|  |  |
| --- | --- |
| ICSLogo_sm.JPG | **Contact:**  Chelsea Teagarden  Senior Technical Recruiter  [cteagarden@icsnets.com](mailto:rrobinson@icsnets.com)  410-901-1002 |
|  |  |

|  |  |
| --- | --- |
| Job Title: | **Senior Gap Team Analyst – SME/ Defensive Threat Analyst** |
| Location: | **Arlington, VA** |
| Schedule: | **TBD** |
| Remote Work Authorized: | **None** |
| Travel: | **None** |
| Clearance Level: | **Secret Required/Top Secret Preferred** |

**Project Overview:**

Provides Threat and Gap Analysis support to a cabinet level federal agency. Contributes to a team of information assurance professionals working to improve technical security posture. Duties include writing reports, briefing event details to leadership, and coordinating remediation with personnel throughout the globe.

Must possess six (6) years of substantive IT knowledge and demonstrate hands-on expertise and/or training in areas of emerging technologies. The candidate must have hands-on experience and expertise with threat detection, gap analysis, threat hunting methodologies, and an understand of the capability of hacking tools and how they are used to exploit vulnerabilities and features in enterprise networks. Previous Red Teamwork is a plus.

The candidate must be a self-starter with, keen analytical skills, curiosity, agility, and adaptability. The ability to work quickly, willingness to work on ad hoc assignments, work independently as needed, strong written and verbal communication skills, and recognizing the importance of being a team player. In addition, the candidate should possess the following skill set:

* Experience analyzing Azure/O365 Logs and their logging platform (eg: Sentinel, Unified Audit Logs, Log Analytics, AAD Audit Logs, Office Activity Logs, etc)
* Advanced Splunk user with the ability to leverage the more advanced statistical features.
* Experience performing incident response using a modern EDR tool.
* Experience performing forensic analysis on the different flavors of Windows OS’s.
* Experience identifying gaps in analysis and creation of detection methodologies to address the gaps.
* Experience analyzing Network Security logs (eg: Firewall, Zeek (Bro))
* Experience with MITRE ATT&CK framework
* Be familiar with tools like Nessus, Burp, and Metasploit Framework/Pro.
* Firm understanding of network and system architecture and analysis. Fundamentals of network routing & switching, assessing network device configurations, and operating systems (Windows/\*nix)
* Experience Scripting in languages such as PowerShell, Bash, Python, Perl or Ruby.
* Must be able to work alone or in a small group.

***Daily Responsibilities:***

* Analyze and document Red Cell activities to identify detection gaps
* Resolve gaps found through monitoring Red Cell activities
* Create new detection methodologies that highlights suspicious activity
* Briefs executive summary and findings to stakeholders to include Sr. Leadership
* Researches and maintains proficiency in tools, techniques, countermeasures, and trends in computer network vulnerabilities, data hiding and network security and encryption.
* Provide support to incident response teams through capability enhancement and reporting.
* Mentor Jr and Mid staff members by creating and teaching latest techniques in ethical hacking and vulnerability analysis.

**Certifications (Preferred but not absolutely required)**

* GCIA, GCIH, or GCFE
* CISSP
* Certified Ethical Hacker
* CCNA

**Years of Experience:**

8+

**Education:**

A Bachelor’s degree in Computer Science, Information Systems, Engineering, Telecommunications, or similar field required. Master’s degree preferred