

# Implement and Explain Advanced Cybersecurity Defense Strategies

## 1. Application of Zero Trust Architecture

To enforce Zero Trust Architecture, access controls were applied across the following two security layers:

### Network Layer

- Implemented network segmentation using VLANs and firewalls with strict Access Control Lists (ACLs).
- Deployed Intrusion Detection and Prevention Systems (IDPS) to monitor and block unauthorized traffic.
- Established a VPN with strict authentication to ensure encrypted remote access.

### Data Layer

- Enforced encryption for sensitive data at rest and in transit.
  - Implemented Data Loss Prevention (DLP) controls to prevent unauthorized data exfiltration.
  - Applied strict access control and classification policies to regulate data access and handling.
- .
- 

## 2. Defense in Depth Implementation

Three distinct layers of security were implemented to establish a Defense in Depth strategy:

### Perimeter Security

- Firewalls were configured to filter incoming and outgoing traffic based on predefined rules.
- Deployed Intrusion Detection Systems (IDS) to identify and respond to malicious activities.
- VPN implementation to secure remote connections and prevent unauthorized network access.

### Endpoint Security

- Installed Endpoint Detection and Response (EDR) tools to monitor and mitigate threats.
- Enforced device authentication and policy-based access controls.
- Regular security patching and system hardening to reduce vulnerabilities.

#### Application Security

- Deployed Web Application Firewalls (WAF) to prevent SQL injection and XSS attacks.
  - Conducted secure code reviews and vulnerability assessments.
  - Implemented input validation and output encoding to prevent common web-based attacks.
- 

### 3. Supply Chain Security

#### Example of Risk Identification & Mitigation

**Risk Identified:** A third-party software dependency introduced a critical vulnerability that could be exploited remotely.

#### Mitigation Strategy:

- Implemented a Software Bill of Materials (SBOM) to track all dependencies and their security status.
  - Conducted vendor security assessments before integrating third-party software.
  - Established a regular patch management process to ensure timely updates and vulnerability fixes.
- 

### 4. Advanced Security Model: Clark-Wilson Model

#### Application to Secure a System

The Clark-Wilson model was applied to enforce integrity constraints within a database system.

- **Well-formed Transactions:** Ensured data modification could only occur through controlled procedures (e.g., using stored procedures and application-layer controls).
- **Separation of Duties:** Restricted direct database access and implemented a layered approval process for changes.

- **Integrity Verification:** Regular audit logs and integrity checks to ensure compliance with security policies

## Implement Incident Response and Handling

### Incident Response Plan

#### **Preparation**

- Establish security policies and response procedures.
- Ensure staff is trained in incident handling.
- Maintain updated backups and security tools.

#### **Identification**

- Monitor logs and alerts for anomalies.
- Use IDS/IPS to detect suspicious activities.
- Confirm and classify the incident type.

#### **Containment**

- Isolate affected systems to prevent spread.
- Disable compromised accounts.
- Apply temporary security controls.

#### **Eradication**

- Remove malicious files or unauthorized access.
- Patch vulnerabilities.
- Perform forensic analysis.

#### **Recovery**

- Restore systems from clean backups.
- Validate security measures.
- Resume normal operations with monitoring.

### Digital Forensics

1) Picked out package shown below

2) Went through follow -> TCP Stream -> Show as: Raw -> Save file as..

