Deloitte. | Google Cloud

***CONTENT OVERVIEW***


***Introduction***

***Scenario 1***
Cloud migration as a catalyst for SOC modernization

***Scenario 2***
Adopt MDR and modernize SOC to build a hybrid model

***Scenario 3***
Transform SOC to catch up with modernized IT (DevOps, Platform engineering)

***Conclusion***


# ***FUTURE OF SOC***
# *TRANSFORM THE HOW*

## *Introduction*

When facing the question of whether to evolve or optimize a Security Operations Center (SOC), security leaders have numerous risks and rewards to consider. Disruptions to normal operations, migration challenges, compatibility issues, advantages of new technologies, and learning curves for the teams involved are many important factors to consider.

Previously in our "Future of the SOC" series, we explored the conditions in which security leaders could evolve their tooling versus conditions in which leaders could double down and improve their existing tooling.

In "Future of the SOC: Evolution or Optimization - Choose Your Path," we laid out a decision matrix to help navigate the decision on whether to *change* or *stay*. In this paper, we explore the *change* decision tree through the lens of three common scenarios as drivers for transformation: Cloud migration, Managed Detection and Response (MDR) adoption, and DevOps evolution.

Chronicle

# Scenario 1

## Cloud migration as a catalyst for SOC modernization

Proposing SOC modernization amid a broader organizational migration is an excellent way for security leadership to capitalize on an organization's capacity for change. Similar to application migration discussions, the SOC can choose to Rehost, Replatform, or Re-architect their technologies to accommodate both the expanding threat landscape that cloud technologies present and optimize existing detection and monitoring capabilities in place for the on-premises (on-prem) environment.

One specific challenge to overcome with the move to cloud is the increase in telemetry log volume. Restructuring the approach to log aggregation to accommodate this increase often allows organizations to "go back" and onboard previously unattainable log sources due to their volume, such as endpoint technologies including *auditd, winlog, sysmon* or even Endpoint Detection and Response (EDR) equivalents, as well application telemetry (observability).

### *Transform technology*

Aided by the refreshed capacity for change, technologies at the core of the SOC are arguably most ripe for transformation as opposed to the people and process components. The technological shift to cloud allows the SOC to add, remove, and reprioritize tooling.

#### Detection technology

At the core of the SOC, the Security Information and Event Management (SIEM) as a technology component is prime for change alongside a broader cloud migration. Moving from on-prem to Software-as-a-Service (SaaS)-based SIEMs allows for a paradigm shift and frees up resources to help solve new problems that might arise:

- On average, cloud migrations generate more telemetry than previously gathered on-prem
- Threat detection isn't exotically new in the cloud, just slightly nuanced and different in approach
- The shared fate model of cloud means that providers are equals in responsibility for the maintenance of the Confidentiality, Integrity, Availability (CIA) triad when it comes to organizations' SIEM infrastructure
- SaaS SIEMs introduce:
  - Scale to address not only net-new cloud volume, but new visibility for on-prem through scalable capacity to support additional on-prem log source ingestion and unlock new potential for threat visibility
  - Reduced engineering overhead, required to maintain underlying hosting infrastructure and associated on-call rotations
  - Reduced granular customizability to use cases, since one is buying a service rather than self-hosting

Organizations are typically not new to the concept of Security Orchestration, Automation, and Response (SOAR), or at least automation for security operations at large if undergoing an organizational shift to cloud. Cloud migrations empower SOAR, not only in SaaS flavors of the technology carrying many of the same operational benefits described above for SIEM, but in its ease of interaction with many of the organization's new infrastructure technologies.

Specifically, cloud infrastructure is Application Programming Interface (API)-first in design, lending itself to programmatic interactions that empower enrichment, updates, and remediation actions as a result of playbook automations. However, this ease of programmatic interaction is rarely fully leveraged. Even if it could be technically easier to perform remediation actions with a Cloud Service Provider (CSP) infrastructure as opposed to on-prem variants, the risk-averse nature of the business often migrates to the cloud alongside the application workloads themselves. As a result, teams may still lack the ability for autonomous remediation in some cases.

***NOTE***

*EDR is an interesting edge case, because while workstation and on-prem server visibility is often strongly aided in the migration to the cloud (via SIEM products that remove cost or volume barriers that existed historically), cloud compute workloads themselves often prove difficult in deploying a consistent endpoint solution to maintain parity with their on-prem equivalents.*

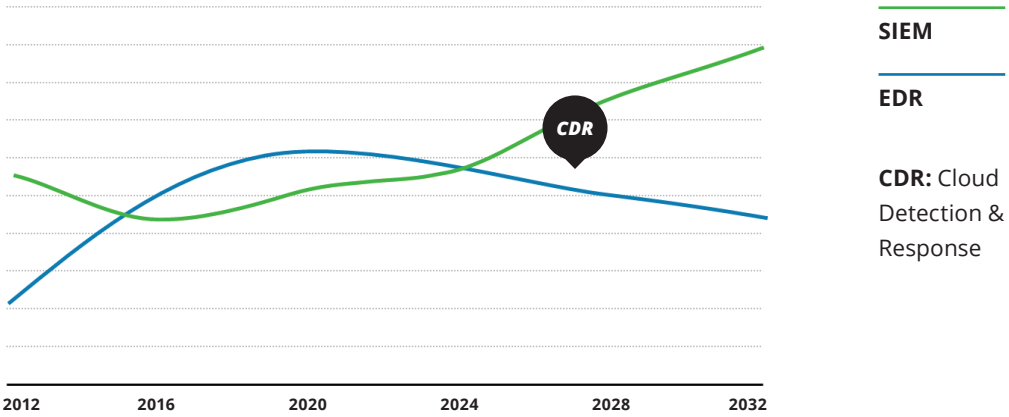
Likewise, Network Detection and Response (NDR) is another interesting edge case, with an argument to be made on whether it matters in the cloud. There are offerings surrounding NDR with a cloud focus, but it may be a valid approach to reduce NDR/traffic sniffing if network traffic in the Cloud is encrypted by default and a high volume of traffic is ultimately microservices talking to other services.

## Shift to Next-Gen SIEM

There are still SOCs that have moved to the model with EDR at the center and struggle to adapt to environment changes. A cloud migration challenges this model by bringing back the necessity and importance of the SIEM.

There's been a significant rebalancing back to SIEM-centric SOCs as organizations realize the benefits of data correlation and aggregation beyond endpoints. While endpoint telemetry remains imperative as workforce models change to remote-first, it is now also recognized as one piece of a much larger puzzle.

**Criticality for SOC**



## The "connecting tissue" technologies

During a cloud migration, there's an interesting opportunity to re-assess and re-approach the way in which several specific components of the SOC are designed in relation to the overall architecture of the interwoven fabric of security technologies.

