Deloitte. | Google Cloud

FUTURE OF THE SOC

PROCESS CONSISTENCY AND CREATIVITY: A DELICATE BALANCE

Introduction

As an industry, it has reached the point where the presence of an enterprise scale Security Operations Center (SOC) has become nearly ubiquitous at large organizations. Gone are the days of selling the importance of centralized log collection, the necessity of security tooling such as security information and event management (SIEM) and budgets and championing the need for a highly trained team of cybersecurity specialists. The question to ask now is "How do we evolve the existing capabilities within our ever present SOCs to match the rapidly changing business environment and threat landscape?"

Under the current onslaught of threats such as ransomware, many organizations continue to struggle to find the right balance between prevention, detection, and response security capabilities for their organizations. For larger organizations, it means building, refining, and evolving their SOCs.

> An interesting analogy for the inception and evolution of the SOC is aircraft safety. It was only a few decades ago when aircrafts were something that were made by hobbyists and were able to be flown anywhere there was sky. Over time, the industry realized that with so many airplanes and pilots there needed to be some level of regulation and process. The Federal Aviation Administration (FAA) was born, together with regulatory agencies of other countries, to provide needed regulation. The processes by which planes stay airborne became highly controlled using automated computer systems, and in general, the processes by which pilots interact with air traffic systems became rigid—but safe!

What has not changed, however, is that humans are still responsible for creatively navigating by exception. In 2009 when Chesley Sullenberger deftly landed Flight 1549 in the Hudson River in New York it was the pilot that did so, as there was no procedure or automation to solve for a massive bird strike upon take off. This example underscores the point of this paper; highly standardized processes can provide an effective baseline for system development, but human innovation and creativity is still required to obtain success in extraordinary or dynamic situations. In order to operate in the world today, the modern SOC needs to build processes to adapt to both sides of this coin.

Coming full circle, the important point of the SOC process is that there needs to be a thoughtful distinction drawn between where a SOC should have a tight, repeatable, measurable process, and where a creative pilot can perform maneuvers like landing on a river when the metaphorical flock of birds are hit. This paper highlights ways to create a consistent set of core processes, yet still allow room for creativity within the process set for your SOC.

Chronicle

SOC basics reimagined

So if we as security professionals accept that the state of Enterprise Security Operations needs to evolve, we must admit that attaining that evolution will be a complex challenge—and with any complex challenge, in order to solve it we must have a solid understanding of why we are where we are today. The SOC is continuously under siege with an oversaturation of tools and data. In order to cope with the flood, security organizations often fall back on their existing processes as a guide. As previously stated, those processes may be built upon decades of old thinking and may be in need of a refresh.

Let's take a look at what a security blanket of the operational process may look like. The model SOC of the early 2000s was likely built around the following core processes:

- Vendor tool-driven alert triage using a "follow the sun" model with defined handoffs
- Compartmentalized Incident Response (IR) with documented Standard Operating Procedures (SOPs) including formal incident declaration steps
- Atomic use case design and development processes and subsequent analyst playbook development
- Mostly static reporting
- Intelligence consumption built around vendor provided feeds of atomic indicators of compromise (IOCs) (that may or may not have been integrated with tooling to drive detections)
- Point in time projects to gather data on environmental knowledge, including Configuration Management Database (CMDB) verification, asset enumeration, and data flow assessment
- Outsourcing of operational components used for select security processes to reduce operational cost and allow for "follow the sun" operations

Strong thought out processes are sometimes (unfairly) seen as the most boring of the people, processes, and technology triad. But they are what differentiate mature organizations with capabilities from those with a collection of the latest shiny toys. What's important to acknowledge is that all the functions and processes above are still important today and should not be jettisoned as a foundation for operations. Rather, they should be simply that, a foundation from which we build, rather than the primary focus of the program.

Let's take a look at the same list of core processes from the early 2000s SOC model to think about what operations could look like if the most fundamental elements were solidified in process, but were enhanced by incremental improvements using modern technology and creativity.

