Cybersecurity Action Team

Autonomic Security Operations

10X Transformation of the Security Operations Center

Iman Ghanizada, Dr. Anton Chuvakin

Google Cloud

Table of Contents

Executive Summary 3

- Landscape is evolving: 3
- Attackers are evolving: 3
- The SOC must evolve dramatically to tackle these new challenges: 3
- Autonomic Security Operations to Transform your SOC: 3

Introduction 4

The SOC mission 5

Why the SOC needs to transform? 6

- Business Transformation 6
- Expanding Attack Surface 8
- Talent Shortage 9
- Why should future SOC be different? 11

What is Autonomic Security Operations? 12

- 10X People 12
  - 10X analyst productivity and effectiveness 13
  - 10X coverage of threats and assets 15
  - 10X knowledge sharing 15
- 10X Process 16
- 10X Technology 17
  - 10X Visibility 17
  - 10X Speed 18
  - 10X Signals 18
  - 10X TCO 19
- 10X Influence 20

How to achieve Autonomic Security Operations 21

- People Transformation 22
- Process Transformation 24
- Technology Transformation 25
- Influence Transformation 27

Conclusion 29

Executive Summary

Landscape is evolving

- Digital transformation changes an organization's attack surface. Cybersecurity risks are expanding beyond the classic SOC use cases and applying to fraud, identity theft, and threats traditionally handled by other teams. Operational fusion is needed now more than ever.
- Technological evolutions in modern computing architecture are constantly changing and more security controls are appearing at all levels of the stack. This increases the volume of data and the potential adverse events that a SOC needs sensory coverage to monitor.
- Supply chains are expanding in depth, and the magnitude of their impact is increasing as the shift away from monolithic applications is boosted by dependencies on purpose-built technologies across first party, third party, and open source software.
- Network-centric security models are superseded by identity-centric access models as services and architectures exist in and across clouds.

Attackers are evolving

- Attackers are taking advantage of these complexities to increase their stealth and ability to persist in an organization while they carry out their mission, and their mission has been increasingly focused on destabilizing organizations and holding them ransom, as well as continuing to steal their valuable information.
- These highly persistent threats are often undetectable by traditional approaches and require strong threat hunting capabilities and robust threat intelligence to detect.

The SOC must evolve to tackle these new challenges

- While cloud environments streamline the ability to detect and respond to threats, most organizations are adopting multi and hybrid-cloud approaches and SOC teams are struggling to ramp up their skill sets and toolsets to adapt to these new architectural paradigms.
- The conventional SOC is not equipped to handle these challenges. There is a shortage in talent that cannot be solved by adding more people alone, the processes that support the SOC mission have not been revamped to meet cloud-centric workload needs, and the technologies that are used inside of a SOC are not capable of streamlining detection & response at scale.

Autonomic Security Operations to transform your SOC

- So overall, in the face of these challenges, we have an opportunity to do a 10X transformation of the SOC, and so is born Autonomic Security Operations.
- ***Autonomic Security Operations*** is a combination of philosophies, practices, and tools that improve an organization's ability to withstand security attacks through an adaptive, agile, and highly automated approach to threat management.
- Our ability to increase & upskill talent to distribute and automate processes with powerful cloud-native technologies will drive our approach to effectively manage modern-day threats at cloud-scale.

Introduction

Cloud transformation has enabled businesses to bring new capabilities to market and enter new markets more rapidly, innovate more easily, and scale more efficiently. While the introduction of this new technology paradigm may reduce overall technology risk, the increasing reliance of businesses on technology puts more intellectual property at stake. Moreover, the access to infrastructure at scale allows developers to create new experiences that augment our lives, where we're more dependent on technology now more than ever. In order to protect our businesses and people in a digital-native world, Security Operations teams need to adapt to a new operating model to adequately prevent, detect, and respond to adversaries in the rapidly evolving techno-centric planet.

Our approach to modernizing and transforming the Security Operations Center (SOC) to maintain velocity with the ever-evolving climate of technology is heavily dependent on human ability to creatively problem solve security challenges at scale. This engineering-centric perspective allows us to focus on developing solutions to security problems rather than maintaining status quo through day-to-day operations of threat management.

In this whitepaper, we'll discuss:

- Why does the SOC need to transform?
- What is Autonomic Security Operations?
- How to achieve Autonomic Security Operations?

As you embark on your transformation journey, bear in mind that we're challenging a decades-old problem. Similar to the Cloud Transformation -- the SOC transformation will require a massive cultural shift in thinking, investments from your leadership, and a highly empowered workforce to overcome these obstacles and pioneer threat management together.

The SOC mission

The concept of a Security Operations Center (SOC) was born in the 1990s at large global enterprises. The original SOC "DNA" likely came from a Network Operations Center (NOC).

The first security operation centers were created to centralize expertise focused on detection and response. Over time, their charter had expanded to compliance monitoring and an array of other objectives, sometimes quite broad.

Today, a SOC is primarily a team, then a set of practices and finally a set of tools focused primarily on the detection and response of threats. By this definition we can imply that the SOC will probably exist in 10 years and perhaps even more.

Over the course of the past quarter of a century the SOC charter has evolved. Some objectives became very different, some much harder, some easier, and some stayed the same. The core functions of a SOC today include detection of threats, facilitating response to threats, providing feedback upstream to prevent future threats, as well as other auxiliary functions that vary by company and industry. How this gets done varies by each company, as the people, processes, and underlying technologies used by the SOC can be dramatically different from one organization to another.

Nevertheless, the SOC mission is to protect an organization from security threats by rapidly detecting and responding to attackers in the most effective way that mitigates the most harm. The SOC mission is certainly not about ensuring that the organization is never hacked - this is perhaps impossible.

The original SOC involved a large room of people watching display screens where curated alerts blinked into existence. Today, especially due to the nature of our digital-native and distributed workforce, there are many more virtual and federated SOCs.

Why was *your* SOC created? What value should you expect from *your* SOC today? There are definitely organizations that created their first SOC due to compliance mandates and other reasons such as industry requirements. If your SOC was created to satisfy an auditor request, it may or may not be realizing the higher mission of a SOC described above. Today, if you are managing a SOC, whether you are doing it fully in-house, involving an MSSPs and partners, or operating in a hybrid model, you should expect to see evident detection and response value.

In addition, while the need for automation continues to increase, the demand for humans in the SOC will persist for the foreseeable future. As necessary automation gets implemented, attackers will continue getting more sophisticated, and this will always require the creative human element to defend against. In light of this, we believe that the charter of the SOC will evolve heavily in the next 10 years, however, the mission will always remain the same. SOC mission only becomes more important in our digital-native world.

Why does the SOC need to transform?

Business Transformation

While the core mission of the SOC has very much remained the same -- detect and respond to threats to protect your organization -- their charter has exponentially increased in scope and complexity.

Technology architecture aside, the adversaries used to be fewer and farther between as building malware and penetrating organizations was not the most approachable of tasks. Nowadays, one quick Google search of “How to build malware” and you may find yourself deeply researching the many ways you can easily build undetectable malware.

Moreover, since the early 2000s when the concept of cloud computing started to take flight, the global number of internet users has nearly quadrupled from 1.2 billion active users to over 4.6 billion active users. Simply put, there are significantly more adversaries active in the world today. They are smarter, faster, and have access to more insight on a much more organized internet than any generation before them.

Now, we haven’t even got to the scope, size, and complexity of modern computing architecture. Modern computing architecture has become significantly more sophisticated with the advent of cloud computing. And through the economies of scale, cloud providers are able to drive businesses through a digital transformation at a fraction of the cost than the pre-cloud era.

With virtually all businesses going through this journey of transforming their products, services, and operations to be digital-native, the opportunity that exploiting an organization presents to an adversary is much more compelling than before. Mass disruption, financial gain, hacktivism, competitive intelligence and IP theft, or geopolitical motives are among the many intentions that have become and will continue to be more prevalent in the digital-native era.

