SOC Analyst - Incident Handler (Junior)

Role Summary

The SOC analyst & incident handler role is a junior level position providing an opportunity to work in a fast-paced collaborative environment defending a variety of customers and their infrastructure from cyber threats. We are looking for someone who loves working in Information Security, who enjoys hunting the bad guys, protecting systems, identifying anomalies, who can think out of the box, who can understand what may happen if something is not working as expected.

Responsibilities

• Analysis and verification of security threat monitoring alerts to produce incident identification, classification and prioritization
• Create, improve and maintain security monitoring alerts based on correlation of different sources of data
• Operate and maintain various IDS/IPS working close with security/network architects to take security monitoring and defences to the next level
• Respond to security incidents and investigations working close with customers and IT providers, following SLA requirements
• Conduct forensics/malware analysis to extract indicators of compromise for further mitigation and containment, evaluating incident scope and impact
• Report to the SOC Manager and the involved customer CISO/CIO

Qualifications

Minimum qualifications:

• Computer/ Telecommunications Engineering degree or a related discipline
• Strong technical understanding of network fundamentals and common Internet protocols
• Knowledge of system administration and security architecture
• A degree of familiarity with the main security monitoring tools (FW, IDS/IPS, Endpoint security, WAF, SIEM)
• Fluent in English (written and spoken)
• Self-motivated with the ability to work independently and as a team member in a challenging environment

Ideal qualifications:

• Proficient in understanding Operating Systems and their architectures: Windows, Unix/Linux, and OSX Operating Systems
• Programming or Scripting in Bash or Python
• Good understanding of Cyber security landscape: Cyber kill chain, TTP, threat intelligence, malware business
• Good understanding of information security concepts: defence in depth, BYOD management, data loss protection, risk assessment and security metrics
• Strong analytical and problem-solving skill
• Strong communication and presentation skills along with the ability to work in a highly collaborative environment
• Exhibits initiative, follow-up and follow through with commitments
• Manages multiple priorities in a high-pressure environment
• Related Certification (GCIH, GCFA, GCFE, GREM, CISSP) is a plus