ESG SHOWCASE

Stellar Cyber Open XDR and SOAPA

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

ABSTRACT: Security operations are in a perilous state at many organizations. SOC personnel are forced to do their job on a security-tool-by-security-tool basis, increasing the time and cost around tasks like threat detection and incident response. In 2016, ESG created a model for security operations technology called a security operations and analytics platform architecture (SOAPA) intended to address issues around security point tools sprawl. SOAPA is a tightly integrated architecture designed for high volume data collection/processing, advanced analytics, and security operations process automation. Open XDR from Stellar Cyber aligns well with SOAPA from a technology and operations perspective. Based upon this, Stellar Cyber may help organizations improve security operations efficacy, efficiency, and productivity.

Overview

According to a recent ESG research study, 63% of organizations believe that security analytics and operations is more difficult today than it was two years ago. This is due to several external and internal factors (see Figure 1).[1]

In this case, external factors are those that cybersecurity professionals have no control over. As external conditions change, SOC teams must integrate these changes into their security analytics and operations plans. External factors making security analytics and operations more difficult include:

- The dangerous threat landscape. Cybercriminals and nation states are collaborating to engage in targeted attack campaigns like business email compromise (BEC), data theft, and ransomware. SOC personnel must monitor their tactics, techniques, and procedures (TTPs) and capture the IoCs they use for threat prevention and hunting. Unfortunately, few organizations have the right skills, tools, or staff sizes to keep up.
- The ever-growing attack surface. Large organizations are embracing SaaS applications, public cloud infrastructure, and IoT devices to support business initiatives. Overwhelmed security operations teams must prevent, detect, and respond to threats across this growing attack surface.

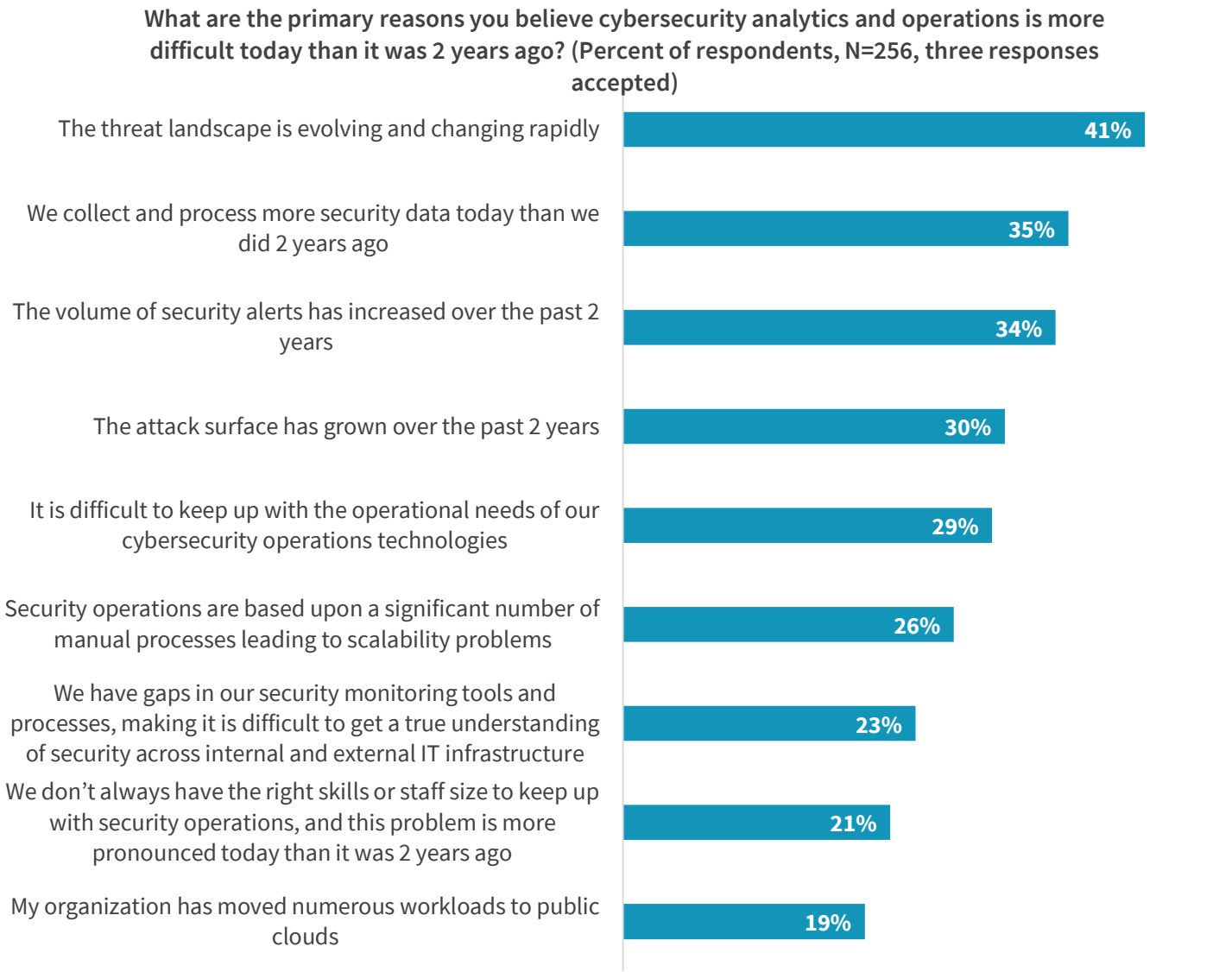
In addition to external changes, SOC personnel must address daunting and systemic cybersecurity issues affecting their organizations. These issues include:

