Cyber Security Analyst (L1)

Job Description:

The Cyber Security Analyst provides 24x7 eyes-on-glass service; formed from a team of security analysts with some years of experience. The monitoring and identification tier are responsible for the real-time monitoring and identification of security incidents. Analysts staffed at Level 1 monitor the MDR Centre main channel event streams within the MDR Centre security information and event management (SIEM) platform, SOAR and other MDR Centre tools. They identify suspicious activity, open an incident investigation and perform preliminary investigation to validate the incident. If the incident is determined to be more complex and requires more time and/or deeper expertise to analyze, the Tier 1 – Analyst will transfer the open investigation to Tier 2 for further analysis and escalation.

Cyber Security Analyst is also responsible for providing a combination of strategic, tactical and operational intelligence to the MDR Centre and its constituency. They gather and analyze tactical cyber threat and vulnerabilities intelligence and provide timely intelligence support to incident responders and guidance to threat hunter.

In addition, Cyber Security Analyst is responsible for the validation and analysis of investigations passed up from Tier 1 analysts. Tier 2 incident responder and investigator will complete the documentation of the investigation, determine the validity and priority of the activity and escalate to the SOC Manager. Analysts staffed at Level 2 would be senior staff.

Key Responsibilities:

- Performs real-time monitoring of security alerts generated by various MDR tools deployed by True Digital.
- Investigates potential security incidents under the guidance of playbooks and procedures.
- Analyses and assesses security alerts.
- Validates, classifies and opens security incident cases or escalates to Level 2 analysts.
- Serves as a primary contact point for reporting potential security incidents.
- Document security incidents as identified by the case management process.
- Provides feedback on enhancing the operations of the cyber security operations center.
- Responds to security alerts generate within the SLA time window.
- Establishes priority intelligence requirements for all key stakeholders.
- Demonstrates an understanding of business processes, risk management, and related standards and regulatory requirement.
- Performs threat modeling to identify, classify, prioritize and rate threats based on thorough analysis of the organization's top risks and critical assets, and derive appropriate use cases to be implemented into the MDR platform.
- Investigates and researches known indicators, correlate events, identify malicious activity, and discover new sources to provide early warning for a variety of threats.

- Analyzes internal and external threat intelligence data sets, including vulnerabilities intelligence, detect and track emerging threats and security trends.
- Produces timely, accurate, relevant and predictive intelligence by identifying and reporting on malicious actors, campaigns, and other relevant activities.
- Produce and deliver timely, actionable threat intelligence to foster situational awareness, enables proactive decision-making, and promote enhance active defense measures within True Digital.
- Monitors open source information feeds and threat actor activity to identify activity levels and indicators for threats, targets of interest and possible attack vectors.
- Work with the other MDR Centre team to ensure that actionable indicators of compromise are incorporated into appropriate technologies.
- Proactively recommends short-term and long-term changes based on threat intelligence to improve MDR Centre tools and detection capabilities.
- Recognizes successful intrusions and compromises through review and analysis of relevant event detail information.
- Investigates potential security incidents - recognizes attacks based on techniques, tactics and procedures and differentiates false positives from true intrusion attempts.
- Follow up and track investigations to resolution.
- Further validate, classify incidents and update security incident cases.
- Alert system and information owners of intrusions and potential intrusions and compromises to their network infrastructure
- Escalate security incidents to appropriate teams
- Provide an assistance during remediation of security incidents.
- Security services management including finetuning security use cases.
- Fine tuning SIEM tools and reducing false positives.
- Update the MDR tools as necessary.
- Continuously improve the MDR services.
- Maintain and provide data required to calculate the MDR Centre services' SLAs, KPIs and KRIs.
- Update MDR processes and procedures as necessary.
- Follow and implement the change management process.
- Publish regular reports to internal teams.
- Conduct regular information security awareness sessions to the general community of the organization.

Qualifications:

- Bachelor degree in a related field such as information security, management or computer engineering.
- Platform-specific certifications are desirable.
- Good working knowledge of security concepts for both Windows and Unix related operating systems.
- Good working knowledge of network concepts.
- Familiar with well-known SIEM tools (e.g. Splunk and ELK) and dashboard/analytic tools (e.g. Grafana).
- Familiar with SOAR and UEBA tools.
- Working experience in a MDR Centre, Security Operations Centre (SOC), Managed Security Service Provider (MSSP) or enterprise network environment preferred