UDACITY

FedF1rst Security Assessment

Anderson Okai

31st jun

How to Use this Template

- We have provided these slides as a guide to ensure you submit all the required components to complete your project successfully.
- When presenting your project, remember that these slides are merely a guide. We strongly encourage you to embrace your creative freedom and make changes that reflect your unique vision as long as the required information is present.
- You can add slides to the template when your answers or screenshots do not fit on the previously provided pages.
- Delete this and all other project instruction slides before submitting your project.
- **Remember to add your name and the date to the cover page.**

Project Scenario

Project Scenario

In the swiftly evolving digital age, Fed F1rst Control Systems stands at the cusp of a significant transformation, pushing the boundaries of cybersecurity to safeguard its technological frontier. As the organization embarks on integrating cutting-edge tools and technologies, from Windows environments to the inclusion of MacBooks, and ventures deeper into the cloud, the role of a security engineer has never been more pivotal. Amidst this backdrop, you, as a security engineer, are thrust into the heart of this transformation.

Your mission: to navigate the complexities of digital security, ensuring that every technological advancement—be it through securing desktop environments, fortifying email communications, or aligning with stringent cybersecurity standards—translates into a fortified defense against the cyber threats of tomorrow. Your efforts will not only secure Fed F1rst's digital assets but also shape the very foundation of its future in the digital realm.

Welcome to the forefront of cybersecurity at Fed F1rst Control Systems, where your expertise is the key to unlocking a secure, innovative future.

Section One: Develop a hardening strategy

Windows 10 Hardening

In the dynamic environment of Fed F1rst Control Systems, maintaining the security integrity of desktop environments is crucial to safeguard corporate data and ensure uninterrupted business operations. As part of your responsibilities, you are required to conduct a comprehensive security review of a Windows 10 desktop. This task involves identifying vulnerabilities that could potentially compromise system security and proposing actionable remediation steps to mitigate these risks.

- *Log onto the Windows 10 desktop machine using Udacity-Student with a password of UdacityRocks!*
- *Perform a thorough security analysis focusing on key areas such as system updates, user permissions, antivirus status, firewall settings, and third-party applications*
- ***Identify 6 specific security issues** that pose a risk to the system's integrity*
- *For each identified issue, provide a detailed remediation strategy to address and resolve the vulnerability*

Windows 10 Hardening

Many parts can be hardened in Windows 10, but it can be challenging to find them. You can find the way to 10 different settings:

- **System Updates:** Settings > Update & Security > Windows Update
- **Antivirus Status:** Settings > Update & Security > Windows Security > Virus & threat protection
- **Firewall Settings:** Control Panel > System and Security > Windows Defender Firewall
- **AutoRun/AutoPlay:** Control Panel > Hardware and Sound > AutoPlay
- **User Account Control settings:** Control Panel > User Accounts > User Accounts > Change User Account Control settings
- **Password Policies:** Type in `gpedit.msc` in a CLI, then navigate to Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy
- **Audit Policy (logging):** Type in `secpol.msc` in a CLI, then navigate to Local Policies > Audit Policy
- **Guest Account settings**: Run the command `net user guest` in a CLI
- **Administrator Account settings:** Run the command `net user Administrator` in a CLI
- **BitLocker Drive Encryption:** Right-click on any system drive in File Explorer

Windows 10 Hardening

1. System Updates
Description: The Windows 10 system is not up to date with the latest security patches and updates. Remediation: Navigate to Settings > Update & Security > Windows Update and ensure that the system is configured to download and install updates automatically. Regularly check for updates manually to ensure no critical updates are missed.
2. Antivirus Status
Description: The antivirus software is not active or up to date, leaving the system vulnerable to malware and viruses. Remediation: Navigate to Settings > Update & Security > Windows Security > Virus & threat protection. Ensure that Windows Defender Antivirus is enabled and up to date. Configure the antivirus to perform regular scans and update definitions automatically.
3. Firewall Settings
Description: The Windows Defender Firewall is disabled or improperly configured, exposing the system to network attacks. Remediation: Go to Control Panel > System and Security > Windows Defender Firewall. Ensure the firewall is enabled for all network profiles (Domain, Private, and Public). Configure inbound and outbound rules to limit access to essential services only.