### *Extract, Transform, Load (ETL)*

- Changes in tooling can suggest an expansion in visibility, which can likely be federated to additional cross-functional security teams to provide more cohesive cyber operations. Visibility expansion can lead to cost savings and tooling consolidations with multiple teams benefiting from centralized logging and analytics capabilities
- ETL modernization in the form of Cribl, Kafka, or other similar technologies can unlock this centralization of logging, allowing for enterprise "data brokering" to emerge in support of use cases beyond security
  - These modernization efforts often coincide with significant cost reduction opportunities, allowing organizations to reduce log density by removing unneeded fields and thereby reduce data clutter and overall ingestion costs.
- Cloud providers (and more broadly, security vendors that dabble in more than SIEM/SOAR) that are also in security have ecosystem benefits realized in the ETL space as well. For example:
  - Google Cloud and Workspace customers also leveraging Google SecOps are given turnkey integrations to ingest this infrastructure and productivity platform telemetry with next to no effort on the part of customers
  - Microsoft Azure customers leveraging Sentinel are given turnkey integrations to allow realized value of ingesting the broader Defender and Microsoft Security stack with next to no effort on the part of customers
- Sometimes a cloud migration itself is conducive to new ways of ingesting and storing logs. As a simple example, storage buckets have become a friendly intermediary for telemetry, allowing for convenient splitting of telemetry to enable multiple stakeholders beyond just security

### *Cloud storage*

- "Cloud-native" SIEMs can offer storage advantages, both in terms of ETL as outlined above, and for broader use cases such as compliance and operational metrics/reporting
- Cloud-native SIEMs reduce the burden on managing storage as opposed to legacy on-prem alternatives
- Cloud storage can often be not only lower-cost, but can also be easier for data management thanks to the realized benefits of cloud services that abstract much of the management away from the end users, allowing them to instead focus on outcomes

### *Threat detection*

- Detection engineering as a discipline can tap into deployment and development norms that the cloud teams can harness—this can lead to codified approaches to detection, such as Detection-as-Code (DaC). Leveraging cloud build pipelines Continuous Detection, Continuous Response (CD/CR) approaches to detection can also empower programmatic, auditable, and consistent delivery of threat detection content

## *Transform process*

Just because the business is shifting workloads to the cloud during a migration doesn't mean its processes change overnight to accommodate these new ways of working. On the contrary, the old way of doing things often comes to the cloud, even if the processes themselves make little sense within the new environment.

Specific to security operations, there are a few categories that force process changes via the technology migration:

### Alert enrichment

Focusing on the net-new cloud components, the way you detect and triage potentially compromised hosts and identities can change with the shift to cloud.

- *Everything* is identity-based—compute, storage, and of course identities themselves
- Infrastructure identifiers are ephemeral
  - Internet Protocol (IP) addresses are rarely static
  - Images are routinely updated and redeployed
  - Containers are spun up and spun down repeatedly
- While the Configuration Management Database (CMDB) of the cloud estate becomes 'easy' when maintained and provided by a CSP, this can become tedious to dissect during an alert triage to understand what and who a service/resource was at a given time, given the aforementioned ephemeral nature
  - **Examples:** Cloud Asset Inventory in Google Cloud and Resource Inventory Management in Amazon Web Services (AWS)

### Alert prioritization

The proliferation of cloud services has created many new possibilities, but also has introduced new risks. Prioritizing alerts both from existing environments and the development of net-new is critical to allow for efficient response. One common theme that arises during cloud migrations is that a "baseline" is impossible to establish for more than a few weeks or months due to rapid migration of workloads that can shift what "normal" looks like for a tenant, project, identity, or workload type. Working closely with architecture and platform/cloud engineering teams to understand conventions and continually reinforce adherence to said conventions is work that pays dividends in the long run.

### Remediation changes (more auto in cloud)

- Policy-driven deployments and environments allow for easier (than on-prem) auto-reversion of undesired infrastructure changes
- Since everything is heavily identity-driven, revocation of credentials/keys can be effective in minimizing the blast radius of an attacker given that persistence arguably becomes harder to achieve when many resources require CSP compromise versus solely application compromise given the CSP's managed service/abstracted nature

- Incident response and associated forensics has interesting changes, as endpoint forensics can become difficult in the cloud, especially for serverless or -as-a-Service (-aaS) deployments. Network quarantine and sink of flow logs for forensics can be made easier due to virtualized networking conventions.

### Timeline to start hunting

- With more emphasis on automating atomic alerting, it allows analysts more time to focus on more interesting work, such as threat hunting
- The richness and completeness of cloud telemetry offers an opportunity to threat hunters as opposed to often fragmented and incomplete counterparts of on-prem. The barrier to entry is reduced when gathering, aggregating, and exploring this telemetry across CSPs
- Cloud's scale offers easier exploration of massive amounts of data, whether specific to the cloud itself or combined with existing on-prem estates

## *Transform people*

In the scenario of cloud migration being a catalyst for SOC modernization and change, the "people" component is arguably the least prone to drastic change between the canonical People, Process and Technology triad. While this might seem counter-intuitive, we propose that while people can be ripe for transformative growth, this is not net-new as a result of the cloud migration itself. Security tool bloat, solution changes and personnel shortages are not new in the cloud - they simply persist through the migration.

There are however several considerations:

### New skills are needed

- Often, the shift to cloud provides a dynamic in which the SOC is left playing catchup on existing skillset needs in conjunction with those needed to become proficient in the new stack of technologies and terminology
  - The "Information Technology (IT)" side is much faster and people need to adjust to faster IT processes around them (DevOps, Agile)
- Strong collaboration with cloud engineering teams supporting the migration are essential to provide quick help in identifying new process use cases for the SOC, whether through threat modeling new application architectures in the cloud, detection engineering that prioritizes new threat detection content, or through teaming with incident response teams to perform remediation actions on identified compromises
- A shift to an engineering mindset (for analysts) to help own the end-to-end detection lifecycle, notably in helping to create playbooks, is often re-emphasized, though again, it's not a change specific to cloud migrations

### Skills difficulties - mentorship in a new way of working

With the rapid adoption of post-pandemic remote work and increasing volumes of security incidents, mentorship techniques often leveraged in the traditional workspace (shoulder surfing incident triage, overhearing

conversations in the office) are no longer available, or are more difficult to utilize while upskilling analysts. This only exasperates the difficulty in skilling up in new domains such as cloud.

***NOTE***

*This is not an endorsement of a Return-to-Office (RTO) mandate, but rather a call to action in acknowledging this issue and the need to explore new ways to mentor junior personnel to fill skills gaps and develop the next generation of industry leaders.*

## *Key takeaways*

**Enhanced log management and integration:**

With the increase in data volume due to cloud migration, there is a critical need to restructure log management strategies. This includes adopting advanced ETL tools like Cribl or Kafka to facilitate centralized logging and data brokering, thereby supporting broader security and operational use cases and fostering easier integrations between closed ecosystems.

