RMF EXAMPLE

Title: RMF Process for WatchGuard (**Moderate Impact System**) Using Tenable Nessus

Company: Winterfell Cyber Solutions

Name: Shane Ebanks

Date: 2/20/2025

Version 1.0

RMF EXAMPLE

TABLE OF CONTENTS

RMF EXAMPLE

INTRODUCTION

Project Title: RMF Process for WatchGuard (**Moderate-Impact System**) Using Tenable Nessus

This project details the implementation of the Risk Management Framework (RMF) for **WatchGuard**, a moderate-impact system managed by **Winterfell Cyber Solutions**. WatchGuard supports critical operations, handling moderately sensitive information that demands a balanced approach to security and compliance. The goal is to ensure compliance with federal security standards while strengthening defenses against threats and vulnerabilities—all with a touch of Game of Thrones-inspired humor.

The project will apply the RMF process to WatchGuard to establish effective security controls, manage risks, and evaluate the system's security posture. These efforts will focus on reducing security risks to an acceptable level and ensuring that WatchGuard meets the compliance requirements necessary for systems with moderate impact levels.

OVERVIEW OF THE RMF PROCESS AND ITS APPLICATION TO MODERATE SYSTEMS

1. OVERVIEW OF THE RMF PROCESS

The **Risk Management Framework (RMF)** is a structured approach designed to ensure that systems are secured and compliant with federal security requirements. The RMF helps to manage risks throughout the **lifecycle of a system** and is especially important for systems like **WatchGuard** that handle **moderate-impact** data. This process is crucial for mitigating the risks to confidentiality, integrity, and availability while adhering to federal guidelines.

For **moderate-impact systems** like **WatchGuard**, the RMF process must be followed to ensure that security controls are appropriately implemented and maintained. Since **moderate impact systems** handle **sensitive but unclassified information**, there is an increased risk to security, making the implementation of these controls even more critical.

RMF STEPS IN THE CONTEXT OF A MODERATE-IMPACT SYSTEM

The RMF process consists of **six distinct steps**, and each step is designed to ensure that security risks are appropriately identified, mitigated, and monitored over time. Below is a breakdown of each step and its application to a **moderate-impact system** like **WatchGuard**.

I did not include the Preparation Phase of the Risk Management Framework (RMF) process because, while it is a critical foundational step, my focus is on the core steps that directly impact system authorization and risk mitigation. However, the Preparation Phase plays a vital role in ensuring an effective and efficient RMF process by establishing the necessary groundwork before security controls are selected and implemented.

RMF EXAMPLE

During this phase, key activities include identifying and categorizing the system, defining roles and responsibilities, conducting essential risk assessments, establishing a governance structure, and ensuring organizational readiness. While it does not directly involve system authorization, skipping or inadequately addressing this phase can lead to inefficiencies and security gaps later in the RMF process.

1. **Categorize the System**:

    - **Purpose**: Determine the system's impact on operations if compromised and assign the correct security categorization.

    - **For WatchGuard**: As a **moderate-impact system**, **WatchGuard** must categorize its information systems in line with **FIPS 199**. This will focus on assessing the **confidentiality**, **integrity**, and **availability** of the data. Since **WatchGuard** processes sensitive but unclassified data, it is categorized as **moderate impact** (impact level **MOD**) for the system's operational integrity and data sensitivity.

2. **Select Security Controls**:

    - **Purpose**: Identify appropriate security controls from established frameworks such as **NIST SP 800-53** to protect the system and its data.

    - **For WatchGuard**: Based on the **moderate impact** categorization, appropriate security controls (from **NIST SP 800-53 Rev. 5**) will be selected. These controls will address areas like access control, audit and accountability, incident response, and system integrity. Given the increased security risks associated with moderate-impact data, WatchGuard will implement stricter controls such as encryption for data **at rest** and **in transit**, **multi-factor authentication (MFA)**, and regular vulnerability assessments.

3. **Implement Security Controls**:

    - **Purpose**: Apply the selected security controls to the system to safeguard its information.

    - **For WatchGuard**: The selected security controls must be integrated into the **WatchGuard** system. This involves configuring and deploying technical measures (e.g., encryption software, firewall configurations) as well as administrative processes (e.g., role-based access controls, security training). Given the sensitivity of the data being handled, it's essential to ensure that all controls are implemented comprehensively and correctly.

4. **Assess Security Controls**:

- **Purpose**: Evaluate the effectiveness of the implemented security controls to ensure they are working as intended.

- **For WatchGuard**: Security assessments will be conducted on **WatchGuard** to evaluate whether the implemented controls are functioning effectively. Tools such as the **Tenable Nessus** vulnerability scanner will be used to identify any vulnerabilities in the system. Penetration testing, risk assessments, and security audits will be performed to ensure that controls provide the intended protection, and that the system can withstand potential security threats.

5. **Authorize the System**:

    - **Purpose**: Obtain formal authorization to operate (ATO) from the Authorizing Official based on the security posture of the system.

    - **For WatchGuard**: After assessing the system's security posture, the findings will be compiled into a Security Assessment Report (SAR). The **System Owner** will present this information to the **Authorizing Official** to request an **Authorization to Operate (ATO)**. The **Authorizing Official** will consider the system's security risks, the effectiveness of the controls, and any potential mitigations before granting the ATO. Given the sensitive nature of **moderate-impact data**, this decision will be carefully reviewed to minimize security risks.

6. **Monitor Security Controls**:

    - **Purpose**: Continuously monitor the system to detect and respond to emerging threats or vulnerabilities.

    - **For WatchGuard**: Continuous monitoring is essential for maintaining the security of **WatchGuard**. This involves tracking system activity, conducting regular vulnerability scans, monitoring logs for suspicious activities, and applying patches and updates as necessary. Monitoring tools and practices, such as intrusion detection systems (IDS), automated patch management, and security information and event management (SIEM) tools, will be employed to ensure the ongoing effectiveness of the security controls and to detect and respond to any new threats that may arise.

2. USE OF TENABLE NESSUS VULNERABILITY SCANNER

To assess **WatchGuard**'s security posture, the **Tenable Nessus vulnerability scanner** will be used to perform thorough vulnerability assessments. Nessus is a highly effective tool for identifying security weaknesses, vulnerabilities, misconfigurations, and potential risks within a system.

In the context of the **RMF process**, Nessus will serve the following purposes:

- **Scanning system components**: Performing vulnerability assessments on **WatchGuard**'s servers, databases, applications, and network components to identify any security gaps.

- **Assessing security control effectiveness**: Evaluating the effectiveness of the security controls implemented to protect sensitive information within the system.

- **Generating vulnerability reports**: Nessus will generate detailed reports that identify risks such as missing patches, outdated software, or misconfigurations. These reports will provide actionable insights to remediate vulnerabilities.

- **Guiding remediation**: Based on the findings of the Nessus scans, appropriate remediation actions will be implemented to ensure compliance with security standards and reduce risks to the system.

- **Continuous monitoring**: Nessus will be used as part of the ongoing monitoring phase to assess the system's security on a regular basis and help detect emerging vulnerabilities.

