Deloitte.

SOC CMM

The next generation SOC

A risk-based approach towards a Cyber Fusion Center

MAKING AN IMPACT THAT MATTERS since 1845

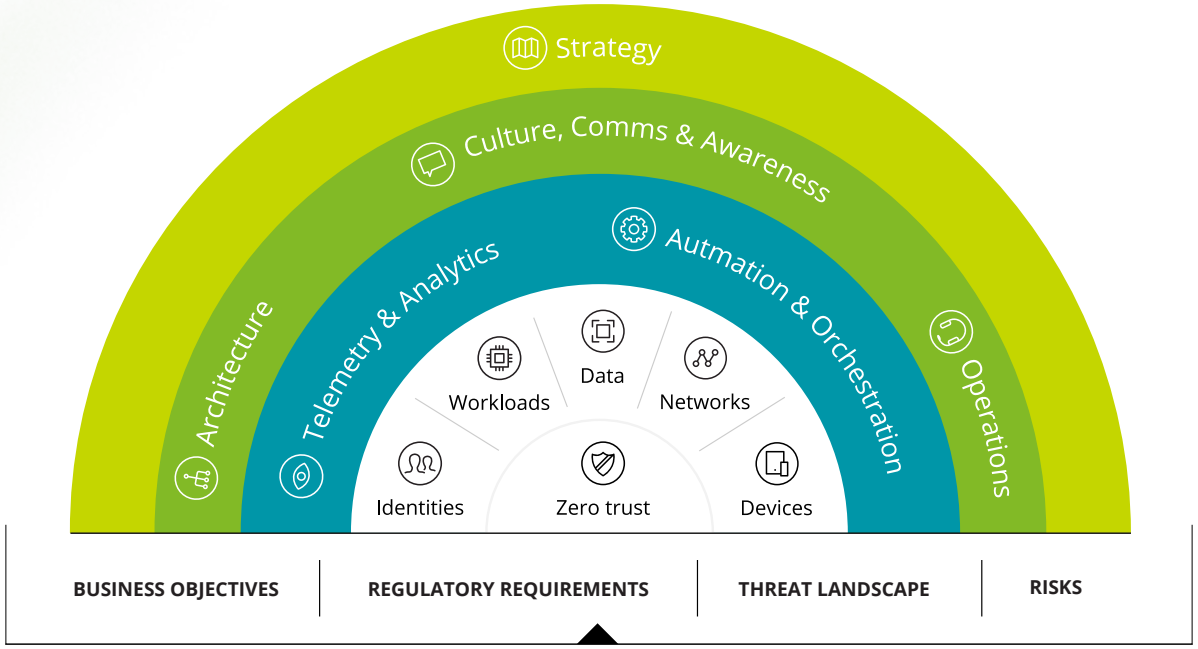
Table of contents

Executive summary

Keeping up with market trends is the natural way that organizations evolve. In fact, aiming for a competitive edge, organizations have been implementing emerging technologies to optimize their processes, foster growth, and continuously innovate. This digital transformation is no longer a choice, but a strategic imperative that drives new opportunities as well as new challenges to overcome.

Cyber attackers are becoming more and more sophisticated, developing new attack methods and outmatching the typical cyber defenses. Therefore, actions need to be taken to continuously monitor and efficiently respond on time to cyber threats. Technologies guarding the most critical business assets should be deployed and a tailored governance model should be defined and aligned between all organization's stakeholders. To match the ever-evolving attacker capabilities and deal with the complexity of managing cyber threats, a Security Operations Center (SOC) is becoming a strategic asset in an organization by providing essential cyber security capabilities to help increase resilience against cyber-attacks.

The implementation of a Cyber Fusion Center (CFC), also known as the next generation SOC, drives the compliance with the best security practices and frameworks such as SOC-CMM, SANS, NIST and MITRE ATT&CK®. Additionally, since the CFC itself is a main driver towards a Zero Trust posture, it should itself adopt the Zero Trust motto: "Never trust, always verify".
Deloitte's Multidisciplinary Zero Trust Framework, highlights the CFC's central role when adopting specifically on the **Strategy** and **Enabling** Layers.



STRATEGY LAYER
Zero Trust strategy should be aligned to the business drivers in a way that the journey is supporting the business, ensuring organization-wide adoption, future readiness and agility

GOVERNANCE LAYER
Zero Trust governance ensures a cohesive top-down strategy that considers stakeholder consensus to achieve necessary cultural, architectural and operational changes

ENABLING LAYER
Enabling layers help automate & orchestrate enforcement policies while continually analyzing enforcement decisions to identify Zero Trust violations

CORE DOMAINS
A Zero Trust model is built upon strong foundational capabilities across five fundamental domains. The maturity across these domains will ultimately determine Zero Trust maturity

Throughout this article we will detail the key challenges faced by traditional SOCs and how they can be transformed into a successful, cutting-edge, business and risk-oriented SOC. In addition, we will provide an overview of our proven, comprehensive *Cyber Fusion Center Journey* followed by a benchmark with industry trends collected from our experience supporting worldwide organizations with SOC transformation programs.

