Google Cloud | Deloitte.

Future of the SOC: Evolution or Optimization —Choose Your Path

Chronicle

Abstract

The landscape: The SOC of the future will be more automated and use AI to detect and respond to threats, as well as support the team.

The options: Organizations can either optimize their current SOC or transform it into a more automation-first model.

Take charge: Optimize your current SOC for heightened speed, enriched content, reduced costs, and empowered staff.

Embrace transformation: Invest in new technologies and processes to evolve your SOC and enable time-saving automation.

Decision time: The landscape is evolving fast, so choose wisely based on your organization's budget, risk tolerance, and technical capabilities.

Introduction

Security operations centers (SOCs) have an increasingly difficult job of protecting evolving and expanding organizations, which produce astronomical amounts of relevant security data. The job of the SOC is to help develop the appropriate mix of people, process, and technology to handle that job.

Earlier in our "Future of the SOC" series, we shared that when done right, the SOC is "people first, process second, and tools third." We cover SOC people and skills in "Future of the SOC: SOC People—Skills, Not Tiers" and SOC processes in "Future of the SOC: Process Consistency and Creativity: a Delicate Balance". Once you have hired and trained the correct people, and defined your required processes, you must make sure that your tooling supports your SOC's mission.

Why evolve your SOC…or not?

The SOC's mission requires a reliance on a broad range of tools to get the job done. Over the years, this toolset has expanded and evolved, often comprising of a incongruent mix of legacy tools and newly acquired technologies. The scale of modern business and the sophistication of threat actors require the SOC to maximize visibility across a growing estate and employ disparate data sets. Our defenders find themselves between a rock and a hard place; tools are necessary, but the lack of staff, lack of time, and expansion of data make the care and feeding of this complex tool ecosystem infeasible.

As a solution, many SOCs find themselves wrestling with a decision to change their ways or continue burning out, barely managing their current technology stack. Is there a way for the SOC to evolve or change their approach? Doing do would improve their ability to detect and respond to threats, and protect their organizations from cyberattacks. Maintaining the status quo risks falling behind as business and IT threats continue to evolve.

We propose there are two approaches for the SOC in this situation:

Transform your SOC. This involves completely overhauling your SOC, from its architecture and processes to its staffing and training. Typically, this means evolving to a more engineering-led approach such as Autonomic Security Operations.

Optimize your SOC. This involves making incremental improvements to your SOC, such as adding new tools and technologies, refining some processes, or improving your incident response processes.

The decision of whether to transform or optimize your SOC will depend on several factors, including your budget, your risk appetite, and your technical capabilities. However, it is important to take decisive action as the risks of doing nothing are too great, especially as cyberattacks become more sophisticated and frequent.

If you decide to transform your SOC, you will need to invest in new technologies and processes. This can be a costly and time-consuming process, but ultimately rewarding. A transformed SOC can be more efficient and effective at detecting and responding to growing and changing threats.

If you decide to optimize your SOC, you will focus on improving the efficiency and effectiveness of your existing processes. This less costly and less time-consuming approach may not be as effective as SOC transformation.

Tools and challenges

The only way for a modern SOC to survive is to rely on a variety of tools to monitor and protect the organization from cyber threats. Tool proliferation continues across the industry, however the majority of SOCs manage a complex list of technologies such as:

Security Information and Event Management (SIEM):
A SIEM collects and analyzes security logs and events from a variety of sources, such as firewalls, network devices, and applications. This data can be used to detect threats, investigate incidents, and comply with security regulations.

Security Orchestration, Automation, and Response (SOAR):
A SOAR platform automates security tasks, such as incident response, threat hunting, and compliance reporting. This can free up security analysts to focus on more strategic work and improve the speed and efficiency of security operations.

Endpoint Detection and Response (EDR):
An EDR solution collects and analyzes data from endpoints, such as laptops, desktops, and servers. This data can be used to detect threats, investigate incidents, and remediate vulnerabilities.

Extended Detection and Response (XDR):
An XDR solution is a more advanced version of EDR that collects and analyzes data from a wider range of sources, such as endpoints, networks, cloud applications, and identity and access management (IAM) systems. This data can be used to provide a more comprehensive view of threats and improve the speed and accuracy of threat detection and response.

