HWG Sababa

HWG Sababa HyperSOC™

Transforming Cybersecurity from Reaction to Resilience



A SOC Model Under Pressure

Today's security operations centers (SOCs) are expected to secure increasingly complex digital ecosystems while simultaneously navigating budget cuts, staff shortages, stricter regulations, and sophisticated threats.

Despite rising expectations, many enterprises still operate fragmented security environments – siloed tools, high false-positive rates, and slow incident response times. Alert fatigue drains teams. Compliance audits create bottlenecks. And when incidents happen, the lack of contextual visibility across IT, OT, IoT, and cloud surfaces makes root cause analysis and risk containment painfully slow.

Security leaders are under pressure not just to detect threats, but to prove risk reduction, deliver measurable outcomes, and align their investments with broader business objectives.

Why the Traditional SOC Model No Longer Fits



• **Cyber complexity is rising.**
The organizations are increasingly facing attacks across multiple environments,including OT,cloud,and hybrid.With data volumes growing at 30%YoY[1] and an average of over 45 security tools per company[2], these environments are becoming harder to protect.



• **Talent remains scarce.**
With a global shortfall of 4 million cybersecurity professionals[3], the situation is expected to worsen by 2028. The skills gap in security operations will deepen, with one-third of all senior roles projected to remain unfilled for over a year[4].



• **Compliance is tightening.**
EU regulations like NIS2, DORA, CRA, and sectoral frameworks (e.g., IEC 62443) now demand fast reporting, lifecycle visibility, and built-in controls.



• **C-Suites want proof.**
CISOs are now asked to tie security metrics to business KPIs – operational uptime, compliance readiness, and financial exposure.

Traditional MSSPs often fall short, offering narrow detection services or inflexible platforms that don't scale across sectors or risk models.

[1]How Hyperautomation Is Used to Reduce Gaps and Inefficiencies in Network Cybersecurity, IDC, September 2023
[2]The more cybersecurity tools an enterprise deploys, the less effective their defense is, ZDNET
[3]ISC² 2024 Cybersecurity Workforce Study
[4]Predict 2025: There Will Never Be an Autonomous SOC, Gartner, December 2024
(https://www.gartner.com/doc/reprints?id=1-2KBPAKPG&ct=250220&st=sb)

Why HyperSOC™

24/7/365 Monitoring
Always on, always ready, with around-the-clock threat detection and response.

AI-Powered & Automated Operations
Uses AI and automation to reduce noise, speed actions, and deliver contextualized, rapid responses.

Unified IT + OT Visibility
End-to-end monitoring across IT, OT, IoT, cloud and hybrid ecosystems.

Vendor-Agnostic Integration
Protect existing investments with vendor- agnostic integration – no costly replacements.

Tailored Playbooks & Methodologies
Proven response frameworks and SLAs that adapt to your environment.

Certified Expertise
300+ certifications across disciplines ensure world-class skills and execution.

CARES
Full visibility into security posture, KPIs, tickets, and documentation through CARES – a dedicated customer portal

Modular, Scalable Design
Tiered service model that grows with your security maturity.

Introducing HyperSOC™

HWG Sababa's HyperSOC™ redefines the SOC- as-a-Service model by combining deep visibility, intelligent orchestration, and expert human oversight across IT, OT, IoT, cloud and hybrid environments. It's designed not just to detect threats – but to outpace them.

By integrating real-time monitoring, threat intelligence, and hyperautomation through the proprietary PULSE™ platform, HyperSOC enables organizations to simplify complexity, accelerate response, and gain operational confidence – all while staying audit-ready. Its tiered model adapts to sector-specific risks and regulatory demands, making it ideal for both critical infrastructure operators and digitally evolving enterprises.

Vendor-agnostic, easy to integrate, and supported by strategic advisory, HyperSOC helps security leaders turn security monitoring into a business-aligned capability that is scalable, resilient, and ready for what's next.

