Solution Showcase

JASK: Security Operations Through Enterprise Visibility and Advanced Context

Date: April 2018 **Author:** Jon Oltsik, Distinguished Analyst and ESG Fellow

Abstract: When it comes to security operations, large organizations face a troubling situation. Each year, they increase security operations budgets and purchase/deploy new types of technologies, but these investments deliver incremental benefits at best. Unfortunately, new technologies increase security operations complexity and exacerbate problems associated with manual processes, staffing deficiencies, and skills shortages. To address these issues, progressive organizations are building a tightly integrated security operations and analytics platform architecture (SOAPA) to help them meet objectives like accelerating security investigations and remediation tasks and bolstering SOC productivity. JASK is designed to supplement these SOAPA projects and deliver real near-term benefits.

Overview

According to ESG research, 72% of organizations believed in 2017 that security operations had become more difficult than it was two years previously.[1] Why? More than one-quarter (26%) of cybersecurity professionals said that the threat landscape is changing and evolving, making it difficult to keep up, 19% pointed to increasing volumes of security alerts, 18% said they have gaps in security monitoring leading to blind spots, and 18% complained that they don't have the right skills for security operations and analysis.

Aside from these complexities, security operations and analysis are also fraught with numerous challenges (see Figure 1). For example:

- **Infosec is challenged by the total cost of ownership.** Large organizations spend millions of dollars annually on security operations but still face overwhelming workloads, hundreds of daily security alerts, constant cyber-attacks, network penetrations, and data breaches. Given this, CISOs rightly complain about the return on their cybersecurity operations investments.

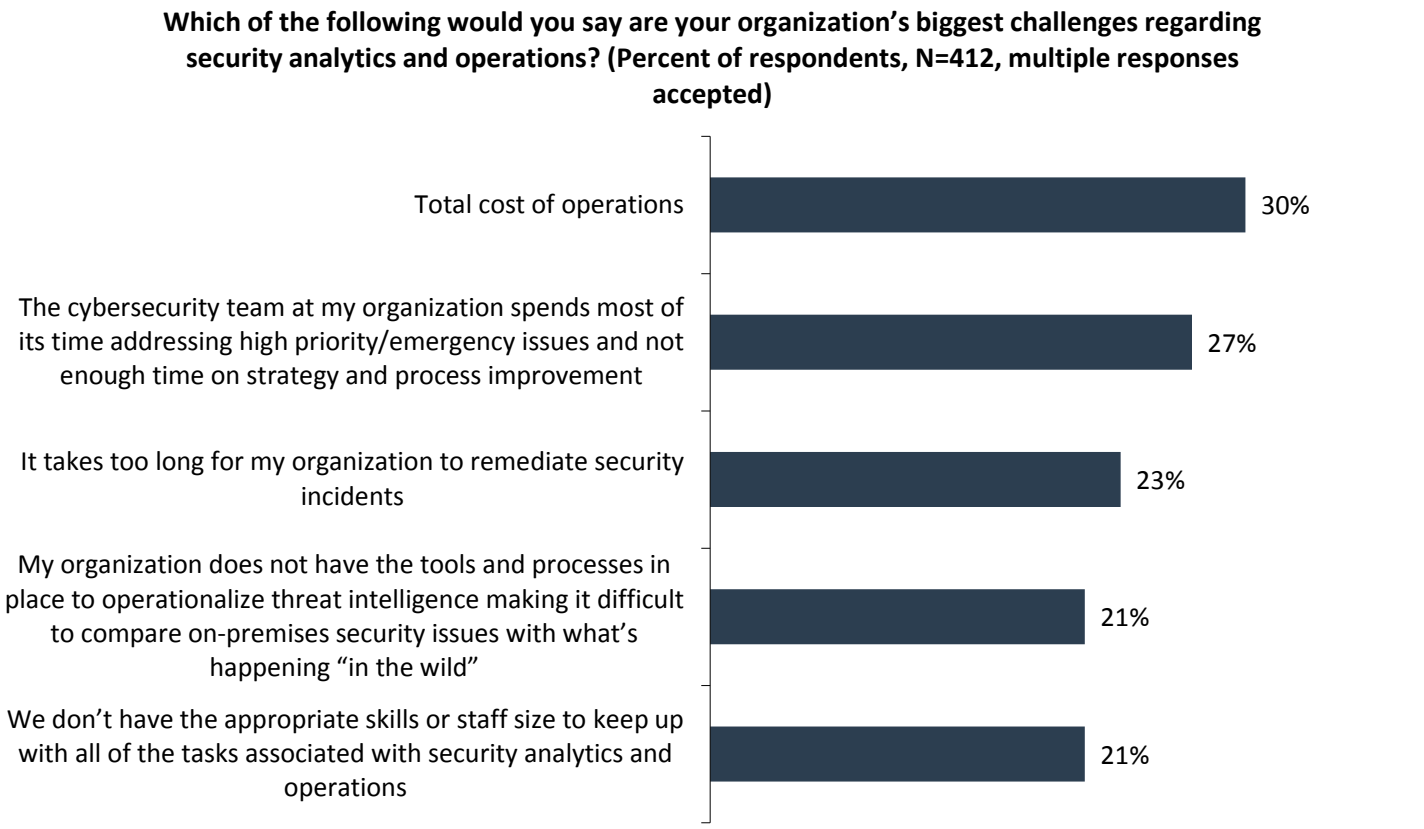
- **The cybersecurity team spends its time responding to emergencies.** More than one-quarter (27%) claim that their cybersecurity team spends most of its time addressing high priority/emergency issues and not enough time on strategy and process improvement. This not only leads to staff attrition and burnout but also limits the ability to plan for future threats, mitigate growing business risks, or keep up with necessary staff training.

