

IT Security Analyst

Job purpose:

Security Analyst will implement IT security systems to protect the organization's from cyber attacks. You will also help develop organization wide best practices for IT security. You will monitor computer networks for security issues, install security software and document all security issues or breaches you find.

You need to be proficient with Hybrid systems and have experience in installing security software and documenting security issues. In addition, you will have excellent written and oral communication skill and understand patch management and firewalls, antivirus and IDPS concepts.

Key Accountabilities:

- Monitor TLS estate computer networks for security issues.
- Investigate security breaches and other cyber security incidents.
- Install security measures and operate software to protect systems and information infrastructure, including firewalls and data encryption programs.
- Document security breaches and assess the damage they cause.
- Work with IT Security Manager to perform tests and uncover network vulnerabilities.
- Assist to fix detected vulnerabilities to maintain a high-security standard.
- Research security enhancements and make recommendations to IT Security Manager
- Install security measures and operate software to protect systems and information infrastructure, including firewalls and data encryption programs.
- Examine security systems and web applications
- Monitoring security access across TLS
- Assist to conduct security assessments through vulnerability testing and risk analysis
- Assist to performing both internal and external security audits
- Analyse security logs from various system for breaches
- Assist to verifying the security of third-party vendors and collaborating with them to meet security requirements
- Review daily security logs for abnormal events and escalate to IT Security teams.
- Assist to conduct technical vulnerability assessments (including regular penetration testing) of IT systems and processes, identifying potential vulnerabilities, makes recommendations for risk mitigation.
- Perform technical risk assessments of new and existing systems, identifying potential weaknesses and recommending suitable protection measures.
- Support configuration and operation of firewalls, encryption, and other security measures
- Support the delivery of an effective Security Testing Schedule

Knowledge, skills and experience

Essential

- Strong networking fundamentals. Understand TCIPIP, VLAN's, DNS, load balancing and software-defined layer 2/3 rule configurations.
 - Required technical knowledge of hybrid estate.
 - Experience in reviewing technical security events.
 - Ability to set up security configuration of devices.
 - Experience of testing and reviewing security solutions
 - Strong reasoning and advisory skills, with the ability to effectively engage with and influence senior management.
 - Ability to communicate confidently and effectively with staff at all levels in the organisation.
 - Ability to work with third parties to understand critical security bottlenecks.
 - A degree in an Information Technology or Computer Science discipline *or significant hands-on experience*
 - A strong technical understanding and background
 - Must be capable of researching/evaluating emerging cyber security threats and understand the methods needed to manage them
 - Knowledge of network protocols and technologies such as TCP/IP, PKI, Network Security Groups etc.
 - Knowledge of end point detection & response, User activity monitoring systems
 - Knowledge of platform as a service (PaaS) and software as a service technologies (SaaS)
 - Experience using Azure Security suite (advantageous), Office 365 Advance protection, Security & Compliance centre, Cloud app security, Windows Defender ATP & Intune
- Certs – Security+, CompTIA Security+, CompTIA Cloud, Azure Security (advantageous)

Planning & Organising

- Assists to build and continually improve IT security for TLS and its members
- Assist to manage and develop the organisations approach and understanding of IT security.
- Ability to work with project teams.
- Ability to resolve conflict and to deal with competing priorities.

Dimensions

- Technical subject matter expert for the business.

The professional body for solicitors