Google Cloud | Deloitte.

Future of the SOC

SOC PEOPLE: SKILLS NOT TIERS

Introduction

The second article of the "Future of the Security Operations Center (SOC)" series discusses what is arguably the most important component of a SOC—its people. Geared towards cyber security practitioners, including those who are just beginning their journey in security operations, as well as SOC leaders who are wrestling with finding the desired balance between outsourcing and insourcing their operations, this article conceptualizes the problems and reimagines solutions for the people side of your SOC.

This is a new phase of the digital revolution where network edges are extended to a point of entanglement with the physical world, expanding hybrid and an increasingly multi-cloud core—all of which necessitates a rethinking of the SOC workforce model. What are the most effective ways to maximize the time (the most precious of commodities) spent by the SOC workforce into measurable security outcomes of the organizations they serve? Can the tiered SOC model be evolved and adjusted enough to respond to the demands of today or is the time ripe for a new paradigm?

The genealogy of today's SOC workforce model stems from the IT help desk. This approach originated from the application of the hierarchical industrial-age assembly line: passing issues from first to second line and further up. In simpler times, this model was sufficient—technology density was low and problems could be solved with in-person interactions, all at a minimal cost.

Due to the finite number of potential issues, detailed step-by-step troubleshooting procedures justified hiring entry-level staff with expectations of high turnover. The vast body of first line help desk staff was easily replaceable and trainable to perform repetitive tasks without applying judgement.

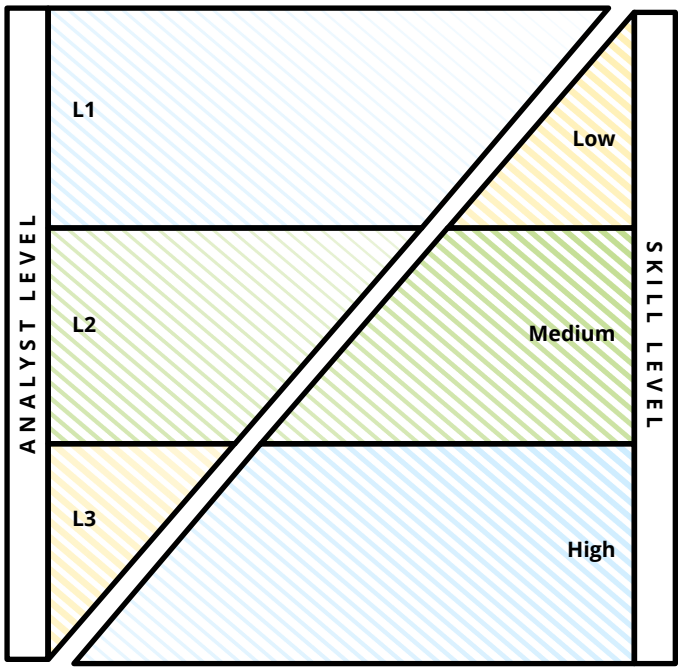
The deficiencies of applying this help desk approach to security events are glaring for anyone who has recently worked in a modern day SOC; there are simply not enough person-hours (or expertise) at the first line to properly evaluate every flashing light. Continuing to employ help desk tiers within a SOC poses three distinct sets of challenges:

Chronicle

1 **SOCs can no longer pair every event with a human analyst.** The help desk model simply does not scale, and as a consequence, vast numbers of events go unnoticed each day within enterprise SOCs.

2 **First line analysis of security events is essentially the challenge of finding key signals in a sea of distracting noise.** This is not an inherently routine task to be given to a machine or junior resources. Unlike widgets on the production line, security events should be considered as part of contextual fabric. This context, among others, includes an understanding of the threat's capability and intent as well as the business functions of impacted assets or people.

3 **Good judgment comes from experience.** In today's SOC, however, those with the least experience make the highest amount of judgment calls. At best, those decisions are a result of following rigid binary trees that don't account for the nuances of business context nor the threat landscape. At worst, decisions are made simply because a ticket has to be closed within the time allotted to the Service Level Agreement (SLA). The cost of bad judgement made during a two-minute triage of a strange event may be as significant as the result of a missed intrusion.