3) Uncovered real PDF file from package, opening it in Adobe Acrobat

tcp.stream eq 3

Packet list Hex value ffd8ff Find Cancel

Options: Narrow & Wide Case sensitive Backwards Multiple occurrences

No.	Time	Source	Destination	Protocol	Length	Info
737	17.618120	67.180.72.76	128.121.136.217	TCP	62	4125 → 30107 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
738	17.635939	128.121.136.217	67.180.72.76	TCP	60	30107 → 4125 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
739	17.636025	67.180.72.76	128.121.136.217	TCP	54	4125 → 30107 [ACK] Seq=1 Ack=1 Win=17520 Len=0
744	17.686008	128.121.136.217	67.180.72.76	FTP-DA...	1078	FTP Data: 1024 bytes (PASV) (SIZE Understanding the FTP PORT Command.pdf)
745	17.687225	128.121.136.217	67.180.72.76	FTP-DA...	1514	FTP Data: 1460 bytes (PASV) (SIZE Understanding the FTP PORT Command.pdf)
746	17.687275	67.180.72.76	128.121.136.217	TCP	54	4125 → 30107 [ACK] Seq=1 Ack=2485 Win=17520 Len=0
747	17.705298	128.121.136.217	67.180.72.76	FTP-DA...	1514	FTP Data: 1460 bytes (PASV) (SIZE Understanding the FTP PORT Command.pdf)
748	17.706521	128.121.136.217	67.180.72.76	FTP-DA...	1514	FTP Data: 1460 bytes (PASV) (SIZE Understanding the FTP PORT Command.pdf)
749	17.706575	67.180.72.76	128.121.136.217	TCP	54	4125 → 30107 [ACK] Seq=1 Ack=5405 Win=17520 Len=0
750	17.707817	128.121.136.217	67.180.72.76	FTP-DA...	1514	FTP Data: 1460 bytes (PASV) (SIZE Understanding the FTP PORT Command.pdf)
751	17.754716	128.121.136.217	67.180.72.76	FTP-DA...	1514	FTP Data: 1460 bytes (PASV) (SIZE Understanding the FTP PORT Command.pdf)
752	17.754813	67.180.72.76	128.121.136.217	TCP	54	4125 → 30107 [ACK] Seq=1 Ack=8325 Win=17520 Len=0
753	17.755948	128.121.136.217	67.180.72.76	FTP-DA...	1514	FTP Data: 1460 bytes (PASV) (SIZE Understanding the FTP PORT Command.pdf)
754	17.757265	128.121.136.217	67.180.72.76	FTP-DA...	1514	FTP Data: 1460 bytes (PASV) (SIZE Understanding the FTP PORT Command.pdf)
755	17.757292	67.180.72.76	128.121.136.217	TCP	54	4125 → 30107 [ACK] Seq=1 Ack=11245 Win=17520 Len=0
756	17.770213	128.121.136.217	67.180.72.76	FTP-DA...	1514	FTP Data: 1460 bytes (PASV) (SIZE Understanding the FTP PORT Command.pdf)
757	17.770280	67.180.72.76	128.121.136.217	TCP	54	4125 → 30107 [ACK] Seq=1 Ack=12705 Win=17520 Len=0

Sequence Number: 1 (relative sequence number)  
Sequence Number (raw): 4066345043  
[Next Sequence Number: 1025 (relative sequence number)]  
Acknowledgment Number: 1 (relative ack number)  
Acknowledgment Number (raw): 4222223421  
0101 .... = Header Length: 20 bytes (5)  
Flags: 0x018 (PSH, ACK)  
Window: 33580  
[Calculated window size: 33580]  
[Window size scaling factor: -2 (no window scaling used)]  
Checksum: 0xd8e6 [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
[Timestamps]  
[SEQ/ACK analysis]  
TCP payload (1024 bytes)  
FTP Data (1024 bytes data)

```

0000 00 16 36 a9 08 20 00 01 5c 22 a5 82 08 00 45 00 6 . . . . . E
0010 04 28 07 07 40 00 34 06 a6 76 80 79 88 d9 43 b4 ( . @ 4 . . v y . C
0020 48 4c 75 9b 10 1d f2 5f 80 53 fb aa 04 3d 50 18 HLU . . . . . S . =P
0030 83 2c d8 e6 00 00 25 50 44 46 2d 31 2e 32 20 0d % . . . . . DF-1.2
0040 25 e2 e3 cf d3 0d 0a 20 0d 38 20 30 20 6f 62 6a % . . . . . 8 0 obj
0050 0d 3c 3c 0d 2f 4c 65 6e 67 74 68 20 39 20 30 20 << /Len gth 9 0
0060 52 0d 2f 46 69 6c 74 65 72 20 2f 46 6c 61 74 65 R /Filt r /Flate
0070 44 65 63 6f 64 65 20 0d 3e 3e 0d 73 74 72 65 61 Decode >> strea
0080 6d 0d 0a 48 89 2b 54 e0 35 31 36 d4 33 35 52 30 m H +T 516 35R0
0090 00 42 54 13 00 05 0b 4b 3d 73 33 05 73 03 0b 65 B] . . . . . K s3 s...
00a0 e4 5c 05 5e fd cc 5c 43 05 97 7c 5e 00 9f d7 08 \ ^ _ C [ . . . .
00b0 43 0d 65 6e 64 73 74 72 65 61 6d 0d 65 6e 64 6f C endstr eam endo
00c0 62 6a 0d 39 20 30 20 6f 62 6a 0d 34 36 0d 65 6e bj 9 0 o bj 45 en
00d0 64 6f 62 6a 0d 36 20 30 20 6f 62 6a 0d 3c 3c 0d dobj 6 0 obj <<
00e0 2f 54 79 70 65 20 2f 58 4f 62 6a 65 63 74 0d 2f /Type /X Object /
00f0 53 75 62 74 79 70 65 20 2f 49 6d 61 67 65 0d 2f Subtype /Image /
0100 4e 61 6d 65 20 2f 69 6d 31 0d 2f 46 69 6c 74 65 Name /im 1 /Filt
0110 72 20 2f 44 43 54 44 65 63 6f 64 65 20 0d 2f 57 r /DCTDe code /W
0120 69 64 74 68 20 37 35 32 0d 2f 48 65 69 67 68 74 idth 752 /Height

