SIEM

SECURITY INFORMATION AND EVENT MANAGEMENT

AUTEUR : DELAUTRE BENJAMIN

SOMMAIRE

- Résumé de l'épisode précédent – Les ***IoC***
- Avant propos sur les disciplines ***SEM***, ***SIM*** et ***SIEM***
- Tentative de distinctions des trois disciplines
- Brève explication des fichiers **logs**
- Comment fonctionne le SIEM
- Quelques exemples
- **Bonus** (une question de bon sens ?)

RÉSUMÉ DE L'ÉPISODE PRÉCÉDENT…

- Dans la veille précédente, deux nouvelles notions avaient été abordées :
  - ***IoC*** (*Indicator of compromise*) une trace laissée sur un réseau ou dans un système d'exploitation qui indique, en général, une intrusion informatique
  - ***IoA*** (*Indicator of Attack*) un évènement ou une trace qui indique qu'une attaque est en cours sur un réseau
- Ces deux indicateurs, qui peuvent se compter par millier pour les plus grands réseaux, sont concentrés dans des outils qu'on appelle des ***SIEM*** *(Security Information and Event Management*) qui permettent de mieux lire l'ensemble de ces évènements et informations.

SEM, SIM, SIEM – *KÉZACO ?*

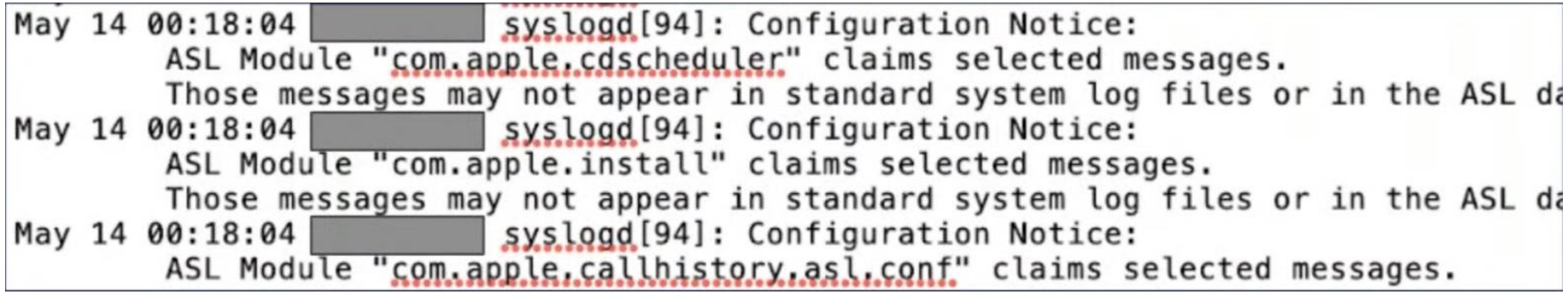
- SEM, SIM et SIEM sont des **disciplines de sécurité informatique** qui utilisent des outils d'inspections des données pour stocker et interpréter les logs et les events sur un réseau.
- Ces différents courants sont parfois difficiles à différencier (distinction au slide suivant)
- Pour les dates d'apparitions de ces disciplines : abstentions de ma part (problèmes de sources)
- Ces disciplines disposent de leurs propres outils qui permet de monitorer les réseaux.

HISTOIRES D'ACRONYMES DE PROCESS

- ***SIM*** – *Security Information Management*
  - Stockage sur le **long terme, rapport** et analyse de fichier log
  - EN SIMPLE, voyons le comme un processus à spectre large sur le long terme, où plusieurs données peuvent être analysées méthodiquement
- ***SEM*** – *Security Event Management* :
  - Monitoring en **temps réel**, corrélations d'évènements et notifications.
  - En SIMPLE, des **types spécifiques d'événements** utilisateur qui peuvent constituer des signaux d'alerte ou indiquer aux administrateurs des informations spécifiques sur l'activité du réseau
- ***SIEM*** – *Security Information AND Event Management* :
  - Combine le SIM et le SEM et fournit des analyses en temps réels ainsi que des alertes de sécurité

