sqrrl

Target. Hunt. Disrupt.

DATASHEET

SQRRL ENTERPRISE
USE CASE: USER AND ENTITY BEHAVIOR ANALYTICS (UEBA)

Find Deeper Meaning by Cutting Through the Noise

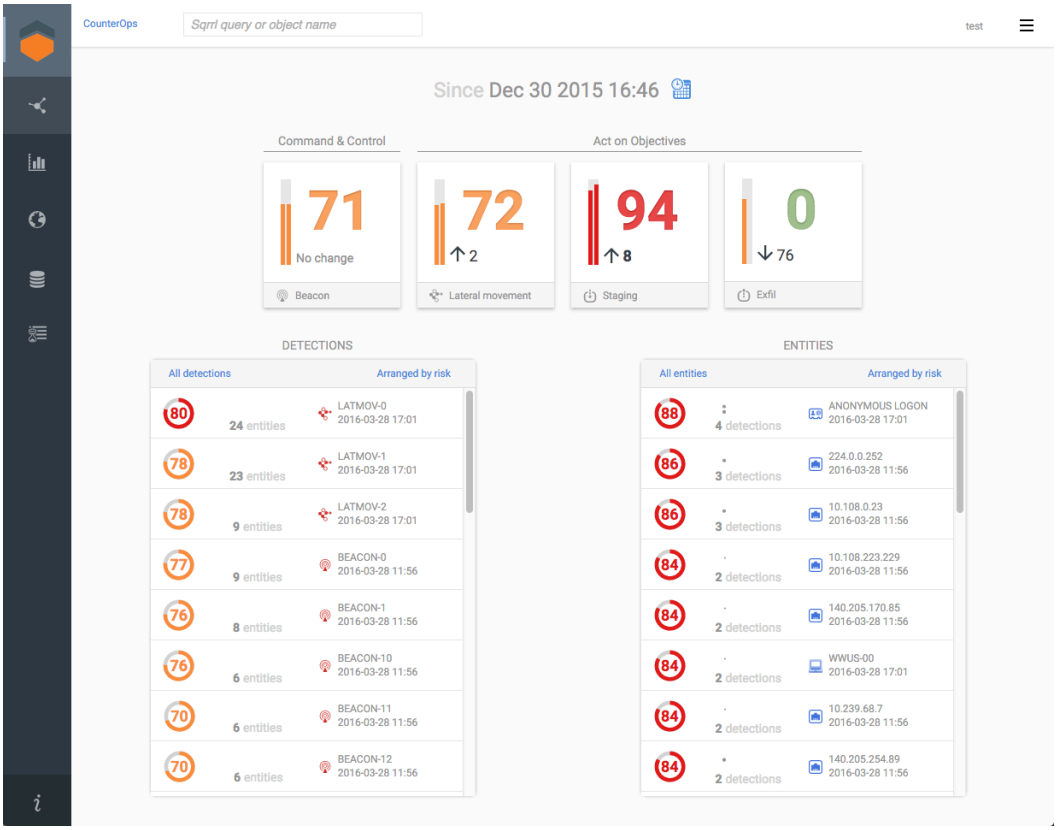
User and Entity Behavior Analytics (UEBA) is defined as the use of advanced analytics (e.g., machine learning) to baseline entity activity (e.g., users, devices, servers, applications, etc.) and calculate risk in order to identify security anomalies against those baselines. These anomalies can be aligned to adversary behaviors such as lateral movement and malware command and control. UEBA complements rule or signature-based approaches (such as SIEMs) and identifies security anomalies that they miss. UEBA is most effective when it leverages Big Data storage and processing to bring together a wide variety of datasets and to look for anomalies across them and at their intersection.

Why is UEBA Important?

Today's advanced attackers are able to bypass many traditional perimeter defenses, such as firewalls, intrusion prevention systems, and web gateways. The IT perimeter of large organizations is too porous and jagged to effectively defend. The mindset of security executives and managers has now shifted from solely focusing on preventative security measures to that of more efficiently detecting advanced attacks that are in progress and minimizing the impact of these incidents.

UEBA and SIEMs

SIEMs are powerful detection tools that aggregate logs and alerts, but they typically rely on simple correlation rules that aren't able to spot the footprints of advanced attackers. Correlations can detect threats in real time, but advanced attacks occur over months or even years. UEBA does not rely on signatures or rules, utilizing advanced algorithms and risk scoring methodologies to correlate events over a much longer timeline. Many organizations are now using UEBA techniques in combination with a SIEM to provide higher levels of security and improved detection of advanced threats.



