sqrrl Target. Hunt. Disrupt.

DATASHEET

SQRRL ENTERPRISE
TARGET. HUNT. DISRUPT.

An Advanced Threat Detection and Response Platform

Organizations face a growing number of adversaries threatening their networks. And even if they diligently gather data from all of their relevant security devices, often there is too much data to make sense of. What if you could easily investigate the threats hidden in all the noise? Now you can.

Analyzing the Data

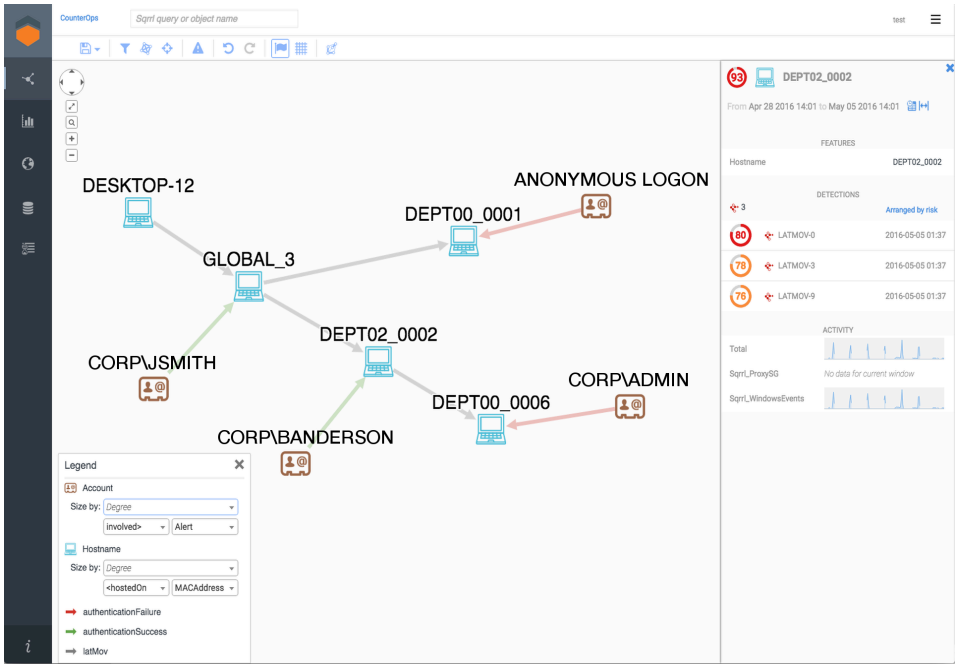
Making sense of petabytes worth of data is no easy task. In order to fully leverage aggregated security data, Sqrrl's employs powerful data analytics techniques that help analysts reveal the risks and threats that are present in their enterprise network. Sqrrl consumes and fuses diverse security datasets, including network traffic logs, user directory and identity information, proxy data, external intelligence feeds, DNS logs, and customer transactions. Sqrrl uses this data to reveal suspicious behavior, pinpoint the actors involved, and assess the organization's risk exposure.

