CIS Controls v8.1 - IG3

Policies and Procedures

CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Prepared for: Client Company

Prepared by: YourIT Company

Table of Contents

Purpose

Implementation Groups (IGs) are the recommended guidance to prioritize implementation of the CIS Critical Security Controls (CIS Controls)

Scope

"IG3 is comprised of an additional 23 Safeguards. It builds upon the Safeguards identified in IG1 (56) and IG2 (74) totaling the 153 Safeguards in CIS Controls v8.

An IG3 enterprise commonly employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight. An IG3 enterprise must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare.

Safeguards selected for IG3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks."

Sanctions/Compliance

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

CIS Control 01 - Inventory and Control of Enterprise Assets

CIS Controls v8.1 - IG3 CIS Control 01 Inventory and Control of Enterprise Assets	**Other Requirements** N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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.

Guidance
Enterprises cannot defend what they do not know they have. Managed control of all enterprise assets also plays a critical role in security monitoring, incident response, system backup, and recovery. Enterprises should know what data is critical to them (CIS Control 3), and proper asset management will help identify those enterprise assets that hold or manage this critical data, so that appropriate security controls can be applied.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CIS1.1 - Establish and Maintain Detailed Enterprise Asset Inventory: Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.

- CIS1.2 - Address Unauthorized Assets: Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.

- CIS1.3 - Utilize an Active Discovery Tool: Utilize an active discovery tool to identify assets connected to the enterprise’s network. Configure the active discovery tool to execute daily, or more frequently.

- CIS1.4 - Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory: Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise’s asset inventory. Review and use logs to update the enterprise’s asset inventory weekly, or more frequently.

- CIS1.5 - Use a Passive Asset Discovery Tool: Use a passive discovery tool to identify assets connected to the enterprise’s network. Review and use scans to update the enterprise’s asset inventory at least weekly, or more frequently.

References

- CIS Controls Cloud Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-cloud-companion-guide
- CIS Critical Security Controls v8 Mobile Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mobile-companion-guide
- CIS Controls v8 Internet of Things Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-internet-of-things-companion-guide

CIS Control 02 - Inventory and Control of Software Assets

CIS Controls v8.1 - IG3 CIS Control 02 Inventory and Control of Software Assets	**Other Requirements** N/A

Policy

The organization will implement internal controls to satisfy the following requirement:

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.

Guidance

A complete software inventory is a critical foundation for preventing attacks. Attackers continuously scan target enterprises looking for vulnerable versions of software that can be remotely exploited. For example, if a user opens a malicious website or attachment with a vulnerable browser, an attacker can often install backdoor programs and bots that give the attacker long-term control of the system. Attackers can also use this access to move laterally through the network. One of the key defenses against these attacks is updating and patching software (CIS Control 7). However, without a complete inventory of software assets, an enterprise cannot determine if they have vulnerable software, or if there are potential licensing violations.

Responsibilities

The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CIS2.1 - Establish and Maintain a Software Inventory: Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, decommission date, and number of licenses. Review and update the software inventory bi-annually, or more frequently.

- CIS2.2 - Ensure Authorized Software is Currently Supported : Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise’s mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.

- CIS2.3 - Address Unauthorized Software: Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.

- CIS2.4 - Utilize Automated Software Inventory Tools: Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.

- CIS2.5 - Allowlist Authorized Software: Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.

- CIS2.6 - Allowlist Authorized Libraries: Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, and .so files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.

- CIS2.7 - Allowlist Authorized Scripts: Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, and .py files are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.

