HWG Sababa

Security Operations Center: in-house or outsource?



In the face of today's rapidly evolving threat landscape, companies find themselves at a crossroads when deciding the fate of their Security Operations Center (SOC). The strategic choice between maintaining SOC functions in-house or outsourcing them demands careful consideration. This whitepaper aims to shed light on the factors influencing this decision, providing valuable guidance for Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) to make informed choices tailored to their specific needs.

While in 2018-2023 the global number of cyberattacks grew 61%, Italy has seen the growth of 300%[1]. In addition to that, the pace of complex cyberattacks has increased too – the average dwell time between a breach and an active stage of an attack, has dramatically reduced from 2+ months to slights over 3 days[2]. It makes companies look for security solutions, which would provide ongoing security monitoring across their interconnected infrastructures, analysis of alerts and identification of attack patterns at their earliest stages, and fast and accurate response and remediation.

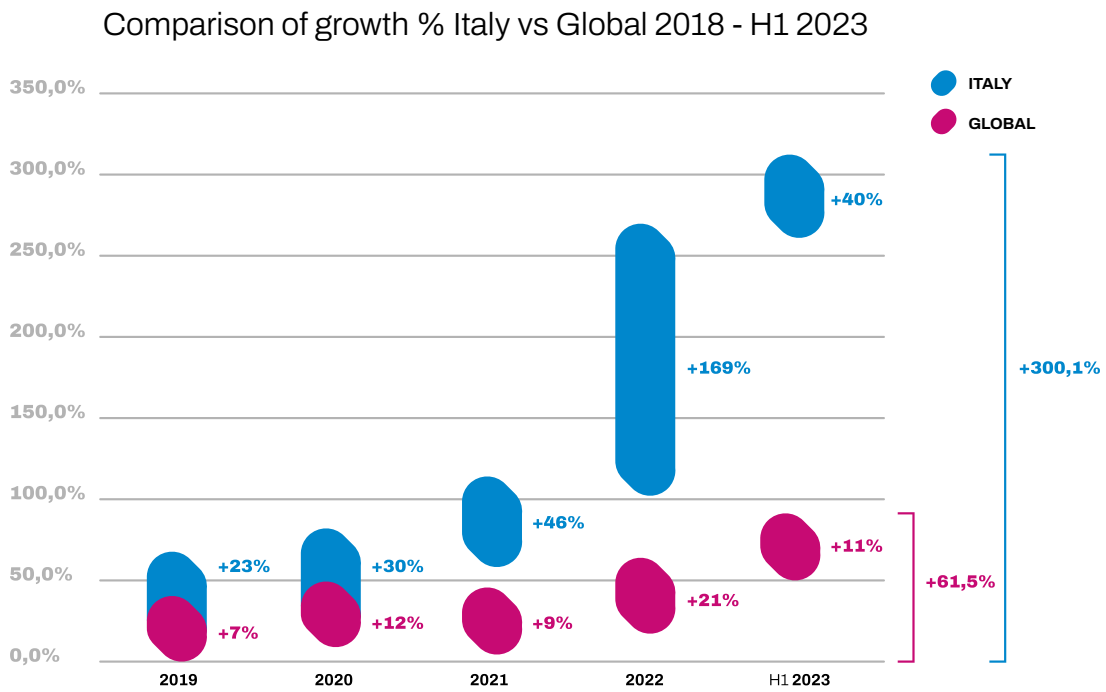


Image 1 *- Cyberattack growth 2018-2023, Clusit*

[1]Clusit Report 2023

[2]X-Force Threat Intelligence Index 2023, IBM

The portrait of a typical SOC user is changing too, varying across verticals. In addition to Finance and Critical Infrastructures, which are among early SOC adopters, and Government and Manufacturing industries, which are hit harder that the other Italian enterprises in 1H23[3], companies from Utility, Transportation, Retail, Fashion and Telco tend to consider and adopt various SOC strategies to increase cyber resilience of their organizations. On top of comprehensive IT security, their objectives include safeguarding their operational technology (OT) systems, interconnected networks, communications, IoT and IIoT devices and smart infrastructures, ensuring security for financial and supply chain operations, intellectual property, and customer data, through constant control and orchestration of the array of the security solutions used within the organizations. This variety of verticals going to SOC as their strategic cybersecurity investment, identifies multiple aspects impacting a list of requirements to managed security providers. Security solutions must be tailored with respect to vertical compliance, existing infrastructure, security maturity, business objectives, and available security management resource.

