International Journal of Cognitive Informatics and Natural Intelligence
Volume 15 • Issue 4

Cyber Threat Hunting:
A Cognitive Endpoint Behavior Analytic System

Muhammad Salman Khan, Canadian Nuclear Laboratories, National Innovation Center for Cyber Security, Canada
Rene Richard, Digital Technologies, National Research Council Canada, Canada*
https://orcid.org/0000-0002-1342-6225
Heather Molyneaux, Digital Technologies, National Research Council Canada, Canada
Danick Cote-Martel, Canadian Nuclear Laboratories, National Innovation Center for Cyber Security, Canada
Henry Jackson Kamalanathan Elango, Digital Technologies, National Research Council Canada, Canada
Steve Livingstone, Canadian Nuclear Laboratories, National Innovation Center for Cyber Security, Canada
Manon Gaudet, Digital Technologies, National Research Council Canada, Canada
https://orcid.org/0000-0002-2119-9149
Dave Trask, Canadian Nuclear Laboratories, National Innovation Center for Cyber Security, Canada

ABSTRACT

Security and information event management (SIEM) systems require significant manual input; SIEM tools with machine learning minimize this effort but are reactive and only effective if known attack patterns are captured by the configured rules and queries. Cyber threat hunting, a proactive method of detecting cyber threats without necessarily knowing the rules or pre-defined knowledge of threats, still requires significant manual effort and is largely missing the required machine intelligence to deploy autonomous analysis. This paper proposes a novel and interactive cognitive and predictive threat-hunting prototype tool to minimize manual configuration tasks by using machine intelligence and autonomous analytical capabilities. This tool adds proactive threat-hunting capabilities by extracting unique network communication behaviors from multiple endpoints autonomously while also providing an interactive UI with minimal configuration requirements and various cognitive visualization techniques to help cyber experts quickly spot events of cyber significance from high-dimensional data.

KEYWORDS

Cognitive Analysis, Cognitive Command and Control, Cognitive Machine Learning, Cyber Security Operation Center, Cyber Threats, Endpoint Behavior, Prediction, SARIMA, Streaming, Time Series, Training

1. INTRODUCTION

A Cyber Security Operations Center (CSOC) is a centralized operational facility to continually monitor, identify, analyze, and defend against cyber-attacks and threats. A CSOC should have clear visibility into the data and situational awareness (SA) to enrich cyber analysis with local and global contextual information for identification and detection of threats (Carson Zimmerman, 2014). Cyber adversaries have acquired machine intelligence capabilities to deploy state-of-the-art sophisticated

DOI: 10.4018/IJCINI.20211001.oa9 *Corresponding Author

and autonomous tools to launch and deploy threats (Omid E. David & Nathan S. Netanyahu, July 2015) (Kevin M. Peters, March 2019) (Konstantinos Demertzis, Lazaros Iliadis, April 2015). A continuous war of attrition for both defenders and attackers (James P. Farwell & Rafal Rohozinski, August 2012) has reached a state in which attack objects such as malware are becoming self-aware and smart and are able to successfully penetrate defenses, as demonstrated by recent breaches and attacks (Sana Siddiqui, Muhammad Salman Khan, Ken Ferens, & Witold Kinsner, March 2016) (Sana Siddiqui, Muhammad Salman Khan, Ken Ferens, & Witold Kinsner, July 2017) (Kate O'Flaherty, December 2018) (Sana Siddiqui, May 2017). One of the main problems lies in keeping up with the ever-changing Tactics, Techniques, and Procedures (TTPs) of attacks that are mutating and using advanced intelligent techniques to hide their patterns; these attacks remain beyond state-of-the-art defense tools such as firewalls, Intrusion Detection/Protection Systems (IDS/IPS), and anti-malware technologies (Muhammad Salman Khan, December 2018).

In the current landscape of rapidly evolving cyber threats, a CSOC must be equipped with an advanced suite of tools and technological products that provide complete visibility into the environment and ensure the required security posture of the organization based on risk analysis and processes by a qualified security team. Required defense technologies should be identified based on a combination of the current skillset of the Security Operation Center (SOC) team as well as planned future training requirements. A CSOC should have a capability maturity improvement model to continually enhance the security capabilities. At a minimum, a CSOC should have four capabilities (Babu Veerappa Srinivas, n.d.): (1) Protection and Detection Technologies such as Firewalls, Antivirus, Intrusion Detection System, Intrusion Prevention System, Honeypots, Sandboxes, Endpoint Threat Detection and Response, Malware Analysis, and Forensics, (2) Analytical and Correlation Platforms such as Security Analytics, SIEM, and Visualization Tools, (3) Orchestration Tools such as Workflow Management, Response Orchestration, and Case Management, and (4) Threat Hunting and Intelligence.

2. CYBER THREAT HUNTING

Cyber threat hunting is gaining popularity as the cyber landscape is becoming more complex and dynamic. Threat hunting is a proactive cyber defense methodology that employs searching for threats with little to no knowledge of particular threat objects. In a way, threat hunting can be described as an exploratory cyber data analysis to find events of cyber significance. Furthermore, threat hunting can be defined as iteratively searching through data for either threats that have evaded the underlying cyber defenses or an indicator of a threat that may happen soon (such as any sign of the first stage of a kill chain, i.e. phishing emails or illegitimate port scanning for Reconnaissance stage) (Theodor Liliengren, Paul Lowenadler, May 2018). In a typical SOC, threat hunting commences with a search for threats that have evaded the rule-based cyber defenses but are known through either their behavior or their signatures (Lyndsey Franklin, Meg Pirrung, Leslie Blaha, Michelle Dowling, & Mi Feng, October 2017). Therefore, in this case, threat hunting requires threat intelligence to extract indicators of threats that can then be searched by human cyber experts manually using available tools and technologies. This is different from cyber Incidence Response (IR) methodologies, which are dependent on tools such as firewalls, anti-malware tools, and IDS/IPS. All these tools require configuring rules, writing queries, or updating signatures to detect known threats and generate cyber events. IR processes start event/incidence analysis by triaging the events for which an alert was raised by the defense tools already configured for threat detection (Tim Bandos, June 2019). Conversely, cyber threat hunting aims to uncover new patterns and evidence for threats that are not known or were not captured previously by any cyber defense tools. Threat intelligence does enrich threat hunting tasks but may not be required to start threat hunting (Jai Vijayan, April 2016). Therefore, threat hunting methodology involves four fundamental iterative steps (Robert M. Lee & David Bianco, July 2019) (Chiheb Chebbi, June 2018): (1) creating a hypothesis, (2) investigating by using tools and techniques, (3) uncovering new patterns or signatures, and (4) informing and enriching analytics.