sqrrl Target. Hunt. Disrupt.

PROPOSAL

Proposal For
ALTERATIONS TO THE NIST CYBERSECURITY FRAMEWORK

April 2017

Submitted to:
National Institute of Standards and Technology

Submitted by:

Ely Kahn
VP Business Development
Sqrrl Data, Inc.
www.sqrrl.com

TABLE OF CONTENTS

125 Cambridge Park Dr.
Suite 401
Cambridge, MA 02140

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

www.sqrrl.com
@SqrrlData

1.0 SQRRL OVERVIEW

Sqrrl Data, Inc. (“Sqrrl”) was born out of the National Security Agency (NSA). With their roots in the U.S. Intelligence Community, Sqrrl’s founders have worked with some of the world’s largest, most complex, and most sensitive datasets for the last decade. While at the NSA, Sqrrl’s founders developed a sorted, distributed key/value store called Accumulo.

Sqrrl is the threat hunting company that enables organizations to target, hunt, and disrupt advanced cyber threats. Sqrrl’s industry-leading Threat Hunting Platform unites link analysis, User and Entity Behavior Analytics (UEBA), and multi-petabyte scalability capabilities into an integrated solution. Sqrrl reduces attacker dwell time by detecting adversarial behavior faster and with fewer resources through the use of machine learning, and enables effective threat hunting. As an incident response tool, it enables analysts to investigate the scope, impact, and root cause of an incident more efficiently and thoroughly than ever before.

Sqrrl is headquartered in Cambridge, MA. Users of Sqrrl Enterprise include Fortune 100 companies in finance, telecom, healthcare, and large government agencies.

2.0 PROPOSED EDITS TO THE NIST FRAMEWORK

I. Proposed Edits to NIST Cybersecurity Framework

Insert under DE.DP-2: "Detection processes incorporate both detection of threats by automated systems and by human-driven threat hunting"

II. Justification for Edits

A. Summary: Currently, the section on detection methods focuses principally on automated detection. However, in modern SOCs, detection processes involve both an automated and a human-driven component. This latter approach is referred to as "threat hunting," which is defined as proactively and iteratively searching for threats that have evaded detection by automated detection systems.[1]

There are three key reasons for why threat hunting should be explicitly included in the definition of detection processes:

First, threat hunting is distinct from automated detection. Automated detection mechanisms, such as firewalls, IDS/IPS, SIEMs, and newer advanced analytic tools continuously run in the background firing off alerts using heuristics, matching algorithms, and statistical models. Threat hunting, on the other hand, is a human-driven process that is designed to look for the threats that automated systems miss.[2] Hunters are continuously innovating and adapting to new attacker techniques, and often detecting attacks that sit in the gaps of automated systems.

The second reason for this explicit inclusion is that threat hunting is one of the fastest-growing trends in cyber security and is rapidly becoming a security staple for SOCs. In a recent industry study, 86% of security professionals stated that their firms engaged in some form of threat hunting.[3] This number is likely to continue to rise as the industry standardizes detection methodologies which best incorporate automated and human-driven detection. Additionally, a 2017 Information Security Community study found that 79% of information security staff feel that threat hunting should or will be their top priority in the upcoming year.[4] Finally, Gartner (a top IT research and advisory firm) is currently developing research to solidify threat hunting as one of the key functions of a SOC.[5]

---

[1] Lee, Robert M., Lee, Rob, "The Who, What, Where, When, Why and How of Effective Threat Hunting, SANS Institute Infosec Reading Room
[2] Ibid.
[3] Cole, Eric, "Threat Hunting: Open Season on the Adversary," SANS Institute InfoSec Reading Room, 2016
[4] Jai, Vijayan, "Threat Hunting Becoming Top of Mind Issue for SOCs," Darkreading, 2017, accessed 4/7/2017
[5] Chuvakin, Anton, "Planned: A Quick Paper on Threat Hunting – Ideas Sought," Gartner Blog Network, 2017, accessed 4/6/2017

Finally, threat hunting is critical to improving the efficiency and operational effectiveness of modern SOCs. The value from manual hunts derives from the fact that automated detection systems cannot catch 100 percent of attacks. Instead of just being focused on one or two steps of the attack kill chain (see: fig. 1.1) hunters are able to identify intruders at any stage of an attack. Threat hunting allows analysts to mitigate the effect of breaches by identifying them before adversaries are able to act upon their objectives. In a survey of 494 organizations conducted by the SANS Institute, 52% of respondents said that hunting techniques had found previously undetected threats on their enterprise. Additionally, 74% of respondents stated that threat hunting reduced their attack surfaces and 59% stated that threat hunting improved the speed and accuracy of their responses to threats.[6]

Fig. 1.1: the Cyber Threat Kill Chain

B. Threat Hunting Background Information

History and Definitions of Hunting

The term “threat hunting” originated with the US Air Force in the mid-2000’s, when they began to use teams of security analysts to conduct “friendly force projection on their networks.[7] As it was adopted by the private sector, analysts began referring to these practices simply as “hunting,” leading to the term “threat hunting” being widely adopted by the early 2010’s. Human-driven detection entails security analysts searching through their network in order to find suspicious behavior.[8] Although the industry standard for threat hunting is still being finalized, the vast majority of hunts can be grouped according to the Threat Hunting Loop (fig. 1.2). This is an iterative process wherein hunters identify areas deemed to be especially vulnerable, investigate said areas, and then incorporate intelligence and information gained into future hunts.[9]