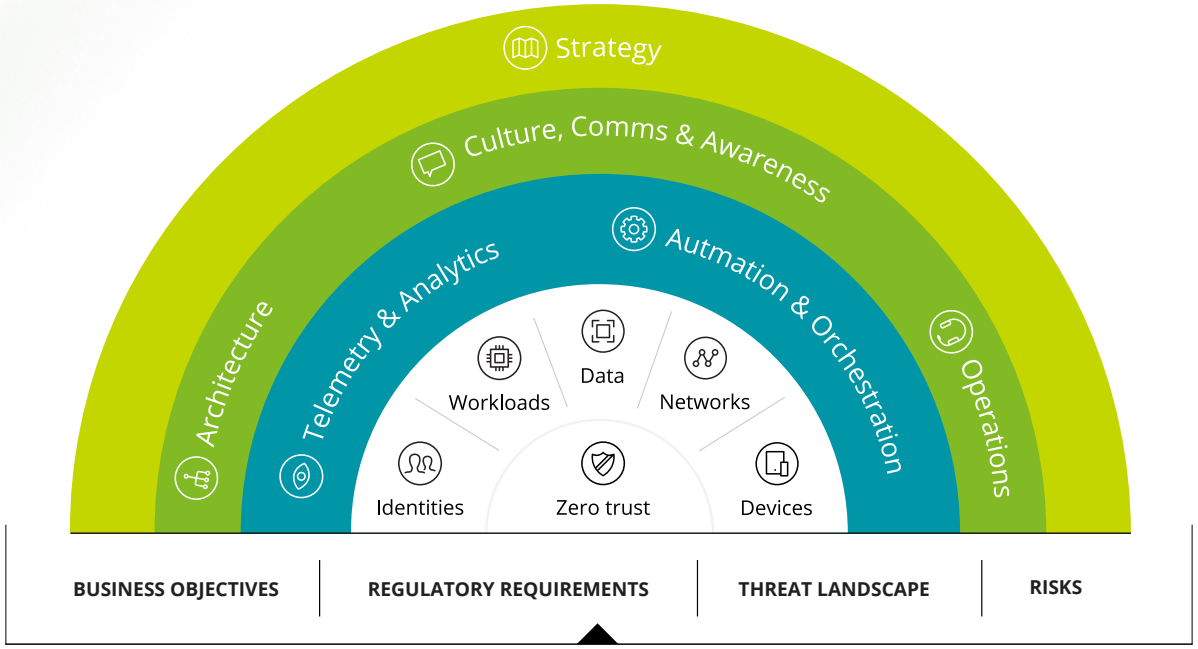
Zusammenfassung

German version of the Executive summary

Mit den Markttrends Schritt zu halten, ist die natürliche Art und Weise, wie sich Unternehmen weiterentwickeln. Um sich einen Wettbewerbsvorteil zu verschaffen, haben Unternehmen neue Technologien implementiert, um ihre Prozesse zu optimieren, das Wachstum zu fördern und kontinuierlich innovativ zu sein. Diese digitale Transformation ist keine Wahl mehr, sondern ein strategischer Imperativ, der neue Chancen und Herausforderungen mit sich bringt, die es zu bewältigen gilt.

Cyber-Angreifer werden immer raffinierter, entwickeln neue Angriffsmethoden und überwinden problemlos die typischen Cyber-Abwehrmaßnahmen. Daher müssen Maßnahmen ergriffen werden, um Cyberbedrohungen kontinuierlich zu überwachen und effizient und rechtzeitig darauf zu reagieren. Technologien, die die kritischsten Geschäftsressourcen schützen, sollten eingesetzt werden, und ein maßgeschneidertes Governance-Modell sollte definiert und zwischen allen Stakeholdern des Unternehmens abgestimmt werden. Um den sich ständig weiterentwickelnden Fähigkeiten von Angreifern gerecht zu werden und die Komplexität des Managements von Cyberbedrohungen zu bewältigen, wird ein Security Operations Center (SOC) zu einem strategischen Vermögenswert in einem Unternehmen. Es stellt wichtige Cybersicherheitsfunktionen bereit und erhöht so die Widerstandsfähigkeit gegen Cyberangriffe.

Die Implementierung eines Cyber Fusion Center (CFC), auch bekannt als SOC der nächsten Generation, fördert die Einhaltung der besten Sicherheitspraktiken und -frameworks wie SOC-CMM, SANS, NIST und MITRE ATT&CK ®. Da das CFC selbst eine Autorität für eine Zero-Trust-Haltung ist, sollte es sich außerdem das Zero-Trust-Motto zu eigen machen: “Never trust, always verify”. Das multidisziplinäre Zero-Trust-Framework von Deloitte unterstreicht die zentrale Rolle des CFC bei der Einführung einer Zero-Trust-Haltung, insbesondere auf der Strategy und Enabling Layer.



STRATEGY LAYER
Die Zero-Trust-Strategie sollte so auf die Unternehmensfaktoren abgestimmt sein, dass sie das Unternehmen unterstützt, und eine unternehmensweite Anwendung, Zukunftsorientierung und Agilität sicherstellt.

GOVERNANCE LAYER
Zero-Trust-Governance gewährleistet eine einheitliche Top-Down-Strategie, die den Konsens der Stakeholder berücksichtigt, um die notwendigen kulturellen, technischen und betrieblichen Veränderungen zu erreichen.

ENABLING LAYER
Die ENABLING-Ebene hilft bei der Automatisierung und Umsetzung von Entscheidungen. Gleichzeitig werden diese laufend analysiert, um Verstöße gegen Zero Trust zu erkennen.

CORE DOMAINS
Ein Zero-Trust-Modell basiert auf starken Geschäftsfähigkeiten (foundational capabilities) in fünf grundlegenden Bereichen. Der Reifegrad in diesen Bereichen beeinflusst am Ende die Zero-Trust-Reife.

In diesem Artikel beschreiben wir die wichtigsten Herausforderungen, mit denen traditionelle SOCs konfrontiert sind, und wie sie in ein erfolgreiches, hochmodernes, geschäfts- und risikoorientiertes SOC umgewandelt werden können. Darüber hinaus geben wir einen Überblick über unsere bewährte, umfassende Cyber Fusion Center Journey, gefolgt von einem Benchmark mit Branchentrends, die wir durch unsere Erfahrung bei der Unterstützung weltweiter Unternehmen bei SOC-Transformationsprogrammen gesammelt haben.

Key challenges

A Security Operations Center (SOC) is a critical function within an organization, engaging people, technology, services and processes to ensure real-time monitoring and analysis of security events, aiming to continuously monitor and enhance an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

The world is increasingly interconnected, bringing about new risks alongside new growth opportunities. As the risk of financial loss and reputational damage are continuously increasing, businesses can no longer afford to rely solely on reactive measures. A Cyber Fusion Center (CFC) demonstrates its worth to the business by embracing a proactive approach to risk management and enhancing the organization's ability to meet compliance, obligations and protect the business from harm.

While working with multiple cross-country organizations from a wide variety of sectors, we have concluded that traditional SOC strategies do not manage to achieve the full potential of what we envision to be a cutting-edge CFC.
This fact is mainly due to the following:

01
Working in silos

SOC teams are often isolated in the organization and not fully integrated with IT/tech teams leading to delayed and slower response times.

02
IT/Technology Driven

SOCs were originally created by IT/Tech teams. Detect & respond activities are frequently very inefficient due to lack of meaningful business and risk context when an alert is raised.

03
Blindspots

Digital transformation enabled organizations to quickly adopt new technologies and devices, exponentially increasing the attack surface and creating multiple blind spots, especially on Cloud services (SaaS), the IoT/OT world and on the Application Level.

04
Embryonic or absence of advanced detection capabilities

Traditional SOCs rarely integrate advanced capabilities required to detect emerging threats in hyperconnected environments.

05
Talent

Shortage of cybersecurity professionals sparks intense competition for talent, which in turn poses challenges in retaining the skillset of SOC teams, mainly due to the high job turnover.

During the last few years Deloitte has supported several organizations in different industries to evolve their SIEM/SOC practice, by driving a risk-based approach to enable this transformation considering their risk appetite, industry threat landscape and established SIEM/SOC capacity and capabilities.

