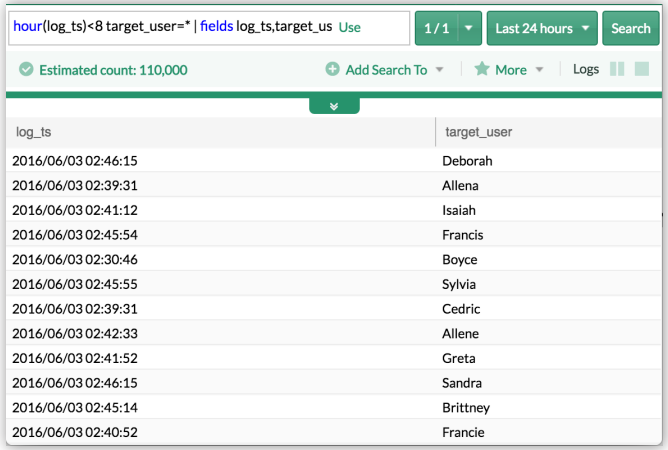
Assurer une productivité dans un contexte informatique sécuritaire représente un véritable dé i pour les entreprises. Voici ci-dessous le top 10 des cas d'usage du SIEM pour une sécurité opérationnelle.

LE TOP 10 DES CAS D'USAGE SIEM

1. Activités d'authentification

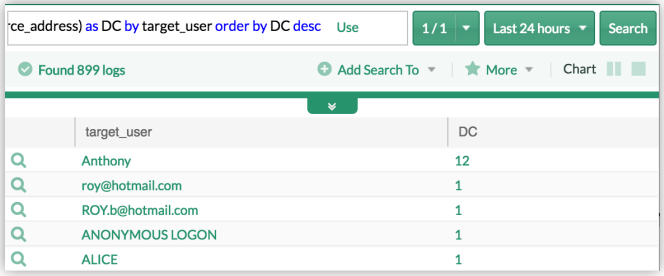
Tentatives d'authentification anormales, tentatives d'authentification aux heures non ouvrées etc., en utilisant des données provenant de Windows, Unix ou toute autre application d'authentification.



log_ts	target_user
2016/06/03 02:46:15	Deborah
2016/06/03 02:39:31	Allena
2016/06/03 02:41:12	Isaiah
2016/06/03 02:45:54	Francis
2016/06/03 02:30:46	Boyce
2016/06/03 02:45:55	Sylvia
2016/06/03 02:39:31	Cedric
2016/06/03 02:42:33	Allene
2016/06/03 02:41:52	Greta
2016/06/03 02:46:15	Sandra
2016/06/03 02:45:14	Brittney
2016/06/03 02:40:52	Francie

2. Comptes partagés

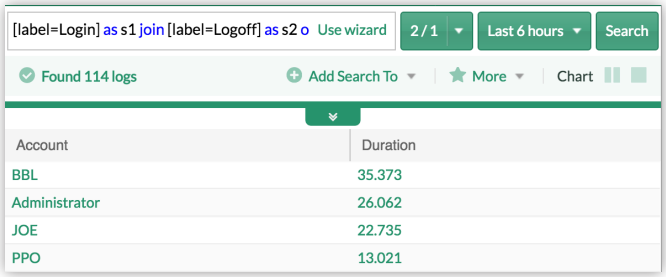
Requêtes de session provenant de sources multiples (internes/externes) pour un même compte utilisateur, durant un temps donné, en utilisant des données de login issues de source comme Windows, Unix, etc.



target_user	DC
Anthony	12
roy@hotmail.com	1
ROY.b@hotmail.com	1
ANONYMOUS LOGON	1
ALICE	1

3. Activités de sessions

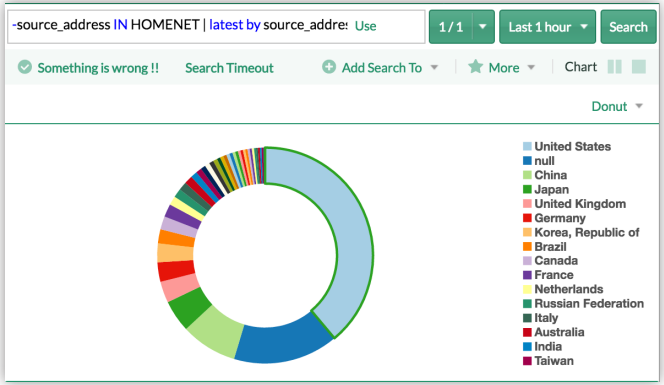
Durée de session, sessions inactives etc., en utilisant les données de « login » de session provenant spécifiquement de serveur Windows.



