

CIS Top - 20 Critical Security Controls (V 7.0)

Basic

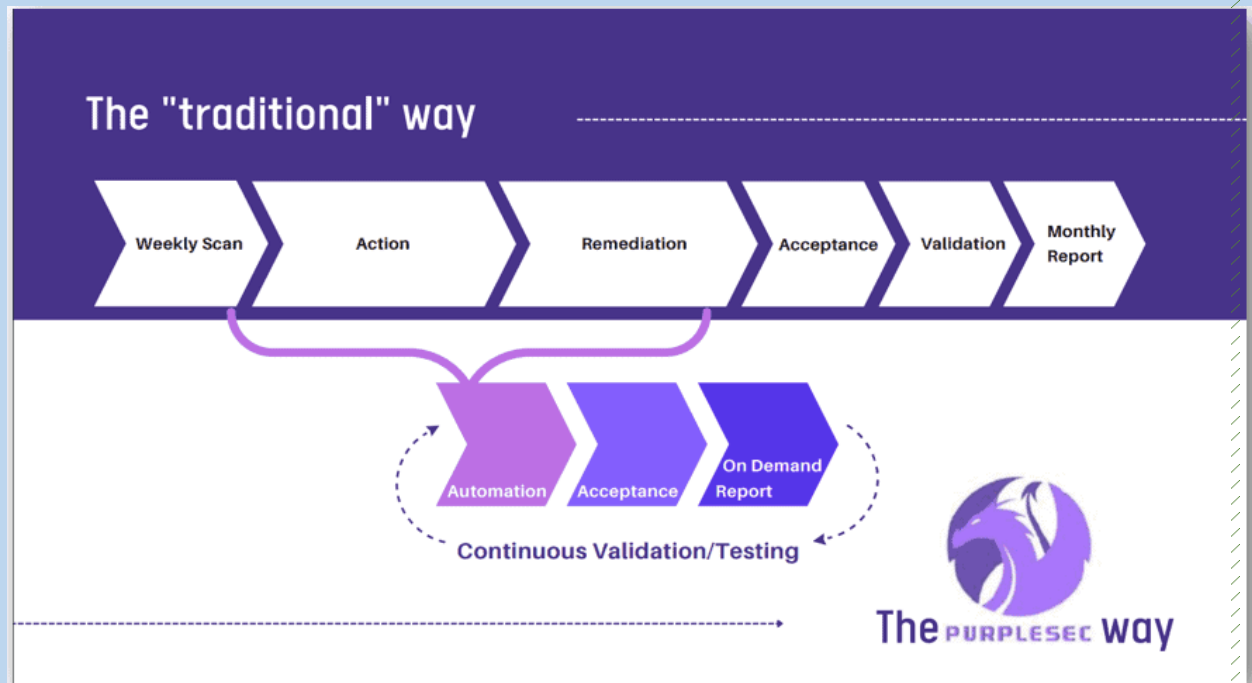
1. Inventory and Control of Hardware Assets: Maintain an up-to-date list of all hardware assets in your organization's network to track and manage them effectively. Example: Using asset management software to track computers, servers, and network devices.



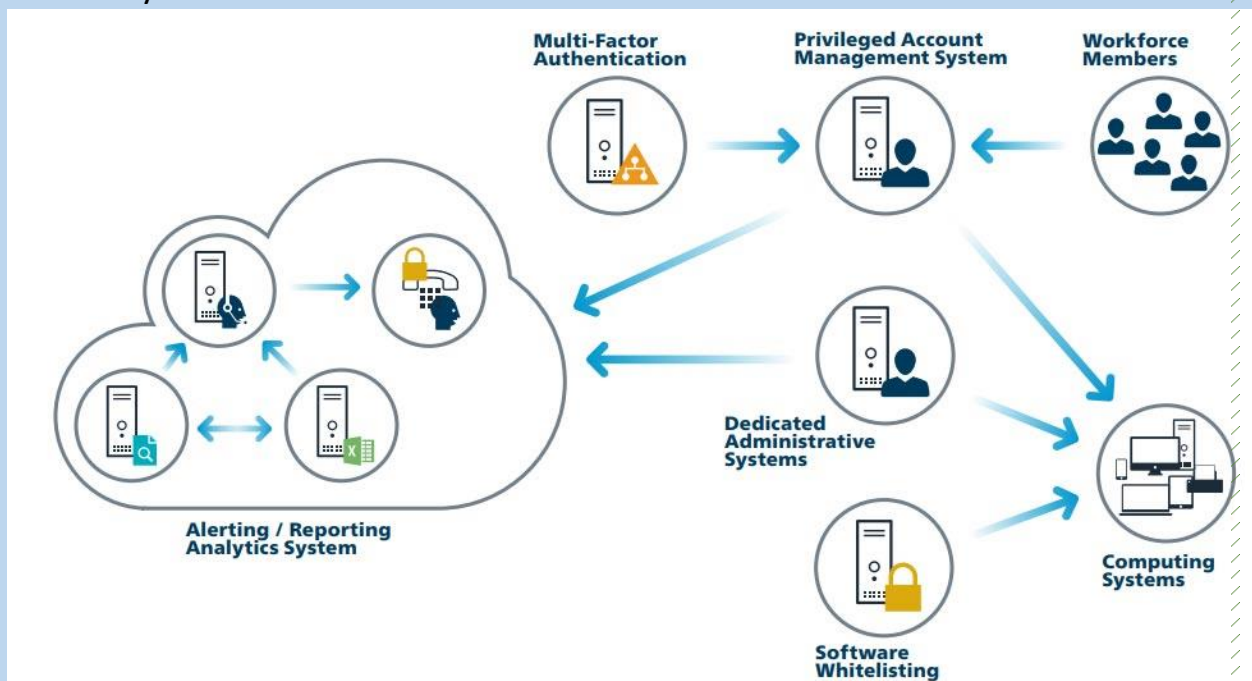
2. Inventory and Control of Software Assets: Keep a comprehensive inventory of all software used in your organization to ensure proper licensing and security patching. Example: Using software inventory tools to track applications and their versions.



