Title:	OCTO - Tier 3 SOC Analyst	**Region:**	District of Columbia
Req ID:	592369		

Details

Requisition Details

Req. Class:	CYSEV1 : 3-Senior	**Region:**	District of Columbia
Title:	OCTO - Tier 3 SOC Analyst		
Req. Status:	Open		
No. of Openings:	1		
Start Date:	05/13/2019		
No New Submittals After:	04/30/2019		

Worksite Address:	200 I Street SE
Agency Interview Type:	Both Phone and In Person
Advanced Technical Screening Required?:	No
Existing Incumbent Resource?:	No

Hours/Units per day: 8

Days per week: 5

Requisition Description

Engagement Type: Contract

Short Description: 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.

Complete Description: SUMMARY The SOC Analyst - Tier 3 is cybersecurity technical resource responsible for providing technical analytical oversight over 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 responsible 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 2 analysts—distinguishing these events from benign activities, and escalating confirmed incidents to the Incident Response Lead. ? 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, verify, 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 SOC. ? Coordinate with and provide expert technical support to enterprise-wide technicians and staff to resolve confirmed incidents. ? Report common and repeat problems, observed via

resolve confirmed incidents. ? Report common and repeat problems, observed via trend analysis, to SOC management and propose process and technical improvements to improve the effectiveness and efficiency of alert notification and incident handling. ? Formulate and coordinate 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. Coordinate escalations with Incident Response Lead and collaborate with internal technology teams to ensure timely resolution of issues. MINIMUM QUALIFICATIONS ? Three to five years of demonstrated operational experience as a cybersecurity analyst/engineer handling and coordinating cybersecurity incidents and response in critical environments, and/or equivalent knowledge in areas such as; technical incident handling and analysis, intrusion detection, log analysis, penetration testing, and vulnerability management. ? In-depth understanding of current cybersecurity threats, attacks and countermeasures for adversarial activities such as network probing and scanning, distributed denial of service (DDoS), phishing, ransomware, botnets, command and control (C2) activity, 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, 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, endpoint protection, 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 analysis of threat intelligence (e.g., exploits, IOCs, 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. ? Excellent ability to multi-task, prioritize, and manage time and tasks effectively. ? Ability to work effectively in stressful situations. ? Strong attention to detail. PREFERRED EDUCATION/CERTIFICATION REQUIREMENTS ? Undergraduate or masters degree in computer science, information technology, or related field. ? SANS GCIA, GCED, GPEN, GCIH or similar industry certification desired. ---------- Contract job description Responsibilities: 1. Coordinates it project management, engineering, maintenance, qa, and risk management. 2. Plans, coordinates, and monitors project activities. 3. Develops technical applications to support users. 4. Develops, implements, maintains and enforces documented standards and procedures for the design, development, installation, modification, and documentation of assigned systems. 5. Provides training for system products and procedures. 6. Performs application upgrades. 7. Performs, monitoring, maintenance, or reporting on real- time databases, real-time network and serial data communications, and real-time graphics and logic applications. 8. Troubleshoots problems. 9. Ensures project life-cycle is in compliance with district standards and procedures. Minimum education/certification requirements: Bachelor’s degree in information technology or related field or equivalent experience

Work Location:	OCTO - 200 I Street, SE Washington DC 20003	**Cost Center:**	OCTO - Office of the Chief Technology Officer
		Project:	

Required/Desired Skills

Required /Desired

Skill	Required /Desired	Amount	of Experience
Hands-on operational experience as a cybersecurity analyst/engineer in a security operations center, or equivalent knowledge.	Required	5	Years
In-depth understanding of cybersecurity attack countermeasures for adversarial activities such as malicious code, DDOS, and phishing.	Required	5	Years
In-Depth Hands-On Experience Analyzing And Responding To Security Events And Incidents With Security Information And Event Management System (SIEM)	Required	5	Years
Strong knowledge of cybersecurity attack methodology to include tactics and techniques, and associated countermeasures.	Required	5	Years
Strong Knowledge Of Tcp/Ip Protocols, Services, Networking, And Experience Identifying, Analyzing, Containing, And Eradicating Cybersecurity Threat	Required	5	Years
11-15 yrs implementing, administering, and operating IS tech such as firewalls, IDS/IPS, SIEM, Antivirus, net traffic analyzers, and malware analysis	Required	11	Years
11-15 yrs yrs utilizing advanced experience with scripting and tool automation such as Perl, PowerShell, Regex	Required	11	Years
11-15 yrs developing, leading and executing information security	Required	11	Years

incident response plans			
11-15 yrs yrs developing standard and complex IT solutions & services, driven by business requirements and industry standards	Required	11	Years
BS Degree in IT, Cybersecurity, Engineering or equivalent experience	Required		

Questions

	Description
Question 1	Absences greater than two weeks MUST be approved by CAI management in advance, and contact information must be provided to CAI so that the resource can be reached during his or her absence. The Client has the right to dismiss the resource if he or she does not return to work by the agreed upon date. Do you accept this requirement?
Question 2	Please list candidate's email address that will be used when submitting E-RTR.
Question 3	There are no reimbursable expenses. Do you accept this requirement?
Question 4	This position is designated to require enhanced suitability by the District of Columbia. Any candidate must get FBI fingerprint background check prior to starting. The candidate must be able to start within 21 days of engagement request. Do you accept this requirement?