By utilizing Tenable Nessus alongside the RMF process, Winterfell Cyber Solutions can ensure that WatchGuard maintains a strong security posture, meets regulatory requirements, and is continuously safeguarded from potential threats.

3. EACH STEP IN RMF (FOR A MODERATE IMPACT SYSTEM)

CATEGORIZING THE SYSTEM (STEP 1):

The first step in the **RMF** process is to categorize the **WatchGuard** system based on the guidelines provided in **FIPS 199**. FIPS 199 helps **determine the potential impact** that the loss of **Confidentiality**, **Integrity**, or **Availability** would have on the system's operations and assets.

For a **moderate impact system**, we assess each system component (e.g., databases, communication systems, and applications) in terms of the potential consequences if compromised. Since **WatchGuard** is handling **sensitive** information, we categorize the impact levels for **Confidentiality**, **Integrity**, and **Availability** as **Moderate**.

FIPS 199 Guidelines Overview:

- **Confidentiality**: The protection of sensitive information from unauthorized access.
- **Integrity**: Ensuring data is accurate, complete, and not modified without authorization.
- **Availability**: Ensuring the system and data are accessible and functional when needed.

Based on the assessment of the system components, **WatchGuard** is categorized as **moderate impact** for all three of these parameters. Here's a hypothetical breakdown:

Impact Analysis Table:

RMF EXAMPLE

System Component	Confidentiality	Integrity	Availability	Impact Description
Web Application	Moderate Impact	Moderate	Moderate	The web application stores and processes sensitive user data. Unauthorized access would compromise personal data, though it is not classified.
Database	Moderate Impact	Moderate	Moderate	The database contains sensitive data (unclassified but sensitive). Unauthorized access or modification could compromise security, thus access must be restricted.
Communication Systems	Moderate Impact	Moderate	Moderate	Communication between systems includes sensitive data transmission. Any disruption or tampering would affect integrity and availability.
Authentication System	Moderate Impact	Moderate	Moderate	Controls access to the system. If compromised, the system's integrity is at risk, as unauthorized users could gain access.
Backup Systems	Moderate Impact	Moderate	Moderate	Backup systems ensure data availability. If backup integrity is compromised, it could result in data loss or recovery issues.
Access Control Systems	Moderate Impact	Moderate	Moderate	Critical for enforcing data access policies. A breach could result in unauthorized access to sensitive data.

Impact Analysis Explanation:

Each system component has been categorized based on the potential risks associated with losing **Confidentiality**, **Integrity**, and **Availability**. Since the **WatchGuard** system processes **sensitive data** and **moderate-impact** operations, it requires **moderate security measures** to protect these components.

- **Confidentiality**: Since the data handled is sensitive but unclassified, unauthorized access could compromise confidentiality. This requires access controls, encryption, and authentication to protect against unauthorized access.

- **Integrity**: Ensuring the integrity of the data is crucial. For example, if the web application or database is compromised, attackers could modify the data, resulting in

significant security risks. For this, we would implement data integrity checks, audit logs, and validation mechanisms to detect any unauthorized changes to the system.

- **Availability**: The system must be operational and available when required. A failure in any of the components (e.g., communication systems or backup systems) could result in service disruptions. Therefore, we must implement redundancy, failover mechanisms, and disaster recovery plans to ensure the system remains functional even during disruptions.

Security Controls Impact:

The categorization of **moderate impact** for **WatchGuard** means that security controls must be robust enough to protect against potential threats to confidentiality, integrity, and availability. Here are examples of how this impacts the security controls:

1. **Confidentiality Controls**:
    - **Encryption**: Data at rest and in transit must be encrypted to prevent unauthorized access.
    - **Access Controls**: Implement **role-based access control (RBAC)** to ensure that only authorized personnel can access sensitive information.
    - **Multi-Factor Authentication (MFA)**: Enforce MFA for system access to strengthen confidentiality.
2. **Integrity Controls**:
    - **Hashing**: Data should be hashed to ensure that it has not been tampered with during transmission.
    - **Integrity Monitoring**: Implement regular integrity checks to identify any unauthorized changes to the system or its data.
    - **Audit Logs**: Maintain detailed audit logs for all critical system actions to detect and investigate potential integrity breaches.
3. **Availability Controls**:
    - **Redundancy**: Deploy redundant systems for critical components like databases and communication systems to ensure continuous availability.
    - **Backup and Recovery**: Implement regular backup procedures and disaster recovery plans to restore data and system functionality in case of a breach or failure.

- **Incident Response**: Develop an incident response plan specifically addressing the availability of the system during security events.

SELECTING SECURITY CONTROLS (STEP 2):

The security controls below represent the moderate baseline requirements for **WatchGuard**, categorized according to the **NIST 800-37** framework. These controls ensure the confidentiality, integrity, and availability of the system, with a particular focus on protecting sensitive data and maintaining system integrity. *****Control enhancements and supplemental controls are not included in this demonstration*****

Access Control (AC)

- **AC-2 (Account Management)**: Ensure that accounts are properly managed by defining roles, ensuring correct privileges, and auditing account activities. This includes the creation, modification, disabling, and deletion of accounts based on user responsibilities.

- **AC-3 (Access Enforcement)**: Implement access control policies to restrict access to system resources and enforce access controls based on user roles, ensuring that only authorized users have access to sensitive data.

- **AC-17 (Remote Access)**: Implement remote access controls and ensure that connections are secure and monitored to prevent unauthorized access to sensitive systems when accessed remotely.

Audit and Accountability (AU)

- **AU-2 (Audit Events)**: Define the events to be audited, including login attempts, data access, and changes to system configurations, ensuring that all actions related to sensitive data are recorded for accountability.

- **AU-6 (Audit Review, Analysis, and Reporting)**: Regularly review audit logs and conduct analysis to detect any anomalies or suspicious activities. Provide reports for compliance and investigation purposes.

- **AU-8 (Time Stamps)**: Ensure that system logs include accurate time stamps for all logged events, providing a reliable audit trail for incident investigations and system monitoring.

System and Communications Protection (SC)

- **SC-12 (Cryptographic Key Establishment and Management)**: Implement controls to establish, manage, and securely store cryptographic keys, ensuring the confidentiality and integrity of data being transmitted or stored.

- **SC-13 (Cryptographic Protection)**: Ensure that data in transit and data at rest is protected using strong cryptographic methods to prevent unauthorized access and tampering.

- **SC-28 (Protection of Information at Rest)**: Protect sensitive data stored on systems (e.g., databases, backups) by encrypting it to ensure confidentiality and integrity in case of a system compromise or data breach.

Incident Response (IR)

- **IR-4 (Incident Handling)**: Develop and implement procedures for handling security incidents, including the identification, containment, eradication, recovery, and follow-up actions for any incidents involving sensitive data.

- **IR-5 (Incident Monitoring)**: Continuously monitor systems for potential security incidents, ensuring that any threats to the confidentiality or integrity of sensitive data are detected and responded to promptly.

- **IR-6 (Incident Reporting)**: Ensure that all security incidents are reported according to established procedures, enabling the organization to track and respond to potential breaches of confidentiality, integrity, or availability.

