ESG SHOWCASE

Continuous Compromise Assessment: A Missing Link in Cybersecurity

Date: July 2020 **Author:** Jon Oltsik, Senior Principal Analyst and Fellow

ABSTRACT: Organizations allocate large and growing security budgets annually, yet many still suffer system compromises and damaging data breaches. It seems that despite these investments, they can't detect or respond to threats in a timely manner, leading to disastrous consequences. To address this, many organizations are turning to network traffic analysis (NTA) technologies. While there are many options available, Lumu provides a comprehensive, cloud-based, easy-to-use offering with multiple layers of defense and analytics for continuous compromise assessment.

Overview

According to ESG research, 63% of security professionals believe that security analytics and operations is more difficult today than it was 2 years ago for several reasons, including (see Figure 1):[1]

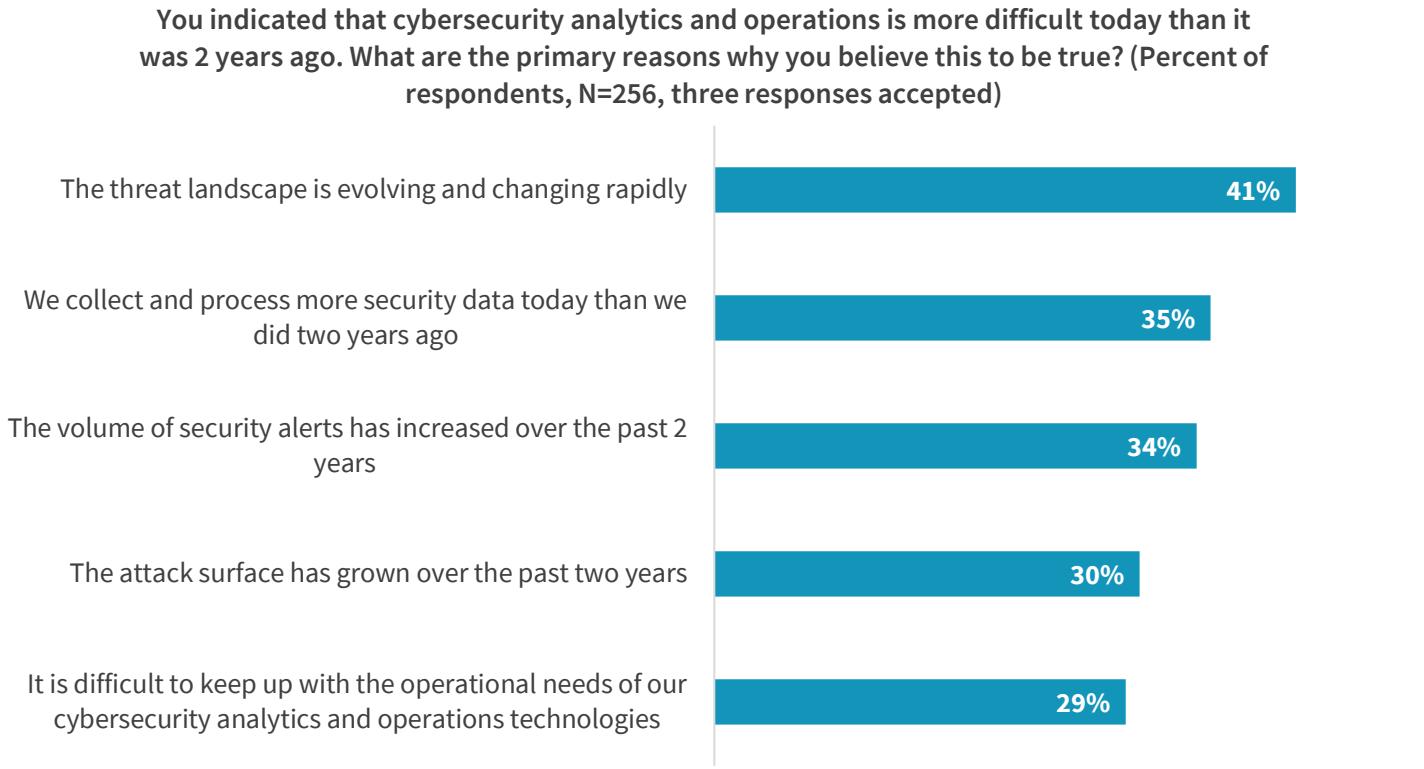
- A growing attack surface. The IT infrastructure has grown unabated over the past few years as workloads move to the public cloud, internal business applications are replaced by SaaS, mobile and IoT devices proliferate, and network traffic skyrockets. Somehow, security professionals must monitor network communications for constant signs of compromise.
- Keeping up with security alerts. Organizations have added new security tools for threat detection, but more tools equate to more alerts. Security analysts must separate signal from noise then prioritize and investigate the most critical alerts. This is increasingly difficult, however, when each tool unleashes a cacophony of individual alarms, forcing security analysts to pivot from tool to tool.
- Detecting and responding to security incidents. Sorting through alerts is especially difficult with regards to "low and slow" attacks that take weeks or months to compromise systems, move laterally across networks, and exfiltrate valuable data. Analysts must recognize individual clues from different tools and then piece them together manually to detect APTs and sophisticated targeted attacks. This takes skills and patience that many organizations don't have.