```



## Understanding the FTP PORT Command

Laura Chappell, Sr. Protocol Analyst

Protocol Analysis Institute

[www.packet-level.com](http://www.packet-level.com); [www.podbooks.com](http://www.podbooks.com)

**Note:** HP Certified Professionals may attend a free course online “Detecting and Preventing Network Scans - Part 1 and Part 2; approx. time: 90 mins. total” at <http://ftp.hp.com/pub/hpcp/chappel.html>.

You may already know that when FTP (File Transfer Protocol) commands cross the wire, they use port 21 by default. You may also know that port 20 is assigned to FTP data. Unfortunately, most FTP data sessions do not actually use port 20.

So you have just taken a trace of an FTP session and noticed that a PORT command crossed the wire. When you looked at the decode, you saw the strangest command sequence:

PORT 10,2,0,2,4,31

[We have several FTP trace files online at <http://www.packet-level.com/traceFiles.htm>.]

What does this mean? First let us take a look at the purpose of the PORT command. Then we will decipher the numbers following the command.

## THE PORT COMMAND

FTP communications use two port number values – one for commands (port 21 by default) and

## Incident Triage

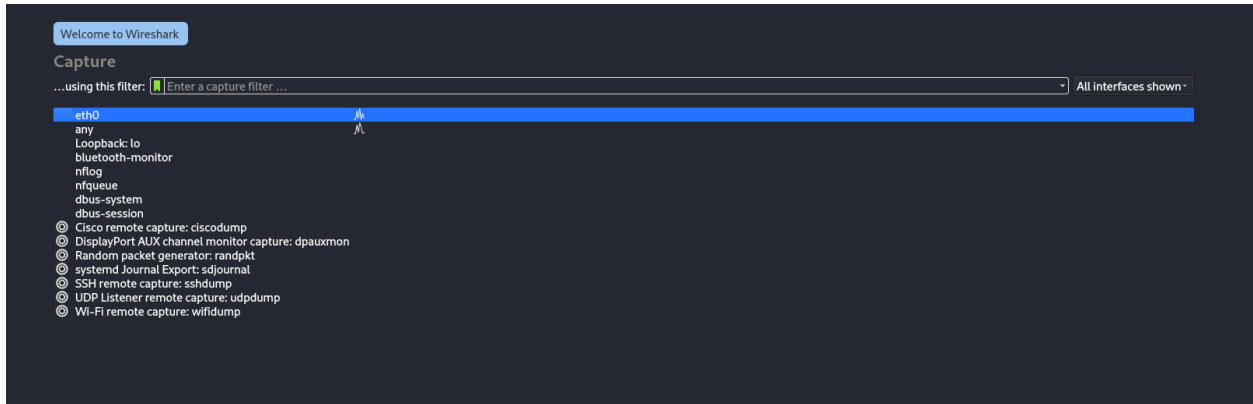
Incident Type	Severity Level	Business Impact	Description
Unauthorized File Transfer (PDF Extraction)	Medium	Potential data leak	A PDF file was transferred via FTP and extracted from a PCAP file. Possible unauthorized data exfiltration
Malware in PDF	High	Security Breach	If the PDF contains embedded malware (e.g., JavaScript, exploits), it could compromise systems.
Failed Unauthorized FTP Login Attempts	Low	Minimal risk	Multiple failed login attempts could indicate a reconnaissance attempt.

