🛡️ Effective Security Documentation Report

🔒 Executive Summary

This report demonstrates the development of professional security documentation, including a cybersecurity procedure document, a process step-by-step guide, security playbooks for incident response scenarios, and a knowledge base structure for organized cybersecurity resources. All sections use structured technical writing standards and mock data where needed to simulate a real-world environment.

---

1. 📜 Technical Writing: Cybersecurity Procedure Document

Document Title:
Firewall Configuration Procedure for Web Servers

Purpose:
To standardize the process of securing public-facing web servers with proper firewall configurations.

Procedure:

Step	Action
1	Access the web server via SSH using administrator credentials.
2	Verify existing firewall status: `sudo ufw status verbose`
3	Set default policies: `sudo ufw default deny incoming`

	`sudo ufw default allow outgoing`
4	Allow essential ports: `sudo ufw allow 22/tcp` (SSH) `sudo ufw allow 80/tcp` (HTTP) `sudo ufw allow 443/tcp` (HTTPS)
5	Enable firewall: `sudo ufw enable`
6	Verify rules: `sudo ufw status numbered`
7	Document changes and notify IT Security for audit recording.

✅ Clear and direct instructions help ensure consistent firewall configuration across all production web servers.

---

2. 📋 Process Documentation: Step-by-Step Guide

Document Title:
Incident Reporting Procedure for Employees

Step-by-Step Guide:

Step	Action
1	**Identify the Incident**: Recognize signs of suspicious activity (e.g., phishing emails, unauthorized access).
2	**Immediate Reporting**: Report the incident within 15 minutes using the "Security Incident Report Form" available on the intranet.
3	**Contact Security Team**: Call the SOC hotline: `1-800-SECURE-01`
4	**Preserve Evidence**: Do not delete suspicious emails, files, or close programs that may hold evidence.

5	**Await Instructions**: Follow directions provided by the IT Security team regarding further action.
6	**Follow-Up**: Cooperate in post-incident investigations if requested.

✅ This ensures quick and effective communication of incidents, minimizing organizational risk.

---

3. 📚 Security Playbooks

Title:
Security Incident Response Playbooks

🔹 Incident Scenario 1: Malware Infection

Objective: Contain and remove malware infection on an endpoint.

Step	Action
1	Isolate the infected machine from the network immediately.
2	Capture system memory and disk images for forensics (`dd`, `volatility`).
3	Identify malware through antivirus and sandbox analysis.
4	Remove malware and rebuild the system if necessary.
5	Review and update endpoint protection signatures.
6	Conduct a post-incident review and update incident logs.

🔹 Incident Scenario 2: Phishing Email Detected

Objective: Respond to and contain a phishing email attack.

Step	Action

1	Quarantine the phishing email from user inboxes using email gateway tools.
2	Analyze email headers and attachments in a sandbox environment.
3	Notify users who received the email about the phishing attempt.
4	Block malicious domains/IPs at the firewall and proxy levels.
5	Conduct phishing awareness reinforcement training.
6	Document incident details and outcomes in incident management system.

✅ Playbooks help ensure that incident response is **consistent, documented, and repeatable**.

---

4. 📂 Knowledge Base Management

Knowledge Base Title:
Company X Cybersecurity Reference Repository

Repository Structure:

Category	Contents	Example Resource
Policies and Procedures	Security policies, acceptable use policies, system hardening guides.	*Access Control Policy v2.0*
Incident Response	Incident playbooks, incident reporting templates, chain of custody forms.	*Phishing Incident Response Playbook*
Threat Intelligence and Tools	Threat bulletins, common vulnerabilities and exposures (CVEs), tool usage manuals (Wireshark, OSSEC).	*Wireshark Basics Guide*

Mock Evidence: Repository Screenshot Example (Folder Structure)

text
CopyEdit

```
/Knowledge_Base
   ├── Policies_Procedures
```

```
|    └── Access_Control_Policy_v2.0.pdf
├── Incident_Response
|    └── Phishing_Response_Playbook.pdf
└── Threat_Intelligence_Tools
     └── Wireshark_Basics_Guide.pdf
```

✅ Organized documentation ensures rapid access to critical cybersecurity resources when needed.

📎 Appendix

Mock Tools Used:

- OSSEC (alert examples)
- UFW (firewall rules and logs)
- Wireshark (sandbox analysis for phishing attachments)
- Git for documentation version control

🟢 Final Notes

Through clear technical writing, structured procedures, well-prepared playbooks, and organized knowledge management, this project fulfills industry best practices for cybersecurity documentation, aligning with real-world SOC and IT Security operations.