Currently, L1 SOC analysts make the highest amount of judgment calls despite having the lowest level of investigation skills. Comparatively, L3 analysts with higher level skills make the lowest amount of judgment calls.

The SOC workforce evolution: Skills not tiers

Today's environment presents the opportunity for a new workforce model for the modern SOC—one where initial triage is handled by the more experienced team member. Immediate challenges come to mind—talent shortages, prohibitive costs, retentions and mountains of alerts—but with the desired balance of skills and automation, what seems impossible can become possible.

A workforce model fit for an entirely different purpose may serve as a useful analog: the Special Forces Operational Detachment Alpha, also known as the "A Team." As the primary operational element of a larger organization, this small team is composed of individuals with all the necessary skills to complete virtually any tactical operation autonomously. The team lead coordinates the actions of their team members and is ultimately accountable for mission success or failure. Each team member is vested with an understanding of how their particular tactic fits within the broader strategic objectives up to the national level. This understanding empowers the team to take disciplined initiative while remaining true to the mission goals when faced by rapid changes in the operational environment.

While this analogy breaks down upon close scrutiny (A team has years of specialized training and are assessed for mental stamina and pain tolerance required to persevere and succeed), this model is helpful as we think about the type of specialized roles needed within today's SOC. Being mindful of time and talent development constraints (which are very real), what is the minimal set of skills, knowledge, and competencies required to determine malicious intent and take immediate actions? In other words, what does the SOC A Team look like?

The SOC A Team should have a broad understanding of their organization's mission and the role of digital systems that their stakeholders increasingly rely on to remain in business. Furthermore, specialization is required along two planes (for example, endpoint and network or systems and applications) and two dimensions (internal and external) in order to make this SOC A Team effective.

PLANE 1

Computing devices

Competencies along this plane include a granular understanding of the operating systems in use by the organization spanning bare metal, virtualization, and containerization.

Internal dimension encompasses an understanding of the particular ways IT deploys, configures, and maintains computing devices, as well as the security controls applied to those devices.

External dimension sheds light on how these devices (including controls) are exploited by cyber adversaries with the intent and capability to cause the organization harm. Along the same line, application security and system/platform security also split as large and separate domains of talent.

PLANE 2

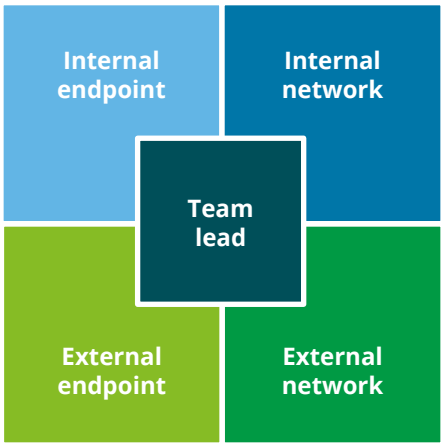
Network traffic

Here, the analysis should be expected to command detailed knowledge of networking features, layers, and protocols. Think ability to read, understand and filter packet headers at the byte level.

Internal dimension requires a general understanding of network-based security controls, coupled with up-to-date knowledge of how those controls are applied within the organization.

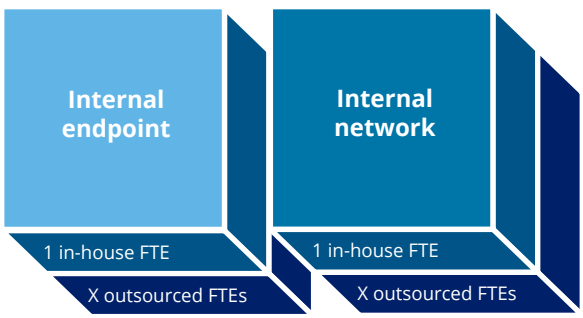
External dimension captures understanding the latest tactics, techniques, and procedures (TTPs) of threat actors based on the organization's threat landscape.