Call to action

Operating a successful Cyber Fusion Center requires a deep understanding of how the SOC is currently operating. This means it is important to evaluate several domains to assess the maturity of a SOC from its business drivers, to people, technology, services and processes. When it comes to transforming a SOC, there is no one-size-fits-all solution. Therefore, Deloitte has developed a proven and comprehensive transformation approach named ***Cyber Fusion Center Journey***, which includes 3 phases leveraging several accelerators and standards:

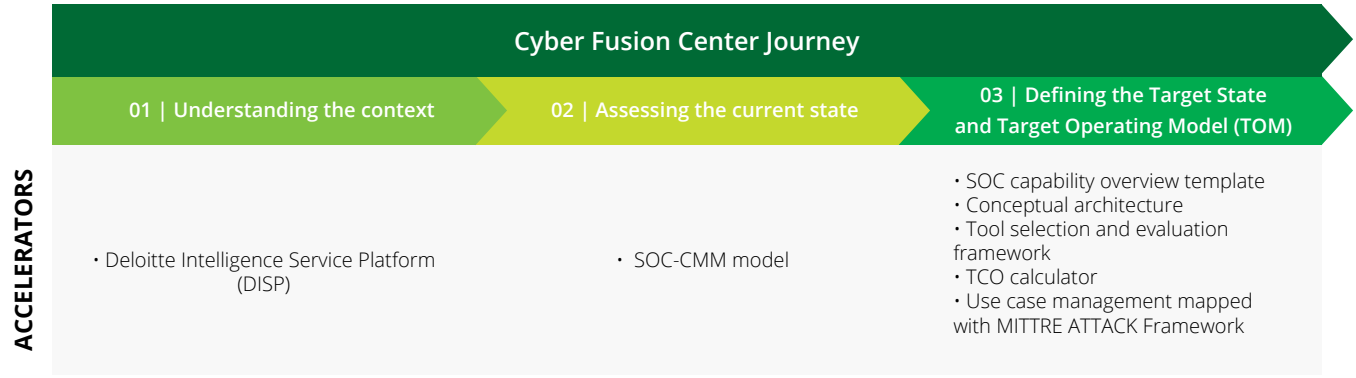


Diagram 1: Cyber Fusion Center Journey

01 Understanding the context

Within our approach, we initiate the transformation by holding several workshops with relevant stakeholders to understand the business, context and risk appetite of the organization alongside with the applicable industry threat landscape.

To have a meaningful threat landscape we leverage our threat intel information available in Deloitte's proprietary intelligence platform, which provides information about cyber threats, trends and the most common tactics used by attackers in the target organization's industry.

Deloitte accelerator:

- Deloitte Intelligence Service Platform (DISP[2]) helps organizations to gain visibility into cyber threats with meaningful and actionable insights, based on their business and technology profiles. Our intelligence services analyses trends impacting the cyberthreat landscape for several industries providing frequent reports with indications and warnings of evolving tactics, conducting program reviews to ensure timeliness and accuracy, cataloging activity to track changes to analytic lines, and efficiently reviewing defensive posture measures (e.g., endpoint detection, alerting rules, operator analysis, security tools, and business processes).

02 Assessing the current state

In phase 2, we conduct an extensive assessment of an organization's SOC by leveraging the SOC-CMM framework, which evaluates the SOC's maturity in 5 domains, by asking questions such as:

Business	People	Processes	Technology	Services
What are the business drivers that led to the implementation of the SOC? What strategy is defined for the SOC? Is there a governance process in place?	Are staffing, sourcing and retainment strategies implemented? Are different tiers/roles defined? Is a training and career progression program defined?	What processes are in place for operating and managing the SOC? Is a SOC handbook defined? Are SOC operation reports produced? Are the use cases defined based on a methodology?	What technologies are used in the SOC? What security capabilities are provided? What log sources are integrated?	Is there a formalized list of services provided by the SOC? Are SLAs defined? Are Incident Management, Vulnerability Management, Forensic Analysis, Threat Intelligence and Threat Hunting, services provided?

[2] https://www2.deloitte.com/us/en/pages/risk/articles/cybersecurity-threat-trends-report-2023.html?id=us:2sm:3yt:db44:eng:abt:031821

Call to action

SOC-CMM accelerator:

The **SOC-CMM model**[3] was initially created as a scientific research project to determine characteristics and features of SOCs, such as specific technologies or processes. From that research project, the SOC-CMM has evolved to become the defacto standard for measuring capability maturity in Security Operations Centers. At the core of the assessment tool lies the SOC-CMM model, that measures maturity across 5 domains and capability across 2 domains (technology & services).