Technology	Data Sources	Focus	Benefits
SIEM	Security logs and events	Threat detection compliance, incident management	Provides a centralized view of security data, can be used to detect threats investigate incidents, and comply with security regulations
SOAR	Security logs and events as well as other data sources	Security automation orchestration, and response	Automates security tasks, such as incident response, threat hunting, and compliance reporting, can free up security analysts to focu on more strategic work and improve the speed and efficiency of security opperations
EDR	Data from endpoints, such as laptops, desktops, and servers	Threat detection and response	Detects threats at the endpoint level, can investigate incidents and remediate vulnerabilities
XDR	Data from endpoints, networks, cloud applications, and IAM systems	Threat detection and response	Provides a more comprehensive view of threats than EDR, can improve the speed and accuracy of threat detection and response

SOC toolset management is a complex and challenging task. However, it is essential for SOCs to get it right. By carefully selecting, managing, and using the right tools, SOCs can improve their efficiency, effectiveness, and resilience in the face of cyber threats.

However, the traditional (SOC) model is no longer sufficient to meet the challenges of today's threat landscape and rapidly evolving business. The sheer number and complexity of the SOC's tools are not the only challenges defenders face.

There are several technology driven challenges the SOC needs to contend with:

Alert overload.
SOC analysts are inundated with alerts, making it difficult to identify and respond to real threats. This data can be overwhelming, and it can be difficult to identify and respond to threats in a timely manner.

Log source and volume growth.
SOCs need to manage many log sources, which can be time-consuming and expensive. SOCs are inundated with security data from a variety of sources, including logs, network traffic, and endpoint sensors.

Limited visibility for cloud.
SOCs often have limited visibility into their environment, making it difficult to detect and respond to threats. Often the business requirements for speed and scale demand a move to cloud, but existing security tool-sets were not chosen with cloud in mind. This lack of visibility can make it difficult for SOC teams to identify and respond to threats in cloud environments.

Lack of automation.
SOCs often rely on manual processes, which can lead to delays in detecting and responding to threats. Many SOCs are still struggling to implement automation due to a lack of resources, experience, or buy-in from senior management.

Skills shortage.
There is a shortage of skilled security professionals, which makes it difficult for SOCs to hire and retain qualified personnel. This can lead to burnout and turnover, which will impact the effectiveness of the SOC.

Evolution of threat actor approaches.
Threat actors are constantly evolving their techniques, making it difficult for SOCs to keep up. This challenge is exacerbated when needing to update defense and detection across a multitude of tools. SOCs are often targeted by attackers because they have access to sensitive data and systems.

Two paths to future SOC

The SOC evolution can be understood using a historical analogy. In the late 1940s, propeller planes handled all passenger and cargo air traffic. The jet era had yet to begin, even though the first military jet planes were in use. Aircraft developers faced a choice: further improve the proven model—faster, larger, more comfortable propeller planes, or make the jump to jets, which offer both advantages and disadvantages. The new technology was different, required different skills to maintain, burned more fuels, etc. In the longer term, it became clear that jets would win, but short-term technical decisions could have been made differently.

Likewise, security leaders are driving for the best outcome for their organization while protecting their customers, employees, assets, and brand from the amplifying sophistication of adversaries. It is the leader's role to invest in protecting its organization's entities and determining the most appropriate time to make a change in tools, technologies, workflows, approaches, or staffing.

An organization could grow so large that its continued growth in visibility and detection becomes unsustainable for budgetary, performance, or talent reasons. For small to medium organizations, investing more in security operations is critical, but staff and/or budget may not be fully equipped to operate completely in-house.

As we mentioned, when referring to today's SOC current state, there are two paths to move forward, which are improving the current model or investing in transforming the SOC to prepare for the future of automation and artificial intelligence at scale. Now let's review these models and decide what to do.

Choice 1: Double down on current investments to optimize your SOC

As time goes on, more data and visibility will become accessible to each investigation if the SOC is able to consume, comprehend, and respond without any gaps or wasted effort in their coverage. To prepare, the organization must consider how to continuously upgrade current solutions in speed, content, cost, and staff.

