SOC ANALYST IN VIENNA, VA

As a Senior Incident Handler you will be responsible for leading and participating in threat actor based investigations, creating new detection methodologies, and provided expert support to incident response and monitoring functions. The focus of the Senior Incident Handler is to coordinate the team to investigate and respond to security incidents. To execute this mission, the Incident Handler will use data analysis, threat intelligence, and cutting-edge security technologies. You will directly support the Security Operations Center by applying analytic and technical skills to investigate intrusions, identify malicious activity and potential insider threats, and perform incident response.

Responsibilities:

- Lead Incident Handling efforts

- General SIEM monitoring, analysis, content development, and maintenance

- Research, analysis, and response for alerts; including log retrieval and documentation
- Conduct analysis of network traffic and host activity across a wide array of technologies and platforms
- Assist in incident response activities such as host triage and retrieval, malware analysis, remote system analysis, end-user interviews, and remediation efforts
- Compile detailed investigation and analysis reports for internal SOC consumption and delivery to management
- Track threat actors and associated tactics, techniques, and procedures (TTPs)
- Capture intelligence on threat actor TTPs and develop countermeasures in response to threat actors
- Analyze network traffic, IDS/IPS/DLP events, packet capture, and FW logs
- Analyze malicious campaigns and evaluate effectiveness of security technologies
- Develop advanced queries and alerts to detect adversary actions
- Coordinate threat hunting activities across the network leveraging intelligence from multiple internal and external sources, as well as cutting-edge security technologies
- Design and build custom tools for investigations, hunting, and research
- Assist in the design, evaluation, and implementation of new security technologies
- Lead response and investigation efforts into advanced/targeted attacks
- Hunt for and identify threat actor groups and their techniques, tools and processes
- Identify gaps in IT infrastructure by mimicking an attacker's behaviors and responses
- Provide expert analytic investigative support of large scale and complex security incidents
- Perform Root Cause Analysis of security incidents for further enhancement of alert catalog

- Continuously improve processes for use across multiple detection sets for more efficient Security Operations
- Review alerts generated by detection infrastructure for false positive alerts and modify alerts as needed
- Develop dashboards and reports to identify potential threats, suspicious/anomalous activity, malware, etc.
- Provide forensic analysis of network packet captures, DNS, proxy, Netflow, malware, host-based security and application logs, as well as logs from various types of security sensors
- A passion for research, and uncovering the unknown about internet threats and threat actors
- Ensure the SOC analyst team is providing excellent customer service and support

Required Qualifications:

- 5+ years of relevant cyber security experience in IT Security, Incident Response or network security with strong knowledge working in a SOC
- 3+ years of experience executing the incident handling process from start to finish, including detecting advanced adversaries, log analysis using Splunk or similar tools, and malware triage
- Experience with creating automated log correlations in Splunk or a similar tool to identify anomalous and potentially malicious behavior
- Demonstrated knowledge of the Splunk search language, search techniques, alerts, dashboards and report building.
- Strong analytical and investigation skills
- Experience with active threat hunting and adversary tracking
- Working knowledge of security architectures and devices
- Working knowledge of threat intelligence consumption and management
- Working knowledge of root causes of malware infections and proactive mitigation
- Working knowledge of lateral movement, footholds, and data exfiltration techniques
- Experience with Netflow or PCAP analysis
- Track record of creative problem solving, and the desire to create and build new processes
- Experience and knowledge of packet flow, TCP/UDP traffic, firewall technologies, IDS technologies, proxy technologies, and antivirus, spam and spyware solutions
- Experience converting intelligence into actionable mitigation and technical control recommendations
- Experience with the Windows file system and registry functions or *NIX operating systems and command line tools
- Knowledge of the underlying logic that security alerts are built upon and apply them when analyzing raw logs and creating new dashboards and alerts

- Knowledge of typical behaviors of both malware and threat actors and how common protocols and applications work at the network level, including DNS, HTTP, and SMB.
- Experience working in fast paced environments, and ability manage workload even during times of stress or escalated activity
- Comfortable with impromptu tasking and loosely defined requirements
- Strong time management and multitasking skills as well as attention to detail
- Strong collaborative skills and proven ability to work in a diverse team of security professionals
- Excellent oral and written communications skills

Preferred Qualifications:

- Experience with one or more scripting languages (e.g., Python, JavaScript, Perl)
- Perform memory and malware analysis
- Experience with computer exploitation methodologies
- Experience as a government contractor

Education Requirement:

- Relevant security certifications (CISSP and GCIA or GCIH)
- Bachelor's degree or higher in a technical field such as Computer Science, Information Security, Information Technology, Computer Engineering, Information Systems, etc.

Send Resume to careers@intellectualpoint.com.