Quickly Observe, Understand, and React

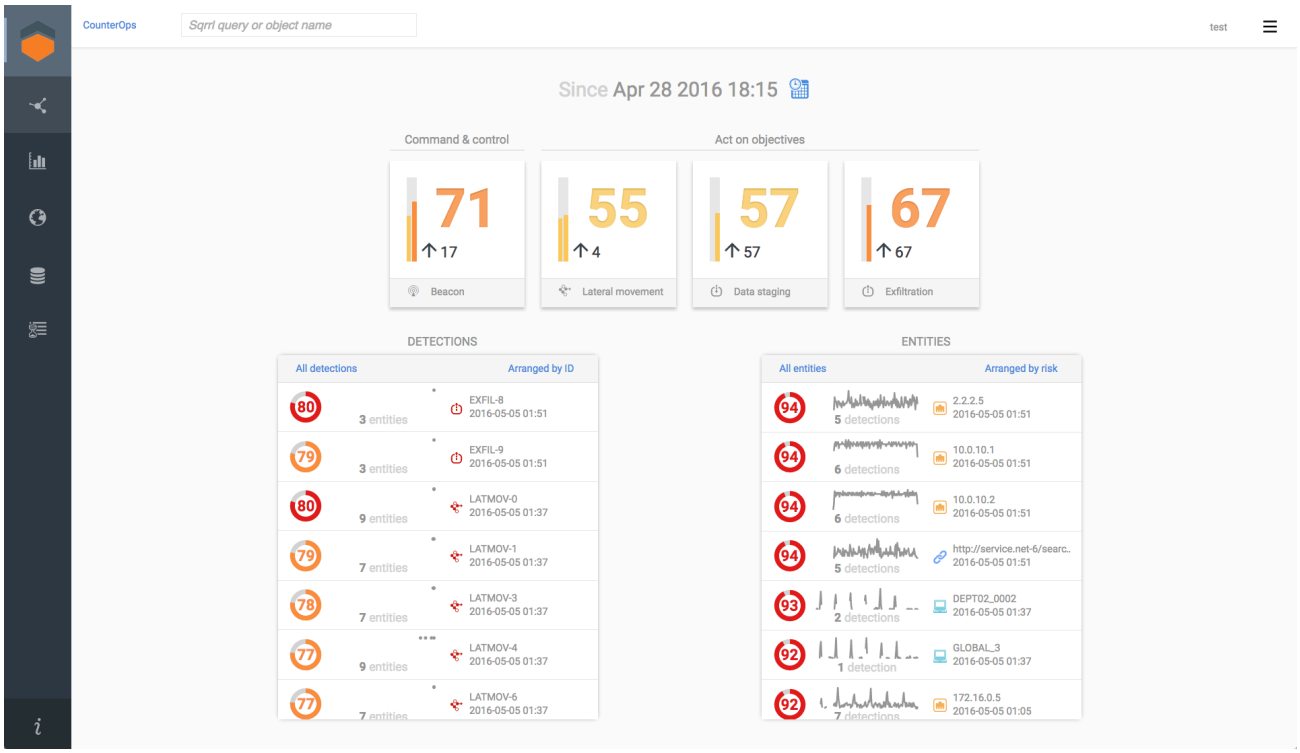
Sqrrl's innovative security approach is based on building a *Behavior Graph* from your enterprise security data. Much like a social graph, a Behavior Graph creates a mapping of entities (e.g. users, assets, applications, websites) and how they're related via their activities (e.g. logins, data transfers, application usage). Sqrrl presents the enterprise Behavior Graph to your analysts using powerful visualizations and advanced analytics that help them quickly identify risky, threatening and abnormal behavior that's indicative of security breaches.

Sqrrl Features:

- Behavior Graph approach to storing, organizing and linking security data
- Kill chain analysis that detects adversary tactics, techniques, and procedures
- User and entity behavior analytics that enable risk-based analysis
- Powerful visualizations, dashboards and reports
- Petabyte-scale search, statistics and query facilities
- Streamlined investigations that link to raw security data



The Sqrrl UI, featuring the Behavior Graph and data exploration



The Sqrrl Homepage with Entity and Detection Risk Scores

The Sqrrl Advantage:

- Contextual, intuitive graph visualization of even the most complex networks
- Automated detection of anomalies and adversary tactics, techniques and procedures
- Real-time search, query, and analysis of entity behaviors
- Simplified breach scoping and analysis
- Efficient fusion of disparate data sets at petabyte scale
- Fine grained access control and protection for sensitive corporate data

Scale Effortlessly on a Powerful Foundation

Sqrrl is built on top of a powerful big data architecture that leverages the benefits of distributed, fast, scalable storage. This foundation lets you modify your capacity on-demand, without reconfiguring existing infrastructure.

Who is Sqrrl for?

- Security analysts who proactively hunt for threats that their signature-based solutions miss
- Incident investigators that need deeper and faster forensic analysis
- MSSPs that are looking to provide and expand advanced threat hunting services to their clients

ABOUT SQRRL

sqrrl Target. Hunt. Disrupt.

Sqrrl was founded in 2012 by creators of Apache Accumulo™. With their roots in the U.S. Intelligence Community, Sqrrl's founders have deep experience working at the intersection of advanced cybersecurity and Big Data problems. Sqrrl is headquartered in Cambridge, MA and is a venture-backed company with investors from Matrix Partners, Atlas Venture, and Rally Ventures.

125 Cambridge Park Dr.
Cambridge, MA 02140

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

www.sqrrl.com
@SqrrlData