**Shift in Detection and Response (D&R) paradigms:**

Cloud migration necessitates a re-evaluation of threat detection and response strategies. The cloud's API-first nature and identity-based security models require SOCs to adapt their processes for alert enrichment, prioritization, and remediation. This includes leveraging cloud-native capabilities for automated responses and integration with cloud engineering practices for continuous threat detection and response.

**Rebalancing of the SOC focus:**

As organizations migrate to the cloud, there's a notable shift from endpoint-centric security models to a broader focus on data correlation and aggregation facilitated by SIEM and SOAR technologies. This shift is crucial for adapting to the dynamic, distributed nature of cloud environments and for effectively managing the increased complexity and profusion of security data.

# *Case study*

A financial services organization, referred to here as "FinCo," recognized the need to modernize its SOC to keep pace with evolving cyber threats and the increasing complex IT environment. FinCo's existing SOC struggled to maintain multiple legacy SIEM platforms, leading to alert fatigue and inefficiencies.

The organization decided to leverage its cloud migration as a catalyst for SOC transformation, collaborating with a major cloud provider to achieve this goal. The security operations team was new to both the cloud provider's platform and its security tools, requiring experience in monitoring the new environment for threats. The migration to the cloud was swift, leading to significant time and resource constraints.

The team faced a steep learning curve with the new tech stack, and there was no standardization across the use case development lifecycle, making it difficult to streamline operations. Additionally, the team lacked incident response, forensics playbooks, and established documentation for cloud-specific threats. Multiple legacy SIEM platforms monitored various components of the organization, leading to alert fatigue and confusion among analysts. This created an opportunity for transformation in line with the business.

The transformation included the deployment of a cloud-native SIEM platform that provided increased visibility into the cloud environment. By consolidating multiple legacy SIEM platforms into a single, cloud-native solution, FinCo reduced operational costs and improved the efficiency of its SOC. The SOC adopted DevSecOps methodologies to integrate security practices into the development lifecycle, enabling continuous monitoring and automated threat detection through Detection-as-Code approaches. These approaches allowed the SOC to evolve in tandem with the broader business, allowing security measures to keep pace with rapid technological advancements and agile development practices.

FinCo's cloud transformation served as a catalyst for a broader SOC transformation. By leveraging a cloud-native SIEM platform, the business achieved enhanced visibility, reduced alert fatigue, and improved incident response capabilities. This transformation not only strengthened FinCo's security posture but also positioned the business to better manage and mitigate cyber threats in an increasingly complex IT environment.

## *Scenario 2*

Adopt MDR and modernize SOC to build a hybrid model

Architecting an organization's security environment can be a challenge when adapting to the business' circumstances and requirements to stay within regulatory compliance while maintaining a competitive edge against adversaries. The SOC warrants creative blueprints to stay at the forefront of protecting the brand with their composition of technologies, processes, and personnel. If the organization has deficiencies in one of these three components, then action needs to be taken in one or multiple of those areas. If the people component is the deviation, then typically this decision has a ripple effect that impacts SOC technologies and processes.

An organization may benefit from selecting an MDR provider wherein they modernize the SOC with new technologies in parallel. This joint model can enable teams to reinvent legacy and stale strategic processes. When adopting a service such as MDR, the original SOC blueprint should be reviewed and transformed to account for a hybrid model that leverages new technologies, processes, and personnel.

The SOC should evolve to a joint model where identified duties are completed by the MDR, their team, or often by both. Transforming to a hybrid model can also result in swift removal and consolidation of essential legacy systems within the SOC's newly envisioned composition.

### *Transform technology*

MDR adoption is a catalyst for reviewing the SOC's composition and re-evaluating the current makeup of technologies to determine if it still reflects the optimal approach. When identifying the right partner to join forces with, the SOC can identify what technologies are compatible and what needs to change for an optimal experience. Transforming the tools that teams utilize each day can have an impact on how security operations are enabled and where ownership lies.

#### Consolidate services

When shifting to a hybrid model, it is natural to review the current products used and the products preferred or suggested by the MDR. To support MDR use cases and standard operating procedures (SOPs), the SOC may need to fill technology gaps to provide additional visibility within the environment. A part of this process can highlight how the new products in question may include features encompassed within other products. It is common to have multiple EDR products in an environment due to previous gaps in features that may be the new standard across many competitors. Take this moment to identify if use cases still require leveraging multiple vendors for endpoint detection capability. This gives the SOC an opportunity to shift use cases, procedures, and capabilities to consolidated products.

Functionality aside, cost becomes a primary driver for deciding what products to procure or move away from. In some cases, the MDR service may provide options to subscribe to a suite of products managed by the service, while in other cases, the SOC owns the procured technology. Depending on the organization size and budget, MDR owning particular products may be a viable consideration to fill gaps in visibility but will raise challenges when shifting MDR vendors or considering custom upstream changes.

For large organizations, it is recommended to procure and own the licenses to each product leveraged in the SOC, and for SMBs (Small Medium Businesses), it may provide less overhead to have the MDR own the technology stack. MDR and service providers can be considered a fluid relationship, but it is valuable for internal teams to be accustomed and well versed in the SOC suite of security products for optimal results when actively defending against adversaries.

It is also common that two of the same or similar tools are leveraged to communicate between the SOC and MDR. For example, consider creating, assigning, and closing tickets between both teams. The SOC may have an existing implementation of one ticketing system, so there needs to be a decision made to see if the MDR operates in the customer-owned implementation or if a viable integration can be made to the MDR's preferred ticketing system. Regardless, for a large enterprise, the recommended approach allows the SOC to have technology ownership with an approach to integrate with other tools.

## Redefine access controls

When migrating to a hybrid MDR SOC model, it is recommended to have granular RBAC (Role-Based Access Controls) for each of the SOC security products. This can empower elevated assistance and insight from the MDR without giving away control and meeting specialized governance requirements, like GDPR (General Data Protection Regulation). Consider labeling each SOC role with team indicators by region, team, and function.

