Cyber Range Lab Assignment 6

SIEM Architecture and Process

Jon Mahoney

SRA 440W

## General Context

The SIEM Architecture and Process learning path describes what a SIEM system is, the functions SIEM systems carry out, and the different SIEM systems provides by organizations. The instructor begins the learning path by explaining the role of a security information and event management system and how SIEMs function. SIEMs are centralized and organized platforms that take in information and output structured data in a clear and concise manner for the purpose of informed decision making. For this reason, SIEM are best used to detect and respond to incidents and provide no protection against incidents. In the videos, the instructor uses the SIEM called Graylog to examine system logs from a malware event. The SIEM provided the instructor with system information such as the location of the device, the name of the device, and even the phone number of the user assigned to the device.

Another SIEM function that is arguably the most critical is the ability to streamline compliance with business and regulatory law. The video describes standards for compliance such as PCI DSS for payment processing, HIPAA for health care information, and Sarbanes Oxley for auditing accountability. For an organization to be compliant with these different log auditing regulations without using a SIEM, they would have to navigate to many different locations to find log files and pick out the relevant information. When using a SIEM system, the system will load incoming log messages in the dashboard, allowing the user to click through each log message and view a compiled report on the event. SIEM systems can interact with different applications, operating systems, hypervisors, and networks. Many different organizations sell SIEMs with different features, but they generally fill the same role of enhancing detection and response. For instance, the IBM and Oracle SIEMs provides automatic anomaly detection by comparing incoming network activity to previously established baselines.

# Screenshot

