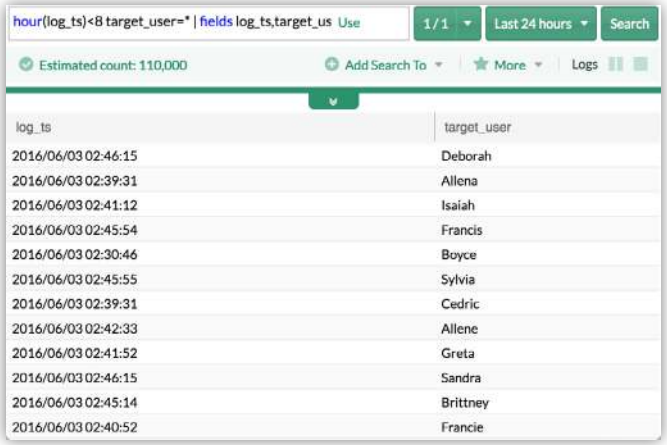
Complexity in business means that enterprises are experiencing a number of challenges in both a business and a security-oriented context. Outlined below, are the top 10 SIEM use cases for security and business operations.

TOP 10 SIEM USE CASES

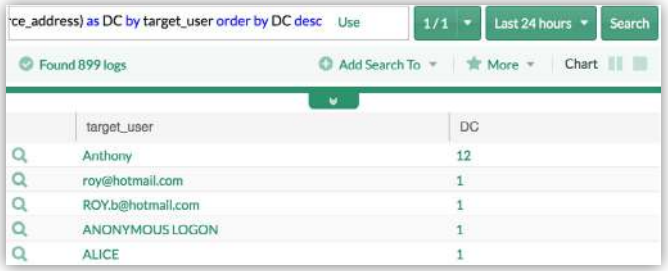
1. Authentication Activities

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



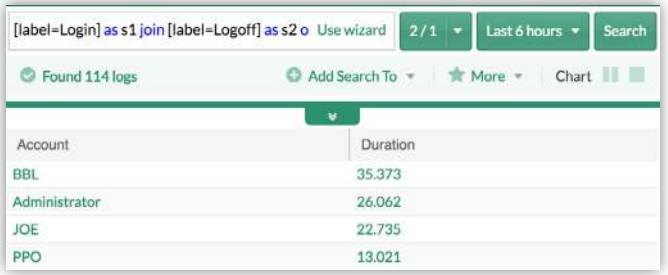
2. Shared Accounts

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.



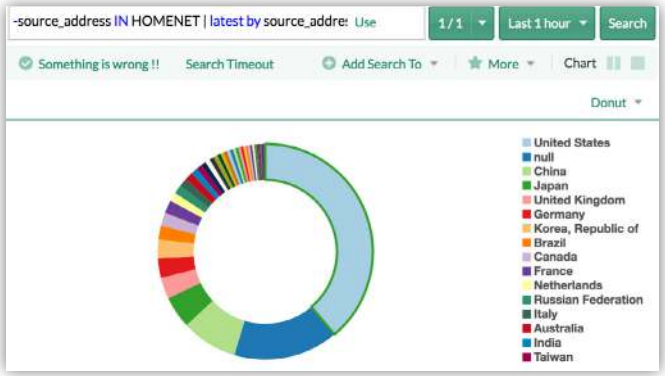
3. Session Activities

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



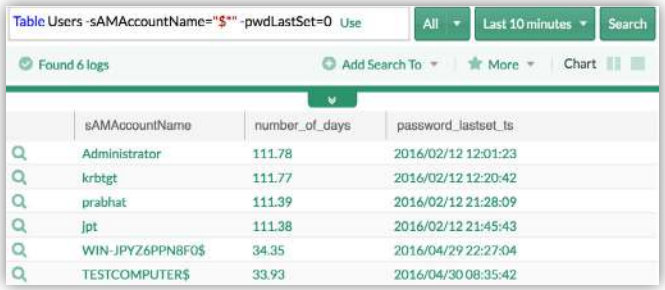
4. Connections Details

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.



