CYBER THREAT ANALYST (LONG-TERM)

PostingID: Company: Criterion Systems, Inc. Position Type: Full-Time Website: www.criterion-sys.com Work Location: Las Vegas Salary: DOE College Major(s): Computer Science; Computer Engineering College Level(s): Graduates

OVERVIEW
Criterion Systems, Inc., based out of Vienna, VA is seeking a Cyber Threat Analyst (Long Term) located in Las Vegas, NV to provide support on a fully funded contract with the U.S. Department of Energy.

Monitor, deter, identify, and investigate computer and network intrusions. Ability to research trends and countermeasures in computer/network 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 and information systems. Candidate must be able to identify suspicious and malicious activity in a heterogeneous network environment and respond appropriately.

Once brought on board, you will be required to successfully pass the CompTIA Security+CE exam.

• 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
• Use of Security Information and Event Manager (SIEM)
• Build correlations
• 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

Qualifications:
• 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.
• Must be willing to work various shifts in a 24x7 environment
• RSA envision /RSA Security Analytics/ HP ArcSight/ IBM QRadar platforms or similar solutions
• Ancillary experience with Information System Security, System Security Plans, Scanning of Systems, C&A Actions
• Simulate the log sources and test the security use-cases in test environment.
• Strong knowledge of networking
• Strong knowledge of common network protocol behavior
• Strong knowledge of information security principles
• Excellent verbal and written communications skills
• Excellent customer service skills
• Other duties as assigned
- Travel up to 10%
- U.S. Citizenship
- Active Secret Clearance, SSBI (Single Scope Background Investigation) or Department of Energy “L” Clearance, with the ability to upgrade to a Department of Energy (DOE) “Q” Clearance or Top Secret Security Clearance

PREFERRED BUT NOT REQUIRED
- 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, SANS GCIA, SANS GCIH, CEH, OSCP

Where To Apply:
Apply online at: recruiting@criterion-sys.com

Criterion Systems is committed to hiring and retaining a diverse workforce. We are proud to be an Equal Opportunity/Affirmative Action-Employer, making decisions without regard to race, color, religion, creed, sex, sexual orientation, gender identity, marital status, national origin, age, veteran status, disability, or any other protected class.