Account	Duration
BBL	35.373
Administrator	26.062
JOE	22.735
PPO	13.021

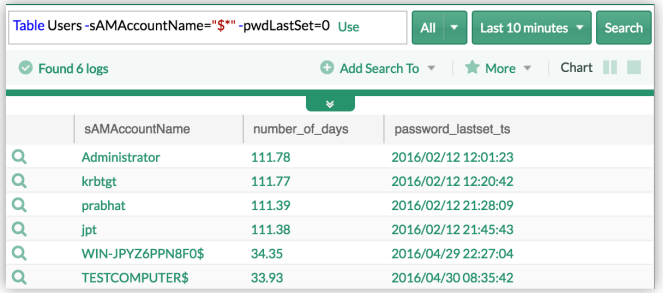
4. Détails de connexions

Comportement suspect incluant les tentatives de connexion sur des ports fermés, les connexions internes bloquées, les connexions faites vers des destinations erronées, etc., en utilisant des données provenant des firewalls, des appareils réseau ou des données de flux. Les sources externes peuvent également être étoffées pour découvrir le nom de domaine, le pays ou autre détails géographiques.



5. Comportement d'administration anormal

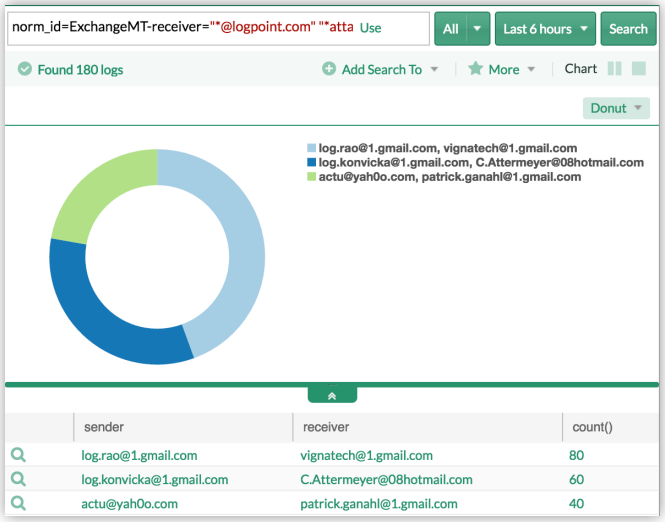
Supervision des comptes inactifs, des comptes avec mots de passe inchangés, activités inhabituelles de compte de management etc., en utilisant des données d'activités de compte AD de management.



sAMAccountName	number_of_days	password_lastset_ts
Administrator	111.78	2016/02/12 12:01:23
krbtgt	111.77	2016/02/12 12:20:42
prabhat	111.39	2016/02/12 21:28:09
jpt	111.38	2016/02/12 21:45:43
WIN-JPYZ6PPN8F0$	34.35	2016/04/29 22:27:04
TESTCOMPUTER$	33.93	2016/04/30 08:35:42

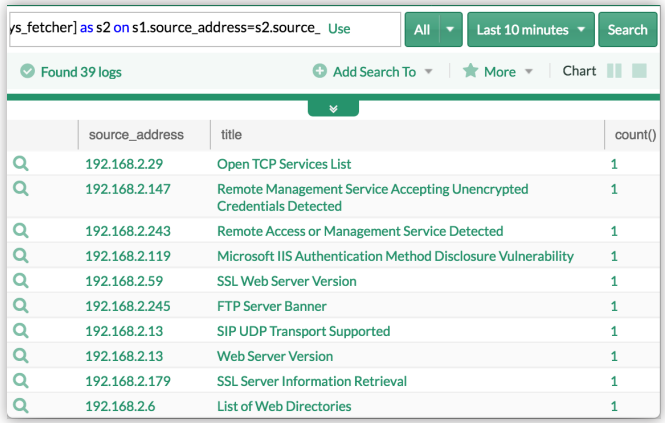
6. Vol d'information

Tentative d'exfiltration de données, fuite d'informations par emails etc., en utilisant des données issues de serveurs mails, d'applications de partage de fichiers, etc.



