SYNERCOMM
SECURE • INTELLIGENT • NETWORKS

CIS Top 20 #16

Account Monitoring and Control

Lisa Niles: CISSP, Director of Solutions Integration

CIS Top 20 Critical Security Controls

CSC # 16

Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.

CIS Top 20 Critical Security Controls

Why Is This Control Critical?

CIS Controls™

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

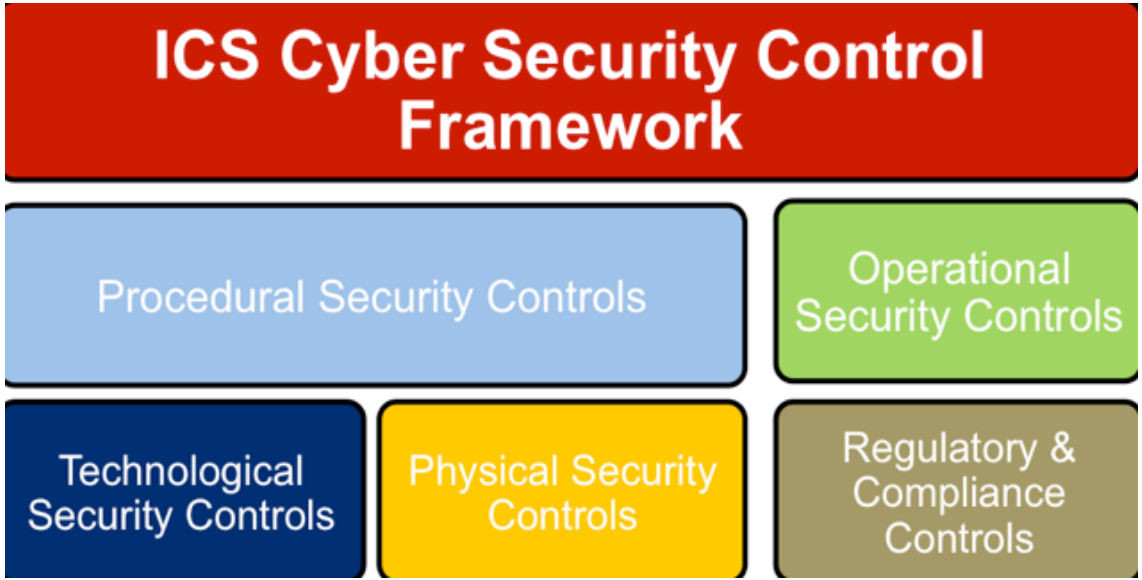
Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Understanding the Control types



CIS Top 20 Critical Security Controls

- 1ST AND FOREMOST
- Account and Identity Management are key security controls and the good processes and procedures are crucial

Account Lifecycle Management

Configuration settings

Two-factor authentication

CIS Top 20 Critical Security Controls

- Key Takeaways from Control 20
  - Don’t forget the logs
  - Missing password requirements
  - Block common attacks

CIS Top 20 Critical Security Controls

- Many organizations fail to perform pen tests for many reasons, mainly out of fear

CIS Top 20 Critical Security Controls

How to Get Started

Step 1. Gap Assessment.

2. Implementation Roadmap
3. Implement the First Phase of Controls
4. Integrate Controls into Operations
5. Report and Manage Progress

CIS Top 20 Critical Security Controls CSC # 18

- Sample Gap questions

1. Does a baseline of users who need access to an information system exist for each system?
2. Is each user account configured to access only the systems necessary to perform their job requirements?
3. Has each user account been properly authorized according to the organization's authorization standards?
4. Do business owners validate the user accounts under their responsibility on a regular basis?
5. Does an automated process exist for comparing the baseline of user accounts to the accounts configured on each system?

CIS Top 20 Critical Security Controls

16.1	Review all system accounts and disable any account that cannot be associated with a business process and owner.
16.2	Ensure that all accounts have an expiration date that is monitored and enforced.
16.3	Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor. Disabling instead of deleting accounts allows preservation of audit trails.
16.4	Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.
16.5	Configure screen locks on systems to limit access to unattended workstations.
16.6	Monitor account usage to determine dormant accounts, notifying the user or user's manager. Disable such accounts if not needed, or document and monitor exceptions (e.g., vendor maintenance accounts needed for system recovery or continuity operations). Require that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators should then disable accounts that are not assigned to valid workforce members.
16.7	Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time.
16.8	Monitor attempts to access deactivated accounts through audit logging.
16.9	Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.
16.10	Profile each user's typical account usage by determining normal time-of-day access and access duration. Reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration. This includes flagging the use of the user's credentials from a computer other than computers on which the user generally works.
16.11	Require multi-factor authentication for all user accounts that have access to sensitive data or systems. Multi-factor authentication can be achieved using smart cards, certificates, One Time Password (OTP) tokens, or biometrics.
16.12	Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).
16.13	Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.
16.14	Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

CIS Top 20 Critical Security Controls

- *16-1* - Review all system accounts and disable any account that cannot be associated with a business process and owner.

