Jakub Olsovsky

Assignment 6 – *Intro to Siem*

Professor Yantorno

CS298-71

**Task 1: Introduction**

Security Information and Event Management System or SIEM is a tool that collects data from various endpoints/network devices across the network, stores them at a centralized place, and performs correlation on them.

**Task 2:**

Two types of Sources:

* Host-Centric Log Sources
  + capture events that occurred within or related to the host
* Network-Centric Log Sources
  + generated when the hosts communicate with each other or access the internet to visit a website

Importance of SIEM:

Not only does SIEM take logs from various sources in real-time but also provides the ability to correlate between events, search through the logs, investigate incidents and respond promptly

**Graphical user interface, application

Description automatically generated with medium confidence**

**Task 3:**

Logging Host-Centric Log Sources and Network-Centric Log Sources can be done on both Windows and Linux operating systems, as well as Web servers.

**Graphical user interface, text, application

Description automatically generated**

**Task 4:**

Here we discuss the importance of using a visual tool like the Security Information and Event Management System

**Task 5: Analysis of Logs and Alerts**

**A picture containing graphical user interface

Description automatically generated**

**Task 6: Lab Walkthrough**

**Graphical user interface, application

Description automatically generated**

**Timeline

Description automatically generated**

**Table

Description automatically generated with medium confidence**

**Graphical user interface, application, Teams

Description automatically generated**

**Graphical user interface, text, application, email

Description automatically generated**

**Solutions for Task 6:**

**A picture containing graphical user interface

Description automatically generated**