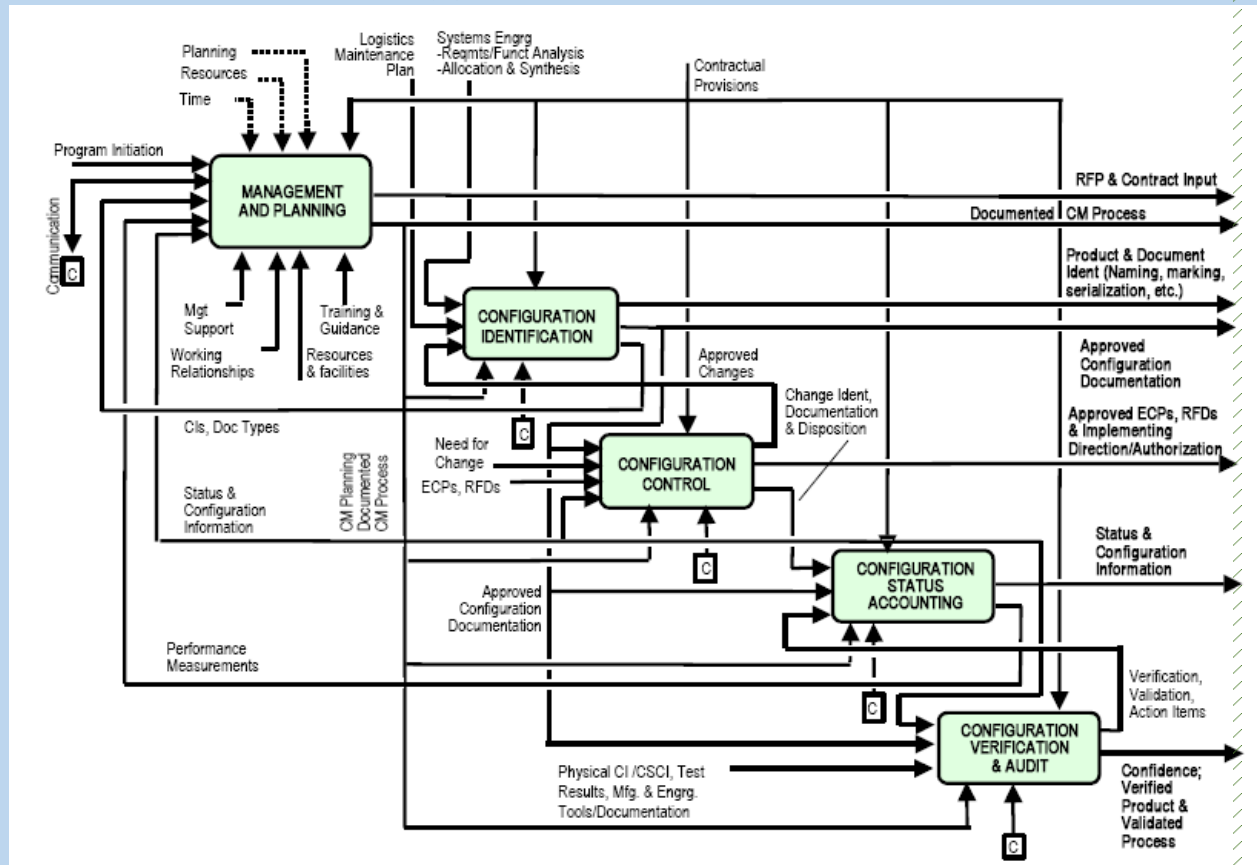
3. Continuous Vulnerability Management: Regularly scan and assess systems for vulnerabilities to identify and address security weaknesses promptly. Example: Conducting weekly vulnerability scans and promptly patching critical vulnerabilities.



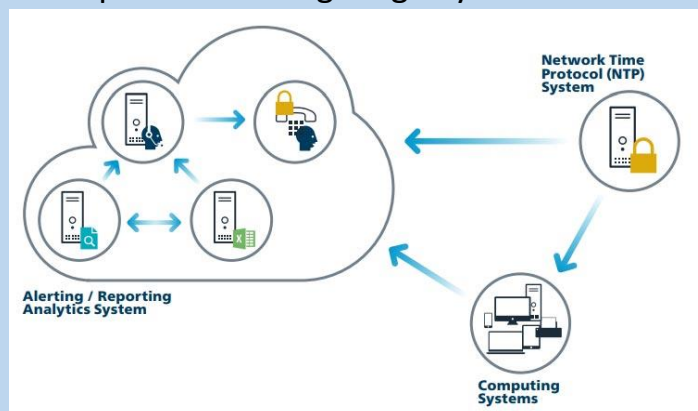
4. **Controlled Use of Administrative Privileges:** Limit access to administrative privileges to authorized personnel only, reducing the risk of unauthorized system changes. Example: Implementing the principle of least privilege, where administrators only have the minimum privileges necessary for their tasks.