The SOC A Team lead ideally has rotated in each of those four roles throughout their career. The team lead is meant to be highly involved and hands on, not just a project manager. They are the first line of defense and first eyes on glass, orchestrating the investigation work through assignments and reviews. In regard to triage, investigation, and response, the SOC A Team ends up with a shift composition of at least five roles:



Organizations should account for the size and complexity of their networks as they ponder the applicable density of skills in each of the four areas. The more fundamental question, however, is whether and when outsourcing any of these roles to an external provider solves the very real challenges of recruiting and retaining operators with such specialized skills.

Organizations that make the strategic decision to outsource its cyber threat detection and response function should look for a managed security partner that brings the desired skills, not tiers, to the table. However, organizations that have made the strategic decision to not fully outsource their detection and response function should consider outsourcing capacity, as opposed to capability. Capability includes the core skills, knowledge, and competencies within each of the four areas described above, in addition to the team lead. Capacity describes the density of the skills sufficient for either the geographical distribution of the SOC or the 24/7 shift schedule. Fundamentally, the SOC needs in-house knowledge for each capability in order to select and manage the desired capacity if it is to be outsourced. At a minimum, the hybrid SOC should have competency in each of the four areas, as illustrated below:



The body of knowledge required for each practitioner to be effective within allof the four specialized roles is as deep as it is wide. At the entry level, some minimum amount of specialized training is required in each area. SOCs need a workforce acquisition and development strategy. This strategy should strive to address the following questions:

Talent planning

- What talent is available on the market?
- What skills am I hiring and in what amounts and combinations?
- What skills are going to be provided by third-party providers (outsourced)?

Talent acquisition

- What is my hiring plan and process?
- How do I market my cyber program to attract the desired people to my SOC?

Workforce development

- What are the minimum sets of skills, knowledge and competencies necessary within each SOC role?
- How do we confirm that our workforce is proficient in those skills?
- Do we build and deliver our own role and level certification program, or outsource it to an outside provider?

Talent retention

- What am I doing to keep my analysts happy and engaged, growing, developing and delivering value to my SOC operation?