LEGACY PROCESS	***ENHANCED PROCESS***
Vendor tool-driven alert triage	Automated triage and queue management that logically processes known outcomes and reduces alerts requiring human intervention
Compartmentalized (IR) with formal incident declaration steps	Cross train SOC personnel so operators can take IR actions to contain and remediate low severity incidents without formal IR process
Atomic use case design and development processes and playbook development	Agile development of detections and detection tuning managed by operational teams on the fly
Static alert-based reporting	Near real-time dashboarding accessible in "self-service" models
Consumption of vendor feeds of atomic IOCs	Automated scoring and aging of indicator lists coupled with automated degradation of indicator value based on source quality and investigation responses
Point in time projects to gather data on environmental knowledge, including CMDB verification, asset enumeration, and data flow assessment	Continuous data collection from network devices and endpoint tools drive asset inventory
Outsourcing of operational components used for select security processes to reduce operational cost and allow for "follow the sun" operations (hybrid SOC theme continues)	Seek vendors that extend service beyond simple triage and escalation to response and remediation activities

Although the advancements above shows improvement, the list of processes is not completely adequate for today's world. Let's take a look at areas of true evolutionary growth that modern SOCs should consider pursuing.

New SOC processes:
"This is not your grandfather's SOC"

Beyond incremental improvements in the value derived from existing processes, the automation and efficiency suggested in the previous table should provide resources time for the development of net-new processes. But what should these processes be? Read on for a list of functions that can help drive real capability growth.

INTELLIGENCE OPERATIONALIZATION

It may be an intuitive statement to claim that the SOC should pursue any and all opportunities to proactively mine and leverage internal and external intelligence data to drive SOC operations. But how does one place proactive threat intelligence processes at the center of SOC operations without causing a collective eye roll from the SOC analysts who have heard this notion countless times before? It is true that claims of proactive threat intelligence may be overused in vendors' sales pitches, but that does not mean that the pursuit is entirely without merit. A robust, mature threat intelligence program should provide the necessary structure and associated processes to collect and interpret ready-made commodity intelligence products as well as internally sourced operational data to answer one simple question: "How does this data relate to a threat my organization should be worried about?"

Several years ago the shift towards use cases and operations being driven by intelligence analysis would have triggered pushback from those stuck in the mindset of source data-driven use case development. It is refreshing to no longer have to persuade SOCs that intelligence operations and threat management frameworks are worth their time and effort.

A modern SOC not only recognizes the need for formalizing intelligence collection using a framework, but systematically puts collected observations into action. One powerful way to do so is through the maintenance and use of Priority Intelligence Requirements (PIRs) to steer intelligence efforts. Because PIRs require consistent review to maintain alignment to the organization's goals and concerns, they naturally align with healthy habits such as proactive threat modeling and threat landscape assessment. Furthermore, business stakeholders, (not just the security team) should be engaged consistently for feedback to make sure they are able to contribute to PIR definition so that they are provided with actionable, timely information. The downstream effect is the SOC is provided with greater insight into the overall business and business operations, which can help enhance the quality of investigations.

While many of you reading may think of your own organization's current situation and realize it may be far from this ideal state, all hope is not lost. SOCs are getting smarter and more informed. Collaborative communities are emerging with organizations in similar industries publicly releasing PIRs and Tactics, Techniques, and Procedures (TTPs) for the community to analyze and use. While deep intelligence collection and analysis is indeed a unique skill set that takes years to hone, security operations groups can benefit from the explosion of intelligence assets and sharing communities, and the growth of intelligence based mindsets within their own operations if they make a commitment to try.