5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers: Apply security best practices to configure hardware and software securely, reducing attack surface. Example: Configuring firewalls and intrusion detection systems on servers to block unnecessary ports and services.

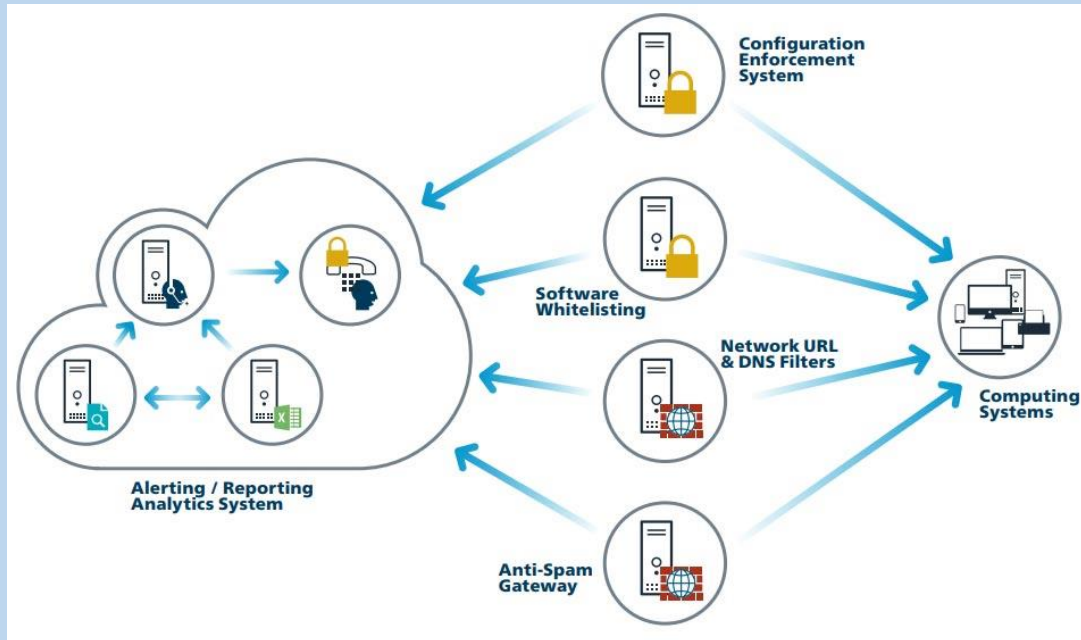


6. Maintenance, Monitoring, and Analysis of Audit Logs: Regularly review and analyze audit logs to detect and respond to potential security incidents. Example: Monitoring log files for unauthorized access attempts and investigating any unusual activities.