Speed

When diagnosing opportunities to improve the speed of an SIEM, an organization can explore improving the following four areas:

1

Time to data accessibility

Time to data accessibility refers to the time delta between event generation from a log source and the time the event is ingested and available in the SIEM. An opportunity to improve would be to identify areas where an Extract Transform Load (ETL) pipeline can incorporate data streaming methods over batching or minimizing the hops between its source and SIEM.

However, this improvement is dependent on the log source vendor and product. Not all products provide this as an option and can require an unrealized level of effort if an organization's current ETL infrastructure isn't utilizing a stream-processing platform such as Apache Kafka, Google Pub/Sub, or Cribl. These systems call for yet another skillset needed in the SOC.

2

Time to return a search

Time to return a search refers to the time to return the results of a desired search query. Improving search time is dependent on the SIEM an organization is using and how the data is stored. SIEMs use different approaches to store large amounts of data to extract the most performance out of its infrastructure. One way an organization can improve its performance is through indexing each field value pair within a defined type to prevent the search from spending time deciding what type of field the query requires, like a wildcard search, which is not performant.

Another opportunity for a customer to improve performance would be converting their log sources to a common schema, such as Elastic Common Schema (ECS), Splunk Common Information Model (CIM), or the emerging Open Cybersecurity Schema Framework (OCSF). This requires consistent effort by a security engineering team to continuously review data coming into the system, since data changes constantly upstream when products incorporate changes.

An unrealized step is the time it takes to develop a search query or queries to return your desired results on a single pane of glass. Mature organizations have spent countless hours saving searches to enhance their workflow for threat hunters and SOC analysts. Improving search queries to narrow results can improve search time by returning fewer results, but being too specific could miss potential malicious activity.

A less-experienced talent pool may not know how the queries were developed because they are utilizing the saved search outcome instead of understanding the steps and information required to get to that outcome. Furthermore, this situation would put the organization at a disadvantage when considering future technology changes as the workforce would have become reliant on this feature for their workflow.

3 Time to escalate

The time to escalate refers to the time it takes to investigate an alert, determine if that alert is a true positive, and require escalation for containment or remediation if so. This area is dependent on the sophistication of an organization's threat modeling and emphasis on developing and tuning detection rules to decrease the rate of false positives. An organization should incorporate a detection rule lifecycle that would include development, tuning, and review.

Security Operations are dynamic; organizational targets may change rapidly and indicators once considered valuable may diminish over time. Developing a standard workflow with escalation contacts is one way to provide a standardized quality gate check and avoid wasted time. Organizations may also consider utilizing a SOAR platform to organize and improve these workflows to automate common or low-level alerts.

4 More log filters to reduce the pain

Some organizations optimize the SOC by deploying more intake filters and tools such as Cribl. The desire to reduce the input often leads to decreased costs. However, it may also lead to losing valuable data for incident response.

Detection content

A SIEM platform is only as sophisticated as the data that it ingests and the content items that are built from that data. We previously mentioned that detection rule development recommends defining a lifecycle for development, tuning, and reviewing for an organization to follow. To improve SIEM content, an organization's goal should be to reduce alert fatigue that stems from false positives, as well as enabling detection rules that have a defined playbook for next steps.

Value of the detection decreases when the organization cannot act upon what has been detected. Content can be expanded further from detection rules by incorporating threat intelligence solutions and machine learning analytics to identify patterns over a period. Threat intelligence provides operators a faster approach to identifying a true positive with already correlated malicious patterns. Artificial intelligence (AI)/machine learning (ML) content items require a large volume of retained data for the analytic model to be trained and tuned by expert individuals who know what they are trying to detect and how to do it following AI/ML principles. It would also need more robust validation, at least for some time.

> ***Improving detection could be a matter of investing in complementary technologies,*** *such as robust EDR/XDR solutions to provide automated threat detection and response through a vendor's proprietary use of threat intelligence.*

Protecting an environment's edge is an important investment to prevent the blast radius of potential breaches by containing the malicious activity automatically. Depending on the vendor, an EDR/XDR investment can provide malware identification, automated prevention of exploits, real-time visibility of endpoints, and machine learning of unknown malware. The indicators of compromise (IOCs) derived from these capabilities provide invaluable insights for the SOC to improve detections in its existing SIEM and build a strong defensive perimeter for the enterprise.

