Deloitte. | Google Cloud

FUTURE OF THE SOC

FORCES SHAPING MODERN SECURITY OPERATIONS

Introduction

Conversation about the ways to make threat detection more effective—the daily bread of Security Operations Centers (SOCs)—goes back to the dawn of the internet. Is it better to identify badness by signatures or through profiling? Automation is the most common way to scale, but is it as effective at finding malicious acts as a manual investigation by specialists? There are too many tools and, over the years, numerous attempts to consolidate visibility into a "single pane of glass" have failed. The late 1980s witnessed the first prototypes of anomaly-based intrusion detection; 1990s—the first automation of response. Then the first SIEM (Security Information and Event Management) products born in the late 90s loudly promised to solve Intrusion Detection System (IDS) alert overload and the dreaded "false positives."

Today these same problems are trying to be solved—fatigue from high rates of false positives, too much data, too many alerts—without noticing that the landscape has shifted in profound ways. Problems are conceptualized and solutions are developed...but by the time those solutions are implemented at scale, the problems they're trying to address are no longer the same.

Solutions envisioned in the 1980s, 1990s, and 2000s would have turned out productive had the problems remained static. But here's the rub: **the junior SOC workforce is taught to apply the same analytical techniques as in the days when weekly log reports were manually scrubbed and logs were measured in megabytes.**

What has changed is more fundamental than the entrance of cloud technology. It's the role of technology in fighting the falling rate of profit. Simply put, while technology in the 20th century helped automate repeatable tasks, the role of technology in the 21st century focuses on the automation of repeatable cognitive processes, in other words—of decisions. Otherwise, automation would take care of the routine tasks, but the amount of non-routine tasks—those that require thinking—would still overwhelm the available human analysts. It is business imperative to make the right decision faster than the competitor.

Data lakes, artificial intelligence (AI), machine learning (ML), big data analytics, cloud and edge computing, Internet of Things (IoT)—you can complete the tech buzzword bingo—are all functions of that imperative, which has led to the exponential growth of attack surface. **In the race for data collection analysis and decisioning, this growth will continue at pace or more likely accelerate in the coming years.**

Let's explore how this context, or awareness, further manifests into the primary "forces" that are driving the need to change the approach to threat management and SOC operation.

This paper defines "forces" as key salient factors that are shaping the modern challenges a SOC must overcome to continuously mature:

- **Expanding attack surface**
- **Security talent shortage**
- **Too many alerts from too many tools**

Chronicle

Force 1: Expanding attack surface

Organizations are rapidly shifting their business models and corresponding technology environments to compete with one another in the digital transformation era. Enterprise data previously held under lock and key is now being shared across multiple business units, partners, and external vendors to meet increasingly agile business needs.

These trends have shifted cyber risk to a collective "ownership of many" security model, with organizations integrating various digital identities to support a highly innovative workforce and data-driven business model.

CLIENT CASE STUDY

New York City Cyber Command (NYC)

To help protect city systems from cyber threats, NYC Cyber Command works with city agencies to ensure systems are designed, built, and operated in a highly secure manner. If any of these systems were compromised and the city's ability to provide critical services—such as public assistance or health care—were impacted, the consequences could be catastrophic for the most vulnerable New Yorkers.

That is why, in addition to enhancing the security of city systems, NYC Cyber Command developed a highly secure, resilient, and scalable cloud infrastructure that helps its cybersecurity experts detect and mitigate threats faster.

In order to support technologies across New York City government, NYC Cyber Command followed a cloud-first strategy using Google Cloud, infrastructure as code, and a BeyondCorp security model that builds upon years of designing zero trust networking.

NYC Cyber Command uses an open source platform and provider-agnostic infrastructure as code tool to help ensure the services are delivered reliably and securely, and the civil servants build knowledge and skills that can be used throughout the city's technology enterprise.

"We went with a cloud-first, zero-trust environment because it met our security and reliability needs," says Colin Ahern, Deputy CISO for Security Sciences at NYC Cyber Command. "Our role is not only to deliver services to residents, but to innovate in the way we provide those services to make sure we are efficient and effective."

New developments in sensing, cloud computing, and analytical technology have empowered businesses to accelerate feedback loops from the marketplace, and make decisions within shorter cycles.

The complexity of new sensing technologies exponentially increases as legacy information technology (IT) infrastructure is integrated into new analytics strategies that rely on emerging technologies. **In essence, many traditional organizations have to secure the past (e.g., mainframes), the present (e.g., servers, PCs, phones) and the future (e.g., containers, serverless, IoT).**

As enterprises gain more business insights into their data, cyber adversaries are presented with a multitude of new opportunities to exploit the expanding attack surface. Their tactics, techniques, and procedures (TTPs) are shifting to keep pace with these major technology shifts. Nowadays, organizations must defend against botnets conducting Denial of Service attacks via IoT devices, cyber criminals offering Ransomware as a Service (RaaS), and increasingly convincing phishing exploits.

