

# FedF1rst Security Assessment



*EMMANUEL AVAH*  
*19-05-2024*



# 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

## 1. System Updates

- Issue: The system is running outdated versions of Windows 10, which leaves it vulnerable to known security vulnerabilities.

- Remediation:

Open the Start menu and click on the Settings icon.

Navigate to Update & Security > Windows Update.

Click on "Check for updates" and install any available updates.

I configured the system to automatically download and install future updates.

## 2. User Permissions

- Issue: The Udacity-Student user account has excessive permissions, potentially allowing unauthorized access.

- Remediation:

Press the Windows key + R to open the Run dialog.

Type "lusrmgr.msc" and press Enter to open the Local Users and Groups management tool.

Locate the "Udacity-Student" user account and review its group memberships and permissions.

I removed any unnecessary permissions or group memberships to minimize the account's privileges.

## 3. Antivirus Status

- Issue: The system has an antivirus solution installed, but outdated and misconfigured.

- Remediation:

Open the Start menu and click on the Settings icon.

Navigate to Update & Security > Windows Security.

Click on "Virus & threat protection" and review the status of your antivirus solution.

I ensured the antivirus software is up-to-date and configured it to perform regular system scans.



# Windows 10 Hardening

## 4. Firewall Settings

- Issue: The system's firewall may have incorrect or outdated settings, leaving it vulnerable to network-based attacks.
- Remediation:

Open the Control Panel.

Navigate to System and Security > Windows Defender Firewall.

I reviewed the inbound and outbound firewall rules and modified them as needed.

I enabled advanced firewall features, such as network profile settings and domain-specific rules.

## 5. Third-Party Applications

- Issue: The system may have installed third-party applications that are outdated, vulnerable, or potentially malicious.
- Remediation:

Open the Control Panel and navigate to the "Programs and Features" section.

Identify any installed third-party applications.

I researched the security status and update information for each application.

I uninstalled and updated any applications that are known to be vulnerable or no longer supported.

## 6. Weak Passwords

- Issue: The "UdacityRocks!" password is a weak password, makes it vulnerable to brute-force attacks or password guessing.
- Remediation:

Open the Local Users and Groups management tool (lusrmgr.msc).

Locate the "Udacity-Student" user account and reset the password to a strong, complex password.

I implemented a password policy that enforces the use of strong passwords for all user accounts.

I enabled multi-factor authentication for added security.



# MacOS Hardening

## 1. FileVault Encryption:

By enabling FileVault, the entire contents of the MacBook's storage, including the operating system, applications, and user data, are encrypted. This ensures that even if the device is lost or stolen, the sensitive information it contains cannot be accessed by unauthorized parties, providing a strong safeguard against data breaches.

## 2. Firewall Configuration:

Properly configuring the MacOS firewall allows me to control the flow of network traffic to and from the device. This helps prevent unauthorized access, block malicious incoming connections, and restrict outgoing communication to only the necessary and approved destinations. This layer of network-level protection reduces the risk of successful cyber attacks.

## 3. System Integrity Protection (SIP):

SIP is a security feature that prevents modifications to critical system files and directories, even by the root user. This protection mechanism helps ensure the integrity of the operating system, making it more difficult for malware or unauthorized changes to compromise the device's security and maintain a secure baseline.



# MacOS Hardening

## 4. Application Whitelisting:

Implementing application whitelisting on the MacBooks allows only approved and trusted applications to run. This effectively blocks the execution of unauthorized or potentially malicious software, reducing the attack surface and preventing the infiltration of my corporate environment by harmful programs.

## 5. Endpoint Protection and Antivirus:

Deploying a robust endpoint protection solution on the MacBooks enables real-time monitoring, threat detection, and response capabilities. This helps identify and mitigate malware infections, prevent the spread of malicious code, and provide a comprehensive security layer to safeguard the devices and my overall corporate network.

## 6. User Account Management:

Enforcing strong password policies, implementing multi-factor authentication, and following the principle of least privilege for user accounts enhance the security of the MacBooks. This helps prevent unauthorized access, limits the potential impact of compromised credentials, and ensures that users can only perform the necessary actions, reducing the risk of data breaches or malicious activities.