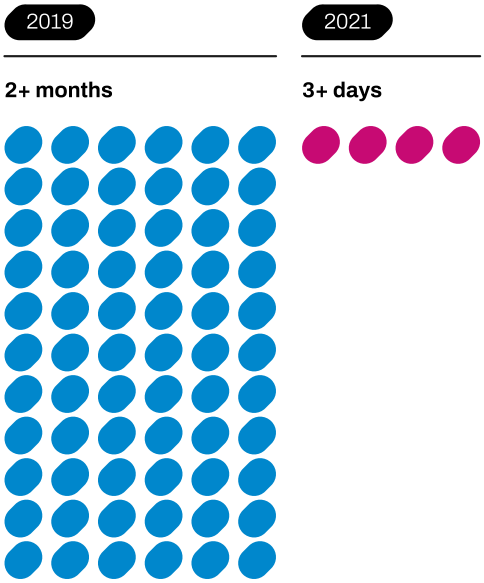
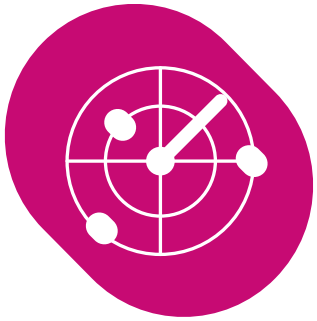


Image 2 - *Average duration of ransomware attacks, 2019- 2021, IBM*

What types of SOC can you choose from?

There is no one right SOC model to operate or deliver modern SOC functions. SOCs vary according to their mission and goals, which are influenced by characteristics such as their risk tolerance, the vertical in which companies operate, level of maturity, skills and expertise, processes and procedures, tooling employed and how security services are leveraged. Saying that, Gartner defines 3 main SOC models – Internal, Outsourced (Tiered) and Hybrid[4]. Till now, internal SOC has been spread among large well-funded enterprises with critical assets to protect. However, the situation is changing as the SOC complexity and expectations are growing.



[3]Clusit Report 2023

[4]Use the Gartner SOC HIT Model, 2021

By 2025, 33% of organizations that currently have internal security functions will attempt and fail to build an effective internal SOC due to resource constraints, such as lack of budget, expertise and staffing. At the same time, by 2025, 90% of SOCs in the G2000 will use a hybrid model by outsourcing at least 50% of the operational workload[5].

Going for fully outsourced or hybrid SOC models, when external cybersecurity experts behave as an essential extension of the internal security teams, has multiple reasons behind. These include:

1. Limited internal security team capacity.

While in 2022, a shortage in cybersecurity experts was estimated at 3.4 million globally, in 2023 this gap reached 4 million[6]. Few companies have complete security teams, and those team members often suffer from too high pressure and professional burnout[7]. Cost-effectiveness - with no need to hire and retain experts who work 24x7 – and easier scalability for the cases your company grows, innovates, changes objectives and has to get compliant, makes companies go for this SOC model.

2. Small variety of security roles.

Not only the number of security experts, but also their proliferation play an important role. Trying to understand how many security functions are actually performed in-house, many companies find out that their internal competences are limited. To be able to address any security aspect throughout the security cycle, companies need *various functions* presented in their teams to work closely to ensure cyber resilience of their organization.