Today's SOCs are facing complexity on two fronts: the sprawling technology landscapes and a proliferation of threats seeking to take advantage of it. Initial approaches simply ingested as many logs as possible to create more searches, and thus more actionable alerts for SOC analysts. Simple right? Experience, however, has shown us that more logs does not equal more security and can actually hinder analysts when provided without actionable context. Basic correlation alerts (while a great fundamental stepping stone in a SOC's maturity) are also not enough.

As their capabilities mature, SOCs will need to confront their sprawling technology landscape. Successful organizations should focus on several themes to address their ever expanding attack surface:

- Close collaboration between the SOC and overall business operations. Cyber must be seen as an enabler for the business and not just a cost center. **Directly addressing business problems and providing concrete examples of actionable resilient solutions can go a long way in proving the SOC's ROI to management.**

- Develop a robust data pipeline capable of ingesting and normalizing petabytes of data at scale. **SOCs should architect their underlying infrastructure with the appropriate speed and scale to process high volumes of data from a diverse set of security devices, while remaining vendor agnostic.** This desired flexibility has caused many organizations to consider major cloud providers due to their ability to automatically provision resources on demand and vast integration capabilities with major security vendors.

- Identify opportunities to incorporate AI and ML to develop anomaly-based alerting. **As organizations continue to rapidly expand, SOCs should consider AI/ML to accelerate their understanding of what constitutes "unusual behavior" throughout their different enterprise technology stacks.** AI/ML models, when applied correctly and ethically, can serve as accelerators for foundational baseline monitoring and empower analysts to investigate more meaningful events.

The attack surface of organizations will inevitably continue to expand as technologies further empower businesses. The modern day SOC must empower its analysts to derive value from its various security functions, while increasing their efficiency through collaboration.

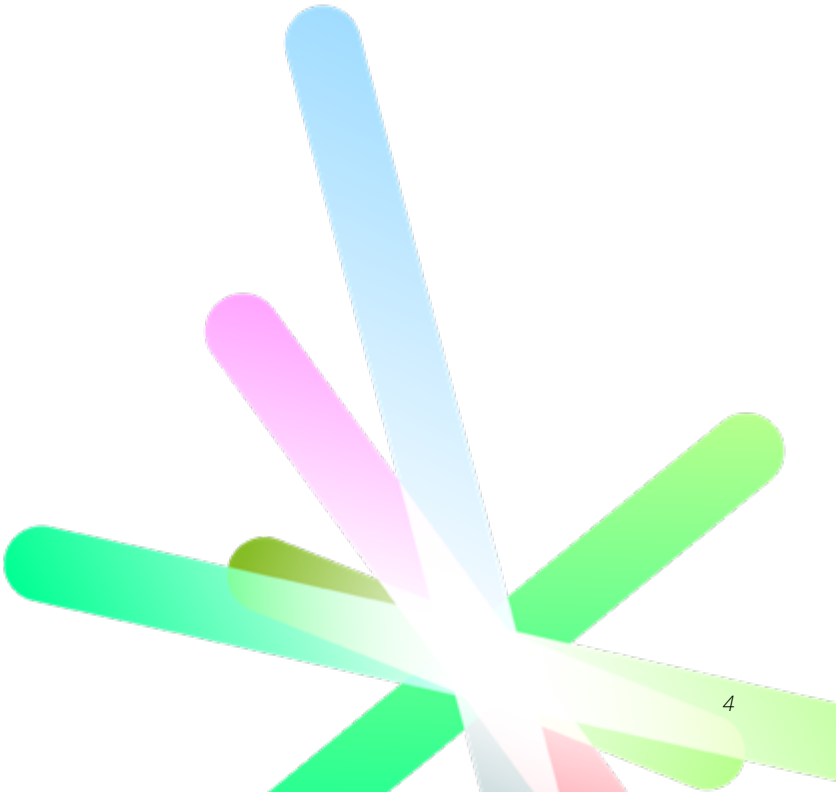
Force 2: Security talent shortage

There is still lots of work to be done for cybersecurity—and specifically for SOC operations—as a community, and as individual organizations, to solve some of the problems outlined above. The number of folks—however—who have the vision, experience, and skills to address them is not growing nearly fast enough. A massive and growing talent shortfall is one of the most critical challenges facing the cybersecurity world today.