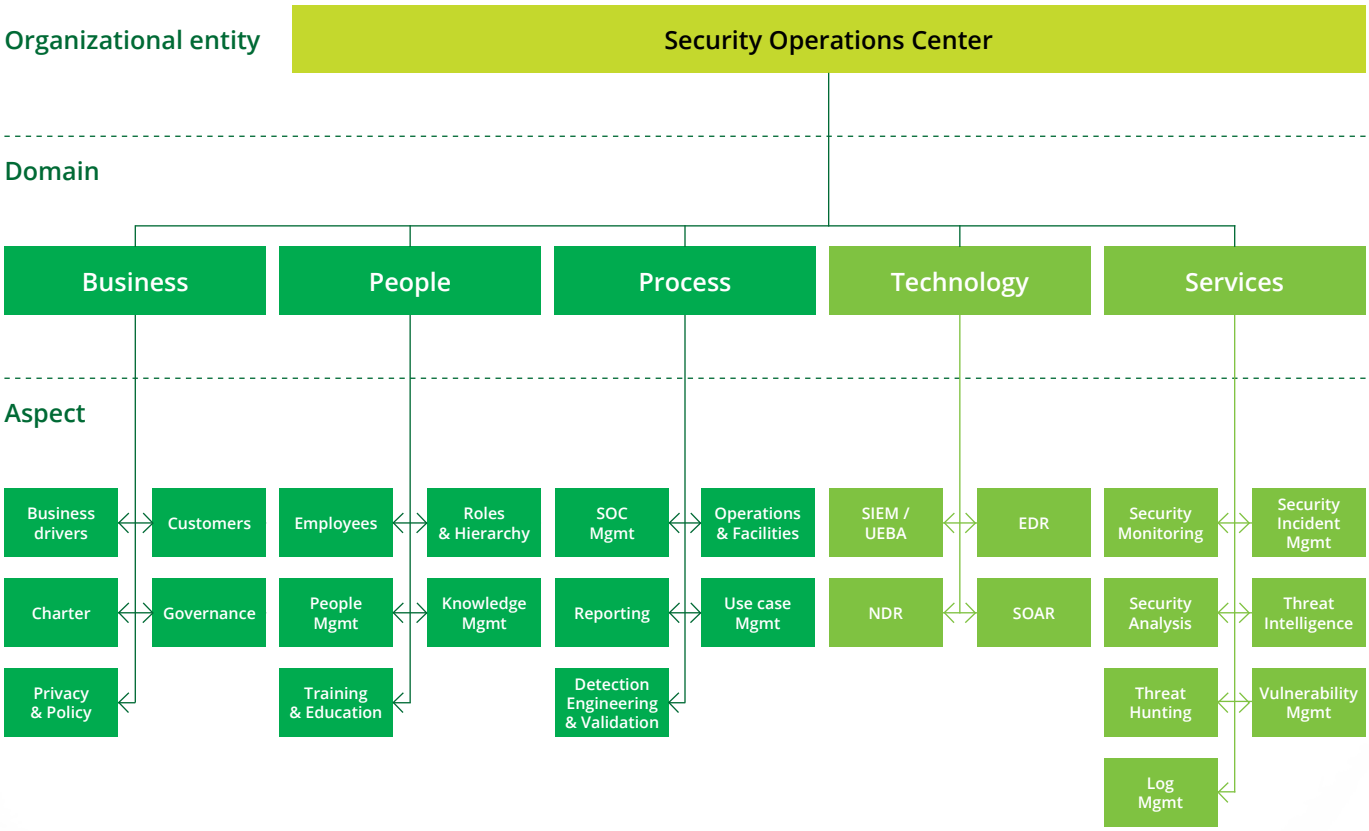


Diagram 2: Domains and capabilities of the SOC-CMM model

03 Defining the target state and Target Operating Model (TOM)

Defining the target maturity for a SOC is key to planning a roadmap and prioritizing the main activities and investments to achieve it. For each domain, specific areas must be addressed, and strategic decisions must be made.

Business (Governance)

One of the key topics in building an effective SOC is to determine where it fits best in the organization's structure and how the various teams and units are interconnected (e.g., Management Team, CSIRT Team, SOC Team, IT/OT Teams). For this matter, a clear structure alongside with roles, responsibilities and processes should be defined, aligned and implemented.

There is a general agreement to setup your cyber governance following a **3 lines of defense model**: this is used to help organizations identify structures and processes to best achieve their objectives and facilitate strong governance and risk management by assuming the existence of three lines – Risk Ownership, Risk Oversight, and Risk Assurance.

[3] https://www.soc-cmm.com/introduction/

Call to action

03 Defining the target state and Target Operating Model (TOM)

Business (Governance)

This approach should be tailored to meet each organization's objectives and enables:

- Governance accountability to stakeholders for organizational oversight;
- Management action to achieve objectives through risk-based decision making;
- Assurance and advice from an independent internal audit.

The **first line** is mainly responsible for the product and service delivery to manage risk while the **second line** supports risk management by providing expertise on risk-related matters. Aiming compliance, the **third line** provides assurance and advice in an independent and objective manner. Once again, there is no one-size-fits-all solution – this is effective when adapted to the organization's structure and is strongly aligned to prioritize interests through cooperation, collaboration, and communication[4].

A successful SOC is reliant on how these 3 lines cooperate with each other and how they are engaged with other business units. For this purpose, it is key to establish a shared responsibility matrix and a governance model to ensure these 3 lines have a common strategy and its priorities are aligned with the business – most of all, it is crucial to avoid working in silos.

Determining how the 3 lines will interact and what their responsibilities are, means to answer questions such as "who maintains SOC-related technologies," "who develops use cases", "who collects and manages intelligence"," and "who is responsible for incident response procedures". It is also critical to ensure that reporting lines and oversight are in place: this helps avoid miscommunication, especially when it comes to accountability.

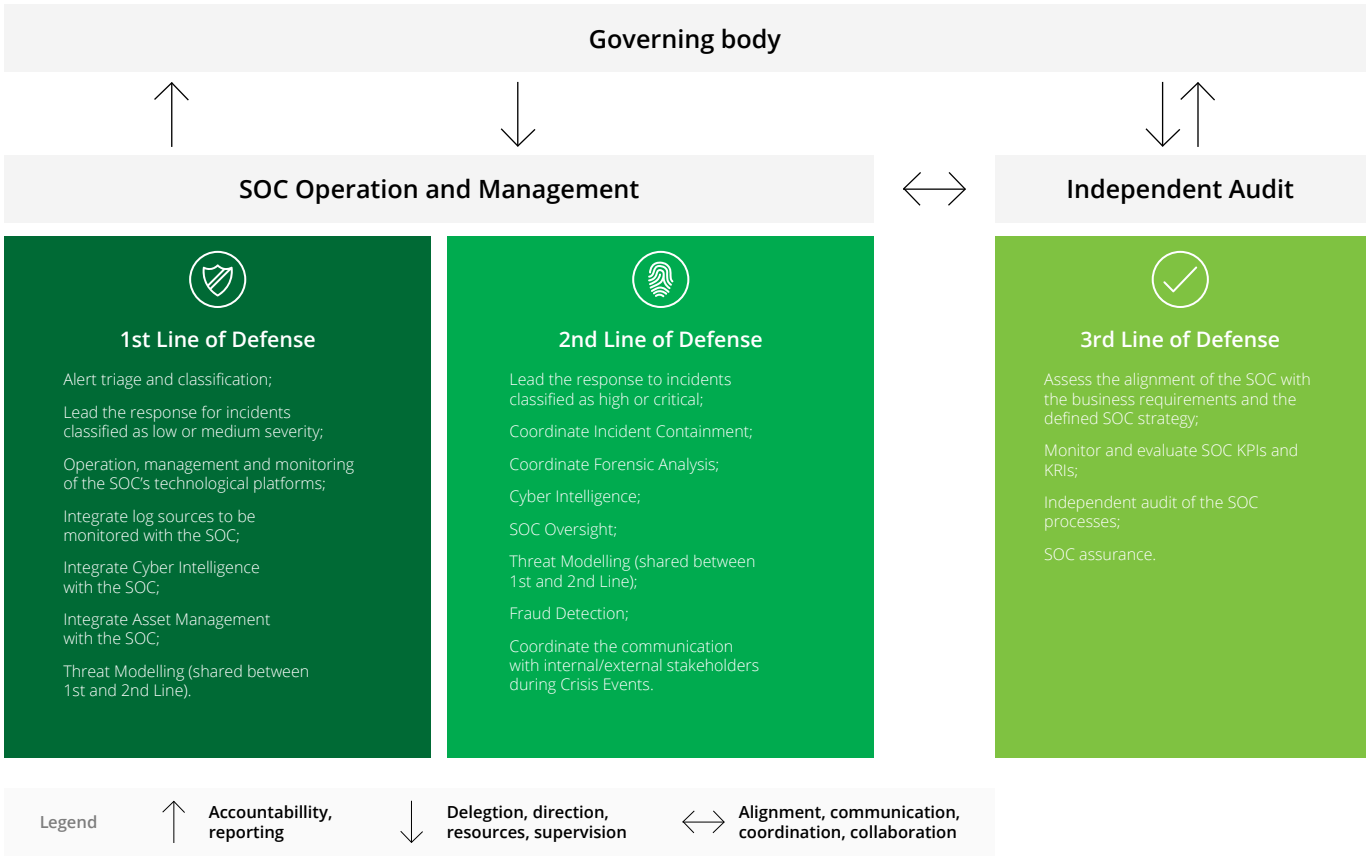


Diagram 3: A high-level example of a shared responsibility model for the 3 lines of defense.