## Demonstrate SOC (Security Operations Center) Fundamentals

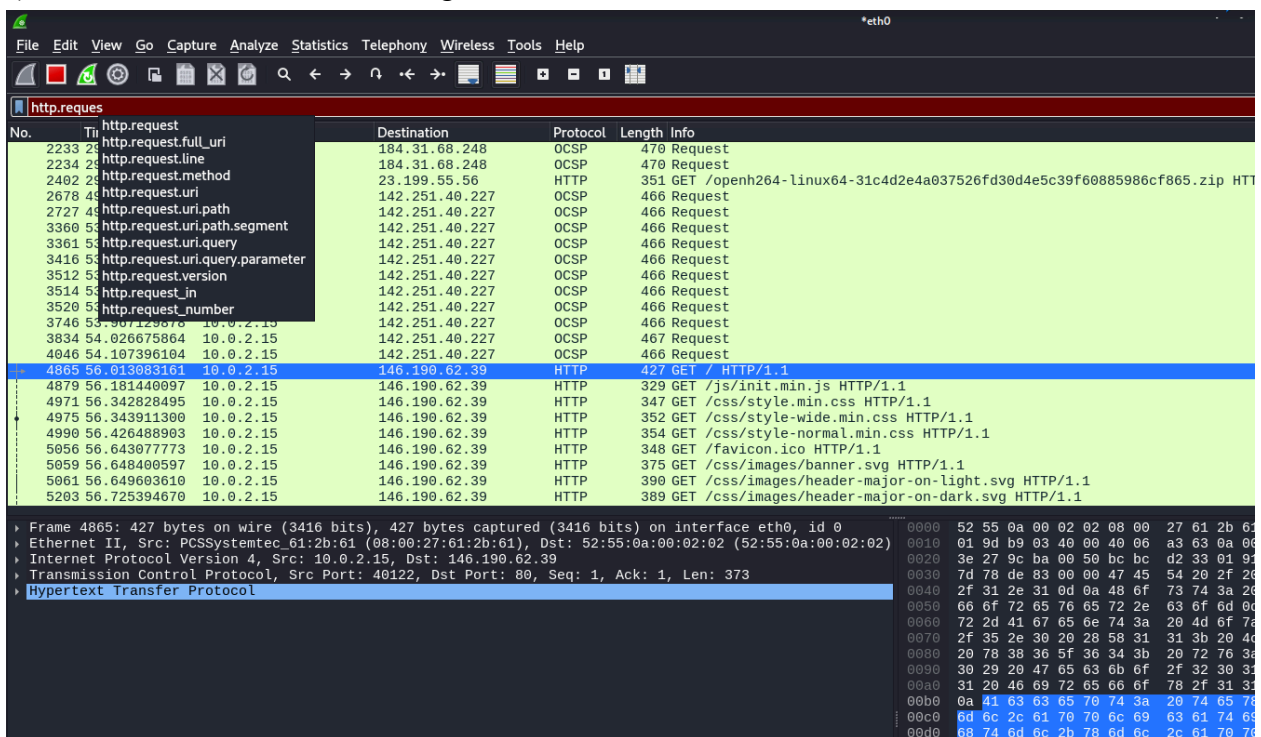
### Primary SOC Roles & Responsibilities

- SOC Analyst (Tier 1): Monitors alerts, performs triage, and escalates incidents.
- Incident Responder (Tier 2): Investigates security alerts, contains threats, and coordinates remediation.
- SOC Manager (Tier 3): Oversees SOC operations, sets policies, and leads major incident response efforts.

### Wireshark Network Activities



## 1) Basic HTTP Website monitoring



- Clearly shows the GET request and the IP address of the destination of <http://httpforever.com/>

## 2) Suspicious Network Scan example

\*eth0 CPU usage: 22.4%

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.syn==1 and tcp.flags.ack==0