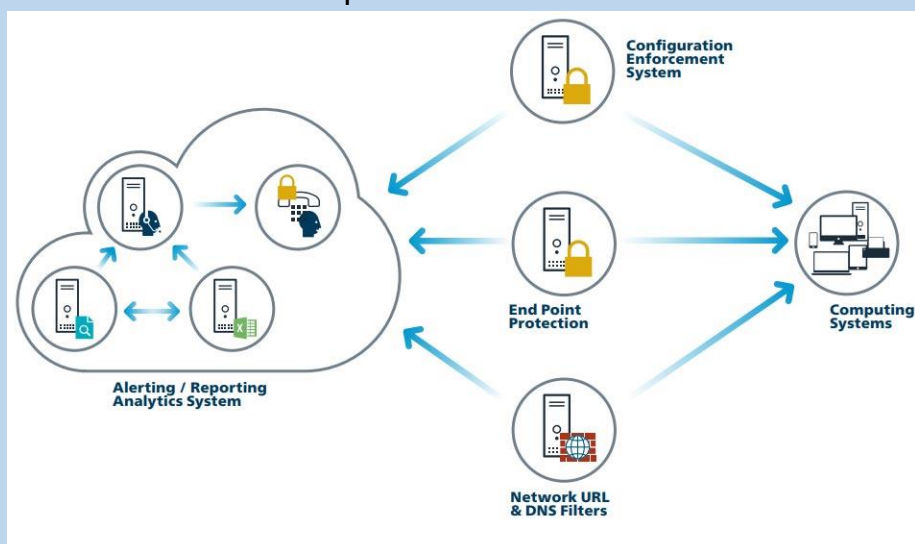


Foundational

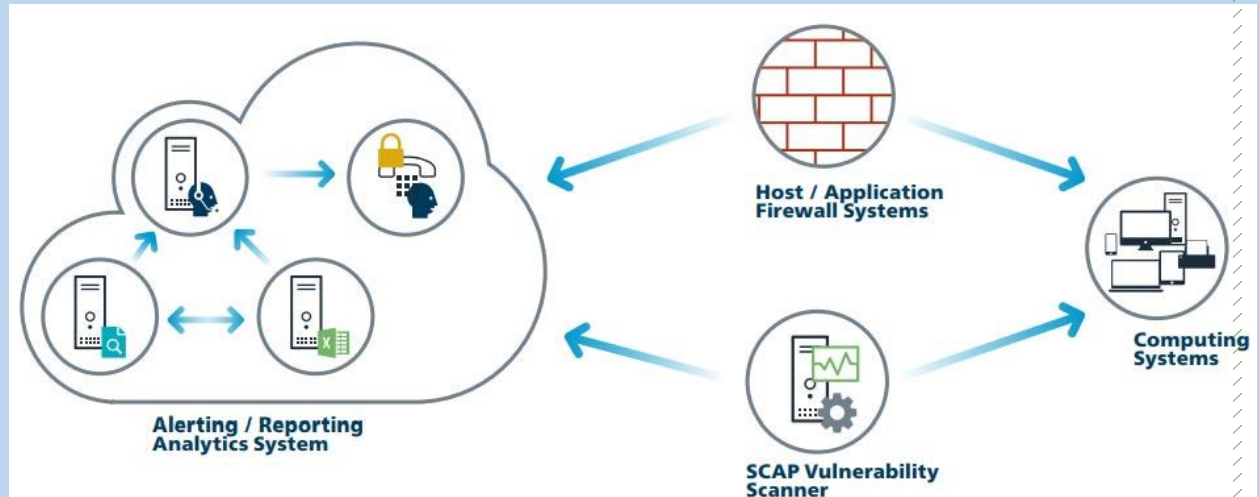
7. Email and Web Browser Protections: Implement security measures to protect against email and web-based threats, such as phishing and malicious attachments. Example: Using email filtering to block malicious attachments and links.



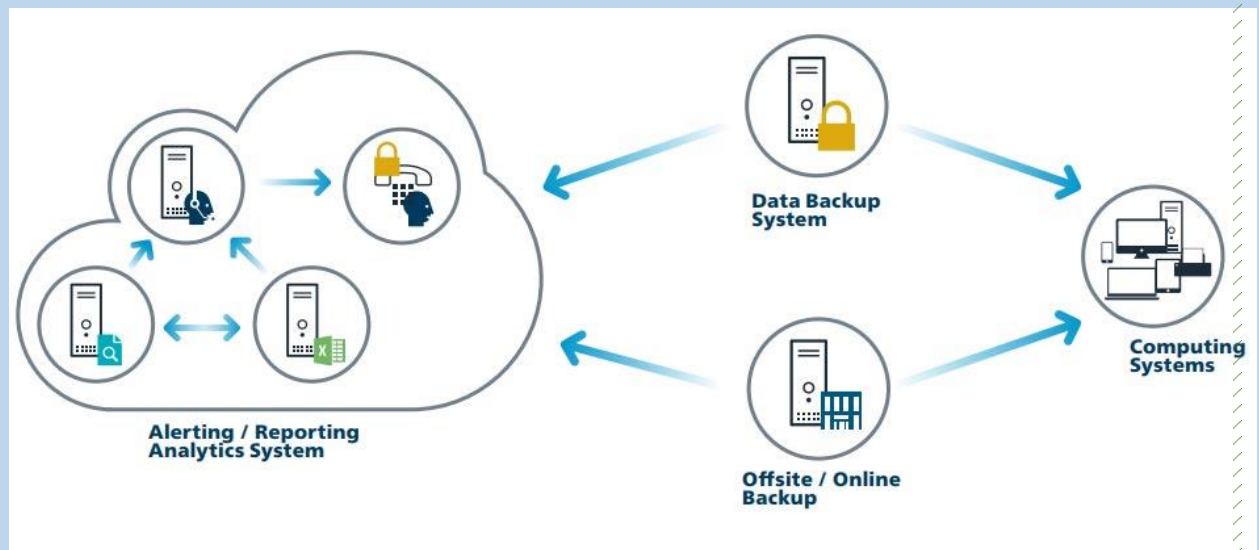
8. Malware Defenses: Deploy antivirus and anti-malware solutions to detect and mitigate malware infections. Example: Running real-time malware scans on endpoints to detect and remove malicious software.



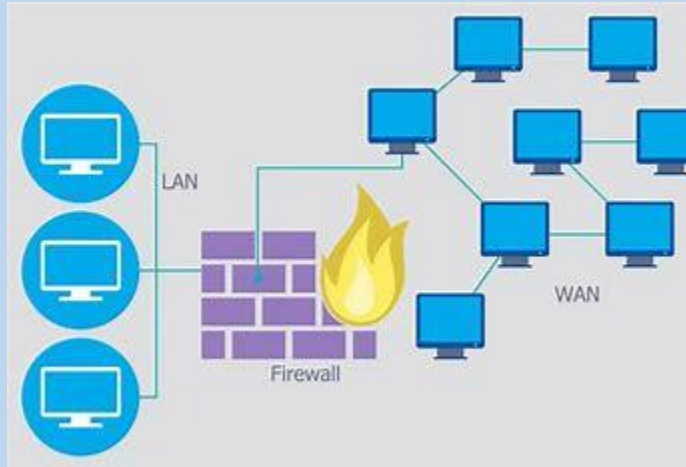
9. Limitation and Control of Network Ports, Protocols, and Services: Disable unnecessary network ports, protocols, and services to reduce the attack surface and limit potential vulnerabilities. Example: Disabling unused and insecure protocols like Telnet and SMBv1.



