ATGBM 2018

Sécurité de l’information

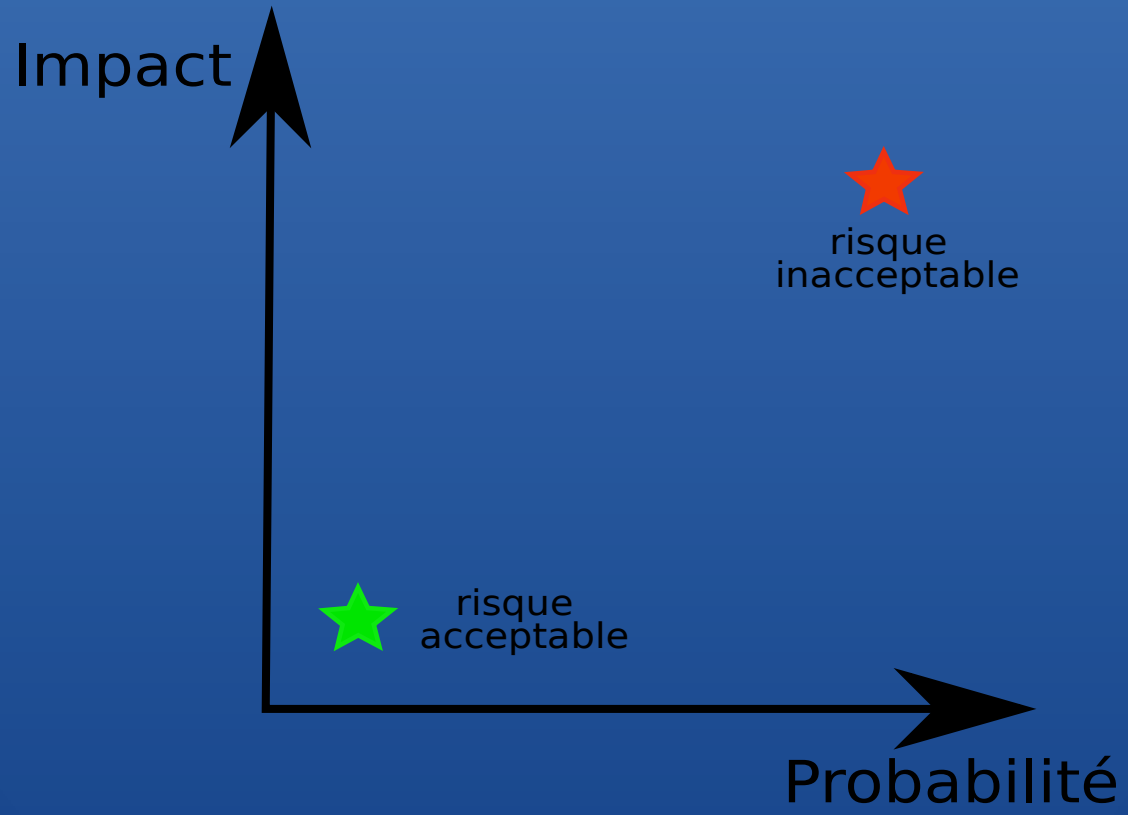
Denis Lebeuf
Responsable de la sécurité de l’information
CISSS de Laval

28 avril 2018

La sécurité de l’information

- Ce n’est pas :
  - une technologie
  - un périmètre
- C’est :
  - un ensemble de processus
  - une gestion des risques

Gestion de risque



Chaîne cybercriminelle

1) Reconnaissance
2) Intrusion
3) Exploitation
4) Escalade de privilèges
5) Mouvement latéral
6) Camouflage
7) Déni de service
8) Exfiltration

1 - Reconnaissance

- L’attaquant étudie sa cible pour trouver failles et vulnérabilités
- Armes utilisées :
  - Google
  - réseaux sociaux
  - outils de balayage réseau

→ Soyez discrets sur les réseaux sociaux

→ Restez anonyme dans les forums de discussion

→ Ne réutilisez pas vos mots de passe

2 - Intrusion

- L’attaquant infiltre le réseau
- Armes utilisées :
  - courriels d’hameçonnage
  - sites Web compromis
  - accès fournisseurs

→ Maintenez fureteur et antivirus à jour

→ Méfiez-vous des courriels, en cas de doute, validez l’origine

→ Limitez et contrôlez les accès des fournisseurs

3 - Exploitation

- L’attaquant utilise des failles du système pour en prendre le contrôle
- Armes utilisées :
  - fichiers piégés
  - virus, rançongiciels et mineurs de crypto-monnaie

