Producing Effective Security Documentation

In this project, I developed a comprehensive set of security documentation for a cybersecurity operations framework. This documentation included clear and actionable guides for firewall configurations, patch management procedures, detailed incident response playbooks, and an organized knowledge base repository.

1. Cybersecurity Procedure Document: Firewall Configuration & Implementation

The first security control I focused on was implementing a **network firewall** to secure ingress and egress traffic, reducing the firm's external attack surface. The firewall control is essential for segmenting the network and enforcing access control policies at the network layer.

📘 **Document Highlights:**

- **Objective:** Deploy and configure a firewall to ensure secure communication and protect the internal network from external threats.
- **Tools Used:** pfSense firewall appliance
- **Detailed Steps:**
  1. **Physical Installation:**
     - Install the pfSense firewall hardware and connect it to the internal network and the internet-facing router.
     - Ensure all interfaces are connected to appropriate internal and external segments.
  2. **Interface Configuration:**
     - Configure LAN and WAN interfaces with static IP addressing and set up the internal and external routing rules.
  3. **Defining Access Control Rules:**
     - Create rules to allow HTTP/S and DNS traffic from external clients to internal web servers.
     - Block all inbound traffic from non-approved IP ranges, particularly from countries identified as high-risk.
     - Set up rules that limit outbound traffic to only authorized destinations.
  4. **Geo-Blocking:**
     - Use pfSense’s geo-blocking feature to restrict access from countries deemed high-risk for cyber threats, such as North Korea or Russia.
  5. **Logging and Monitoring:**
     - Configure logging for all dropped packets to alert network administrators of potentially suspicious activity.
     - Set up real-time alerts for critical events such as port scans, denial-of-service (DoS) attacks, or unauthorized login attempts.

6. **Testing and Verification:**
    - Conduct simulated traffic tests from blocked regions to verify that the geo-blocking works as intended.
    - Verify that the logging and alerting systems are functioning by triggering intentional drops and confirming the alerts are sent to the Security Operations Center (SOC).

- **Outcome:** The procedure document was successfully implemented and ensured that the firewall provided an added layer of protection to the financial records and internal resources.

2. Process Documentation: Patch Management Procedure

The next part of the documentation involved detailing a **patch management process** to ensure all systems, applications, and devices within the network remain secure and up-to-date. Keeping systems patched is crucial for defending against known vulnerabilities and minimizing the risk of exploits.

🛠️ **Patch Management Guide:**

- **Title:** Patch Management Standard Operating Procedure (SOP)
- **Frequency:** Patches will be reviewed weekly, with a monthly patching window designated for deployment.
- **Detailed Steps:**
    1. **Vendor Bulletins and Patch Identification:**
        - Monitor patch release notifications from major vendors (e.g., Microsoft, Adobe, Cisco, etc.) via official channels.
        - Subscribe to mailing lists and threat intelligence feeds to stay informed about critical patches and zero-day vulnerabilities.
        - Review security advisory bulletins and identify which patches are applicable for the organization's environment.
    2. **Approval and Scheduling:**
        - Log into the internal **Windows Server Update Services (WSUS)** platform to review and approve patches.
        - Schedule patch installation during a dedicated window (Sunday 2–5 AM) to minimize user disruption.
        - Coordinate with department heads to notify them about any expected downtime.
    3. **Test Patching:**
        - Select a random subset (1-5% of systems) to apply the patches to and monitor for any failures or incompatibility issues.
        - Track all issues through a ticketing system and resolve them before proceeding with the broader rollout.
        - Conduct additional tests if necessary for high-risk patches.
    4. **Deployment:**
        - Use **Group Policy** or **System Center Configuration Manager**

(SCCM) to deploy the patches to all systems.
    - Ensure that devices on the network are automatically updated, particularly security-critical systems like servers and admin workstations.
5. **Reporting and Documentation:**
    - After deployment, generate and review patch installation reports to identify failures or systems that missed the patch cycle.
    - Review error logs to ensure that no significant issues occurred and that all patches were applied successfully.
    - Create a patching log that contains details on all updates applied, the systems affected, and any issues found.
6. **Post-Deployment Testing:**
    - Perform post-patching testing to confirm that critical systems and services (e.g., file servers, web servers) are functioning correctly.
    - Conduct vulnerability scans to ensure that known vulnerabilities have been addressed.

- **Outcome:** The patch management process ensures that all systems are maintained with the latest security patches, reducing exposure to vulnerabilities and maintaining system stability.

3. Security Playbooks: 2 Incident Response Scenarios

Security playbooks are critical for ensuring that teams can effectively and quickly respond to security incidents. Below are two detailed incident response playbooks I created to address potential cybersecurity threats.

