Sqr rl and CDM

THREAT HUNTING FOR
CDM PHASE 3

For More Information:

Ely Kahn
VP Business Development
Sqr rl Data, Inc.
ely@sqr rl.com
202-330-2992
www.sqr rl.com
TABLE OF CONTENTS

1. EXECUTIVE SUMMARY ................................................................. 3
2. CDM OVERVIEW.............................................................................. 3
3. THREAT HUNTING OVERVIEW ..................................................... 4
4. SQRRRL OVERVIEW ...................................................................... 4
5. SQRRRL FOR MNGEVT .................................................................. 6
6. SQRRRL FOR OMI .......................................................................... 7
7. CDM INTEGRATION ......................................................................... 8
1. EXECUTIVE SUMMARY
Sqrrl's Threat Hunting Platform is uniquely suited to support CDM Phase 3 MNGEVTs and OMI requirements. Sqrrl's Threat Hunting Platform features:

- Machine learning and graph algorithms to detect kill chain behaviors
- Sqrrl’s Security Behavior Graph, which leverages link analysis to enable analysts to easily create attack narratives
- Big Data processing and storage using Hadoop and Apache Accumulo

MNGEVT use cases include APT detection, insider threat detection, and malware detection. OMI use cases include alert investigations and incident investigations.

2. CDM OVERVIEW
The Continuous Diagnostics and Mitigation (CDM) program is a dynamic approach to fortifying the cybersecurity of government networks and systems. CDM provides federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.¹

CDM Phase 3 focuses on “What is happening on the network?” and builds on the CDM capabilities provided by Phases 1, 2, and BOUND. For CDM Phase 3, “the network” includes network and perimeter components, host and device components, data at-rest and in-transit, and user behavior and activities. Phase 3 focuses on moving beyond asset management to a more extensive and dynamic monitoring of security controls. This will include prepare and respond to incidents, ensure software/system quality is integrated into the network/infrastructure, detect internal actions and behaviors to determine who is doing “what,” and finally, mitigate security incidents to prevent propagation throughout the network/infrastructure.

CDM Phase 3 includes both Manage Events (MNGEVT) and Operate, Monitor, and Improve (OMI) capabilities. MNGEVT and OMI integrate to provide complementary processes and procedures to strengthen Agencies’ security postures. MNGEVT focuses primarily on the identification of security threat vectors, detection of security violation events and classification of event impact. OMI focuses on in-depth root cause analysis of security incidents and security mitigation response/recovery. An incident report is the structured security record used by MNGEVT and OMI to maintain and share event and mitigation information.²

¹ Sourced from https://www.dhs.gov/cdm
² Sourced from DHS CDM Attachment N-3-Manage Events Requirements document
3. THREAT HUNTING OVERVIEW

Threat hunting is the proactive, iterative, human-driven, and analytical approach to detect cyber adversaries that have evaded detection by existing cyber defenses. Threat hunting as a concept has existed within the Department of Defense for the last 10 years, but over the last 12-18 months adoption of hunting techniques has exploded within government and industry. As an example, Department of Defense has stood up dozens of Cyber Protection Teams whose mission is focused on threat hunting and incident response. Similarly, DHS has stood up a Hunting and Incident Response Team (HIRT) within the National Protection and Programs Directorate.

Within the vendor community, Sqrrl has established itself as both the thought and market leader when it comes to threat hunting. Sqrrl’s threat hunting methodology supports a variety of different types of hunts, including threat intel-driven, x-driven, and kill-chain driven hunts. Sqrrl’s threat hunting methodology is depicted in Figure 2.

4. SQRRL OVERVIEW

Sqrrl provides a Threat Hunting Platform that is enables security analysts to target, hunt, and disrupt advanced cyber threats. Sqrrl’s threat hunting software is deployed in both Fortune 50 companies and large government agencies. Their customers include some of the biggest companies in manufacturing, telecommunications, and financial services and government agencies such as the Transportation Security Administration and Department of Defense Special Operations Command (SOCOM). Gartner (“How to Hunt for Security Threats”, April 6, 2017) identified Sqrrl as the only pure-play threat hunting platform, and Sqrrl has been identified as a top hunting solution by SC Magazine, Network World, Info Security Products Guide, CRN, SINET, and the Cybersecurity Excellence Awards.

Sqrrl’s industry-leading Threat Hunting Platform (THP) unites link analysis for search and visualization, machine learning-powered kill chain analytics, and multi-petabyte
scalability capabilities into an integrated solution. Its unique approach enables security analysts to discover threats faster and reduces the time and resources required to investigate them. Unlike traditional signature- or rule-based detection solutions, Sqrrl’s THP detects the Tactics, Techniques, and Procedures (TTPs) of cyber adversaries using kill chain analytics. It leverages network, endpoint, identity, and threat intelligence datasets and integrates with various Security Information and Event Management (SIEM) tools.

Sqrrl is ideally suited for Security Operations Center (SOC) teams, and is deployed as Hadoop-based software appliance installed on a cluster of commodity servers. Sqrrl’s THP manages the ingest, storage, and analysis of log files from sources that include endpoints, servers, security and network devices, SIEMs, and custom applications. In addition to providing storage and query of raw data, Sqrrl’s THP creates linked data models (i.e., graph ontologies) that aggregate and organize the raw data into entities and relationships that analysts explore and analyze using Sqrrl’s web-based visual analysis interface.

