Cyber Security Analyst

As a member of a team of experienced security analysts and engineers the candidate will focus on security information and event management (SIEM), analysis/correlation of events, security incident handling in complex corporate environments, contributing to the overall performance and success of the Security Operations Center (SOC).

Duties & responsibilities

- Managing the response to alerts and identification of the underlying issue
- Creating correlation rules in SIEM to detect new threats
- Performing Security Incident Handling
- Conducting Computer/Network forensics
- Providing Cyber Threat intelligence

Required Skills

- Bachelor's degree in computer science or related field
- Understanding of advanced concepts in networking, firewalls, proxies, SIEM, antivirus, IDS/IPS, DLP, Operating systems, Databases
- Experience with scripting languages (bash, perl, python, etc.)
- OS: Windows, UNIX/Linux
- Databases: SQL
- Networking: TCP/IP protocol suite (IP, TCP, UDP, HTTP, DNS, SMTP, FTP, etc.)
- Security: IDS/IPS, firewalls, vulnerability scanners, etc.

Preferred Skills

- Experience in SIEM platforms (Arcsight, Qradar, etc.)
- Experience in data science concepts, machine learning, etc.
- Knowledge of computer/network forensic tools, technologies and methods