



Position Title: Security Operations Analyst

Description:

The Security Operations Analyst provides operational support & analysis for a diverse set of network and endpoint security technologies. The Security Operations Analyst will operate technologies that prevent and detect threats, monitor alert data from technologies and correlate with intelligence sources to determine the type & severity of the threat and recommend appropriate actions, including escalation to senior staff.

Key Responsibilities

- Operate and manage network security technologies including firewall, proxy, IDS, and network access control
- Operate and manage endpoint security technologies including advanced threat prevention and endpoint forensics
- Participate in security incident response through in-depth, technical (log, forensic, malware, packet, etc.) analysis
- Collect security incident metrics & data to enable reporting to senior management

Experience Requirements:

- Experience with network security technologies such as firewalls, proxies, network and host-based intrusion prevention, security information/event management, endpoint security, anti-virus/anti-malware, etc.
- Familiarity with analysis & research methods
- B.S. in Computer Science or Engineering or similar technical program
- 2-4 years in a technical analyst role
- Information security experience a plus

Professional Competencies:

- ☑ Strong written and oral communication skills
- ☑ Actively collaborates and pitches in when necessary to support team success
- ☑ Able to work on multiple activities at the same time, organizing and prioritizing as needed to accomplish goals
- ☑ Enables process improvement by stimulating ideas through discussion and collaboration

Smrity

smriti@desiderate.in

9811676086