Cost

The common cost of SIEMs that organizations need to be made aware of is the volume of data they ingest and the duration they retain it. In a direct correlation, the more data ingested, the longer it is retained, and the larger the team size, the higher the cost. An approach to reducing data cost would entail truncated field keys and dropping fields before ingesting into the SIEM. If the data is mission-critical for investigations, diverting selected data to a more cost-efficient database to be used as a lookup table for investigations is another approach to trim the size of one's data. However, operators become less efficient by requiring extra steps with non-integrated platforms to perform investigations.

The cost difference switches from hard dollars to soft dollars within an organization as operators take more time to operate in their roles. Leaders in an organization will need to compromise on what tools they invest in, how much visibility they have, and accept risk to justify their allocated budgets.

Staff

Security professionals are highly sought after and organizations struggle to retain talent as competitors pay top dollar to expand their security teams. Organizations need to balance hard vs soft dollars by investing in professionals' training and hoping they won't depart soon after.

On the other side, the cost of finding and hiring talent increases because of the sheer demand for security professionals. There isn't a direct solution since security operations is an evolving industry that requires continuous learning.

Organizations require continuity despite any talent setbacks. Many have heard the phrase, "Be prepared for anyone to win the lottery." To lessen the impact of talent churn, organizations should focus on lowering the time it takes to onboard new team members and emphasize documenting systems and procedures to reduce unwritten veteran knowledge. Creating a culture of learning, failing fast, and valuing each team member for their contributions—small or large—all help protect the company.

Summary

When making this choice, organizations should prepared to continuously upgrade their SIEM solutions to keep up with the increasing amount of data and visibility that will become available in the future. *To handle increasing data and visibility, organizations must continuously upgrade their SIEM solutions in speed, content, cost, and staff.*

Speed:
Improve time to data accessibility, return a search, and escalate by incorporating data streaming methods, indexing fields, and using a SOAR platform.

Content:
Reduce alert fatigue, enable detection rules, and expand content with threat intelligence and machine learning.

Cost:
Reduce data cost by truncating field keys, diverting data, and compromising on tools, visibility, and risk.

Staff:
Onboard new team members quickly, document systems, and create a culture of learning.

Organizations must continuously upgrade their SIEM solutions to keep up with the future.

Choice 2: Invest in transformational change for your SOC

When the result of assessing a security organization indicates that the best path forward is to invest time, money, and effort into a different strategy, then it is time to identify what changes are required and what can stay the same. Security leaders need to look ahead to consider their in-house skillsets, partnered skillsets, budget, and technologies when determining where to increase investment or make changes.

Identifying which components are compatible with new invested technologies and which components need to be replaced will be crucial in determining a cost-effective approach to transforming the environment for the next generation of SOC.

SIEM technology change: Software-as-a-Service (SaaS) SIEM arrives

Traditionally, many implementation strategies involved hosting a SIEM on-premise for various reasons. These could include prior investments, cost, security, or compliance. Security in the cloud has quickly become the safer and more efficient option for many organizations. This comes with less management and overhead of the lower half of the Open Systems Interconnection (OSI) model. This same principle has transformed where software is hosted and how it is managed with SaaS applications. If a SIEM is consumed in a SaaS model, organizations become customers of the application, thereby removing the requirement to patch and manage the backend infrastructure of the desired SIEM.

Chronicle SIEM utilizes the power of Google search so customers can focus on detection and operation of in their environment, instead of managing a solution to prevent loss of availability.

Better data / UDM/structured / pre-enriched

Visibility into organizational activities is the goal of a SIEM tool. However, data generated from different sources and vendors makes it difficult to organize and aggregate. Preprocessing data before it is available in the SIEM allows for a common schema to be used to efficiently search and aggregate across an entire environment. Chronicle SIEM utilizes Unified Data Model (UDM) as a universal data model for all log sources. This approach enables a SIEM to move away from index-based searching and detecting and towards outcome- and narrative-based investigations.

