Target. Hunt. Disrupt.

DATASHEET

SQRRL ENTERPRISE
USE CASE: INCIDENT RESPONSE & INVESTIGATION

Clarity in Assessment. Speed in Response.

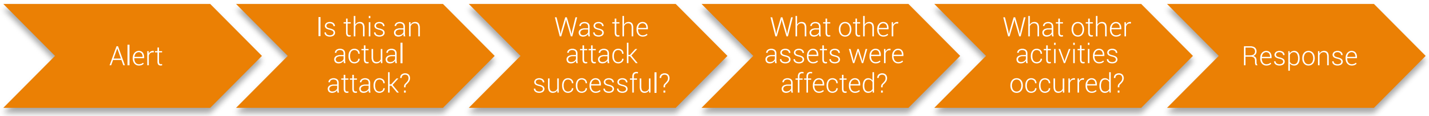
Detecting advanced threats is only the first step in remediating an incident. Effective incident response and investigation is a process, spanning across alert triage, incident analysis, and remediation. Whether the process is being carried out by a full CSIRT or a single analyst, each time an alert is generated there are four questions that must be answered.

Validation Questions:

1. Does this alert indicate an actual attack?
2. If so, was the attack successful?

Scoping Questions:

3. For successful attacks, what other assets were affected?
4. What other activities occurred as part of this attack?


Alert
Is this an actual attack?
Was the attack successful?
What other assets were affected?
What other activities occurred?
Response

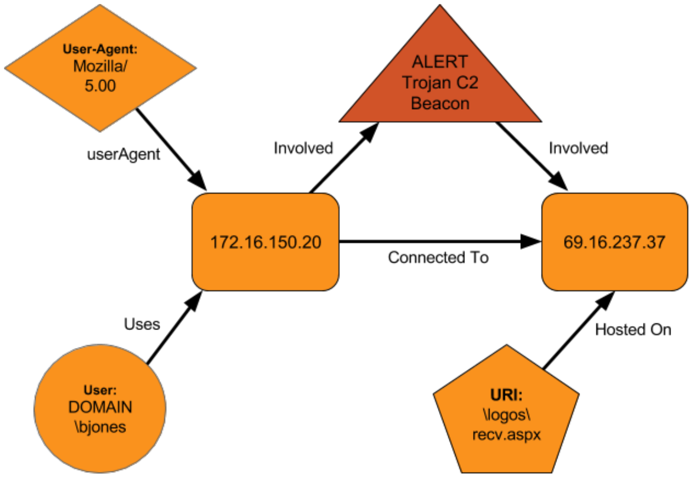
Validating Alerts

Validation is the process of determining whether an alert is either a true or false positive. Even if an alert is deemed to have truly picked something up, it does not necessarily mean there was an incident. Clarity is what analysts need to maximize their time and make these determinations faster and with more certainty.

To obtain that clarity, analysts must be able to investigate an alert and determine both the impact that a potential incident could have and the confidence with which it was generated. Sqrrl makes it easy to assess the state of your IT infrastructure and gather additional data about endpoints, applications, and network traffic. Sqrrl enhances your investigation by making sense of your data and leveraging it.