In fact, nowhere in IT is the talent shortage more pronounced than in the cyber arena. A 2019 workforce study by (ISC)2 estimated the number of unfilled cyber roles globally at four million[1]. The study also found that the number rose by over one million in just a single year. This skills gap is dire in every geographic region and industry, and impacts organizations of all sizes. And industry trends indicate the majority of CISOs and security practitioners don't see the problem getting any better. **Zooming into the talent shortage problem more specifically within the SOC, the SANS 2019 SOC Survey found that the most frequently cited barriers to excellence were a lack of skilled staff followed by absence of effective orchestration and automation.[2]** In some locations, there is simply no way to find more people, even if you pay more than generous salaries.

Looking at the demand side of cyber talent scarcity, there are numerous drivers and signals that explain the need for more jobs. Some of the ones already discussed are the expansion of IT infrastructure, digital commerce, mobility, cloud, and en masse digitization of identities - all of which have exploded the threat attack surface as well as the incentives fo cybercrime. And the rising cost per incident is too widely reported to even bother defending with another redundant statistic. And the rising cost per incident is too widely reported to even bother defending with another redundant statistic. **Within the SOC, a more direct challenge is seen in the onboarding and training period for Level 1 analysts, which lasts almost a year, but leads to an average tenure of only about two years[2] - a low return on investment.** Those ground truths alone explain much of the spike in demand for cyber solutions and cyber talent.

Now flip the lens to the supply side view of the cyber workforce crisis. Cybersecurity vendors have responded by flooding the market with more security tools, each with specialized areas of focus. But this has simply compounded the labor scarcity challenge. More security tools = more alerts that have to be triaged. The growing specialization of security solutions drives a corresponding need for more security personnel, as well as more specialization in cybersecurity roles. Partly in response to talent shortages and the need for specialization, SOCs have settled on a two or three-tier structure for analysts with the entry Level 1 tier typically being the largest and often outsourced. Specialization tends to reside in the hands of a smaller and bandwidth-constrained group of more expensive and harder to hire and retain Level 2 and 3 analysts. Post triage, IR (incident response) teams take over to execute containment and further investigation. This team, in particular, has to have a high level of familiarity with the growing number of security tools as well as the underlying infrastructure to orchestrate remediation steps. Those associated training costs drive up overall SOC and talent retention costs.



1. (ISC)2 Cybersecurity Workforce Study. (2019). Strategies for Building and Growing Strong Cybersecurity Teams. https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx

2. Crowley, C. & Pescatore, J (2019). Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey. Sans. http://assets.extrahop.com/whitepapers/Survey_SOC-2019_ExtraHop.pdf

CLIENT CASE STUDIES

1

A US-based health care sector market leader was contending with constantly growing security telemetry volumes, more alerts, and analyst burnout. In the organization's two-tier structure, the smaller subset of Level 2 analysts had to take on a disproportionate number of cases. Meanwhile, Level 1 analysts were underutilized. High volume threats like phishing still required investigations to be conducted entirely by a limited number of Level 2 resources.

The security team evaluated existing market leaders and emerging technologies based on architectural, economic, and functional criteria. The organization selected a Software-as-a-Service (SaaS)-based security analytics platform that offered a predictable, fixed pricing model; curated threat investigation and hunting workflows; and searched through petabytes of data with sub-second latency. As a result, they were able to shift entire categories of threats into the hands of Level 1 analysts, while also limiting TTI (time to investigate) on phishing incidents to under 15 minutes.

2

A US-based manufacturing firm was contending with constantly growing security telemetry volumes, more alerts, and low analyst retention due to burnout. The firm's leadership decided to engage a Managed Security Service Provider (MSSP) to take on routine tasks. They conducted market research to identify an MSSP with experience to address both traditional IT and Operational Technology (OT) threats.

The firm also leaned in on the selected MSSP to upskill the existing team—the Level 1 analysts who were now freed up to conduct higher-level cognitive work. The hands-on training program included conducting threat hunts together—initially with the MSSP in the lead role, and then supporting the analysts as they gained confidence and experience. This approach enabled the MSSP to gain a better understanding of the environment early on in the engagement, resulting in a significantly lower rate of false positive alerts.

Vendors also have to do more to improve the quality of detection capabilities and reduce false positive rates, while organizations and SOC teams have to do more to implement and invest in automation. Without that, SOC teams—already stretched and overworked—will likely continue to experience burnout. Outsourcing security operations to managed service providers has provided added bandwidth to triage the high volume of low fidelity noisy alerts. But the problem of advanced threats going unseen remains (and can't be fully tackled) by a sub-group of hard to find and hard to retain human resources.

