FUTURUM. TECHNOLOGY INSIGHTS FOR BUSINESS LEADERS

HOW TO DESIGN YOUR SECURITY OPERATIONS CENTER (SOC) TO WORK SMARTER, NOT HARDER

June 2020

DANIEL NEWMAN
Founding Partner + Principal Analyst

SHELLY KRAMER
Founding Partner + Senior Analyst

IN PARTNERSHIP WITH

splunk>

Published: June 2020

TABLE OF CONTENTS

3 Introduction

4 Why Security Information and Event Management (SIEM)?

6 Why Security Orchestration Automation and Response (SOAR)?

7 User and Entity Behavior Analytics (UEBA)?

8 Optimization of the SOC

10 Why Consider a Vendor Neutral SIEM/SOAR Technology Platform

11 What to Look for in a SOC Portfolio

12 What Does the C-Suite Want (and Need) in a SOC?

13 Conclusion and Key Takeaways

INTRODUCTION

Today's Major Security Operations Center Challenges

In today's digital economy, data isn't just a means to create value, it has value itself. If banks were the target of the last century, data is the target of this century. The increasing use of tactics like social engineering and deep fakes, coupled with the ever-present threats of global warfare and infrastructure attacks endanger everything from email servers to our phones. Securing data in the 21st century requires a holistic approach to security operations that starts from the boardroom on down.

Transformational technologies have changed, and will continue to change, everything about the way we live and work. Adapting our security operations by integrating technology into how we identify and manage cybersecurity threats and challenges must be a key component of organizations' digital transformation shifts.

That's where security operations centers (SOCs) come in. SOCs are an integral part of organizations' efforts to combat cybersecurity threats and generally work separately from, but in conjunction with, IT operations. A SOC is a centralized, dedicated team of experts using a variety of tools to protect against threats. They identify system weaknesses proactively — detecting, analyzing and responding to threats in near real time.

IT security pros largely agree on the need for SOCs. In a 2019 study done by Ponemon Research on improving the effectiveness of security operations centers, survey respondents were asked: "How important is your organization's SOC to its overall cybersecurity strategy?" An overwhelming 67% of respondents spoke to the importance of a SOC, with 40% responding that a SOC is **Very Important**, and another 27% indicating that a SOC is **Essential**. While it's refreshing to see the high level of importance attributed by IT pros to cybersecurity and SOCs, we know from our work in the security sector that key security operations challenges exist.

Security operations (SecOps) leaders report their biggest challenges include:

- Overcoming resource-intensive issues to stay ahead of cyberthreats
- Detecting hidden, unknown threats with legacy tools that are often overly complex and unscalable
- Navigating an acute talent shortage, with little to no change in sight
- Optimizing SOCs that are built on disconnected, disparate systems (80% of SOCs today)
- Combatting shadow data (55% of data within most organizations is either dark, untapped or unknown)

In addition to the major challenges identified above, others exist. Organizations often lack the budget to replace legacy systems with more sophisticated technologies. Further challenges include SOC teams' lack of clarity about the mission of a SOC, challenges in selecting the right technology solutions, a lack of documented or scaleable processes, and team members who possess both the hard and soft skills needed for success.

In this white paper, we'll take a look at some of the key considerations for the design or improvement of an effective SOC, as well as how the role of a SOC team can be refocused for more effective operations and better data security. Data analytics and data-driven decisions are increasingly required to keep pace with new threats. We'll examine how legacy and manual processes can be automated, and the role that machine learning can play in freeing up scarce resources for higher-level tasks.

In short, when security operations centers can work at the speed of machines and allow your staff to work smarter, not harder — everybody wins.

WHY SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)?