- Free Tools
  - AD Info Free - Set very specific filters for AD objects, and report on them in amazing detail.
  - Event Logs - If you want to pass event logs off to a SIEM
  - Thycotic, Centrify, CyberArk, Beyond Trust, SCCM
- Commercial Tools
  - AD Audit Plus - Real-time auditing of all things Active Directory

CIS Top 20 Critical Security Controls

- *16-2* - Ensure that all accounts have an expiration date that is monitored and enforced.
- Tools
  - This is more of a process than a tool

CIS Top 20 Critical Security Controls

- *16-3* - Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor. Disabling instead of deleting accounts allows preservation of audit trails
- **Tools**
  - AD Info Free - Although the automation part is only available in the standard edition.
  - Powershell - disabled accounts
  - Powershell - password exceeds max age (and other commands)
  - Powershell - passwords that never expire

CIS Top 20 Critical Security Controls

- *16-4* - Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

- Tools
  - This is more of a process than a tool. Just remember to get all the accounts a user had access to, not just AD

CIS Top 20 Critical Security Controls

- *16-5* - Configure screen locks on systems to limit access to unattended workstations.

- **Tools**
  - Linux - Shell, X sessions, and TTYs
  - GPO - several methods depending on the situation

CIS Top 20 Critical Security Controls

- *16-6* - Monitor account usage to determine dormant accounts, notifying the user or user's manager. Disable such accounts if not needed, or document and monitor exceptions (e.g., vendor maintenance accounts needed for system recovery or continuity operations). Require that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators should then disable accounts that are not assigned to valid workforce members
- **Free Tools**
  - Inactive User Tracking - by Netwrix, auto build and send reports via email
  - Powershell - You will have to automate the report notifications

CIS Top 20 Critical Security Controls

- *16-7* - Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time.
- **Free Tools**
  - GPO - configure account lockout policies
  - Troubleshoot locked accounts - Troubleshoot where account lockouts are coming from

CIS Top 20 Critical Security Controls

- *16-8* - Monitor attempts to access deactivated accounts through audit logging.

- Tools:
  - This is facilitated by enabling and collecting audit logs on servers and endpoints. Your SIEM needs to be able to correlate login attempts to deactivated accounts, so an integration into your Active Directory or LDAP will be critical to making this easy for you.

CIS Top 20 Critical Security Controls

- *16-9* – Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.
- **Free Tools**
  - 389 Directory - Open Source LDAP server based on Fedora Linux
  - Apache DS - Directory server written in Java
  - Oracle Internet Directory - Oracles implementation, based on LDAP v3
- Commercial Tools:
  - Centrify

CIS Top 20 Critical Security Controls

- *16-10* – Profile each user's typical account usage by determining normal time-of-day access and access duration. Reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration. This includes flagging the use of the user's credentials from a computer other than computers on which the user generally works.
- **Commercial Tools**
  - ADAudit Plus - Real-Time Monitoring of User Logon Actions with alerting and reporting

CIS Top 20 Critical Security Controls

- *16-11 –* Require multi-factor authentication for all user accounts that have access to sensitive data or systems. Multi-factor authentication can be achieved using smart cards, certificates, One Time Password (OTP) tokens, or biometrics.
- Tools
  - Centrify
  - Beyond Trust
  - Okta

CIS Top 20 Critical Security Controls

- *16-12* – Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).
- **Free Tools**
  - Fine-Grained Password Policies - specify multiple password policies within a single domain. You can use fine-grained password policies to apply different restrictions for password and account lockout policies to different sets of users in a domain.
  - CISSecurity.org - Best Practices for effective password policies

CIS Top 20 Critical Security Controls

- *16-13* – Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.
- **Free Tools**
  - **Notes**: Everything going across the network should be encrypted, especially credentials. Using a packet capturing tool, system administrators can quickly identify if credentials are being sent in the clear over the network.

CIS Top 20 Critical Security Controls

- *16-14* – Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.
- Free Tool
  - GPO - How to prevent Windows from storing a LAN manager hash of your password in Active Directory and local SAM databases

CIS Top 20 Critical Security Controls

CIS Top 20 Critical Security Controls

Thank you for Attending.