🎮 **Playbook 1: Ransomware Detection**

Ransomware remains a significant threat to organizational data, often resulting in encryption of critical files and demanding a ransom for decryption. This playbook focuses on how to respond if ransomware is detected on the network.

- **Detection Method:** The company's Endpoint Detection and Response (EDR) software identifies the unauthorized encryption of multiple files across several machines in a short time window.
- **Incident Response Steps:**
    1. **Immediate Action:**
        - **Isolate the affected machine(s)** from the network to stop the spread of ransomware. Disconnect these machines from the internal network and disable Wi-Fi connections.
        - **Notify the Security Operations Center (SOC)** team, executive leadership, and IT to begin coordinating the response.
    2. **Containment:**
        - Perform a network-wide scan to identify any additional infected systems.
        - Apply network-wide segmentation to isolate critical systems.

3. **Backup Activation:**
    - Immediately **activate backup systems** to restore critical data from the latest secure backups.
    - Prioritize restoring key systems (e.g., accounting, HR) that are essential for business continuity.
4. **Forensics and Recovery:**
    - Perform a forensic analysis to determine the attack vector, spread pattern, and other relevant details.
    - **Investigate ransomware strain** and confirm whether it is known or custom-built. This will help determine the next steps for decryption or remediation.
    - If available, **use decryption tools** or recover files from backup.
5. **Documentation and Reporting:**
    - Document the **Indicators of Compromise (IOCs)** (IP addresses, file hashes, etc.) and share them with the threat intelligence community.
    - Submit a formal report to legal, compliance, and external authorities (if necessary).
    - Conduct a **post-incident review** with all stakeholders to discuss lessons learned.
6. **Preventative Measures:**
    - Enhance **email filtering** to prevent phishing attempts.
    - Enforce **user training** on recognizing malicious attachments and links.
    - Update **antivirus signatures** and endpoint security protocols to detect newer ransomware strains.

- **Outcome:** A complete recovery process that minimized downtime and contained the ransomware without paying the ransom.

🕵️ Playbook 2: Insider Threat – Data Exfiltration

Insider threats involve malicious or negligent actions by employees who may leak or steal sensitive data. This playbook outlines steps to respond to data exfiltration attempts.

- **Detection Method:** A Data Loss Prevention (DLP) system triggers an alert after detecting unauthorized file transfers to cloud storage services, such as Dropbox or Google Drive, outside of the company's approved methods.
- **Incident Response Steps:**
    1. **Immediate Action:**
        - **Lock the user account** immediately and ensure the user cannot access sensitive systems or perform further actions.
        - **Preserve logs and system records** of all the user's activity during the time of the suspected data exfiltration.

2. **Investigation:**
    - **Review user activity logs** and capture screenshots of any evidence pointing to the exfiltration.
    - Conduct an **interview with the user** to understand the context and intent of the activity.
3. **Mitigation:**
    - **Notify HR and legal teams** to begin reviewing any potential misconduct or policy violations.
    - **Audit affected data** to determine the scope of the exfiltration and whether any sensitive information was disclosed.
4. **Documentation and Reporting:**
    - Create an internal report for senior leadership detailing the exfiltration attempt, including the user involved, data affected, and any evidence found.
    - Ensure all findings are documented for compliance and regulatory purposes.
5. **Follow-Up Actions:**
    - If the exfiltration was accidental, update security protocols to prevent similar incidents in the future.
    - Review **employee monitoring practices** and ensure proper security awareness training for all staff.
6. **Security Enhancement:**
    - Enforce **stronger access controls** and ensure that **least-privilege access** is implemented for all users.
    - **Enhance DLP policies** to provide more detailed alerts and proactive blocking of suspicious file transfers.

- **Outcome:** Swift action prevented further data loss and allowed the team to mitigate any damage.

4. Knowledge Base Management

The cybersecurity documentation repository is structured to ensure easy access to vital procedures, guides, and reference materials for the team. This repository is continuously updated and serves as a central hub for cybersecurity information.

📚 **Repository Overview:**

- **Category 1: Procedures**
    - *Firewall Implementation and Configuration*
    - *MFA Setup Guide*
    - *Email Filtering Policy*
- **Category 2: Process Guides**
    - *Patch Management SOP*
    - *Incident Reporting Form*
    - *Account Provisioning Checklist*

- **Category 3: Reference Materials**
    - *NIST SP 800-53 Summary Sheet*
    - *ISO 27001 Compliance Checklist*
    - *Common Cybersecurity Acronyms*

The repository is stored on the company's internal SharePoint and includes version control to track updates over time. The documentation is also indexed to ensure quick searchability and to provide the team with the information they need during high-pressure incidents.