sqrrl

Target. Hunt. Disrupt.

DATASHEET

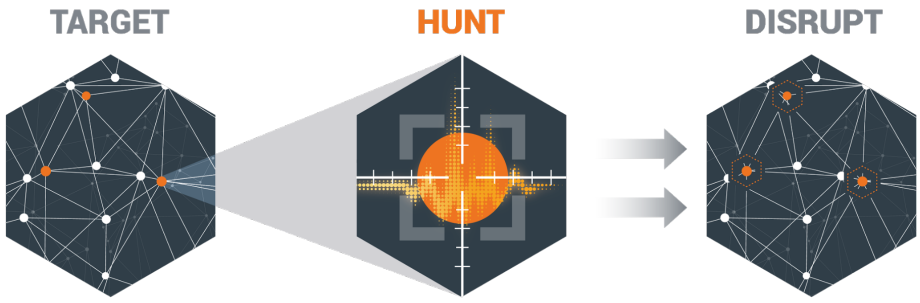
SQRRL ENTERPRISE
USE CASE: CYBER HUNTING

Proactively uncover hidden threats through cyber hunting

The days when Security Operations Center analysts could sit back and wait for alerts to come to them have long passed. Recent breaches at companies and government agencies have shown that traditional measures like firewalls, IDS, and SIEMs are not enough.

Today's threats demand a more active role in detecting and isolating sophisticated attacks. Cyber Threat Hunting is the process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions.

Most organizations already hunt in more of an ad hoc way through log analysis while others may be more committed to hunting, but lack sophisticated tools to collate and analyze large amounts of data to identify the digital footprints of an attacker.



Question Driven Investigations

Hunting trips are iterative and start with questions or hypotheses. An initial question or hypothesis might be based on the steps of the cyber kill chain, and be something like "Is data exfiltration happening?" or "If there is data exfiltration happening, it's most likely going on through this part of the network." A hunter would then investigate that subnet, letting those questions drive the investigation. Hypotheses help figure out what data you need to examine and what analytic techniques might be most fruitful. A hunting investigation should ideally yield Indicators of Compromise (IoCs), especially the tactics, techniques and procedures (TTPs) of an adversary, which can be fed back into your automated security solutions. The process of consistently improving your automated defenses is the ultimate goal of hunting.

The Sqrrl Edge

Sqrrl's unified threat hunting platform allows an analyst to integrate, explore, and analyze massive, disparate datasets to find advanced threats. By creating visual models using linked data, Sqrrl is able to generate a clear contextual picture for analysts. It powers cyber hunting via the following features:

- **The Sqrrl Behavior Graph,** an advanced graph visualization that provides immediate context to the security analyst about the assets, actors, and events present on their network and endpoints.
- **TTP Oriented Detectors,** automated behavioral analysis over Sqrrl's linked data model that pinpoints adversary Tactics, Techniques, and Procedures.
- **User and Entity Behavior Analytics,** leveraging advanced data science to profile and analyze users, machines, web domains and any other entity of interest.
- **Risk-based Dashboards and Entity Profiles,** helping analysts quickly recognize and investigate the most recent suspicious activities.
- **Out-of-the-Box Data Source Connectors,** streamline the process of loading and utilizing massively diverse data sets for optimal cyber security use.

Leveraging Data Science

Making sense of Big Data is no easy task, but analytics tools have the potential to multiply the effectiveness of a hunter's powers by automating common tasks and isolating anomalies far faster than a human analyst ever could. Hunters need tools like Sqrrl's threat hunting platform to implement data science techniques without requiring them to be data scientists. These include:

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

Building a Hunting Framework

Hunting is most effective when it is iterative, habitual, and adaptable, complementing the rest of your security ecosystem. Sqrrl has distinguished itself as a thought leader in the practical application of hunting. The Hunting Loop is a model for how hunts should be effectively carried out, from hypothesis creation to the gathering of Indicators of Compromise (IoCs), and on to the enrichment of analytics and automation. Sqrrl's threat hunting platform provides a single pane of glass for analysts to perform Linked Data Analysis across their security datasets, making it uniquely effective at discovering TTPs in the hunting loop.

Advice from a Hunter

"Organizations are realizing that their existing traditional security solutions, such as firewalls and SIEMs, are not finding everything that they need to find. On the detection side they're doing well for what they do, but the problem is that signature-based or even intelligence-based network monitoring systems are limited. Attackers are virtually unlimited in what they can do. Adversaries are very flexible and agile, so that's what we have to be."

-David Bianco, Sqrrl's Security Technologist; former Manager of Mandiant's Hunt Team

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