Windows 10 Hardening

4. User Account Control (UAC) Settings
Description: User Account Control settings are set to a low level, which can allow unauthorized changes to the system. Remediation: Navigate to Control Panel > User Accounts > User Accounts > Change User Account Control settings. Set the UAC slider to the highest level to ensure that all changes to the system require administrative approval.
5. Password Policies
Description: Weak password policies can lead to easily compromised user accounts. Remediation: Open the Local Group Policy Editor by typing gpedit.msc in the CLI. Navigate to Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy. Set policies for minimum password length, complexity requirements, maximum password age, and password history.
6. AutoRun/AutoPlay
Description: AutoRun/AutoPlay is enabled, which can automatically execute malicious software from external devices. Remediation: Navigate to Control Panel > Hardware and Sound > AutoPlay. Disable AutoPlay for all devices by unchecking the "Use AutoPlay for all media and devices" option. Additionally, configure specific device settings to prevent automatic execution of programs.

MacOS Hardening

As Fed F1rst Control Systems embarks on enhancing its workforce productivity tools, the decision to integrate MacBooks into the corporate ecosystem marks a significant technological advancement. Prior to deployment, it is essential to ensure these devices are configured for optimal security to protect sensitive corporate information and maintain compliance with industry standards. Your task is to identify and explain six essential security configurations that must be implemented on the MacBooks before they are distributed to employees, ensuring a secure and efficient work environment.

- **Identify six security configurations** that should be applied to MacBooks before they are deployed to employees
- For each configuration, provide a rationale explaining its importance

MacOS Hardening

1. Enable FileVault Disk Encryption
Rationale: FileVault encrypts the entire drive, protecting data from unauthorized access. This is crucial in case the MacBook is lost or stolen, as it ensures that sensitive information remains inaccessible without the correct encryption key. Enabling FileVault ensures that all data stored on the MacBook is secure, even if physical security is compromised.
2. Set Up System Integrity Protection (SIP)
Rationale: SIP is a security feature that helps prevent potentially malicious software from modifying protected files and directories on the MacBook. By restricting root-level access to system files, SIP adds an extra layer of protection against malware and other threats, ensuring the integrity and stability of the operating system.
3. Enforce Strong Password Policies
Rationale: Implementing strong password policies, including requirements for password complexity and regular changes, reduces the risk of unauthorized access. Strong passwords are the first line of defense against brute-force attacks and other password-based intrusions, making it harder for attackers to gain access to the system.

MacOS Hardening

4. Enable Firewall Protection
Rationale: The built-in macOS firewall helps block unauthorized incoming connections, preventing potential intrusions. Enabling and configuring the firewall ensures that only trusted applications and services can communicate with the MacBook, reducing the risk of network-based attacks.
5. Install and Configure Endpoint Protection Software
Rationale: Endpoint protection software provides real-time protection against malware, viruses, and other security threats. By installing and configuring reputable endpoint protection software, the MacBooks are continuously monitored for potential threats, ensuring prompt detection and remediation of any malicious activity.
6. Configure Automatic Software Updates
Rationale: Keeping the operating system and all installed applications up-to-date is crucial for protecting against known vulnerabilities. Configuring automatic software updates ensures that the MacBooks receive the latest security patches and updates as soon as they are available, reducing the risk of exploitation through outdated software.

Section Two:
Create Security Policies

Email Policy

In an era where email is a critical communication tool for businesses, it's equally a prime target for cyber threats, potentially compromising sensitive information. Fed F1rst Control Systems recognizes the importance of securing its email communications to protect against such vulnerabilities. Your task is to contribute to the development of an email policy by specifying five security-related items that should be included. These items will guide employee behavior regarding the use of corporate email systems, aiming to minimize security risks and safeguard company data.