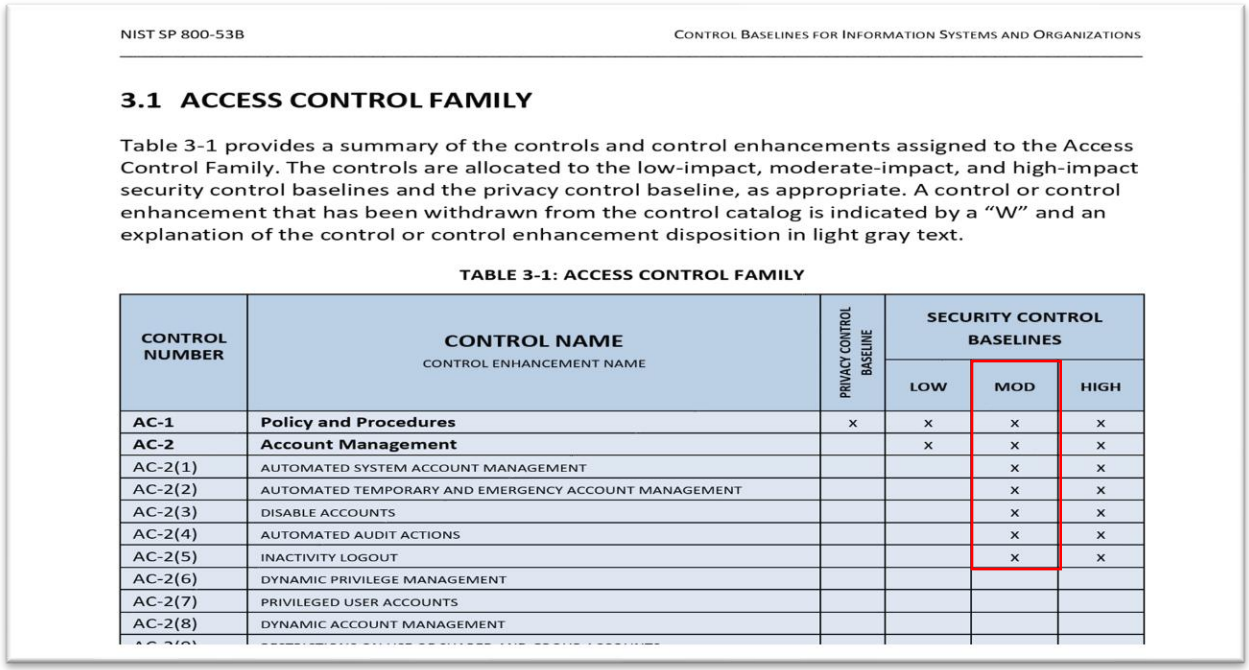
System and Communications Protection (SC) – Additional Considerations

- **SC-7 (Boundary Protection)**: Implement boundary protection measures such as firewalls, intrusion detection/prevention systems, and secure gateways to protect the system's external interfaces from unauthorized access.

- **SC-8 (Transmission Confidentiality and Integrity)**: Ensure that communication channels, both internal and external, maintain confidentiality and integrity of transmitted data through the use of encryption, secure protocols, and integrity checks.

The below diagram is a representation of how baseline controls are identified for low, moderate and high-impact systems.

RMF EXAMPLE



NIST SP 800-53B — CONTROL BASELINES FOR INFORMATION SYSTEMS AND ORGANIZATIONS

3.1 ACCESS CONTROL FAMILY

Table 3-1 provides a summary of the controls and control enhancements assigned to the Access Control Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate. A control or control enhancement that has been withdrawn from the control catalog is indicated by a "W" and an explanation of the control or control enhancement disposition in light gray text.

TABLE 3-1: ACCESS CONTROL FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AC-1	**Policy and Procedures**	x	x	x	x
AC-2	**Account Management**		x	x	x
AC-2(1)	AUTOMATED SYSTEM ACCOUNT MANAGEMENT			x	x
AC-2(2)	AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT			x	x
AC-2(3)	DISABLE ACCOUNTS			x	x
AC-2(4)	AUTOMATED AUDIT ACTIONS			x	x
AC-2(5)	INACTIVITY LOGOUT			x	x
AC-2(6)	DYNAMIC PRIVILEGE MANAGEMENT				
AC-2(7)	PRIVILEGED USER ACCOUNTS				
AC-2(8)	DYNAMIC ACCOUNT MANAGEMENT				

IMPLEMENTING SECURITY CONTROLS (STEP 3):

AC-2 (Account Management):

- Implemented **Role-Based Access Control (RBAC)**, assigning user roles and ensuring users only have the privileges necessary to perform their job functions.
- Integrated **multi-factor authentication (MFA)** for users accessing sensitive data, further strengthening account security by requiring multiple verification factors.
- Regularly reviewed and updated accounts, ensuring that permissions remain in alignment with users' current responsibilities and removing access promptly when no longer required.

AC-3 (Access Enforcement):

- Developed and enforced **access control policies** that define who can access specific system resources.
- Configured **access control lists (ACLs)** and **firewall rules** to enforce access restrictions, ensuring unauthorized users cannot access classified or sensitive information.
- Utilized user authentication and authorization mechanisms to prevent unauthorized access to the system based on role and responsibilities.

RMF EXAMPLE

AC-17 (Remote Access):

- Established secure remote access by implementing **Virtual Private Networks (VPNs)** and using **multi-factor authentication (MFA)** to ensure that remote access to the system is tightly controlled.
- Deployed **secure remote desktop solutions** and **end-to-end encryption** to protect sensitive data during remote sessions.

AU-2 (Audit Events):

- Configured the system to **log critical audit events**, including user logins, system configurations, and data access.
- Set up **detailed logging policies** that capture all significant events, ensuring that any unauthorized actions or system changes are recorded for future analysis.

AU-6 (Audit Review, Analysis, and Reporting):

- Established a process to **regularly review and analyze audit logs** for signs of unauthorized activity or unusual access patterns.
- Set up an automated **alert system** that notifies security personnel if potential security incidents are detected based on log data.

AU-8 (Time Stamps):

- Configured **synchronized system clocks** to ensure that all logs contain accurate and consistent timestamps, providing reliable data for incident investigation and compliance reporting.

SC-12 (Cryptographic Key Establishment and Management):

- Implemented a **centralized key management system (KMS)** to manage the generation, distribution, and storage of cryptographic keys used for encrypting sensitive data.
- Ensured that keys were rotated regularly and protected using secure hardware modules.

SC-13 (Cryptographic Protection):

- Applied **strong encryption algorithms** (e.g., AES-256) to protect both data-at-rest (e.g., in databases) and data-in-transit (e.g., during transmission across networks).
- Implemented **SSL/TLS protocols** for encrypting communication channels, ensuring data confidentiality during transfer.

SC-28 (Protection of Information at Rest):

- Encrypted sensitive data on storage devices and within databases to ensure that information remains protected, even if physical devices are compromised.
- Utilized secure file systems and storage encryption technologies to safeguard data integrity and confidentiality.

