or have been dealing with issues that were symptomatic of an ongoing threat but did not know that was the root cause of those help desk tickets. Customer services employees may have to field calls from customers inquiring if their financial and personal information was impacted or if there will be delays with products they depend on.

Managers are essential so that they can ensure the appropriate number of people are available to help manage the incident and to communicate up to senior executives. It is important that managers relay information correctly so IR teams need to be trained to communicate well to those who do not know the IR or IT lingo that is used between other IR and IT people. That is to ensure the extent and impact of the incident are not watered down.

Public relations people are needed to help get the message out properly to media outlets that are requesting information about the breach. News of the breach, depending on the organization, could make international news. Shareholders and other investors or third parties that interconnect with the affected agency could cause more stress on the organization than is necessary. Other employees need to be trained not to post messages on social media or speak to anyone outside the organization about what happened because rumors may spread quickly.

The legal team may need to be involved if the compromise impacts personal or customer information or a ransom is demanded. Legal will then have to determine what the organization needs to do in order to comply with local, state, and federal laws, or regulatory requirements.

In summary, everyone in the organization needs to be trained in the IR process and understand their role, even if it is only to not discuss the incident outside the organization.

Organizations should prepare for incidents by having tabletop exercises that test the IR response plan. It should be made clear when an IR plan is being tested - to prevent misinformation from spreading.

If an organization does not have an IR team they should locate experienced organizations in their area and contact their local FBI or Secret Service office. The FBI or Secret Service can provide information on steps the organization should take to help with responding to the incident.

What to document:

State of this control [Implemented, Planned, Not in Place, Not Applicable]

Does the organization have an IR response plan?

Does the IT team have the contact information for their local FBI and Secret Service field office?

Does the organization test the IR process?

Are employees trained on how to respond to a security incident?

Designate Personnel to Manage Incident Handling

Document the roles of the IR process and who is responsible for the role.

Establish and Maintain Contact Information for Reporting Security Incidents

Document the contact information for everyone involved in the IR process. The contacts should include law enforcement.

Establish and Maintain an Enterprise Process for Reporting Incidents

Document how incidents are reported.

Document how often employees are reminded of the method to report incidents.

Establish and Maintain an Incident Response Process

Document the IR process. It should include:

1. who is contacted including activating the call tree process
2. how was the event determined to be an incident
3. process based on the device impacted
4. steps to take to identify, contain, eradicate, and the process for the post-incident activity

Assign Key Roles and Responsibilities

Document the roles and their respective responsibilities.

Document the training provided to each person in their respective roles.

Define Mechanisms for Communicating During Incident Response

Document how communication will occur during an incident. This is essential because an organization does not want to tip off the attackers that they are aware of their presence.

Conduct Routine Incident Response Exercises

Document the IR exercise process. The process can be tabletop or the actual steps are carried out except contacting law enforcement.

Conduct Post-Incident Reviews

Document who is involved in post-incident reviews. These reviews are essential so that the organization understands the vector of attack, mitigations, and methods of monitoring to ensure the weakness does not reappear in the organization.

Establish and Maintain Security Incident Thresholds

Document the process the organization takes to determine if an event is a real security incident. This is important because if there is a third party that maintains services in an organization, they may perform the activity without alerting the organization and their activity may trigger alerts or a system administrator performs a vulnerability scan and forgets to tell anyone or scans the wrong LAN segment or hosts.

CIS Critical Security Control 18: Penetration Testing

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker. -https://www.cisecurity.org/controls/penetration-testing/

This control deals with performing security testing that identifies and exploits vulnerabilities within the organization's security boundary. Penetrating Testing (Pen-test) requires a significant amount of knowledge of system administration, networking, security analysis, application security, creativity, and critical thinking. Pen-tests could be performed by someone or a team within the organization (red team), outsourced to a third party, or software applications that can automate the testing. Each one has its advantages and disadvantages.

The red team will likely be a specialized team with knowledge of the devices and software within the organization. Their job is to think like an adversary and determine where vulnerabilities are presented before adversaries do. They also write reports and explain how to mitigate the vulnerabilities found. However, since they know the IT architecture, there may be some bias in their testing or they may overlook some threats. Working as a team and alternating roles could help mitigate the bias.

Outsourcing to a third party requires coordinating when the attack will occur. It also requires having a few people on standby to call and cease the testing if it significantly impacts production. The third-party may also exfiltrate data from the organization so there will need to be agreements in place that the data will be protected and securely destroyed when the assessment is complete. However, they have the advantage of not knowing the IT architecture so may find vulnerabilities that were overlooked by someone with familiarity with it.

A security analysis may take the approach of emulating a specific threat actor that is known to target the organizations in a given industry. They can then plan the test and replicate their actions. The replication will often come from threat intelligence sources of the known behavior of the adversary. Minimum, this helps the analyst know if their existing defenses can help mitigate and detect the attacks. The threat emulation is scaled down from a thorough pen-test but provides useful insight when planned carefully and the emulation accurately repeats an adversaries activities.

Automation using software applications will require a significant amount of knowledge about its platform to understand the extent and how aggressive it will test system and applications. There also needs to be a clear understanding of how to stop the automated pen-testing if necessary. However, it provides the benefit of performing well-known attacks and can also emulate the behavior of known threat actors.

Pen-tests are worthwhile investments. Selecting the best approach will be an organizational decision or it may be required to have a third-party based on industry regulations. A pen-test must include physical testing as well. Someone’s job may be a lot easier if they can walk into a computer room and begin typing commands on an unlocked server or workstation or gain access to other sensitive areas such as sitting in on meetings where intellectual property-related discussions are going on. Organizations should plan to conduct a thorough pen-test at least once a year. Though, organizations should also take action to mitigate the vulnerabilities found and not just have a pen-test performed for the sake of ‘compliance.’

What to document:

State of this control [Implemented, Planned, Not in Place, Not Applicable]

Does the organization have a pen-test program?

Does the organization perform internal pen-tests?

Establish and Maintain a Penetration Testing Program

Document the pen-test program process and procedures. The document should include who is involved in the planning of the pen-test and their roles. The training for each person based on their role should also be documented.

Perform Periodic External and Internal Penetration Tests

Document how often external pen-tests occur for the organization.

Document how often the pen-tests occur within the organization. Check any regulatory compliances within your respective industry as a baseline.

Remediate Penetration Test Findings and Validate Security Measures

Document the process for reviewing and the people involved with determining the plan of action for remediating the findings.

The documentation should include the plan for fixing the vulnerabilities and creating a test plan to validate the security controls in place work to mitigate the findings.

Creating an SSP: Final Thoughts

An SSP is a document that provides details on the security implementation within your organization. There are many more controls than the 18 identified by the CIS Critical Security Controls. However, it is a good starting point to better understand your organizational processes and identify the most common weaknesses that may exist within your organization.

I would suggest testing your controls periodically. If you are having a slow day then test one, two, or three controls and document the date, results, and method of testing the control so that it is repeatable. If you receive an alert from a security control implementation, then that is a test because it is demonstrating that it is in place and working as expected. Make a note of one of the times you were alerted. If there is a new project being developed or a plan to bring in new devices, then consult the SSP to see potential impacts and plan for how it is going to be tested before the project rolls out or the product is onsite. The SSP is a "living" document that should be consulted often and updated with control tests or changes to the organizational security requirements.