SOC Analyst Job

Employer Name:

SpiderID: 12421717

Location: Chandler, Arizona

Date Posted: 4/15/2022

Wage: Negotiable

Category: Information Technology

Job Code: 2022-149

Supports the creation of cyber-intelligence tools / methods and assists with research and analysis in order to mitigate and eliminate data and cyber security risks. Assists with the development of acceptance criteria for cyber security architecture.   
  
Job Responsibilities  
  
\* Monitoring and analyzing network traffic, Intrusion Detection Systems (IDS), security events and logs; Prioritizing and differentiating between potential intrusion attempts and false alarms.  
  
\* Develop, maintain, and follow SOC Standard Operating Procedures (SOPs).  
  
\* Proactively reviewing large data sets for anomalous activity, and support daily and monthly reporting per shift.  
  
\* Create detective content for monitoring devices such as IDS and SIEM and advise on proactive blocks for security architecture.  
  
\* Creating and tracking security investigations to resolution.  
  
\* Composing security alert notifications and other communications.  
  
\* Advising incident responders in the steps to take to investigate and resolve computer security incidents.  
  
Minimum Qualifications  
  
Bachelor's Degree in Computer Science or a related field or equivalent experience.  
  
2 years of experience in systems security. Active Secret Clearance.  
  
Certifications  
  
Certified Ethical Hacking (CEH) Certification or CompTIA CySA+ AND (within 6 months of hire) any from the CSSP Analyst, Infrastructure Support, or IR from the DOD8570 list (or other similar certifications as approved by Government)  
  
Other Job Specific Skills   
  
\* Staying up to date with current vulnerabilities, attacks, and countermeasures.   
  
\* This position requires the ability to work a shift schedule.   
  
\* The ideal candidate should be able to multitask and give equal attention to a variety of functions while under pressure.  
  
\* Experience in handling incident response.

Start Date:   
  
  
Position Type: Full-Time Permanent  
  
  
Years of Experience Required:   
  
  
Education Required:   
  
  
Overnight Travel:   
  
  
Vacation Time:

Contact Name: Dunhill Professional Search

Company: Dunhill Professional Search