Req. 1: Advanced Cybersecurity Defense Strategies Report

1. Zero Trust Architecture (ZTA) Implementation

- **Principle:** "Never trust, always verify" with strict identity verification regardless of location.
- **Application:**
    - **Network Access Control:**
        - Implement micro-segmentation to divide the network into isolated segments.
        - Enforce multi-factor authentication (MFA) to access each segment.
    - **Application Access Control:**
        - Apply role-based access control (RBAC) within critical applications.
        - Grant only necessary permissions per role and continuously monitor for unusual activity.

2. Defense in Depth (DiD) Explanation and Application

- **Concept:** A layered security approach deploying multiple defenses.
- **Application:**
    - **Physical Security:**
        - Secure data centers with biometric authentication, surveillance cameras, and restricted access.
    - **Network Security:**
        - Utilize firewalls, intrusion detection/prevention systems (IDPS), and encrypted communications (VPNs, SSL/TLS).
    - **Endpoint Security:**
        - Deploy anti-malware software, endpoint detection and response (EDR) solutions, and strict patch management.

3. Supply Chain Security Demonstration

- **Focus:** Identify and mitigate risks from third-party vendors.
- **Application:**
    - **Risk Identification and Mitigation:**
        - Conduct thorough security assessments of third-party software vendors.
        - Mandate robust code-signing procedures and integrate a software composition analysis (SCA) tool to monitor vulnerabilities in third-party components.

4. Advanced Security Model Application

- **Model:** Bell-LaPadula Model for maintaining data confidentiality.
- **Application:**
    - Implement “no read up, no write down” policies within a classified information management system to ensure that users only access data according to their security clearance.

Conclusion

- **Summary:** This report demonstrates a multi-layered security framework by integrating Zero Trust principles, Defense in Depth strategies, supply chain risk management, and advanced security modeling to safeguard critical systems.

Req. 2: Incident Response Plan (IRP)

1. Preparation

- **Incident Response Team (IRT):**
    - **Incident Manager:** Coordinates response efforts.
    - **Forensic Analyst:** Handles data collection and forensic analysis.
    - **IT Support:** Assists in technical containment and recovery.
    - **Communication Lead:** Manages internal and external communications.
- **Tools and Resources:**
    - **Forensic Tools:** FTK Imager for data collection.
    - **Log Management:** SIEM tools for real-time monitoring.
    - **Documentation Templates:** Chain of custody forms, incident report templates.
- **Training and Awareness:**
    - Regular drills and cybersecurity training sessions.

2. Identification

- **Detection Methods:**
    - Monitor logs using SIEM tools.
    - Leverage employee reports and automated alerts.
- **Initial Documentation:**
    - Record time, date, and nature of the incident.
    - Capture screenshots of anomalies.

3. Containment

- **Short-Term Containment:**
    - Isolate affected systems from the network.
    - Disable compromised accounts.

- **Long-Term Containment:**
    - Apply temporary fixes or patches.
    - Redirect traffic if necessary.

4. Eradication

- **Root Cause Analysis:**
    - Use FTK Imager and review log files to trace the attack vector.
- **Removal of Threats:**
    - Delete malicious files and software.
    - Patch vulnerabilities.

5. Recovery

- **System Restoration:**
    - Restore systems from clean backups.
- **Verification:**
    - Monitor systems for signs of reinfection and confirm all threats are removed.

Req. 3: Demonstrate SOC (Security Operations Center) Fundamentals

SOC Functions and Operations

- **Overview:** Describe SOC objectives, operations, and integration into overall security strategy.
- **Primary SOC Roles:**
    - **Incident Responder:** Investigates and mitigates security incidents.
    - **Threat Analyst:** Monitors threat intelligence feeds and analyzes potential threats.
    - **Security Engineer:** Implements and maintains SOC tools and infrastructure.

Monitoring Fundamentals

- **Monitoring Tool:**
    - Configure a monitoring tool (e.g., SIEM like Splunk, ELK, or OSSIM).
- **Network Activity Monitoring:**
    - Demonstrate monitoring of at least two types of network activity (e.g., firewall logs, IDS/IPS alerts, network traffic anomalies).

Alert Management

- **Security Alerts:**
    - Generate evidence of two different security alerts.
    - Document generation, investigation process, and resolution steps for each alert.

Basic Threat Detection

- **Threat Analysis:**
    - Identify at least one threat (e.g., malware infection, unusual outbound traffic).
    - Provide analysis of how the threat was detected using SOC tools (correlation rules, anomaly detection).

Req. 4: Develop and Implement Security Policies and Governance

Security Policy Document

- **Framework:** Develop a written security policy covering:
    - **Access Control:** Define resource access guidelines.
    - **Data Protection:** Explain data handling, encryption, and storage protocols.
    - **System Use Policies:** Outline acceptable use of corporate systems.

Governance Structure

- **Roles and Responsibilities:**
    - Define roles (e.g., CISO, IT Manager, Compliance Officer) responsible for policy enforcement.

Compliance Requirements

- **Security Standards:**
    - Reference at least one recognized standard (e.g., ISO 27001, NIST CSF) in the policy.

Policy Implementation

- **Communication and Enforcement:**
    - Demonstrate how policies are communicated (training sessions, newsletters, acknowledgment forms) and enforced within the organization.

Req. 5: Produce Effective Security Documentation

Technical Writing

- **Cybersecurity Procedure Document:**
    - Develop a step-by-step guide for implementing a security control (e.g., multi-factor authentication).

Process Documentation

- **Step-by-Step Guide:**
    - Document a security task (e.g., patch management or incident reporting) with detailed instructions or flowcharts.

Security Playbooks

- **Incident Response Scenarios:**
    - Create playbooks for at least two different incident response scenarios, outlining detection, roles, containment, eradication, recovery, and post-incident review.

Knowledge Base Management

- **Document Repository:**
    - Organize a repository with at least three categorized resources (best practices, regulatory requirements, tool configuration guides).