***KEY***

- ● *Can Do*
- ● *Cannot Do*
- ○ *No identifiable obstacles, no specific permissions*

| Permission | Threat hunter / Detection engineer<br>*Region: Internal* | Platform engineer<br>*Region: Internal* | SOC Manager<br>*Region: Internal* | Analyst<br>*Region: External* |
|---|---|---|---|---|
| Searching of data | ● | ● | ● | ● |
| Retro hunting | ● | ● | ○ | ○ |
| Development / enablement of detections | ● | ● | ● | ● |
| Creation of visualizations | ● | ○ | ○ | ● |
| Onboarding of log sources | ● | ● | ● | ● |
| Parsing / normalization of data | ● | ● | ● | ● |
| Administration of platform configurations | ● | ● | ● | ● |
| Generation of reports | ○ | ○ | ● | ● |

**Example granular SIEM RBAC model**

When implemented effectively, the organization and MDR can effectively delineate roles and responsibilities within their SOPs when responding to an incident. The industry is driving towards a "single pane of glass" where the SOC owns their technology suite and prefers to onboard the MDRs as contractors, but granular RBAC is a requirement to achieve this approach effectively.

MDRs do not prefer this because it makes their use cases, playbooks, and business intelligence logic transparent with the SOC and requires a level of effort to implement. MDRs also do not prefer leveraging the SOC's products because it can lead to deviation from processes that could result in inefficient outcomes and increased risk of mistakes. The controversial issue is: what MDR intellectual property can be shared when it is exposed to their customer? Cybersecurity is one large community with a common goal to protect respective brands and companies, but at the end of the day, it is still considered a business function.

Regardless of technology, there will be engineering considerations and levels of effort when identifying and implementing integration points with the MDR's workflow. Creative internal engineering may be required when security products don't have supported integrations available, and a custom solution may need to be developed. These custom integration solutions will need to be maintained and supported by internal engineering teams until the respective product releases a generally available and supported solution for integration.

## *Transform process*

Transforming technologies and working with an external provider to enhance security operations will result in process and procedure changes. Sharing responsibilities and collaborating on day-to-day activities can be crucial for not only a smooth transition, but a continued effort to improve. Multiple teams and players need to account for a joint operating structure and understand the workflow while incorporating iterative feedback loops to steer towards automation becoming adopted within their processes. The immediate win for many midsize organizations is expanding visibility and coverage from 8-hour 5-day shifts to 24-hour 7-day coverage. However, there can be friction in the early stages before muscle memory of responsibilities takes effect.

### Define joint operations workflow

New players in the game correlates to rebuilding team chemistry. It is critical for the SOC to clearly articulate the details in workflows between their internal team and the MDR team. Have each team define an end-to-end pipeline of the lifecycle of an event that triggers an alert and indicates procedure milestones for the teams to understand where and when the baton gets passed.

It is recommended to have a full debrief and deep dive of the SOC culture to determine if expectations are aligned. In the initial operating stages, it is imperative that transparent communication of tasks is spotlighted to the team, so that each group understands the average level of effort. Once outliers are identified, the process can be iterated upon in the logical areas to reduce resistance.

At the outset of joint operations, assign teams a timeline and goals to uncover opportunities to improve processes and workflows in SOC SOPs. For example, after about one month of following the end-to-end pipeline, it may become clear that there is room for improvement that goes beyond shifting responsibilities. This clarity and frustration with the process can be a trigger for automating pieces of the SOC SOP.

When adopting the next generation of security technology, the focus should be on reducing standard and repeatable steps that activated automation can accomplish. When leveraging a security operation suite of technologies, the SOC's SOAR product should have the ability to integrate with the majority of the technology stacks. To be effective in developing an automated process, the team should consider creating a defined SOP and execute on it. The automation opportunities can naturally be identified and then prioritized.

To implement effective collaboration between the SOC and the MDR provider, it is essential to establish a well-documented RACI (Responsible, Accountable, Consulted, and Informed) matrix. This matrix will clearly delineate responsibilities and roles, determining that each team member understands their specific duties and how they contribute to overall security operations.

Additionally, a documented communications plan is crucial for maintaining alignment across the joint team. This plan should include a structured meeting rhythm and a detailed reporting structure, which will facilitate regular updates, foster transparency, and endeavor to provide that stakeholders are consistently informed about progress and applicable emerging issues. By implementing these tools, the SOC and MDR teams can enhance their coordination, streamline workflows, and ultimately improve the efficiency and effectiveness of joint operations.

### Build strong team connections

It is important to have a strong and motivating culture in the SOC. This will enable continuous progress and improvement when working within the SOC. Defending the organization's brand is a thankless effort with much responsibility of a potential miss. The SOC leaders should recognize this effort and applaud the team for continuous improvement and long hours during an investigation.

Leading cybersecurity organizations reward and recognize the effort of select contributors in the organization to help their efforts to not go unnoticed.

Include motivational messaging and recognition of the cybersecurity team and select individuals at quarterly all-team meetings to highlight the heroic actions the team may have executed against.

### Initial transition approach

There are various approaches to defining workflows for the SOC and MDR teams. However, it is crucial to establish clear goals and timelines to review successes and areas for improvement in the current process. For instance, the SOC and MDR can follow defined milestones such as outlining the pipeline, scheduling the initial debrief, initiating the transition, conducting follow-up sessions for a full debrief, and preparing to commence operations, as detailed below.

***Planning phase***

- **Understand the current state of operations:** Gather a broad understanding of the SOC's existing operations
- **Define roles and responsibilities:** Identify and secure mutual agreement on roles and responsibilities between the SOC, MDR, and other involved parties
- **Service management parameters and operational metrics:** Collaborate with customer domain managers to define service management parameters and operational metrics, including Key Performance Indicators (KPIs), Service Level Objectives (SLOs), and Key Risk Indicators (KRIs)
- **Transition plan and milestones:** Develop, review, and finalize the transition plan and specific milestones, securing written approval from the customer's executive sponsor or designee

***Knowledge aquististion***

- **Conduct Knowledge Transfer (KT) sessions:** Engage in KT sessions with the SOC, MDR, and service provider teams to understand supporting technologies, daily operations, associated processes, SOPs, and the interaction model with other teams
- **Adapt to SOC culture:** The MDR should integrate with the SOC culture to meet requirements and understand limitations, endeavoring to provide that potential improvement opportunities are well received
- **Review incident response (IR) plan:** Understand the different SOC roles and responsibilities, technical architecture, lifecycle of an incident, tool ownership, main points of contact for SOP communication, and Level of Effort (LoE) for various SOP tasks
- **Assess and update SOPs:** Identify potential gaps in SOPs and collaborate with the team to add required procedures

***Shadowing phase***

- **Shadow operations teams:** Observe the incumbent service providers' operations teams and/or the Customer Operations team in their day-to-day activities to understand and document lessons learned, known issues, exception scenarios, priorities, and dependencies
- **Refine SOPs:** Develop new SOPs and update existing ones based on the knowledge transition, and review and refine continuous improvement processes

***Reverse shadowing***

- **Assume operational responsibilities:** Begin delivering day-to-day and ad-hoc assistance activities, including incident management, change management, health monitoring, and report publishing, while monitoring daily operations and providing feedback and recommendations
- **Address pending queries:** Understand and address pending queries regarding open issues, incidents, ongoing bug fixes, or enhancements