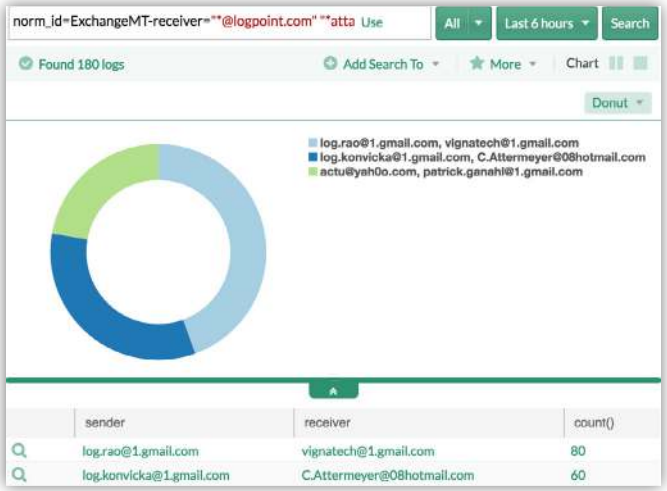
5. Abnormal Administrative Behavior

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



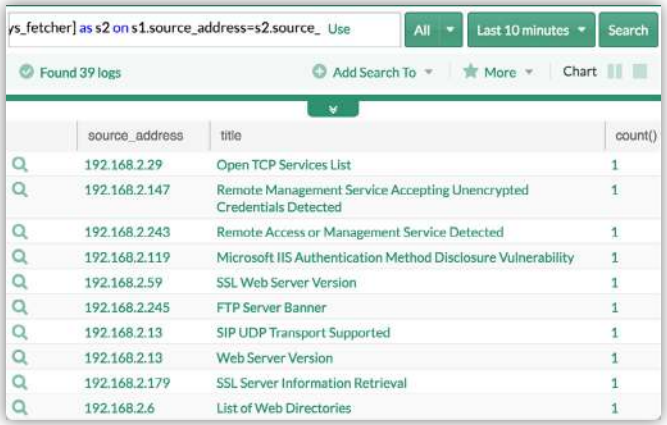
6. Information Theft

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



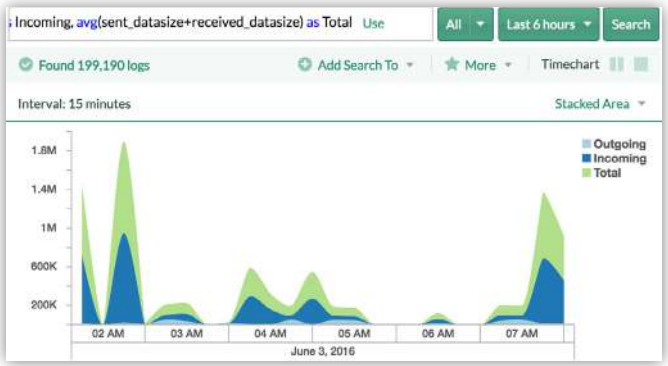
7. Vulnerability Scanning and Correlation

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



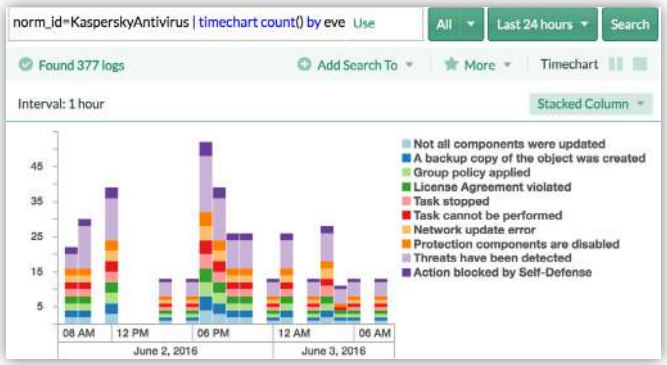
8. Statistical Analysis

Statistical analysiscan 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.



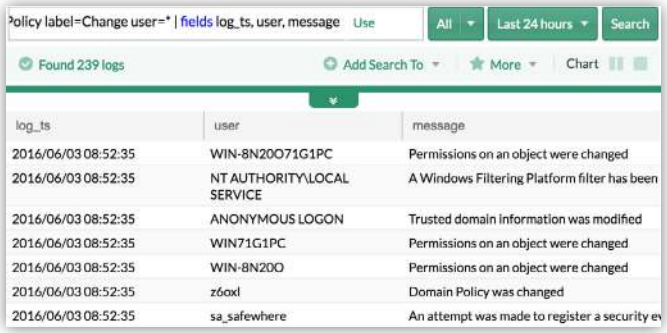
9. Intrusion Detection and Infections

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