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 **Master**

Field : **Computer Science**

Specialty : **Computer Systems Engineering**

"Ingénierie des Systèmes Informatiques (ISI)"

Theme

Threat hunting methodologies: a comparative study

Presented by **:**

- Mr. Maouche Chafik
- Mr. Mehanneche Mohamed Seddik

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

Cyber attackers are getting extremely skilled at gaining unnoticed access to systems. It's not uncommon for an organization to be completely oblivious to an intrusion for days, weeks, or even months.

Companies can't just sit back and wait for an automated alert to notify them that their security has been compromised. It must actively monitor the network for potentially malicious behavior. That is why there is a shift toward a more proactive approach: threat hunting.

In this thesis, we will have a look at different threat hunting methodologies and compare each aspect of them, so that companies can be able to choose the most suitable methodology to implement in their environment.

Key Words : threat hunting, proactive approach, hypothesis based hunting, threat hunting intelligence, cyber security.

Résumé

Les cyber criminals deviennent extrêmement habiles à obtenir un accès inaperçu aux systèmes. Il n'est pas rare qu'une organisation soit complètement inconsciente d'une intrusion pendant des jours, des semaines, voire des mois.

Une entreprise ne peut pas simplement s'asseoir et attendre une alerte automatisée pour être informée que sa sécurité a été compromise. il doit surveiller activement le réseau pour détecter tout comportement potentiellement malveillant. A cause de ca il y a un changement vers une approche plus proactive: threat hunting.

Dans cet article, nous examinerons les différentes méthodologies de threat hunting et comparerons chaque aspect d'entre elles, afin que les entreprises puissent choisir la méthodologie la plus adaptée à leurs environement.

Mots Clés : chasse aux menaces, approche pro-active, chasse basée sur des hypothèses, threat hunting intelligence, cyber-sécurité.