Sqrrl Dashboard with Kill Chain and Entity Oriented UEBA Risk Scores

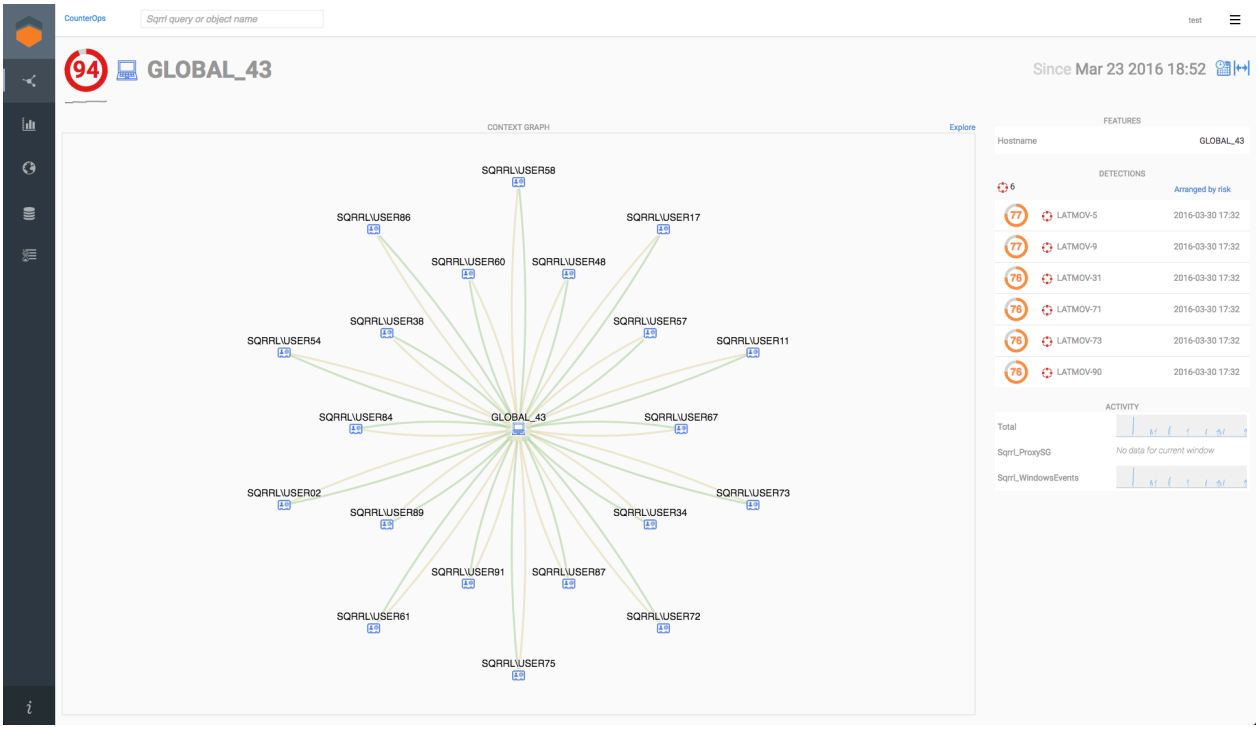
Sqrrl's Differentiated UEBA: The Behavior Graph

Sqrrl's approach to UEBA is unique because it leverages the Behavior Graph, a powerful and contextual visualization for detecting and tracking threats. The Behavior Graph streamlines the work of security analysts by laying out any network or IT environment in an intuitive linked data model. Sqrrl can fuse together petabytes of diverse datasets into these common models. The linked data model, laid out as a graph allows Sqrrl to use proprietary graph algorithms to detect anomalies associated with specific Kill Chain behaviors. These graph algorithms provide Sqrrl with a greater level of accuracy in detection than other solutions.

In addition to graph algorithms, Sqrrl's UEBA leverages:

- Machine learning
- Risk scoring
- Peer group analysis
- Bayesian statistics

Generating risk scores for various entity types is a critical way in which Sqrrl communicates what it finds via UEBA to an analyst. TTP detectors look across collections of entities and can aggregate and prioritize risk for both entities and TTPs. Analysts can use these risk scores as starting points for threat hunting investigations.



Sqrrl Entity Profile with UEBA Derived Risk Scores

Sqrrl UEBA Use Cases

UEBA goes hand in hand with a number of potential use cases that Sqrrl is ideally suited for including:

- SOCs that want effective starting points for proactive **Threat Hunting**
- **Incident Investigators** that need more efficient forensics and anomaly detection
- Analysts looking to detect and deter **Insider Threats**
- **MSSPs** looking to provide threat hunting services to their clients

125 Cambridge Park Dr
Cambridge, MA 02140

p: (617) 902-0784
e: info@sqrrl.com

www.sqrrl.com
@SqrrlData