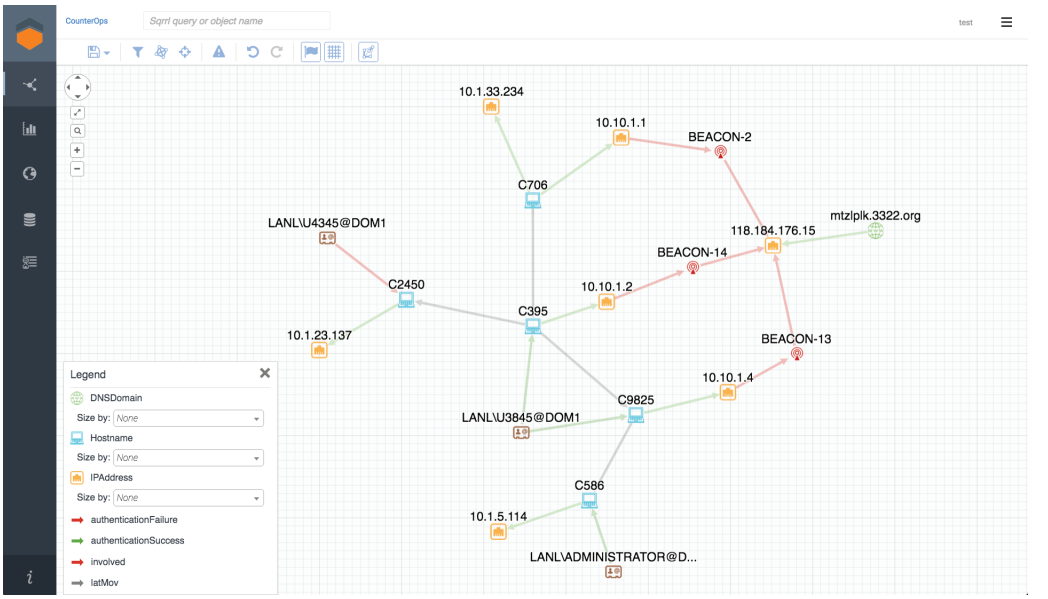
SOLUTION REVIEW

Next-generation Security Analytics



DETAILS

Vendor	Sqrrl
Product	Threat Hunting Platform
Price	Starting at $25,000
Web	www.sqrrl.com
Innovation	Advanced Analytics
Greatest strength	TTP Detectors

While this Innovator didn't exactly coin the term "threat hunting," it certainly has given it form and substance. By developing its Threat Hunting Reference Model, Sqrrl has taken the first step to formalizing the threat hunting process. Since it has built its product around this model, it has an excellent start on a commanding place in the market. Many on the Sqrrl team are scientists from NSA so, as one would expect, the technology and data science is sound. The model is unusual in that it has begun to define the threat hunting process and it has come from a relatively unknown company.

Models such as these generally are viewed as self-serving marketing hype. Having spent much of our time in threat hunting, we can attest that such definitely is not the case here. The model is solid as a threat hunting frame work and it makes a lot of sense.

Sqrrl installs on a Hadoop cluster and can be hardware or cloud-based. This is Sqrrl's second year in our Innovators issue and over that year it has been busy continuing its innovation. The company has added new functionality since last time we looked at it. They have improved their built-in analytics to provide additional observation as to where to take the hunt.

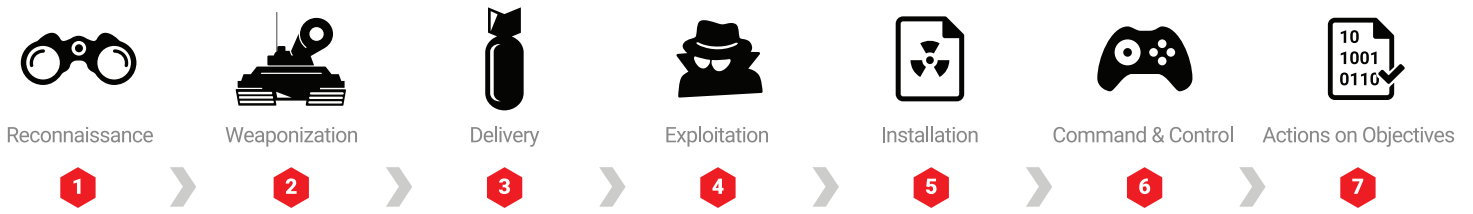
As the company that is building its future on the concept of threat hunting, our obvious question for them was, "How's this threat hunting thing working for you in the marketplace?" The answer was unequivocal: "Extremely well. Threat hunting is more than indicator search. It includes sophisticated analytics and visualization. We're beginning to see budgets assigned to hunting."

– Peter Stephenson, technology editor

Sqrrl's Unique Approach to Security Analytics

Instead of searching only for general anomalies, Sqrrl's security analytics are focused on detecting the **kill chain behaviors and Tactics, Techniques, and Procedures (TTPs)** of cyber adversaries.

CYBER THREAT KILL CHAIN



In this context, a tactic refers to some actions an attacker takes within a phase of the kill chain. For example, beaconing is a tactic that can be used in the Command and Control phase. A technique refers to how an attacker might choose to go about performing a tactic. For example, "hide in plain sight by using a common port/protocol" is a technique that might be implemented to perform beaconing activity. Finally, a procedure refers to the steps that an adversary takes to perform a technique.

An example of this might be the specific use of a protocol like HTTP to try and send data from a server within a network out to a command and control point. Each of Sqrrl's TTP detectors is a suite of analytics that map to higher-level tactics along the kill chain. The analytics contributing to each detector look for the hallmarks of specific techniques and procedures in order to make determinations about potential attacker behaviors.

GREATEST STRENGTH

Sqrrl's TTP Detectors

"You will uncover indicators before they fire, preventing damage to the enterprise."

SC MAGAZINE RECOMMENDED

Each of the detectors below come with Sqrrl out-of-the-box and need minimal configuration, so that analysts can get hunting for threats sooner and more effectively than ever.

Lateral Movement	Sqrrl tracks lateral movement by connecting unusual authentications across multiple assets and entities, and is able to recognize specific graph-based patterns that are indicative of an attacker moving across various hosts.
Beaconing	Sqrrl detects beaconing at regular pulse-like intervals by using signal processing techniques to cut through the noise of network traffic and detect custom malware infections that may not have known signatures.
Data Staging and Exfiltration	Sqrrl's analytics can determine when data staging and exfiltration are happening by looking for spikes in network traffic and anomalous data flows that show large amounts of data are being moved to a single point in or outside the network.
DNS Tunneling	Sqrrl detects DNS Tunneling, a technique used by malware to covertly send information out of a network, by grouping and analyzing DNS traffic according to an internal endpoint making the request, and the external registered domain it is querying for.
Domain Generation Algorithm	Sophisticated malware uses Domain Generation Algorithms (DGAs) to defeat DNS sinkholes and blacklists, which Sqrrl detects by by singling out unregistered and random websites in DNS traffic.