References

- CIS Controls Cloud Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-cloud-companion-guide
- CIS Critical Security Controls v8 Mobile Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mobile-companion-guide
- CIS Controls v8 Internet of Things Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-internet-of-things-companion-guide

CIS Control 03 - Data Protection

CIS Controls v8.1 - IG3	**Other Requirements**
CIS Control 03 Data Protection	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

Guidance
Data is no longer only contained within an enterprise's border; it is in the cloud, on portable end-user devices where users work from home, and is often shared with partners or online services that might have it anywhere in the world. In addition to sensitive data an enterprise holds related to finances, intellectual property, and customer data, there also might be numerous international regulations for protection of personal data. Data privacy has become increasingly important, and enterprises are learning that privacy is about the appropriate use and management of data, not just encryption. Data must be appropriately managed through its entire life cycle. These privacy rules can be complicated for multi-national enterprises of any size; however, there are fundamentals that can apply to all.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CIS3.1 - Establish and Maintain a Data Management Process: Establish and maintain a documented data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS3.2 - Establish and Maintain a Data Inventory: Establish and maintain a data inventory based on the enterprise’s data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.

- CIS3.3 - Configure Data Access Control Lists: Configure data access control lists based on a user’s need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.

- CIS3.4 - Enforce Data Retention: Retain data according to the enterprise’s documented data management process. Data retention must include both minimum and maximum timelines.

- CIS3.5 - Securely Dispose of Data: Securely dispose of data as outlined in the enterprise’s documented data management process. Ensure the disposal process and method are commensurate with the data sensitivity.

- CIS3.6 - Encrypt Data on End-User Devices: Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.

- CIS3.7 - Establish and Maintain a Data Classification Scheme: Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS3.8 - Document Data Flows: Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise’s data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS3.9 - Encrypt Data on Removable Media: Encrypt data on removable media.

- CIS3.10 - Encrypt Sensitive Data in Transit: Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).

- CIS3.11 - Encrypt Sensitive Data at Rest: Encrypt sensitive data at rest on servers, applications, and databases. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.

- CIS3.12 - Segment Data Processing and Storage Based on Sensitivity: Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.

- CIS3.13 - Deploy a Data Loss Prevention Solution: Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's data inventory.

- CIS3.14 - Log Sensitive Data Access: Log sensitive data access, including modification and disposal.

References

- CIS Controls Cloud Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-cloud-companion-guide
- CIS Critical Security Controls v8 Mobile Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mobile-companion-guide
- CIS Controls v8 Internet of Things Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-internet-of-things-companion-guide

CIS Control 04 - Secure Configuration of Enterprise Assets and Software

CIS Controls v8.1 - IG3	**Other Requirements**
CIS Control 04 Secure Configuration of Enterprise Assets and Software	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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).

Guidance
As delivered from manufacturers and resellers, the default configurations for enterprise assets and software are normally geared towards ease-of-deployment and ease-of-use, rather than security. Basic controls, open services and ports, default accounts or passwords, pre-configured Domain Name System (DNS) settings, older (vulnerable) protocols, and pre installation of unnecessary software can all be exploitable if left in their default state. Further, these security configuration updates need to be managed and maintained over the life cycle of enterprise assets and software. Configuration updates need to be tracked and approved through configuration management workflow process to maintain a record that can be reviewed for compliance, leveraged for incident response, and to support audits. This CIS Control is important to on-premises devices, as well as remote devices, network devices, and cloud environments.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CIS4.1 - Establish and Maintain a Secure Configuration Process: Establish and maintain a documented secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS4.2 - Establish and Maintain a Secure Configuration Process for Network Infrastructure: Establish and maintain a documented secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS4.3 - Configure Automatic Session Locking on Enterprise Assets: Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.

- CIS4.4 - Implement and Manage a Firewall on Servers: Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.

- CIS4.5 - Implement and Manage a Firewall on End-User Devices: Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

- CIS4.6 - Securely Manage Enterprise Assets and Software: Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled Infrastructure-as-Code (IaC) and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.

- CIS4.7 - Manage Default Accounts on Enterprise Assets and Software: Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.

- CIS4.8 - Uninstall or Disable Unnecessary Services on Enterprise Assets and Software: Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.

- CIS4.9 - Configure Trusted DNS Servers on Enterprise Assets: Configure trusted DNS servers on network infrastructure. Example implementations include configuring network devices to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.

