CYBER FOCUSED OPS (FORENSICS, INTEL, MALWARE) MANAGER IN HERNDON, VA

Job Description:

The Focused Operations Manager reports to the Security Operations Director within the CISO organization. This position is in support of a Defense Contractor security operations center (SOC).

Responsibilities include:

- Investigate alerts and incidents at the Tier III level with the Security Operations team to detect threats and investigate intelligence received.
- Being able to brief the CISO/Security Operations Director to provide an accurate depiction of the current threat landscape and associated risk
- Understanding threat campaigns, techniques, and indicators of compromise (IOCs).
- Collaborating with the Security Operations team to recommend remediation and recovery strategies and/or improvements to the security environment.
- Maintaining situational awareness of cyber activity per the DIB by reviewing open source reporting for new vulnerabilities, malware, or other threats that have the potential to impact the organization.
- Utilizing a malware and threat repository.
- Working with security tools or with Security Engineering or IT Operations teams regarding logs reviewed or alerts received.
- Utilizing PCAP where necessary.
- Reverse engineering malware.
- Using knowledge and awareness/expertise surrounding hacker/hacktivist groups and advanced persistent threats conducting computer network exploitation and attacks against Defense contractors.
- Ability to recognize signatures, tactics, techniques and procedures associated with preparation for and execution/implementation of such attacks.
- Creating, launching and managing internal phishing campaigns.
- Assisting law enforcement and counter intelligence offices with cyber investigations as necessary; providing forensic and network analysis.
- Managing focused operations staff and support areas to include insider threat, forensics, intel investigation, and malware analysis

Qualifications

- Bachelor's degree and 10-12 years of experience, or Masters and 8-10 years.
- Five (5) years' experience with cyber intelligence analysis.
- Experience with threat analysis and malware reverse engineering.

- Experience working in a Security Operations Center (SOC) or related response team.

Certifications

- One or more of the following highly desired: CISSP, GREM, GCTI

Clearance

- Candidates must be US citizens and able to obtain and/or maintain a Department of Defense Secret or Top Secret security clearance as a condition of employment

Send Resume to careers@intellectualpoint.com.