Technical Writing and Documentation Report

1. Introduction

In this project, I set out to demonstrate my ability to create clear, comprehensive technical documentation for cybersecurity processes. I developed a cybersecurity procedure for a specific security control, documented a step-by-step process for patch management, crafted detailed incident response playbooks for two common scenarios, and built a structured knowledge base repository for ongoing reference. This report serves as both a practical guide and a living document to support our cybersecurity operations.

2. Cybersecurity Procedure Document

2.1. Security Control Implementation: Endpoint Firewall Configuration

Purpose:

To implement a standardized endpoint firewall configuration that minimizes unauthorized access and reduces the overall attack surface of our workstations and servers.

Scope:

This procedure applies to all corporate-owned endpoints (e.g., Windows, Linux, and macOS systems).

Procedure:

1. **Identify Approved Services and Ports**

- **Collaboration:** Work with application owners and network teams to identify which services need to be accessible (e.g., HTTPS on TCP 443, RDP on TCP 3389).

- **Documentation:** Record all approved ports and services, noting any exceptions required for legacy applications.

2. **Configure Inbound and Outbound Rules**

- **Inbound Rules:**

- Set a default-deny rule for all inbound traffic.

- Create explicit allow rules only for necessary services (e.g., permit HTTPS and RDP as needed).

- **Outbound Rules:**

- Generally allow outbound traffic but block access to known malicious IP ranges and non-essential services (e.g., unauthorized file-sharing protocols).

3. **Enable Logging and Alerting**

- **Logging:** Enable logging for both inbound and outbound traffic to capture any connection attempts.

- **Alerting:** Configure alerts for repeated failed access attempts or traffic on high-risk ports.

4. **Test and Validate**

- **Verification:** Use network scanning tools (such as Nmap) to verify that only the approved ports are open.

- **Review:** Document any discrepancies and adjust rules as necessary.

5. **Ongoing Maintenance**

- **Review Cycle:** Conduct quarterly reviews to ensure firewall rules remain aligned with current business requirements and emerging threats.

- **Updates:** Update the approved services list and adjust firewall configurations based on new applications or changes in the threat landscape.

3. Process Documentation: Patch Management Step-by-Step Guide

Effective patch management is critical to maintaining system security. Below is my documented step-by-step guide for patch management:

1. **Inventory and Assessment**

- **Asset Listing:** Compile an up-to-date inventory of all systems, including servers, workstations, and network devices.

- **Criticality Assessment:** Rank systems based on their importance and exposure to risk.

2. **Patch Acquisition**

- **Monitoring Sources:** Subscribe to vendor notifications and security bulletins (e.g., Microsoft, Linux distributions) to stay informed of new patches.

- **Verification:** Check patch authenticity using checksums or digital signatures provided by the vendor.

3. **Testing in a Staging Environment**

- **Deployment:** Apply patches in a non-production environment to evaluate potential impacts.

- **Compatibility:** Run critical applications and services to confirm that the patch does not introduce any issues.

4. **Deployment to Production**

- **Scheduling:** Schedule patch deployments during approved maintenance windows to minimize disruption.

- **Automated Deployment:** Use patch management tools (e.g., WSUS, SCCM, or Ansible) to roll out updates across systems.

- **Manual Installation:** For specialized or smaller systems, perform manual patch installation while documenting each step.

5. **Verification and Reporting**

- **Post-Deployment Checks:** Verify that systems are operating normally after patch deployment by running health checks.

- **Documentation:** Generate and review a patch compliance report, noting any systems that require follow-up.

6. **Continuous Improvement**

- **Review Process:** Analyze any patch failures and update the patch management process as necessary.

- **Feedback Loop:** Incorporate lessons learned into future patch cycles and schedule regular training sessions.

4. Security Playbooks

Security playbooks provide a detailed response plan for handling incidents. I have developed two playbooks to guide the response to common security events.

4.1. Playbook 1: Malware Infection (Endpoint)

Scenario: A workstation exhibits signs of malware infection, such as random pop-ups, unexpected behavior, or performance degradation.