→ N’accédez jamais Internet à partir de la console d’un équipement

→ Maintenez les équipements à jour

→ Effectuez des copies de sauvegarde

4 - Escalade de privilèges

- L’attaquant augmente son emprise au point d’entrée initial
- Armes utilisées :
  - outils d’exploitation des failles du système
  - programmes piégés
  - logiciels de cassage de mots de passe

→ Cloisonnement des tâches : ayez un compte administrateur et un compte personnel

→ N’allez jamais sur Internet et n’ouvrez aucun courriel avec le compte administrateur

5 - Mouvement latéral

- L’attaquant étend son emprise et cherche les cibles plus intéressantes
- Armes utilisées :
  - outils de balayage réseau
  - outils d’écoute réseau (« sniffer »)

→ Modifiez les mots de passe de défaut des équipements

→ Activez le chiffrement des communications (http vs https)

Cloisonnement du réseau

6 - Camouflage

- L’attaquant masque ses activités pour éviter la détection
- Armes utilisées :
  - désactivation des antivirus et de la journalisation

→ Activez la journalisation et surveillez les journaux

→ Apprenez ce qui est normal et ce qui ne l’est pas

→ Validez périodiquement l’état du système

7 - Déni de service

- L’attaquant perturbe les systèmes visés soit comme diversion, dans le but direct de causer du tort ou pour obtenir une rançon
- Armes utilisées :
  - virus informatiques (ex : Stuxnet)
  - rançongiciels
  - attaques par saturation de la bande passante ou des services

Effectuez des copies de sauvegarde

8 - Exfiltration

- L’attaquant copie ou transfère les données sensibles vers un endroit qu’Il contrôle
- Armes utilisées :
  - tunnels : échange de données sous le couvert d’un protocole autorisé
  - communications échelonnées dans le temps

Maintenez un inventaire précis de vos équipements

Internet des objets

IoT

De plus en plus d'appareils sont connectés en réseau afin d'en faciliter l'utilisation et la gestion

- Faciles d'utilisation et accessibles de partout, mais :
  - équipements souvent très bavards
  - la grande majorité comporte des failles de sécurité
  - aucun mécanisme de mise à jour n'est prévu

→ Il faut isoler ces appareils dans des sous-réseaux sécurisés

Services infonuagiques

Services de calculs, de logiciels ou de conservation des données offerts par le biais d'Internet

- La sécurité des informations est confiée au fournisseur
- Pratiques et accessibles de partout, mais :
  - USA PATRIOT Act et CLOUD Act
  - il est essentiel de chiffrer les données
  - qui a le contrôle de la clef de chiffrement?

    (DropBox, Google Drive, …) VS (SpiderOak, TeamDrive, Riot, …)