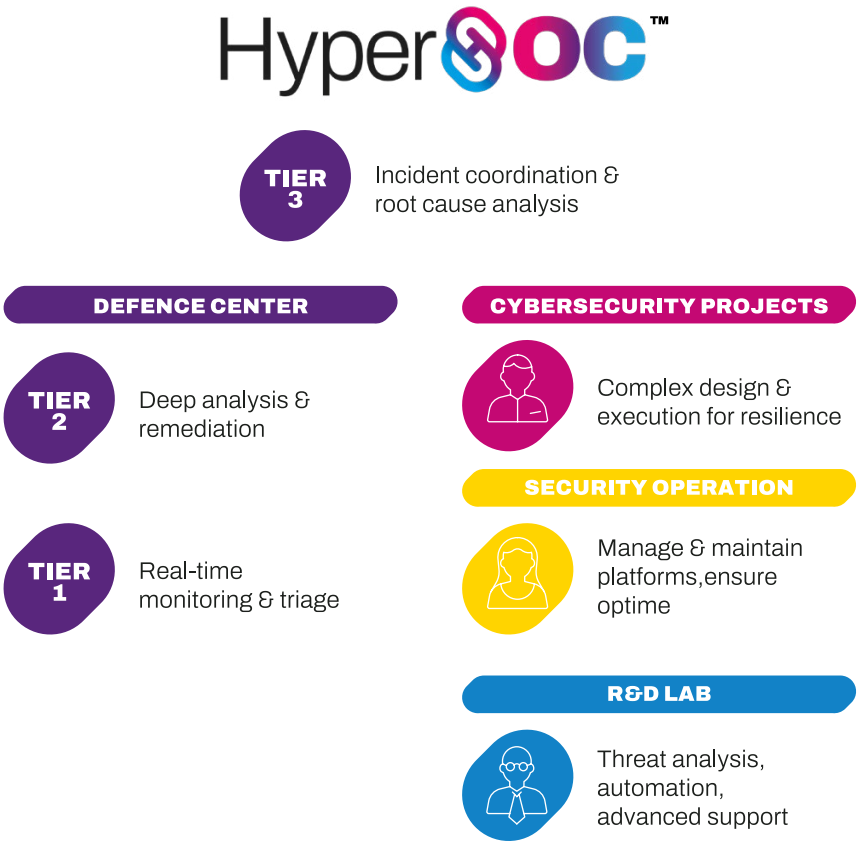


Figure 1 *- HyperSOC: levels and roles*

HWG Sababa

The Operational Engine Behind HyperSOC™

PULSE™ is HWG Sababa's proprietary platform – the backbone of HyperSOC™. Seamlessly integrated with external tools and aligned with frameworks like NIST and MITRE ATT&CK, PULSE standardizes and streamlines SOC operations. It enables:

- Real-time visibility and orchestration across environments
- Native integration with client ecosystems (no rip-and-replace)
- Automation of detection, triage, and containment workflows
- Built-in regulatory readiness and continuous improvement

PULSE transforms SOC operations into a proactive, intelligent, and scalable security engine – ready to meet today's complexity and tomorrow's demands.

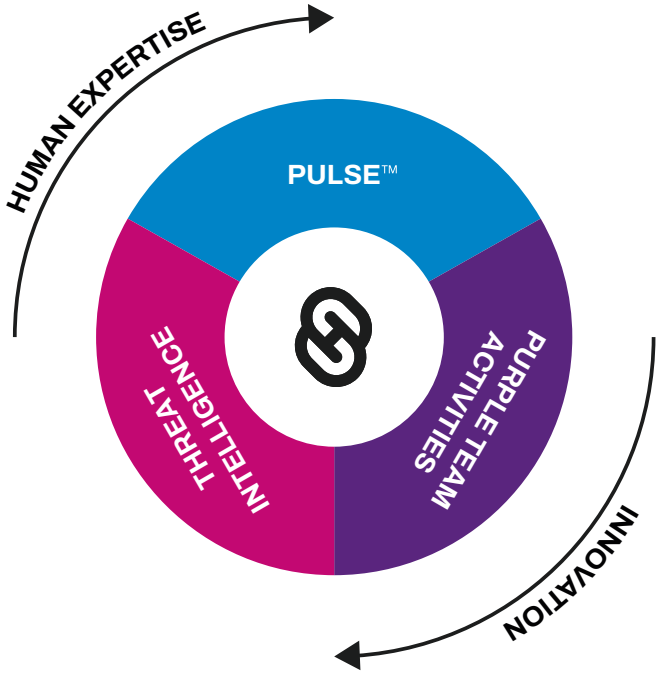


Figure 2 *- The operational engine behind HyperSOC*

Threat Intelligence, integrated into every layer of HyperSOC, transforms fragmented data into actionable insight. By combining proprietary feeds, vendor telemetry, and third-party intelligence, the SOC gains a unified, real-time view of the evolving threat landscape. This intelligence powers detection and triage with operational precision – from adversary profiling and dark web monitoring to weekly security bulletins and the annual Threat Landscape Report. The result is contextual clarity that helps prioritize risk and accelerate response.

Beyond detection, HyperSOC delivers **continuous threat validation**. Expert analysts conduct targeted threat hunting and deep investigations based on real indicators of compromise. These efforts are reinforced by integrated Purple Team simulations, which test defenses against real-world attacker tactics. Together, these practices ensure not just accurate alert handling, but measurable improvements in threat visibility, readiness, and resilience.