- **Identify five security-related items** that should be included in the company's email policy
- Each item should address a specific aspect or behavior related to email use

Email Policy

1. Mandatory Use of Multi-Factor Authentication (MFA):

- Description: All employees must use multi-factor authentication when accessing corporate email accounts.
- Rationale: MFA adds an additional layer of security, reducing the risk of unauthorized access even if passwords are compromised.

2. Prohibition of External Email Forwarding:

- Description: Employees are prohibited from auto-forwarding corporate emails to external, non-corporate email addresses.
- Rationale: This prevents sensitive information from being inadvertently or maliciously shared outside the company, protecting corporate data from unauthorized access.

3. Regular Password Changes and Complexity Requirements:

- Description: Employees must change their email passwords every 90 days and adhere to complexity requirements (minimum length, combination of letters, numbers, and special characters).
- Rationale: Regular password changes and strong password requirements reduce the risk of password-based attacks, such as brute force or dictionary attacks.

4. Email Encryption for Sensitive Information:

- Description: Sensitive information, including personal data and confidential company information, must be encrypted before being sent via email.
- Rationale: Encryption ensures that sensitive information remains protected during transmission, reducing the risk of interception and unauthorized access.

5. Phishing Awareness and Reporting Procedures:

- Description: Employees must complete regular phishing awareness training and promptly report any suspicious emails to the IT security team.
- Rationale: Training employees to recognize and report phishing attempts reduces the likelihood of successful phishing attacks, protecting the company from potential data breaches and financial loss.

BYOD Policy

As Fed F1rst Control Systems embraces a Bring Your Own Device (BYOD) policy to enhance flexibility and productivity, the security of corporate data on employee-owned devices becomes a critical concern. These devices, ranging from smartphones to laptops, introduce various security challenges that must be addressed to protect both the company's and employees' information. Your role is to contribute to the development of a robust BYOD policy by writing the Security section. This will ensure that employees can use their own devices without compromising the organization's digital security.

- Draft the **Security section of the BYOD policy**
- Cover Apple and Android smartphones, and Windows 11 and macOS laptops
- Include **6 security measures** relevant to these devices
- Focus on diverse security aspects such as access, data protection, and incident management

BYOD Policy

1. Device Enrollment and Management:
   - Description: All employee-owned devices used for work purposes must be enrolled in the company's Mobile Device Management (MDM) system.
   - Rationale: MDM allows IT administrators to enforce security policies, manage device configurations, and remotely wipe corporate data if a device is lost or stolen.

2. Strong Authentication and Access Control:
   - Description: Devices must be configured to use strong authentication methods, such as biometric authentication (fingerprint or facial recognition) or complex passwords. Multi-Factor Authentication (MFA) must be enabled for accessing corporate applications and data.
   - Rationale: Strong authentication reduces the risk of unauthorized access, even if a device is lost or stolen.

3. Data Encryption:
   - Description: All corporate data stored on personal devices must be encrypted using industry-standard encryption protocols. This includes data at rest and data in transit.
   - Rationale: Encryption ensures that sensitive information remains protected from unauthorized access, even if the device is compromised.

4. Regular Software Updates and Patching:
   - Description: Employees must ensure that their devices' operating systems, applications, and security software are regularly updated and patched to the latest versions.
   - Rationale: Regular updates and patches address known vulnerabilities and protect devices from malware and other security threats.

5. Secure Communication:
   - Description: Employees must use secure communication methods, such as Virtual Private Networks (VPNs), when accessing corporate resources over public or unsecured networks.
   - Rationale: VPNs provide a secure, encrypted connection, protecting corporate data from interception and unauthorized access.

6. Incident Management and Reporting:
   - Description: Employees must promptly report any security incidents, such as lost or stolen devices, suspected malware infections, or unauthorized access, to the IT security team. Devices must be configured to allow remote wipe capabilities.
   - Rationale: Timely incident reporting and the ability to remotely wipe corporate data help mitigate potential data breaches and limit the impact of security incidents.

Section Three: Self Assessment

Windows Desktop Compliance

Maintaining robust security measures across all devices is crucial. As part of the organization's commitment to cybersecurity, adhering to the National Institute of Standards and Technology (NIST) guidelines is a top priority. Your task involves evaluating a Windows 10 desktop against specific *NIST SP 800-53 Rev. 5* controls. This exercise is designed to assess the desktop's compliance with established security standards, ensuring the integrity, confidentiality, and availability of the system's information.

