AHEAD

Next-Gen Security Operations:

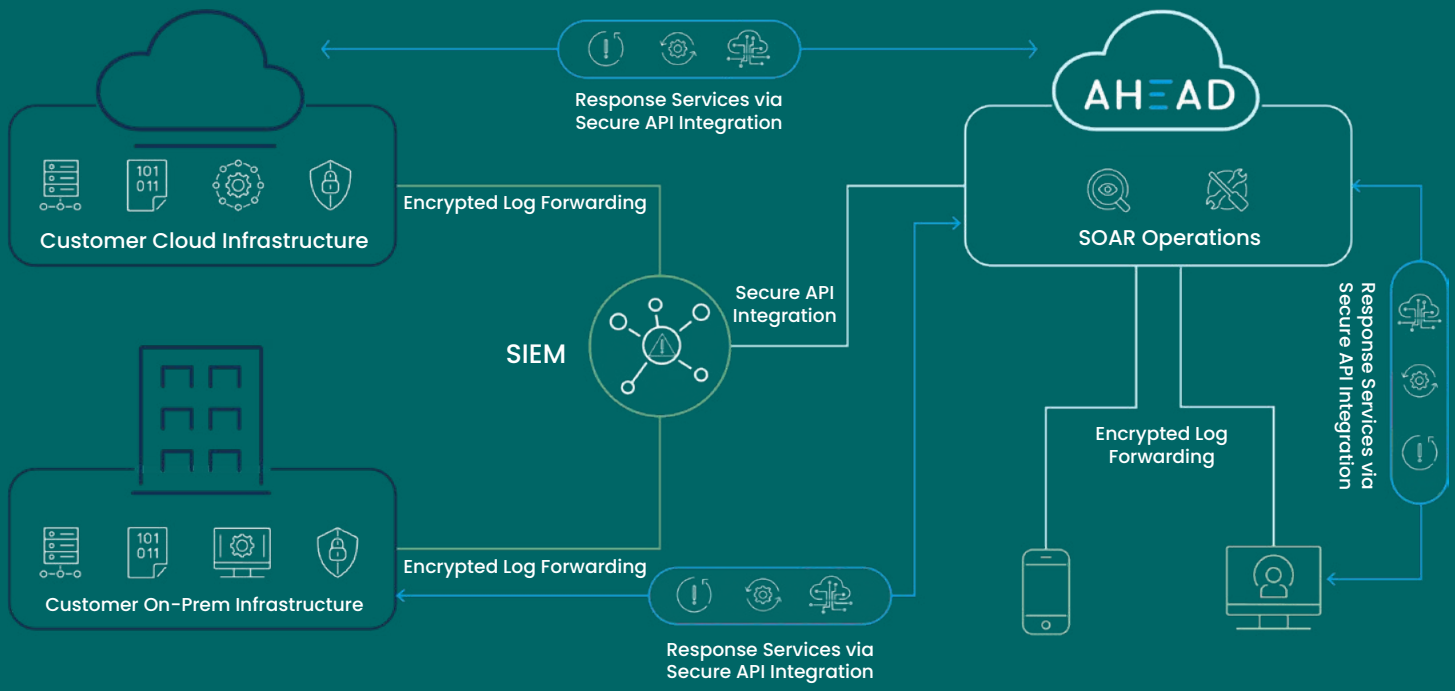
Delivering a Modern SOC in Today's Evolving Security Landscape

It's now common knowledge that organizations need a cybersecurity program to detect and respond to the threats that are constantly trying to make them front page news. But with the ever-growing complexity of modern threats and threat actors—and the near uncontrollable sprawl organizations face via their technological footprint—maintaining a robust, scalable, and adaptable Security Operations Center (SOC) to mitigate these challenges can be overwhelming.

Traditional security processes and tooling have proven unable to keep pace, creating gaps in visibility and protection, decreasing the ability to detect and respond to threats, and ultimately increasing overall risk posture. In overcoming these challenges, organizations should look to embrace and build a Security Operations Center capable of supporting their diverse, dynamic, and ever-growing environment to detect and respond to emerging threats via modular, scalable, and automated processes.

Table of Contents

Managed SOC: Architecture



Security Operations Centers are a Business Imperative

As a surprise to no one, the number of threat actors out in the wild continues to rise year over year. With average ransomware payouts approaching $1M last year, these groups have identified an incredibly lucrative business model and, like all businesses, continuously look to maximize efficiencies and profits for their "shareholders." Cybercriminals are constantly working to improve their product, often performing their own research and development to identify new zero-day vulnerabilities or novel methods to exploit existing ones – or even buying the information from other groups. As defenders from these threats, we have always been at an inherent disadvantage – one that becomes immediately apparent to anyone who has sat through an introductory business class. What happens when you pit one organization's profit center against another organization's cost center?