Threat hunting—critical, not auxiliary

Threat hunting has historically been thought of as an advanced capability for an SOC, with only more mature programs formally standing up such teams with dedicated effort to carry out campaigns. However, by frontloading the effort of combing through and cleaning an environment's data into a standardized format that speaks in a common manner, the SOC has rich opportunities to threat hunt off trailheads that systems flag and raise. This alleviates the need to wait to stand up a program only once it reaches a certain level of maturity.

One example of threat hunting as a first-class use case within Chronicle SIEM is the concept of an Investigative View, aided by prevalence and other baselining statistics for a given entity within the environment. Analysts are presented with anomalies and potential trailheads bubbled out from the pack visually, with contextual data from sources such as Virus Total aiding in identifying false positives, and quick pivots to other relational objects made possible by a common data schema and automated contextual enrichment. Threat hunting, while still valuable as a more formalized and matured capability, can be additionally democratized and thus scaled through leveraging a SaaS SIEM.

EDR: not just antivirus

Akin to the SIEM's threat detection maturation journey, EDR provides significantly greater capabilities than legacy antivirus (AV) operating on atomic indicators, while additionally including centralized management and response capabilities—perfect to tie back into a broader tech stack with the rich telemetry it provides.

> *When thinking about the security of an enterprise in the analogy of an onion, EDR and similar variants (XDR) form an impressive outer layer around the SIEM.*

This allows the more basic use cases—or streamlined use cases, in terms of telemetry to detect being single-source opposed to correlation-based—to push out from the SIEM, while gaining automated quarantine and remediation activities in the process.

This partnership between technologies allows for richer correlation-based detection to thrive at the SIEM layer, while still taking full advantage of the detailed endpoint telemetry and alerts on rules triggered and acted upon to gain insight and visibility into an environment. Most enterprises already leverage EDR/XDR solutions with their legacy stack, so what changes?

In a modernized SOC stack, EDR telemetry serves as an important source of visibility when cost and compute scaling no longer restrict ingestion to solely EDR alerts for "passthrough" use cases. These alerts instead become contextual points of reference as a form of events, further enriched and correlated with the centralized body of data in the SIEM.

Additionally, while quarantine and remediation actions may still be triggered by rules generated on local agents, tying your actions to a SOAR platform allows for more accurate responses to be executed by logic performed up stream in the SIEM and SOAR, while the organization can still benefit from local threat containment provided by local agents.

SOAR: automation first

The goal of standardizing your data in a common schema and applying standardized workflows is to identify repetitive patterns to automate with technology. Removing as many manual steps as possible and relying on operators to make conditional decisions on an outlying pattern will vastly improve a security organization by increasing focus on more complex threats and detections. Chronicle SIEM has built a foundational-level approach to standardize data to seamlessly and bidirectionally complete cases in Chronicle SOAR and minimize manual intervention and steps between screens.

Threat-informed SOC

Whether gathered through open-source feeds, industry-focused groups such as Information Sharing and Analysis Centers (ISACs) or fully curated through an in-house program, threat intelligence provides valuable context and insights for the SOC—helping to prioritize what to focus on and when, and empowering the SOC to act proactively, rather than reactively.

Hunting off threat intelligence data is tedious and introduces significant toil for analysts that is difficult to scale—both due to people and the load it imposes on systems to search. You may have 20, 50, 100, or more relevant search indicators off the latest report, and a team can expedite this process by leveraging lists and scripts to programmatically upload and run queries. But this is still an incredibly manual process, limiting one's ability to scale and impeding time to detection, if a match is found.

Chronicle SIEM addresses this concern through automated hunting of threat intelligence indicators, both through platform-provided feeds from sources such as the Department of Homeland Security (DHS) and Mandiant, and offering extensibility to support custom integrations for one's own internal or sharing community-managed threat intelligence platform (TIP).

Upon ingest of an IOC, Chronicle automatically searches the environment over the entire corpus of data to identify matches and it does so in the background without analyst intervention, until hits are identified.

Expanded upon this by leveraging SOAR playbooks to automatically pick up indicator hits and vet them further before tossing to a human analyst to cast final judgment.