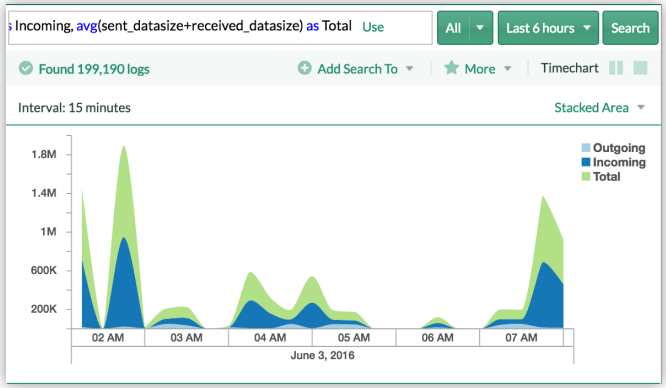
7. Scan de vulnérabilité et corrélation

Identification et corrélation des vulnérabilités de sécurité détectées par des applications comme Qualys avec d'autres événements suspects.



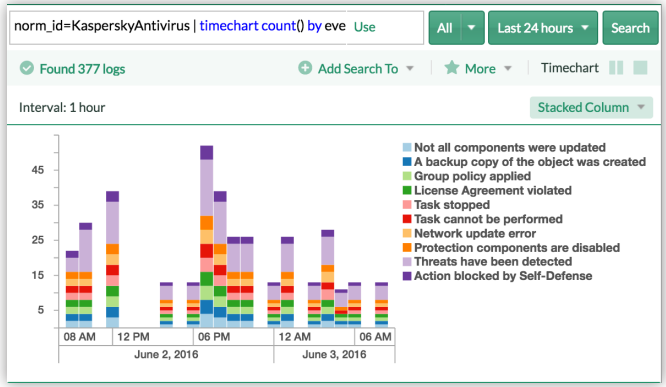
8. Analyse statistique

Des analyses statistiques peuvent être faites pour étudier la nature des données.
Des fonctions comme la moyenne, la médiane ou le quantile, etc. peuvent être utilisées.
Les données numériques de sources diverses peuvent servir à établir des relations de type ratio de bande passante entrante/sortante, utilisation des données par application, comparaison, etc.



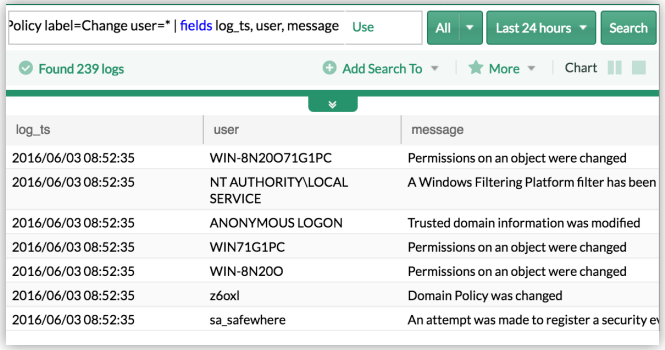
9. Détection d'intrusion et infections

Sont établies en utilisant les données des IDS/IPS, antivirus, applications anti-malware, etc.



10. Modifications système

Effectué en utilisant les données de changement de configuration, les changements de règles, les violations de règles, etc.



LE TOP 10 DES CAS D'USAGE SIEM

LOGPOINT
Unified Simplicity

MIEL

Parc Burospace 5
91571 Bièvres Cedex
France
+33 1 60 19 34 52
http://www.miel.fr
contact@miel.fr