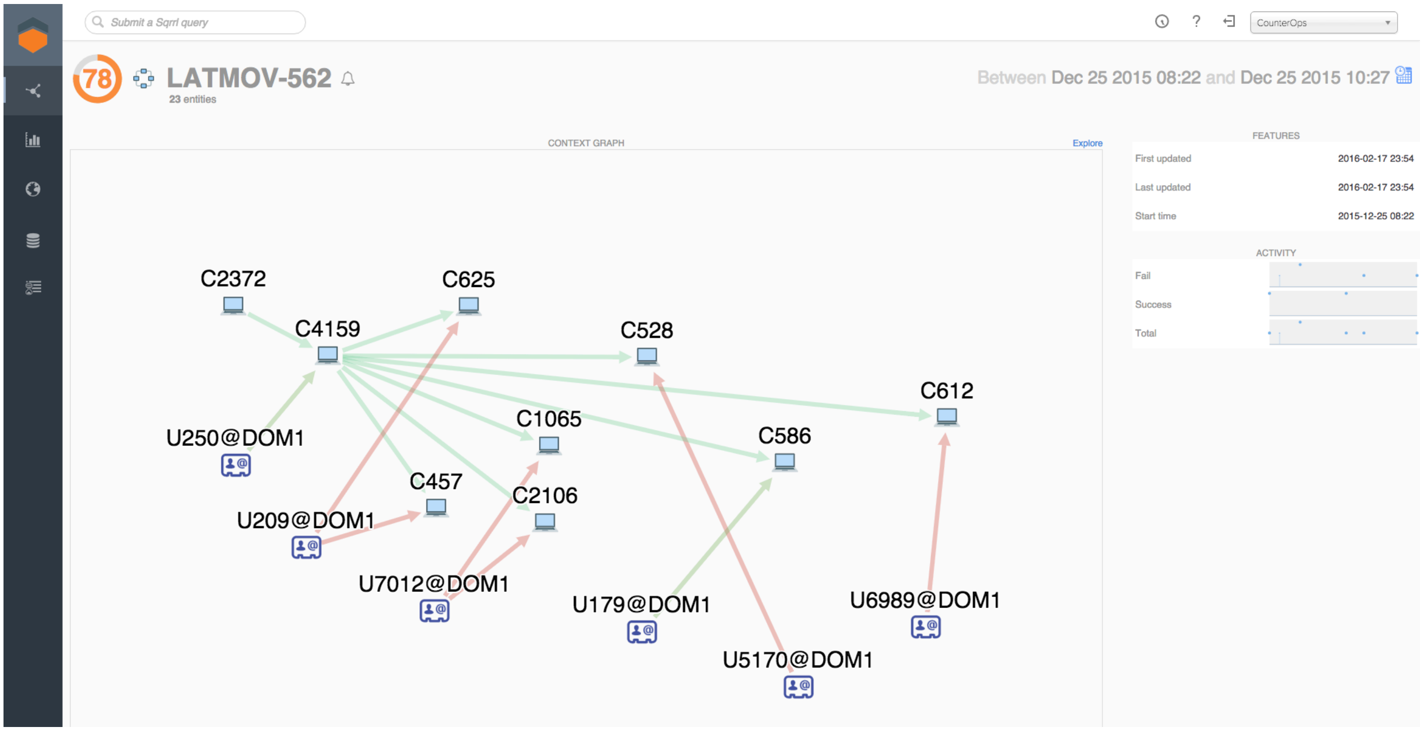
Using Context Graphs

Context graphs are a very effective way of both resolving alerts and scoping incidents. IDS alerts can be represented as a graph that extracts knowledge from line-oriented log files and shows how entities and relations connect to each other visually. In this example, the rectangles represent two endpoints, both involved in a command and control (C2) beacon alert entity, representing the traffic that was alerted on. The User, User-Agent and the URI value associated with the request are added to the graph, so right away you can see what the triggering request was and whether you should care about it. Sqrrl leverages advanced context graphs to give analysts unparalleled clarity.



Scoping the Incident

Once a threat is found, containing and responding to it is far from the last step in resolving the incident. To answer the two questions involved in the scoping phase (i.e. what other assets and what other activities were involved in the attack), analysts must then correlate data from various sources, conduct root cause analysis, and scope the impact of an incident. Correlating gathered intel with other known threats or incidents is another advanced data fusion practice that Sqrrl lets you do with ease. Gathering and contextualizing information is critical in developing effective analyses both of vulnerabilities in your own infrastructure and of threats menacing you over time.



First updated	2016-02-17 23:54
Last updated	2016-02-17 23:54
Start time	2015-12-25 08:22

Sqrrl Detection Profile with Context Graph

The Sqrrl Advantage

Sqrrl's detection and response platform reduces investigation timeframes from an average of 30 days to just a few hours. This results in both cost savings and a more efficient use of security resource, so that analysts can redeploy to other activities such as hunting. Sqrrl's benefits include:

- Contextual, intuitive graph visualization of even the most complex networks
- Automated detection of anomalies and adversary tactics, techniques and procedures
- Aggregating and fusing petabytes of disparate data sets
- Real-time search, query, and analysis of entity behaviors
- Blast radius analysis made simpler through contextual visualizations
- Fast drill downs into connected, underlying datasets

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