While computer-related degrees and continuing practical IT education have been around for a long time, cybersecurity degrees and education have not kept pace. Unfortunately, training more IT workers and cybersecurity practitioners alone won't be enough to fill the talent gap that exists today. The reality is that every information worker, across all business functions, needs ongoing cybersecurity training in today's world. **Yet, cybersecurity awareness in non-IT roles is severely lacking and a large reason why phishing attacks continue to account for over 30 percent of breaches (according to Verizon's 2019 Data Breach Investigations Report).[3]**

The cyber talent gap problem isn't going away anytime soon, but expanding the ground level workforce entering the market each year can help in the long run. This can be achieved with partnerships between corporations and educational institutions that help develop technical cyber security skills as part of their curriculum and further address the supply side of the equation.

Meanwhile, organizations should invest in greater automation, better detection technologies, industry-level intelligence sharing (collaboration), and greater organization-wide (top down) cybersecurity awareness and focus.

3. Verizon Enterprise. (2019). 2019 Data Breach Investigations Report. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

Force 3: Too many alerts from too many tools

Security today seems to live in the age of "more"—more IT assets to secure, more telemetry data, more security tools, more alerts, and of course, more threats.

All of those affect the SOC, overwhelming it with signals. Years ago, this problem was widely presented as "too many false alerts"—the dreaded false positives. Today, a SOC may be overwhelmed with signals in general: some false, some true but hard to contextualize, and some merely informational. Naturally, an increase of IT assets and coverage of assets by security monitoring and new security tool types all lead to more signals.

For example, in some breaches, a company's security team failed to take action after detecting potentially malicious activity. They had been receiving hundreds of alerts every day that were mistakenly dismissed as false—but were, in fact, real. At other organizations, SOC analysts may be discarding real alerts as false for many other reasons. In their quest to reduce false positives and maintain a manageable queue, alerts are quickly tuned down to reduce noise, while some of that "noise" may actually be an early indication of the intrusion.

In fact, recent fascination with machine learning for threat detection added a new category of signals — mathematically anomalous but operationally irrelevant—on top of many SOCs work queues. While not technically false, they are of no help to the overstretched SOC analysts and often require elaborate triage activities to validate. For example, a new user logging in several times to a new system late at night may indicate business activities that are only performed at the end of quarter, and are anomalous for a system that looks at 30 days of profiling data. Similarly, a sudden flood of failed logins may indicate an automated process that was misconfigured to connect to the wrong system—an operational issue, but not a threat.

Even the existing security tools—from firewalls to EDR (Endpoint Detection and Response) to CASB (Cloud Access Security Broker)—generally deliver more telemetry. Big data analytics is growing in importance and today the customer is the one paying for it. Hadoop and other scalable data storage—whether on-premise or in the cloud—often comes with a large cost, whether for the tools themselves, for hardware, or for cloud computing resources.

This increase of data leads to a paradox: there are too many alerts, yet not enough useful alerts from all the data being collected. On top of this, advanced threats may in fact not trigger the alerts at all, or until the very last stage of their attack - data exfiltration. Then, add in poorly-formed alerts, whether ML-derived or rule-based, which overwhelm human analysts. Fragile, context-less alerts that are hard to triage may contribute to the frustration of SOC analysts, leading to faster burnout, and ultimately to more missed important security indications. In reality, a single alert very rarely represents a smoking gun; but more often than not, a thread to pull (by a human) that reveals a smoking gun. On the other hand, relying on junior analysts to handle the increasing alert volumes alone won't work. No organization can hire faster than the growth of technologies and threats.

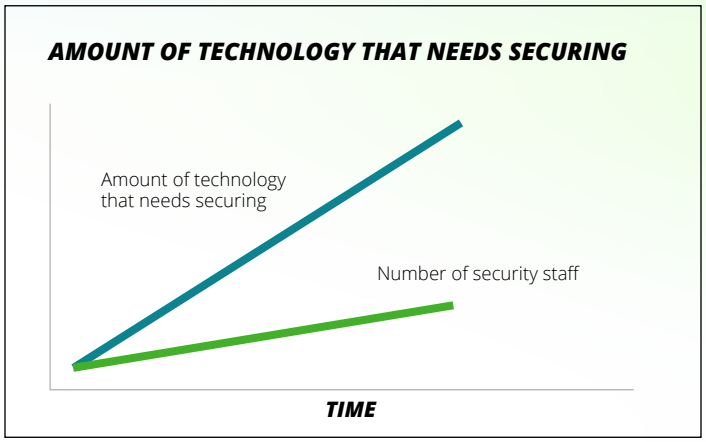


Figure 1: There is a growing risk of dedicated security staff not keeping pace with the ever expanding enterprise IT footprint that requires monitoring (Source: Google Cloud)