[4] The Institute of Internal Auditors (2020, July). The IIA's Three Lines Model (The Institute of Internal Auditors). three-lines-model-updated-english.pdf (theiia.org)

Call to action

03 Defining the target state and Target Operating Model (TOM)

People (Operative Model)

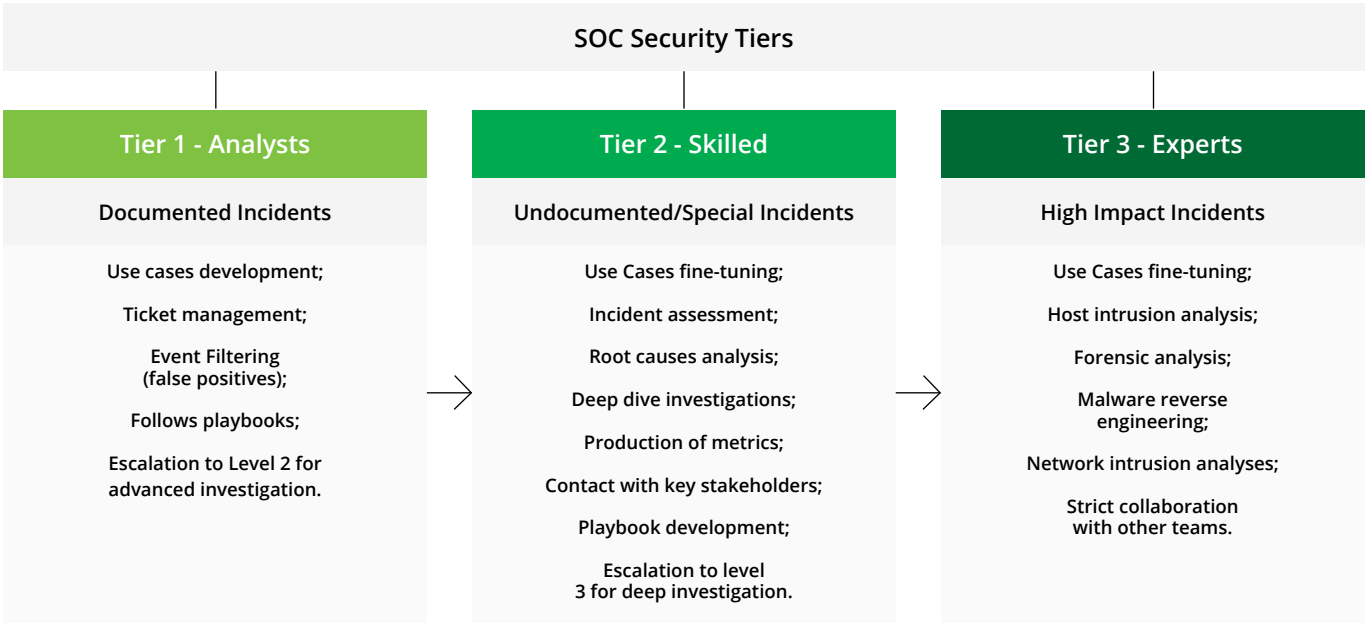
The continuous evolution of the cybersecurity threat landscape demands quick reaction to change, adopting and implementing new detection rules and improving response capabilities. The difference between a successful and unsuccessful response to an attack is likely on the effectiveness of a SOC team. Therefore, choosing the right **operating model is one of the main decisions**.

Typically, the SOC is structured with 3 tiers which are actioned depending on the incident criticality:

01 Tier 1 analysts are the first to respond - they typically analyze the incident, classify it according to its criticality and respond to incidents marked with a low critically following a documented playbook.

02 If a playbook has not yet been designed or if the incident requires specific expertise the incident is transferred to Tier 2.

03 If required, Tier 3 experts are involved as they have the necessary expertise and a deep knowledge of the organization and its infrastructure.



A summary of the main typical responsibilities for the 3 tiers

Selecting the operative model is a strategic decision that should consider several decision items such as the industry sector, organization's size, business needs, operating hours, and allocated budget. Pros and cons for these decision items should be in mind when defining the operative model. Typically, three main options are considered: internal, external or hybrid.

Internal
A highly customized solution, an **internal SOC** is best suited for large organizations with a mature approach to risk management. Keeping the SOC entirely internal means that all the expertise is retained within the organization and operates with a higher level of commitment, ensuring that incidents are prioritized as appropriate. On the other hand, it limits exposure to external practices and broader threat landscape, leading the SOC to become isolated.