- CIS4.10 - Enforce Automatic Device Lockout on Portable End-User Devices: Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft (Registered Trademark) InTune Device Lock and Apple (Registered Trademark) Configuration Profile maxFailedAttempts.

- CIS4.11 - Enforce Remote Wipe Capability on Portable End-User Devices: Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.

- CIS4.12 - Separate Enterprise Workspaces on Mobile End-User Devices: Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.

References

- CIS Controls Cloud Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-cloud-companion-guide
- CIS Critical Security Controls v8 Mobile Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mobile-companion-guide
- CIS Controls v8 Internet of Things Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-internet-of-things-companion-guide

CIS Control 05 - Account Management

CIS Controls v8.1 - IG3 CIS Control 05 Account Management	**Other Requirements** N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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.

Guidance
It is easier for an external or internal threat actor to gain unauthorized access to enterprise assets or data through using valid user credentials than through hacking the environment. There are many ways to covertly obtain access to user accounts, including: weak passwords, accounts still valid after a user leaves the enterprise, dormant or lingering test accounts, shared accounts that have not been changed in months or years, service accounts embedded in applications for scripts, a user having the same password as one they use for an online account that has been compromised (in a public password dump), using social engineering techniques to obtain a password, or using malware to capture passwords or tokens in memory or over the network. Defenders need to ensure that controls are in place to protect enterprise accounts, especially those with higher privileges.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CIS5.1 - Establish and Maintain an Inventory of Accounts: Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must at a minimum include user, administrator accounts, and service accounts. The inventory, at a minimum, should contain the person’s name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

- CIS5.2 - Use Unique Passwords: Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using Multi-Factor Authentication (MFA) and a 14-character password for accounts not using MFA.

- CIS5.3 - Disable Dormant Accounts: Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.

- CIS5.4 - Restrict Administrator Privileges to Dedicated Administrator Accounts: Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user’s primary, non-privileged account.

- CIS5.5 - Establish and Maintain an Inventory of Service Accounts: Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

- CIS5.6 - Centralize Account Management: Centralize account management through a directory or identity service.

References

- CIS Controls Cloud Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-cloud-companion-guide
- CIS Critical Security Controls v8 Mobile Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mobile-companion-guide
- CIS Controls v8 Internet of Things Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-internet-of-things-companion-guide

CIS Control 06 - Access Control Management

CIS Controls v8.1 - IG3	**Other Requirements**
CIS Control 06 Access Control Management	N/A

Policy

The organization will implement internal controls to satisfy the following requirement:

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.

Guidance

Where CIS Control 5 deals specifically with account management, CIS Control 6 focuses on managing what access these accounts have, ensuring users only have access to the data or enterprise assets appropriate for their role, and ensuring that there is strong authentication for critical or sensitive enterprise data or functions. Attackers will compromise any account that will grant them access to a network, especially administrator accounts that have elevated privileges. Accounts should only have the minimal authorization needed for the role. Developing consistent access rights for each role and assigning roles to users is a best practice. Developing a program for complete provision and de-provisioning access is also important. Centralizing this function is ideal.

Responsibilities

The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CIS6.1 - Establish an Access Granting Process: Establish and follow a documented process, preferably automated, for granting access to enterprise assets upon new hire or role change of a user.

- CIS6.2 - Establish an Access Revoking Process: Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.

- CIS6.3 - Require MFA for Externally-Exposed Applications: Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.

- CIS6.4 - Require MFA for Remote Network Access: Require MFA for remote network access.

- CIS6.5 - Require MFA for Administrative Access: Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a service provider.

- CIS6.6 - Establish and Maintain an Inventory of Authentication and Authorization Systems: Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.

- CIS6.7 - Centralize Access Control: Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.

- CIS6.8 - Define and Maintain Role-Based Access Control: Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.