The complicated relationship between SOC staffing and automation

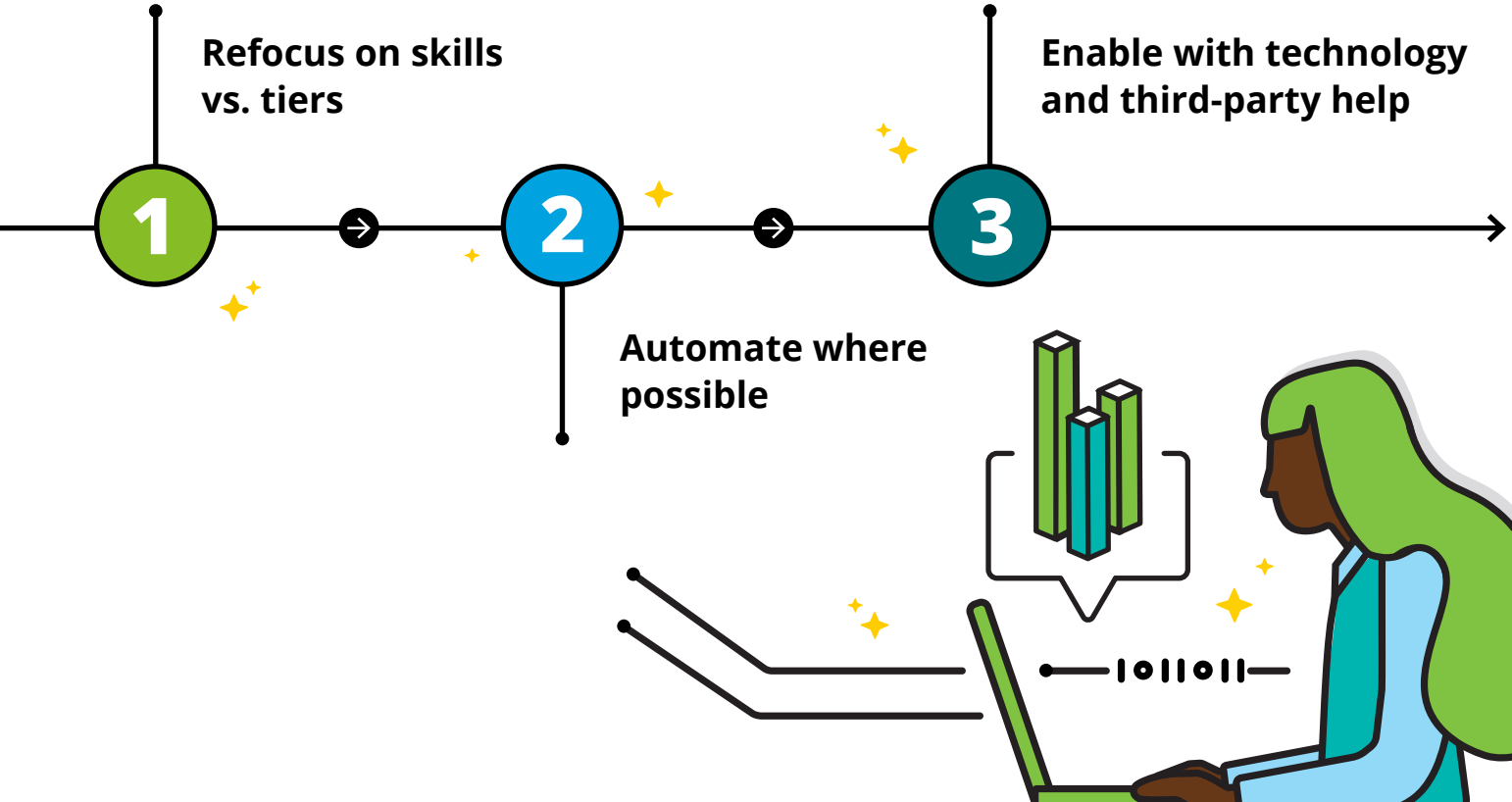
So the question now becomes: how do you empower a newly developed, robust SOC A Team to focus on meaningful alerts and not drown in a sea of noise, low-priority signals, and false positives? While people are the focus, automation via defined processes and supported by robust Security Orchestration Automation and Response (SOAR) technology can help increase the efficiency of a SOC's staff. Ultimately, SOAR and other automation tools serve as a force-multiplier for people, not a replacement for them.

Unfortunately, automation and orchestration has become as much of a sales buzz word as analytics or machine learning. Today's SOCs are expected to protect more with less, with executives often treating automation as the justification for decreasing their existing SOC staff. Many hear the common refrain, "Why would we keep this full time equivalent (FTE) when we can automate and have the same work done more consistently at a fraction of the cost?"

Yes, automation is increasingly replacing the common tasks of an entry level/L1 SOC analyst. Yes, automation allows SOC analysts to be more efficient in their investigations by stitching together various referential data in a single pane of glass. Yes, automation decreases the size of the proverbial top of the alert funnel by consistently replicating monotonous tasks more efficiently than a human analyst ever could.

However, the nuance that is often lost when approaching automation and its impact on the SOC staffing is to automate decisions where possible and where it makes sense. Just because a SOC process can be automated does not necessarily mean it should. No SOC engineer wants to explain why an executive's laptop was automatically re-imaged due to a false positive (happens more than you would think!). Each organization will need to determine how much risk they are willing to accept when some mistakes inevitably occur due to automation and require tuning.

Rethinking the organization of the modern SOC towards skills rather than tiers, coupled with a heightened focus on automation, can significantly mitigate today's widespread shortage of people and skills in cybersecurity. A gap between SOC human resources and alerting/investigation workload may remain, but the good news is that there is an opportunity to further close that gap through technology-driven enablement, helping to improve SOC personnel productivity, retention and sense of accomplishment.