When exploring how to make your security operations center work smarter, not harder, the process begins with a security information and event management (SIEM) platform. There are five key reasons that integrating a SIEM into business operations is essential. Workflow management:

- Helps to ease the skills gap
- Provides the ability to accelerate threat detection and response
- Allows organizations to leverage data generated by IT, business units, and security systems, including apps and devices (turning machine data into tangible business outcomes)
- Provides real-time security monitoring, advanced threat detection, incident investigation and incident response for optimized threat management (TM)
- Allows SOC teams to use purpose-designed frameworks and workflows and pre-built dashboards to streamline their TM operations

Workflow management and easing the skills gap. Most security operations teams must rely on an abundance of tools, having to constantly toggle between tabs and the constant flow of alerts. It takes a lot of brainpower for humans to accurately triage and handle inbound events. This requires a magic mix of technical skills, soft skills and creativity skills — which is often difficult, if not impossible to find.

At the Tier 1 level, security teams need basic security knowledge, solid networking expertise and an understanding of application layer protocols. They must also possess database and query language capabilities, coding/scripting ability, expertise in regulatory compliance, and be adept at troubleshooting, vulnerability scanning, and investigations.

At the Tier 2 level, security teams need an even greater depth of expertise, including an understanding of Unix and Windows, familiarity with basic parsing and command lines, experience with security monitoring tools, and troubleshooting capabilities. Individuals must possess the requisite security clearances, superior critical thinking skills, and excellent communication and writing skills.

Think those skills are easy to find? Think again. In the 2019/2020 Official Annual Cybersecurity Jobs Report published by Cybersecurity Ventures), it is predicted there will be 3.5 million unfilled cybersecurity jobs by 2021, up from one million in 2014. That's why optimizing Security Operations isn't a *'nice to have,'* or a *'we'll get to that at some point'* option — it's a business mission-critical one.

A SIEM allows for a managed, scalable workflow and concurrently provides a solution to the skills gap. We believe that by integrating a SIEM into security operations, it is possible to achieve the automation of upwards of 90% of Tier 1 analyst work, along with a reduction of almost 50% of team time spent on optimizing detection and response logic by the end of 2020.

Accelerate detection and response. At the enterprise level, there is a mountain of data generated on a daily basis. Managing that data is no easy task. Extracting key insights and leveraging that data is even more difficult. Today's threat levels are complicated and come at SOC teams from myriad directions at lightning speed. It's a challenge for humans, even highly skilled ones, to keep up with the speed and pace of today's threats. Automation can play a big role here, eliminating mundane, repetitive tasks and allowing your SecOps team to focus on more important things.

Leveraging data from throughout the organization. Deploying a cloud-based, unified security operations center is a game-changer. A SIEM takes all of an organization's event raw data — massive amounts of data generated by

IT, business units, security systems, as well as apps and devices in use throughout the organization, and synthesizes it to produce a higher set of fidelity alerts. A SIEM facilitates the detection, management, investigation, search, containment, and remediation of threats and other high-security issues. In some instances, these alerts will need to be reviewed by humans, and in other instances they can be handled by the technology solution, but overall, organizations can expect to see a rapid increase in their ability to detect and respond to security threats.

Monitor at the speed of business – in real time. Business is operating at warp speed and your security operations needs to keep pace. Integrating advanced analytics into the equation enables your SIEM to deliver your SOC and SecOps team a powerful assist, starting with managing and accessing network traffic and intrusion data. An SIEM provides endpoint protection, delivers threat intel and malware authentication, processes wire data, and analyzes assets and identities. As part of a SOC, an analytics-driven SIEM can monitor all security activity, correlate and sequence events, validate alerts and then prioritize, review, and investigate security instances, and can even decide the best path to resolution.

Workflows and dashboards make all the difference. A SOC is only as good as the information it provides. SOC teams must gain insights as well as visibility into network traffic data — and that's where workflows and dashboards make all the difference. Threat complexity, interoperability issues within other security tools, increased security team workload, and a lack of alignment with business needs and the support of senior leadership — which provide SOC funding — are all challenges SOC teams face. A SIEM platform that features easy-to-understand, scalable workflows and user-friendly dashboards unlocks data across all operations, empowering users to see what they need to see when they need to see it.

WHY SECURITY ORCHESTRATION AUTOMATION AND RESPONSE (SOAR)?