This also presents a generous divide between the traditional enterprise businesses going through the cloud migration, versus the rapidly-launching cloud-native organizations. The cloud migration is an opportunity to transform the way businesses work, but also gives organizations a shot at reimagining how they secure their business and protect their end-users.

Through this transformation, there can be significant gaps in security if organizations are not adequately funding security programs and training their workforce through all of the changes that the cloud presents to them. How you design, operate, and manage security across your cloud(s) and non-cloud infrastructure requires a hefty investment towards reskilling your team to adapt to the new operating model.

An unfortunate common theme of many cloud transformations is that the SOC requirements get deprioritized when organizations have tight timelines and budgets to drive their teams to the cloud. The reason being, most SOC teams are too busy fighting fires and don't have the spare cycles to focus on adapting their use cases to cloud workloads and modernizing their own infrastructure. Missing this opportunity to modernize with the business only makes the threat management problem worse, as a cascading effect of perceived value causes a lack of funding among a plethora of other issues that minimize the efficacy of the SOC.

Many business leaders also assume that the cloud is inherently secure because there is a general misunderstanding of the shared responsibility model and the difference in preventive security vs detection & response to threats. Of course, they are partially correct - cloud infrastructure is certainly more secure than their data centers. However, their own usage of the cloud often isn't. Analyst firms often remind us that the vast majority of cloud security problems and data breaches occur due to the fault of cloud users and not cloud service providers.

Expanding Attack Surface

The rapid digitization due to COVID-19 forced people to look to technology for new ways to work and live at home. Everyone, including their kids, needs a laptop, webcam, and necessary office equipment to work & to attend school. Pair this with the transformation of massive industries such as health-tech, electric vehicles, fin-tech & decentralized finance, smart homes & connected appliances -- there is more than an exponential rise in the usage and dependency on technology today.

In the enterprise, the new cloud operating model presents the idea of microservices and codified immutable infrastructure that can be built, destroyed, and re-deployed on command. These same microservices are what power modern EVs, health-tech, IoT devices, and all rapidly transitioning industries worldwide. This microservices model has shifted the way which we architect the organizations' technology stack. In the past, we used to think of the castle and moat analogy and layered defense model centered around network defenses to protect organizations. But today, we're thinking of minimally-designed immutable infrastructure that is built-for-purpose and rooted in strong access control models.

Threat modeling still exists — and it's more important now than ever. However, it has evolved from the old monolithic days of infrequent threat modeling. Rather, it has to be hyper agile, baked-in to your iterative development lifecycle, and understand the context of all the new data sources, network paths, and access patterns that come with the cloud operating model. Strong threat modeling with your DevOps counterparts will help alleviate your SOC workload.

On top of that, while DevOps teams build, deploy, and manage this new infrastructure stack, the SOC doesn't usually have the inner knowledge of how the cloud technology stack works, most of the time due to the sheer fact that they've been to busy responding to incidents than having time to ramp up and build depth in cloud. Also, cloud has accelerated technology development, to where the industry evolves very quickly from service to service based on developer needs. Just 10 years ago, virtual machines were still the core of developer workloads, then PaaS models like Google App Engine, and now the rage is all about container-based architectures and serverless models that minimize ops time for developers. These new architectural paradigms present unique challenges to Security Operations teams who have struggled to keep up with the speed of innovation.

This growing technology stack, rapid digitization of the world, and expanding scope of enterprise assets has resulted in more data -- more data results in more unknown threats, more false positive alerts, and more noise overall. This is bad news for the ill-prepared workforces who have not been able to modernize and adapt.

On the flipside, the good news is that the cloud model is inherently more secure than on-premise models. The shared responsibility model of the cloud allows organizations to focus on securing only the necessary components that fall within their purview. For example, in the past it was very common to have to monitor all of your network flow logs for certain threat use cases like DDoS, whereas today, with Google Cloud's rapidly scalable and fully-owned end-to-end infrastructure, DDoS by attack has largely become a threat of the past for most modern workloads. There are countless more use-cases that the shared responsibility matrix takes on, so it's incredibly important to understand where responsibilities lie in the shared responsibility matrix as this gives you an opportunity to repurpose your workforce towards other jobs that need to be done. Moreover, Cloud Service Providers typically do a great job of onboarding and transforming the business teams to a more secure-by-design DevOps approach, where teams start to take advantage of building secure architecture patterns, configuration, and corrective

tools to prevent configuration drift. This new model is inherently more secure than what had existed in traditional on-premise environments... and Google Cloud evolves it further with Shared Fate approaches. Still, the difference now is that there are 4x more internet users today, exponential amounts of data, the value of data is increasing, and the reliance on technology is embedded in the DNA of our everyday lives.

Talent Shortage

Let's address the growing talent shortage head on. While we continue to hear about millions of unfilled roles in security, there hasn't been any meaningful impact from all of the work that has been done to try to fill this gap. This challenge won't be solved by just hiring more people as that has proven to be incredibly challenging and it will take more than just people to address the effectiveness of the security workforce. There are many issues contributing to this factor and there are also many ways in which we can approach this problem to both improve hiring, the growth of our talent, and their effectiveness, which we will describe later in this paper.

Cybersecurity can be a challenging industry to get into, even given a wide variety of career paths within this field ranging from operations, engineering, marketing, legal, UX, product, sales, and beyond. Within security operations teams alone, there are a variety of operational roles from analysts, to data scientists, incident responders, security engineers, and this continues to evolve as the SOC transforms to meet tomorrow's needs. The journey to navigate into these fields is not well defined or even understood, and there is often much friction between security purists and their necessary adjacencies.

Security teams are cost-centers, not revenue generating teams, so the case for headcount is always an uphill battle. On top of that, it is near impossible to quantify true risk in cybersecurity, for this reason, organizations sometimes don't invest in their security teams until a significant breach happens.

We also need to address the need for hiring more candidates from diverse backgrounds and seeding them for leadership positions. While the security profession holds a slightly higher representation of marginalized backgrounds in the field, this falls flat when it comes to representation in leadership positions. As noted in the ISC2 Innovation through Inclusion report, studies show, particularly a comprehensive study from McKinsey & Company, that organizations with racially and ethnically diverse leadership teams benefit both company culture and bottom line revenues, while also adding to the overall confidence of an organization's security posture. The problems that we're faced with require unique and creative approaches to problem solving. More teams that are representative of the real world will help us solve for the challenges we face in the real world, and more leaders who come from the various backgrounds in the real world will help inspire all of the security personnel to approach challenges from unique perspectives.

And let's face it -- education programs in the field often fall short. There is difficulty bridging the gap between technical practitioners and academics. This is most evident in the SOC, where the most talented practitioners are often analysts-by-passion and not by-education. The SOC needs to be aware of the adjacent roles that support their mission, while also finding ways to seed and ramp new talent, and building a connective layer of education to drive more awareness to this industry.

This is compounded with the rapidly evolving nature of technology and adversaries, where there is often much change to keep up with when DevOps teams are operated in fast-paced, rapidly iterating environments and Security Operations teams are trying to react to the latest threats without underlying knowledge of the systems at work.

By the way, to be clear, there is a very different mission between DevOps/DevSecOps and SecOps. One is focused on building, deploying, and managing code securely, another is focused on detecting and responding to threats. The former, often foregoing security best practices which as a domino effect, cascades into much more threat management work in a high-stress environment for the latter.

That high-stress environment that the SOC operates in is what inhibits growth. Most SOC teams are overutilized and burn-out is a common theme of these teams, whether entry level or senior. When the quality of life is affected, the quality of work is affected, that is why companies like Google have a rigorous approach to work-life-balance and mental wellbeing across their security operations program to ensure they're able to respond fast and respond effectively.