- Massive security telemetry collection, processing, and analysis. Security teams are collecting growing volumes of security data including threat intelligence, logs, network packets, cloud logs, and EDR telemetry. Furthermore, many organizations are retaining this data for longer periods of time. As security data pipelines grow, SOC teams are asked to moonlight as data and storage engineers.

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

- The growing volume of security alerts. More security tools equate to an increasing volume of security alerts that need to be triaged, investigated, prioritized, and otherwise addressed. This is difficult to do, especially for under-staffed SOCs.
- Security operations complexity. SOC teams must not only detect and respond to attacks but also coordinate with IT operations on remediation actions. This is especially difficult as alert volumes and workloads increase.

Figure 1. Factors Making Cybersecurity Analytics and Operations More Difficult



Source: Enterprise Strategy Group

It is worth noting that many security professionals complain that security operations rely on too many point tools, and too many informal/manual processes. Furthermore, research from ESG and the Information Systems Security Association (ISSA) indicates that 74% of organizations claim that they've been impacted by the global cybersecurity skills shortage, leading to increasing workloads, open requisitions, and a security team that is too busy to use its security technologies to their full potential.[2]

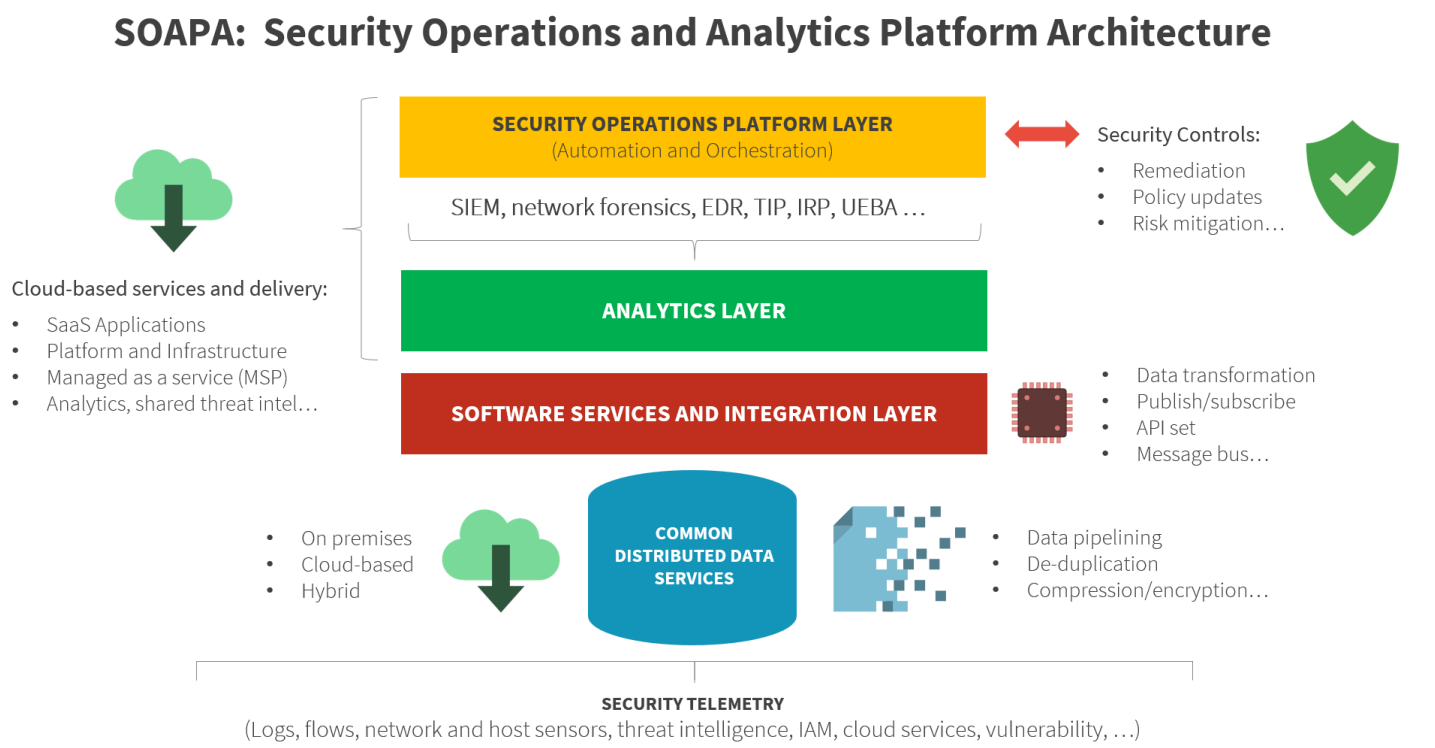
[2] Source: ESG Research Report, *The Life and Times of Cybersecurity Professionals 2018*, May 2019.

Toward a Security Operations and Analytics Platform Architecture (SOAPA)