This solution isn't perfect, as Chronicle SIEM solely does this automated searching for domains and IPv4 addresses for now. However, there are plans to add support for hashes in the near future, and through detection rules or additional scripting, this automated hunting can be achieved with workarounds to reduce and eliminate the manual toil of indicator hunting.

AI to the rescue

How can Generative AI (GenAI) be effectively used in a SIEM? There is a high demand and low supply of talent available for cybersecurity organizations, and each time a new analyst or experienced hire is onboarded, they must become familiar with the syntax or User Interface (UI) of the technology suite used. GenAI allows for natural language searches with an output that the operator can learn over time. Chronicle SIEM, for example, leverages SecPaLM natural language search to build queries directly in the search bar.

Additionally, other AI/ML techniques offer significant promise in putting a dent in the outstanding demand for analyst hours. Statistical modeling approaches within UEBA engines to establish environment baselines and identify anomalies that arise are one example of more advanced techniques finding their way into a SOC's toolkit to minimize manual toil and analyst hours spent resolving incidents.

Some things really do stay the same

The line of delineation for engineers and management of the SOC becomes visible at the log generating source. The SOC may have the ability to invest in software requirements for an enterprise's assets, but other teams in the enterprise must still manage the output of these assets.

A modular and structured logging architecture enables flexibility if new components require replacement with minimum downtime and continuous visibility in an environment. As a SaaS solution, Cribl provides a middle layer that can handle many inputs to many destinations for logs to flow into. This feature creates stability in one's pipeline by modularly changing log generating sources and log delivery destinations.

While the detection engineering paradigm shifts to modernize along with the adversarial landscape through techniques leveraging AI/ML models, UEBA baselining, detection-as-code, and other advanced approaches, the basics of atomic detections still possess incredible value and will be augmented by these more advanced techniques rather than replaced.

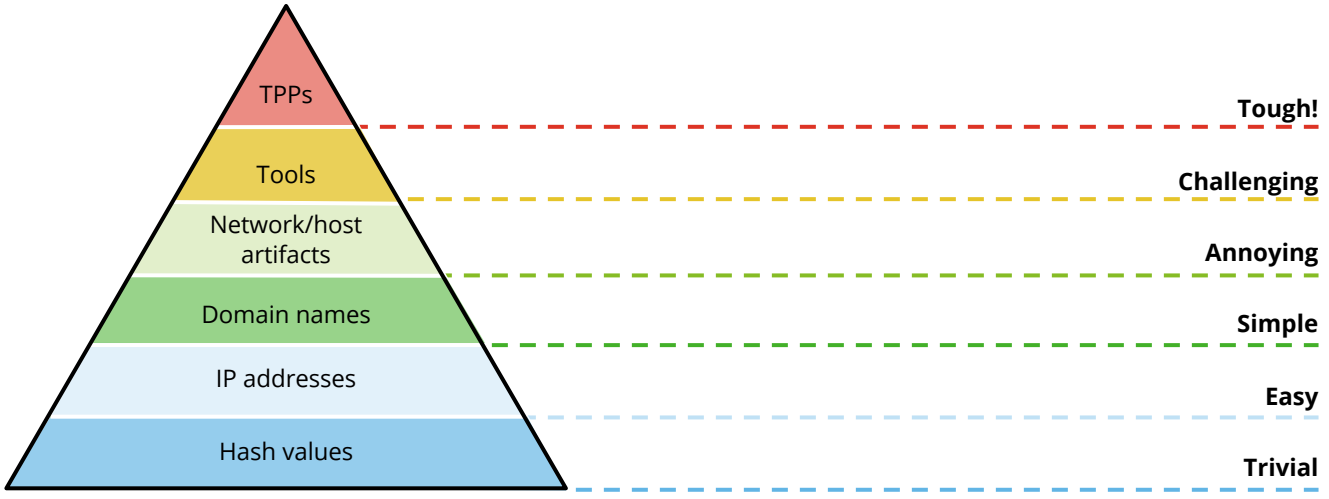
Atomic detections make up the base layers of the "Pyramid of Pain"—the "simple, easy, trivial" items such as domains, IP addresses, and hashes referenced in this visual. Arguably, some items in even the tool and artifacts categories fall into this "atomic" bucket, as they can be pre-canned and "simple."