LES LOGS – PARTIE I

- Un fichier **log** est un historique de tout et de tout ce qui se passe dans un système, y compris des événements tels que des transactions, des erreurs et des intrusions.
- Les informations de **base d'un log** sont :
  - **Le temps** : à quelle heure s'est passé l'évènement
  - **Les informations utilisateurs** : qui a fait quoi
  - **Les infos de l'évènement** : quelles actions ont été faites,…



LES LOGS – PARTIE 2

- D'où viennent les logs et qui en produit ? PRESQUE tout. Liste non exhaustive :
  - Firewall
  - Apps
  - Appareils connectés (IoT)
  - Réseau
  - Serveurs
  - Services Web

(Une personne qui aime beaucoup les logs)

LES LOGS – PARTIE 3

- Les types de logs :
  - ***Event logs*** – high-level log qui enregistre des informations sur le trafic et l'utilisation du réseau, telles que les tentatives de connexion, les tentatives de mot de passe infructueuses et les événements d'application.
  - ***Server logs*** - document contenant un enregistrement des activités liées à un serveur spécifique dans une période de temps spécifique.
  - ***System logs*** - syslog, est un enregistrement des événements du système d'exploitation. Il comprend les messages de démarrage, les modifications du système, les arrêts inattendus, les erreurs et les avertissements, ainsi que d'autres processus importants. Windows, Linux et macOS génèrent tous des journaux système.
  - ***Authorization logs*** - incluent une liste de personnes ou de bots accédant à certaines applications ou certains fichiers.
  - ***Change logs*** - Les journaux des modifications incluent une liste chronologique des modifications apportées à une application ou à un fichier.
  - ***Availability logs*** - suivent les performances et la disponibilité du système.
  - ***Resource logs*** - fournissent des informations sur les problèmes de connectivité et les limites de capacité.
  - ***Threat logs*** - contiennent des informations sur le trafic du système, des fichiers ou des applications qui correspondent à un profil de sécurité prédéfini au sein d'un pare-feu.

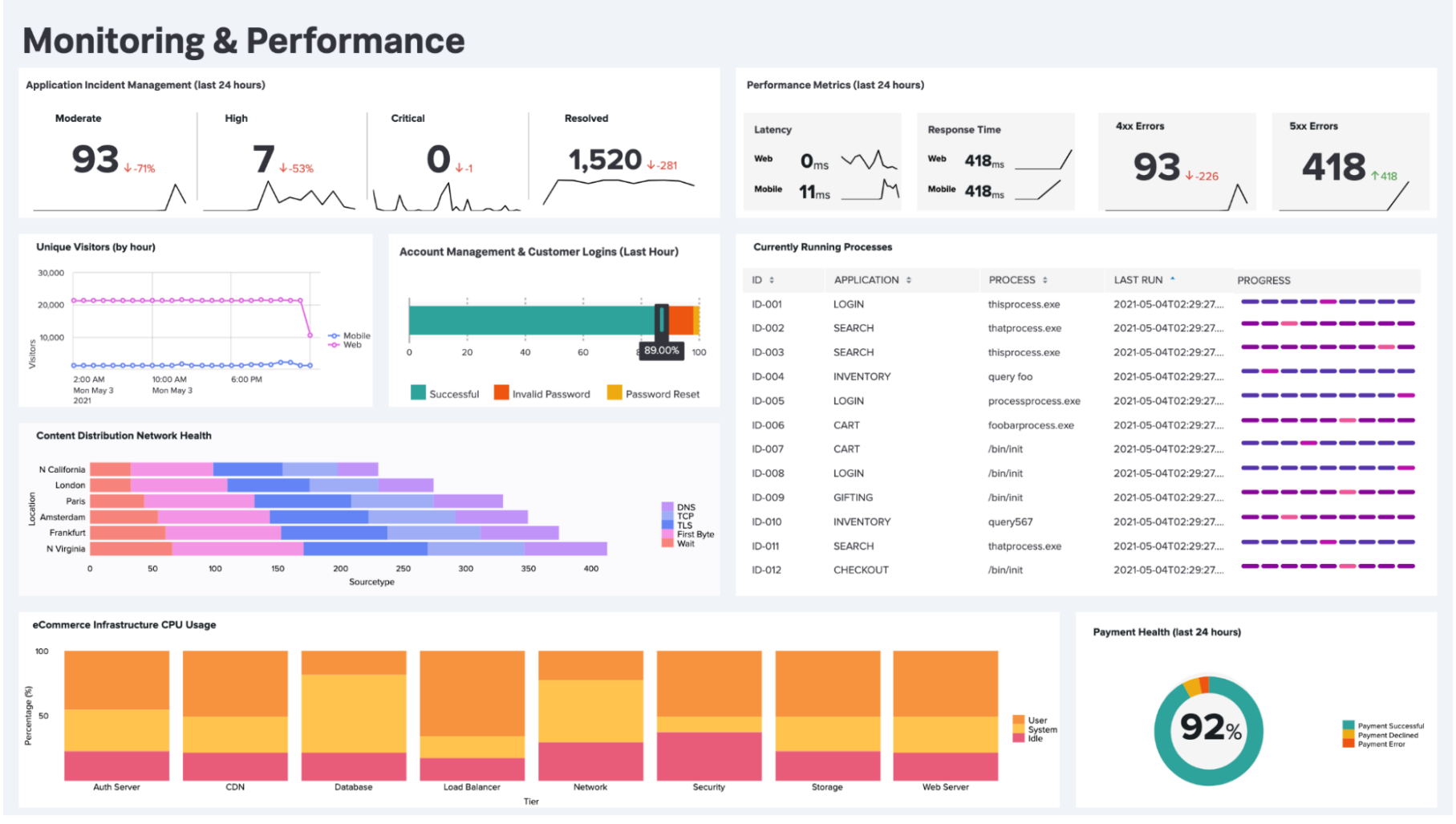
COMMENT FONCTIONNE LE SIEM CONCRÈTEMENT ?