Humans cannot scale to cover all alerts, but machines (such as ML algorithms) on their own just don't cut it. As the SOC increases in maturity, the solution to the problem of too much of everything may come from many sources:

- Humans are—and will be—needed to both perform final triage on the most obtuse security signals (similar to conventional SOC Level 3+) and to conduct a form of threat hunting (i.e. looking for what didn't trigger that alert)
- Machines will be needed to deliver better data to humans, both in a more organized form (stories made of alerts) and in improved quality detections using rules and algorithms—all while covering more emerging IT environments
- Both humans and machines will need to work together on mixed manual and automated workflows such as those enabled by SOAR (Security Orchestration, Automation, and Response) tools today

The future thus will rely on humans powered by automation, not only for enriching the data but also for making better, quicker decisions with regard to observed security signals.

How should SOCs evolve?

So, how can existing SOCs prepare for the future and new ones be built for the future? The forces discussed in this paper affect the operations of today's SOC. These forces also run a risk of reducing the SOC's effectiveness over time or even overwhelming some SOCs entirely.

What needs to be done and what can be done realistically? While many will say automation is the answer, SOC automation today is predominantly focused on automating the routine tasks (enriching logs with context and threat intel), as well as automating some remediating actions (with the decisions to do so largely remaining in human hands).

Indeed, the 20th century brought task automation, which is essentially an industrial revolution of "alert manufacturing". It was meant to relieve humans from mundane tasks like looking up an indicator on numerous websites and internal repositories. And you know what? It actually did—at least for SOCs with highly mature and automated processes. However, people at such SOCs are still overwhelmed.

The 21st century must conquer the next frontier for automation—automating the decisions and some of the related cognitive processes. While some vendors already promise that today, the operational reality of today's SOC does not support this claim.

Therefore, relief can come from the next level of automation—that of decisions—and of humans maintaining their focus on the hardest tasks.

What can be done today to make it real? Evolve SOC people, processes, and technologies. But how?

Use intelligent tools to empower collective decision making

Most companies have too many tools and often these tools are not utilized to their full capability. Still, technology needs to ingest large disparate data types as traditional SIEMs struggle to handle it well. To enable hunting, such telemetry needs to be correlated and alerted in more than just basic rule correlations. A lot more threat intelligence is needed—tools that make use of intelligence to easily make security decisions and tools that are closer to the potentially impacted technology to make a narrower, and hence, more reliable set of decisions. Finally, tools like SOAR that unify and organize other tools to form a higher-order intelligent collective emerge as a central need in the SOC, alongside SIEM and other telemetry analysis tools.

Design, implement, and automate tested and proven processes

A good SOC implements a well-organized process that works, but also does not suppress the creativity of its analysts. Strong technology processes already exist; however, SOAR and analytics are paving the way for automation in decisions - not tasks. Ultimately, it is very hard to automate a process you don't actually have yet. While SOAR allows for processes to be consistent and fast, those processes need to exist and be defined first. Later, one can insert more decision automation where simple cognitive processes, first undertaken by humans, have proven to be correct over time.

Form an ecosystem of smart people within and outside of your organization

Let's face it: your SOC will never be able to hire enough people. It is time to accept that. What does this mean for the people aspect of your SOC? This likely means that almost every SOC of the future is a hybrid model that works together with service providers—be it your MDR (Managed Detection and Response), co-managed SIEM, managed EDR, or a full-on MSSP. Another piece of good news is that as more decisions are shifted to machines—and not just tasks—humans can be used for uniquely human tasks.

Follow-up papers will take a deeper dive into the evolving definition of the "next generation" SOC workforce and the need to strategically outsource certain capabilities. As automation begins to reduce the dependency on Level 1 analysts, organizations should think critically about how to drive more meaningful investigations within their existing staff, while justifying their ROI in a costefficient manner.

LET'S TALK

Arun Perinkolam
Principal
Deloitte & Touche LLP
aperinkolam@deloitte.com

Christopher Trollo
Senior Manager
Deloitte & Touche LLP
ctrollo@deloitte.com

Max Kovalsky
Senior Manager
Deloitte & Touche LLP
mkovalsky@deloitte.com

Alexi Wiemer
Manager
Deloitte & Touche LLP
awiemer@deloitte.com

Dr. Anton Chuvakin
Head of Security Solutions Strategy
Google Cloud
chuvakin@google.com

Ansh Patnaik
Director, Cloud Security Products
Google Cloud
anshpatnaik@google.com

Philip Bice
Global Business Development Manager
Google Cloud
philipbice@google.com