

Complexity in business means that enterprises are experiencing a number of challenges in both a business and a security-oriented context. Outlined below, are the top 10 SIEM use cases for security and business operations.

TOP 10 SIEM USE CASES

1. Authentication Activities

Abnormal authentication attempts, off hour authentication attempts etc, using data from Windows, Unix and any other authentication application.

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. Shared Accounts

Multiple sources (internal/external) creating session requests for a particular user account during a given time frame, using login data from sources like Windows, Unix etc.

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

3. Session Activities

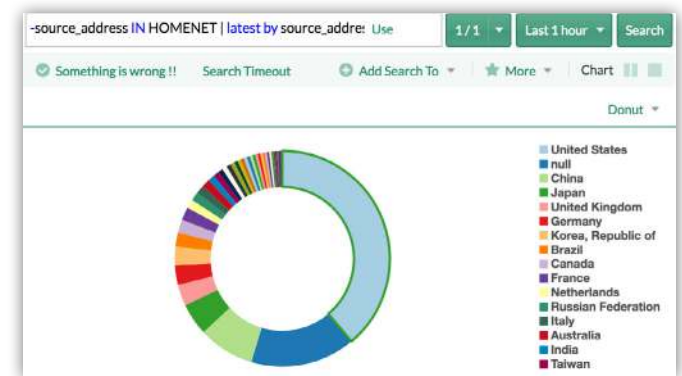
Session duration, inactive sessions etc, using log in session related data specifically from Windows server.

Account	Duration
BBL	35.373
Administrator	26.062
JOE	22.735
PPO	13.021

4. Connections Details

Suspicious behavior includes connection attempts on closed

ports, blocked internal connections, connection made to bad destinations etc, using data from firewalls, network devices or flow data. External sources can further be enriched to discover the domain name, country and geographical details.



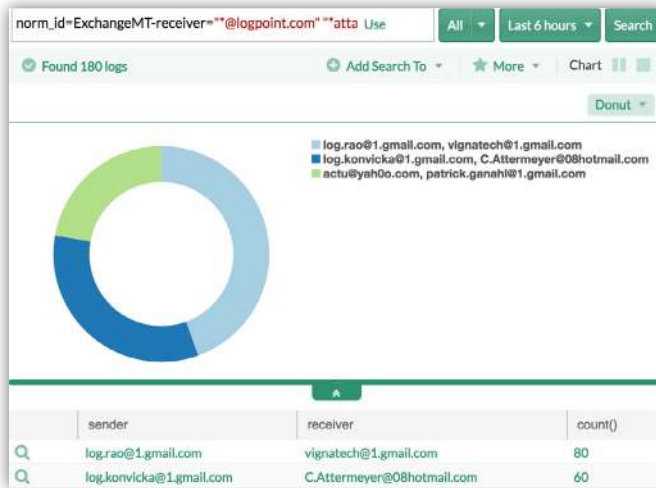
5. Abnormal Administrative Behavior

Monitoring inactive accounts, accounts with unchanged passwords, abnormal account management activities etc, using data from AD account management related activities.

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

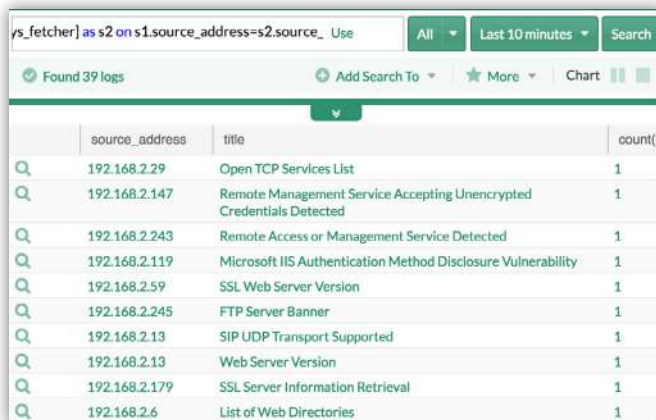
6. Information Theft

Data exfiltration attempts, information leakage through emails etc, using data from mail servers, file sharing applications etc.



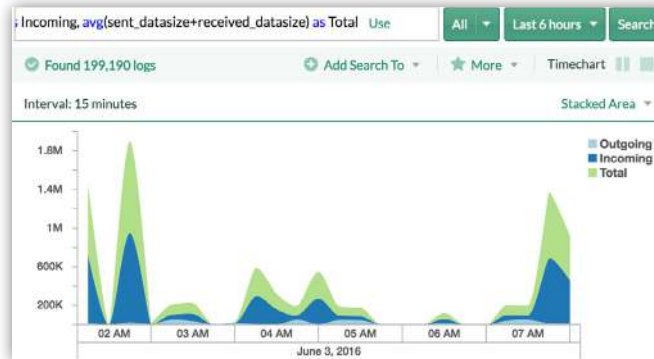
7. Vulnerability Scanning and Correlation

Identification and correlation of security vulnerabilities detected by applications such as Qualys against other suspicious events.



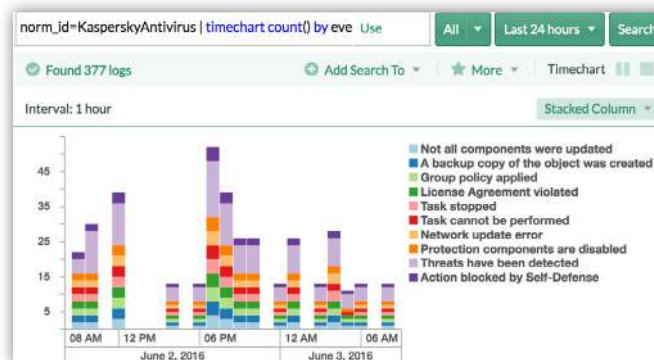
8. Statistical Analysis

Statistical analysis can be done to study the nature of data. Functions like average, median, quantile, etc. can be used. Numerical data from various sources can be used to monitor relations e.g. ratio of inbound to outbound bandwidth usage, data usage per application, comparison etc.



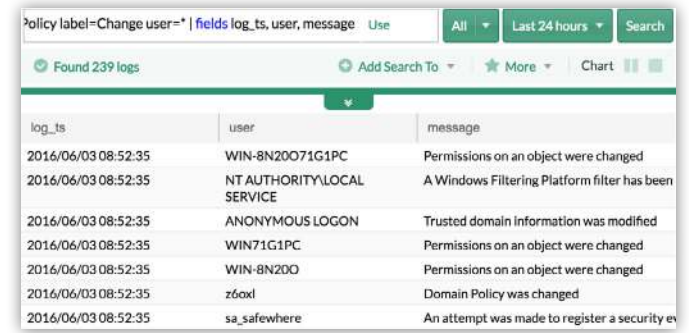
9. Intrusion Detection and Infections

Can be performed by using data from IDS/IPS, antivirus, anti-malware applications etc.



10. System Change Activities

Is carried out by using data for changes in configurations, audit configuration changes, policy changes, policy violations etc.



TOP 10 SIEM USE CASES

logpoint

LogPoint.com

Contact us for more information:

Email: hwo@logpoint.com

Phone: +44 01454 203860