- **Security incidents take too long to remediate**. This is consistent with data from the annual Verizon Data Breach and Incident Response (DBIR) report, where organizations report that it often takes them months before discovering

[1] Source: ESG Research Report, *Cybersecurity Analytics and Operations in Transition*, July 2017. All ESG research references and charts in this solution showcase have been taken from this research report.

cyber-attacks in progress on their networks. Meanwhile, cyber-adversaries enjoy lengthy "dwell time" on the network where they are free to conduct reconnaissance operations, find and exfiltrate valuable data, and plot foolproof escape plans.

Figure 1. Top Five Security Analytics and Operations Challenges



Source: Enterprise Strategy Group

Analysts must collect, correlate, and analyze far too much information—which is often what is causing the missed compromises. This is due to the fact that 40% of organizations have between 10 and 25 different security operations tools today, while 30% have between 26 and 50 security operations tools. This leads to a situation with too any alerts, too many screens, and not enough context. Taken together, the ESG data presents a distressing picture. While organizations dedicate vast budget dollars toward security operations, they continually fall behind cyber-adversaries' tactics, techniques, and procedures (TTPs) and the growing volume of security alerts. Furthermore, security operations teams are in constant firefighting mode, yet security incidents go undetected on the network for months at a time.

CISOs must internalize this data and realize that throwing more money at broken processes, under-skilled workers, and ineffective tools is a recipe for failure. At this point, security operations requirements have evolved beyond current staff skills, processes, and security point tools. Clearly, something must change.

SOAPA to the Rescue

Over the past fifteen years, large organizations built cybersecurity operations organically, adding various proprietary security technologies such as SIEM, vulnerability scanners, threat intelligence feeds, network security analytics tools, endpoint detection and response (EDR) systems, etc., over time. Each of these tools collects its own data, does its own analytics, and provides its own reporting and user interface. Unfortunately, this security operations model forced the SOC

team to rely on manual processes and human intelligence for aggregating, parsing, contextualizing, and analyzing a multitude of logs, alerts, and reports from an army of point tools. As if this wasn't bad enough, the SOC team had to sort through this morass of data, decide which alerts to investigate (and which to drop), gather some sort of context regarding the alert and the environment, and work with IT operations to prioritize remediation actions.

Today's security operations depend upon a complex system of disconnected point tools and manual processes that can't scale or easily change to address changing threats. How can organizations abandon this failing strategy? As management guru Tom Peters stated: "Almost all quality improvement comes via simplification of design, manufacturing, layout, processes, and procedures." In other words, CISOs must create a simplified security operations "system" that aggregates technology, automates processes, and enables greater productivity from cybersecurity staff.