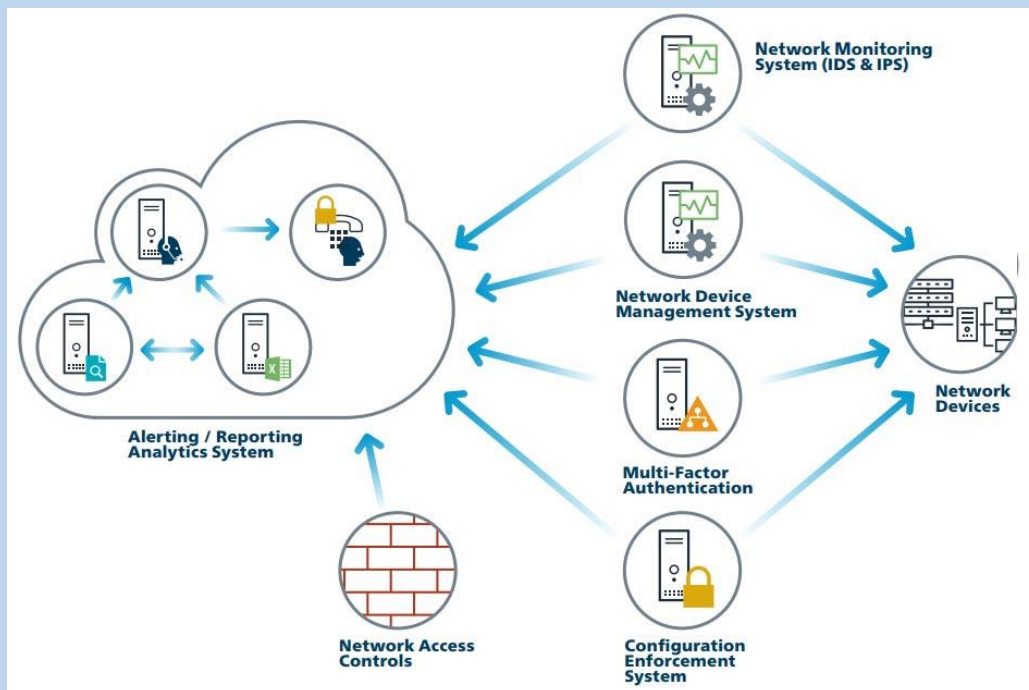
10. Data Recovery Capabilities: Establish mechanisms for data backup and recovery to ensure data integrity and availability in case of data loss or breaches. Example: Regularly backing up critical data to an off-site location.



11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches: Apply secure configurations to network devices to prevent unauthorized access and ensure proper network segmentation. Example: Configuring firewalls to only allow essential traffic and blocking all other incoming requests.




















12. **Boundary Defense:** Implement security controls at network boundaries to protect against external threats. Example: Deploying intrusion detection systems and intrusion prevention systems to monitor and block malicious traffic.

