Security Operations Center Analyst

Role Description

Analyzes a variety of network and host-based security logs (Firewalls, NIDS, HIDS, Syslog). Administers, monitors and troubleshoots antivirus activities. Assists with security-related software and firmware (e.g., endpoint, vulnerability scanners, firewalls, IPS/IDS, DNS, proxy) to maintain security and service continuity. Assist with the resolution of security-related infrastructure. Participate in security incident response through in-depth, technical (log, forensic, malware, packet,) analysis. Perform security alert detection and analysis capabilities across multiple technologies to ensure that security incidents are identified in a timely manner. Escalate and support potential security incidents in line with appropriate processes. Support communications of potential security incidents via multiple channels. Participate in the response to potential security incidents by identifying and communicating relevant supplementary information.

Levels

Level	Education	Years' Experience
Junior	Bachelor or Equivalent in related field	0 to 2
Journeyman	Bachelor or Equivalent in related field	2 to 5
Senior	Bachelor or Equivalent in related field. Master's Preferred in related field	5 to 8
SME	Bachelor or Equivalent in related field. Master's Preferred in related field	8 or more

Clearance(s)

One or more of the following clearances may be required:

Secret / Top Secret / SCI Eligibility / Agency Specific