***30-day initial operating transition***

- **Commence monitoring and operations:** Start operations as per the defined SOP, with each team assuming their roles and responsibilities
- **Feedback and improvement:** Take notes on feedback and improvement opportunities at each defined stage, identifying what worked well and what areas of improvement to discuss in the full debrief

***Full debrief***

- **Review initial operations:** Discuss the first 30 days of operations, allowing representatives from each SOP stage to provide feedback on their LoE for tasks and areas for improvement
- **Evaluate KPIs and SLAs:** Review KPIs and their estimated SLAs, making required adjustments to provide realistic SLA goals for improving the SOP

***Steady state***

- **Implement changes:** Apply the changes identified during the full debrief and begin steady-state operations between the SOC and MDR
- **Regular debriefs:** Establish a monthly or quarterly cadence for full debriefs to iterate and improve the defined SOPs continuously

***Transition completion***

- **Validate transition activities:** Ensure that in scope planning and transition activities have been completed as defined in the transition plan
- **Obtain signoff:** Provide confirmation of transition activity completion to the customer and obtain their signoff, then start independently delivering the services as defined in steady-state activities

## *Encouraged*

Prepare goals and timelines for steady-state SOC operations with MDR.

Debrief MDR with SOC team culture and have dedicated personnel to communicate with the SOC.

Undergo mock trial run of the defined pipeline before steady state.

Recognize and applaud the effort for defending a true positive incident.

## *Discouraged*

Generalized RACI matrix between SOC and MDR before steady state.

MDR having a pool of resources with no dedication to the customer for a large enterprise SOC.

Skipping team debrief sessions before or after SOC steady state.

Assigning MDR responsibilities that the SOC cannot enable or provide enough insight or access for.

## *Transform people*

When the SOC seats can't be filled by a team with the desired skill sets, then leveraging teamed services to achieve goals becomes important. The structure of roles and responsibilities across many facets of the SOC, such as engineering and detection and response, need to be refactored to have a clear understanding of what actions need to be taken and by whom. A teamed MDR service can offer engineering guidance in the form of a staff augmentation engineer to: service your SOC continuous iteration and improvement on ingestion of unsupported log sources, enhance data normalization to a common schema, create net new detection use cases, and develop custom playbook actions or integrations for your environment.

### Baseline coverage

Discovering and retaining talented team members is an industry-wide challenge since people grow in their career and transition to new roles and companies. Having a general skills and experience matrix for each SOC role and systemized onboarding and training plans will provide proper hiring guidance to identify talent who can be fully operational in their role 30-90 days after onboarding. Moreover, formalizing onboarding procedures and training plans for role and technology stack familiarization is crucial for effectiveness. Focus on achieving base coverage on tasks, then lean on the talent of the team to identify improvement areas and fill gaps. Remember that leaning on the talent of the team to fill gaps is temporary, not permanent.

Each SOC role should have its Knowledge, Skills, and Abilities (KSA) requirements aligned with the execution requirements of each SOP stage, specifically the responsibilities and expectations of each specific tier within the SOC, whether internal or outsourced. When implemented effectively it enables teams to leverage past skills and experiences to engineer iterative improvements to operational tasks. This also highlights areas where the SOC requires maturity and/or more resources to do their jobs without burnout. Enable teams to host internal training sessions and embrace creative approaches to improve team workflows. If the creative alternatives create too much overhead, then that is an indicator that the SOC may need additional assistance from a service provider or MDR to do their job effectively.

### Clarify roles in joint operations

When transitioning to a hybrid model with a MDR provider, it is critical to define and refine roles and responsibilities. The current L1 and L2 analyst responsibilities (if such a model is still in use) may no longer be the same when working with a MDR provider. The SOC should create a coverage model that is representative for shift hours to have 24/7/365 operating coverage. Share this with the MDR and work with them to come to a mutual understanding and alignment.

As SOPs improve and the MDR approach matures, the teams should be investing in automation opportunities. When these opportunities arise, embrace the

improvement and refine the RACI with a shifting goal post mindset. It is recommended to leverage the additional time saved from automation to enable the SOC to engineer other insights and grow in their careers, while working with the MDR provider to align with what is expected and achievable.

### Managing the unexpected

Managing risk is a fundamental aspect of SOC operations, whether it involves mitigating the impact of an incident or addressing personnel gaps due to life changes. Organizations should consider and be prepared for unexpected changes in staff availability, such as sudden departures or natural attrition. To address this, the SOC should collaborate with their MDR provider to develop contingency plans for quick, temporary coverage during personnel transitions. Having dedicated MDR team members assigned to the SOC can be highly beneficial during these periods, as they possess the required context and experience to maintain operational continuity without significant disruption.

Effective contingency planning helps new team members, who are being onboarded, have clear guidance and points of contact to understand their responsibilities for tasks, issues, and workflows. The speed at which new members can acclimate to the environment depends on how well-defined the existing processes are. Ideally, new team members should be given 30-90 days to fully integrate and become operationally effective.

## *Key takeaways*

### Embrace the unfamiliar

The SOC is transforming and utilizing a different approach that may be atypical to the organization's previous strategy or culture. Use this as an opportunity to transform culture to embrace forward-thinking approaches. Create a comfortable timeline to give the team the time it needs to take on additional tasks apart from day-to-day operations. Establish a phase of co-operation between legacy and joint operations. Use the transitory time to embrace the change and account for different people involved.

### Make peace with discomforting timelines

The security organization is often perceived as operating above their full capacity/bandwidth due to the long list of competing priorities that may include managing technical debt, conducting vendor POCs (Proof of Concepts), or recovering from a large incident. It is important to know that many of these critical initiatives will not be completed overnight and require a unified strategy and team to execute properly. Once the team has accepted that this will be an ongoing process, the team can focus carefully on transforming the SOC's technology, process, and people. Instill confidence in the SOC vision and execute on the defined milestones.

# *Case study*

A technology company, referred to here as "TechCo," embarked on a journey to adopt a new MDR provider and modernize their SOC, focusing on the three pillars of transformation: technology, process, and people. TechCo faced tight deadlines to transform their SOC due to the expiration of legacy MDR and technology contracts.

Despite having experience with a previous MDR, the security operations team was new to both SIEM and SOAR products, as well as the associated processes of its new MDR provider. The transformation was executed in a phased approach, aiming to provide live operational workflows within 90 days. However, the team encountered challenges due to the new MDR provider's lack of access to legacy tools and documentation, which hindered efficient requirement gathering and timely execution.

Additionally, the previous MDR did not have dedicated SOC personnel for TechCo, resulting in gaps in client knowledge and culture. This necessitated resilient and transparent communication between the new MDR provider, TechCo, and the legacy MDR provider throughout the migration process.