Call to action

03 Defining the target state and Target Operating Model (TOM)

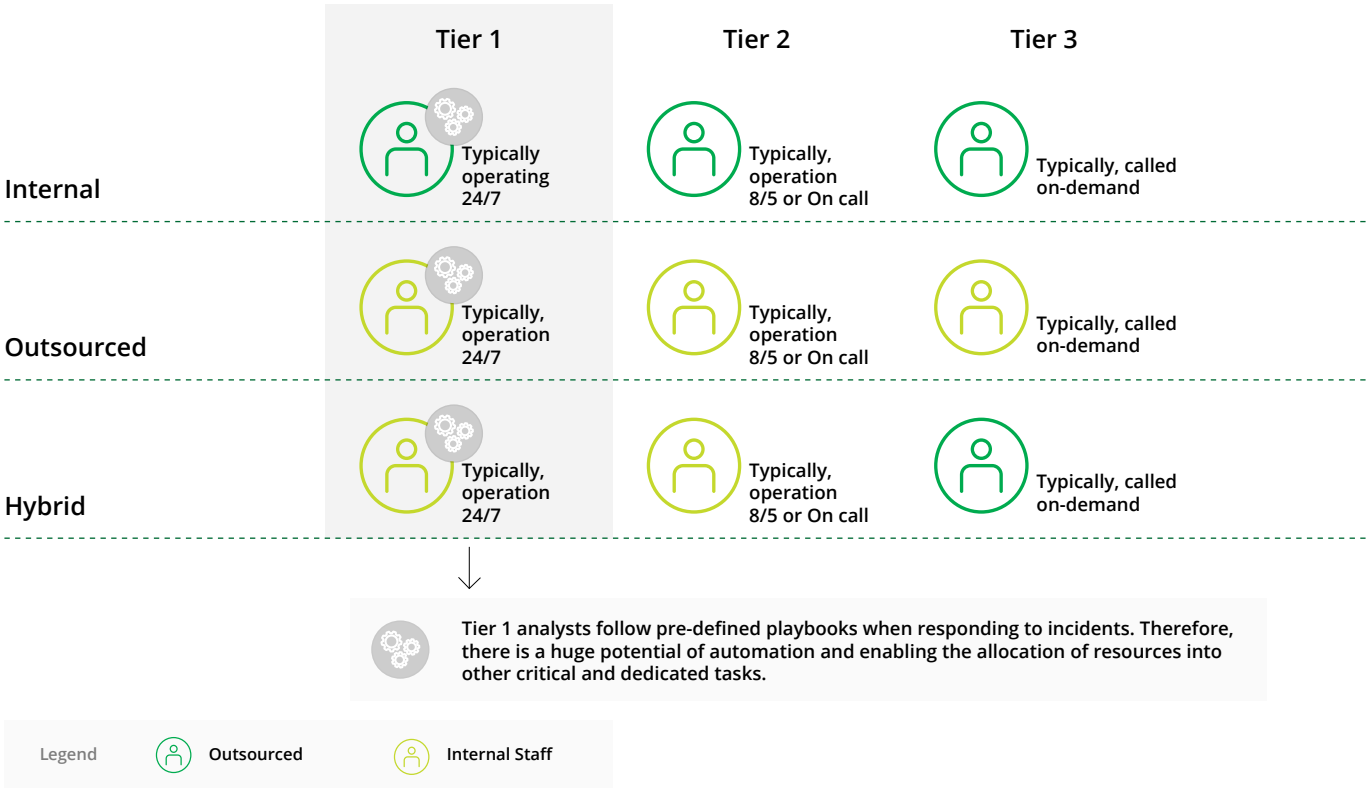
People (Operative Model)

Outsourced
Faster to implement and usually requires a lower investment, this **external operative model** delegates SOC management to an external provider, typically a Managed Security Services Provider (MSSP), who is responsible for providing on-demand, fully trained personnel and continuous threat monitoring. The downsides when adopting this operational model are (1) external teams rarely hold business context which is key to evaluate the impact of an incident and (2) additionally create dependency on a vendor for a critical function.

Hybrid
In a hybrid operating model, external SME expertise is complemented by internal knowledge and capacity. Choosing a hybrid model allows the organization to benefit from the human and technological resources of the external provider, while retaining senior analysts in-house, and can serve as an optimized solution for a lack of capacity or resources to operate 24/7. Due to the inherent characteristics of the function (highly repetitive, rotating shifts and associated costs), tier 1 is typically outsourced or replaced by automation solutions, while tier 2 and 3 specialists with more specialized knowledge are retained in-house to handle more critical incidents.

A different hybrid setup strategy could be service based: there are certain capabilities which require specific expertise that usually is difficult to have internally, or it is recommended to have an external perspective (e.g. Threat Hunting, SAP/Application Security Monitoring, Cyber Wargaming).

While this model can be more complex to implement than the previous ones, the benefits outweigh the drawbacks in most cases, making this option a growing market trend.



Introducing automation on tier 1 on a tier-based CFC

Call to action

03 Defining the target state and Target Operating Model (TOM)

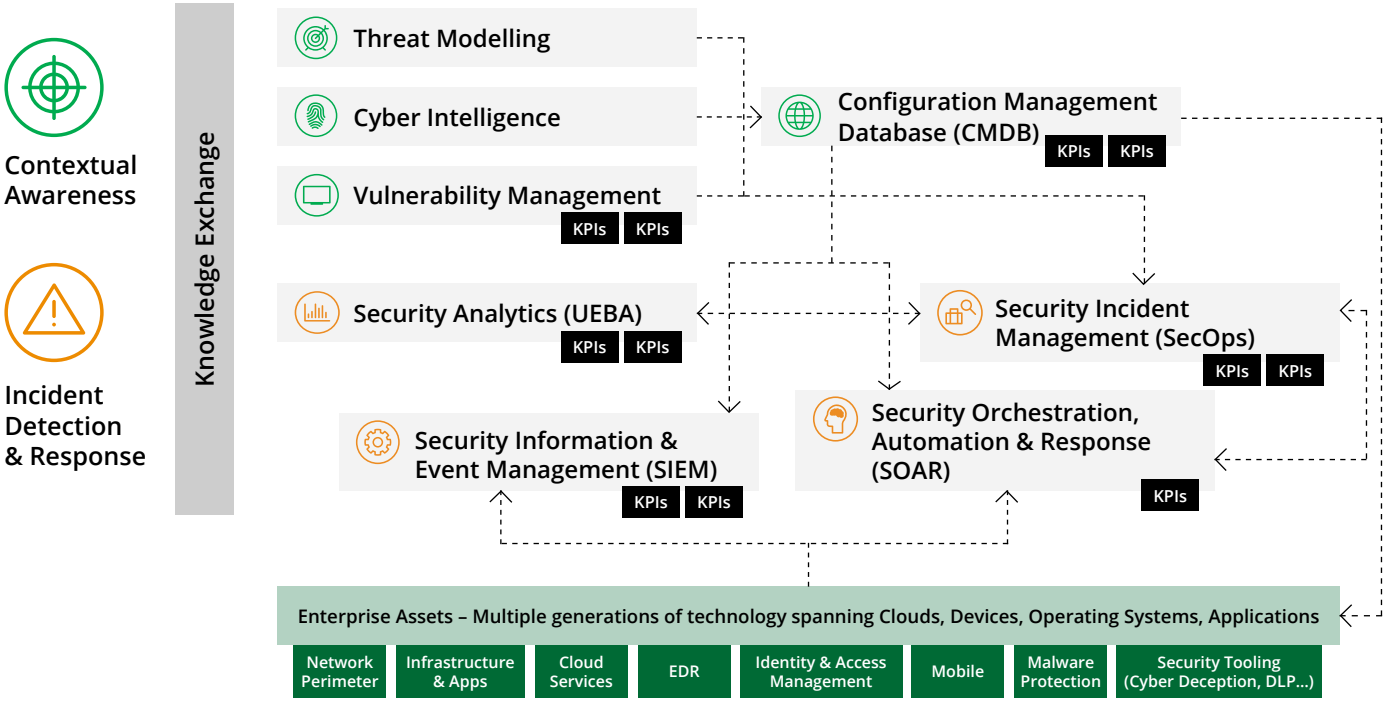
People (Operative Model)

Processes
Defining repeatable and auditable processes is key in every business and likewise it is so in a SOC. Not only to ensure service continuity as team changes but also to operate a SOC: from the basis on who to communicate and when, to the response playbooks ensuring organizations are responding to incidents in a consistent, effective manner.
Frequently, traditional SOCs lack documented processes, a unified knowledge-sharing platform for use-case playbooks, and a defined procedure for implementing new use-cases with a risk-based approach.

