الجزائرية الديمقراطية الشعبية الجمهورية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

المدرسة العليا للإعلام الآلي - 08 ماي 1945 – بسيدي بلعباس
Ecole Supérieure en Informatique
-08 Mai 1945- Sidi Bel Abbes

Thesis

To obtain the diploma of **Engineer**

Field : **Computer Science**

Specialty : **Computer Systems Engineering**

"Ingénierie des Systèmes Informatiques (ISI)"

Theme

Threat hunting using an ELK-based SIEM system

Présenté par **:**

- Mr. Maouche Chafik
- Mr. Mehanneche Mohamed Sedik

Presented on : **06/07/2022** In front of the jury composed of :

- Mr. KAZI TANI Mohammed Yassine	President
- Mr. BENDAOUD Fayssal	Supervisor
- Ms. ANANI Djihed	Reviewer

Academic Year : 2021 / 2022

Abstract

Log management is an essential part of the life cycle of information security. This approach consists in defining a set of technical and organizational measures to cope with the various threats to the information heritage of an organization. In this perspective, the SIEM solution makes it possible to examine and centralize the large number of event logs generated by the different units of the SI. These logs are a wealth of information essential for safety. They provide information about access to the system by users, network anomalies, outages, compliance with regulations and security policy, intrusions and data theft, etc.

Key Words : Log management, Centralized analysis, Gestion de l'information et des événements de sécurité, Chasse aux menaces, cyber-sécurité.

Resumé

La gestion des journaux est une partie essentielle du cycle de vie de la sécurité de l'information. Cette approche consiste à définir un ensemble de mesures techniques et organisationnelles pour faire face aux différentes menaces pesant sur le patrimoine informationnel d'une organisation. Dans cette perspective, la solution SIEM permet d'examiner et de centraliser le grand nombre de journaux d'événements générés par les différentes unités du SI. Ces journaux sont une mine d'informations essentielles pour la sécurité. Ils renseignent sur l'accès au système par les utilisateurs, les anomalies du réseau, les pannes, le respect de la réglementation et de la politique de sécurité, les intrusions et vols de données, etc.

Mots Clés : gestion des journaux, Analyse centralisée, chasse basée sur des hypothèses, threat hunting intelligence, cyber-sécurité.