Threat detection is only one part of the equation — organizations also need smart incident response. For enterprises, the pairing of SIEM and security orchestration, automation and response (SOAR) is the true formula for success. Together, they allow teams to gain deeper insights and also shorten incident response times. Security teams can automate tasks and workflows — the entire SOC flows more efficiently.

A SOAR provides a foundational structure, documenting processes into playbooks that make it easy for SOC teams to know what actions to take. It becomes a uniform process across the organization. SOC team can also support a broad range of SOC critical functions like event and case management. Equally important, and probably the greatest value-add to a SIEM, is the fact that SOAR platforms unify the efforts all SOC team members. They bring people, processes and technology together, serving as the hub of security operations, and delivering a much-needed bird's eye view into daily SOC operations.

Let's go back to processing versus process. Your SIEM takes all of an organization's threat data, synthesizes it, and produces a higher set of fidelity alerts (aka processing). However, it's your SOAR capabilities that really allow your SOC to deliver value. Your user and behavior event analytics (UEBA, see below) capabilities help enhance threat visibility, accelerate investigation, and increase productivity. The key value proposition SOAR delivers is the integration of the SOC team's tools and processes. This allows the SOC team to:

- **Focus on security operations**
- **Focus on decisions that require human input**
- **Use machine learning to automate detection and accelerate playbook response times**
- **Ease integration with existing infrastructure**

If you have an SIEM, do you really need a SOAR within your security tools ecosystem?

Think about SIEM and SOAR like two different parts of the brain. Together, SIEM and SOAR are the security nerve center of your organization. Security automation improves the resilience and capability of your organization. If your goal is increased transparency for your SOC team, along with more effective, more efficient and more secure operations, that answer is a definitive yes.

If you have an SIEM,
do you really need a SOAR within
your security tools ecosystem?
FUTURUM.

USER AND ENTITY BEHAVIOR ANALYTICS (UEBA)?

Optimized security operations are where it's at. But SIEM/SOAR platforms aren't only capable of delivering rapid detection and response capabilities. Best-in-class SOC solutions should augment your SIEM with behavioral analytics powered by machine learning. User and entity behavior analytics (UEBA) uses machine learning to detect unknown threats and atypical user behavior. It looks for patterns that don't match established baselines and identifies potential security threats faster and more effectively than humans. Think processing malware email alerts in 40 seconds, versus 30 minutes or more.

I like to think of UEBA as the superhero of SOC operations, as these solutions often do their best work when everything else has failed. UEBA solutions aren't new, but surprisingly they are not gaining wider acceptance as the cybersecurity threat landscape expands, especially within the enterprise. Research from Gartner in mid-2019 showed that sales of standalone UEBA solutions are doubling YoY and were predicted to top $200 million by the end of 2019. In my opinion, best-in-class SOC solutions don't use a standalone UEBA offering, they integrate it. I believe that moving forward, we'll see fewer standalone solutions and more UEBA functionality incorporated into product offerings — it only makes sense.

The nitty gritty? UEBA can processes a variety of variables — things like network activity, application activity, login attempts, removeable media, badge scans, printer activity — comparing the variables with the baselines that have been set over time. These baseline activities include user activity, department activity, regional activity and company activity as a whole. This allows the UEBA solution to both know what normal behavior looks like, as well as to detect anomalous behavior that could indicate an insider threat or a compromise of user credentials. A UEBA can also correlate multiple anomalous activities that could be tied to a single security incident.

The beauty of an SIEM augmented with UEBA machine learning capabilities is that the system can not only enhance threat visibility by detecting unknown threats and unusual user behavior, but can also quickly evaluate and score threats, automating incident response. This helps accelerate investigation within the organization and drastically increases productivity of the SecOps team, compensating for resource or personnel shortages. Reducing the load on your SOC team frees them to focus on other, more important things, which benefits your whole organization.

In short, it's easy to see how a fully optimized SOC is worth its weight in gold. SIEM plus SOAR, and UEBA solutions that use advanced analytics, data enrichment, data science, AI and machine learning all wrapped up in one, easy to use platform is clearly the way to go.

