INCIDENT RESPONSE ANALYST IN WASHINGTON, DC

IP is seeking an Incident Response Analyst to support threat monitoring, detection, event analysis and incident reporting. The Security Operations Center is a 24/7 environment. The Incident Response Analyst will be responsible for monitoring enterprise networks and systems, detecting events and reporting on any and all threats that are directed against those systems regardless of their classification level or type. The Incident Response Analyst is expected to collaborate with leadership to develop metrics based on situational awareness and threat monitoring at an enterprise level that will be reported based on the approved plan and supporting checklists. The Incident Response Analyst must be able to rapidly address security.

Typically, the client's sensor grid acquires millions of events per day and events are analyzed and categorized in accordance with the Cyber Security Incident Response Plan. The Incident Response Analyst will provide the client with a full comprehensive array of analytical activities in support of external threat monitoring, detection, event analysis and incident reporting efforts to include: presentation reviews, internal and external threat reporting, analysis of inbound and outbound public internet traffic, suspicious e-mail messages, administer access request to specific public sites, communicate and coordinate the characterization of events and the response.

The Incident Response Analyst shall orient their skill sets to the following tools (this is not a complete inventory):

- ArcSight SIEM
- Splunk
- RSA Netwitness
- FireEye
- Sourcefire (Snort)
- Bro IDS
- Fidelis XPS
- HB Gary Active Defense

Functional Responsibilities: The Incident Response Analyst may perform any or all of the following: Provides support for complex computer network exploitation and defense techniques to include deterring, identifying and investigating computer and network intrusions; providing incident response and remediation support; performing comprehensive computer surveillance/monitoring, identifying vulnerabilities; developing secure network designs and protection strategies, and audits of information security infrastructure. Provides technical

support for continuous monitoring, computer exploitation and reconnaissance; target mapping and profiling; and, network decoy and deception operations in support of computer intrusion defense operations. Provides technical support for forensics services to include evidence seizure, computer forensic analysis and data recovery, in support of computer crime investigation. Researches and maintains proficiency in open and closed source computer exploitation tools, attack techniques, procedures and trends. Performs research into emerging threat sources and develops threat profiles. Provides technical support for a comprehensive risk management program identifying mission critical processes and systems; current and projected threats; and system vulnerabilities.

Qualifications

- Shift 1 time: 6AM - 2:30P
- Minimum of six (6) years of general work experience and three (3) years of relevant experience in functional responsibility.
- Bachelor's Degree, or an equivalent combination of formal education, experience.
- Candidate should have strong analytical and organizational skills.
- Candidate should have concise writing skills, excellent MS Word skills as well as other MS Office Applications
- Experience with securing various environments preferred.
- Experience working a SOC and doing incident response is preferred.
- Experience and education preferred in CEH, eCPPT, OSCP, GCFW, GCIH, other relevant IT security certifications, or advanced vendor certifications such as Splunk Certified Architect or SourceFire Certified Administrator; Security+, Network+, GSEC, or other relevant IT security product certifications such as Tenable Certified Nessus Auditor, ArcSite Certified Systems Analyst, or SnortCP CISSP, CISM, or ISO 27001

Send Resume to careers@intellectualpoint.com.