To compound this, the average organization is much less likely to attract top-tier security talent than companies that are known to innovate and fund their security programs. Think about organizations like Netflix, Facebook, and Snap who research and publish their work in the industry. We need a better approach to empowering within.

Solving for the talent shortage by strictly hiring more talent is simply not enough, we need to reorient our vision of the security workforce and we'll dive into how we'll achieve this later in the paper.

Why should future SOC be different?

The natural evolution of the world is only going to continue driving our human dependence on technology upward. Think about all the industries that have digital transformations underway -- autonomous electric vehicles, interconnected healthcare devices that regulate our bodies, brain-machine interfaces as depicted by Elon Musk's Neuralink, utility providers that supply our daily necessities. All of these industries are built on data. Compromises of these systems and this data are no longer a matter of leaked social security numbers and identity theft. Lives are dependent on technology, and cybersecurity will inevitably start to be seen as an honorable service in society as cybersecurity personnel exist to protect more than businesses and intellectual property, rather, protecting people from harm.

Tangentially, with all of these new data sources comes evolving computing stacks, and with new computing stacks comes new patterns and architectures attackers can take advantage of to achieve their mission. With an ever-increasing number of data, where it's projected that 50% of the world's data, or 100 zettabytes, to exist in the cloud by 2025 -- our current SOC model is not set up to proactively detect and respond to threats across that much data, let alone today's data.

Many of these new industries and technology stacks are built with a massive dependence on a third party supply chain. As microservices were created to break down functions within monolithic applications, companies themselves and open-source projects are coming into existence simply to prioritize the development and innovation of the smallest service that can make the biggest impact for organizations. This supply chain continues to grow and get more complex as data moves across organizations, environments, partners, and personnel at the speed of light. This complexity opens many opportunities for adversaries to get into organizations through these trusted relationships, and the SOC will need to be able to protect their businesses and consumers against a seemingly insurmountable problem.

While the mission remains the same, the future of the SOC is very different from what we have been operating over the last several decades. If we want to get ahead of the exponential influx of data, highly persistent and growing number of adversaries, never-ending talent shortage, and the criticality of cyberattacks - we need a new model. We need a model that enables the SOC to break out of its rigid, centralized silo and "operations center" and focuses on outcomes.

Let's reimagine the SOC as a security operations center of excellence, that has no constraints to its existence, but rather, solves security challenges through an engineering-centric approach to develop scalable and provable outcomes -- in a similar light of their DevOps counterparts. No more hiring for geographical talent, rather, hire to creatively problem-solve outcomes for the security use cases that your business is challenged with, wherever the talent may be. The management of modern-day threats needs to be an autonomic function of an organization, where Security Operations activities flow naturally with the rapid growth and evolution of people, processes, and technologies. We believe that achieving a state of **Autonomic Security Operations** is the answer to the SOC of the future.

What is Autonomic Security Operations?

Autonomic Security Operations is a combination of philosophies, practices, and tools that improve an organization's ability to withstand security attacks through an adaptive, agile, and highly automated approach to threat management. It is built on four pillars of exponential improvement:

- 10X People
- 10X Processes
- 10X Technology
- 10X Influence

You need to exponentially improve the abilities and effectiveness of your people. Distribute and automate your security processes and workflows. Leverage cloud-native technologies that can operate at planet-scale with minimal operational overhead to focus on solving security challenges. And lastly, have a deep integration and significant influence across your organization to improve the efficacy of your preventive defenses to minimize the amount of threats that your team has to detect and respond to.

Achieving an autonomic state of existence for Security Operations is not measured by the success of one pillar, rather, the improvements you make across all four pillars will synergize to exponentially improve your ability to manage modern-day threats at scale.

Rid yourself of the idea that a SOC is a room full of people looking at a screen with fancy dashboards. Whether you call your team a Detection & Response team, Security Operations team, or you are a SOC, we believe that the future of security operations demands that we solve challenges with distributed workforces who integrate with cross-functional teams across organizational risks to achieve a state of autonomic and operational fusion. Focusing on the skills needed to creatively develop and engineer scalable solutions to modern threats is paramount to protecting organizations against their risk categories in today's day and beyond.

10X People

To be 10 times more effective with the people component, your SOC cannot achieve this by increasing the personnel by a factor of 10.

As of today, both threats and technology resources that need effective security are increasing at a much faster pace than people entering the workforce. SOC personnel shortages are often less about a lack of people, but about having the right approach with the right talent to creatively problem-solve security use cases that organizations may face. It is absolutely impossible for most organizations to 10x their headcount in a SOC. Even when companies have a significant breach, the SOC usually fades back into the background after the business has recovered and the new injection of capital usually goes towards hiring security personnel across the board. Thus, SOC “burnout” is a real problem.

This talent shortage challenge is not dissimilar to the challenges that traditional IT Operations teams operating in a NOC had faced. Before DevOps, there was a world with Developers, QA, and IT Operations teams. IT operations sat in a NOC responding to availability incidents, and these same challenges the SOC faces today existed among these teams. When DevOps came to light, the philosophy intended to eliminate the silos, advocate for an automation-centric approach, and drive a heavy emphasis on transparency, collaboration, continuous improvement, and deployment. This way, they were able to be upskilled while also leveraging technology to distribute the work and drive utilization downward to solve similar burnout challenges.

For a more highly specialized operations team, the idea of Site Reliability Engineering (SRE) came to light from Ben Treynor Sloss at Google. This team's core focus was to spend 50% of their time on operations and 50% of their time on automation, acting as a force multiplier and engineering scalable outcomes for deep-rooted operational issues. Perhaps, it's time to shift our thinking in security operations to be more like Site Reliability Engineering (SRE). Don't be surprised, this is actually how Google and the transformative Security Operations teams of the world operate today. Detection engineers develop solutions to solve detection challenges at scale and not shuffle through traditional analyst workflows. They also manage the alerts their solutions create, and use that data to further refine their detection logic.

In light of this, we think of a 10x People improvement as the following:

10X analyst productivity and effectiveness

An exponential improvement in your analysts productivity and effectiveness will be centered around the transformation of people, where people will be empowered to automate, upskilled to solve high-order challenges, and augmented with technology that can increase their abilities and throughput.

At Google and across other industry-leading security operations teams, the role of an analyst is not simply to manage cases and perform tier-1 level work. Analysts are engineers, architects, project managers, and are empowered to be leaders of their subject matter focus. At such a SOC, the concept of Level 1 to Level 3 analysts is a thing of the past, rather, you should organize teams based on aligning skills to the use cases that fall under their purview.

Getting your analysts to take on a much larger scope will require a significant cultural shift in your SOC, so your ability to inspire and empower your team to think differently is a critical element of this transformation. Reinforced learning, stretch opportunities, problem-ownership, and career alignment can help you build a more talented and goal-oriented workforce. Also, talent can be and should be sourced beyond the staff you hire within your SOC. It takes a lot of time to hire, ramp, and seed talent in your pipeline. Partners, contractors, and service providers can provide key functions like consulting, advisory, engineering, and operations capabilities to help fill gaps where you may not have the capacity at the moment. There is no reason why you shouldn't take advantage of all of the people at your disposal to achieve your mission.

This will also need to be paired with a conscious approach to work-life balance, rotations, and meeting your team where their needs are as there is no 10X productivity if your team is suffering from burnout and poor morale. Humans operate at their highest productivity when they're not suffering from decision fatigue and operating in a state of anxiety. Doesn't this sound similar to the evolution of software development? We continue finding ways to abstract the unnecessary things away like building and managing servers so that engineers can simply focus on code and doing what they were hired to do.