La messagerie électronique MSSS est un service infonuagique

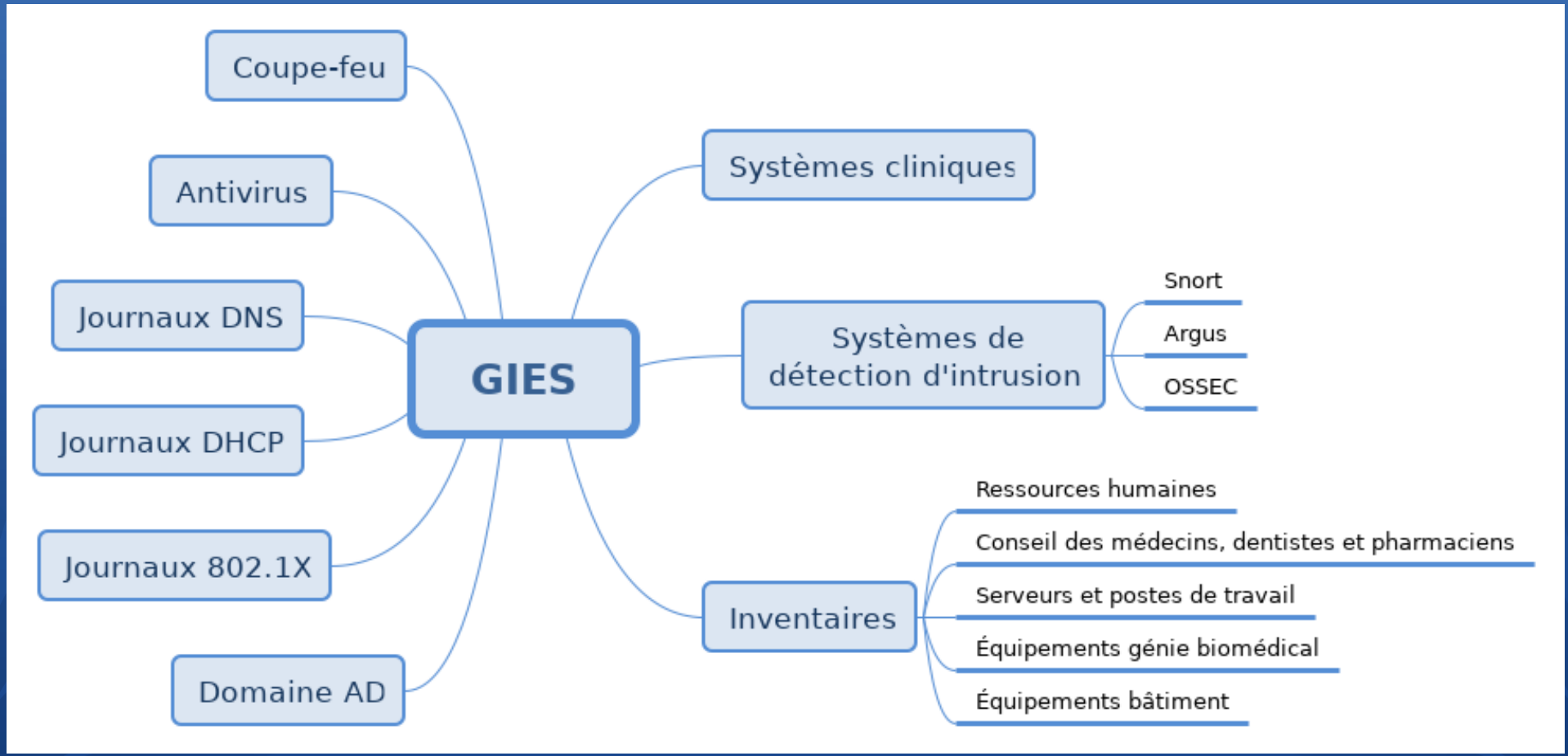
Système de GIES

