**Req. 1**

**Advanced Cybersecurity Defense Strategies Report**

**1. Zero Trust Architecture (ZTA) Implementation**

Zero Trust Architecture (ZTA) operates on the principle of "never trust, always verify," enforcing strict identity verification regardless of the user's location within or outside the network.

**Application in Project:**

- **Network Access Control:** Micro-segmentation was implemented to divide the network into isolated segments, ensuring that even if a segment was compromised, the breach could not spread laterally. Each segment required multi-factor authentication (MFA) for access.
- **Application Access Control:** Role-based access control (RBAC) was applied within critical applications. Users were only granted permissions necessary for their role, and continuous monitoring was implemented to detect and respond to unusual activity patterns.

**2. Defense in Depth (DiD) Explanation and Application**

Defense in Depth is a layered security approach that deploys multiple defensive mechanisms to protect information and systems.

**Application in Project:**

- **Physical Security:** Data centers were secured with biometric authentication, surveillance cameras, and restricted access areas to prevent unauthorized physical access.
- **Network Security:** Firewalls, intrusion detection/prevention systems (IDPS), and encrypted communications (VPNs, SSL/TLS) were utilized to safeguard the network perimeter and internal traffic.
- **Endpoint Security:** Anti-malware software, endpoint detection and response (EDR) solutions, and strict patch management protocols were deployed on all devices connected to the network.

**3. Supply Chain Security Demonstration**

Supply chain security focuses on identifying and mitigating risks from third-party vendors and service providers.

**Application in Project:**

- **Risk Identification and Mitigation:** A thorough security assessment was conducted on a third-party software vendor providing critical system updates. The assessment

identified a lack of proper code-signing practices as a potential risk for supply chain attacks.
To mitigate this risk, the vendor was mandated to implement robust code-signing procedures. Additionally, a software composition analysis (SCA) tool was integrated to continuously monitor for vulnerabilities in third-party components.

**4. Advanced Security Model Application**

**Bell-LaPadula Model Description and Application:**

The Bell-LaPadula model focuses on maintaining data confidentiality through mandatory access controls, primarily used in military and governmental contexts.

**Application in Project:**

The Bell-LaPadula model's "no read up, no write down" policies were implemented in a classified information management system. Users could only read data at or below their security clearance level and write data at or above their clearance level, preventing unauthorized data disclosure.

**Conclusion**

This report outlines the integration of multiple cybersecurity defense strategies to create a robust, multi-layered security framework. It addresses access control through Zero Trust Architecture, implements layered defenses via Defense in Depth, mitigates supply chain risks, and applies advanced security modeling with the Bell-LaPadula model to effectively safeguard critical systems

Req. 2

**Incident Response Plan (IRP)**

**1. Preparation**

- **Incident Response Team (IRT)**: Identify team members, roles, and responsibilities.
    - 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**:
    - Monitoring logs using SIEM tools.
    - 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 to analyze compromised systems.
    - Review log files to trace the attack vector.
- **Removal of Threats**:
    - Delete malicious files and software.
    - Patch vulnerabilities.

**5. Recovery**

- **System Restoration**:
    - Restore from clean backups.
    - Monitor systems for any signs of reinfection.
- **Verification**:
    - Ensure all systems are functioning normally.
    - Confirm no residual threats remain.

To be continued