OPTIMIZATION OF THE SOC

The success of any SOC is dependent on an enterprise's ability to carefully bring together security technologies, tools and talent with the devices, processes and applications it must protect. There are many choices when it comes to the framework or platform on which a SOC can be designed, as well as the how the SOC will be used or managed. We recommend that an organization should become "the boss of" their SOC. Everything you do, and every decision you make should be with a view toward an end situation where your SOC will work smarter, not harder.

Achieving this requires a proactive, not a reactive, SOC model. You'll want it to be plug-in ready and have critical automation and machine learning tools, along with robust analytics. A single suite SOC that integrates third-party solutions, minimizes user uncertainties, support calls, and work interference is crucial.

The ten essential capabilities we believe any SOC must deliver are as follows:

Ingest. At its most basic level, a SOC must have the ability to ingest massive amounts of data from myriad sources (data sources and volume will only continue to grow).

Detect. A SOC must have the ability to detect threats and anomalous behavior or instances across a wide range of data sets.

Predict. A SOC is in the business of continuous, proactive monitoring, analyzing and overseeing the security systems of an organization around the clock. Its ability to predict system weaknesses or threat instances in a proactive, rather than a reactive manner is an essential component in evaluating the overall efficacy of a SOC. The better a SOC is at predicting, the more effective it will be overall.

Automate. Automation in a SOC is no different than the use of automation elsewhere in the enterprise operating at the speed of light (which is every enterprise). The best strategy is to automate, automate, automate wherever possible. This reduces workload on staff and helps compensate for both resource and personnel shortages.

Orchestrate. A best-in-class SOC will orchestrate incident response, giving analysts information they need quickly, empowering them to make the right decisions and drive automated responses where applicable. Effective orchestration is an ongoing process to respond to

incidents, while also monitoring and learning from the response itself — improving ongoing and future responses. This could include the automation of workflow actions, like resetting credentials and patch application, updating firewalls or rules within the SIEM processes.

Recommend, recover, remediate. SOCs can (and should) recommend action based on data, threat analysis and user behavior data. Moreover, following an incident, the SOC should work to restore systems and recover any lost or compromised data, always with a view of returning the network to its optimum operating state, pre-incident.

Investigate. The aim of a SOC is to protect from security breaches by identifying, analyzing and reacting to cybersecurity threats. Following an incident, it is the job of the SOC to trace problems to their source, figure out what happened and why, so as to prevent recurrence.

Collaborate. A SOC should be a hub, a command post and a correlation point for every security event within an organization. The best SOCs bring people, processes and technology together, facilitating collaboration between security and IT operations teams, as well as others within the organization.

Manage cases. Effective case management is a game-changer for security operations centers. When SOCs can effectively manage case backlog, provide incidence response in a timely manner, and also meet the needs of the organization, it's a beautiful thing. An optimized SOC can provide automated alert grouping case creation, case assignment recommendations, case prioritization, and integrated crisis management.

Report. SOC reporting provides insight and stakeholder assurance, both internal and external, and proactively addresses risk across the organization. This is especially significant for enterprises governed by compliance regulations like HIPAA, PCI DSS, GDPR, CCPA, and others. SOC reporting can reduce compliance costs and time spent on audits, help ensure the organization meets contractual obligations, proactively address risk, and even help increase trust and transparency within the organization.