COMMENT FONCTIONNE LE SIEM CONCRÈTEMENT ?

- DONC, L'outil SIEM est le logiciel qui remplit la fonction de **centre de commandes de sécurité axée sur l'analyse**. Toutes les **données d'événements** sont rassemblées dans un emplacement **centralisé**.
  - **Vue d'ensemble des événements notables** de votre environnement pouvant indiquer des incidents de sécurité potentiels.
  - **Détail de tous les événements notables** identifiés dans votre environnement, pour permettre leur tri.
  - **Registre de toutes les investigations en cours**, ce qui vous permet de suivre votre progression et votre activité lorsque vous enquêtez sur plusieurs incidents de sécurité.
  - **Analyse des risques**, pour évaluer les systèmes et les utilisateurs de votre réseau afin d'identifier les risques.
  - **Intelligence des menaces**, conçue pour apporter du contexte à vos incidents de sécurité et identifier les acteurs malveillants connus dans votre environnement.
  - **Renseignement sur les protocoles**, qui capture des données de paquet pour fournir des renseignements utiles sur le réseau à des fins d'investigations de sécurité, pour identifier le trafic, les activités DNS et les activités e-mail suspects.
  - **Renseignement sur les utilisateurs**, qui vous permettent d'investiguer et de superviser l'activité des utilisateurs et des actifs dans votre environnement.
  - **Intelligence Web** pour analyser le trafic web sur votre réseau.

