Position: Security Operation Center (SOC) Analyst

JOB SCOPE

SOC Analysts serve as crucial first responders to security threats, alerts, and incidents, as part of Spectrotel 24/7 SOC team. Our Analysts are responsible for triaging security alerts detected by FortiSIEM, FortiEDR, and DarkTrace NDR, analyzing all available data to determine if a cyber-attack is occurring, scoping the extent of a suspected attack, coordinating efforts to contain attacks, performing forensic investigations to determine the details around threats and attacks, and providing guidance on remediation actions.

DUTIES AND RESPONSIBILITIES

- SOC Service Monitoring, Analytics and Cyber Threat Analysis;
- Continuous & persistent monitoring of security technologies/tool data and network traffic which result in security alerts generated, parsed, triggered, or observed on the in-scope managed networks, enclaves, systems or security technologies;
- Analyzing, triaging, aggregating, escalating and reporting on client security events including investigation of anomalous network activity, and responds to cyber incidents within the network environment or enclave;
- Correlation and trend analysis of security logs, network traffic, security alerts, events and incidents;
- Continuously works to tune security tools to minimize false positives and maximize detection and prevention effectiveness. Collaborates with the owners of cyber defense tools to tune systems for optimum performance;
- Analyzes malware and attacker tactics to improve network detection capabilities. Collaborates with external companies or government agencies to share open source or classified intelligence;
- Distributes use case context, vulnerability and threat advisories as relevant to optimize security tools, SIEM and client awareness;
- Incident categorization and severity assignment consistent with client criteria;

- Event and incident handling consistent with applicable client plans and processes;

- Integration of activities with standard reports, such as shift reports, along with client communication protocols;
- Documents and provided feedback to engineers for custom views, channels, and other content for Incident Response, Insider Threat Management (ITM), and other threat detection use cases into disparate enclaves in the customer environment;
- Support calculation of security metrics related to Managed SOC Services offering;
- Drive SIEM content development, tuning, and review.

REQUIRED SKILLS:

- Prior experience working in any of the following three: Security Operations Center (SOC), Network Operations Center (NOC), Computer Incident Response Team (CIRT)
- Experience in the detection, response, mitigation, and/or reporting of cyber threats affecting client networks
- Experience in computer intrusion analysis and incident response
- Working knowledge of Intrusion detection/protection systems
- Knowledge and understanding of network devices, multiple operating systems, and secure architectures
- Working knowledge of network protocols and common services
- System log analysis
- Current experience with network intrusion detection and response operations (Protect, Defend, Respond and Sustain methodology)
- Experience responding to and resolving situations caused by network attacks
- Ability to assess information of network threats such as scans, computer viruses or complex attacks
- Working knowledge of WAN/LAN concepts and technologies
- SIEM content Analysis, Development and Testing
- 6 months recent experience (within the last 2 years) with Fortinet
- Familiarity with packet analysis to include: HTTP Headers & Status codes, SMTP Traffic & Status codes, FTP Traffic & Status Codes
- Excellent written and verbal communication skills;
- Personality traits: Naturally curious and inquisitive nature; persistent and determined; loves solving problems and puzzles; analytically rigorous; uncompromising integrity.

EXPERIENCE

Desired:

- ForiSIEM, FortEDR, and Dark Trace NDR
- Familiar knowledge of Process and IT service management concepts such as ITIL and ITSM

Education / Certification /Training

- Bachelor's Degree in Management Information Systems, Computer Science is preferred.
- Certifications related to security (such as Security+, GSEC, GCIH, GCIA, CISSP, NCSF, etc.)
- Certifications in Fortinet

Spectrotel is an Equal Opportunity Employer. All applicants will be considered for employment without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, veteran or disability status, or any other legally recognized protected basis under federal, state, or local laws, regulations or ordinances.