The transformation involved deploying cloud-native SIEM and SOAR platforms to enhance visibility, detection, and response capabilities. It also aimed to improve processes and workflows between the new MDR provider and TechCo. Part of this transformation included establishing standard conventions and consolidating inefficient or redundant workflows. The objective was to design an end-to-end pipeline process for detection and response to enable daily operations.

The new MDR provider assigned dedicated staff to TechCo, endeavoring to provide that the MDR manager and analysts were fully integrated into TechCo's operations. Previously, end-to-end documentation was not centralized, so this transformation also involved creating a centralized repository for many aspects of their SIEM and SOAR platforms, accessible to specific teams. This documentation encompassed data onboarding requirements (e.g. log source details, ingestion methods, supported formats for normalization, and log source points of contact), detection rule details (legacy rule names, new rule names, legacy SIEM logic, new SIEM logic, MITRE ATT&CK® mappings), integration details (integration names, points of contact, locations of securely stored secrets), and SOAR playbook details (SOPs, required integrations, and opportunities for automation improvement).

TechCo had the opportunity to have both MDR providers co-operate, allowing the new MDR and TechCo to leverage 30 days to shadow workflows and response procedures before terminating the legacy MDR services. The new MDR provider's well-defined requirements and processes compelled TechCo to improve accordingly.

The dedicated staff from the new MDR provider fostered a pattern of iterative improvement with TechCo, establishing a relationship akin to an extension of TechCo's SOC team rather than a separate entity. TechCo's SOC transformation resulted in enhanced visibility, detection, and automated response capabilities, with the opportunity to continuously iterate and improve its service using next-generation SOC technologies and processes, supported by a proficient MDR provider.

# *Scenario 3*

Transform SOC to catch up with modernized IT (DevOps, Platform engineering)

In some organizations, the speed of change in both business and IT is outpacing the ability of the SOC (and security in general) to keep up. This can be due to a number of factors, such as the adoption of DevOps and platform engineering practices, which results in a more agile and dynamic IT environment. As a result, SOCs may find themselves struggling to collect, analyze, and respond to security threats at a speed that matches that of their IT peers. If business and IT pull forward, while security pushes back, in our experience, security will almost always lose.

The main challenge is that when the IT counterpart to security is much faster (hours vs. months, in some cases), security needs to "speed up or shut up." Agile IT with 1990s-style slow security will fight, and the modern approach (IT) will normally win… putting the organization at risk.

These transformations require SOCs to become more agile, proactive, and effective in detecting, responding to, and mitigating security threats. In other words, it needs to catch up. By aligning closely with DevOps and platform engineering teams, SOCs can foster a culture of security as code, integrate security into the development process, and endeavor to provide that security is a shared responsibility across the organization.

The goal of this transformation is to create a SOC that is more responsive to threats, more efficient in its operations, and better able to aid the needs of the business—at their speed. This section discusses some of the specific changes involved in transforming an SOC to catch up with modernized IT.

## *Transform technology: Automation, integration, and enhanced data*

Technology changes include adopting new tools and technologies that are more in line with the DevOps and platform engineering methodologies. This might include tools like SIEM and SOAR, as well as various DevOps toolsets and other IT automation. For some organizations, a security team may be even further behind and be in the stage predating SIEM deployment. In addition, technology changes encompass both tool changes and architecture changes.

### Architecture changes

One specific change is to establish reliable, bidirectional data flows among the SOC, DevOps tools, and foundational IT infrastructure. This facilitates prompt sharing of security alerts, enabling timely remediation actions.

- Modern IT lessons also lead some SOCs to a security data fabric or security data broker models. This may mean using technology like Cribl or similar tools to ingest data into a detection pipeline or a modern SIEM.

- Another useful area where SOC both borrows from and aligns with modern IT is detection use case development. This covers new log types, but also new detection choke points and new trust boundaries [like Virtual Private Cloud Service Controls (VPC-SC) for cloud].

Security in general cannot be out of alignment with changes in IT architecture; use cases need to match what IT decides to do. And the same as in IT, watch for deviations: non-pipeline deployment is an alert (!)... most of the time. Can you really baseline against policy/procedure for a modern approach?

Finally, it is easy to pollute modern IT architecture thinking with a "strategically" placed, outdated tool. A SOC that insists on firewall appliances among the containers likely won't get very far.

### Tools changes

Several tool changes can support a SOC transformation to match the speed and agility of modern IT. These changes include implementing modern SIEM/SOAR tools to enhance threat visibility, streamline incident investigations, and automate response capabilities.

- Effective integration with cloud-native security tools can bolster the security of cloud environments and applications
- Consider transitioning to cloud-native SIEM products for greater scalability, ease of data aggregation, and enhanced analytics and threat intelligence capabilities
- SOAR platforms are essential for automating repetitive tasks and improving incident response times. They should integrate with broader IT automation systems for a more effective workflow
- Integrating security with modern CI/CD can improve the efficiency of security workflows. This integration can automate tasks, such as SOAR to Jira work, pipelines, and change logs, and present them in various news formats

### Data sources/collection changes

To align with the shift towards cloud-native and DevOps practices, it's crucial to adapt data collection strategies. Enable full logging and telemetry collection from cloud environments, containerized applications, and CI/CD pipelines.

Cloud brings both new telemetry sources and new context sources. Prioritize enriching this data with metadata from sources like Docker to gain a deeper understanding of asset relationships, vulnerabilities, and potential attack vectors within these dynamic environments.

### More DevOps ideas: Detection-as-Code

Detection-as-Code (DaC) represents a paradigm shift in threat detection, aligning security practices with modernized IT and DevOps methodologies. By treating detections as code (even if they are not written in a proper programming language), security teams can leverage the benefits of version control, automated testing, and CI/CD pipelines. This approach facilitates that detection rules are consistent, up-to-date, and thoroughly vetted before deployment.

In the context of SOC modernization, DaC plays a pivotal role in creating a holistic detection framework. It enables security teams to codify detection

rules, intending that they are easily shareable, auditable, and adaptable to evolving threats. Moreover, by integrating DaC into CI/CD pipelines, organizations can automate the testing and deployment of detection rules, reducing manual effort and accelerating response times.

The adoption of DaC also fosters collaboration between security and DevOps teams. By treating detections as code, security teams can work closely with developers to propose that security is integrated into the development process from the outset. This collaboration not only enhances the security posture of applications but also streamlines the development lifecycle by identifying and addressing security issues early on.

Furthermore, DaC complements other DevOps practices, such as Infrastructure as Code (IaC) and Policy as Code (PaC). By codifying security policies and infrastructure configurations, organizations can automate security checks and enforce compliance throughout the IT environment. This automation reduces the risk of human error and endeavors to provide that security is consistently applied across the entire infrastructure.