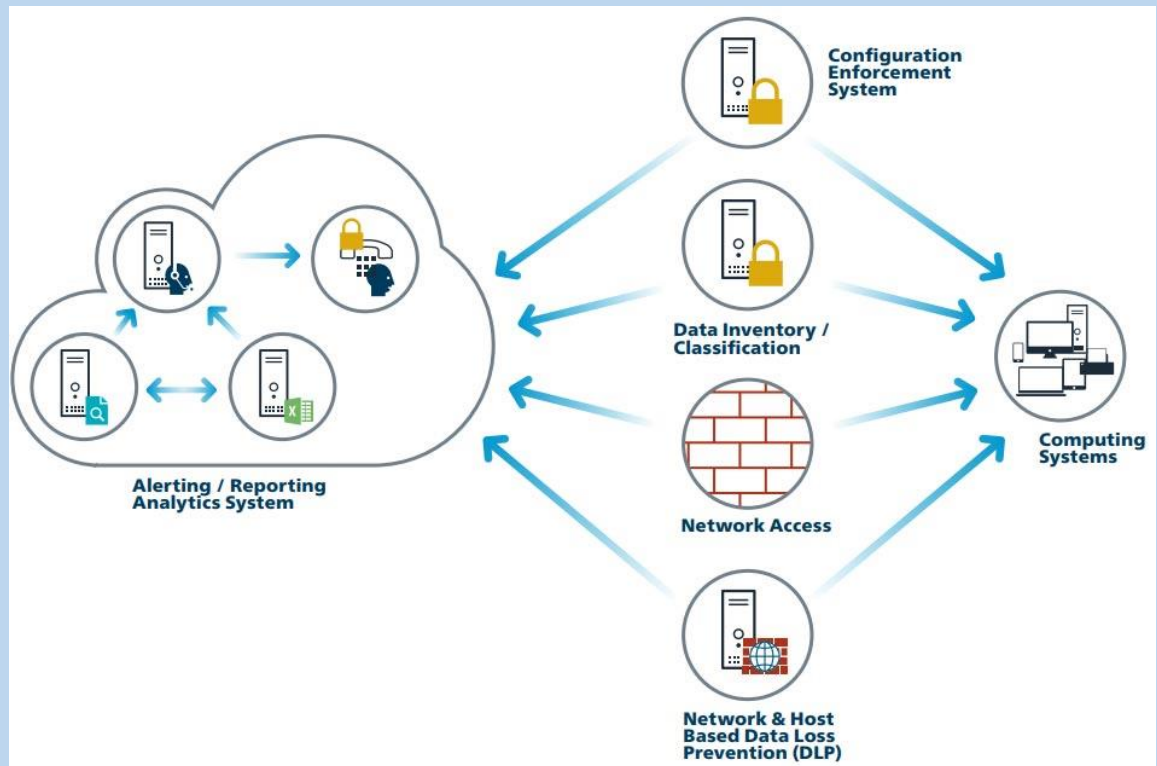


13. **Data Protection:** Implement encryption and access controls to safeguard sensitive data from unauthorized access and disclosure. Example: Encrypting sensitive data at rest and in transit using strong encryption algorithms.

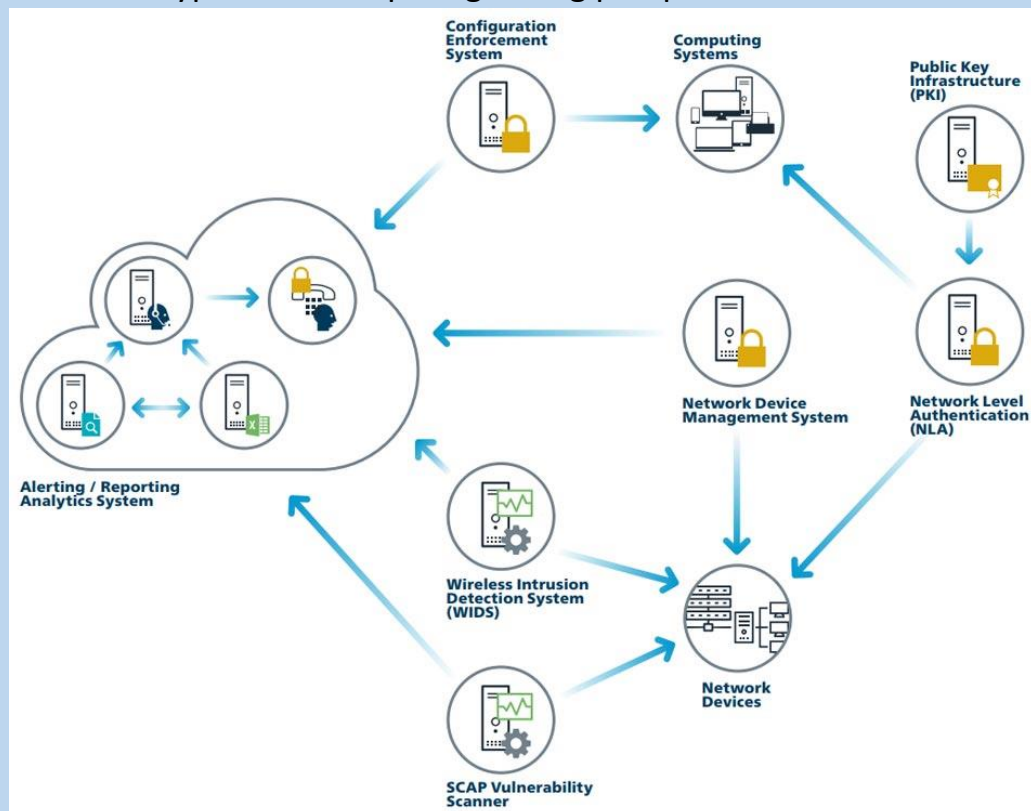
CIS Control 13: Data Protection

Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	Implementation Groups		
					1	2	3
13.1	Data	Identify	Maintain an Inventory of Sensitive Information	Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider.			
13.2	Data	Protect	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.			
13.3	Data	Detect	Monitor and Block Unauthorized Network Traffic	Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			
13.4	Data	Protect	Only Allow Access to Authorized Cloud Storage or Email Providers	Only allow access to authorized cloud storage or email providers.			
13.5	Data	Detect	Monitor and Detect Any Unauthorized Use of Encryption	Monitor all traffic leaving the organization and detect any unauthorized use of encryption.			
13.6	Data	Protect	Encrypt Mobile Device Data	Utilize approved cryptographic mechanisms to protect enterprise data stored on all mobile devices.			
13.7	Data	Protect	Manage USB Devices	If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.			
13.8	Data	Protect	Manage System's External Removable Media's Read/Write Configurations	Configure systems not to write data to external removable media, if there is no business need for supporting such devices.			
13.9	Data	Protect	Encrypt Data on USB Storage Devices	If USB storage devices are required, all data stored on such devices must be encrypted while at rest.			