# Section Two: Create Security Policies

---



# Email Policy

## Password Management:

- Employees must use strong, unique passwords for their email accounts.
- Passwords must be changed periodically, and the use of password management tools is recommended.
- Employees are strictly prohibited from sharing their email passwords with anyone, including colleagues or IT support staff.

## Attachment and Link Handling:

- Employees must exercise caution when opening attachments or clicking on links in emails, even if they appear to be from trusted sources.
- Employees should verify the legitimacy of the sender and the content before taking any action.
- The use of antivirus software is mandatory, and employees must keep their antivirus software up-to-date to detect and prevent the spread of malware.

## Sensitive Information:

- Employees must avoid sending sensitive or confidential information, such as personal data, financial information, or trade secrets, via email unless it is encrypted or secured using approved methods.
- Employees must follow the company's guidelines for handling and protecting sensitive information in email communications.

## Acceptable Use:

- My corporate email system is provided for business purposes only. Employees are prohibited from using the email system for personal activities, illegal purposes, or the distribution of inappropriate content.
- My company reserves the right to monitor and review email communications for compliance and security purposes.

## Incident Reporting:

Employees must report any suspected security incidents, such as phishing attempts, data breaches, or unauthorized access to their email accounts, to the IT department or designated security personnel.

Employees must follow the company's established process for reporting such incidents, and the company will take appropriate actions in response.



# BYOD Policy

## 1. Access Control:

All employee-owned devices, including Apple and Android smartphones, as well as Windows 11 and MacOS laptops, must be enrolled in my company's Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) solution before they can access corporate resources.

## 2. Data Protection:

All corporate data stored on employee-owned devices must be encrypted using approved encryption methods, such as AES-256 or equivalent. This requirement applies to both smartphones and laptops.

## 3. Incident Management:

Employees must report any suspected security incidents, such as device loss, theft, or unauthorized access, to the IT department or designated security personnel immediately. Prompt reporting is crucial for mitigating the potential impact of such incidents.

## 4. Security Training and Awareness

Employees participating in the BYOD program will be required to undergo regular security training and awareness sessions to ensure they understand the security risks associated with using their personal devices and the necessary measures to protect corporate data.

## 5. Secure Container

Employees must use a secure container or sandbox application to isolate corporate data and applications from personal content on their devices. This helps to maintain the confidentiality and integrity of my company information, preventing inadvertent data leaks or unauthorized access to sensitive data.

## 6. Approved Applications

Employees are only permitted to use company-approved applications and software on their devices for accessing corporate resources. The use of unauthorized applications is strictly prohibited. The company will provide a curated list of approved apps for each supported device platform, ensuring that these applications meet the necessary security and compliance requirements.



# Section Three: Self Assessment

---



# Windows Desktop Compliance

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



# Windows Desktop Compliance

## Remediation solutions

- Open the "Local Users and Groups" management console by pressing the Windows key + R, typing "lusrmgr.msc", and pressing Enter.
- In the "Local Users and Groups" window, expand the "Users" folder and double-click on the "Administrator" account.
- In the "Administrator Properties" window, under the "General" tab, check the "Account is disabled" option.
- Click "Apply" to save the changes and close the window.

Enable the Windows Firewall by navigating to the "Windows Defender Firewall with Advanced Security" and setting the profile states to "On" for the Domain, Private, and Public profiles.

Enable User Account Control (UAC) by navigating to the "User Account Control Settings" and setting the value to "Notify me when apps try to make changes to my computer (default)".

Configure the local security policy to enforce strong password requirements, such as minimum length, complexity, and expiration. This can be done by navigating to the "Local Security Policy" editor and updating the "Account Policies" and "Password Policy" settings.

Disable the built-in Guest account by navigating to the "Local Users and Groups" management console and setting the "Guest" account to "Disabled".

Enable system logging and auditing by navigating to the "Local Security Policy" editor and configuring the "Audit Policy" settings to log the desired events.

Ensure Windows Defender Antivirus is enabled and automatically updated by navigating to the "Windows Security" app and enabling the "Real-time protection" and "Cloud-delivered protection" features.