So you've decided to automate, now what?

When organizations begin their automation journey, there may be clear use cases where enrichment, automation, and curation are some of the key areas to explore and exploit.

For example - an organization's SOC team has learned about a malicious domain that is part of a threat campaign actively targeting that organization's industry. The goal now is to uncover users and endpoints that may have communicated with that domain, divulged credentials, and potentially also downloaded malware. Answering these questions involves slow and complex queries against a mountain of security telemetry spanning numerous security data sources. It also requires correlating the telemetry with user, asset, and threat context.

In this example, Domain Name System (DNS) can share the assets that accessed the domain in question, but you'd have to look at web proxy (or other) logs to determine whether credentials were posted and a sizable file was downloaded. Unfortunately, you won't have hostnames in all your logs, so you first have to translate source IPs to hostnames using Dynamic Host Configuration Protocol (DHCP) data. And for each asset that you uncover as potentially compromised, even more voluminous and rich but complex Endpoint Detection & Response (EDR) logs need to be sifted through to confirm whether the rest of the kill chain played out. That's just an abbreviated version of the typical playbook and it has already turned into a sequence of slow, complex queries with joins and subqueries in the Security Information Event Management (SIEM) or log management syntax of your choice. These everyday tasks require a highly experienced, scarce and overworked Tier 2 or 3 analyst resource.

Enrichment

Looking at this from the beginning, what if the common data schema of your security analytics solution already took care of de-duplication and enrichment? In this scenario, DHCP data is automatically and continuously used to correlate source IPs to hostnames, and events across data sources representing the same event (but with non-overlapping information) were deduplicated and combined into a pre-enriched singular, canonical meta event written in plain language. Now, you could simply search on the domain in question and see a distinct set of deduplicated, easy to understand events representing the evidence with no complex queries and no syntax to learn.

Automation

Second, what if this went a step further and the correlation of all threat intelligence was automated against that simplified, pre-enriched common data schema? Why should SOC teams have to manually (or on a scheduled basis) pick and choose specific threat intelligence sources to correlate with specific data source telemetry over limited slivers of time? Changing that current state reality through enrichment and automation would already represent a huge win in terms of SOC productivity. Analysts would no longer have to write a query to find threat intelligence matches to assets and users.

More importantly, detection rules for much more sophisticated threat scenarios could be far simpler to author and interpret with the suggested base enrichment and automated correlation. This comes with the caveat that the impact of this automation is highly dependent on the continuous evaluation of actionable, meaningful intelligence. "Garbage in, garbage out" is another all too common SOC refrain. More intelligence feeds do not necessarily mean better protection, and this is particularly true in current times when SOCs are expected to justify their budget and Return On Investment (ROI) to their business stakeholders.

Curation

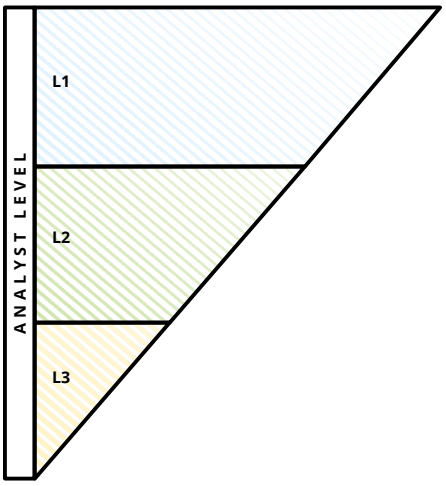
The third opportunity for technology driven enablement is curation, referring to multidimensional, interconnected and context rich views specifically designed and optimized for security threat investigations and hunts. It implies effective point and click pivot navigation across threat, asset and user dimensions of analysis, without the need to write any queries. It assumes operation on top of the pre-enriched and pre-correlated data model described earlier. The end goal of curation is to replace the learning curve of proprietary syntaxes with intuitive visualization. The desired outcome is greater productivity through democratization of investigations and hunts into the hands of any analyst.

