Threat Hunter

Responsibilities

- Perform intrusion analysis using SIEM technology, packet captures, reports, data visualization, log analysis and pattern analysis.
- Finetune EDR for blocking and reporting based on customer business need
- Assist SOC Analyst by providing next level in-depth analysis
- Conduct pro-active threat hunting and analysis
- Respond to security incidents and perform investigation
- Characterize suspicious binaries and be able identify traits, C2, and develop network and host-based IOCs
- Interact and assist other investigative teams
- Through review and analysis of cyber threats, provide both internal & external parties key information to respond to threat.
- Analyzing data from technical security controls, such as firewalls, IPS/IDS, enterprise AV, network analyzers
- Deploy and maintain EDR sensors and tools
- Identify incident root cause and develop proactive mitigation steps

Education

- Bachelor's degree in Computer Science, Computer Engineering, Information Technology or IT related field.

Knowledge and Technical Skills

- Effective written and verbal communication skills to interact with customers
- Keeps current on the current IT threat landscape and upcoming trends in security
- Knowledge on Information security best practices & network security architecture, Cyber Kill chain and MITRE ATT&CK Framework
- Hands-on experience in SOC devices such as SIEM and EDR
- Hands-on working experience with EDR will be advantage
- Strong knowledge of Linux, Windows system internals.
- Strong knowledge of web applications and APIs
- Demonstrated relevant experience as a key member of a threat intel, incident response, malware analysis, or similar role.
- Strong knowledge of malware families and network attack vectors.
- Knowledge of the TCP/IP networking stack or network IDS technologies
- Experience with IT infrastructure
- Experience with operational security, including security operations center (SOC), incident response, malware analysis, or IDS and IPS analyse