THREAT MODELING

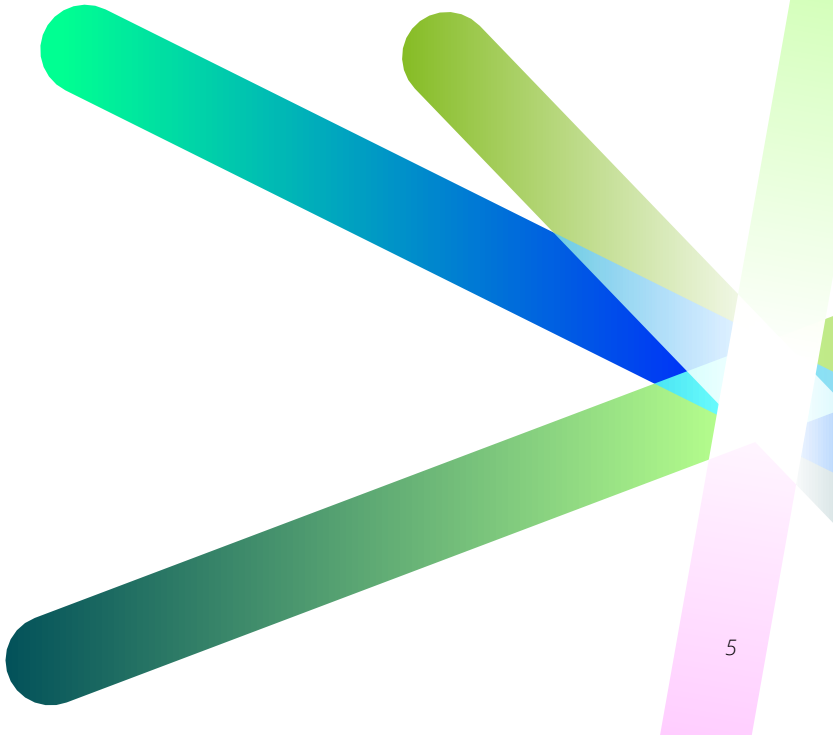
One core capability for the modern SOC that goes hand in hand with intelligence operationalization is threat modeling. In fact, the value of modeling as a process extends beyond its own boundaries and should shape all security operations, from detection development, to threat hunting, to metrics design and implementation. As such, it behooves the SOC to have a defined process for how threat modeling will be conducted and who the expected consumers are for various models.

Threat modeling frameworks have become buzz words in and of themselves. In some situations that pendulum has swung too far and simply saying the words "MITRE ATT&CK" and tagging events with a TTP is interpreted as intelligence operationalization or modeling. To combat this trend, it is important to understand how to separate the hype from the value and how to use frameworks effectively as a cornerstone for downstream processes.

The real path to success in this area is to commit to the notion of driving SOC operations through the collection and analysis of internal and external intelligence sources interpreted within the guardrails of a framework such as ATT&CK. This process should be consistent, continuous, and should—by design—collect and integrate business contextual information from business owners themselves (e.g., impending mergers and acquisitions, external business partner relationships, foreign entity relationships). After all, very few organizations exist where the primary product is security operations. Personnel assigned to threat modeling activities should be granted adequate focused time to make and foster these external connections.

This contextual and organizational data should be paired with intelligence and threat research to make educated decisions around security posture and prioritization. Ultimately, all SOC investigations and their subsequent conclusions should be couched with the language of a threat management framework such as MITRE. This can help ensure that the SOC is monitoring and responding to the right threats across all phases of the attack lifecycle. These insights can identify potential coverage gaps and be used to augment existing SOC metrics.

Finally, those performing modeling should be well positioned in the SOC to have operational authority to shape detection and code development efforts, tool purchases, and operational playbooks and job aids. It is a security operations manager's decision whether to designate dedicated time and resources for these efforts, or protect portions of the team's time for the effort, but in any case the practice should be acknowledged and protected and the impact on operations should be documented and measured through formalized procedural rigor.



AGILE DEV/SEC OPS

The security community has become increasingly vocal in its belief that out-of-the-box use cases from nearly any vendor do not cut it anymore. This is not to disparage vendor's products; it is simply an admission that anything intended to be globally applicable to thousands of customers in a constantly evolving threat landscape is bound to come up short for the most pressing threats. A marriage of out of the box use cases with robust and continuous engineering of detections and process automations is needed for the modern SOC to keep pace.