Core Functions: Always On

At the heart of HyperSOC lies a set of fundamental capabilities that ensure 24/7 proactive monitoring and response readiness. These are powered by robust detection logic, AI-driven operational automation, and access to the CARES customer portal for full visibility and collaboration.

Integrated use case–driven detection, platform health monitoring, and threat hardening mechanisms form the core of day-to-day protection – enabling rapid threat containment and continuous improvement.

These always-on capabilities are not optional add-ons – they're built into the very core of HyperSOC. While powerful by default, they're built to scale.

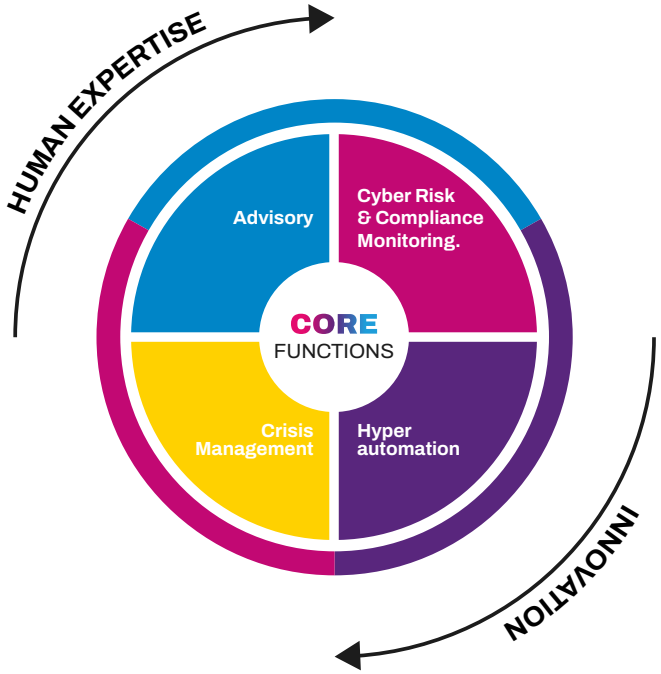


Figure 3 *- HyperSOC's core functions*

As organizations face increasingly complex risk environments, advanced service layers – such as **Hyperautomation, Advisory, Cyber Risk & Compliance Monitoring**, and **Crisis Management** – have been natively integrated at a foundational level. As HyperSOC functions scale with customer maturity, they can be progressively expanded to support specific governance, compliance, and resilience objectives.

From Core to Complete

While the core capabilities of HyperSOC establish a solid baseline, forward-leaning organizations often require deeper insight, faster response, and greater strategic alignment. That's where HyperSOC scales up – with modular, advanced functions that elevate the SOC from a reactive service center to a strategic asset embedded in business resilience. These next-level components can be activated based on organizational needs, delivering expanded intelligence, expert guidance, and dynamic response capabilities.

Hyperautomation

What truly sets HyperSOC apart is the seamless integration of advanced AI, machine learning, and orchestrated workflows to suppress noise, reduce analyst fatigue, and accelerate response from the very first signal. Through intelligent correlation, contextual enrichment, and dynamic prioritization, it measurably reduces MTTD and MTTR while freeing internal teams to focus on higher-value, strategic, risk-based initiatives. It also enhances SOC visibility across critical operational domains that have traditionally remained behind customer-only administrative boundaries. Combined with closed-loop containment under customer governance, this ensures swift, coordinated action against emerging threats without operational bottlenecks (figure 5).

55%
of SOC alerts fully automated*
– from ingestion to response, without human intervention

95%
faster detection and response for medium- and low-priority incidents, slashing time and workload

85%
reduction in response time for high-priority threats, with AI-driven triage and precision targeting

Figure 4 *- Key performance improvements enabled by hyperautomation*

**This figure refers to the internal operations of our SOC*
***The above statistics are taken from HWG Sababa Hyperautomates Their Managed SOC to Fuel Customer ROI - Torq*

Cyber Risk & Compliance Monitoring

HyperSOC delivers continuous, real-time visibility into an organization's overall risk posture - not only in terms of cyber risk exposure, but also through the lens of enterprise risk management and regulatory compliance. By aggregating telemetry from IT, OT, IoT, cloud, and third-party ecosystems, we provide actionable insights into vulnerabilities, attack paths, anomalous behaviour, and governance gaps. This function enables organizations to transition from a reactive stance to a state of continuous improvement, where cyber and compliance risks are monitored dynamically and addressed proactively before they escalate into business disruption or regulatory breaches.

