SOC Analyst - Incident Handler (Senior) / Barcelona

Role Summary

The Senior SOC analyst & incident handler role is a senior level position providing an opportunity to work in a fast paced collaborative environment defending a variety of customers and their infrastructure from cyber threats. This is a leader position, that demands the ability to mentor and advise others, leading the team to continuous improvement.

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,
- Lead the response 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,
- Advice and train junior team members,
- Proactive monitoring on cyber threat landscape by performing research and study on latest security threats and vulnerabilities to ensure operational tools and processes are up to date.

Qualifications

Minimum qualifications:

- Computer/Telecommunications Engineering degree or a related discipline,
- More than 3 years of relevant experience in the field of information security,
- Experience working in a Security Operations Center (SOC) environment,
- Strong technical understanding of network fundamentals and common Internet protocols,
- Knowledge of system administration and security architecture,
- Knowledge of the main security monitoring tools (FW, IDS/IPS, HIDS, WAF, SIEM)
- Experience or proven knowledge of at least one IDS technology,
- 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,
- Scripting experience 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,
- Three or more years working in a Security Operations Center (SOC) environment,
- Strong analytical and problem solving skill,
- Strong communication, presentation, and leadership 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.

Bonus:

- Experience working with AWS or Azure infrastructure,
- Previous experience with malware reverse engineering,
- Related Certification (GCIH, GCFA, GCFE, GREM, CISSP) is a plus.