The adoption of DaC is a critical step in SOC modernization. By treating detections as code, organizations can create a more agile, proactive, and efficient security operations center that is better equipped to address the evolving threat landscape.

## *Transform process*

### Learn process from modern IT—Use CI/CD thinking

To keep pace with the speed and agility of modern IT, SOCs can adopt CI/CD principles for security updates and patches, assisting rapid vulnerability response. This involves establishing automated pipelines that streamline the testing, approval, and deployment of security fixes, reducing manual effort and minimizing exposure to threats.

A threat intelligence-driven approach is essential to prioritize security incidents effectively. By understanding the organization's critical assets and aligning security efforts with broader business goals, SOCs can focus on specific significant threats, adjusting resource allocation and reducing the impact of security incidents.

Integrating security into CI/CD pipelines is vital for vulnerability management, particularly in cloud-native environments. This integration enables automated security testing at each development stage, identifying and addressing vulnerabilities early in the development lifecycle.

DevOps practices, like binary authorization for containers and signed libraries for internal repositories, can enhance security by continuously analyzing workloads and preventing supply chain injections. These practices shift security left, helping mitigate risks before they manifest in production environments.

Adopting a reliability-focused approach, inspired by Google's Site Reliability Engineering (SRE), emphasizes the availability and health of the SOC platform itself. This proposes that security tools and processes are resilient and capable of supporting the organization's security needs.

Blameless post-incident reviews foster a culture of learning and continuous improvement within the SOC. By focusing on identifying root causes and implementing corrective actions, rather than assigning blame, SOCs can enhance their ability to prevent future incidents and improve overall security posture.

### Relentless focus on process automation

Automating routine tasks and incident response workflows to improve efficiency and to remain effective, SOCs should consider undergoing a transformation mirroring the agile nature of modern IT and DevOps practices. This shift necessitates:

***Automation and process adaptation***

- **Embrace automation iteratively:** Start small, focusing on automating routine tasks and incident response workflows. Establish feedback loops to continuously refine automation efforts
- **Adopt Agile methodologies:** Replace rigid processes with flexible ones that can adapt to the rapid pace of change inherent in DevOps environments
- **Implement version control:** Apply version control principles to security playbooks, detection rules, and configurations for better tracking and incident response
- **Address IT bottlenecks:** Recognize that legacy IT systems and practices can sometimes hinder security automation efforts and proactively work to address these challenges (we have encountered cases where IT was in fact behind security in terms of maturity)

***People and culture***

- **Foster a DevOps mindset in the SOC:** Cultivate a culture of agility, collaboration, and continuous improvement among security analysts
- **Embed security in development:** Encourage security engineers to work directly within development teams, promoting a "security as code" philosophy
- **Prioritize knowledge sharing:** Break down traditional tiered analyst structures, empowering team members to handle incidents and share knowledge effectively

### Key Takeaway

A modern SOC should be an integral part of the DevOps ecosystem. It should prioritize speed, automation, and a mindset that treats security as an essential component of the development process from the outset.

### Additional considerations

- While automation is vital, recognize the ongoing need for human oversight to develop, maintain and update automated systems
- Propose that the SOC's capacity for scaling keeps pace with the growth of threats and organizational assets

By implementing these changes, organizations can evolve their SOCs into proactive and efficient units, better equipped to address the dynamic security landscape.

## *Transform people*

In addition to changing the technology and processes within a SOC, it is crucial to also focus on fostering a change in mindset and approach among the people involved. SOC analysts need to be able to think and work in a more agile and DevOps-oriented way. They need to be able to adapt promptly to change and be able to work effectively in a collaborative environment.

### SOC to D&R: A culture journey

***Cultivating a culture of adaptability and growth***

The effectiveness of SOC transformation depends on empowering people to embrace change and continually evolve. Key focus areas include:

- **Fostering a DevOps mindset:** Cultivate a culture of agility, collaboration, and continuous improvement among SOC analysts, aligning with the fast-paced and iterative nature of DevOps
- **Embracing continuous learning:** Prioritize ongoing skill development in areas like cloud security, threat intelligence, and automation. Provide resources and opportunities for analysts to stay abreast of the latest security trends and leading practices
- **Promoting knowledge exchange:** Encourage regular cross-functional knowledge-sharing sessions between DevOps and security teams. This fosters a deeper understanding of shared challenges and facilitates the development of more effective security practices
- **Encouraging cross-team collaboration:** Assign analysts to temporary rotations or joint projects within DevOps teams. This provides valuable hands-on experience and strengthens collaboration across functions

***Building a 'fail fast, learn faster' environment***

- **Normalize experimentation and learning from mistakes:** Create a safe space for analysts to try new approaches, even if they don't regularly achieve the expected results. Celebrate lessons learned from failures as opportunities for growth and improvement
- **Avoid a 'hero mentality':** Discourage the tendency for analysts to stick solely to familiar tasks. Encourage a broader exploration of security challenges to expand skill sets and collective knowledge

By fostering an environment that supports continuous learning, experimentation, and collaboration, organizations can empower their SOC teams to adapt to the evolving threat landscape and effectively safeguard their assets.

### Evolving skills

***Upskilling for a modern SOC***

The skills required in today's SOC are evolving rapidly. To remain effective, analysts need to develop knowledge in several key areas:

- **Mastery of modern tooling:** Provide in-depth training on cloud-native security solutions, automation platforms, and threat intelligence tools. These technologies form the foundation of a modern SOC's capabilities
- **Understanding developer workflows:** Encourage analysts to learn scripting or basic coding principles. This will facilitate better communication with developers, enhance automation capabilities, and enable analysts to understand the security implications of code changes

- **Building strong communication skills:** Effective collaboration with DevOps and platform engineering teams is essential. Emphasize the development of communication skills that foster trust and shared goals

***Beyond technology: Adapting to new paradigms***

- **Cultivating architectural knowledge:** Deepen analysts' understanding of cloud infrastructure, application architectures, and emerging technologies. This knowledge is critical for effectively managing security in dynamic and evolving environments
- **Embracing new ways of working:** Equip analysts to adapt to the rapid pace of change inherent in DevOps. Understanding and aligning with these new approaches will enable the SOC to integrate effectively with the broader development lifecycle

By investing in the continuous development of these skills, organizations can build a SOC team that's ready to tackle the complexities of modern security challenges and collaborate effectively with their technology counterparts.