These atomic detections provide excellent coverage against low-hanging fruit in the environment, such as a CobaltStrike beacon spinning up, script kiddies launching various tools in their Kali box, or even known, advanced adversaries leveraging infrastructure that has been identified, documented, and tracked by security researchers in the form of threat intelligence.

These detections are excellent targets for automation and good ways to baseline environment norms. A SaaS SIEM like Chronicle provides these types of detections in the form of click-to-enable Curated Detections, with the opportunity to alleviate manual toil for the low-hanging fruit.

New technologies and standardized workflows drastically improve a security organization's environment; however, despite all the new releases, it is still important to have deep knowledge (democratized and documented) of the enterprise's environment.

This knowledge empowers quick decision-making during an incident. Nothing can guarantee that an organization won't get breached, but preparation and the ability to detect and react quickly can reduce the blast radius. Working with non-security technologies and staff creates a barrier in a workflow that still requires human intervention and experience of organizational structure to move quickly and reduce lasting impact from any incident.



Summary

SaaS SIEM is the future of SIEM. It is more secure, efficient, and cost-effective than on-premise SIEM. Also, better data is essential for a successful SIEM. Pre-processed data in a common schema allows for efficient search and aggregation.

SOAR automation reduces manual toil; a SaaS SIEM can seamlessly integrate with SOAR to automate tasks.

Threat hunting is critical for a proactive SOC; a SaaS SIEM can democratize and scale threat hunting. Threat intelligence helps prioritize threats and hunting; a SaaS SIEM can automate the hunting of threat intelligence indicators.

AI/ML can help to reduce analyst toil; a SaaS SIEM can use AI/ML to generate queries, baseline environments, and identify anomalies.

Finally, even in a transformed SOC, some things really do stay the same. Log collection, atomic detections, and deep human knowledge of the enterprise environment remain essential for a successful SIEM. This enables quick decision-making during an incident.

Part 3—How to choose for you?

Eventually, all organizations will transform—that's the nature of cybersecurity, and more broadly, technology as a discipline. *Today, organizations must answer: How? Why? And when?*

Whether choosing to leverage technological updates and migrations as a catalyst for transformation or to double down on people and process to improve current systems, organizations must plan for change regardless. Security and risk mitigation are not disciplines with a finish line—they continually move and morph along with the world.

How do you decide which road is right for you?

Here are the dimensions:

- Security budget
- Capacity for change
- Tools and customizations
- Strength/size of SOC talent

This table shows some of the details for decision support:

Security Budget

CHANGE

- Spend on current tools is unsustainable due to rapidly increasing spend
- Tool cost model makes visibility needs infeasible

STAY

- Not enough money for anything but keeping up
- No budget for running two tools during transition period

Capacity for change

CHANGE

- Current SOC model broken or unsustainable
- Executive mandate to change
- Piggyback on organizational migration

STAY

- Little or no capacity for change in IT or security
- SOC not a change priority

Tools and customizations

CHANGE

- Current tools don't solve problems or over capacity
- Clear and consistent practices; a change process in place
- Current tools can't cover expansion plans and new environments
- Current tools not popular with analysts

STAY

- Tools deliver on current and near-future goals
- SOC is powered by triable, undocumented knowledge

Strength/size of SOC talent

CHANGE

- Team too small to use current tools and practices

STAY

- Team is sufficient to keep up, skills match current tools
- Team is unwilling to learn new tools

There are a number of switches and knobs that make the various approaches to SOC optimization or transformation applicable for your unique situation.

The first common switch is a lack of visibility, stemming from organizational structure silos, engineering difficulties in log aggregation and normalization, or the cost-prohibitive nature of data gathering and retention. Would a tooling solution that eliminates cost and engineering barriers solve for the organizational structure and political difficulties—or in reverse, would organizational transformation enable proper use of tooling and personnel already in place?

Another switch is a lack of focused effort, which could stem from inefficient, misaligned resources, a lack of properly-skilled resources to hire, or cost constraints limiting the scale to which the organization can fill necessary roles.