We cannot achieve an exponential improvement in productivity and efficacy without a heavy emphasis on automation. Automation takes shape in many form factors, as a means to simplify the log ingestion and management process to the ability to manage detections or specific workflows at planet scale. Automation augments a human's abilities in the SOC, where humans can achieve outcomes they are incapable of alone, henceforth improving productivity and effectiveness. There will be no robots who replace the SOC in the near future, simply due to the fact that as defenses get smarter, adversaries get smarter as well. You will need to approach all problems with an automation-first mindset so that you can minimize the ops time of your team and have them focus on higher order tasks. After all, the alert fatigue issue will only grow as data grows.

10X coverage of threats and assets

As the attack surface increases, the need to cover more assets — more old and new, from mainframes to clouds - requires the SOC to not only increase their coverage of assets, but also get ahead of evolving data sources so that they are not an obstacle to rapid technological growth.

Using automation for achieving — or at least getting close to — complete coverage of monitored assets is one example. After all, there are no “rogue servers” in the cloud and every asset can be found via an API.

As IT around the SOC adopts DevOps and other related approaches, the SOC needs to be plugged into the new systems of record, new change management and other modern infrastructure elements.

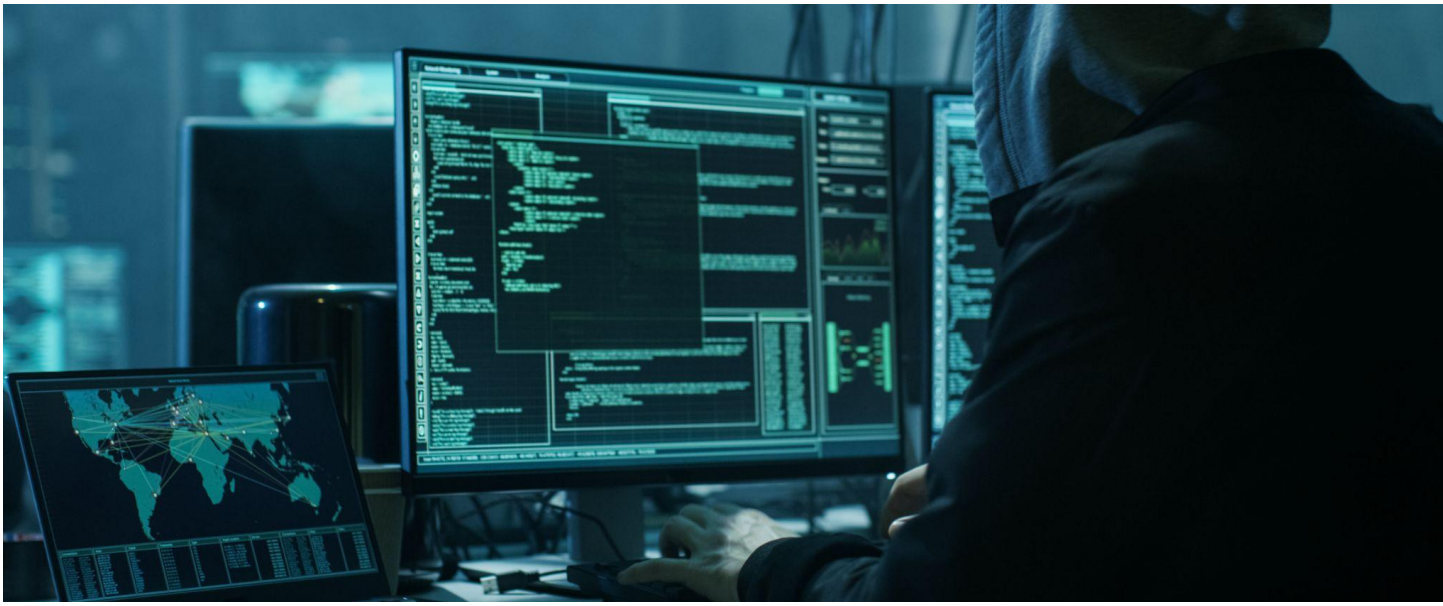
FInally, as applications become more secure by default, the SOC will be 10X more likely to focus on the threats and challenges that truly necessitate human involvement.

10X knowledge sharing

For many years, many in the industry have lamented that attackers share information more effectively than the defenders. Whether it applies to intelligence sharing or sharing tools, defenders have lagged behind in many cases.

Achieving a 10X improvement calls for a dramatic increase in defender sharing. Cloud providers aim to play a key role in both threat and safeguard sharing. As detection content formats like Sigma and YARA-L become more prominent, open sourced and community detections will grow, therefore boosting SOC data sharing and ultimately productivity.

Community repositories of detection logic (like SOC Prime and various GitHub repositories of detection code) also boost industry and cross-company sharing, thus increasing the overall resilience against cyber attackers.



10X Process

Making old and stale security processes run at 10X speed seems like an implausible endeavor. However, given the threat landscape, evolving (and growing) attack surface and more alerts from a wide array of security tools, we need to develop an adaptive approach to optimizing new and existing processes.

Automation plays a big role, such as for turning human time of minutes or even hours into machine time of seconds for many routine SOC tasks such as enrichment.

SOC process automation, such as via Security Orchestration Automation and Response (SOAR) tools, delivers 10X speed, but also 10X consistency and 10X traceability and auditability. This means that the security operation processes would not only run faster, but will have fewer mistakes, higher consistency in achieving the same outcomes, as well as much higher auditability. Auditability would be useful for multiple purposes, and not only for audit and compliance. For example, it would be much easier to perform blameless postmortems after an incident and execute continuous improvement activities. It would also simplify reporting and metrics on security operation activities delivered to senior management. Auditability also serves as the checks and balances system for automation. Most security teams distrust automation because many issues are not a one-size-fits-all approach, so naturally, we need to review the work our machines perform to ensure they meet their expected outcomes.

This may get the SOC to dramatically reduce the MTTD and MTTR metrics - time to detect and time to respond. Note that time to recover is harder to reduce, but as cloud computing increases the automation capabilities, including for remediation activities, time to recover will naturally follow suit. Pairing up automation for detection and triage with well-defined playbooks for remediation can also accelerate your MTTR. Future AI will learn human activities and then create recommended playbooks automatically.

When detection tools respond to queries fast (as Chronicle does), all detections are converted to detection code, automation is implemented, and fewer “human-speed” processes are in place, it is very clear how MTTD can improve by a factor of 10. Thus, your SOC involves towards Autonomic Security Operations.

The origins for dramatically faster time to respond (MTTR) are similar: automation, consistent and predictable processes running at machine speed, as well as effective knowledge sharing for identifying the priority of an incident, backed up by robust threat intelligence.

This does not mean that an advanced nation state intrusion can be resolved in minutes. Top tier threat actors and the incidents they cause may still require human experts, operating at human speeds, taking time to figure out what exactly happened. That said, automation does free up time for humans to focus their efforts on the more sophisticated attackers instead of dealing with the bulk of alerts, which may be less likely to impact the business.

Now, how can one achieve dramatically faster development of detection content such as rules and models? Naturally, this process starts from effective threat intelligence collection practices as well as a robust process for turning intelligence into detections.

Finally, a 10X improvement would also entail having much less toil and dramatically less process friction, both within the SOC, and between the SOC and other parts of the organization.

10X Technology

Many SOCs struggle with their security products, both inside and adjacent to the SOC. With the average SOC carrying dozens of tools in their toolbox, tool sprawl is a real challenge. Pair that with the lack of deep interoperability between products, vendors, and use cases and you have a really fun juggling act in the SOC.

Technology will need to drive towards a more unified approach, even with highly differentiated capabilities and very separate intentions. That means that technologies will need to start having more semantic awareness of their adjacencies and integrations, so that the workflow in the SOC can truly be optimized and we don't spend too much time re-training our tools to think the way they should be operating. The old days were about monolithic thinking, how can we pair every feature and function into one product and try to solve threats. This clearly doesn't scale when the world is eliminating monoliths from their technology stacks and migrating to purpose-built microservices stacks that combine to solve for the business needs.