No.	Time	Source	Destination	Protocol	Length	Info
9	0.071595100	10.0.2.15	35.190.72.216	TCP	74	46930 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=21013
22	0.321745599	10.0.2.15	23.63.240.10	TCP	74	47024 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=281981
74	1.907934456	10.0.2.15	34.107.221.82	TCP	74	35978 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=239154
83	1.924872486	fd00::ba95:6683:403...	2600:1901:0:38d7::	TCP	94	51826 → 80 [SYN] Seq=0 Win=33120 Len=0 MSS=1440 SACK_PERM TSval=273948
89	1.934971936	fd00::ba95:6683:403...	2600:1901:0:38d7::	TCP	94	51834 → 80 [SYN] Seq=0 Win=33120 Len=0 MSS=1440 SACK_PERM TSval=273948
96	2.531647156	10.0.2.15	34.117.188.166	TCP	74	60988 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=26687
109	2.616531985	10.0.2.15	34.117.188.166	TCP	74	32772 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=26687
138	2.819325565	10.0.2.15	142.251.40.227	TCP	74	56500 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=135667
193	3.522682815	10.0.2.15	34.49.51.44	TCP	74	49622 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=26819
223	3.675184086	10.0.2.15	35.190.72.216	TCP	74	51146 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=21013
265	4.028779728	10.0.2.15	34.149.100.209	TCP	74	58120 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=378790
281	4.095511745	10.0.2.15	23.63.240.33	TCP	74	33346 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=229670
310	4.343283996	10.0.2.15	52.24.225.206	TCP	74	51136 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=32338
319	4.438497762	10.0.2.15	34.160.144.191	TCP	74	54212 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=69759
357	4.533745598	10.0.2.15	23.63.240.33	TCP	74	33348 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=229670
377	4.653417689	10.0.2.15	34.107.243.93	TCP	74	46580 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=30470
411	4.994288020	10.0.2.15	34.120.158.37	TCP	74	59012 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=60076
428	5.096131343	10.0.2.15	34.107.243.93	TCP	74	46592 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=30470
508	5.333606708	10.0.2.15	34.120.158.37	TCP	74	59022 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=60076
549	5.510485630	10.0.2.15	34.120.158.37	TCP	74	59038 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=60076
579	5.613132091	10.0.2.15	34.120.158.37	TCP	74	59050 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=60076
616	5.677421680	10.0.2.15	34.120.158.37	TCP	74	59066 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=60076
663	6.086898355	10.0.2.15	34.120.158.37	TCP	74	59078 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=60076
801	6.195777237	10.0.2.15	34.120.158.37	TCP	74	59080 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=60076

Frame 4860: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0

Ethernet II, Src: PCSysSystemtec\_61:2b:61 (08:00:27:61:2b:61), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 146.190.62.39

Transmission Control Protocol, Src Port: 40122, Dst Port: 80, Seq: 0, Len: 0

0000 52 55 0a 00 02 02 08 00 27 61 2b 61  
0010 00 3c b9 01 40 00 40 06 a4 c6 0a 00  
0020 3e 27 9c ba 00 50 bc bc d2 32 00 00  
0030 7d 78 dd 22 00 00 02 04 05 b4 04 02  
0040 7e 0e 00 00 00 00 01 03 03 07

- Simulated a suspicious network port scan by using another VM to simulate the command “nmap -sS <target\_IP> “ onto this VM
- Used the filter “tcp.flags.syn==1 and tcp.flags.ack==0” to discover SYN packets to confirm suspicious activity.

# Develop and Implement Security Policies and Governance

## 1. Access Control Policy

**Objective:** Ensure only authorized individuals access systems and data.

**Policy:**

- User authentication must be enforced using multi-factor authentication (MFA).
- Role-based access control (RBAC) is implemented, granting access based on job responsibilities.
- Accounts must follow the principle of least privilege (PoLP).
- Inactive accounts will be disabled after 30 days of inactivity.
- Logs of access events must be maintained and reviewed weekly.

**Enforcement:**

- System administrators are responsible for enforcing access policies.
- Regular access reviews will be conducted every quarter.

## 2. Data Protection Policy

**Objective:** Protect the confidentiality, integrity, and availability of sensitive data.

**Policy:**

- All sensitive data must be encrypted at rest (AES-256) and in transit (TLS 1.2+).
- Data classification levels (e.g., public, internal, confidential) must be defined.
- Regular data backups must be performed and tested monthly.
- Data access must be logged and monitored.
- Employees handling sensitive data must undergo annual security awareness training.

**Enforcement:**

- Data protection officers oversee encryption compliance.
- IT teams conduct regular audits to ensure policy adherence.

### 3. System Use Policy

**Objective:** Define acceptable use of organizational IT resources.

**Policy:**

- Company systems must only be used for authorized activities.
- Personal use of company systems should be limited and must not interfere with work.
- Installation of unauthorized software is strictly prohibited.
- External devices (USB drives, external hard drives) require IT approval before use.
- Employees must report security incidents immediately.

**Enforcement:**

- IT administrators will monitor system usage logs.
- Non-compliance may result in access revocation or disciplinary action.