References

- CIS Controls Cloud Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-cloud-companion-guide
- CIS Critical Security Controls v8 Mobile Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mobile-companion-guide
- CIS Controls v8 Internet of Things Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-internet-of-things-companion-guide

CIS Control 07 - Continuous Vulnerability Management

CIS Controls v8.1 - IG3 CIS Control 07 Continuous Vulnerability Management	**Other Requirements** N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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.

Guidance
Thousands of vulnerabilities are published each year, with several more that are unknown. Cyber defenders are constantly being challenged from attackers who are looking for vulnerabilities within their infrastructure to exploit and gain access. Defenders must have timely threat information available to them about: software updates, patches, security advisories, threat bulletins, etc., and they should regularly review their environment to identify these vulnerabilities before the attackers do. Understanding and managing vulnerabilities is a continuous activity, requiring focus of time, attention, and resources.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CIS7.1 - Establish and Maintain a Vulnerability Management Process: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS7.2 - Establish and Maintain a Remediation Process: Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.

- CIS7.3 - Perform Automated Operating System Patch Management: Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

- CIS7.4 - Perform Automated Application Patch Management: Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

- CIS7.5 - Perform Automated Vulnerability Scans of Internal Enterprise Assets: Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans.

- CIS7.6 - Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets: Perform automated vulnerability scans of externally-exposed enterprise assets. Perform scans on a monthly, or more frequent, basis.

- CIS7.7 - Remediate Detected Vulnerabilities: Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.

References

- CIS Controls Cloud Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-cloud-companion-guide
- CIS Critical Security Controls v8 Mobile Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mobile-companion-guide
- CIS Controls v8 Internet of Things Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-internet-of-things-companion-guide

CIS Control 08 - Audit Log Management

CIS Controls v8.1 - IG3	**Other Requirements**
CIS Control 08 Audit Log Management	N/A

Policy

The organization will implement internal controls to satisfy the following requirement:

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

Guidance

Log collection and analysis is important for an enterprise's ability to detect malicious activity quickly. Sometimes audit records are the only evidence of a successful attack. Attackers know that many enterprises keep audit logs for compliance purposes, but rarely analyze them. They know there's very little risk of being exposed through the audit logs if the logs are never analyzed. As a result, attackers use this knowledge to hide their location, malicious software, and activities on victim machines. Due to poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target enterprise knowing. Logging records are critical for incident response. After an attack has been detected, log analysis can help enterprises understand the extent of an attack.

Responsibilities

The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CIS8.1 - Establish and Maintain an Audit Log Management Process: Establish and maintain a documented audit log management process that defines the enterprise’s logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS8.2 - Collect Audit Logs: Collect audit logs. Ensure that logging, per the enterprise’s audit log management process, has been enabled across enterprise assets.

- CIS8.3 - Ensure Adequate Audit Log Storage: Ensure that logging destinations maintain adequate storage to comply with the enterprise’s audit log management process.

- CIS8.4 - Standardize Time Synchronization: Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.

- CIS8.5 - Collect Detailed Audit Logs: Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.

- CIS8.6 - Collect DNS Query Audit Logs: Collect DNS query audit logs on enterprise assets, where appropriate and supported.

- CIS8.7 - Collect URL Request Audit Logs: Collect URL request audit logs on enterprise assets, where appropriate and supported.

- CIS8.8 - Collect Command-Line Audit Logs: Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.

- CIS8.9 - Centralize Audit Logs: Centralize, to the extent possible, audit log collection and retention across enterprise assets in accordance with the documented audit log management process. Example implementations include leveraging a SIEM tool to centralize multiple log sources.

- CIS8.10 - Retain Audit Logs: Retain audit logs across enterprise assets for a minimum of 90 days.

- CIS8.11 - Conduct Audit Log Reviews: Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.

- CIS8.12 - Collect Service Provider Logs: Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events.

References

- CIS Controls Cloud Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-cloud-companion-guide
- CIS Critical Security Controls v8 Mobile Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mobile-companion-guide
- CIS Controls v8 Internet of Things Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-internet-of-things-companion-guide

Truncated Sample Document