In the SOC, we'll need to start thinking about our tools in this same microservices-like fashion, where we engineer our use cases with a stack of technologies that can be positioned to achieve the expected outcomes, all while ensuring our technology stack has that deep semantic awareness of it's adjacencies. So, in light of that, there are a few key priorities to think about when achieving 10X improvement across your technology stack.

10X Visibility

Many organizations realized that their SOCs must have complete, comprehensive visibility over all security activities and all their assets, whether on premise or across clouds. After all, you need a threat actor to exploit a vulnerability against an asset for there to be a risk.

This is much easier said than done, especially when organizational IT has grown in layers, from mainframes to VMs to containers and now serverless stacks over the course of decades. However, a modern SOC must be able to deliver complete visibility, and this means you are relying on more than logs, but also on endpoint, network, IoT, cloud telemetry sources, signals, and whatever happens to be next.

The visibility of data can also be increasingly useful when it is enriched with deep metadata, as this provides the SOC the ability to assess reachability, identify lateral movement opportunities, assess the blast radius and further drive down MTTR by reducing investigation times with rich context at the investigators disposal. Leveraging powerful visualization technologies like Looker can improve your SOCs ability to stitch together a story and have critical insight into the interactions happening across your environment.

These requirements indicate not only ability to collect, normalize and enrich the data collected but also your ability to scale as the needs for visibility increase. In essence, such comprehensiveness should not come at a cost, and should not come with a speed handicap.

10X Speed

Many of the security operations centers that started with traditional Security Information and Event Management (SIEM) products in the 1990s are used to very slow query speed. It is not uncommon to have data searches and reports that require the user to take a coffee break, and, in the worst case, a vacation. Today's speed of digital business makes this an unworkable timeline for security.

While modern SIEM products would typically produce results within minutes, that is too slow for a 10x SOC. In light of this, one obvious way to deliver a 10x technology stack is to improve the speed of data retrieval, searches, reporters and dashboards by a factor of 10. Fortunately with products like Chronicle this is easily possible and achievable as it's built on Google's backbone and highly performant technical infrastructure. Normalized data searches across any time frame regularly run in a quarter of a second in Chronicle, and it operates at petabyte-scale and years of data.

Many organizations collecting telemetry data still struggle with data collection and specifically with data source onboarding. For example, while it is technically simple to connect certain supported data sources to an SIEM, it may require a security team to reach across organizational boundaries and face friction. Moreover, the data sources may ultimately be integrated in the security tool, but then lack the semantic awareness in any of the other tools in the stack.

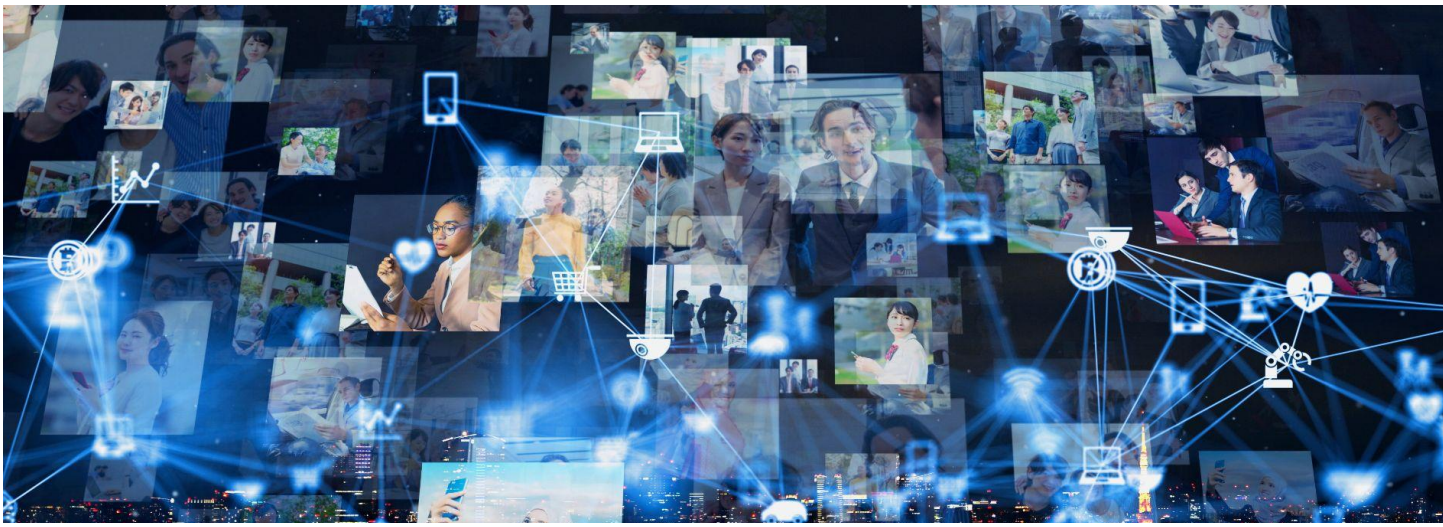
In light of this, a 10x improvement requires dramatically increased speed for data source onboarding and needs a normalized approach to its underlying data model that is consumable by its integrations without having to re-engineer the context. Fortunately with modern cloud data sources such as those on GCP such immediate onboarding with a unified data model is very much a reality.

10X Signals

Many security vendors promise dramatically clear signals and improved detection quality. However, this is very difficult to achieve on real threats acting in real environments. For example, no product that relies on searching raw log data can predictably deliver good detection signals without significant work by the security team.

This means that good quality detection and investigation signals require that the product process the data upon collection, fuse the data into a coherent timeline and the story, and provide a clear path to actionable insights for the end users consuming the signals.

This will also ensure that signals are more clean in nature, and that we can drive down the issues with alert fatigue due to signals that are just built on static environments and a lack of contextual awareness. If we want to battle the alert fatigue challenge, the quality of detection signals will certainly play a significant role in driving this down.



10X Reduced TCO

Every CxO will need to ensure that the tools they invest in are aligned to the outcomes they expect from the money spent on the investment. In security, it is nearly impossible to quantify risk management, so the case for optimizing cost is always top of mind for every CxO. The #1 concern is, “we spend all of this money on these products, but, we’re still unsure whether we’re secure or not”. So while this paper is not focused on philosophizing a possibility of quantified risk management so that you can provide your board with a clear number of revenue harm that you mitigated with your security tooling, we need to make a point that the modernized SOC does a much better job of optimizing their TCO across their security stack.

With the advent of the cloud, organizations can exponentially increase the value provided by their technology stack by shifting from traditional capital expenditures to operational expenditures that provide added benefits of transferring management responsibilities to the vendor or CSP. It’s no mystery that the shift to operational expenditures is the direction of all industries. Security personnel should be focused on security, not on infrastructure management. Yes, there is certainly less flexibility when you don’t own your entire infrastructure, but if you focus on the outcomes you’re trying to achieve with your use-cases, you can take advantage of the extra labor hours and personnel to focus on higher order challenges. This reduction of operational overhead is not an elimination of headcount, rather, it is reprioritizing your personnel to focus on creatively engineering better results, focused more on security, while your cloud service provider can handle scalability and other responsibilities.

Security Operations is also a really expensive capability to maintain. At the core of it, it’s a gigantic data lake that has an exponential growth in data, and has an exponential growth in operations and manipulation of the data. As more businesses migrate to the cloud, as more industries become transformed through technology, this massive data lake will continue to grow at an unimaginable rate. Unfortunately, Security Operations is also constrained by a budget and does not have an infinite money pool, so organizations need to be very careful not to sacrifice security for a need to control. Rather, sacrifice the need to control by migrating to cloud-native tools and managed services that offer better pricing economics, therefore optimizing your budgets. That way you can use extra money towards enhanced coverage, talent, and other use cases.