### Redefining roles: Humans and machines in harmony

The modern SOC embraces the strengths of both humans and machines. It's not about replacing analysts, but empowering them to focus on what they do better:

- **Embedded security specialists:** Integrate security engineers directly into development teams, fostering a proactive "security as code" approach
- **Collaborative problem-solving:** Prioritize knowledge sharing and teamwork over rigid escalation procedures. Empower many team members to tackle incidents and contribute their experience
- **Humans as the architects of automation:** Recognize that while automation is crucial, it requires human oversight and maintenance. Humans build, refine, and modify the machines that enhance the SOC's capabilities

## *Key takeaways*

### Empower analysts with an engineering mindset

Equip SOC analysts with the skills and knowledge to work effectively alongside developers and DevOps teams. This includes learning to code, understanding development workflows, and adopting a proactive approach to security.

### Humans excel at creativity and strategy

Leverage human strengths in areas like creative problem-solving, strategic thinking, and complex decision-making. Machines handle routine tasks, freeing analysts to focus on high-value activities that require human capabilities.

By embracing this collaborative model, organizations can build an SOC that is both efficient and adaptable, capable of addressing the ever-evolving threat landscape. Remember, it's the combination of human ingenuity and machine power that will drive the future of security operations.

# *Case study*

An industrial machinery manufacturing company, referred to here as "ManufacturingCo," recognized that a modern SOC requires more than just cutting-edge cloud-native tools. It demands a fundamental shift in philosophy, embracing the principles of DevOps, SRE, and other modern IT practices.

Frustrated by manual processes, a reactive security posture, and increasing analyst burnout, ManufacturingCo sought to bridge the gap between its SOC and the incredibly agile nature of its development and IT operations. Their transformation focused on two specific areas:

***1.*** Automation that sought to streamline tasks like threat intelligence enrichment and alert triage, enabling analysts to focus on higher-value activities.

***2.*** Establishing a collaborative platform to break down silos and foster effective communication and knowledge sharing between security, development, and operations teams.

Inspired by SRE, the SOC adopted KPIs and SLOs to measure effectiveness and drive continuous improvement. Security infrastructure was managed as code, bringing version control, automation, and consistency. Observability was prioritized, providing real-time insights into security events and system health. And through a shift-left approach, security was integrated earlier into the Software Development Lifecycle (SDLC), empowering developers to champion secure coding practices.

The results were transformative. Incident response times decreased significantly. The SOC shifted from reactive to more proactive and integrated, focusing on threat hunting and vulnerability management. Agility increased, allowing the SOC to adapt efficiently to evolving threats and business circumstances. And perhaps most importantly, a culture of shared responsibility for security emerged, strengthening the relationship between security and development teams.

ManufacturingCo's accomplishments underscore the power of Dev(Sec)Ops in building a modern, effective SOC. By embracing automation, collaboration, continuous improvement, and a shift-left approach, organizations can bridge the gap between security and IT, empower analysts, and cultivate a security-conscious culture.

# *Conclusion*

In today's rapidly evolving technology landscape, SOCs should be agile, proactive, and integrated to effectively safeguard organizational assets and brand reputation. They should employ rigorous processes while staying agile in the face of threats and business changes.

The three scenarios explored in this paper—cloud migration, MDR adoption, and alignment with DevOps philosophy—highlight the diverse pathways through which SOCs can modernize and enhance their capabilities when seeking *change* or *evolution*.

**Scenario 1:** Cloud migration as a catalyst for SOC modernization

While cloud migration offers an opportunity for SOCs themselves to rehost, replatform, or rearchitect their technologies alongside the business, they should also address the expanding threat landscape and update existing detection and monitoring capabilities in the process. Enhanced log management and integration is a necessity, detection and response paradigms shift, and SOC focus rebalances from endpoint-centric models to broader data correlation and aggregation facilitated by SIEM and SOAR tech.

**Scenario 2:** Adopt MDR and Modernize SOC to Build Hybrid Model

Adopting an MDR provider can drive the modernization of SOC technologies and processes, resulting in a strengthened security posture through a hybrid model that leverages the strengths of both internal teams and external parties. This transformation involves consolidating services and platforms, re-defining roles and responsibilities alongside their associated access controls, and building strong team connections and culture to foster collaboration.

**Scenario 3:** Transform SOC to catch up with modernized IT (DevOps, Platform engineering)

In organizations where the speed of IT change outpaces security, SOCs should adopt agile, proactive, and integrated approaches to keep up. This involves embracing automation, integrating security into CICD pipelines, and fostering a DevOps mindset amongst SOC analysts.

Common amongst the three scenarios, several key takeaways ring true:

1

**Enhance log management and the SOC technology platform:** Restructure and update the SOC technology platform to handle increased data volumes, aid broader security and operational use cases, and fully leverage modernized technologies. This helps the organization maximize its investment while maintaining agility to stay ahead of adversaries.

2

**Rebalance SOC focus by shifting Detection and Response paradigms:** Adapt detection and response strategies to leverage cloud-native capabilities and automation to enhance efficiency and effectiveness, moving away from endpoint-centric models to broader data correlation and aggregation to effectively manage the increased complexity and volume of security telemetry

3

**Build a collaborative and agile culture:** Foster a culture of collaboration, continuous improvement, and shared responsibility to effectively support the needs of the business and IT organizations while also investing in the people that drive the SOC.

4

**Above all, people matter:** Endeavor to provide that all approaches are supported by the requisite people, culture, mindset, teamwork, and leadership/sponsorship. Emphasize the importance of embracing change and investing in the continuous development and well-being of the humans that make up the SOC.

By embracing these principles and strategies, SOCs can transform into agile, proactive, and integrated units capable of addressing the dynamic security landscape, supporting the rapid pace of modern IT and business environments, and scaling to handle the next generation of threats facing organizations. The SOC is no longer a cost center but a strategic asset. It's a testament to the power of innovation, the resilience of human spirit, and the unwavering commitment to protect and defend.

By embracing change, SOCs can unlock their full potential and remain at the vanguard of cybersecurity, ready to face the challenges the future may hold. The future is not something we enter. The future is something we create. And by doubling down on the systems, processes, and humans that drive this discipline forward, the future of the SOC is brighter than ever.

## AUTHORS


***Dr. Anton Chuvakin***
Senior Staff Security Consultant
Office of the CISO
*Google Cloud*
chuvakin@google.com

***Mitchell Rudoll***
Advisory Specialist Master
Google Cloud Security Practice
*Deloitte & Touche LLP*
mrudoll@deloitte.com

***Robert Boshonek***
Advisory Managing Director
Google Cloud Security Practice
*Deloitte & Touche LLP*
rboshonek@deloitte.com


**Deloitte.**


This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms or their related entities (collectively, the "Deloitte Network"), is, by means of this communication, rendering professional advice or services. Before making any decisions or taking any action that may affect your finances, or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication. As used in this document, "Deloitte" means Deloitte Consulting LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright 2024 Deloitte Development LLC. All rights reserved.