



Security Architect

Job Description

Security Architects examine the systems of their companies for vulnerabilities. On local area networks, wide area networks, and virtual private networks, they do penetration tests, risk analysis, and ethical hacks. To analyse effectiveness and efficiency, they also evaluate routers, firewalls, and similar technologies.

Security Architects have hacker mentalities. They strain the capabilities of computer and network security mechanisms. Security architects plan and implement architectural modifications to strengthen security structures after locating weaknesses in current systems.

Key Responsibilities

- Deploying new and enhanced systems while managing and maintaining current system security measures.
- Making sure that everyone in the company follows the rule of least privilege.
- Executing and managing IAM security architecture (Identity & Access Management).
- Conducting security audits on third-party applications and services.
- Managing and coordinating training programs for security awareness.
- Carrying out vulnerability testing, risk analysis, and security evaluations on the finished infrastructure

Qualifications Needed

- Knowledge of UNIX, Linux, and Windows.
- Understanding of the COBIT, ITIL, and ISO 27001/27002 frameworks.
- Knowledge of network segmentation, network access restrictions, firewalls, IDS/IPS, and other perimeter security measures.
- Architecture creation and definition for network security.
- Knowledge of the many wireless security features, including routers, switches, and VLAN security.
- Understanding of DNS-related security concepts, such as routing, authentication, VPNs, proxy services, and DDOS mitigation technology.
- A working knowledge of cloud risk assessment techniques and third-party auditing.