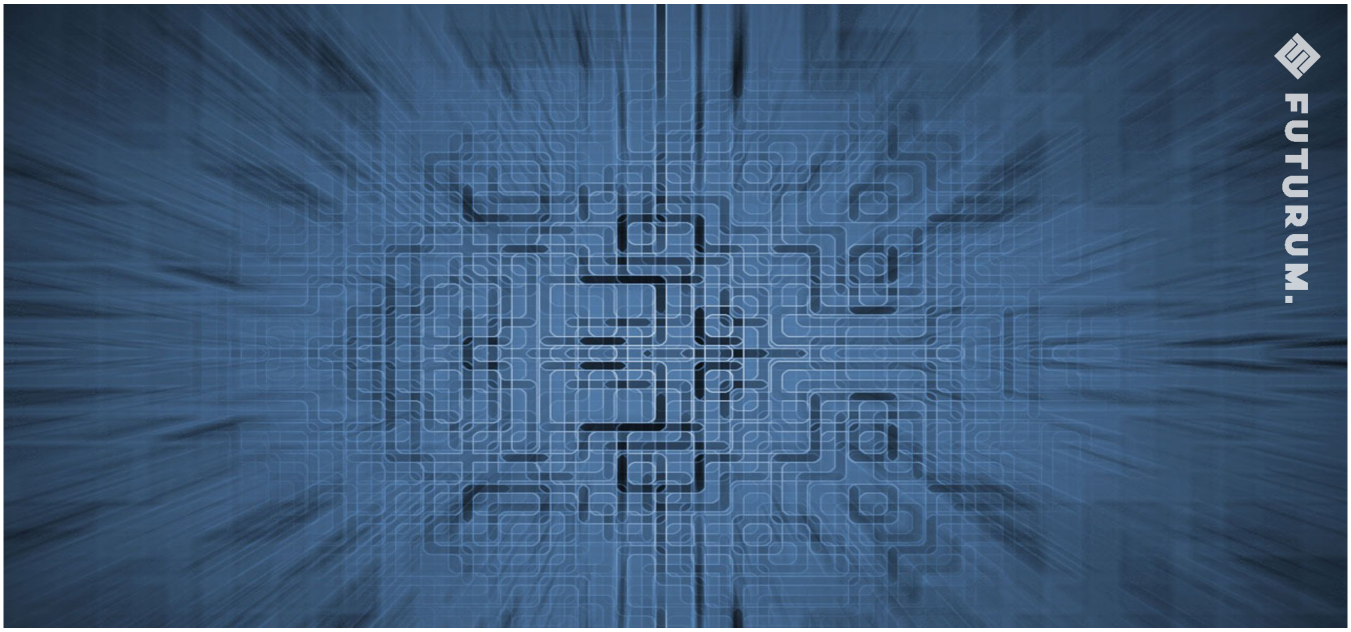
WHY CONSIDER A VENDOR NEUTRAL SIEM/SOAR TECHNOLOGY PLATFORM

Choosing the right security platform and tools is not an easy task, made all the more difficult by an array of options and the challenges of integrating the new with the existing. Start with the basics: On average, security teams have some 25 or more tools they use in a SOC, so opting for a solution that aligns with the most commonly used security tools is important.

A solution that has a strong partner ecosystem is also important, but perhaps even more of a value add is a technology solution that is vendor agnostic. A vendor shouldn't care where my data comes from. Wherever that is, they can help me make use of it — making that technology purchase decision much less anxiety producing. When you go that route — with a vendor agnostic solution provider — it's possible for vendors who are experts in their domain to coexist in one ecosystem with no friction. It also prevents proprietary "traps" — getting stuck with a vendor and a product that you don't love, yet are forced to use.

Setting up a SOC can be a challenge, particularly when it comes to putting in place the processes and data flows required to capture, ingest and analyze data from endpoints across the enterprise, as well as the data storage systems within the enterprise. While there are many tools on the market, and more being released every day, not all tools are the best fit, nor do the best tools always fit right. For many, the least expected challenge is found in change management — pulling together all the pieces, configurations and implementation processes required to get from A to B successfully.

When you work with a vendor agnostic solution offering, you can avoid brand tunnel vision getting in the way. What is brand tunnel vision? Solution vendors are going to promote their offerings first, in fact most are, because it only makes sense. So, while there might be a better solution for what it is you need in setting up your SOC, it's possible to get stuck using something that isn't necessarily the best solution, but it's the best solution the vendor can offer. Best for you? Perhaps not. Best for them? Definitely.



WHAT TO LOOK FOR IN A SOC PORTFOLIO

What do organizations look for in a SOC portfolio? That's easy. They look for volume, speed and flexible analytics. As is true in so many cases, it's usually a smart bet to go with what tech champions love.

