SECURITY OPERATIONS INTRUSION ANALYST

Posting ID:  
Company: Criterion Systems  
Company Website: www.criterion-sys.com

Company: Criterion Systems  
Company Website: www.criterion-sys.com

Position Type: Full-Time Employment  
Work Location: Las Vegas, NV

Position Type: Full-Time Employment  
Work Location: Las Vegas, NV

College Major(s): Computer Science  
Salary: N/A

College Major(s): Computer Science  
Salary: N/A

College Level(s): Bachelor’s Degree

OVERVIEW

The candidate will be part of the Security Operations Center (SOC) working in a 24x7 environment. The position requires interaction with security personnel at customer sites, various levels of management, and outside agencies. Applicant must be a positive, flexible, self-starter requiring minimal supervision, and able to excel in a fast-paced environment. Communication skills are critical with the ability to verbalize and provide documentation to both technical and non-technical audiences. Applicants must be detail-oriented and have the ability to multi-task effectively.

Duties and Responsibilities:

Monitor, deter, identify, and investigate computer and network intrusions. Ability to research trends and countermeasures in computer/network including vulnerabilities, exploits, and malicious activity. Develop and maintain in-depth knowledge and hands-on experience with computer network security techniques and best practices. Technical focus on the monitoring and analysis of large, distributed and complex network. Candidate must be able to identify suspicious and malicious activity in a heterogeneous network environment and respond appropriately. Responsibilities include, but are not limited to:

- Proficient written and verbal communication with customer representatives
- Research new and evolving threats and vulnerabilities with potential to impact the monitored environment
- Read and understand network packet capture files
- Monitoring and analysis of network and IDS information
- Log collection, analysis, correlation, and alerting
- Identification of suspicious/malicious activities
- Identification and tracking of malicious code
- Reporting malicious activity to client locations with recommendations for remediation
- Review and management of incident resolutions
- Travel up to 10%

Required Skills:

- Must possess active Q or TS clearance, or ability to obtain Q clearance
- US Citizenship required
- Must be willing to work various shifts in a 24x7 environment
- Strong knowledge of networking, common network protocol behavior and information security principles
- Excellent customer service skills
Qualifications / Education:

- Bachelor’s Degree in Computer Science, Information Systems, Information Security or related technical discipline AND 2 years IT experience OR 4 years professional IT experience.
- One or more years’ previous experience in network intrusion analysis is highly desired
- Experience with network and host-based IDS/IPS
- Experience with SIM/SIEM technologies
- The following information security training is highly desired: SANS GSEC, GCIA, GCIH, or CEH, OSCP.

Other:

The above statements are intended to describe the general nature and level of work being performed by people assigned to this job. They are not intended to be an exhaustive list of all responsibilities, duties, skills, or working conditions. Candidates for this position will undergo a government background investigation and must meet the requirements for access to sensitive government information.

How to Apply

Email your resume to Marcie Cheney at Marcie.Cheney@Criterion-sys.com.