These challenges have been exacerbated in 2020 by a global pandemic. Security professionals find themselves working at home with increasing workloads and limited access to colleagues. Threat detection and response suffer as a result.

This is an unacceptable situation that increases cyber-risk and can lead to costly and damaging data breaches. CISOs can't continue using the same ineffective processes and technologies and expect to address these challenges. Clearly, something more is needed.

[1] Source: ESG Research Report, *The rise of cloud-based security analytics and operations technologies*, December 2019.

Figure 1. Top 5 Security Analytics and Operations Difficulties



Source: Enterprise Strategy Group

Modern Network Security Analytics to the Rescue?

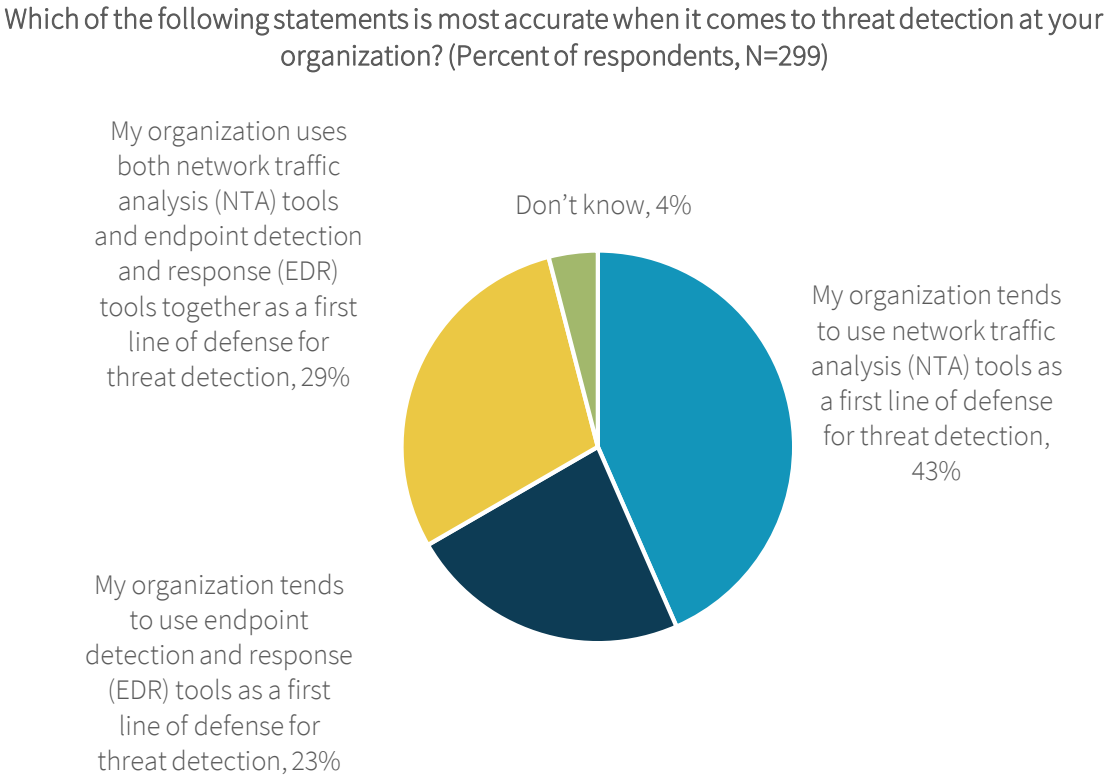
When organizations contemplate new tools for threat detection and response, they have a wide array of choices focused in areas like endpoints, networks, cloud security, and threat intelligence. This confusing situation brings up an obvious question: What's the best starting point?

Many security teams focus first on network security analytics to help them illuminate attacks and find compromises. This fact is illustrated by ESG research, as 87% of organizations use network traffic analysis (NTA) for threat detection and response today, and 43% say that NTA acts as a "first line of defense" for detecting and responding to cyber adversaries (see Figure 2).[2] This means that security analysts have "eyes on glass" using NTA tools as their primary means of understanding network behavior and illuminating compromises. When threats are detected, they use NTA tools for further investigation, supplementing this data by pivoting to other security telemetry and monitoring tools.

Why start with the network? As the old cybersecurity adage states, "The network doesn't lie." In other words, all cyber-attacks follow similar patterns, using networks for reconnaissance, lateral movement, and data exfiltration. Therefore, if you have strong network traffic analytics, you can accurately detect compromises in a timely manner and improve threat response.

[2] Source: ESG Master Survey Results, *The Threat Detection and Response Landscape*, April 2019.