### Governance Structure

- **Chief Information Security Officer (CISO):** Oversees policy development and enforcement.
- **IT Security Team:** Implements security measures and conducts audits.
- **Department Managers:** Ensure team compliance with policies.
- **Employees:** Adhere to security policies and report violations.

### Compliance with Security Standards



NIST Cybersecurity Framework (CSF) guidelines, specifically:

- **PR.AC-1:** Identities and credentials are managed for authorized users.
- **PR.DS-1:** Data-at-rest is protected.
- **PR.PT-1:** Removable media use is restricted.

## Produce Effective Security Documentation

### Multi-Factor Authentication (MFA)

#### 1. Security Control Implementation

**1.1 Overview** Multi-Factor Authentication (MFA) enhances security by requiring users to provide multiple forms of verification before accessing systems. This reduces the risk of unauthorized access due to compromised credentials.

#### 1.2 Implementation Steps

##### 1. Define MFA Policies

- Require MFA for all administrative accounts.
- Enforce MFA for remote access.
- Select supported authentication methods (e.g., TOTP, biometric, hardware token).

##### 2. Select an MFA Solution

- Choose an MFA provider (e.g., Microsoft Authenticator, Google Authenticator, Duo Security).
- Ensure integration with existing authentication systems.

##### 3. Deploy MFA

- Enable MFA in identity management settings.
- Configure MFA enforcement policies for users.
- Conduct initial testing with a pilot group before organization-wide deployment.

##### 4. User Enrollment and Training

- Provide step-by-step enrollment instructions.
- Offer training on MFA usage and recovery options.
- Implement a support channel for troubleshooting.

##### 5. Monitor and Maintain MFA

- Regularly review authentication logs for suspicious activity.
- Update MFA policies based on security assessments.
- Reassess MFA configurations periodically to align with security best practices.

## **2. Process Documentation: Patch Management**

**2.1 Purpose** Patch management ensures that software vulnerabilities are promptly addressed, reducing the risk of exploitation.

### **2.2 Step-by-Step Guide**

- 1. Identify Systems Requiring Patching**
  - Use vulnerability scanners to detect outdated software.
  - Prioritize patches based on severity.
- 2. Test Patches**
  - Deploy patches in a controlled environment.
  - Monitor for compatibility issues.
- 3. Schedule Patch Deployment**
  - Establish maintenance windows to minimize disruption.
  - Notify users of potential downtime.
- 4. Apply Patches**
  - Deploy patches using automated tools.
  - Verify successful installation.
- 5. Monitor and Validate**
  - Conduct post-patch testing.
  - Roll back patches if issues arise.

## **3. Security Playbooks**

### **3.1 Incident Response Scenario 1: Phishing Attack**

**Steps to Follow:**

- 1. Detect and Report**
  - Identify suspicious emails reported by users.
  - Use email security tools to analyze headers and links.
- 2. Contain and Mitigate**
  - Block malicious domains and revoke compromised credentials.
  - Alert affected users and provide security awareness training.
- 3. Investigate and Document**
  - Analyze logs to trace the source.
  - Identify affected accounts or systems.
- 4. Recovery and Lessons Learned**
  - Restore any compromised systems.
  - Update email filtering policies.
  - Review and enhance phishing awareness programs.

## 3.2 Incident Response Scenario 2: Unauthorized System Access

### Steps to Follow:

1. **Detect and Alert**
    - Monitor authentication logs for unusual access attempts.
    - Notify security teams of anomalies.
  2. **Contain the Threat**
    - Disable compromised accounts.
    - Restrict access to critical systems.
  3. **Investigate the Breach**
    - Review logs to identify attack vectors.
    - Conduct forensic analysis if necessary.
  4. **Remediate and Improve Security**
    - Enforce stricter access controls.
    - Require password resets and MFA activation.
    - Update security policies and conduct a security audit.
- 

## 4. Knowledge Base Management

**4.1 Structured Document Repository** A centralized repository ensures that cybersecurity documentation is easily accessible. The repository includes:

1. **Authentication and Access Control**
  - MFA implementation guides
  - Password policy documents
  - Single Sign-On (SSO) best practices
2. **Incident Response**
  - Security playbooks
  - Incident report templates
  - Log analysis techniques
3. **System Hardening and Patch Management**
  - Secure configuration guides
  - Patch deployment policies
  - Vulnerability scanning procedures