Advisory

The HyperSOC advisory function provides clients with expert, ongoing guidance to align their cybersecurity strategies with evolving threats, regulatory expectations, and business goals. Our advisors operate as an extension of the client team, offering support on architecture design, compliance mapping (e.g., NIS2, DORA, CRA), threat modelling, and incident readiness. This ensures that cybersecurity is not an isolated function, but a business-aligned discipline built on risk intelligence and long-term resilience.

Crisis Management

HyperSOC is more than incident response - it prepares organizations to face crises with confidence. We help create critical procedures, provide stakeholder training, and test readiness through cyber drills and tabletop exercises. When a crisis occurs, we bring in the right mix of vertical experts and SOC analysts to contain threats, coordinate recovery, and manage communications, ensuring minimal disruption, faster recovery, and sustained trust.

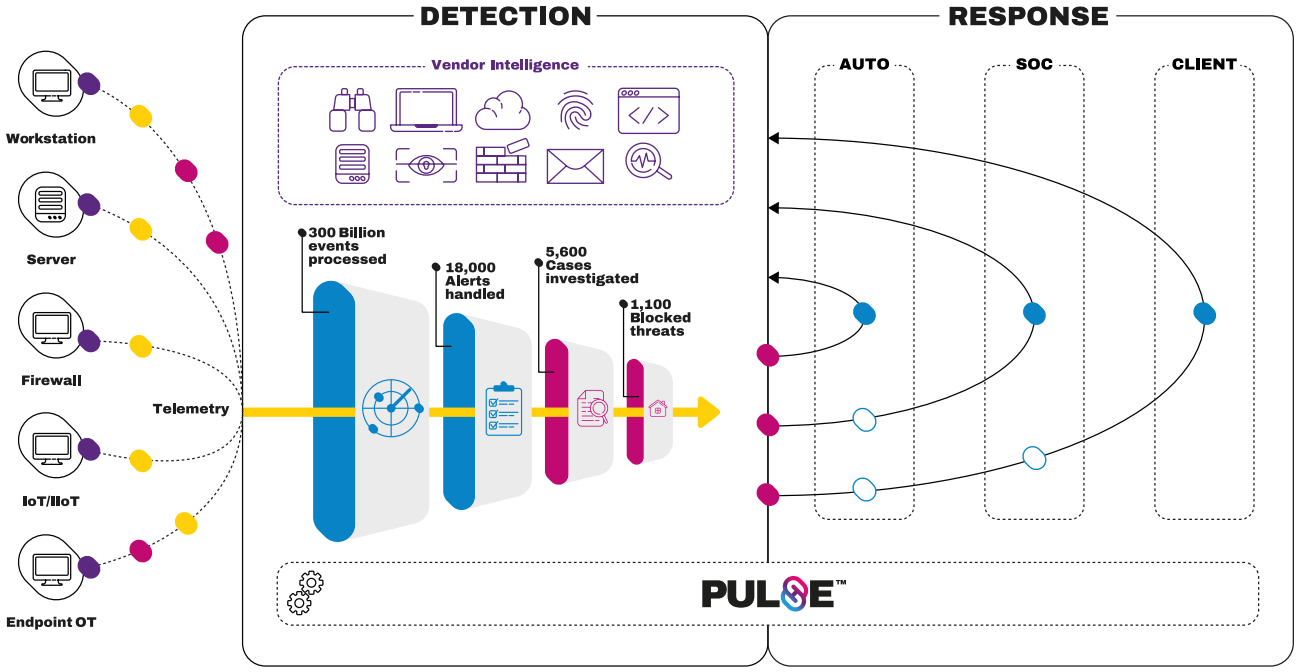


Figure 5 *- From telemetry to response - the full journey. Raw signals are collected, analyzed, and turned into action. With Hyperautomation built in, there's no need to wait for additional context or trigger manual actions.*

HyperSOC™ Business Value Across the Organization

- 24/7 visibility into the security landscape, with reduced incident response times and a unified platform aligned to industry frameworks and performance metrics.
- Seamless integration across IT, OT, and cloud environments, deployed with minimal disruption to existing systems.
- Compliance made easier with real-time dashboards, structured incident documentation, and audit-ready reporting.
- Flexible service models and vendor-neutral architecture that adapt to diverse procurement and operational needs.
- Measurable ROI through consolidated security tooling, improved risk reduction, and optimized operational costs.
- Increased organizational resilience backed by clear metrics that safeguard brand reputation, ensure service continuity, and build stakeholder trust.



To see how HyperSOC™ can align with your organization's security and business goals, download the full IDC Spotlight today.

HyperSOC™ and Pulse™ are trademarks of HWG Sababa.

HWG Sababa

Follow us on:

www.hwgsababa.com