- **Review the provided 14-item list** from *NIST SP 800-53 Rev. 5*
- Evaluate the Windows 10 machine for compliance with each item
- For each item, determine if it is:
  - **Met:** The Windows 10 machine complies with the NIST guideline
  - **Not Met:** The Windows 10 machine does not comply with the NIST guideline
  - **NA (Not Applicable):** The NIST guideline does not apply to this Windows 10 machine

Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
Built-In Administrator account is disabled	Not Met
Windows Firewall is enabled	Met
Automatic updates are enabled	Met
User Account Control (UAC) is enabled	Met
Strong password policies are enforced	Not Met
Guest account is disabled	Met
System logging and auditing are enabled	Met
Windows Defender Antivirus is enabled and up to date	Met
Remote Desktop Services are configured securely	Not Met
Internet Explorer Enhanced Security Configuration (IE ESC) is enabled	NA
USB ports are disabled or restricted to authorized devices only	Not met
Network access controls are implemented, including VLAN segmentation and port security	Not met
Remote Registry service is disabled	Met
Windows Updates are configured to download and install updates automatically	Met

Windows Desktop Compliance

Ensuring the Windows 10 desktop at Fed F1rst Control Systems meets all *NIST SP 800-53 Rev. 5* controls is vital for maintaining a strong security posture. After identifying controls that are not met, the next step is to outline straightforward remediation actions. Simplifying the remediation process by focusing on concise, one-line solutions will facilitate a more efficient path to compliance. This approach enables you to quickly address vulnerabilities and enhance the system's security with minimal complexity.

- Review the list of *NIST SP 800-53 Rev. 5* controls previously identified as "Not Met"
- For **each control not met**, provide a short remediation solution. This should be a direct action that can be taken to address the gap
- Ensure the solution is specific enough to be actionable and relevant to a Windows 10 environment

Windows Desktop Compliance

Write your remediation solutions below. **You should write one solution to one row, adding rows as necessary.**

Remediation: Disable the built-in Administrator account and create standard user accounts for all users. Windows Firewall is enabled Met Automatic updates are enabled Met User Account Control (UAC) is enabled Met Strong password policies are enforced Not Met
Remediation: Implement a strong password policy requiring a minimum password length of 12 characters, a mix of uppercase and lowercase letters, numbers, and special characters, and regular password changes. Guest account is disabled Met System logging and auditing are enabled Met Windows Defender Antivirus is enabled and up to date Met Remote Desktop Services are configured securely Not Met
Remediation: Implement USB device control policies to restrict unauthorized use or allow only specific devices. Network access controls are implemented, including VLAN segmentation and port security Not Met
Remediation: Enable Network Level Authentication (NLA), restrict remote access to authorized users, and use strong encryption for remote connections. Internet Explorer Enhanced Security Configuration (IE ESC) is enabled NA (not applicable for modern browsers) USB ports are disabled or restricted to authorized devices only Not Met.
Remediation: Configure VLANs to segregate network traffic and implement port security to restrict access to network ports. Remote Registry service is disabled Met Windows Updates are configured to download and install updates automatically Met

CentOS Compliance

As part of Fed F1rst Control Systems' ongoing commitment to cybersecurity excellence, aligning with the Cybersecurity Maturity Model Certification (CMMC) framework is essential. This task is designed to evaluate the security posture of a provided CentOS Virtual Machine (VM) against a set of 15 CMMC controls. Your objective is to assess each item's compliance, ensuring that the VM meets the stringent requirements set forth for protecting sensitive information. This exercise is crucial for identifying gaps in security practices and ensuring that the VM is fortified against potential cyber threats.

