OCTO – SOC Analyst -Tier 2

Short Description:
The SOC Analyst is a tier 2 tech resource responsible for monitoring, detecting, analyzing, remediating, and reporting on cyber events and incidents impacting the tech infrastructure of the District of Columbia. Serves as advanced escalation point.

Skills/Required Years of Experience:
Hands-On Operational Experience As A Cybersecurity Analyst/Engineer In A Security Operations Center (Required 5 Years)
Prior Work With Cybersecurity Attack Countermeasures For Adversarial Activities Such As Malicious Code and DDOS (Required 2 Years)
In-Depth Hands-On Experience Analyzing And Responding To Security Events And Incidents With A Security Information And Event Management System (Required 2 Years)
Strong knowledge of cybersecurity attack methodology to include tactics and techniques, and associated countermeasures. (Required 2 Years)
Strong Knowledge Of Tcp/Ip Protocols, Services, Networking, And Experience Identifying, Analyzing, Containing, And Eradicating Cybersecurity Threat (Required 2 Years)
6-10 yrs developing, maintaining, and recommending enhancements to IS policies/requirements (Required 6 Years)
6-10 yrs performing vulnerability/risk analyses of computer systems/apps (Required 6 Years)
6-10 yrs identifying, reporting, and resolving security violations (Required 6 Years)
Bachelor's degree in IT or related field or equivalent experience (Required)

Complete Description:
The SOC Analyst – Tier 2 is cybersecurity technical resource responsible for providing logical technical analysis, support, and guidance over to a team of Tier 2 and 1 SOC Analysts to monitor, detect, analyze, remediate, and report on cybersecurity events and incidents impacting the technology infrastructure of the Government of the District of Columbia. The ideal candidate will have an advanced technical background with significant experience in an enterprise successfully leading a SOC team or unit or area of responsibility for analysis and correlation of cybersecurity event, log, and alert data. The candidate will be skilled in understanding, recognition, and root-cause detection of cybersecurity exploits, vulnerabilities, and intrusions in host and network-based systems.

SPECIFIC TASKS
– Utilize advanced technical background and experience in information technology and incident response handling to scrutinize and provide corrective analysis to escalated cybersecurity events from Tier 1 and 2 SOC Analysts—distinguishing these events from benign activities, and escalating confirmed incidents to the Incident Response Lead Tier 3 Analysts and/or SIEM Engineer.
– Provide in-depth cybersecurity analysis, and trending/correlation of large data-sets

such as logs, event data, and alerts from diverse network devices and applications within the enterprise to identify and troubleshoot specific cybersecurity incidents, and make sound technical recommendations that enable expeditious remediation.
– Proactively search through log, network, and system data to find and identify undetected threats.
– Support security tool/application tuning engagements, using McAfee ESM and McAfee ePO, with analysts and engineers to develop/adjust rules and analyze/develop related response procedures, and reduce false-positives from alerting.
– Identify and ingest indicators of compromise and attack (IOC's/IOA's) (e.g., malicious IPs/URLs, etc.) into network security tools/applications to protect the Government of the District of Columbia network.
– Quality-proof technical advisories and assessments prior to release from the SOC.
– Coordinate with and provide in-depth technical support to enterprise-wide technicians and staff to resolve confirmed incidents.
– Report common and repeat problems, observed via trend analysis, to SOC management and Tier 3 SOC Analysts and propose process and technical improvements to improve the effectiveness and efficiency of alert notification and incident handling.
– Formulate andSupport development of technical best-practice SOPs and Runbooks for SOC Analysts.
– Respond to inbound requests via phone and other electronic means for technical assistance, and resolve problems independently with minimal supervision. Coordinate escalations with Tier 3 SOC Analysts and collaborate with internal technology teams to ensure timely resolution of issues.

MINIMUM QUALIFICATIONS
– Three or more years of demonstrated operational experience as a cybersecurity analyst/engineer handling cybersecurity incidents and response in critical environments, and/or equivalent knowledge in areas such as; technical incident handling and analysis, intrusion detection, network and hos log analysis, penetration testing, and vulnerability management.
– In-depth understanding of current cybersecurity threats, attacks and countermeasures for adversarial activities such as probing and scanning, phishing, ransomware, command and control (C2) activity, distributed denial of service (DDoS), etc.
– In-depth hands-on experience analyzing and responding to security events and incidents with most of the following technologies and/or techniques; leading security information and event management (SIEM) technologies, endpoint detection and response (EDR), intrusion detection/prevention systems (IDS/IPS), network- and host-based firewalls, network access control (NAC), data leak protection (DLP), database activity monitoring (DAM), web and email content filtering, vulnerability scanning tools, secure coding, etc.
– Strong communication, interpersonal, organizational, oral, and customer service skills.
– Strong knowledge of TCP/IP protocols, services, and networking.
– Knowledge of forensic analysis techniques for common operating systems.
– Adept at proactive search, solicitation, and detailed technical analysis of threat intelligence (e.g., exploits, IOCs/IOAs, hacking tools, vulnerabilities, threat actor TTPs) derived from open-source resources and external entities, to identify cybersecurity

threats and derive countermeasures, not previously ingested into network security tools/applications, to apply to protect the Government of the District of Columbia network.
– Good ability to multi-task, prioritize, and manage time and tasks effectively.
– Good ability to work effectively in stressful situations.
– Strong attention to detail.

PREFERRED EDUCATION/CERTIFICATION REQUIREMENTS
– Undergraduate degree in computer science, information technology, or related field.
– SANS GCIA, GCIH, GCED, GPEN, or similar industry certification desired.

This position requires shift work, and the capacity to be on-call after hours and in support of emergency and special event operations. This position does not require a U.S. Government security clearance. A background check to include criminal and credit check is required. On-going travel is not anticipated.
Responsibilities:
1. Determines enterprise information assurance and security standards.
2. Develops and implements information assurance/security standards and procedures.
3. Coordinates, develops, and evaluates security programs for an organization. Recommends information assurance/security solutions to support customers' requirements.
4. Identifies, reports, and resolves security violations.
5. Establishes and satisfies information assurance and security requirements based upon the analysis of user, policy, regulatory, and resource demands.
6. Supports customers at the highest levels in the development and implementation of doctrine and policies.
7. Applies know-how to government and commercial common user systems, as well as to dedicated special purpose systems requiring specialized security features and procedures.
8. Performs analysis, design, and development of security features for system architectures.
9. Analyzes and defines security requirements for computer systems which may include mainframes, workstations, and personal computers.
10. Designs, develops, engineers, and implements solutions that meet security requirements.
11. Provides integration and implementation of the computer system security solution.
12. Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems.
13. Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle.
14. Ensures that all information systems are functional and secure.

Background check is required, if selected for the position.
There are no reimbursable expenses allocated to this position.