3. Cybersecurity beyond IT.

With the digitalization process going on across industry verticals, the security scope extends beyond IT. By 2027, 75% of security teams are expected to have on-boarded at least five tools to manage cyber-physical systems (CPS) security in operational, production or mission-critical environments, which is a major increase compared with one or two they might use today[8]. It makes enterprises prefer SOC providers experienced in OT and IoT/IIoT security projects, with deep vertical skills to address some specific needs and respect compliance against vertical security standards.

4. Efficiency.

Outsourced SOCs manage vast volumes of data and security events, often numbering in the millions of events per second (EPS). They implement extensive sets of rules and playbooks, far exceeding the out-of-the-box offerings from security vendors and internal effort results. This heightened level of automation and efficiency ensures that your organization is better equipped to detect and respond to threats promptly.

[5]SOC Model Guide, Gartner, 2021

[6]ISC2 Cybersecurity Workforce Study: Looking Deeper into the Workforce Gap, 2023

[7]We Need To Talk More About Burnout In Cybersecurity, Forrester, 2023

[8]Market Guide for Operational Technology Security, Gartner, 2023

5. Workforce distribution.

With a globally distributed workforce, outsourced SOCs have enough people to work in shifts and operate around the clock. While internal night shift employees sleep, the outsourced SOC team remains vigilant, protecting your organization and its assets from cyber threats no matter where they originate. This global coverage is crucial for businesses with customers and partners across the world.

6. Data security & sustainability.

One of the most compelling arguments for outsourcing the SOC is data security and sustainability. Contrary to concerns about data exposure, a reputable SOC provider, being structured into several Tiers, adheres to stringent security protocols. They are well-equipped to safeguard your sensitive information, often more effectively than an in-house team, which may be more susceptible to insider threats or accidental data breaches.

7. Access to the latest security technologies.

Finally, the level of protection provided by an outsourced SOC can be a significant deterrent against advanced persistent threats (APTs) or accidental ransomware attacks. Lack of context related to what is seen, detection and response automation and orchestration are the greatest challenges for full utilization of the internal SOC capabilities[9]. The external SOC providers are equipped with the latest technologies, threat intelligence, and incident response strategies – beyond any standalone vendor can offer – reducing the likelihood of successful cyberattacks.

What other factors to watch out when choosing a SOC provider?

Whatever SOC model works better for your organization, there are some additional factors and trends, which may impact your decision in 2024:

Security provider consolidation.

Having to ensure protection across IT, OT and IoT domains, companies find themselves working with multiple security providers. Aiming at finding the right balance in the number of contractors to work with, 75% of companies have been consolidating the number of their suppliers in 2023 – from 29% in 2020[10], preferring those providers with broader offerings.

[9] SANS SOC Survey 2023

[10] Integrating SASE, XDR and Other Security Vendor Consolidation Trends in Security Strategy, Gartner 2022

Current supply chain challenges.
Cyberattacks, including state-sponsored ones, add pressure to supply chains alongside the rising costs, labour shortages, and certain product delays[11]. Shorter supply chains are easier to protect end-to-end, while the preference of the local suppliers, including security providers, guarantees easier compliance with the standards.

Generative AI application.
In fact, artificial intelligence is serving as an impressive tool to identify and prevent cyber-attacks. Organizations integrate AI for more efficient and scalable SOCs, with *generative algorithms* intended to transform decision-making, business communication, and threat management. This evolution promises to streamline existing processes, improve detection capabilities, and automate threat hunting activities. In the medium term, this integration of AI is expected to gradually replace lower-level analysts, enabling them to redirect their focus towards higher value-added activities. So the customer's choice would fall on SOC providers with years of experience and multiple certifications in place.

Assess, Plan, Act



Selecting the right SOC for your organization demands a strategic and tailored approach. Staying aware of the evolving threat landscape, the diversity of SOC models, and key considerations influencing the decision-making process, you can enhance your organization's security posture.