The ESG data clearly indicates that current security operations strategies aren't working well. ESG believes that one of the fundamental problems here is the lack of tightly integrated security operations technologies. Today's point tools don't share data, so they can't correlate alerts or track suspicious behavior across a kill chain. This places an added security operations burden squarely on an already overburdened SOC staff. Even the most talented SOC teams won't keep up with the scale of a growing workload.

What can be done? Since 2016, ESG has advocated for an end-to-end, tightly coupled security operations technology architecture where security products share data, feed multiple analytics engines, and take automated incident response and risk mitigation actions. ESG calls this a security operations and analytics platform architecture (SOAPA, see Figure 2).

Figure 2. SOAPA



Source: Enterprise Strategy Group

SOAPA is a bottom-up architecture composed of a:

- Common distributed data service. SOAPA has a foundation of a common data pipeline for batch and streaming data that creates a flexible schema for all security analytics engines. In this way, SOAPA provides massive amounts of security data for all types of analytics—from real-time threat detection to long-term retrospective investigations spanning months or even years of security data.

- Software services and integration layer. This layer serves as a bridge between security data and analytics engines that consume the data. In simple terms, the software services and integration layer provides common APIs and messaging services, making all security data available to analytics engines when they want it and in the format they want it in.

- Analytics layer. Security data is made available to various security tools that monitor and analyze factors like user/entity behavior, network traffic, threat intelligence analysis, and SIEM. The SOAPA analytics layer is designed for end-to-end data analysis, providing high-fidelity alerts to help SOC teams accelerate threat detection and incident response.