As if all this wasn't bad enough, organizations aren't doing themselves any favors with how rapidly their technology landscape is shifting and growing to try to keep up with the demands of their own business. In the rush to embrace these cutting-edge technologies, more often than not, security operations is unable to keep up. Tools and processes built for a static and on-prem environment can't support the dynamic and elastic nature of modern infrastructure and cloud-hosted services, not to mention even having the knowledge and skillsets to understand how they all work. All of this equates to a field day for threat actors as they look to exploit this perfect storm for an easy payday that the organization can't see or react to before it's too late.

In order to mount the level of defense necessary to protect their organizations, Security Operations Centers must evolve with the business to become the next generation SOC, both in the tools they leverage and the processes that drive them.

The SOC Needs Transformation Too

Digital transformation has been the name of the game for business and IT, and it's past time for security operations to join in. Just as the impetus for this transformation at the IT level is to maintain competitiveness and enable the business to operate more efficiently and effectively, an organization's security operations need to transform to stay competitive with the next generation of threats and maintain their ability to respond to them with speed and potency.

In order to run an effective and efficient Security Operations Center, an organization must:

1. **Be capable of ingesting, processing, and correlating large and disparate data sets from any source**
2. **Analyze that data at speed and scale to surface the potential threats that deserve attention**
3. **Establish robust and mature investigative processes that can be flexible enough to adapt to the dynamic environment, yet provide enough structure that an analyst can follow them**
4. **Maintain a modular orchestration and automation layer that can abstract the minutiae and highlight what is important**

Every(log), Everywhere, All at Once

The production and continuous use of new data is a trend that will only increase – and with the proliferation of connected devices – will do so at an exponential rate. Every time that data is used, or even viewed, there is also a log of that event (often times multiple logs from the various data sources in line between the user and that data). Now multiply that for every user and every piece of data being accessed across every instance of that data to understand the scale of the problem that Security Operation Centers face on a day-to-day basis.

What's more, consider the fact that organizations rarely homogenize on a single vendor across their tech stack. Other than a standardized structure of the log data, one vendor's logs are going to look completely different than another's, making the correlation of all this data over time a not-so-trivial task. The tools leveraged by a next generation SOC must provide a solution for these challenges and be able to do so at a speed and scale that can match the pace at which threat actors can move throughout an environment. **Thus, a log-source-agnostic common schema capable of ingesting logs from any source, via any method, and in as close to real time as possible is a critical foundation of a next generation SOC.**

A Stack of Needles

With all the logs in one place, 'search' becomes an invaluable function to security teams. When organizations are generating and ingesting logs on the scale of multiple terabytes per day, it is all too easy to get lost in a torrent of data whose relevance is yet undefined. Turning this log data into actionable and operational intelligence becomes a data analysis problem – one that is only solvable if the data arrives in a timely and consistent format. Once that data exists, is parsed, normalized, indexed, and ultimately quickly and easily searchable, what remains is a mountain of data from which teams must locate relevant, prioritized, and contextualized security information.

A "needle in a haystack" is an oft-repeated metaphor demonstrating the problem security operations teams face, but even that isn't quite accurate. The reality of investigating modern security threats is better defined as finding a *particular* needle in a stack of needles. Making sense of the noise and surfacing the security threats that truly matter in a timely fashion is a necessity of a next-generation SOC. The limited resources available must be spent responding to the right threat at the right time. This modern threat detection platform becomes the key to transforming the sheer volume of incoming log data to the *'who, what, when, where, and how'* needed to properly investigate—and make sense of—a security threat.