Scenarios for change

Consider these scenarios where organizations choose whether to optimize or transform SOC:

An organization may not like the current SOC tool stack, but lack the capacity for change. In this case, the decision to optimize for now will essentially make itself.

An organization may take a deep dive into their existing stack's strengths, weaknesses, and limitations. Can optimization efforts address the stack's shortcomings and can the legacy stack meet foreseen future business needs adequately? If the answer is yes and it has "spare" capacity for change, transforming the operation is the right call.

A mature organization with strong capabilities in engineering integrations, automation, threat hunting, etc., that has reached technological limitations to grow or has a small team without time or money to dedicate to maturing legacy technology, transformation is the right call with good outcomes likely.

Remember that there is no one-size-fits-all, magical tool that can solve all security problems for an organization. Before making a purchase decision, review other decision dimensions and allocate time for implementation; no one should flip the buy switch and assume a tool "just works."

Rather than a single binary decision, the best solution considers an organization's unique complexities to weave a tapestry of different tools that changes over time. Personnel shortages can be solved through training initiatives or external services for spot support. Engineering limitations can be solved through tooling migrations and updates.

Living with the choice

How do you know you made the right decision? Establish metrics to monitor performance and hold yourself accountable. Examples include X% increase in visibility (environments, namespaces, total assets, # net new data sources available), X% improvement in detection coverage according to Y framework, # fewer human actions per case, X% decreased time to contain/remediate/etc.

Naturally, the decision to optimize and not transform is a point-in-time decision. It is recommended to revisit the decision as new threats, business needs, and new tools emerge.

Regardless of the path chosen, regular check-ins will help leaders analyze performance and re-assess if the path traveled is still the best choice for your particular scenario. These check-ins may be annually or more frequently, but they should all follow a similar framework.

> *Revisit the original goals and priorities that led you to select your path.*

Re-educate yourself on why decisions were made and what factors contributed at that point in time. Consider if those factors have changed. If so, how? Does that change anything in approach? If you change your path now, what efficiencies can you realize from the work completed since you last checked in? If things continue smoothly, educate yourself on what went well and why. Where might you apply these learnings elsewhere in the organization?

Are the points of consideration still as relevant as the last time the organization charted a course? Are the same people involved this time around? Are the constraints the same? Are things better or worse, and more importantly, why?

Conclusion

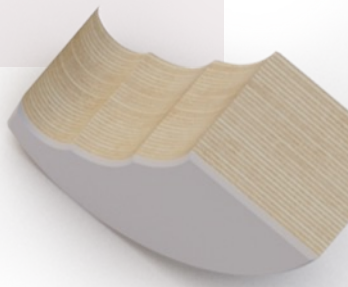
Both updating to a new technology stack and maximizing a legacy stack carry inherent risks.

These risks need to be thoroughly assessed to make the best decision for the business at that point in time. A few such risks include disruptions to normal operations, migration challenges, compatibility issues, and learning curves for the teams involved.

The reality is that rip and replace of tooling with the latest and greatest, co-operation of legacy systems alongside the new, and doubling down on legacy systems all result in a lot of work—albeit different work with varying outcomes. The investment in increasing environment visibility pays dividends down the line when investigating incidents or tying in various tools to speak to one another in a more cohesive ecosystem. The investment in existing tooling may result in a lack of flexibility and visibility long term, but it saves on training and enablement time for teams to upskill.

Assess if you made the right decision before you do anything drastic like flushing your old technologies and processes. Run concurrent ops and prove out your value before cutting the old. This is harder if you are in the "optimize what I have" camp, but setting appropriate goals and metrics for yourself helps if you can show improvement.

Finally, keep in mind that in the long term everyone needs to transform—that's the nature of cybersecurity, and more broadly, technology as a discipline.



Authors

Anton Chuvakin
Senior Staff Security Consultant
Office of the CISO
Google Cloud

Upen Sachdev
Principal
Deloitte & Touche LLP

Dan Lauritzen
Senior Manager
Cloud Security Practice
Deloitte & Touche LLP

Mitchell Rudoll
Specialist Master
Google Cloud Security Practice
Deloitte & Touche LLP

Alexander Glowacki
Senior Consultant
Google Cloud Security Practice
Deloitte & Touche LLP