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