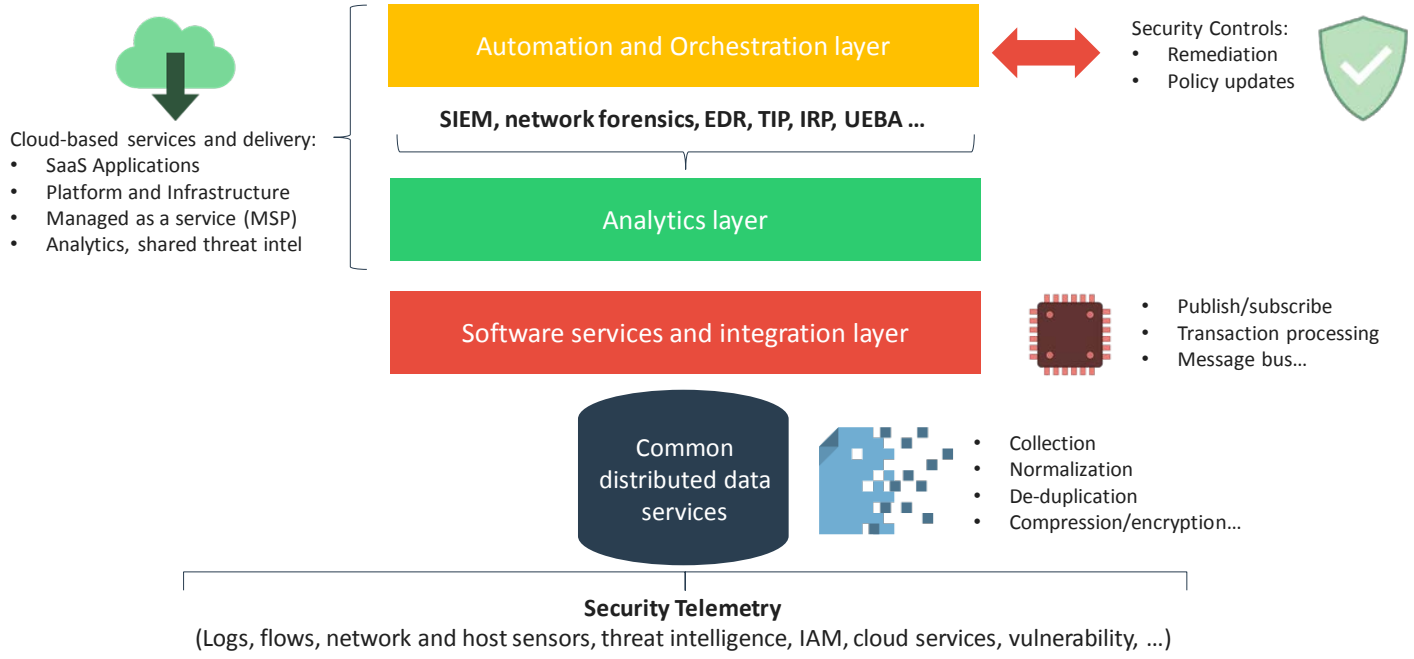
ESG research indicates that organizations are starting to execute on security operations strategies intent on meeting these goals. For example:

- Two-thirds (66%) of organizations say that security analytics is mostly done in a siloed way by different individuals using different tools, but their organizations are moving toward a more consolidated and integrated approach.
- Seventy-one percent of organizations say that they are actively integrating disparate security analytics and operations tools, and that security technology integration is either important or one of their highest priorities.

ESG believes that security technology consolidation and integration projects will lead organizations to turn today's army of point tools into a security operations and analytics platform architecture (SOAPA), composed of (see Figure 2):

1. A common distributed data service. To make real-time impactful decisions, security operations must be based upon the collection, processing, analysis, and prioritization of massive amounts of security telemetry. As such, SOAPA centralizes data management with a common distributed data services foundational layer. This layer enables efficient and effective data sharing amongst security operations tools (and between organizations).
2. A software services and integration layer. This SOAPA middleware sits between the data and the analytics applications. It is then used as a messaging bus to publish and push security data to analytics tools in a common format. Modern solutions are applying AI/ML to ingest diverse data sources more efficiently, while adding contextual connections for faster and effective decision making on irregular discoveries.
3. An analytics layer. Various types of security analytics engines are programmed to consume security data based upon different triggers and events. In recent years, security analytics have added data science and machine learning capabilities to build data models, calculate "normal" behavior, and better identify anomalies. In this way, leading security analytics engines can correlate and contextualize multiple security alerts and monitored assets, helping security analysts sort through cybersecurity noise and identify real issues and prioritize remediation efforts.
4. An automation and orchestration layer. After analytics engines identify real problems, security and IT operations must coordinate on incident response and remediation tasks. To facilitate these processes, SOAPA includes an automation and orchestration layer, supporting tasks like case management, collaborative workflows, and process automation.

Figure 2. SOAPA Architecture



Source: Enterprise Strategy Group

By integrating security operations point tools into a tightly coupled system, SOAPA creates a security tools ecosystem that can help organizations improve security efficacy through more accurate and timely threat detection. What's more, SOAPA can help streamline security operations through automation, orchestration, and workflow management between security and IT operations teams. Little wonder then why enterprise organizations are pursuing a SOAPA strategy.