Figure 2. NTA Is a First Line of Defense for Threat Detection



Source: Enterprise Strategy Group

NTA Considerations

There are many NTA tools to choose from, which can make the selection process perplexing for security teams. CISOs must move forward by assuming they are already compromised and look for solutions that can illuminate network traffic with the right analytics and functionalities. ESG believes the best NTA tools will feature:

- A wide variety of network telemetry. To piece together multi-staged APTs and other types of targeted attacks, NTA tools should collect, process, and analyze network metadata, including DNS queries, network flow, firewall/proxy logs, and SPAM activities and then align this metadata with timely threat intelligence. Network telemetry should also be collected across the entire attack surface including corporate networks, WAN connections, and cloud-based applications. This wide-angle view can help uncover and combine individual clues that may go unnoticed on their own.

- The ability to detect patterns based upon IoC correlation. The first thing any good NTA tool should do is detect pedestrian attacks by correlating traffic patterns and flagging confirmed indicators of compromise (IoCs). Detecting everyday threats can contain attacks, reduce analysts' workload, and initiate immediate remediation through manual actions or automated processes in conjunction with approved runbooks utilized by security orchestration, automation, and response (SOAR) tools. In this way, organizations can operationalize IoCs in real time for improved threat prevention.

- Advanced analytics to discover sophisticated attack patterns. Beyond obvious attacks, it's critical to look for meaningful anomalies. While somewhat hidden, these anomalies can be pieced together, forming a kill chain in combination. Leading NTA tools will collect network metadata from a variety of sources and feature advanced

analytics that detect, enrich, and combine these anomalies and then analyze them in context with the tactics, techniques, and procedures (TTPs) used by cyber-adversaries. This analysis not only pieces individual events into a time series kill chain, but also aligns these campaigns with threat intelligence as further evidence. The best solutions will retain network metadata for long periods of time so it can be compared with newly discovered attack campaigns and IoCs for retrospective investigation.

- Tight integration into the existing security operations infrastructure. CISOs don't want to buy new standalone security technologies. Rather, they want each new tool to integrate and improve their existing security operations and analytics platform architecture (SOAPA). In this way, NTA tools must interoperate with other security technologies like security information and event management (SIEM) systems, SOAR, and endpoint detection and response (EDR) tools.

NTA solutions must also be easy to deploy, use, and scale over time. To accommodate these requirements, many NTA solutions are delivered as SaaS offerings. Network metadata is collected on-premises and then shipped to the cloud for deep analytics and long-term storage.

NTA solutions with this functionality should help organizations detect and understand compromises in real time. Investigations can be supported and accelerated with detailed forensic data representing an attack timeline. The results? Security teams can decrease cyber-risk, accelerate threat detection and response, and streamline security operations.

Enter Lumu

Many NTA products available today were designed as network performance tools and later evolved into cybersecurity solutions. However, Lumu was purposely designed to analyze network traffic to measure compromise intentionally and continuously. As such, Lumu aligns well with the NTA capabilities detailed previously. According to the company, its mission includes, "making the life of the security practitioner better, making compromise more difficult, and making companies feel in control of their disperse, complex infrastructure."

Lumu accomplishes these objectives through its ability to collect, normalize, and analyze a wide range of network metadata, including DNS, NetFlow, proxy and firewall access logs, and spam boxes. The level of visibility these data sources provide gives LUMU the ability to understand network behavior, leading to conclusive evidence uncovering security incidents and system compromises.

How does Lumu do this? Through what it calls the "illumination process." First, Lumu collects network metadata and then correlates this data against known IoCs to detect and report on existing compromises. Lumu then analyzes the remaining network metadata looking for "anomalies of interest." Rather than simply report these anomalies to analysts for further investigation, Lumu performs deep correlation analysis to measure the distance between these anomalies and TTPs used for cyber-attacks. In this way, Lumu can uncover details like a seemingly benign web domain registered by known cyber-adversaries. Deep correlation results in alerts that uncover high probability security incidents. Finally, Lumu stores customer metadata for 2 years. When new attack campaigns are discovered, Lumu looks for previously undetected compromises by playing back and correlating historical metadata against these new IoCs.

Lumu's NTA is unique and comprehensive. CISOs looking for security analytics and operations help may want to seek out Lumu and evaluate how Lumu can help them with continuous compromise assessment.

The Bigger Truth

Current methods for compromise detection aren't working; there are simply too many tools, too many manual processes, and not enough skilled security analysts to get the job done effectively or efficiently. Since the network "doesn't lie,"

security professionals believe that improved network security analytics can help them dig out of the current hole, but not all NTA tools are created equally.

SOC teams should look for NTA tools that provide comprehensive coverage across the attack surface while monitoring and analyzing the right network metadata for rapid threat detection and response. There are lots of products to choose from in this space, but Lumu is designed specifically for continuous compromise assessment. Thus, Lumu has the potential to help organizations reduce risk, improve ROI on security assets, and accelerate threat detection/response.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188