Job ID: 2018-0003

Security Operations Center Analyst

Job Summary

Cysiv is currently seeking a Security Operations Center Analyst to join a growing security team. We are looking for extremely talented people with a passion for technology and an eye toward stability, flexibility, innovation, and security. The ideal candidate will have a strong background in IT security and is comfortable with both customer-facing and security implementation roles.

Principal Duties & Responsibilities

- Detection, monitoring, analysis, resolution of security incidents; participate in providing containment recommendation
- Coordinate escalations to external client support teams to ensure timely delivery of incident resolutions
- Perform network/system/application/log intrusion detection analysis and trending
- Perform tuning of the SIEM filters and correlations to continuously improve monitoring
- Participate in the security incident handling efforts in response to a detected incident, and coordinate with other stakeholders and clients
- Ensure that Service Level Agreements are met
- Maintain standard operating procedures, processes and guidelines
- Automate security analysis, administration and remediation procedures, workflows and tasks
- Maintain awareness of trends in security regulatory, technology, and operational requirements
- Shift rotation will be required for this role.

Qualifications

Education & Experience

- Graduate with a degree from a recognized university with specialization in Computer Sciences or a related discipline, combined with a minimum of three (3) years of directly related practical experience and demonstrated ability to carry out the functions of the job.
- SIEM experience with ELK Security Analytics, QRadar, RSA Netwitness, and Splunk
- Thirst for knowledge, inquisitive nature, keen interest in actively participating in SOC expansion
- Experience working in an IT Security Operations Center, using SANS methodology
- Experience and extensive knowledge of Security Information Event Management
- Experience in Intrusion Detection or Prevention Systems
- Knowledge of: TCP/IP, computer networking, routing and switching
- Experience in Linux and Windows based devices at the System Administrator level
- System log forensics (Syslog, Event Viewer)
- EC Council: C|HFI, ECAS or SANS: GIAC, GCFA, GCIH, GREM or other certifications are preferred
- Strong troubleshooting, reasoning and problem solving skills
- Ability and experience in writing clear and concise technical documentation
- Knowledge of: Strong Authentication, End Point Security, Internet Policy Enforcement, Firewalls, Web Content Filtering, Database Activity Monitoring (DAM), Public Key Infrastructure (PKI), Data Loss Prevention (DLP), Identity and Access Management (IAM) solutions
- Knowledge of Cysiv suite of security tools