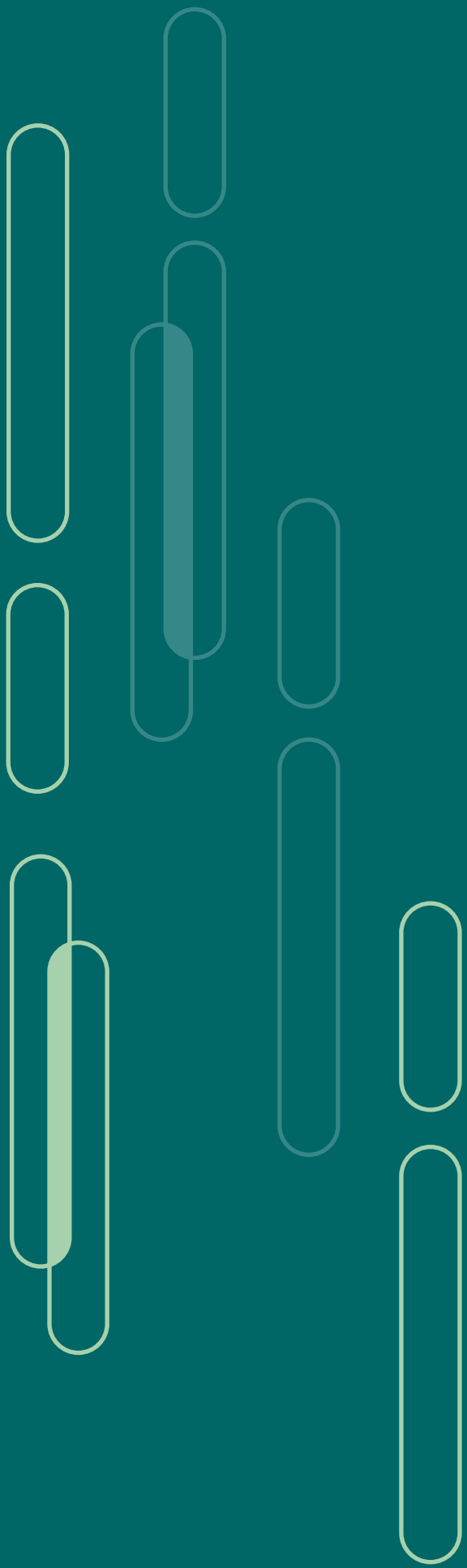
Investigating The Known Unknowns

A continued trend in breach reports is the not insignificant number of security incidents that occur as a direct result of misconfigurations or human error. As organizations continue to transform and embrace new technology to drive efficiencies and competitive advantages, that same technology can sometimes represent a radical shift in skillsets and knowledge to manage and operate – and the consequences of getting it wrong can mean showing up as a statistic in the next breach report. However, there is at least some encouraging data coming from those reports. Errors and misconfigurations have shown a downward and levelling-off trend as the cause of major breaches, so we know that we're doing *something* right. This can likely be attributed to the rapid training and knowledge development that has gone into these new technologies, both on the IT and security operations sides of the business.

For security, however, the work doesn't stop there. While properly securing the environment is the first step, security operations teams also have the added work of knowing how to detect, investigate, and respond to potential security concerns in lockstep with new technologies and organizational changes. In addition to (and possibly more important than) the training aspect is establishing mature and flexible investigative processes—capable of integrating with any source of data—that can abstract as much as possible for analysts so that they can focus on a defined process. Technology will always be changing. It's impossible to think that any one security analyst will know every intricate detail of how *Tool A* versus *Tool B* functions, or the level of log verbosity between *Vendor Y* and *Vendor Z*. But they can, however, be trained and guided to the point where the end goal of an investigation remains the same – to provide any and all relevant context about a security alert so that someone more familiar with the technology or business process can answer the

question: "Is this malicious behavior?" These processes and communication flows must have provisions to identify who that person or group is as well as the ability to request, collect, and action feedback to effectively close the loop on any security investigation.

Once a Security Operations Center has all of these things, their last and most concerning hurdle is **time.** In a game where success is determined by *seconds* and *minutes*—yet the most common reported measurement is in *days* and *months*—the SOC needs all the help it can get to reduce the time spent across all aspects of security operations.