IR-4 (Incident Handling):

- Developed a detailed **incident response plan (IRP)** that outlines procedures for identifying, containing, eradicating, recovering from, and following up on security incidents.
- Trained the security team on **incident handling protocols** to ensure rapid and efficient responses to incidents.

IR-5 (Incident Monitoring):

- Set up **24/7 monitoring systems** to continuously track system performance and detect potential incidents in real-time.
- Utilized **intrusion detection systems (IDS)** and **security information and event management (SIEM)** tools to monitor for suspicious activity.

IR-6 (Incident Reporting):

- Created a clear **incident reporting process** that defines who should be notified, the timeline for reporting, and what information should be included.
- Ensured that all incidents were logged and reported promptly to facilitate response and investigation.

SC-7 (Boundary Protection):

- Installed and configured **firewalls**, **intrusion prevention systems (IPS)**, and **network segmentation** to protect the internal network from external threats.
- Monitored network traffic and enforced policies to prevent unauthorized access through external interfaces.

SC-8 (Transmission Confidentiality and Integrity):

- Deployed **end-to-end encryption** and **secure communication protocols** to protect data in transit, ensuring confidentiality and integrity.

RMF EXAMPLE

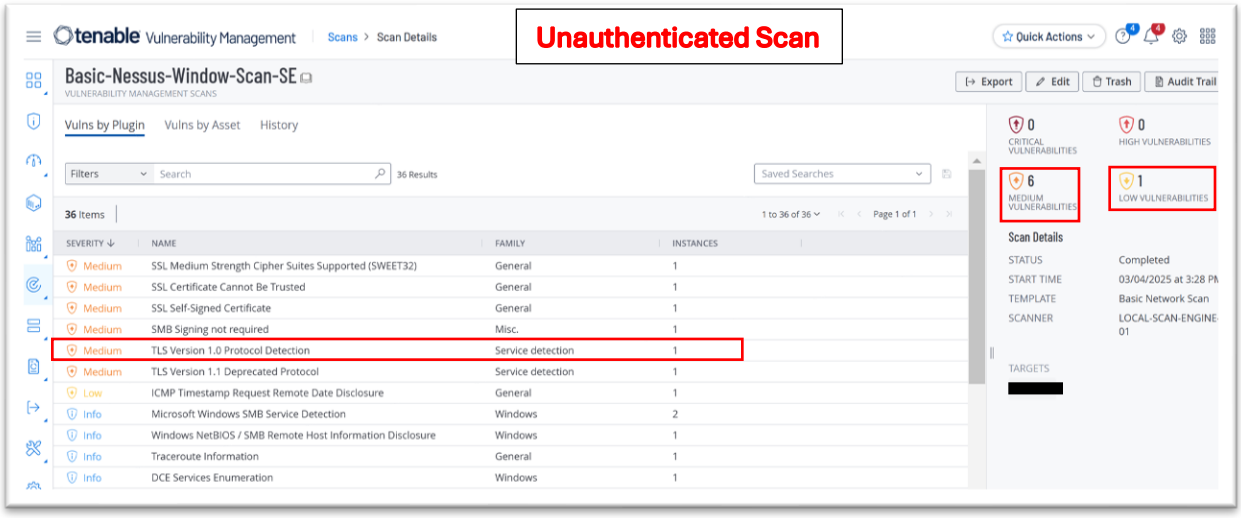
- Used **digital signatures** and **checksums** to verify the integrity of transmitted data.

ASSESSING SECURITY CONTROLS (STEP 4):

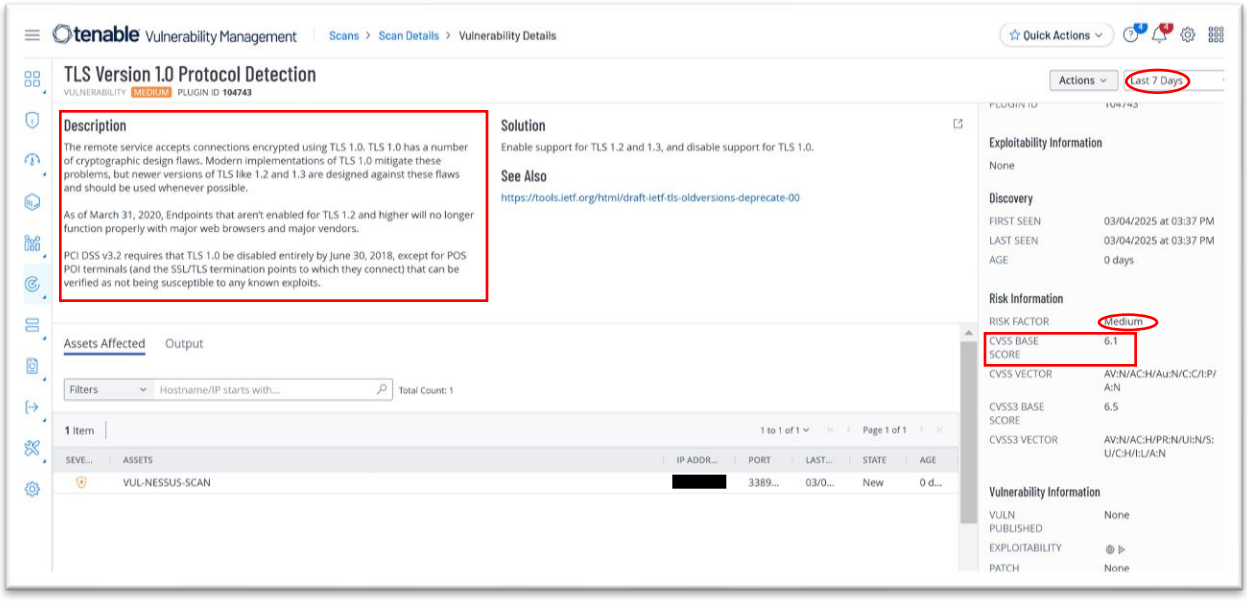
"The scans below does not accurately represent the implemented controls above. Its purpose is to demonstrate the vulnerability scanning process and how vulnerabilities are identified, recorded, and mitigated using Tenable (Nessus). The scan is conducted on a Windows Virtual Machine (VM) within Microsoft Azure and does not expose sensitive data."

After conducting an *unauthenticated scan*, a summary of the findings is displayed noting any low, moderate, or high severity vulnerabilities related to the security controls. I chose to identify a medium vulnerability to provide an example of assessing controls. The **TLS Version 1.0 Protocol Detection** vulnerability indicates that a system is using Transport Layer Security (TLS) 1.0, which is an *outdated and insecure* cryptographic protocol. TLS 1.0 has known security weaknesses, including susceptibility to attacks like **BEAST (Browser Exploit Against SSL/TLS)** and does not support modern encryption algorithms.