10X Influence

The SOC can only truly be 10X and transformative if it also has strong influence over the upstream elements of the security lifecycle. You can make a significant impact on the amount of alerts that get into your SOC if your team has a strong integration with your DevOps practice. A deep understanding of how infrastructure and applications are securely built, deployed, and managed across your organization paired with your ability to influence this design can only improve your ability to catch attackers at their earliest onset, or even better, prevent them from getting in entirely.

Approaches like zero trust, when well implemented, really cut down on the noise that SOC analysts and engineers have to deal with. Especially with modern-day computing stacks that are heavily centered around access models, paired with a global and remote workforce, the need to shift towards zero trust access models is more important now than ever.

Your vulnerability management program is one of the most important elements of achieving a state of strong defensibility of your organization. Vulnerabilities need to be caught, prioritized for criticality, and patched on the fly. Driving towards a state of automating patch management is critical to building a strong security posture, while also catching the vulnerabilities caused by errors (i.e. misconfigurations) and correcting them automatically. After all, misconfigurations are the largest cause of breaches. How can your SOC truly defend your organization when a developer had privileged access and opened up your firewall to the world? An exponentially more effective SOC has a deep understanding of the vulnerability management process and how it's integrated into the development lifecycle, as well as the controls that are in place to prevent developer mistakes.

Developer mistakes happen and will continue to happen, even as tools automatically catch and correct configuration drift. Sometimes the configuration may not have been defined well from the start, so monitoring against a poor baseline may not prove much value. In a world where blame has netted no results, a key skill needed to drive influence across the adjacencies is developer empathy. Following an empathy-based approach will help you understand deeply rooted security issues and how you can tailor your solutions to adapt to developer needs at scale.

The modern SOC absolutely has to have influence across their adjacencies to improve defenses, minimize the amount of alerts that the SOC needs to action on, and drive a better and continuous feedback loop to action on identified threat vectors in the SOC.

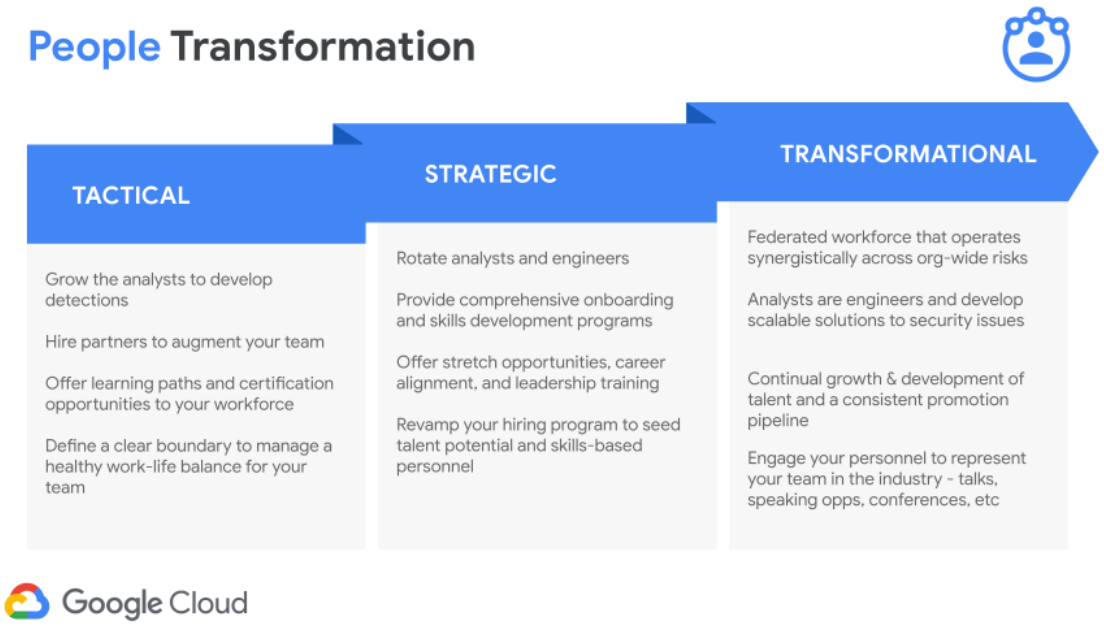
How to achieve Autonomic Security Operations

Transforming your SOC from a reactive operations room to a state of Autonomic Security Operations is an aspiration that won't be easy. Similar to the cloud transformation, a program of this scale is a multi-year journey that will require deep investments from your leadership, organization-wide evangelism, and the help of partners who can support you through this journey.

Don't forget, achieving a state of Autonomic Security Operations is a combination of philosophies, practices, and tools that will improve your organization's ability to withstand security attacks. There is no single metric to describe when you're in this state of existence, rather, when you are able to achieve exponential improvements over the four pillars of people, process, technology, and influence, your key Security Operations metrics will follow suit.

Whether you're a small DevOps-centric organization that needs to take advantage of MSSP offerings, or if you are a large enterprise that wants to DIY, there are several themes which we'll discuss to help you transform your SOC, centered around the four pillars.

People Transformation



One of the foundational principles of advanced security detection and response teams, such as the one at Google, is that people who are researching threats, developing detection logic and those who respond to alerts and other signals are the same people.

Philosophically, you can think of it as a sort of DevOps for security operations where people who develop the code (in this case, detection logic) are the same people who operate it (in this case, respond to signals and alerts). The engineering characteristics for detection engineers are not necessarily the skills of software engineers, rather, they need to be writing queries, rules, automation scripts, building playbooks, manipulating data sources, etc. These skills can be developed at scale by hiring security engineering managers who are also inspirational leaders and can take a hands-on approach to upskilling an entire team.

As you start to invest in your teams, think about all of the concepts we discussed earlier about intrinsic human motivation, goal setting, talent acquisition and seeding growth within your teams. The DevOps philosophy was more than just a statement of recommendations, it became a way of life for engineers who championed this belief system.

You should also absolutely take advantage of industry certifications. There are concerns that practitioners will raise against certifications, but the reality is that certifications provide a plethora of benefits with no downside.

- Certifications provide theoretical knowledge to upskill your workforce at a low cost.
- Certifications offer diverse & underrepresented groups accessibility into the field, a critical and largely untapped workforce in the battle against growing adversaries.
- Certifications help security professionals become more effective communicators & build influence across their adjacencies by building foundational knowledge beyond their core subject matter of expertise.
- Certifications help recruiters filter through preferred candidates by finding talent who has the skills more closely aligned with the SOC roles.

The SANS Institute offers a lot of hands-on technical training programs & certifications particularly geared towards Security Operations professionals. ISC2 and ISACA offer technology-agnostic certifications that help your Security Operations personnel understand the bigger picture and the lifecycle of an attack beyond what happens in the SOC. Cloud certifications offer your SOC teams the ability to gain depth and subject matter expertise in the cloud that they operate in. There is a reason why the Google Cloud Professional Cloud Architect certification is the highest paying certification in the world. These cloud certifications are extremely comprehensive and for the reasons above, you should be incentivizing your workforce to pursue extended learning opportunities while also building on their hands-on technical skillset and investing in their career growth in parallel. A good rule of thumb is to consider allocating 20% of your team's time towards knowledge sharing and learning.

