UNLV, Howard R. Hughes College of Engineering

CYBER THREAT ANALYST

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

OVERVIEW
Criterion Systems, Inc., based out of Vienna, VA is seeking a Cyber Threat Analyst to support fully-funded contract in Las Vegas, NV. The Cyber Threat Analyst (CTA) will support a rapidly changing environment with short suspense deliverables and diverse work assignments in support of a U.S. Government Agency Security Operations Center. The position requires familiarity with classified and unclassified computer security and intrusion analysis.

The right candidate will have an excellent professional demeanor, good people skills, the ability to excel in a multi-tasked and dynamic environment, the ability to work remotely and independently, prioritize tasks, and the ability to take complex technical information and relate those details to management.

Qualifications:

ESSENTIAL SKILLS & RESPONSIBILITIES:
- Bachelor's Degree in Computer Science, Information Systems, Engineering, or other related discipline
- Minimum of two (2) years related experience with Bachelor's Degree or six (6) years related experience without Bachelor’s Degree
- Minimum one (1) year of experience in network intrusion analysis or computer network security or equivalent experience and training
- Embedded with the Network Intrusion Analysts, the Cyber Threat Lead will be primarily responsible as subject matter expert (SME) for all custom intelligence-based alerts, and will be the representative of the organization in all threat-related activities
- Significant written and verbal communication is required for this role, including site notices, analysis reports and executive summaries of cyber threats and APT activity, ticketing and documentation, and formal and informational briefings to community Computer Network Defense (CND) professional staff and senior management
- Collaborate with the IDS Engineers and SIEM Engineers to reduce false positives while maximizing capture of suspect traffic
- Present new technical details of relevant activity detected (when applicable) in the semi-monthly classified Incident Responder Technical VTC
- Must be proficient at analyzing and interpreting network traffic for indications of malicious activity
- Process historical intelligence reports and update database(s) as required
- In depth analysis into historical alerts and/or incidents of interest
- Coordinate training sessions for the SOC-RTAs and other personnel on interesting and relevant cases designed to improve their monitoring and analysis skills
- Cross-train with other Threat Analysts and Network Intrusion Analysts in the organization to provide redundant skills coverage
- Collaborate with Long Term Analyst on monthly report information and metrics
- Other duties as assigned
- U.S. Citizenship
- Department of Energy (DOE) "Q" Clearance or Top Secret Security Clearance
DESIRE BUT NOT REQUIRED:

- SANS GSEC, SANS GCIH, SANS GCIA, CEH or equivalent certification
- High-level briefing experience to senior level management highly desired

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.

Where To Apply:

Apply online at: recruiting@criterion-sys.com