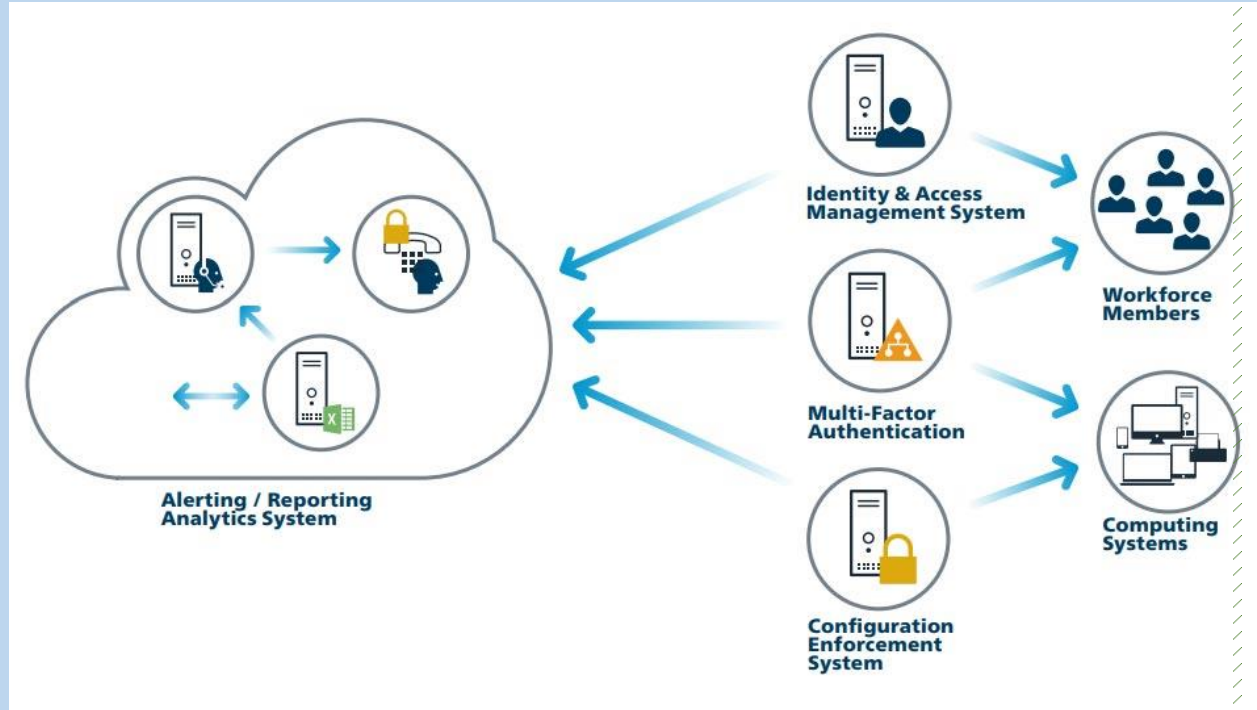
14. Controlled Access Based on the Need to Know: Grant access to resources based on the principle of least privilege and the specific job roles of users. Example: Limiting access to confidential financial data to only the finance team members who require it.



15. Wireless Access Control: Secure wireless networks by implementing strong authentication and encryption mechanisms. Example: Using WPA3 encryption and requiring strong passphrases for Wi-Fi access.

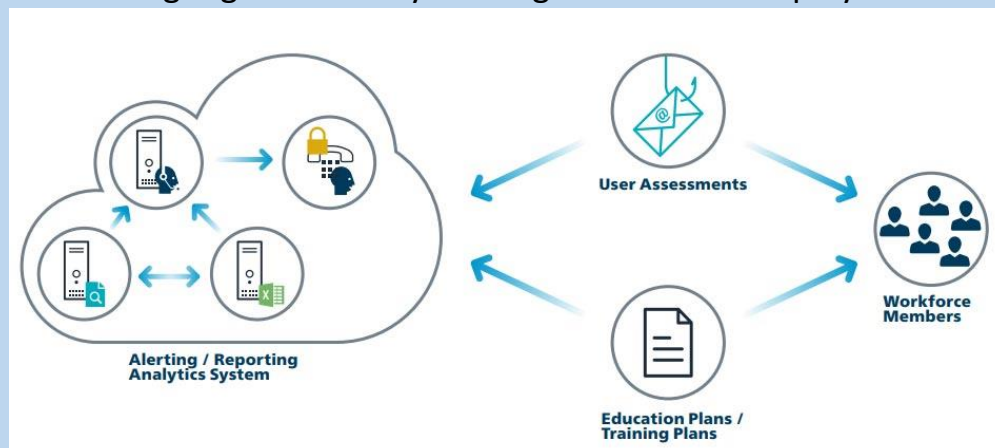


16.Account Monitoring and Control: Continuously monitor user accounts for suspicious activities and promptly disable or remove inactive or compromised accounts. Example: Setting up alerts for failed login attempts and disabling accounts that show signs of unauthorized access.