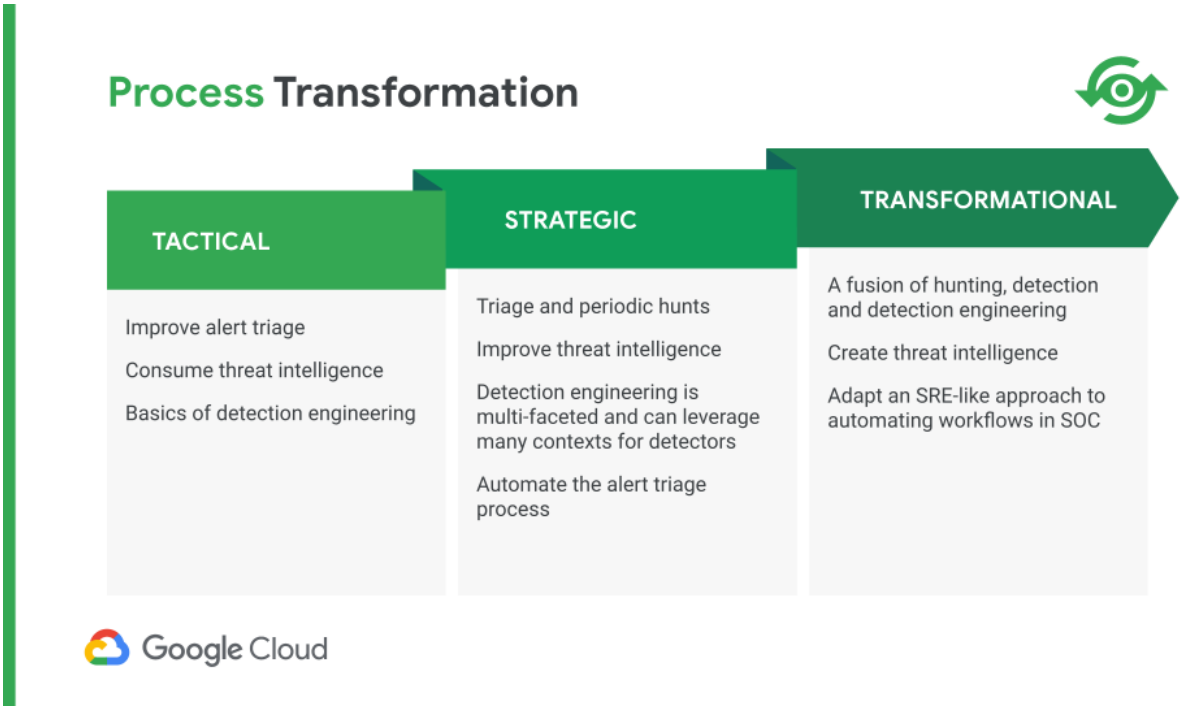
Beyond certifications, organizations like the SANS Institute offer several paid and unpaid learning opportunities, and there are many regional Information Sharing and Analysis Centers (ISACs) that allow practitioners to knowledge-share and learn from one another. These also offer opportunities for your people to become thought leaders and engage in tangential activities to upskill and uplevel their abilities. Oftentimes, having peers and mentors outside of your organization can offer new insight into problem solving.

Think about how you can partner with your organizational leaders, including talent management and human capital teams, to bring an exciting new light to the battle against the adversaries.

Five key actions to take:

- Remove walls in a SOC that separates analysts and engineers
- Identify skills needed in your SOC, start to hire skills, not levels
- Boost productivity with automating routine tasks (via SOAR & managed services)
- Take advantage of partners & 3rd parties
- Create a culture of extended learning, empowerment, and innovation

Process Transformation



Improving security operations processes sounds like a boring task, but process excellence does separate the 10X SOC from a minimally-performant SOC that may not be able to manage the threats the organization encounters. There are several dimensions for improving it in the SOC.

However, one of the key principles to keep in mind is that an excellent security operations team has both a consistent and predictable process set, but also leverages human creativity necessary to fight the top-tier attackers. Fighting automated attacks is typically easier to defend against as signatures and patterns are identified and the scale of the cloud can handle things like distributed attacks. Fighting highly persistent adversaries that take their sweet time maneuvering through your environment, even weeks and months, is a challenge that requires human thinkers to solve.

Thus, improvements to process will need to boost consistency without derailing and ruining creativity of the human analysts. Balancing this is difficult, and some processes definitely focus on consistency, such as consistent alert triage. On the other hand, some processes, such as threat hunting and red teaming (a process adjacent to SOC), definitely skew heavily towards more creativity.

One of the key processes to improve is of course the detection engineering process. To deal with the threats that your organization faces, your SOC will need to create detection logic, whether in the form of the rules or algorithms and machine learning models.

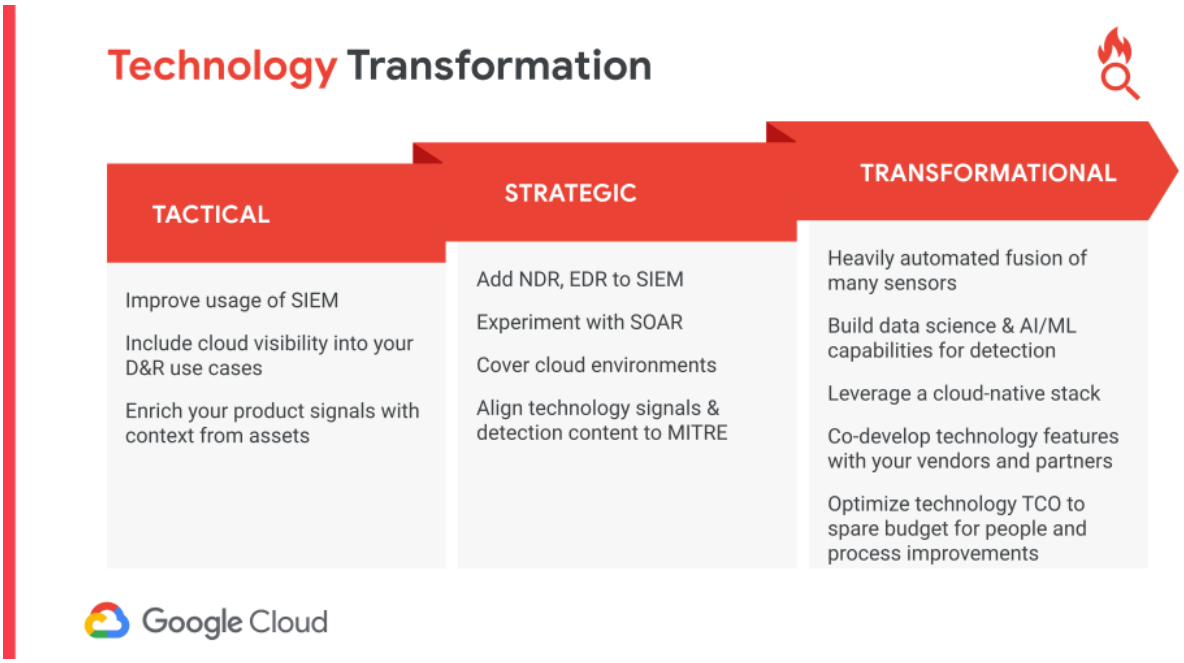
Also note that for some organizations process improvement will not take until the transformational stage. For example, organizations that do not do any threat hunting or intelligence creation practices would need to create those processes from scratch and then refine them.

Some organizations that are starting their SOC journeys start with the detection logic provided by their vendors, then evolve to tuning and refining, and then evolve to their own detection logic. At transformational stage, your own threat research and custom threat intelligence as well as hunting operations and incident response will create and refine your detection content.

Five key actions to take:

- Solidify the basics; don't hunt before you can detect well
- Focus on threat intelligence to boost other SOC work
- Drive an "SRE" approach - evolve to 50% time towards automation work
- Add hunting, testing and analytics afterwards
- More transparency will allow more creative problem solving

Technology Transformation



For many organizations, transforming security technologies is difficult. This may be due to entrenched interests, expensive products, and lengthy support contracts. Many of the technologies that are in current use such as SIEM actually have a use in a transformed SOC. Many of the improvements to effectiveness of these technologies is about leveraging your highly talented teams to improve how the technology is used and optimize the processes they interact with. They are not really about replacing technologies in bulk.