Enter JASK

As an architectural solution, SOAPA is generally composed of disparate security tools from assorted technology vendors. Unfortunately, this may place the integration burden on security teams, forced to cobble together a SOAPA architecture out of homegrown or open source software. Few organizations have the software development or engineering skills needed for this task.

Enter JASK, a security technology startup based in San Francisco, California and Austin, Texas. JASK's management team is made up of industry veterans with years of experience in security operations, data science, and artificial intelligence, and the company's mission is to fundamentally change how security operations is done today.

JASK's security operations platform, the Autonomous Security Operations Center platform, aligns well with SOAPA as it is:

- **Built on data collection and processing.** JASK deploys various on-premises and cloud-based sensors to collect and process network, device, user, and application data. JASK can also consume various types of data from existing security tools and threat intelligence, supporting existing security operations workflows. To gain a better understanding of this information, JASK applies machine learning algorithms upon data ingestion. In this way, JASK has the ability to detect anomalous security events in real time. It also begins the parsing and contextual connection autonomously. JASK maintains a large data repository to piece together "low-and-slow" attacks over lengthy periods of time. As an example, when an endpoint suddenly beacons to an unknown IP address, JASK can equate this seemingly random event to lateral network movement, endpoint configuration changes, and software downloads that took place weeks or months ago.

- Using open source and cloud for scale and integration. JASK uses open source technologies like Hadoop and Apache Spark to provide a more open, extensible, and customizable architecture. Furthermore, JASK analytics engine lives in the cloud to deliver the scalable CPU and storage resources needed to analyze massive security data pools.

- Instrumented with a modern analytics engine. JASK is built around data science principles and machine learning algorithm clustering. The goal? Correlate network, device, user, and application data with cyber threat intelligence (CTI) to reduce thousands of security alerts down to between 3 and 10 "actionable insights"—true security risks that demand high priority investigations and remediation. As part of this process, JASK analytics work in concert with existing security ecosystem tools from vendors like Carbon Black, Cylance, FireEye, Demisto, Splunk, and many others in an effort to accelerate triage and get to the root cause of problems.

- Able to support existing security operations processes and technologies. JASK is designed to be non-disruptive by cooperating with existing tools and workflows. For example, JASK can supplement SIEM systems like IBM QRadar, ArcSight, and Splunk, helping to accelerate security investigations and remediation actions. To align with the SOAPA automation and orchestration layer, JASK works with ecosystem partners such as JIRA, Resilient, and ServiceNow.

With a background in security operations, the JASK development team is also well aware of how difficult it is to work in a SOC, staring at screens and bouncing among reporting tools. To address this, the JASK user interface presents security data in a "baseball card" view with a summary of the highlights that led the system to generate a JASK Insight, a prioritized notification of a collection of data that indicates a combination of events or activities that should be investigated. This starting point allows analysts to dig into the data to further investigate indicators of compromise (IoCs) and subsequent malicious behavior that led JASK to its conclusion. In this way, JASK believes it can help accelerate security investigations and remediation actions while boosting cybersecurity staff productivity.

JASK also remains committed to supporting analyst workflows, supplementing existing systems and processes. The company recently announced the JASK Navigator Console, a visually driven investigation console that presents security analysts with compromise activity containing all the context needed to determine a logical path to resolution. To further support enterprise operations, JASK also developed team support via customizable workflow queues. With the ability to represent user groups or teams, JASK Insights can be assigned to triage disparate resources. Insight's status can also be adjusted to help improve visibility into the overall status of all assigned tasks.

The Bigger Truth

Famed physicist, Albert Einstein, is purported to have said that the definition of insanity is doing the same thing repeatedly but expecting different results. Regrettably, this is exactly what many large organizations are doing today when it comes to security operations. They try to keep up with the latest threats by adding new types of detection and analytics engines, but these steps provide incremental improvements at best and in many cases, only exacerbate security operations complexity problems.

Smart CISOs realize that it's time to stop throwing good money after bad. Rather than add more point tools, they've initiated projects to consolidate and integrate security operations technologies, creating a SOAPA architecture capable of supporting current and future security operations needs.

The JASK team seems to understand this transition as its security operations technology aligns well with SOAPA. Furthermore, JASK does not demand that organizations "rip and replace" existing security operations processes and technologies. Rather, JASK can supplement an existing security operations infrastructure, helping organizations accelerate security investigations and prioritize remediation actions. As organizations get comfortable with JASK, they can offload existing security operations functionality to the JASK platform over time.

Moving forward, CISOs should strive to vastly improve security operations efficacy and efficiency and enhance existing security operations processes without adding technology complexity. Given JASK's design, CISOs may find it worthwhile to assess how its security operations technology can help them meet these requirements.

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