Deloitte accelerator:

- Use case playbooks mapped with MITRE ATT&CK Framework

Technology
Technology plays a key role to deliver the proposed SOC services, with the adequate tools. However, it is often a pain-point as there are many solutions in the market that have overlapping capabilities and, depending on the organization ecosystem, some solutions may be more fitting than others. Proper requirements engineering is vital for the selection of the most appropriate tool.



Technology Conceptual Architecture

As part of requirements engineering, it is also important to investigate how these tools integrate (e.g. Ticketing tool, CMBD, SIEM, SOAR, Vulnerability Management) and how much effort is needed to maintain these tools.
These are relevant inputs to calculate the total cost of ownership (TCO) of the SOC. For this purpose, Deloitte created a TCO calculator for the most common security tools used in a SOC.

Deloitte accelerator:

- Tool selection and evaluation framework
- TCO technology calculator

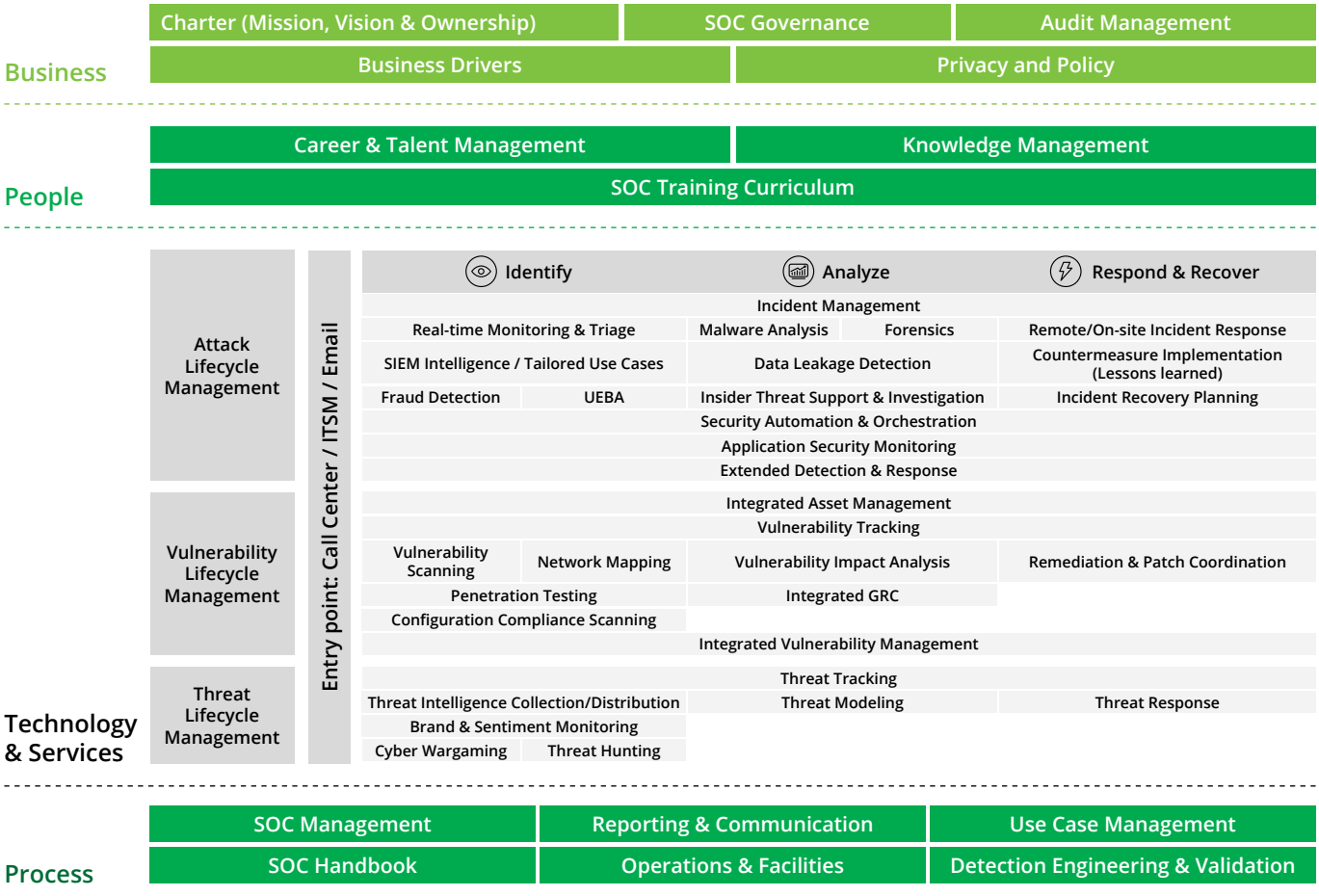
Call to action

03 Defining the target state and Target Operating Model (TOM)

Services (Capability Model)

Defining which services shall be provided by the SOC is often a complex but vital task to ensure that the SOC meets its intended purpose. For this matter, it is important to have a clear vision of what is the maximum potential of a SOC and define which capabilities make sense to integrate based on the organization's expectations, budget, attack surface that should be monitored as well as a threat modelling exercise. Many SOCs perform threat modelling based on MITRE ATT&CK information to determine their monitoring capabilities, and their most relevant attack techniques

Deloitte developed the SOC+ capability framework which includes a complete SOC template model that we usually use to bootstrap and accelerate the discussions on the desired capabilities of an organization.



SOC capability overview template

Take it to the next level

Taking the Cyber Fusion Center (CFC) to the next level implies enhancing or improving the capabilities, processes, or effectiveness of the CFC's operations. Developing a world-class security operations center requires continuous improvement approach. Security teams can use automation solutions to improve response times and reduce human error when addressing incidents.