As a starting point, developing a culture of continuous Dev/SecOps should create more fluid and dynamic detection development through streamlined coding, testing, and deployment processes and wider distribution of permissions to create detections in security tool sets. The underlying goal should be to drive for less human analysis and more robust engineering to solve security challenges. An example for doing this is covered in **Google Cloud Autonomic Security Operations paper**.

The SOC's development teams should consider more than native tool engineering and configuration. Integration of tool sets and streamlined workflows greatly improve the operational team's efficiency and effectiveness and may ultimately lead to better outcomes. In order to create a team capable of vast and timely development to support such goals, it is critical to break down silos and have teams work arm in arm on a daily basis. There should be as little space as possible between analysts and security engineers who live in security tools and event response and those who may automate response processes on the fly. Breaking the silos can drive insight from those responding to the outcomes of detections and create faster feedback cycles that will enhance current and future development. This attainment of organic developer response also plants the seed of a reward for operators to think about ways to solve operational challenges with code. If an analyst's recommendation to automate portions of tickets enrichment or to automate remediation of common high fidelity alerts, the broader team realizes the benefit in the form of reduced operational burden and is conditioned to search for future opportunities to do the same.

Agile development also creates more opportunity for rapid testing of rules and other detection content. Sub processes should exist to programmatically test, review, and tune or remove rules that are non-performant. An effective testing process should include the following:

TESTING SUB PROCESS	COLLABORATING SOC TEAM
High level rationalization of existing rules for relevance	Intelligence and threat modeling
Live and active testing of existing rule sets for performance	Downstream rule consumers including analysts and hunters
Penetration testing or breach and attack simulations to test rule effectiveness	Red team, purple team, or threat surface reduction teams

Achieving a truly agile development approach is not without some challenges. However if properly managed, the response to challenges may present opportunities for even further value. Primary among these challenges is the need for skilled developers. Modern developers need to be fluent in things such as cloud native technologies, microservices and infrastructure as code, and Application Programming Interfaces (APIs). These skills often do not exist within the traditional SOC and need to be sourced elsewhere. While the SOC Manager may immediately respond with dismay that there is yet another requirement to staff a resource with highly competitive skills, there are rewards for the effort.

Beyond the improvement of operations discussed above, hiring and staffing competent development specialists should inherently introduce knowledge of development best practices. Today that includes the skills previously mentioned, as well as a working knowledge of industry standards and leading practices such as how to address the OWASP Top 10.[1] Not only will the development products be higher quality due to the factors listed above, but the developers themselves can become sources of subject matter experts for defense against poor coding and development practices, a very common source of breach in today's threat landscape.

Working with legacy Managed Security Service Providers (MSSPs) can be another common hurdle depending on the degree to which the MSSP and internal operations teams gel. The "otherness" of a MSSP relationship and all-too-common junior level of contracted resources may make it infeasible to allow true development across all MSSP analysts and engineers. It is possible to overcome these potential limitations of a MSSP relationship by defining processes to proactively gather and categorize ideas for improvements and additional system integration opportunities.

Finally, there is the challenge of personnel management. Despite all the efforts outlined above, it is likely that the development and operational teams within the SOC will still have distinct relationships and cultures—this is ok. The goal is not to drive uniformity across all resources, but to ensure process interdependencies are accounted for. For example, intelligence informs threat modeling, which drives ideation and prioritization for detection development, which drives response playbook definition, which leads to production operations, which return feedback on the suitability of the detection code and response workflow, which in turn provides more requirements for improvement through development. Inserting interactions between the development team throughout this chain speeds the time to value of all steps. This is where security operations "fusion" truly comes to life.