Where the A Team can help

As these low hanging fruit use cases are addressed, the SOC can start tackling thornier automation topics. What controls are put in place in case an automated script malfunctions and accidentally brings down an entire production environment system it's querying for referential data? What is the automation approval process to confirm that the entire organization (not just the SOC) has approved the potential risk of automating more sensitive tasks that can impact users such as automatic disabling of accounts? How often are the automated scripts reviewed, tuned as new data sources are inevitably onboarded and decommissioned?

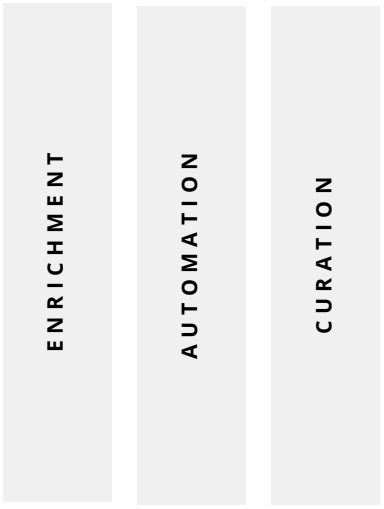
As these grayer areas pop up, SOCs lean on their more senior analysts (the SOC A Team) to provide the necessary institutional knowledge such as business context, existing triage/investigation processes and emerging threat landscape trends to determine what level of automation is acceptable based on their organization's risk tolerance.

Tier-based SOC



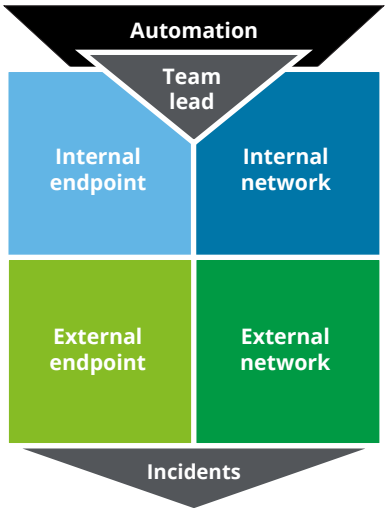
Current tier-based model reduces the amount of judgment calls made by analysts as their technical experience increases.

Technology enablement



Technology empowers analysts to be more meaningful and efficient in their judgment calls.

Skills-based SOC



Appropriate subject matter expertise, coupled with automation, provides an appropriate level of context to judgment calls.

When deployed effectively, automation empowers the SOC A Team with the autonomy necessary to focus on their highly specialized area (e.g. internal/external endpoint, internal/external network). As indicated by the diagram above, an experienced team lead acts as the mentor for the SOC A Team to confirm that the appropriate context from the automated triage is considered before a deeper technical dive occurs. Essentially, the team lead is the first connection that provides the necessary business context that automation natively lacks.

Leveraging their specialized training and experience, the SOC A Team provides the appropriate subject matter expertise for the SOC to be confident in its newly deployed automation processes (for example, do the tactical efficiencies gained from this script outweigh the potential organization risk?). This high performing SOC A Team of experts, supported by high performing computing, significantly reduces the alert firehose while still escalating key events that may provide additional information on the threat and business impact of a potential threat.

Every SOC is a hybrid SOC

When your SOC A Team is organized by skill and not by level, there will be skills that are deemed necessary, yet they cannot be found at the applicable scale. For example, very few SOCs will hire a malware reverse engineer (some do, but they are definitely in the minority), yet all SOCs will encounter malware that they need to analyze. Similarly, a skilled expert on threat intelligence and threat assessment - while necessary for a good SOC - may not be around to hire in your location.

Historically, this led many organizations to make a choice when managed security services just appeared on the market. The choice was to keep a SOC in-house or to outsource to a Managed Security Service Provider (MSSP). This world was very black and white back in the late 1990s.