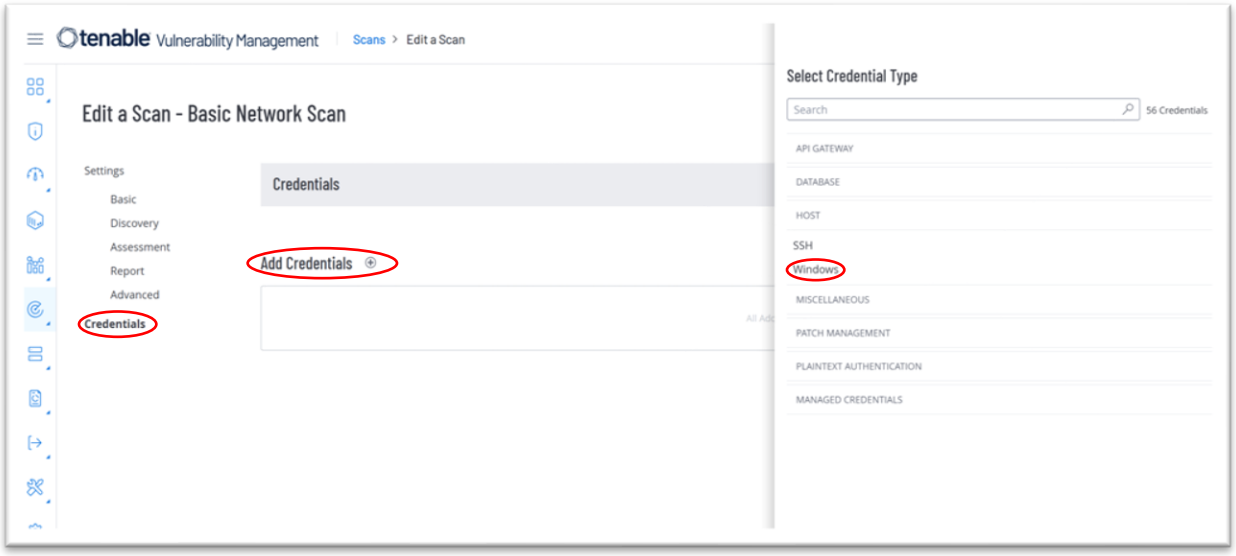
The outdated encryption identified in the System and Communications Protection (SC) controls—**SC-12** (Cryptographic Key Establishment and Management), **SC-13** (Cryptographic Protection), and **SC-29** (Package and Delivery of Information)—is assigned a medium severity rating with a **Common Vulnerability Scoring System (CVSS) score of 6.1**.



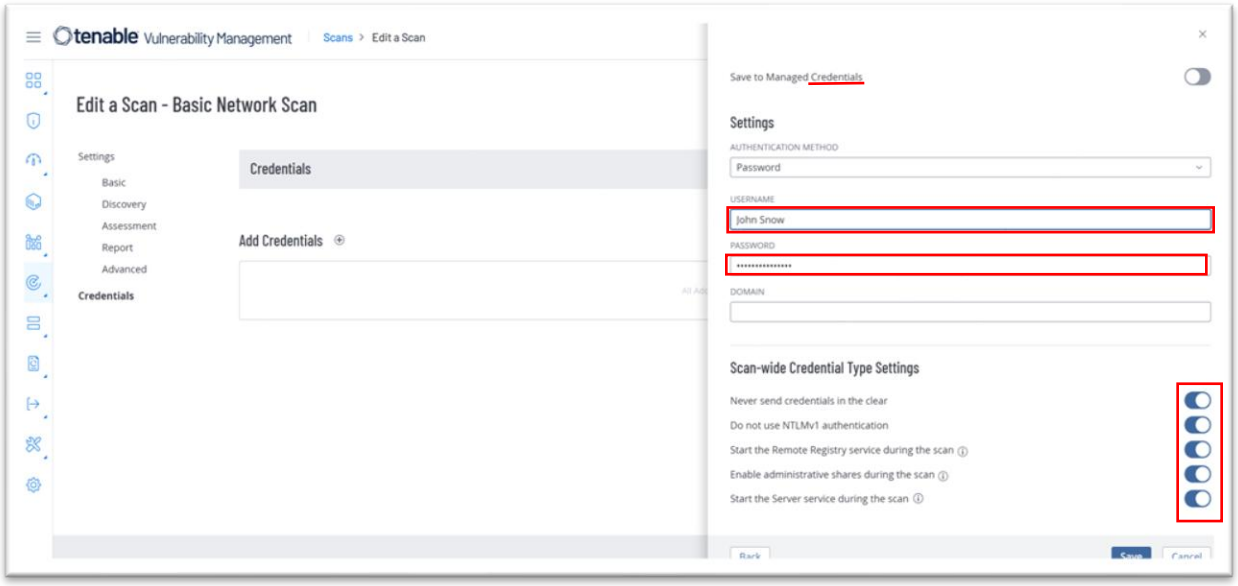
RMF EXAMPLE

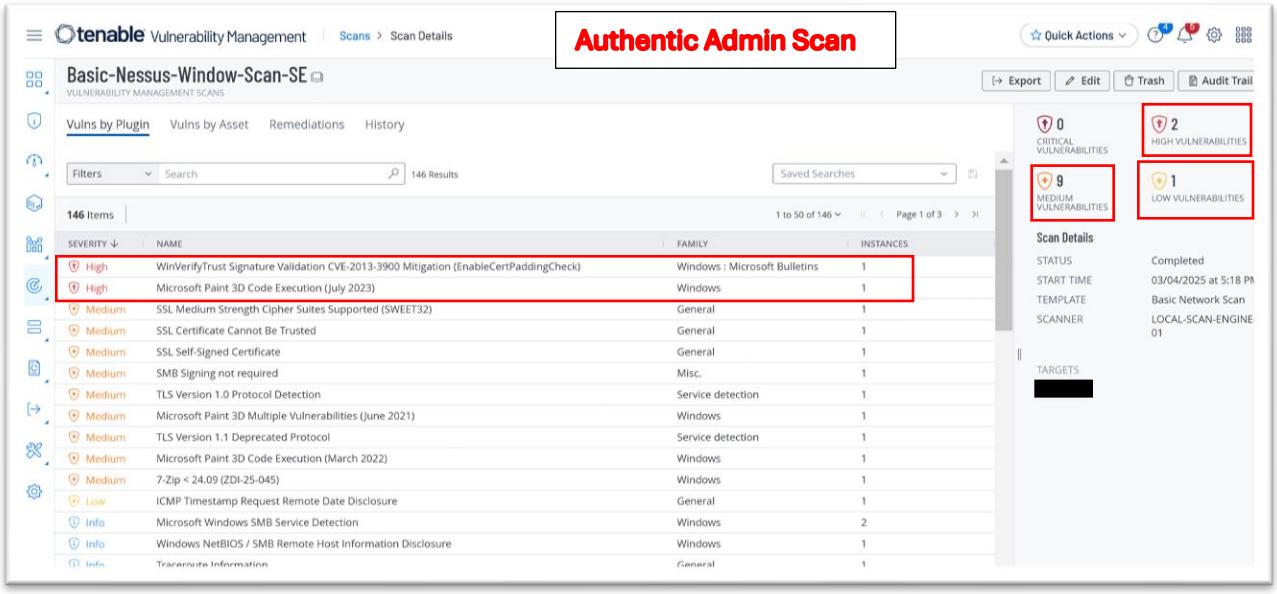


"The diagrams below illustrate the process of conducting an admin-authentic scan on a Windows system. This type of scan provides a more thorough search using administrative credentials. Additional high-severity vulnerabilities were identified and highlighted."