# CentOS Compliance

CentOS CMMC Requirements	Met/Not Met
Current on security updates	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

## 1. Antivirus and Antimalware

Specify the antivirus and antimalware solution that should be installed and configured on the Windows web server, including the required settings and update schedule.

Example: Install and configure Microsoft Defender Antivirus with real-time protection and automatic definition updates.

## 2. Disk Encryption

Specify the disk encryption solution and settings to be applied to the Windows web server, ensuring the protection of sensitive data at rest.

Example: Enable BitLocker drive encryption with a 256-bit AES key and a secure key protector.

## 3. Security Monitoring and Incident Response

Outline the security monitoring and incident response procedures, including the integration with a security information and event management (SIEM) system and the defined escalation process.

Example: Configure the Windows web server to forward security logs to a centralized SIEM system, and establish a documented incident response plan with clear roles and responsibilities.

## 4. Remote Access

Define the approved methods and configurations for remote access to the Windows web server, such as the use of a virtual private network (VPN) or secure shell (SSH).

Example: Enable remote desktop access with multi-factor authentication and configure the Remote Desktop Protocol (RDP) to use only the latest version and strong encryption.

## 5. Backup and Disaster Recovery

Define the backup strategy, including the frequency, retention policy, and the location of the backup storage (e.g., cloud-based or on-premises).

Example: Perform daily incremental backups and weekly full backups to a secure cloud storage service, with a 30-day retention period.



# Windows Server Build Sheet

## 6. Web Application Security

Outline the security measures to be implemented for the web application, such as input validation, cross-site scripting (XSS) protection, and cross-site request forgery (CSRF) protection.  
Example: Implement a web application firewall (WAF) to protect against common web application vulnerabilities, and configure the web server to enforce strict input validation.

## 7. SSL/TLS Configuration

Specify the configuration settings for the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, including the minimum acceptable version and the approved cipher suites.  
Example: Configure the web server to use TLS 1.2 or higher, and enable only NIST-approved cipher suites.

## 8. User Access and Permissions

Define the user access control policies, including the principle of least privilege, and the specific permissions granted to different user roles.  
Example: Limit administrative access to only authorized personnel, and grant users the minimum necessary permissions to perform their assigned tasks.

## 9. Secure Configurations for Third-Party Software

Document the secure configuration settings for any third-party software installed on the Windows web server, such as content management systems or web frameworks.  
Example: Ensure that any third-party software is kept up-to-date, and apply the vendor-recommended security configurations to mitigate known vulnerabilities.

## 10. Secure Communication and Encryption

Ensure that all communication channels to and from the Windows web server are secured using strong encryption protocols and algorithms.  
Example: Enforce the use of HTTPS for all web traffic, with a minimum TLS version of 1.2 and approved cipher suites, and configure secure protocols for any other communication channels, such as SSH or SFTP.



# Enhancing Cloud Security with CASB

## 1. Visibility and Control over Cloud Usage

CASBs offer comprehensive visibility into cloud application usage, data transactions, and user activities across the organization's cloud environment. This allows Fed F1rst to gain better control over shadow IT, enforce policies, and mitigate the risks associated with unsanctioned cloud services.

## 2. Data Protection and Access Control

CASBs enable Fed F1rst to implement granular access controls, data encryption, and DLP (Data Loss Prevention) policies to protect sensitive information stored in the cloud. This helps ensure that data is accessed and shared only by authorized users and in compliance with regulatory requirements.

## 3. Threat Detection and Incident Response

CASBs can integrate with security incident and event management (SIEM) systems to provide advanced threat detection capabilities. By analyzing user behavior, data access patterns, and cloud application activities, CASBs can identify and alert on suspicious activities, enabling Fed F1rst to respond promptly to potential security incidents.

## 4. Compliance and Regulatory Monitoring

CASBs can help Fed F1rst maintain compliance with industry regulations and standards, such as HIPAA, GDPR, or PCI-DSS, by monitoring cloud usage, enforcing data protection policies, and generating comprehensive compliance reports.

## 5. Consolidated Security Governance

By serving as a centralized control point, CASBs allow Fed F1rst to implement and enforce consistent security policies across multiple cloud services and platforms. This simplifies the management of cloud security, reduces the risk of policy drift, and ensures a unified security posture throughout my organization's cloud ecosystem.