1 | https://owasp.org/www-project-top-ten/

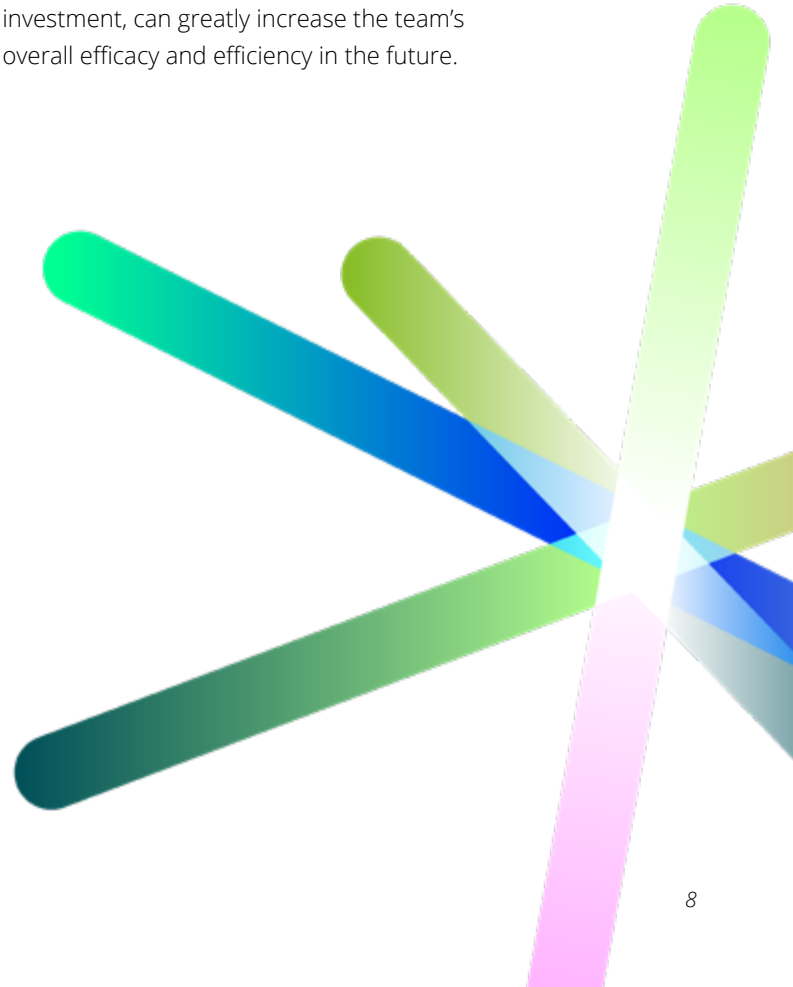
DATA SCIENCE AND ANALYTICS

Unfortunately, even with world class threat intelligence, threat modeling, and continuous Dev/SecOps initiatives, the team may still encounter threats that are using truly novel techniques and methods. There is hope, however, as the combination of statistical and analytical modeling coupled with existing SOC processes provides the SOC a fighting chance.

Modern computing and cloud-enabled services unlock the power to comb through data in speeds and quantities never before possible. Beyond faster processing of known data analysis methods, it is now financially and computationally feasible to use trained and untrained data science techniques to query massive amounts of data for faint signals that may be early warning signs of breach. It's important to note that most compromises may remain undetected for more than six months. The majority of that time isn't spent noisily stomping through the environment snatching and grabbing data as may be the case in extremely late stage attack behavior. So why then would security professionals not look for every opportunity to detect early, low signals of attack?

While this approach to detection is certainly less prescriptive than scenario-driven alerting (and therefore harder to build step-by-step response procedures against) and certainly requires more skilled investigation to effectively act upon. Modern computing and enabled services are powerful capabilities all SOCs should rally around. Such a program is the only way a SOC can possibly identify patterns and anomalies that would have previously remained undetected from legacy SOC methods. We as security professionals are no longer looking for the needle in a haystack by continuously defining what a new needle looks like, we can now query the haystack to tell us what unusual hay looks like. For example, looking at user behavior, anomalies may reveal compromised accounts and systems faster than intelligence or rule-based approaches because of how compromised accounts may stand out against a baseline of typical peer behavior.