Steps:

1. **Detection and Verification**

- **User Report:** The user notifies the SOC about unusual behavior.
- **Initial Analysis:** SOC Analyst reviews system logs and endpoint protection alerts to confirm the presence of malware.

2. **Containment**

- **Isolation:** Disconnect the affected system from the network immediately to prevent lateral movement.
- **Account Measures:** If necessary, reset credentials for the user or disable accounts associated with suspicious activity.

3. **Eradication**

- **Malware Removal:** Run antivirus/EDR tools to clean the system. If malware persists, re-image the system from a known good backup.
- **Forensic Analysis:** Collect evidence for further analysis and to identify the malware vector.

4. **Recovery**

- **System Restoration:** Restore any affected data from backups and ensure the system is fully patched.
- **Verification:** Validate that the system is functioning normally and monitor for any residual signs of infection.

5. **Lessons Learned**

- **Root Cause Analysis:** Determine how the malware infiltrated the system.
- **Policy Update:** Update security policies or user training materials to prevent recurrence.

4.2. Playbook 2: Phishing Email Incident

Scenario: Multiple users report receiving phishing emails prompting for login credentials or containing malicious links.

Steps:

1. **Detection and Verification**

- **User Reports:** Employees forward suspicious emails to the SOC.

- **Analysis:** SOC Analyst examines email headers, links, and attachments for indicators of compromise.

2. **Containment**

- **Block Sender:** Update the email filtering system to block emails from the malicious sender's domain.

- **Isolate Affected Accounts:** If any user credentials are compromised, immediately reset passwords and enforce multi-factor authentication.

3. **Eradication**

- **Remove Phishing Emails:** Clean up affected inboxes using automated scripts or email server tools.

- **Threat Intelligence:** Share indicators of compromise with threat intelligence teams and update detection rules.

4. **Recovery**

- **User Communication:** Issue a company-wide notification and provide phishing awareness training.

- **Monitoring:** Increase monitoring for any signs of credential misuse or related suspicious activity.

5. **Lessons Learned**

- **Filter Improvement:** Refine email filtering rules and update blacklists based on the incident.

- **Policy Enhancement:** Enhance policies related to email usage and conduct regular phishing simulation exercises.

5. Knowledge Base Management

To support our ongoing cybersecurity efforts, I established a structured document repository with categorized resources. This knowledge base enables quick access to key reference materials and guides.

5.1. Repository Structure

1. **Policies and Procedures**

- **Access Control Policy**

- **Data Protection Policy**
- **System Use Policy**
- **Endpoint Firewall Configuration Procedure** (detailed above)

2. **Tools and Technical Guides**

- **Wireshark User Guide:** Instructions on capturing and analyzing network traffic.
- **Patch Management Guide:** Detailed process documentation for patch deployment.
- **Vulnerability Scanning Manual:** Step-by-step guide for using tools like Nessus or OpenVAS.

3. **Incident Response and Playbooks**

- **Malware Infection Playbook** (outlined above)
- **Phishing Email Playbook** (outlined above)
- **Incident Reporting Template:** Standardized form for documenting incidents and tracking remediation steps.

5.2. Access and Maintenance

- **Location:** The repository is hosted on our secure internal SharePoint site, accessible only to authorized personnel.
- **Version Control:** Each document is version-controlled, with a detailed change log to track updates and revisions.
- **Review Cycle:** Quarterly reviews are scheduled to ensure all documents remain current and reflective of our evolving security landscape.

6. Conclusion

Through this project, I have demonstrated my ability to produce detailed and structured technical documentation in the cybersecurity domain. I developed a clear procedure for implementing endpoint firewall controls, provided a step-by-step guide for patch management, created actionable incident response playbooks for malware and phishing incidents, and organized a comprehensive knowledge base for ongoing reference.

This documentation not only meets the rubric requirements but also serves as a practical guide for implementing and maintaining our cybersecurity controls. It will be continually updated and refined as part of our commitment to continuous improvement in security operations.