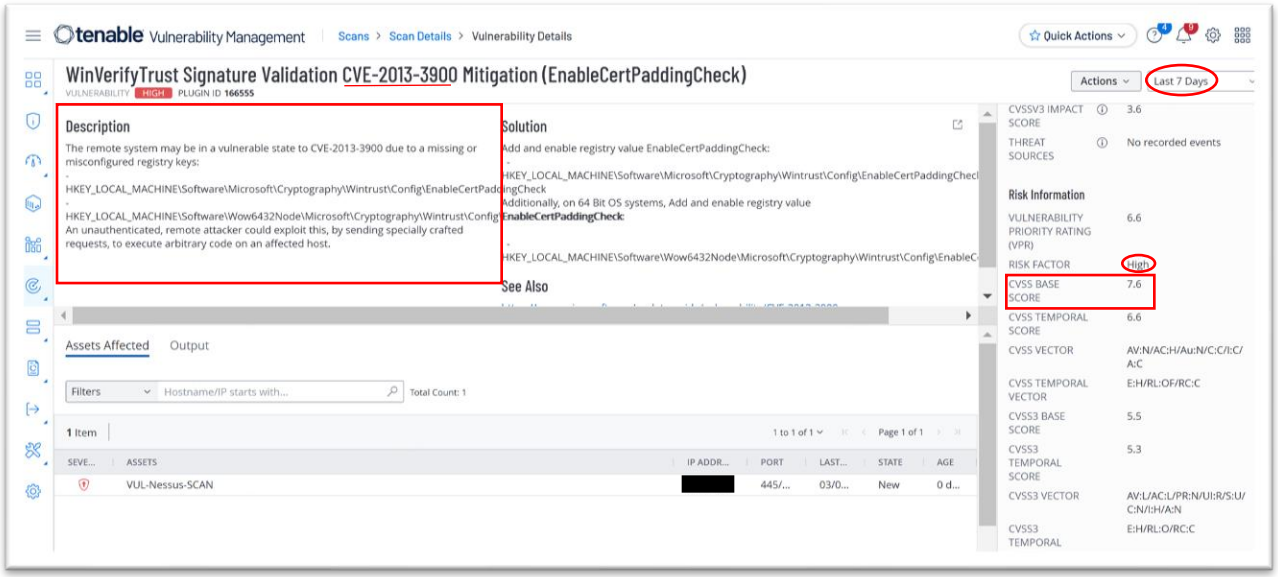


RMF EXAMPLE


tenable Vulnerability Management
Scans > Edit a Scan
Edit a Scan - Basic Network Scan
Settings
Basic
Discovery
Assessment
Report
Advanced
Credentials
Credentials
Add Credentials
Save to Managed Credentials
Settings
AUTHENTICATION METHOD
Password
USERNAME
John Snow
PASSWORD
DOMAIN
Scan-wide Credential Type Settings
Never send credentials in the clear
Do not use NTLMv1 authentication
Start the Remote Registry service during the scan
Enable administrative shares during the scan
Start the Server service during the scan


tenable Vulnerability Management
Scans > Scan Details
Authentic Admin Scan
Quick Actions
Basic-Nessus-Window-Scan-SE
VULNERABILITY MANAGEMENT SCANS
Export
Edit
Trash
Audit Trail
Vulns by Plugin
Vulns by Asset
Remediations
History
Filters
Search
146 Results
Saved Searches
146 Items
1 to 50 of 146
Page 1 of 3
SEVERITY
NAME
FAMILY
INSTANCES
High WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck) Windows : Microsoft Bulletins 1
High Microsoft Paint 3D Code Execution (July 2023) Windows 1
Medium SSL Medium Strength Cipher Suites Supported (SWEET32) General 1
Medium SSL Certificate Cannot Be Trusted General 1
Medium SSL Self-Signed Certificate General 1
Medium SMB Signing not required Misc. 1
Medium TLS Version 1.0 Protocol Detection Service detection 1
Medium Microsoft Paint 3D Multiple Vulnerabilities (June 2021) Windows 1
Medium TLS Version 1.1 Deprecated Protocol Service detection 1
Medium Microsoft Paint 3D Code Execution (March 2022) Windows 1
Medium 7-Zip < 24.09 (ZDI-25-045) Windows 1
Low ICMP Timestamp Request Remote Date Disclosure General 1
Info Microsoft Windows SMB Service Detection Windows 2
Info Windows NetBIOS / SMB Remote Host Information Disclosure Windows 1
0 CRITICAL VULNERABILITIES
2 HIGH VULNERABILITIES
9 MEDIUM VULNERABILITIES
1 LOW VULNERABILITIES
Scan Details
STATUS Completed
START TIME 03/04/2025 at 5:18 PM
TEMPLATE Basic Network Scan
SCANNER LOCAL-SCAN-ENGINE 01
TARGETS

RMF EXAMPLE



AUTHORIZATION PROCESS (STEP 5):

Below are the Authorization to Operate (ATO) package documents required to integrate systems into the working environment. These documents will be submitted to the Authorizing Official (AO) for a determination on whether to approve or deny system operation. These are key documents that will be part of the **ATO package**:

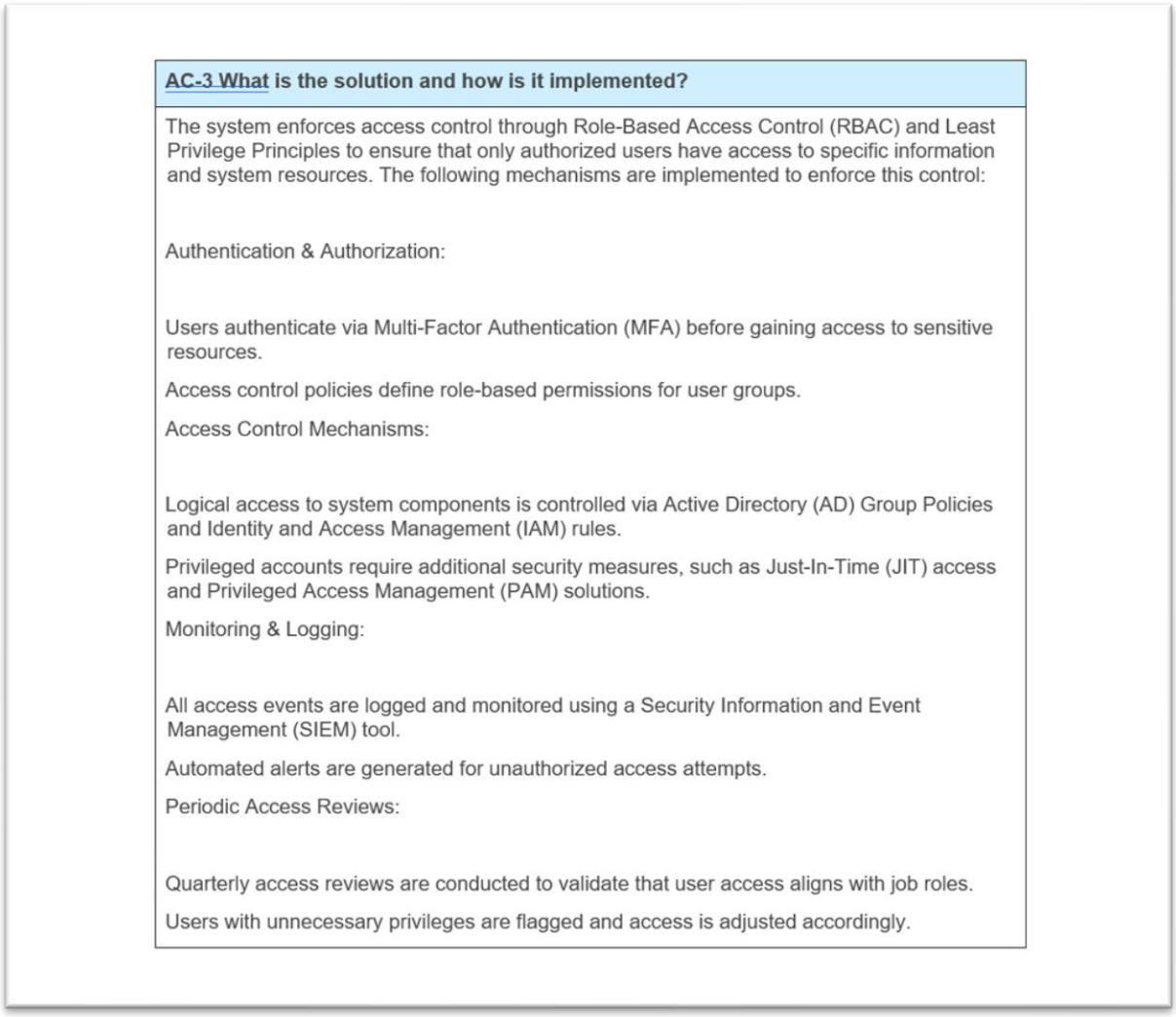
System Security Plan (SSP): detailed descriptions of the implemented controls. (**see below example**)

By implementing these access enforcement measures, the system ensures compliance with NIST 800-53 (AC-3) requirements. These security controls prevent unauthorized access, enforce least privilege, and enhance the system's overall security posture. Regular audits, monitoring, and access reviews ensure continuous compliance while mitigating risks associated with unauthorized system access.

RMF EXAMPLE

AC-3 Control Summary Information
Responsible Role: The system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. Access is granted based on role-based access control (RBAC) principles, ensuring that only authorized users can access specific system components, data, and administrative functions.
Implementation Status (check all that apply): ☒ Implemented ☐ Partially Implemented ☐ Planned ☐ Alternative implementation ☐ Not Applicable
Control Origination (check all that apply): ☐ Service Provider Corporate ☒ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for [Click here to enter text], Date of Authorization

RMF EXAMPLE



AC-3 What is the solution and how is it implemented?
The system enforces access control through Role-Based Access Control (RBAC) and Least Privilege Principles to ensure that only authorized users have access to specific information and system resources. The following mechanisms are implemented to enforce this control: Authentication & Authorization: Users authenticate via Multi-Factor Authentication (MFA) before gaining access to sensitive resources. Access control policies define role-based permissions for user groups. Access Control Mechanisms: Logical access to system components is controlled via Active Directory (AD) Group Policies and Identity and Access Management (IAM) rules. Privileged accounts require additional security measures, such as Just-In-Time (JIT) access and Privileged Access Management (PAM) solutions. Monitoring & Logging: All access events are logged and monitored using a Security Information and Event Management (SIEM) tool. Automated alerts are generated for unauthorized access attempts. Periodic Access Reviews: Quarterly access reviews are conducted to validate that user access aligns with job roles. Users with unnecessary privileges are flagged and access is adjusted accordingly.

The implementation status for **Access Enforcement (AC-3)** was marked as **"Implemented"** because the necessary access control measures are fully in place and actively enforced within the system. Since these controls are not in a planning or partial-implementation phase, marking them as implemented accurately represents the system's security posture.

The control origination was identified as **"Service Provider System Specific"** because access enforcement mechanisms, such as Active Directory Group Policies, Identity and Access Management (IAM) tools, and security monitoring solutions, are implemented and managed at the system level by the service provider.

In the **solution and implementation** section, details were provided to explain how access control mechanisms work in practice. RBAC was chosen to enforce the principle of least privilege by granting access based on job roles, ensuring that users only have the necessary permissions to perform their tasks.

RMF EXAMPLE

Security Assessment Report (SAR): is a formal document that outlines the results of a security assessment conducted on an information system. The purpose of the SAR is to evaluate how well the system's security controls are implemented and whether they meet the necessary standards and requirements, such as those defined by frameworks like NIST, FedRAMP and others. Key components of a SAR typically include:

1. **System Overview**: A brief description of the system being assessed, including its purpose, components, and environment.
2. **Assessment Scope and Methodology**: An outline of the assessment process, the security controls that were evaluated, and the tools or techniques used (e.g., vulnerability scanning, interviews, document reviews).
3. **Findings**: Detailed results of the assessment, including identified vulnerabilities, weaknesses, or gaps in the security controls. This section often includes the **CVSS** (**Common Vulnerability Scoring System**) score to provide context for the severity of each issue.
4. **Recommendations**: Actions or steps to mitigate identified vulnerabilities or improve security posture, along with priority levels for remediation.
5. **Risk Determination**: An analysis of the risks associated with the findings and their potential impact on the system's confidentiality, integrity, and availability.
6. **Compliance Status**: A determination of whether the system meets the applicable security requirements and regulations (e.g., NIST 800-53).
7. **Authorization**: In some cases, the SAR is used to support the decision of an Authorizing Official (AO), who will review the report and determine whether the system can continue operating or if corrective actions are necessary.

Although this document is not included here, during an external audit, the Security Control Assessor (SCA) would provide the Security Assessment Report (SAR) to the System Owner for inclusion in the ATO packet.

Plan of Actions and Milestones (POA&M): addresses the vulnerabilities or weaknesses identified in the scan. (**see attachment example**)

The **Authorizing Official (AO)** plays a critical role in the Risk Management Framework (RMF) and the overall cybersecurity process. The AO is typically a senior executive or designated individual within an organization responsible for the authorization of an information system to operate.

The AO is responsible for ensuring that a system operates in a secure manner, mitigating potential risks to an acceptable level. They rely on the findings from security assessments, including vulnerability scans and control assessments, to make an informed decision. After thoroughly reviewing the security posture, the AO grants or denies the Authorization to Operate

(ATO), ultimately accepting responsibility for the residual risks associated with the system's operation. ***(See attached approval letter example)***

CONTINUOUS MONITORING (STEP 6)

Objective:
To ensure the ongoing security and integrity of moderate systems through regular vulnerability scans, real-time event monitoring, and proactive identification of security risks.