Security Information and Event Management

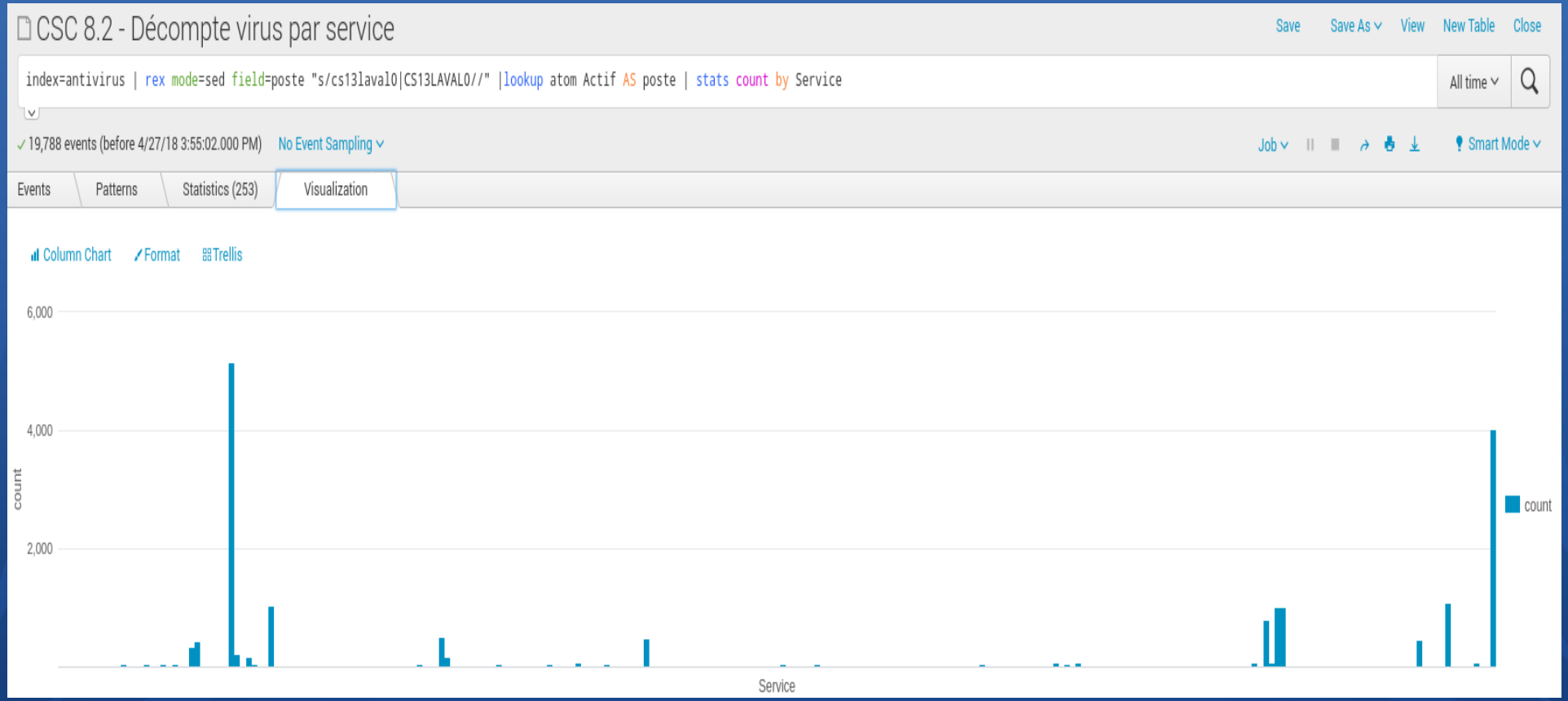
Gestion des informations et événements de sécurité