As I touched on a moment ago, data is the fuel that powers your SOC operations. A solution must have the ability to ingest any data from any source at any time — and at any volume. Volume is the differentiator. The ability to deliver on speed and performance is also important. You'll find some vendors can deliver on speed and performance and others can't.

Look for analytics that are designed to feature usability and flexibility. For example, think "Google for all your internal data" and a user interface that is simple to use.

Lastly, I always look for solutions — any tech solutions — that technical champions love. They know what they need, and they know what they need it to do. When a SOC solution satisfies tech gurus and covers the things they worry most about, that's a solution worth strongly considering.

WHAT DOES THE C-SUITE WANT (AND NEED) IN A SOC?

Truly great leaders generally realize that they don't know what they don't know — and they're always willing to learn. That is nowhere more true than as it relates to cybersecurity and what the C-Suite wants, and needs, in a SOC solution. Let's start with price – flexible pricing options are incredibly attractive to the C-Suite.

The traditional pricing model is fairly basic: However much data you ingest, that's what you pay for. What we are seeing today is more flexibility being built into SOC solution pricing, and I'm a fan. For instance, in an infrastructure-based pricing model, which is more cloud friendly, you only pay for however many BCPUs you dedicate toward the system. There's also a predictive pricing model, for users with only one application (think monitoring ops on a manufacturing floor, where you only want it for that one, discrete app). Bottom line, when it comes to SOC solution offerings, explore pricing options before making a decision, because chances are good that you'll be surprised by what is available.

Our conversations with senior leaders show that the C-Suite understands the value of being able to work across multiple domains. Think about an organization's typical data — for instance printer logs — that can be used as part of the company's threat detection operations. And when the data platform that's the foundation of the SOC can be used not only in security, but also across any domain in the enterprise (e.g. app development, DevOps, infrastructure monitoring, IoT apps, etc.), it's a significant value add. For leaders, it's clear that multiple domain vision boosts risk mitigation, efficiency and visibility, and brings a new mindset that is silo-free to the equation. Smart leaders realize the value of a silo-free value proposition.

Cloud capabilities are also of interest to the C-Suite, as operating in the cloud can help ease expensive data ingestion costs.

C-Suite leaders evaluating SOC solutions look for:

- **Flexible pricing**
- **Multi-domain vision that boosts mitigation**
- **Cloud capability**
- **Data integration into the SOC framework**

CONCLUSION AND KEY TAKEAWAYS

In order for SOCs to work smarter and not harder, organizations need to understand the challenges their security team faces and prioritize budget allocations for security operations. It's important to move from a legacy-focus of yesterday to a data-driven and data-to-everything-and-everyone focus that's needed today.

Organizations must shift from a SOC that is characterized by situational awareness, operation and monitoring, human-driven responses, and human speed operations — that is yesterday's SOC model. It's not going to cut it in the age of rapid digital transformation. Today's best-in-class SOCs — and your security teams who use them — require a command center that is easy to access and easy to use.

Modern SOCs need:

- A decision-making process driven by data and analysis
- Human intelligence augmented by machine learning
- Machine-speed actions for real-time protection

Adopting a modern SOC will allow greater productivity for SOC personnel, freeing them to focus on more important SecOps needs.

There are two key takeaways to keep in mind: (1) Security must align with business outcomes and (2) SOC technology solutions must serve as both a cybersecurity and risk mitigation resource, as well as a solution to the resource and skills scarcity that most, if not all, organizations are currently dealing with.

SOC centers are quickly evolving to become more agile in order to both support the business and enable new initiatives, while also mitigating risk.

We have been evaluating Splunk, the Data-to-Everything Platform, and this white paper is sponsored by Splunk. Splunk technology is designed to investigate, monitor, analyze and act on data at any scale, from any source, over any time period, helping companies and their IT and SOCs teams more rapidly and effectively identify and mitigate risk, improve service levels, and reduce operational costs.

