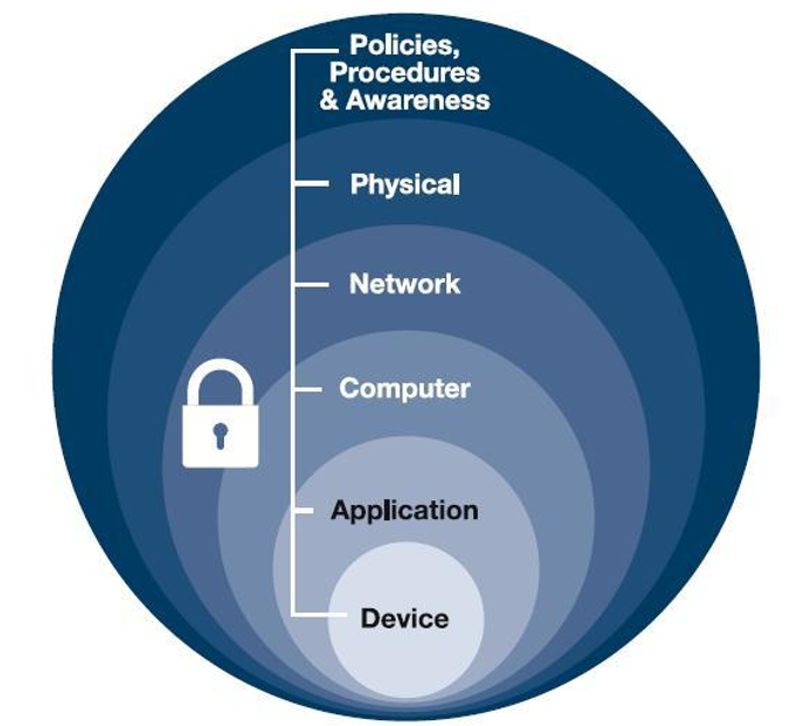
**Cyber Security – Assessment # 4**

**Q1.** You have been hired in Ooredoo Telecom as Cyber Security Architect. Company is expecting you to build a comprehensive layered security architecture in order to improve their defensive posture. Document gist of your recommendations.



**Answer**

**Introduction**

As the appointed Cyber Security Architect at Ooredoo Telecom, I propose the implementation of a comprehensive Defense-in-Depth security architecture. This multi-layered approach aims to strengthen the company’s cybersecurity posture by incorporating a range of controls across various technical and human layers. The goal is to ensure that even if one layer is compromised, subsequent layers continue to protect critical assets.

1. **Device Layer Security**

This is the foundational layer that secures individual endpoints such as mobile devices, laptops, and desktops.

**Recommendations:**

Deploy Endpoint Detection and Response (EDR) tools for real-time threat detection. Implement Mobile Device Management (MDM) solutions to control and secure mobile access. Enforce regular operating system and software patching. Restrict device-level access using BIOS/UEFI passwords and USB control policies.

1. **Application Layer Security**

Application security focuses on preventing vulnerabilities in the software layer.

**Recommendations:**

Implement a Web Application Firewall (WAF) to monitor and block malicious traffic. Follow secure coding practices, especially those outlined in the OWASP Top 10. Use Static and Dynamic Application Security Testing (SAST/DAST) tools. Enforce secure authentication mechanisms such as OAuth 2.0, MFA, and Role-Based Access Control (RBAC).

1. **Computer (Host) Layer Security**

This layer covers the protection of operating systems, servers, and host machines.

**Recommendations:**

Enable host-based firewalls and antivirus/anti-malware software. Configure systems based on CIS Benchmarks for server hardening. Apply least privilege principles to user access. Monitor system activity for unusual behavior or policy violations.

1. **Network Layer Security**

Network security ensures safe data communication between systems.

**Recommendations:**

Deploy Intrusion Detection and Prevention Systems (IDS/IPS). Use firewalls and network segmentation to isolate sensitive environments. Enforce secure communication protocols such as HTTPS, VPN, and SSH. Integrate DDoS protection mechanisms.

1. **Physical Layer Security**

Physical protection is essential for securing infrastructure such as data centers.

**Recommendations:**

Use CCTV surveillance, biometric access control, and security personnel.

Implement mantrap doors and secure facility perimeters. Equip data centers with fire suppression systems, backup power, and climate control.

1. **Policies, Procedures, and Awareness**

Human factors and organizational processes are key to maintaining overall security.

**Recommendations:**

Develop and enforce a formal Information Security Policy. Conduct regular security awareness training for all employees. Maintain a detailed Incident Response Plan (IRP). Run periodic phishing simulations and security drills.

**Additional Strategic Measures**

Perform regular vulnerability assessments and penetration testing. Deploy a SIEM (Security Information and Event Management) solution for real-time monitoring and analytics. Adopt a Zero Trust Architecture to verify every access request.

Ensure compliance with global cybersecurity standards such as ISO 27001 and NIST Cybersecurity Framework.

**Conclusion**

By adopting a Defense-in-Depth approach, Ooredoo Telecom can establish a resilient security posture against a wide spectrum of cyber threats. Each layer in this architecture works in conjunction to minimize risks, detect threats early, and protect the company’s digital assets efficiently.