Ministry of Higher Education and Scientific Research, Iraq

University of Babylon

information technology collage

Information Security Department

Morning Study

Integrated Intrusion Detection System with Security Information and Event Management

A Graduate Project Submitted to the Department of Information Security of the College of Information Technology, University of Babylon, in Partial Fulfilment of the Requirements for the Bachelor's degree in Information Security of Information Technology.

STUDENT'S NAME

Haider Naseer Ali Shokr

Supervised by

Assist. Lec. Noor Razzaq Obaid

2023-2024

ABSTRACT

In the area of Information Warfare, the malicious actors try to penetrate the network devices and delete their traces. To detect such network intrusion, we need to continuously monitor logs of every network-connected device. SIEM solution is used for centralized collection, analysis, normalizing, and correlating all files and data coming from the various devices and gives a centralized view of logs with Dashboards. with capabilities such as incident management, monitoring, preventing, responding, and reporting. HIDS and HIPS inspect each & every packet traveling through the network, preventing, detecting, and generating alerts using pre-defined signatures and Rules. So, we design and implement, a solution by integrating the different IDS/IPS/EDR like Snort, Suricata, Wazuh, and Bro with Elastic SIEM solution to provide enhanced Information Security in an environment.

As for the results, it is a collection of all the logs from various devices, as well as detecting and preventing security threats represented by malware and attacks.