It is important to not treat these methods as magic. They come with their own data requirements, pitfalls, and skills requirements, and—perhaps most importantly—trade-offs of investment versus direct detection return. Still, some modern SOCs have instrumented processes and technologies focused on data science and analytics and have achieved success doing so. To mirror their success, it's important to acknowledge there are new skills to consider and new technologies to purchase and learn. Furthermore, to get the most out of a specialized team of data scientists, they should not be heavily cross loaded, as is common for most SOC practitioners. These skills need to be nurtured and supported as a specialized skill set within the SOC, and one that, with proper investment, can greatly increase the team's overall efficacy and efficiency in the future.



THREAT HUNTING

Despite the efforts of the SOC to ensure that all intelligence has been considered, threat scenarios have been modeled, and all possible detections have been developed and tuned, there will always be new and novel threat scenarios. For such scenarios, threat hunting plays an increasingly important role. As a concept, threat hunting is not new. Rarely though is it thoroughly or completely achieved as a formalized process. The hunting group must be intimately familiar with both trends and patterns in threat actor behavior gleaned from consumption of threat intelligence. Collection and absorption of threat intelligence data should be programmatically defined in process to ensure adequate sources of information are used and that actionable observations are derived. From there, the hunter must either work closely with the threat modeling team or use their knowledge of organizational technology and business functions to threat model how relevant attacks may manifest in the environment. Using threat models as a guide, hunters then proactively (not driven by security tool alerting) gather data from systems in the environment searching for evidence of malicious or anomalous behavior. Finally, it is critical that the hunter document findings and remediation actions to promote lessons learned and create internal intelligence.

Clearly the hunting cycle requires a great deal of skill, creativity, and focus. The capability needs to be a protected function and not someone's third or fourth role within the SOC. (Are you picking up on a common theme with this requirement?) The skills and point of view a hunter must possess are related, but distinct from those of a SOC analyst or security engineer. It takes time to cultivate these skills and build intuition and, for that to happen, hunters must practice their craft as their primary function.

Without the benefit of guiding principles and processes, threat hunting can rapidly become an exercise in chasing the latest TTPs mentioned in the podcast du jour, regardless of its actual potential impact to the organization. On the other hand, if the SOC overcorrects the threat hunting team's ability to operate on hunches and intuition, overly regimented processes may prevent the team from doing what they do best: thinking outside the box to identify exposures not previously known or protected.

SOC: balancing consistency and creativity

Hopefully, by this point we have adequately defended the notion that the modern SOC requires a solid procedural foundation, but also a new set of processes that rely on human innovation. The processes discussed above need to be built upon solid underpinnings of repeatable, procedural steps. As with any defined process, the value of doing so is that the organization can expect repeatable quality results, can enhance operational efficiency, and can greatly accelerate training of junior or cross loaded resources in new skills. But how does SOC management limit the pitfalls of over-engineering processes in the pursuit of the false notion of process maturity as the ideal? The key is maintaining a balance between creativity and procedural maturity.

That said, true innovation can be scary for most security organizations because it is, to a certain extent, a commitment to organic and messy growth rather than measurable procedures. The challenge for a modern SOC leader is thus balancing the desire for consistency—backed by repeatable, predictable, and effective processes on one side—and the desire to harness human creativity, initiative, and perhaps even irrationality on the other side.

A highly functioning modern SOC, one that is able to anticipate and detect threats on their way in rather than on their way out, has likely attained that balance between consistency and creativity. But how is this balance achieved? The trick is to create an unconventional, but somehow harmonious mixture of consistent, repeatable processes and human, anarchic, and spontaneous creativity. Next are some steps to consider to develop this mixture.