Consider the following action plan for a thorough self-assessment:

1. **Evaluate Your Current Security Status:**
Assess the effectiveness of your existing security measures, processes, and procedures. Identify any gaps or vulnerabilities that may expose your organization to potential cyber threats. Be ready to embrace that the maturity of the IT processes and awareness of common cybersecurity threats can be higher than those in OT or IoT domains.

2. **Define Ideal SOC Requirements:**
Determine your specific requirements for a SOC, considering the unique aspects of your organization. Set clear objectives and expectations for potential SOC suppliers, including considerations for internal team collaboration.

[11] European supply chain update – refocusing on reliability - August 2023

3. **Establish Requirements for SOC Suppliers:**
Define critical factors such as 24/7 monitoring, the scope of security functions conducted in-house (IT/OT/IoT), and the expected volume of security events. Consider the integration of playbooks and the extent of automation needed in your security operations.

4. **Assess Internal Capabilities:**
Reflect on the question: "How many security functions are we really capable of doing in-house effectively?" Be honest about the limitations and strengths of your internal security team.

5. **Seek Alignment with Business Objectives:**
Ensure that the chosen SOC model aligns seamlessly with your organization's broader business objectives. Consider scalability, cost-effectiveness, and the ability to adapt to future changes in your business landscape.

Keep in mind that the ideal SOC solution is not one-size-fits-all. It should be a bespoke fit for your organization's unique challenges, objectives, and operational intricacies.

About HWG Sababa SOC

HWG Sababa is an Italian company providing cybersecurity as a complete suite of strategic solutions, managed services and consultancy. Its SOCs in Verona and Vilnius guarantee proactive monitoring of the digital environment across IT, OT and IoT environments, capable of preventing, detecting, analyzing, and responding to cyber threats. HWG Sababa SOC caters enterprises from various verticals, including central banks, energy production sites, telco, healthcare, and other critical infrastructures across the globe.

Though you cannot find two equal SOC projects, as all of them are tailored for each customer, the key functional areas of the SOC remain instant:

- **Detection and response**
  A team of cybersecurity experts monitors the structure 24 hours a day, 7 days a week, identifying even the most complex attacks across IT, OT and IoT domains, already in their initial stages and immediately implementing responses to ensure complete protection.

Intelligence and threat hunting

Provides valuable insights into cyber threats and their actors. Specifically, these activities allow us to trace the origin of attacks and collect substantial evidence for in-depth incident investigations across open source, deep web and darknet.

Exposure management

Potential risks and vulnerabilities that can be exploited by attackers are carefully analyzed and mitigated preventing real attacks, due to a combination of applied threat modelling, vulnerability scanning and risk analysis techniques.

