# 

**REFLECTIVE JOURNAL #2**

Stephen Antwi

One of my major work duties is reviewing incidents to keep the Port of Virginia safe from cyber-attacks. This duty encompasses collaborating with other security analysts in detecting and responding to information security incidents. Also, reviewing incidents entails defining the review`s objectives and scope. It is essential to note that the scope includes the risk type, severity, and duration. Apart from defining the review, the incident review involves gathering and analyzing the relevant data from the incident. In reviewing the incidents, I usually collect data from logs, reports, alerts, emails, tickets, surveys, and feedback from the external sources, affected parties, and the incident response team. I have learned how to use charts, diagrams, tables, and timelines to document, organize and correlate gathered data. Also, incident review encompasses identifying and prioritizing findings and generating and implementing recommendations. Reviewing incidents is necessary for the organization because it helps the security team know some of the cyber threats the organization faces so that it can lay out adequate measures to prevent them.

The other major work duty I performed at my internship is monitoring the organization`s security using Microsoft Sentinel and Microsoft Defender. With the help of the reference architecture, I have learned how to use Microsoft Sentinel and Microsoft Defender to monitor the organization`s security configuration and Azure Stack workloads. This duty is necessary to the organization because it helps in securing the organization`s network system. Monitoring the network system is a critical function to detect and prevent security cyber threats. The third major duty I perform in my internship is reviewing all quarantine emails. In performing this duty, I usually follow the Microsoft 365 Defender guidelines for finding and viewing the quarantine emails. Reviewing the quarantine emails is important because it helps protect the organization`s network infrastructure and users from malicious programs sent through email.

The fourth major work duty I perform is reviewing applicable cyber threat intelligence from cyware. Cyber threat intelligence refers to the evidence-based knowledge or information of the existing or emerging threat`s resources, capabilities, motives, and goals (Cyware Labs, 2023). This duty is crucial because it provides an appropriate context for the organization`s security team to better comprehend and pinpoint the adversaries in addition to informing decisions concerning responding to security hazards. The fifth major work duty I perform as an intern is to monitor Virtual Private Network (VPN) traffic and add pattern correlation documents. Typically, performing this duty involves monitoring and optimizing the organization`s VPN performance by analyzing the VPN logs. Some of the software applications I employ include SolarWinds, Splunk, and LogRhythm. Monitoring VPN traffic is important because it helps in assessing the effectiveness of the organization`s VPN in securing incoming and outgoing traffic.

The sixth and last major work duty I performed in my internship is reviewing policies, updates, and tracking. This duty entails scanning the macro environment for any changes in the regulation of information technology and determining if the organization`s policies comply with the policies. It also entails identifying some of the updates that should be made to the existing policies to enhance their effectiveness in addressing security issues facing the organization. Performing this duty is imperative in the organization because the organization needs to ensure its security policies are up to date. That way, the organization will efficiently secure its infrastructure. I also started working on my project (MITRE ATT&ACK FRAMEWORK).