1 BUILD ON CONSISTENCY (BUT DON'T STOP THERE!)

Once process maturity is determined to be a key goal, it is relatively easy to measure traditional maturity using a Capability Model Maturity Integration (CMMI) inspired maturity model. It must be said, however, that modern SOC leaders should be careful not to become enamored with CMMI level 5 as the highest stage of the organization's evolution, because CMMI-inspired maturity models often consider the most rigid and inflexible—but well-engineered—processes to be the most mature (and by extension the most desirable).

This interpretation of maturity may downplay the positive impact of creative development. The risk of such models is that the creativity of the analysts is stifled, impacting the SOC's ability to react to emerging risks. This adherence to process and lack of ability for the SOC to think critically and creativity provides potential attackers with another opportunity to successfully exploit a vulnerability within the environment, no matter how well planned the supporting processes are. Well-designed controls force attackers to continuously iterate—they must be adaptive and creative to earn their pay. It is important to remember that ultimately the SOC team wins not by defining more robust processes than the attacker, but by out-flanking the attacker en route to his objective.

In some maturity models, the highest maturity level is called "Optimizing." Perhaps this best captures the vision of how a good SOC should look. Ultimately, security professionals are not striving for consistent operations alone; they are aiming for this elusive maturity tier whereby the previous foundational levels are so well entrenched that the SOC can spend its time truly optimizing, in a living, ever-adapting model.

2 INJECT CREATIVITY, THEN KEEP CREATING

However, perhaps the secret snare of achieving the "Optimizing" state is that if you lean too heavily into an adaptive model, consistency may be lost. Without harnessing the inventions of our creativity into a documented, repeatable, procedural process, we as security professionals miss out on the opportunity to share discoveries, train peers, and increase operational efficiency (in other words, we fail to make our lives easier). We are doomed to a state of relying on individual creativity and genius to continuously defend the network. This is the failure mode opposite from the rigid SOC obsessed with process repeatability. If all your SOC runs on is human creativity, individual efforts will be required to defend the enterprise and analysts are likely to burn out due to working too much. Worse yet, perhaps this exhaustion may lead to the team missing the all-too-obvious.

The better road is to build consistency and grow through lower maturity levels, and then let creativity lose within the processes that are already built.

For example, a threat hunter should not be forced to follow a pro-forma flowchart that defines all hunting actions because the hunting process inherently requires the hunter to draw on human creativity to think of ways an attacker may enter an environment that is not adequately defended. Creativity and application of constantly evolving intelligence is part and parcel to this process. However, the SOC should maintain defined processes that delineate situations where hunting is necessary and how hunting must coexist with other SOC processes (roles, expectations, and process boundaries). In this example, we have a consistent model for invoking a creative process such as hunting.

As another example, a consistent, and likely heavily automated, alert triage process may follow a pre-set activity flow for many steps. However, possibly while managing this routine process, an analyst assessing the alert may see something unusual and have a spark of creativity to deviate from the script when necessary. This deviation may later become a part of the playbook, or remain a one-off activity necessitated by the threat actor behavior. In either case, the analyst's interjection may lead to a detection that's impossible with the existing playbook or even overall improvement to the playbook which—in turn—may lead to greater detection rates.

3 KEEP YOUR WORKFORCE ENGAGED

Let's be honest: not many people like to work for the sake of work (financial compensation aside); instead humans derive deep satisfaction from working toward something and seeing that imagined future realized.[2]

Imagining that future is an inherently creative process. A high-performing workforce is not one that only dedicates their energy and intellect to achieve a future articulated by others, but one that influences what the future looks like. Each member of the SOC should have a role in creative evolution of process and capabilities, even if most of their day is spent following processes. The trick is SOC leadership recognizing the value of creativity and protecting a portion of the team's overall time to allow for creative reflection on existing processes. This can be a challenge in an industry plagued by chronic skilled labor shortages; however, by this point in the paper, the alternative of a stagnant SOC should be patently less appealing than slightly reduced productivity. Overworked teams may not see process innovation as the key to improving their situation if their "reward" for creative thought is more work to design and document innovations in hours 70-80 of the work week. It is the job of SOC leadership to protect innovation and champion it however possible.