- Security operations platform layer. When security analytics find something suspicious/malicious, SOC teams can then pivot to the security operations platform layer. This layer can be programmed to take automated actions like gathering additional data for an investigation, quarantining a system, or creating a case management system ticket. Security remediation operations can also be orchestrated with security controls like firewalls, network proxies, and web or DNS gateways. The security operations layer also provides a common workbench and runbooks for complex operations that require manual intervention, such as threat hunting.

SOAPA is designed to address existing security operations challenges related to point tools sprawl, manual processes, and the perpetual cybersecurity skills shortage. By replacing disconnected point tools with an efficient open security operations architecture, SOAPA makes security data available for analysis in real time. Analytics engines attain comprehensive situational awareness, leading to more accurate and detailed security alerts. SOC personnel can then take automated actions, improve collaboration, accelerate and automate processes, and bolster threat detection/response performance.

Stellar Cyber Open XDR and SOAPA

While SOAPA was first conceived as a heterogeneous product architecture, several vendors have developed their own SOAPA offerings. One such vendor is Stellar Cyber with its Open XDR offering. Open XDR emulates SOAPA by providing:

- Interflow for data collection with third-party data support. Stellar Cyber addresses SOAPA's common distributed data services layer with something it calls Interflow for data ingestion and synthesis. Stellar instruments Interflow through a broad range of sensors designed to collect data from various sources including data and applications on the network, servers, containers, physical and virtual hosts, on-premises infrastructure, and public clouds. Interflow processes and normalizes security data with context and makes it available for Stellar Cyber's applications through a scalable and searchable data lake with integrated big data analysis. It is worth noting that Stellar Cyber opens Interflow to third-party data from sources like firewalls, EDR, threat intelligence, and vulnerability scanners. This is the openness in Open XDR.

- Multiple security applications. SOC and threat analysts view security telemetry through many applications depending upon what they are looking for. In the past, this would be accomplished using multiple applications from different vendors, creating some of the challenges described in ESG research. Stellar Cyber seeks to alleviate these issues, as its Open XDR SOAPA provides an abundant menu of applications including network traffic analysis (NTA), next-gen SIEM, user/entity behavior analytics (UEBA), and automated threat hunting and response, among many others. Stellar Cyber backs its analytics with multiple machine learning algorithms to weed out false positives and provide actionable data. It leverages both unsupervised and supervised machine learning including deep learning for different use cases.

- A common dashboard for security operations. All Open XDR applications are accessible through a common UI/UX that can be customized to create dashboards for junior employees, specific roles, or tier-3 experienced analysts. This can help with onboarding and training new SOC personnel, mentoring programs, and developing best practices.

By working with partners, Stellar Cyber's Open XDR can cover a distributed enterprise with a heterogeneous environment across endpoints, networks, and cloud-based workloads, and through Interflow, Stellar Cyber can collect, process, analyze,

and act on the right security data to help organizations accelerate threat detection and response. Finally, using its machine learning algorithms, Stellar Cyber models normal behavior. These models improve over time as the system tracks more activity, leading to greater accuracy for detecting behavioral anomalies.

The Bigger Truth

The data presented in this paper demonstrates that security operations is at a tipping point. Many organizations pieced together security controls, monitoring, and operations over the past 20 years, responding to new threats and requirements. Unfortunately, this forced the SOC team to approach their job responsibilities on a tool-by-tool basis. This, along with manual/informal processes and a cybersecurity skills shortage, led to the current situation where security operations are inefficient, labor-intensive, and increasingly ineffective.

Many CISOs are addressing this untenable situation by consolidating vendors, integrating technologies, and creating their own SOAPAs. On the supply side, innovative vendors are developing tightly integrated SOAPAs of their own. The best offerings follow a bottom-up model with strong data collection/processing, advanced analytics, and a common security operations workbench UI/UX.

Stellar Cyber Open XDR follows this model with Interflow for data collection and transformation, a scalable data lake for storing large volumes of data, machine learning to drive advanced analytics, a multitude of applications, and an innovative UI/UX with integrated automated response. Based on this, CISOs looking to modernize security operations may want to take a closer look.

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