TIER II CYBERSECURITY ANALYST (S105) IN HERNDON

Tier II Cyber Security Analyst - Herndon, VA

Overview

The Tier II Cybersecurity Analyst reports directly to the SOC Manager as part of the Security Operations team within the CISO organization in an enterprise environment.

Responsibilities

Senior Security Analyst will support Tier II analysis and response. Must be capable of working with a security team of varying experience levels to effectively monitor and investigate security incidents as well as make recommendations to improve the security posture of a large organization.

- Perform network security monitoring and incident response for a large organization; coordinate with other corporate sectors to record and report incidents.
- Respond to cybersecurity tickets.
- Investigate and analyze software and tools for approval to be on the corporate network.
- Monitor and analyze Security Information and Event Management (SIEM) alerts to identify security issues for remediation and investigate events and incidents.
- Recognize potential, successful, and unsuccessful intrusion attempts and compromises through reviews and analyses of relevant event detail and summary information from security tools.
- Implement counter-measures and/or mitigating controls.
- Conduct investigative analysis via various security tool portals to include email and endpoint protection tools.
- Prepare briefings and reports of analysis methodology and results.
- Assist security analysts in building operational processes around the SIEM ecosystems
- Develop IDS/IPS and SIEM content and rules
- Perform analyst activities using security tools such as QRADAR SIEM (or similar), Packet Capture, Forensics, Proofpoint, IPS, firewalls, endpoint security, and FireEye
- Assist with forensics and investigations as needed using security tools such as ProofPoint, SIEM, and EnCase

Qualifications

- Bachelors degree and 5-7 years experience or MS and 3-5 years

- Experience implementing SIEM products such as Arcsight, QRadar and/or Splunk in a complex network environment.
- Experience investigating, interpreting, and responding to technical and/or complex IT security data.
- Extensive experience with IT security tools, working technical knowledge of network, server, storage and desktop hardware and software
- Prior experience successfully providing the full range of IT cyber security tasks.
- Strong working knowledge with industry IT security tools
- Technical certifications are a plus
- Must be able to obtain and maintain a DoD Secret Clearance
- U.S. Citizen

Desired Skills

Candidate should have the following traits:

- Excellent analytical and problem-solving skills as well as interpersonal skills to interact with end users, team members, and senior management.
- Subject Matter Expert-level skills in Incident Response and Intrusion Monitoring.
- Strong foundation of Network and Security skills, fundamental knowledge of Windows, Linux and Cisco operating systems, networking protocols and network traffic analysis.

- Desirable certifications include CISSP, GCIH, GCIA, or GCED
- Able to work independently and complete projects with little supervision

Send Resume to careers@intellectualpoint.com.