Finding the right balance between process and creativity is not process or, but process and—and a tricky "and" that is.

2 | *https://qz.com/498951/why-work-a-psychologist-explains-the-deeper-meaning-of-your-daily-grind/*

4 PROCESS IMPROVEMENT IS A COLLABORATIVE PROCESS

This is the space where passion, ingenuity, and creativity can shine. Fixing processes that no longer reflect reality or are too stifling should be in everyone's job description. Every analyst, hunter, or engineer within the SOC should be expected to:

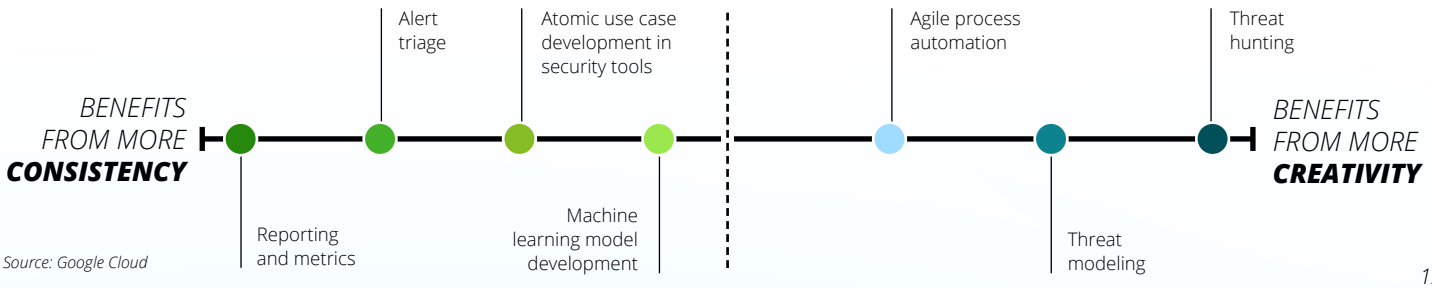
1. Learn the processes
2. Apply the processes
3. Deviate where the processes are insufficient
4. Make the system more efficient through process improvement

Put another way, every member of the SOC, from apprentices to managers, is a problem solver first and foremost. It just so happens that the SOC's primary problems are threat actors who make a living by ensuring the SOC fails at its mission. Solutions to these problems may be innovative ways of resolving inefficiencies via automation (machine processes) or playbooks (human processes), better and faster integration of intelligence into the detection workflows, integration of tools and data to make better decisions, improving detection logic, etc.

While innovation, ingenuity, and creativity should be a key expectation of every role within the SOC, it cannot be argued that the job of an architect is more creative by nature than that of a construction engineer.

Let's outsource threat hunting and initial incident response. It is very clear that both require consistency and creativity to succeed. It is also very clear that hunting runs on creativity (while relying on consistency for some elements) while IR is mostly about consistency (while, of course, relying on creativity to outsmart the attacker).

THE BALANCE OF CONSISTENCY AND CREATIVITY ON A RELATIVE CONTINUUM



Source: Google Cloud

Conclusion

Modern SOCs should seek to set a framework of operational processes that allow for a dynamic set of capabilities capable of solving today's, and tomorrow's threat challenges. The magic of a modern, evolved SOC is about achieving a delicately balanced set of consistent (but not rigid) and creative (but not chaotic) security processes. Excessively rigorous process does not help security, it increases the risk of losing to the attacker who can easily outsmart a "by the book" SOC.

The operational framework of a balanced modern SOC should comprise of new processes (e.g. hunting and data science) and updated versions of time-tested processes (e.g. alert triage and SIEM tuning). By doing so, the security organization can build upon a solid foundation with new and emerging capabilities that require out-of-the-box thinking to truly succeed.

LET'S TALK

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

Dan Lauritzen
Senior Manager
Deloitte & Touche LLP
dlauritzen@deloitte.com

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

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

Trevor Welsh
Global Security Strategist
Google Cloud

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