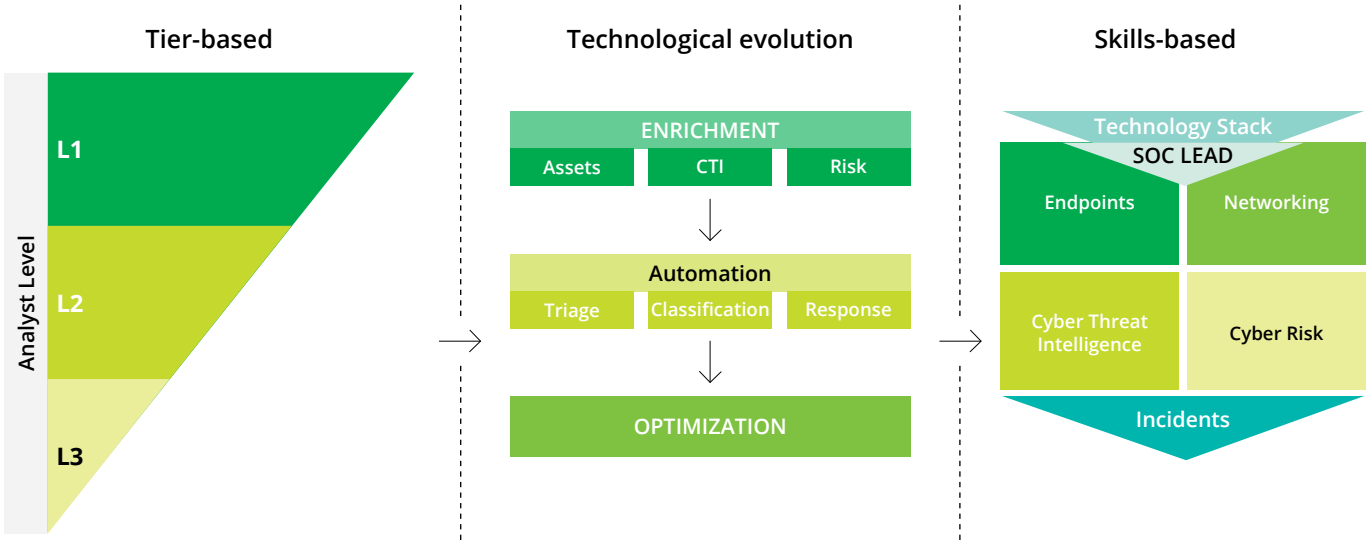
With the exponential growth in technology density, manual resolution of large numbers of alerts is no longer feasible or efficient - there are simply not enough first-line security professionals to properly assess each ticket.

To maximize CFC efficiency, **a security orchestration, automation, and response (SOAR)** solution can be implemented. A SOAR can connect and integrate disparate tools, collect data, and trigger playbooks that orchestrate response workflows.

As automation begins to reduce the dependency on Level 1 analysts, they are now free to focus on more complex and critical non-automated tasks. The result is a significant improvement in response times and team efficiency, leading to increased security maturity and overall business optimization. In addition, this technology enhancement enables a tipping point in the governance model, where the initial triage is handled by the more experienced staff – the **A Team**.

The **A-Team** consists of a small group of highly skilled and experienced individuals with a deep understanding of the organization's mission, each of whom independently possesses the set of skills necessary to identify and respond to malicious intent.

By rethinking the organization of the CFC around skills, not tiers, and focusing on automating decisions where possible and prudent, the A team will have the autonomy necessary to focus on their highly specialized area and uniquely human tasks, resulting in the mitigation of today's widespread cybersecurity talent and skills shortages[5].



The traditional tier-based model leads to the isolation of response activities by different levels of analysts and centralizes crucial operations such as sorting and classification by less experienced analysts.

The progressive technological evolution with its emphasis on automation and optimization reduces the need to have level 1 analysts responding to routine tickets, leaving only more complex tasks to be addressed by more experienced analysts.

The subsequent elimination of level 1 analysts leads to a shift from a tiered model to a skill-based model, where the SOC is made up of SMEs working cooperatively to address incidents as they arise.

Evolution from a tier-based to a skills-based CFC

[5] Google Cloud; Deloitte (2020). Future of the SOC. SOC People: Skills not Tiers. Deloitte_and_Chronicle_Future_of_the_SOC-Skills_Before_Tiers.pdf

Success stories and industry benchmark

Deloitte has a proven track record supporting different clients across several industries and geographies in successful transformation SIEM/SOC projects.

Multinational bank in Europe
(Financial Services)

New regulatory requirements for Financial Services (DORA) and an Internal Audit report demanded an establishment of a new Target Operation Model (TOM) for the SOC and significant increase on the visibility and threat detection over the mainframe infrastructure and adopted cloud services in a major bank in Europe.

KEY OUTCOMES

- Establishment of a Leading-Edge Cyber Security Capability and Security Culture
- Transformation of cyber security capabilities to a high level of maturity
- Central control of distributed security resources
- Integrated security logs from the mainframe infrastructure in the SIEM solution following a threat modelling exercise using the MITRE ATT&CK Framework

Multinational telco in Europe
(Telecommunications)

The Telco's small & mid-size customers demanded a new line of business for these organizations, as they are requiring MSSP services alongside with internet and connectivity services. This originated a transformation of the Telco's external SOC service with increased capabilities and capacities to respond to this demand.

KEY OUTCOMES

- Establishment of a governance model for the SOC with internal resources
- Creation of a sustainable organization and development of an optimized security operating model
- Creation of in-house of key capabilities (from level 1 to level 3)

Multinational retail company in Europe
(Retail)

Following a major cyber incident that remained undetected for weeks, Deloitte supported a retailer company to assess its current SOC maturity state (using SOC-CMM), define a new target state and target operating model based on industry leading best practices while following a risk-based approach.

KEY OUTCOMES

- Establishment of a new governance model for the SOC embedded with the 3 lines of defense model
- Transformation of the current operating model for the SOC from outsourced to hybrid while ensuring the ownership of the SOC
- Creation of in-house of key capabilities (level 3 experts)
- Roadmap of initiatives to ensure contextualized information (e.g. CMBD integration) for the security incidents and a risk-based approach to prioritize what to protect first and increase visibility and threat detection
- Introducing automation with SOAR implementation

Multinational chemical company in Europe
(Chemicals)

Following a Cyber Security Assessment and new regulatory requirements (NIS and NIS 2.0), a major Chemical organization decided to implement a SOC to be able to detect threats in both IT and OT environments.

KEY OUTCOMES

- Establishment of a governance model for the SOC with internal resources and outsourcing L1 and L2
- Assessing the best suitable technology stack for the organization considering IT and OT environments
- Creation of in-house of key capabilities (level 3 experts)
- Introducing automation with SOAR implementation

Contacts

Frederico Macias
Partner & Global TMT
Risk Advisory Leader
fremacias@deloitte.pt

Rob van Os
CEO
SOC-CMM
rob@argos-csa.nl

Georg Schwondra
Partner
Cyber Risk
gschwondra@deloitte.at

Gerald Kattnig
Director
Cyber Risk
gkattnig@deloitte.at

André Sousa
Solution Senior Manager
andrsousa@deloitte.pt

Deloitte.