One of the central capabilities that sets Sqrrl apart from other security solutions is the Security Behavior Graph, a powerful and contextual visualization for detecting and tracking threats. The Security 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 (e.g., flow data, proxy logs, endpoint data, identity data, threat intelligence, vulnerability data, etc.) into these common models. The linked data model, laid out as a graph, allows Sqrrl to use proprietary graph and unsupervised machine learning algorithms (e.g., multivariate Bayesian statistics) 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.

**Figure 3. Sqrrl Architecture**
Sqrrl’s machine learning analytics and graph algorithms provide best-in-class capability to detect various kill chain tactics, such as lateral movement, malware beaconing, DNS tunneling, domain generation algorithms, data staging, and data exfiltration.

Other key features include the ability to save and replay hunts, the ability for a user to create new analytics without the need to write any code, and an extensible risk framework that enables an organization to develop a comprehensive view of risk across Sqrrl’s analytics, vulnerability scans, threat intel matches, and SIEM alerts.

5. SQRRL FOR MANAGE EVENTS
A key goal of MNGEVTs is to conduct advanced threat detection. Sqrrl, as the leading Threat Hunting Platform, is uniquely suited for this requirement. Specific Sqrrl use cases aligned to MNGEVTs include the following:

**Advanced Persistent Threat (APT) Detection**
High profile breaches in the past few years have proven that the most sophisticated attackers won’t be stopped by perimeter security or automated detection systems. These adversaries are skilled enough to avoid tripping the digital tripwire and rule-based detection capabilities of a SIEM, firewall, or IDS. Leveraging threat hunting can allow analysts to locate these threats through the noise, as hunters can dive into a network and identify advanced attackers based on Indicators of Compromise (IOCs), specifically the TTPs that they leave behind. Sqrrl orients analysts towards finding these threats by automating detection of adversarial TTPs along the kill chain, discussed in more detail below. Rather than being left to guess about adversary behavior, an analyst can more easily isolate advanced threats by anticipating their moves based on the kill chain model. Whether it is a hacker moving laterally through different accounts or sending large quantities of data out of the network, Sqrrl will track down and isolate even the most advanced attackers based on the behaviors they cannot avoid exhibiting.

**Data Breach Detection**
When your network is compromised and a breach in your perimeter has let an adversary get in and potentially get out with your data, it is critical that you detect and address the breach as quickly as possible. Using a combination of Sqrrl’s anomaly detection, TTP oriented detectors, and Behavior Graph, an analyst can easily identify where there is outward flow of data from their network. The faster analysts can locate a breach the faster they can remedy them and move on to detecting new anomalies within a network that might indicate that an organization has been compromised.

**Malware Detection**
Malware infections are commonly used to establish command and control nodes within a network from which attackers can organize their actions and ultimately act on their objectives. While malware comes in many different families and types, more advanced malware is often undetectable to signature-based solutions. Sqrrl leverages UEBA to determine specific patterns of behavior, such as malware beaconing, DNS tunneling, and domain generation algorithms, which would indicate that a particular machine or asset has been compromised and is being used by an attacker. This means that Sqrrl
can detect the presence of malware on your network without having to rely on signatures or intel that may be lacking in the case of a custom or previously unseen malware type.

![Sqrrl Screenshot](image)

**Insider Threat Detection**
One of the biggest threats to organizations today is not necessarily the attackers trying to break into systems from the outside, but malicious, motivated insiders trying to steal information from within a company’s network. Sqrrl’s TTP detectors, including data staging and exfiltration detection, can detect suspicious behavior whether it is being carried out by external or internal threats, since Sqrrl looks multiple datasets for any indications that aggregation or mass migration of data is occurring. Armed with behavioral baselining and anomaly detection, Sqrrl can ID and tag malicious insiders before they carry out their objectives.

6. **SQRRL FOR OMI**
A key goal of OMI is to conduct incident investigations and conduct full root cause analysis. Threat hunting and incident investigations are actually quite similar from a functional requirements perspective, and as such, Sqrrl is also used to conduct more effective and efficient alert and incident investigations. Specific Sqrrl use cases aligned to OMI include the following:

*Alert Triage*
SIEMs, firewalls, and IDS can be effective in detecting violations of policies that might indicate malicious behavior, but analysts monitoring these systems are often flooded with alerts and false positives. Alert triage is the process of determining the priority in which alerts are investigated. Often this is done with little context or limited information on the entities involved in an alert. This process is made far simpler through Sqrrl’s comprehensive entity profiles, which provide a rollup of all the information that an analyst may need to determine the scope of an alert, including a risk score and related anomaly detections.

**Incident Investigations**

An incident investigation begins any time that an analyst is confronted with an indicator that there may be malicious or anomalous activity going on in a network. Through its Behavior Graph and risk scoring, Sqrrl is capable of empowering analysts to rapidly and effectively investigate the full context of an alert or a potential IOC. Moving from log-based investigations and to visually intuitive investigations frees up time for analysts to focus on finding new indicators and threats. Sqrrl has helped reduced the Mean Time to Resolution metric for incident investigations by an order of magnitude for some of its customers.

7. **CDM INTEGRATION**

Sqrrl operates within a larger ecosystem of interoperable tools, as depicted in the figure below. This enables users of Sqrrl’s Threat Hunting Platform to ingest datasets from SIEMs, network and endpoint tools, and from threat intelligence and vulnerability feeds. Sqrrl can also integrate with orchestration tools to enable analysts to dynamically take automated remediation actions based on a hunt or investigation.

*Figure 5. Sqrrl Partner Ecosystem*
Sqrrl has reference architectures with various SIEMs and log management solutions (including existing Hadoop or Elastic clusters). Sqrrl’s reference architecture with Splunk is depicted in Figure 6.

Figure 6. Sqrrl / Splunk Integration