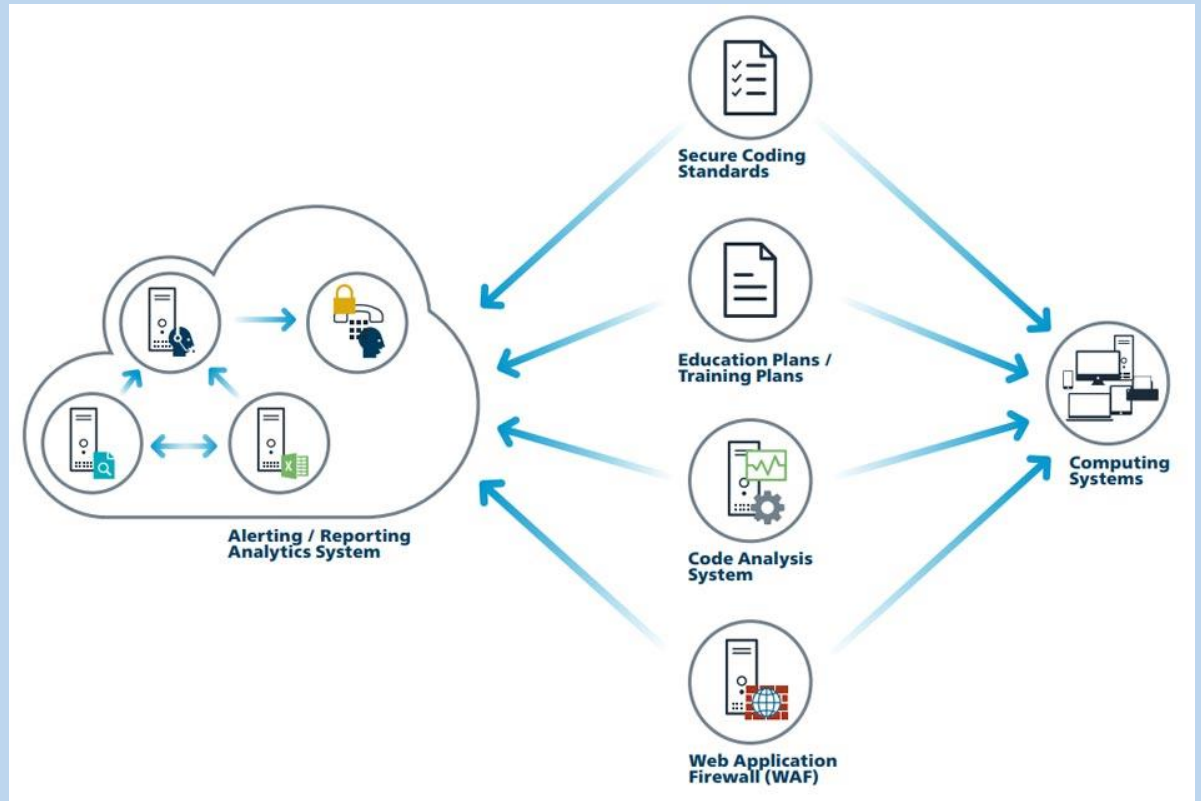


Organizational

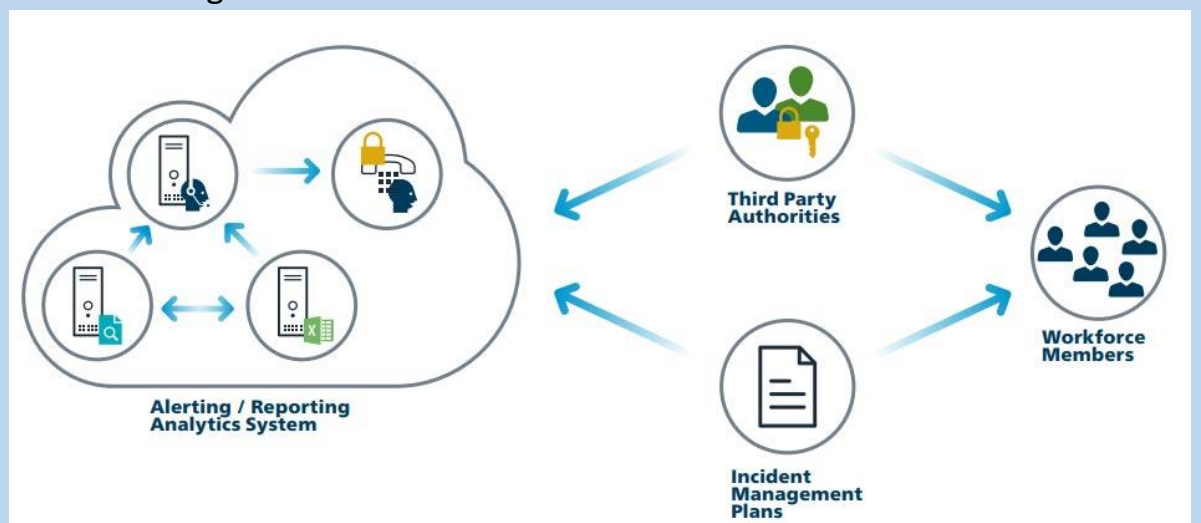
17.Implement a Security Awareness and Training Program: Educate employees about cybersecurity best practices to prevent social engineering attacks and promote a security-conscious culture. Example: Conducting regular security training sessions for employees.



18. Application Software Security: Develop and maintain secure software applications to prevent vulnerabilities and exploits. Example: Conducting code reviews and using secure coding practices to prevent common vulnerabilities like SQL injection.



19. Incident Response and Management: Establish a plan for responding to security incidents to minimize damage and recover quickly. Example: Creating an incident response team that follows a well-defined playbook for addressing data breaches.



20. Penetration Tests and Red Team Exercises: Conduct controlled tests to identify vulnerabilities by simulating real-world attacks. Example: Hiring an external penetration testing company to attempt to breach your organization's network and provide recommendations for improvement.

