SOC Use Case Development Engineer

Job Description

We are searching for a SOC Engineer who will be responsible for analyzing, developing the SOC Use Case and Playbook to detect the Cyber security attack.

The primary function of this position is to analyze the attack result to improve the detection rate and reduce the time needed for incident investigation by using automation.

Responsibilities

- Collaborate with the Security Operations Center (SOC) and Security Engineering teams to improve existing security automation technology
- Assess, design, and improve SOC processes and workflows with an aim on automation through Security Orchestration, Automation and Response (SOAR) and cyber security technology to improve detection flexibility and reliability.
- Build SOC Use Case and Playbooks to properly triage and respond to security incidents while reducing the time needed to analyze each event.
- Analyze SOC alerts statistics and workflows to reduce false positives and properly focus engineering efforts.
- Develop custom scripts to automate current detection and response workflows.
- Enrich Incident results to provide comprehensive view for customers

PREFERRED SKILLS AND EXPERIENCE:

- Understanding of classic and emerging threat actor tactics, techniques and procedures in both pre and post-exploitation phases of attack lifecycles.
- Experience using Python for the purpose of automating security operations and incident response processes.
- Strong understanding of security architecture, tool integration, API development and automation.
- Understanding of common SOC and SOAR processes and workflows.
- Working knowledge of network TCP/IP protocols.

- Experience using Splunk and/or other SIEMs.
- Exceptional written and verbal communication skills.
- Exceptional organizational skills.

BASIC QUALIFICATIONS:

- Bachelor's degree in information systems, information security, computer science, engineering or similar technical field of study with 2+ years of information security experience;
- Experience with network and endpoint security solution, such as IPS, Firewall, Response (EDR) platforms.
- Experience with Python scripting language for automation.
- Experience with operating system internals for both Linux and Windows platforms.