Jackson Walker

Information Security Analyst

POSITION SUMMARY

The information security analyst is responsible for maintaining the security and integrity of the firm's data, hardware and software. Their primary responsibility is to monitor the security systems of the firm and respond to any alerts and warnings generated by those systems including; verifying incidents, preventing the escalation of incidents and remediating confirmed incidents. The security analyst will work with the Director of Information Security and Senior Information Security Analyst, as well as the various IT teams, in communicating and remediating flaws in security systems. The security analyst is responsible for assisting with potential security incidents within the organization, including performing root cause analysis. Additionally, the security analyst will create/update documentation related to information security systems, processes and procedures.

ESSENTIAL DUTIES & RESPONSIBILITIES

Specific duties of this position include, but are not limited to:

- Performs initial analysis, identification, and documentation of network intrusions and computer systems compromises.
- Serves as a member of the CSIRT team and will assist with incident response efforts including, but not limited to: Detection, Verification & Triage, Scoping, Containment, Eradication, Recovery, Remediation
- Identifies and recommends potential solutions to improve the existing security posture and assist with testing/POC efforts as appropriate.
- Maintains and proactively monitors the Firm's information security systems to include:
    - Security Information and Event Management (SIEM) Platforms
    - NGFW Appliances
    - IDS/IPS Systems
    - AV/EDR/XDR Platforms
    - DLP/FRP Systems
    - MFA/SSO Systems
- Identifies and recommends solutions to improve the Firm's security posture and assist with testing/POC efforts as appropriate.
- Proactively research trending Tactics, Techniques, and Procedures (TTP) to aid in the identification of security events that may occur within the organization.
- Leads the firm's patching/software update ~~team~~ efforts to ensure that the firm maintains the most up-to-date operating system and firmware revisions applicable to the systems.
- Monitors email filtering systems such as Anti-Spam, Anti-Malware.
- Maintains and increases professional and technical knowledge through participation in professional development activities including webinars, seminars, conferences and formal training classes.
- Assist with firm's disaster recovery and business continuity planning and testing activities.
- Keep supervisor and peers informed of all changes and threats to ~~the~~ systems.
- Other duties assigned by the employer.

KNOWLEDGE, SKILLS, & ABILITIES REQUIRED

- Bachelor’s degree (four-year college or technical school) Preferred. Field of study: Information Technology, Information Security, Computer Science or related qualifications.
- Preferred certifications include: Comp TIA Security+, ISC2 SSCP, Microsoft Azure Certifications, SANS GSEC
- Familiarity with systems such as: Virtualization, Active Directory, Printing, DNS/DHCP, TCP/IP, Email Systems, LAN/WAN Networking.
- Familiarity with basic scripting e.g. PowerShell, Python.
- Must carry a Firm-managed mobile device and be available after normal working hours.
- Must have at least 3 years of experience in a general IT related role.
- Must have at least 1 year of experience in an information security role or comparable experience
- Be available 24x7 in order to respond to security incidents.
- Will occasionally be required to work more than 37.5 hours a week.
- Must have proficient keyboard skills.
- Some travel to other Firm locations and/or remote training facilities may be necessary.
- Interpersonal skills necessary to communicate effectively in person, by email and telephone to provide information to clients, attorneys and staff with courtesy and tact.