- Review the provided 15-item list of CMMC controls
- Assess the CentOS VM for compliance with each listed control
- For each control, determine if it is:
    - **Met:** The CentOS VM complies with the CMMC control
    - **Not Met:** The CentOS VM does not comply with the CMMC control
    - **NA (Not Applicable):** The CMMC control does not apply to this CentOS VM

CentOS Compliance

CentOS CMMC Requirements	Met/Not Met
Current on security updates	Not met
Ensure separate partition exists for /var	Not met
Disable Automounting of drives	met
Ensure AIDE is installed	Not met
Ensure daytime services are not enabled	Met
Ensure echo services are not enabled	met
Ensure tftp server is not enabled	met
Ensure CUPS is not enabled	met
Ensure DHCP Server is not enabled	met
Ensure FTP Server is not enabled	met
Ensure Samba is not enabled	met
Ensure TCP Wrappers is installed	Not met
Ensure DCCP is disabled	met
Ensure iptables is installed	met
Ensure audit log storage size is configured	met
Ensure audit logs are not automatically deleted	Not met

Section Four:
Cloud Management

Windows Server Build Sheet

As part of Fed F1rst Control Systems' security policy implementation, it is crucial to establish a standardized build process for Windows web servers hosted in the public cloud. A well-defined build sheet ensures consistency, security, and adherence to best practices across all server deployments. In this task, you will create a list of 10 essential items, along with examples, that should be included in a build sheet for a Windows web server hosted in the public cloud.

- **Identify 10 critical items** that should be included in a build sheet for a Windows web server hosted in the public cloud
- Provide a brief **description OR an example** for each item

Windows Server Build Sheet

1. Operating System Version
Description: Specify the version of the Windows Server to be installed (e.g., Windows Server 2019 or 2022).
2. Security Updates and Patches
Description: Ensure the server is up-to-date with the latest security patches and updates.
3. Firewall Configuration
Description: Configure the Windows Firewall to allow only necessary traffic to the web server.
4. Web Server Installation and Configuration
Description: Install and configure IIS (Internet Information Services) for hosting web applications.
5. Secure Sockets Layer (SSL) Configuration
Description: Ensure SSL/TLS is configured for secure communication.

Windows Server Build Sheet

6. User Accounts and Permissions
Description: Define and configure user accounts with the principle of least privilege.
7. Remote Management Configuration
Description: Configure secure remote management settings.
8. Application and Service Monitoring
Description: Set up monitoring and logging for applications and services.
9. Backup and Recovery Plan
Description: Implement a robust backup and recovery strategy.
10. Security Baseline and Hardening
Description: Apply security baselines and hardening measures to minimize vulnerabilities.

Enhancing Cloud Security with CASB

With Fed F1rst Control Systems increasingly leveraging cloud technologies for their operations, the integration of Cloud Access Security Brokers (CASB) into their security framework is more crucial than ever. Given your understanding of CASBs from the course, you're in a unique position to assess how their capabilities can specifically enhance Fed F1rst's security posture.

- Identify **5 specific benefits** of CASBs that would directly enhance the cloud security posture of Fed F1rst Control Systems
- Provide a concise, clear description for each benefit

Enhancing Cloud Security with CASB

1. Visibility into Cloud Usage
Description: CASBs provide comprehensive visibility into cloud applications and services being used across the organization. This helps Fed F1rst monitor and control shadow IT, ensuring all cloud usage is accounted for and managed securely.
2. Data Protection and Compliance
Description: CASBs enforce data loss prevention (DLP) policies to protect sensitive information in the cloud. They help ensure compliance with industry regulations and internal policies by monitoring data transfers and preventing unauthorized data access and leakage.
3. Threat Protection
Description: CASBs offer advanced threat protection by detecting and mitigating threats such as malware, account hijacking, and insider threats in real-time. This enhances Fed F1rst's ability to respond to and neutralize potential security incidents quickly.
4. Access Control and Authentication
Description: CASBs enforce granular access controls and multi-factor authentication (MFA) for cloud applications. This ensures that only authorized users can access sensitive resources, reducing the risk of unauthorized access and data breaches.
5. Shadow IT Discovery and Control
Description: CASBs help identify and manage unsanctioned cloud applications used by employees. This allows Fed F1rst to control shadow IT, mitigate associated risks, and ensure that all cloud services adhere to the organization's security policies.