CYSE 368 Reflective Journal #1

Kenneth A. Piontek

Old Dominion University

Dr. Saltuk B. Karahan

I am not currently enrolled in an internship, I'm well within my career as a Cybersecurity Professional working for the Department of Homeland Security working as an Information System Security Officer overseeing the security operations of two major information systems. In this journal I'd like to reflect on one aspect of my work this week, the challenges, and in as much detail as I'm allowed to provide how I went about solving the problem. Part of my primary and ancillary duties falls within the realm of incident response. While on a completely unrelated matter in which I need to look at some AWS logs in order to obtain an artifact to close out a POAM (Plan of Action and Milestone). I noticed some odd traffic patterns within the vpc (Virtual Private Cloud) flow logs which prompted me to do a further investigation such that it warranted me opening up an incident within our SOAR (Security Orchestra Automated Response) platform where incidents are logged and tracked. I ensured the status of the ticket was set such that everyone who looked at it knew that I was still investigating the issue.

What I had to solve for here is whether the traffic I saw was authorized or not, and if not whether this was malicious or just a policy violation, as well as if unauthorized what damage if any could be determined was done. I continued one with the detection and analysis phase of my investigation obtaining the AWS (Amazon Web Services) service specific log files, which led me to realize that I needed the operating system specific logs from several ec2 (Elastic Compute Cloud) instances and other devices within the security boundary of that system they resided in. Once I had all the information I needed I conducted a series of interviews based on the information I had already gathered. Upon completion of the interviews the determination was made that it was unauthorized and from there I moved onto the containment phase, while the detection and analysis phase continued as well. The services and systems in question were all isolated from any further action by users and prevented from communicating with any other network addresses. At that point the limits of my authority and access were reached and the issue had to be escalated to the team within the SOC along with the notes and artifacts that I had collected. From there the hand off was made from myself to the team better suited to further the investigation and then recommend any corrective actions (technical, administrative, or other) that may need to be taken as a result. In this particular case there were a series of both technical and administrative controls that were put into place as a result of the investigation.

Earlier I detailed what I had to solve while working on this issue, that being whether the traffic I saw was authorized or not, and if not whether this was malicious or just a policy violation, as well as if unauthorized what damage if any could be determined was done. All this was done through a combination of my own efforts and those of two other teams. Before starting the process of implementing the technical and administrative controls an executive summary of the activity had to be completed, submitted and briefed to leadership which I was responsible for. Throughout the course of working on the issue I did have the opportunity to learn more about policy, law, and process within my organization and best practices with regards to technical control implementation within an AWS environment.