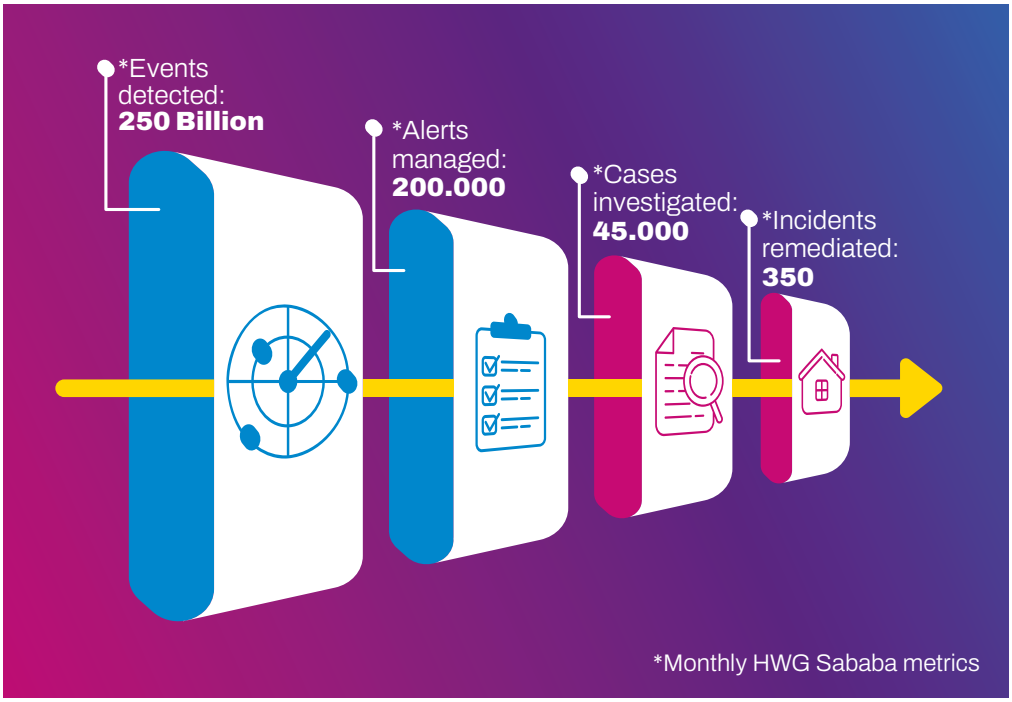
Security automation

When cyberattack attempts repeat, there is a chance to mitigate them automating the effort. Speed up the detection and reduce the response time through automated security operation orchestration, freeing up security experts to focus on more prioritized areas for business.

Observability

Integrate security metrics with non-security KPIs through behavioral analysis of assets across the entire enterprise infrastructure, helping to detect anomalies and cyberattacks at an early stage.

Processing millions of security events every month, the HWG Sababa SOC transforms them into 45.000 of investigated cases, and 350 remediated cases for their clients.

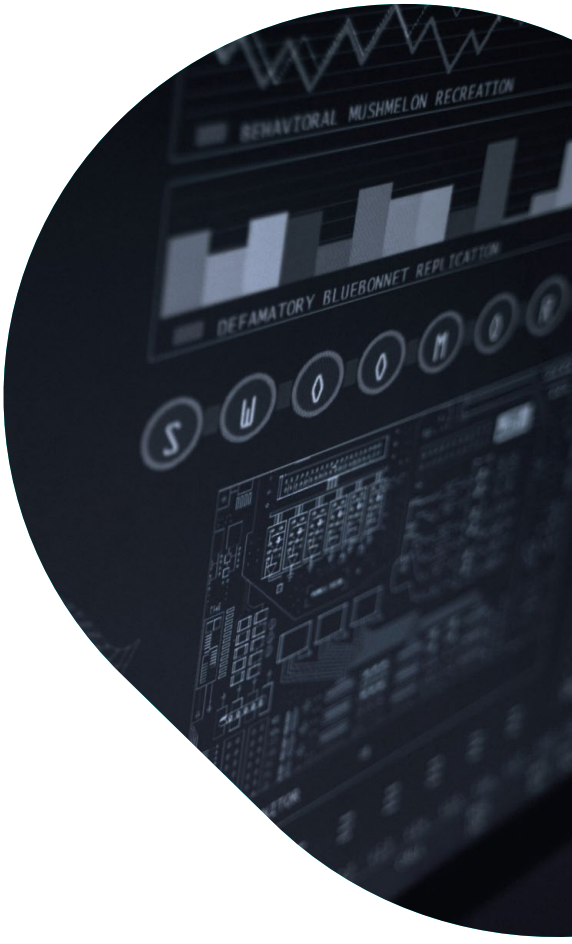


- Up and running since 2008
- Customers 125+/verticals
- Managed IBM EPS 100.000/month
- customized playbooks 200+
- 98% under SLA
- 70 experts, grouped into 3 tiers
- 2 locations
- 24x7x365
- 300+ certifications, including GPEN, GWAPT, CISSP, CCIE, PMP and other

Discover some real cross-vertical SOC cases:

- Ansaldo Energia (Energy)
- Selda Informatica (Government / Healthcare)
- Unit Plus (Transportation)

Contact us to deepen the knowledge about the HWG Sababa SOC



HWG Sababa

Follow us on:

www.hwgsababa.com