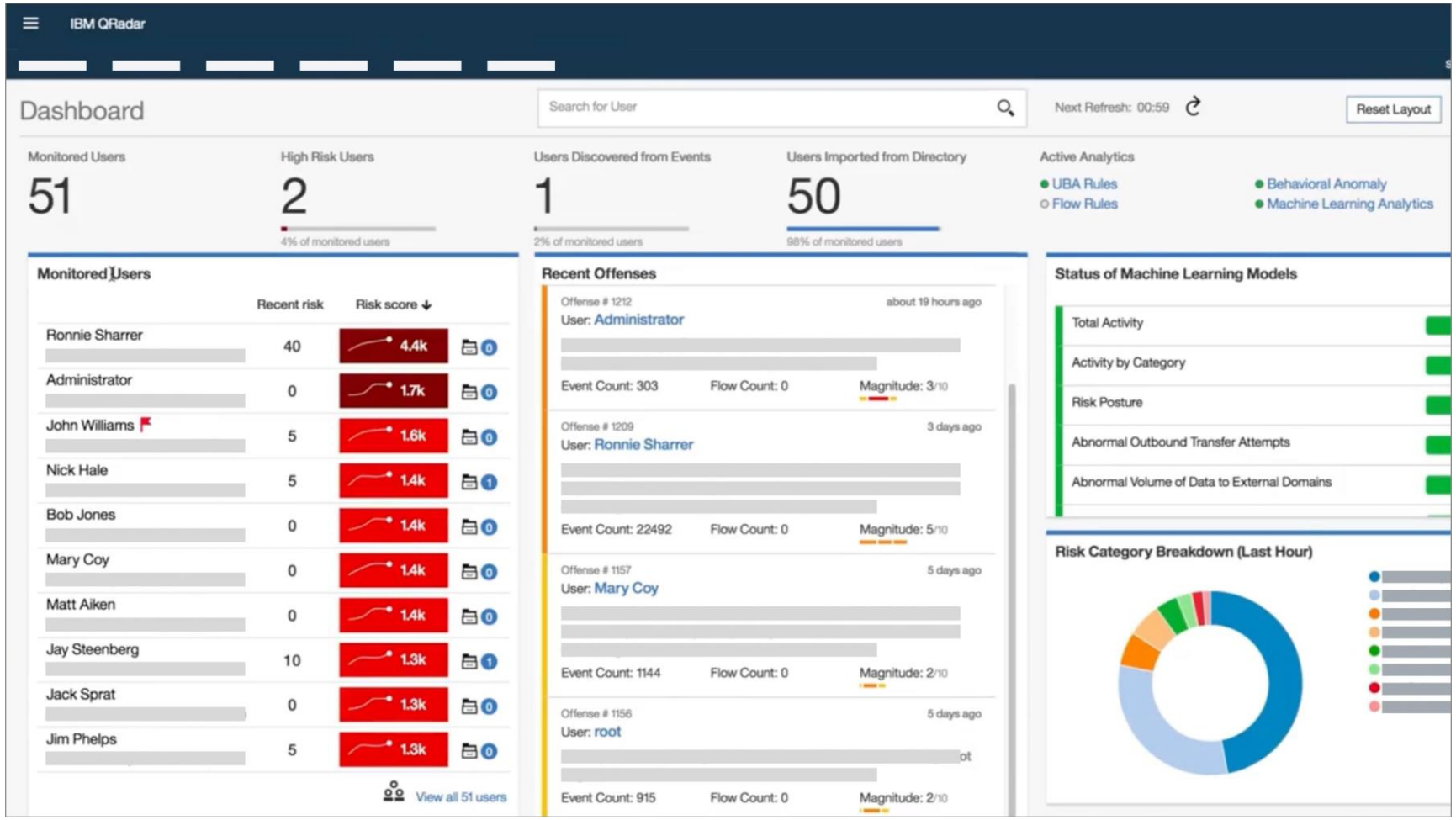
EXEMPLES DE SIEM

- Splunk



EXEMPLES DE SIEM

- IBM Qradar



EXEMPLES DE SIEM

- LogRythm

LIENS

- Témoignage d'un SM : https://cybersecurity-magazine.com/a-brief-history-of-siem/
- Présentation SIEM par Splunk : https://www.splunk.com/fr_fr/data-insider/what-is-siem.html#:~:text=Les%20syst%C3%A8mes%20de%20gestion%20des,aux%20menaces%20en%20temps%20r%C3%A9el.
- Why is SIEM important (by IBM) : https://www.ibm.com/topics/siem

BONUS

- Notre héros, notre Fonzy, le Gandalf de notre Comté Mitnickienne nous a une fois dit que « *il n'avait pas réponse à tout* »… Redonnons-lui foi en son pouvoir en créant des alias !
  - Directement dans votre terminal avec la commande : **alias ludo=sudo** (s'efface à chaque fois que vous fermez votre terminal)
    - Soyez inventifs pour **Arnold (Armand ?)** et **Dave(-id ?)** ☺
  - Pour une solution permanente, ajoutez l'alias dans votre fichier **.bashrc** ou **.zshrc**

MERCI DE VOTRE ATTENTION

KERNEL PANIC. SYSTEM CRASHING.