Security alignment with business objectives
Earlier in this white paper we cited research illustrating the importance that IT security practitioners placed on SOCs in relation to overall cybersecurity strategy. The research agreed on the importance of a SOC for effective cybersecurity operations (cited by 27% as Essential, 40% as Very Important, and 19% as Important). The research cited common concerns that could severely limit the effectiveness of SOCs, ranging from gaps in business alignment to the lack of visibility into IT security infrastructures and network traffic. Faced with ongoing interoperability challenges and a lack of internal expertise and resources, the importance of SOCs is equaled only by the challenges faced by today's enterprise security professionals.

A quick glance at this continuously updated data visualization of the World's Data Breaches and Hacks should serve as a wake-up call. The average cost of a data breach as reported by Ponemon Institute's annual report is $3.92 million, a 1.5 percent increase from the 2018 study. Our own studies and enterprise engagements here at Futurum Research back this up. We consistently have IT and business leaders citing improved security and the ability to mitigate the business risk of cyberattacks atop their list of mission-critical goals and objectives.

Enterprise security is important. IT leaders and cybersecurity leaders must have the support of senior management, and they must work together to ensure alignment of security with business outcomes. When powered by data, dashboards provide visibility and SOC interconnectivity.

We recommend using the power of data to illustrate how a well-designed SOC can not only deliver enhanced security and risk mitigation, but also enable and support new business operations. When you can help leaders understand the value of something they didn't realize they needed, they will discover hidden benefits and unlock business potential.

A SOC can help solve security resource and skills scarcity. SOC solutions can also play an important role in providing a very real solution to skills scarcity issues that plague virtually every organization. Attracting tech talent can be hard — retaining that talent is often even more difficult.

A well-designed SOC can minimize the instance of false alerts, tap into the power of automation and orchestration, and remove mundane, repeatable tasks from the equation. This allows your teams to focus on things they are really interested in, often leading to their best work.

When you approach the conversation about how to design your SOC to work smarter and not harder, whether you're optimizing your current system or exploring creating your first SOC, I urge you to consider these two key takeaways. And as you explore technology solutions, it is worth your time to consider the key differentiators that the [Data-to-Everything Platform] affords.

Attracting tech talent can be hard — retaining that talent is often even more difficult.

IMPORTANT INFORMATION ABOUT THIS PAPER

CONTRIBUTORS:
Daniel Newman
Founding Partner + Principal Analyst, Futurum Research

Shelly Kramer
Founding Partner + Senior Analyst, Futurum Research

PUBLISHERS:
Daniel Newman
Founding Partner + Principal Analyst, Futurum Research

Shelly Kramer
Founding Partner + Senior Analyst, Futurum Research

INQUIRIES: Contact us if you would like to discuss this report and Futurum Research will respond promptly.

CITATIONS: This paper can be cited by accredited press and analysts, but must be cited in-context, displaying author's name, author's title, and "Futurum Research." Non-press and non-analysts must receive prior written permission by Futurum Research for any citations.

LICENSING: This document, including any supporting materials, is owned by Futurum Research. This publication may not be reproduced, distributed, or shared in any form without the prior written permission of Futurum Research.

DISCLOSURES: This paper was commissioned by Splunk. Futurum Research provides research, analysis, advising, and consulting to many high-tech companies, including those mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

ABOUT SPLUNK
Splunk is the world's first Data-to-Everything Platform. Now organizations no longer need to worry about where their data is coming from, and they are free to focus on the business outcomes that can deliver. Innovators in IT, Security, IoT and business operations can now get a complete view of their business in real time, turn data into business outcomes, and embrace technologies that prepare them for a data-driven future.

ABOUT FUTURUM RESEARCH
Futurum is an independent research, analysis, andadvisory firm, focused on digital innovation and market-disrupting technologies and trends. Every day our analysts, researchers, and advisors help business leaders from around the world anticipate tectonic shifts in their industries and leverage disruptive innovation to either gain or maintain a competitive advantage in their markets.

DISCLAIMER: The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. Futurum Research disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of Futurum Research and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Futurum Research provides forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.

CONTACT INFORMATION

Futurum Research, LLC I futurumresearch.com I 817-480-3038 I info@futurumresearch.com

Twitter: @FuturumResearch