But today we live in a world with a dizzying array of options for delegating security tasks. Software as a Service (SaaS) and co-managed models for tools, MSSP and Managed Detection and Response (MDR), managed EDR, various staff augmentation models all compete for enterprise attention. Given the long list of potential tasks and a wide variety of third parties, this is a hard decision to make and no clear way to hire away from this problem.

As staff shortages for SOC analysts fail to disappear, hybrid models will grow and expand. Note that some are used by organizations that have effective and robust in-house SOCs as well, hence breaking off the original model or "in-house or outsourced."

Skills that externalize well

Commonly externalized SOC services include:

- Deeper malware analysis
- Threat intelligence

Occasionally, organizations will also look for help with:

- SIEM, EDR, and other tool management and tuning
- SOC tool tuning and use case analysis

Finally, some organizations will mix managed services for skills like:

- Managed threat hunting

Understandably, anything closely connected to your business and mission can be hard to externalize. Organizational requirements are key here to determine the extent to which outsourcing is possible, ranging from 100% in-house to hybrid to 100% outsourced.

Regardless of the model chosen, the points of emphasis from the A team model still apply: highly skilled, technical workforce (that are often scarce in the marketplace) to work together and understand the fundamental risks to your organization.

Remember that the client remains accountable for the outcome no matter what and some aspects in security and risk cannot be outsourced, by definition.

Thus, division of responsibilities between the client and various third parties should be clear and explicit (to avoid the mistakes like "we pay money, they deliver security" affliction); think specific tasks, not vague messages.

Also, a key consideration is that some third-party offerings are flexible (for example, consulting) while some are not (for example, traditional MSSP). This plays a role in the decision as using the inflexible service for a task that calls for inherent flexibility and agility results in cost overruns and, worst case, failures.

To add to this, it is easier to hand off tasks that are not deeply customized and/or dependent on a peculiar property of your business. For example, a web site monitoring for attacks is much easier to hand off compared to internal user application access anomaly monitoring.

Another principle that works for large organizations is outsource capacity, but not capability. This relies on the fact that to outsource a function well, a degree of internal expertise is required to judge a provider, both in the beginning and over time. Hence, to outsource well, you need to have at least some expertise in the area.

Learn with your outsourcer

Prepare to learn from your third parties and improve your A Team: your MSSP or an MDR may have mature processes and tactics to improve operations. Be aware that the knowledge transfer goes both ways: you may learn about threats from them, and they may learn more about how to secure your particular business.

The decision to include third parties is easier in principle and harder in practice: do it if they can do it faster, better and/or cheaper than you can. Practically, this means that a client building a SOC needs to have enough expertise in all the subjects to tell better from, well, not better.

To summarize, prepare to bring third parties into your SOC to cover the skills gaps. Then prepare to manage a combination of the providers and in-house experts, keeping in mind the capability vs capacity argument.

Conclusion

The genealogy of today's SOC workforce model is the IT helpdesk; however, this model and inspiration may have outlived its usefulness for modern security operations. The modern SOC and even more so the SOC of the future may be built on different principles.

SOCs can no longer pair every event with a human analyst. The model simply does not scale to today's business, IT, and threats. This means automation and outsourcing, but it also means a different skill model, rather than a hierarchical pyramid of the past.

Unlike widgets on the production line, security events should be considered as part of contextual fabric. This implies that a naive per alert model is broken as well, just as the "SOC as a funnel" model. To solve this, one can focus on improving the effectiveness of the early triage activities, rather than simply leveraging junior resources. Where possible, repeatable processes and decisions should be automated, with the initial human triage done by the more experienced team member—armed with the relevant tools, and supported by the desired skills in the applicable scale.

The key learning of many SOC leaders and operators of today is that every SOC ends up being a hybrid model, with one or more of the tasks being handled by the third party. In the ideal state, and with an effective workforce strategy in place, those taskings address the problem of capacity, rather than capability.

Rethinking the organization of the modern SOC towards skills rather than tiers, coupled with a heightened focus on automation, can significantly mitigate today's widespread people and skills shortage in cybersecurity.

Let's talk!

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

Maxim 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

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