However, as organizations evolve and migrate to the cloud, new visibility areas are needed. For example, for many organizations, strategic improvements happen when they evolve from simple log analysis in a SIEM to more automated tools such as Endpoint Detection and Response (EDR) and others. A heavily automated fusion of many sensors covering on premise and cloud environments, shift towards managed services that abstract some responsibilities to your service provider, and automation via SOAR & product differentiators will take you a security operations technology stack to the next level.

Good SOCs utilize automation in data collection to minimize ingest errors and normalization issues. They also use automation to improve detection with Machine Learning (ML), EDR and other technologies. They automate triage to remove false positives and dupes, categorize alerts more accurately, prioritize alert queues and more. They use automation and scripting to automate the enrichment process of data and then pump things back into the triage queue with additional context in the event that the alerts can be automatically closed or re-prioritized with the new context. They can also drive remediation playbooks actions as well.

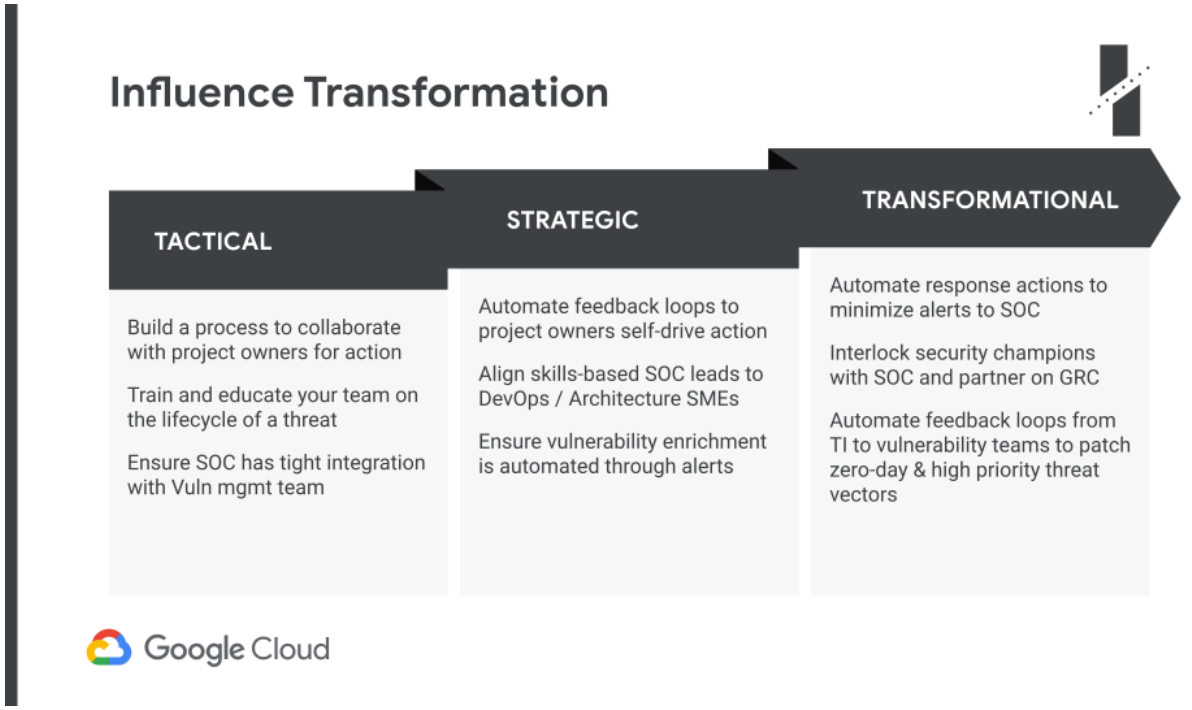
Building automation in particular is very challenging for many organizations. Most SOC-built automation is typically centered around deploying, implementing and utilizing a SOAR tool. But the reality is that you can increase automation by using technologies with differentiated capabilities, as well as ways of receiving technology (i.e. via a managed service model). The sum of all your automation efforts can add up to solving a lot of blind spots so that you can optimize your ops time to focus on higher order security challenges. At later stages, using machine learning and other systems helps automate not just routine but also cognitive tasks in your SOC.

As of today, don't assume that machine learning would deliver magical effectiveness. For highly talented organizations that have ML teams, it takes deep scoping of use cases and datasets to identify opportunities to leverage ML to solve a particular challenge at scale. Due to the high cost of the economy and lack of maturity for ML use-cases here, it’s going to take some time before ML is able to provide the effectiveness it’s promised to provide. As industry observers note, machine learning and similar technologies would likely offer incremental improvements, not game changers, for the near future.

Five key actions to take:

- Don’t discard a SIEM unless you’ve engineered solutions for their use cases
- Expand visibility: NDR, EDR / XDR, cloud, etc
- Be aware that cloud-native security tools will win in the end
- Use SOAR to automate the routine tasks
- Use ML, but don’t expect magic...

Influence Transformation



Building a highly influential team of security operations experts is going to be one of the most rewarding elements of a transformative SOC. The SOC is the closest team to the attackers, so naturally, if they're in a position of influencing upstream and downstream, they may have the most impact in solving security challenges across the organization.

The best SOC teams have a lot of contextual understanding of how things work in the build side of the world. Without this understanding, it's really difficult for SOC teams to have a lot of influence, and oftentimes this leads to shadow IT. Also, if you plan on doing any sort of response automation, you can cause a lot of damage if your automation goes wrong and takes down a production environment. Build deep relationships with your peers, have strong interlocks, and educate your SOC on how to understand the threat models from the beginning, that way you can truly engineer intended outcomes.

Remember, you need an asset, a vulnerability to exploit, and a threat to exploit it to be attacked. So, while vulnerabilities in practice are oftentimes referred to as just code vulnerabilities, the reality is, "patching humans" is equally as important. So, in order to have a lot of impact, you not only have to ensure your vulnerability management team is patching software and has access to your threat intelligence to catch critical vulnerabilities -- but you also need to ensure you have security champions across your development teams to catch the end user vulnerabilities and properly threat model in their development lifecycles. It is also important to ensure that your vulnerability management team is driving actions within your organization to reduce the rate at which new vulnerabilities are being created. Don't forget, you should also correlate the data from your vulnerability management tools with your threats in the SOC to enrich your findings and have more effective outcomes.

Your SOC may be focused on detection and response, but don't forget the value they can provide to the rest of the organization. The influence they have across their adjacencies can drive exponential impact across the program they manage within the SOC. Moreover, if they're able to outsource their knowledge and become thought leaders across your organization, it will only increase the budgets that are provided to your SOC team and their perceived value.

Key Steps To Take

- Educate SOC on the upstream impact of changes (DevOps)
- Don't miss the opportunity to modernize relationship with the business
- Build deep relationships & regular interlocks with SOC adjacencies
- Document the lifecycle of an attack for all created detections
- Ensure key teams get access to SOC context to patch the right vulnerabilities

Conclusion

The intention you set forward to drive your SOC to a better state of existence will pay dividends in the future as you start to realize that you are solving more unique challenges in the world and more people want to come work for you. This is certainly a multi-year journey, but this guidance will provide you with a mental model of how you should be thinking about driving change in your organization. This is certainly not solely the work of your CISO or your SOC leader -- you should take this knowledge and evangelize it across your teams. Consider putting together a “tiger team” focused on planning out how your charter will evolve over the next 30 days, 6 months, and years.

At Google Cloud, we’ve been hard at work building a solution to partner with organizations large and small on this transformational effort towards **Autonomic Security Operations** together. We can help you protect your organization against modern-day threats, whether your digital assets are deployed in our Cloud, on-premise, or other clouds.

By partnering with us on your path to achieving **Autonomic Security Operations**, you’ll have a true modernization journey within reach that will transform your organization’s ability to detect and respond to digital threats, as well as the opportunity to pioneer threat management together.

Whether you’re taking this transformation journey on your own, or you’d like to partner with Google, we’re here to provide valuable insights and help along the way.