[6] Cole, Eric, “Threat Hunting: Open Season on the Adversary,” 2016
[7] Bejtlich, Richard, “Become a Hunter: Fend off Modern Computer Attacks by Turning your Incident Response Team into Counter Threat Operations,” Information Security, 2011
[8] Sqrrl, “A Framework for Cyber Threat Hunting,” Sqrrl Enterprise, 2016, accessed 4/1/2016
[9] Sqrrl, “The Threat Hunting Reference Model Part 2: The Hunt Loop, Sqrrl Blog, 2016, accessed 3/27/2017

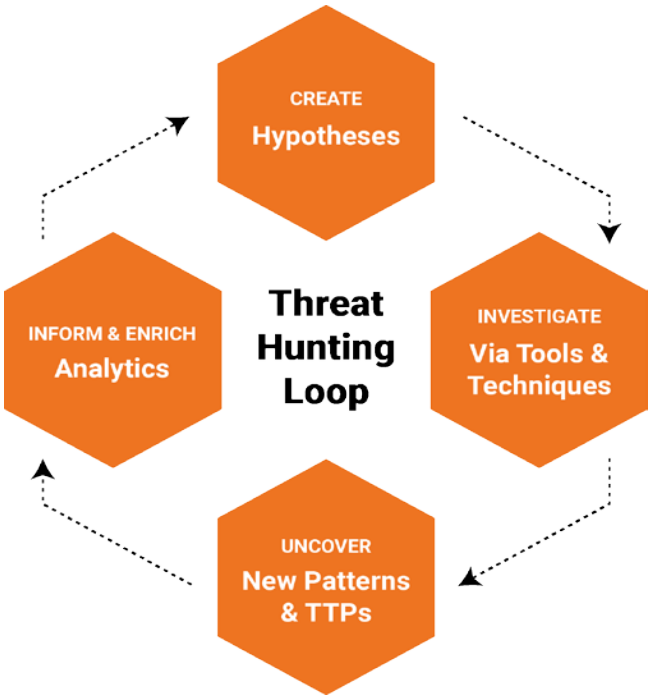

Fig. 1.2: the Threat Hunting Loop

Analysts improve the success of their hunts by incorporating intelligence and information about wider industry trends, malware developments, and adversary tactics, techniques, and procedures (TTPs). Hunters also employ “security information and event management” (SIEM) tools that use machine learning to track long-term trends on the host network and provide data that can be used to formulate future hunts.[10] Using these tools, data gained from manually conducted hunts drives and informs automated systems. The relative efficiency of SOCs can be assessed via the hunting maturity model (fig. 1.3). Using this metric we can observe that SOCs with exceptional detection procedures have high levels of data collection about their network, and use that to define hunt targets.

[10] Long, Michael C., “Scalable Methods for Conducting Cyber Threat Hunt Operations” SANS Institute InfoSec Reading Room, 2016

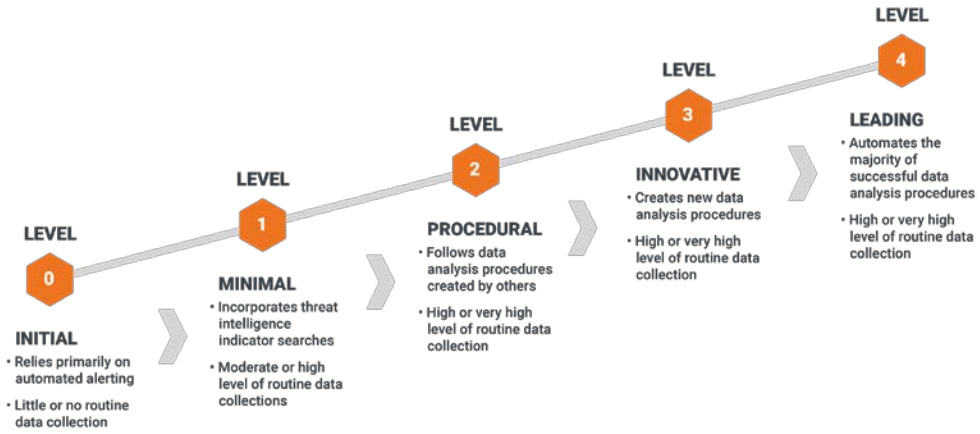

Fig 1.3: The Hunt Maturity Model

II. Submitted Background

C. Ely Kahn is a co-founder and VP of Business Development for Sqrrl. Previously, Ely served in a variety of positions in the Federal Government, including Director of Cybersecurity at the National Security Staff in White House, Deputy Chief of Staff at the National Protection Programs Directorate in the Department of Homeland Security, and Director of Risk Management and Strategic Innovation in the Transportation Security Administration. Before his service in the Federal Government, Ely was a management consultant with Booz Allen Hamilton. Ely has a BA from Harvard University and a MBA from the Wharton School at the University of Pennsylvania.

3.0 INFORMATIVE RESOURCES

Crowd Research Partners, “Threat Hunting: 2017 Report,” Crowd Research Partners, 2017 (https://static1.squarespace.com/static/571af41e3c44d8df0b10d7d8/t/589a27e5d2b8575c64fdba3e/1486497768625/2017-Threat-Hunting-Report.pdf)

Cole, Eric, “Threat Hunting: Open Season on the Adversary,” SANS Institute InfoSec Reading Room, 2016 (https://www.sans.org/reading-room/whitepapers/analyst/threat-hunting-open-season-adversary-36882)

Enterprise Strategy Group, ESG Research Report: Network Security Trends in the Era of Cloud and Mobile Computing, ESG Publishing, 2014 (http://research.esg-global.com/reportaction/networksecuritytrendsincloudmobile/Marketing)

Sqrrl, “A Framework for Cyber Threat Hunting,” Sqrrl Enterpirse, 2016, (http://sqrrl.com/media/Framework-for-Threat-Hunting-Whitepaper.pdf)