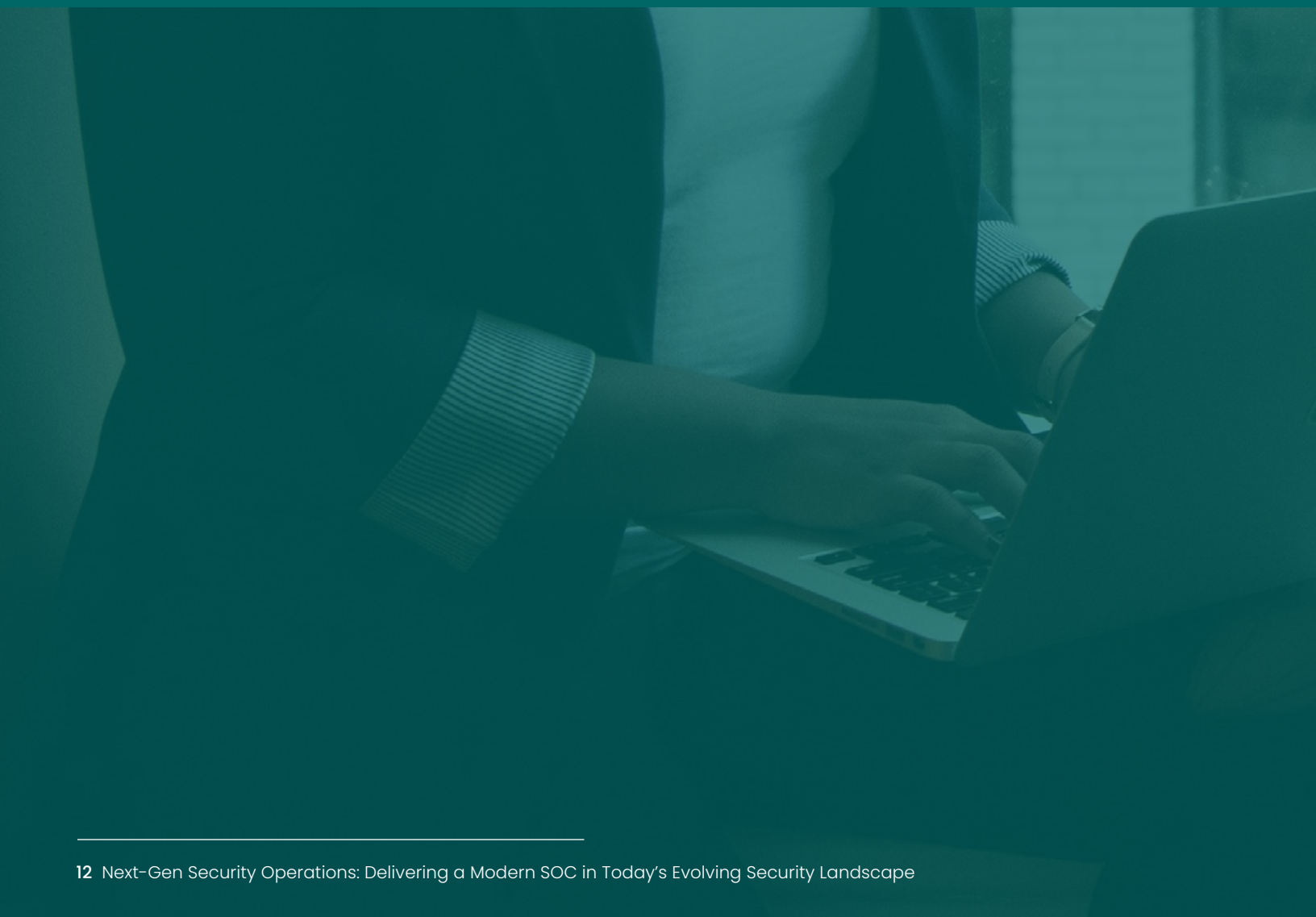


Playing By Different Rules

When working with security incidents, there is a direct (and unfortunate) correlation between the time it takes to respond and the direct and indirect costs that can be attributed to said incident. The longer a threat actor is in the environment, the more difficult, time-consuming, and resource-intensive it becomes to properly eradicate them, which ultimately leads to more damage caused by the threat actor. Security operations as a whole can be boiled down to a race between the operations team and the threat actor, but these races aren't held on a level playing field. The threat actor actively hides their activity to prevent being detected for as long as possible and throws as many obstacles as possible in the path of the security operations team to slow them down. If there is any hope in keeping up, the SOC must start finding and leveraging shortcuts of their own. In this case, that means orchestration and automation anywhere and everywhere possible. This requires solid processes in order for the automation to be effective (automating a bad process just gives you a bad outcome faster),

but when those processes do exist, detection, identification, response, feedback, and closure of security alerts can start being measured in seconds and minutes.

Thus, the commitment to automation must be relentless. Everything is a candidate for automation as long as the possible inputs and outputs can be defined and combined with what actions need to be taken. With that said, at some point within the automation and orchestration process, humans must be involved, typically at a particular decision point. 'Humans-in-the-loop' automation ensures that the collection and presentation of all pertinent information makes it to a security analyst who can then quickly make a decision and set an action—after which the automation takes over again to respond to the alert accordingly.



Milestones Along the SOC Journey

The task of the SOC is one that will never be simple or easy – even when embracing these tenets, security operations remain at a disadvantage given what they are up against. Fortunately, the principles outlined above function in a feedback loop of sorts, with each representing a milestone in the journey and reinforcing one another. The processes and technologies needed to support the identification and ingestion of data sources within an environment naturally enable teams to analyze that data and effectively detect security threats at scale. From there, the need to establish investigative processes capable of supporting both data source flexibility and guardrails for analysis paves the way for relentless automation. While there will always be novel attacks and new vulnerabilities identified, these tenets will put a security operations center in the best possible position to successfully keep pace with both threat actors and their own business as they continuously transform.

For more information on next-gen security operations, or to learn about AHEAD's Managed SOC, get in touch with us today.

Contributing Author:

Tyler Hopperton, Director, Managed Services Delivery

AHEAD

Combining cloud-native capabilities in software and data engineering with an unparalleled track record of modernizing infrastructure, we're uniquely positioned to help accelerate the promise of digital transformation.

National Hubs

ATLANTA
1117 Perimeter Center
W406
Atlanta, GA 30338

CHICAGO
401 Michigan Ave.
#3400
Chicago, IL 60611

SAN FRANCISCO
2000 Crow Canyon Place
Suite 250
San Ramon, CA 94583