- centralisation et uniformisation des journaux de sécurité
- accès rapide aux données temporelles
- corrélations entre les différentes sources
- engins d’analyse : modèles statistiques et d’apprentissage machine
- génération de rapports et d’alertes
- documentation centrale des outils d’analyse
- architecture distribuée

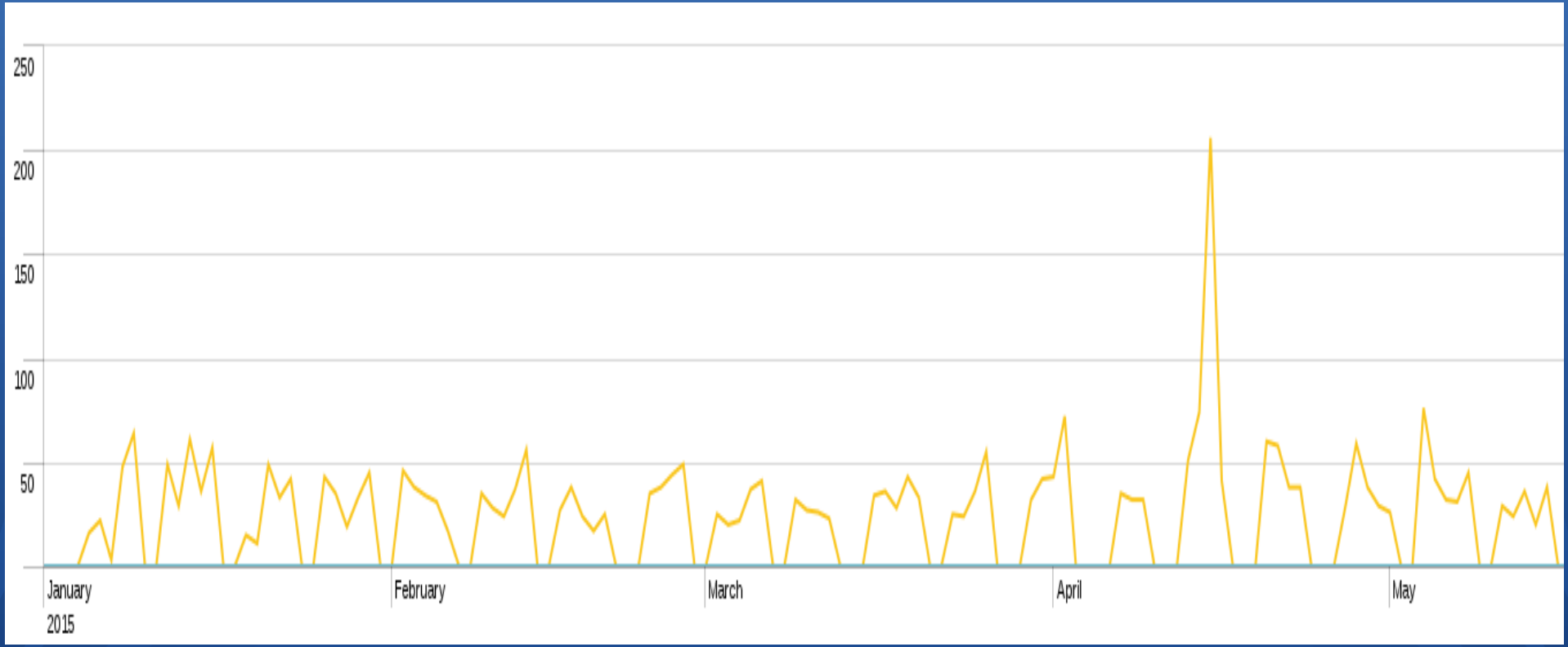
Exemples de sources



Corrélation d'événements

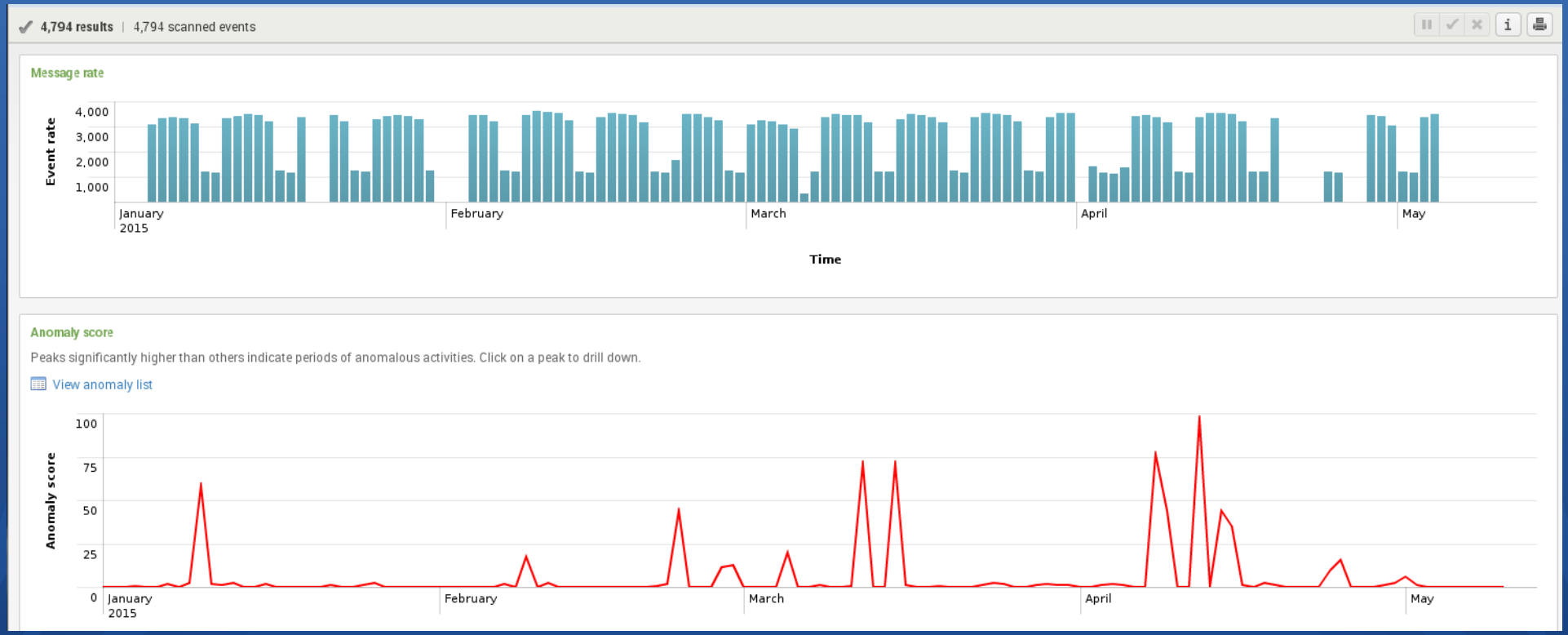


Profil d’accès aux dossiers



Nombre de dossiers patients accédés par jour

Détection des anomalies



Si on résume

Vous êtes la première ligne de défense et vous avez un rôle important à jouer dans la sécurité de l’information.