Continuous monitoring is crucial for maintaining the security of systems. By regularly conducting vulnerability scans, implementing SIEM tools, and maintaining awareness with real-time event monitoring and audit logs, organizations can effectively detect and mitigate security risks to ensure ongoing protection. Security event monitoring and real-time alerts are essential for identifying and addressing any unauthorized access attempts, keeping the system secure and compliant. Here are a few key action steps for conducting continuous monitoring:

1. Schedule Regular Vulnerability Scans Using Tenable Nessus

Action Steps:

1. **Determine Frequency:**
    - Schedule vulnerability scans on a monthly or quarterly basis, depending on the system's risk profile and security needs. More frequent scans may be required if the system undergoes frequent changes or if new vulnerabilities are regularly identified.

2. **Configure Nessus:**
    - Set up Tenable Nessus to scan all **critical** assets within the moderate system environment, including network devices, servers, and endpoints.

    - Ensure that Nessus is configured to scan for known vulnerabilities, misconfigurations, and outdated software.

3. **Automate Scan Reports:**
    - Set up automated reporting within Nessus to generate vulnerability scan results upon completion of each scan.

    - Configure Nessus to track new vulnerabilities identified in each scan and compare them with the results from previous scans to determine trends or recurring issues.

4. **Review and Action:**
    - Designate a security team member to review scan results within **24 hours** of each scan.

    - Document all identified vulnerabilities and prioritize them for remediation based on severity and impact.

2. Implement Additional Monitoring Tools for Security Information and Event Management (SIEM)

Action Steps:

1. **SIEM Integration:**
   - If applicable, integrate Security Information and Event Management (SIEM) tools with the system to collect and analyze security event logs from all **critical** components (e.g., servers, network devices, firewalls).

   - Ensure the SIEM tool is configured to log events such as **authentication attempts**, **privilege escalations**, and **access to sensitive data**.

2. **Real-Time Alerts:**
   - Configure the SIEM system to provide **real-time alerts** for any suspicious activities or security events, including unauthorized access attempts or the detection of malware.

   - Set thresholds for alert severity to prioritize response actions based on the criticality of the event.

3. **Monitor Logs Continuously:**
   - Continuously monitor security event logs **for patterns** indicative of potential security incidents (**e.g., repeated failed login attempts, unrecognized devices accessing the network**).

   - Set up automated processes for investigating any alerts generated by the SIEM.

3. Ongoing Observation for System Security

Action Steps:

1. **Continuous Monitoring Culture:**
   - Reinforce the importance of ongoing observation in system security by training staff and stakeholders on the role of continuous monitoring.

   - Regularly review policies and procedures to ensure that monitoring activities are aligned with industry's best practices and organizational security requirements.

2. **Incident Response Readiness:**
   - Ensure that the security team is prepared to respond to any security events detected during the continuous monitoring process, including escalating incidents to the appropriate personnel or external responders if necessary.

3. **System Configuration Reviews:**
    - Conduct periodic reviews of system configurations to ensure compliance with security policies and to identify any potential weaknesses or areas for improvement.

4. Role of Security Event Monitoring, Audit Logs, and Real-Time Alerts

Action Steps:

1. **Security Event Monitoring:**
    - Continuously monitor security events using the configured SIEM or similar monitoring tools to detect any unusual activity that could indicate an attack or security breach.

    - Key events to monitor include unauthorized access attempts, privilege escalation, failed login attempts, and unusual network traffic patterns.

2. **Audit Logs:**
    - Enable audit logging across all system components to provide a detailed record of all user and system activities. This includes login attempts, system modifications, file access, and any administrative changes.

    - Regularly review audit logs to identify potential policy violations, security breaches, or operational inefficiencies.

3. **Real-Time Alerts for Unauthorized Access Attempts:**
    - Set up real-time alerts for unauthorized access attempts, such as incorrect login credentials, accessing restricted files, or attempts to bypass security controls.

    - Immediately respond to unauthorized access attempts by investigating the source, impact, and taking corrective action, such as locking accounts or disabling access points.

4. CONCLUSION

The **Risk Management Framework (RMF)** is a structured process used to manage security and risk for information systems. For a **moderate impact system**, the RMF process typically involves the following key steps:

1. **Categorize the System**:
    - The system is categorized based on its potential impact (**moderate in this case**), considering factors like confidentiality, integrity, and availability.

2. **Select Security Controls**:

RMF EXAMPLE

- Appropriate security controls are selected from the **NIST 800-53 framework**, tailored to the system's risk level and requirements, with a focus on mitigating risks effectively.

3. **Implement Security Controls**:
   - The selected security controls are implemented across the system to ensure that vulnerabilities are mitigated, and risks are addressed.

4. **Assess Security Controls**:
   - A thorough assessment is conducted to determine if the security controls are functioning as intended. This involves vulnerability scanning and other evaluation methods.

5. **Authorize the System**:
   - An **Authorization to Operate (ATO)** is granted by the Authorizing Official (AO) once the system's security posture has been reviewed and is deemed acceptable, considering any residual risks.

6. **Monitor Security Posture**:
   - Continuous monitoring is crucial for identifying emerging vulnerabilities and ensuring the system remains secure. This involves periodic vulnerability scans, system audits, and real-time event monitoring.

Importance of Robust Security Controls, Vulnerability Scanning, and Continuous Monitoring

For a **moderate impact system**, it is essential to establish robust security controls, conduct regular vulnerability scanning, and maintain continuous monitoring to safeguard against evolving threats. Strong security controls ensure that risks are mitigated, while vulnerability scanning helps identify potential weaknesses in the system before they can be exploited. Continuous monitoring plays a key role in ensuring that security remains effective over time, detecting any new threats and enabling timely response actions.

By proactively identifying vulnerabilities, addressing system weaknesses, and continuously monitoring for suspicious activities, an organization can maintain a strong security posture and minimize the likelihood of a breach.

The use of **Tenable Nessus** greatly enhances the security posture of a moderate impact system. Nessus conducts thorough vulnerability scans to identify potential risks such as misconfigurations, unpatched vulnerabilities, and compliance gaps. By regularly running Nessus scans, security teams can pinpoint areas of concern before they become critical, ensuring that vulnerabilities are addressed in a timely manner.

In addition, Nessus helps organizations maintain **compliance with security standards**, such as those outlined in NIST 800-53 and other relevant frameworks. Its ability to track vulnerabilities

over time, compare results with previous scans, and automate reporting contributes to a more efficient security management process, ensuring that the system adheres to the required security guidelines and remains resilient against potential threats.

5. REFERENCES

Relevant sources:

NIST 800-53 (Security and Privacy Controls)

FedRAMP Moderate Baseline (snapshot example)

FIPS 199 (System Impact Levels)

FedRAMP System Security Plan (SSP) (snapshot example)

Tenable Nessus Documentation (snapshot example)

FedRAMP POA&M Template

FedRAMP Authorization Official Letter example

Websites:

https://www.fedramp.gov/documents-templates/

https://www.first.org/cvss/

https://cloud.tenable.com/

https://portal.azure.com