# Security Operations in 2025

Revisiting the themes, market trends & maturity of SecOps now and looking forward

WAVESTONE

# Introduction

## Start by exploring why this report was created and **what you can expect**...

**Security Operations** is undergoing a fundamental transformation; we're seeing and helping clients reconsider traditional approaches to development and operations. **Why?** Today's security leaders are thinking bigger. In conversations with CISOs and Heads of SecOps, three phrases keep surfacing: consolidation, future proofing and resilience.

Security Operations in 2025 is about more than pure detection and response. It's about aligning with business risk, integrating IT/OT/Product telemetry into a unified monitoring framework, and enabling faster, smarter decisions throughout the detection and response workflow.

Simultaneously, the attack surface has exploded with SaaS, machine identities, and now GenAI tools. **The result?** A threat landscape that's faster, fuzzier, and far more fluid. Widespread campaigns like those perpetrated by Scattered Spider & Shiny Hunters remind us cybercriminals are all-to-ready to exploit this situation. 2025 has also seen a wave of high-impact breaches catalyzed by AI-enabled social engineering & vulnerability discovery techniques, indicating that adversaries are innovating just as fast, if not faster than 2024.

So, what's driving the creation of this year's review? It's the understanding that the capabilities, processes, and tech we relied on even last year are no longer enough.

AI is the paradigmatic example. It isn't just accelerating activities; it's necessitating a rewrite of the entire operating model.

The aim this year is, therefore, to **explore the emergent and transformatory trends impacting SecOps in 2025 through six questions we're often asked by clients.**

Where are we today, and what's blocking us?:

1. Navigating regulatory compliance, what do SecOps teams need to be aware of?
2. The SOC workforce challenge in 2025: burnout, skills gaps, and the way forward
3. Demonstrating Return on Investment, how to build a business case for SOC transformation?

What's next, and how do we get there?:

1. XDR is here, but how are we supposed to use it? Future-proofing your Detection & Response tooling
2. Agentic AI in Security Operations: are SOC analysts out of a job?
3. The changing role of Data in a modern SOC: Connecting security teams & catalyzing business value

We hope you enjoy reading these insights as much as we've enjoyed created them! Until next year ...

**James Maidment**
**Senior Consultant**
UK SecOps Team

# Contents

# 01. Where is Security Operations in 2025?

It's fair to say a lot has happened in the past year, before looking into the six challenges impacting SecOps, let's take a step back and review progress since 2024.

# How has SecOps matured since 2024?

To co-opt a famous phrase,' a week is a long time in SecOps'. Well, how about 52 weeks... This first section offers **a step back on where we stand in 2025**.

### Challenges within and without

'Tis the season for reports and alarming figures: the NCSC's Annual Review notes 204 'nationally significant' cyber events, or 17 a month. Simultaneously, the first global edition of the SOC-CCM report notes stagnant maturity growth, citing persistent retention and governance challenges. In short, internal and external challenges facing CxOs remain pervasive, elusive and evolving.

Consequently, this first section aims to provide clarity on the development of the profession since 2024, and the broader market insights we can learn from Wavestone's 2025 Cyber Benchmark.

### Wavestone's Cyber Benchmark 2025

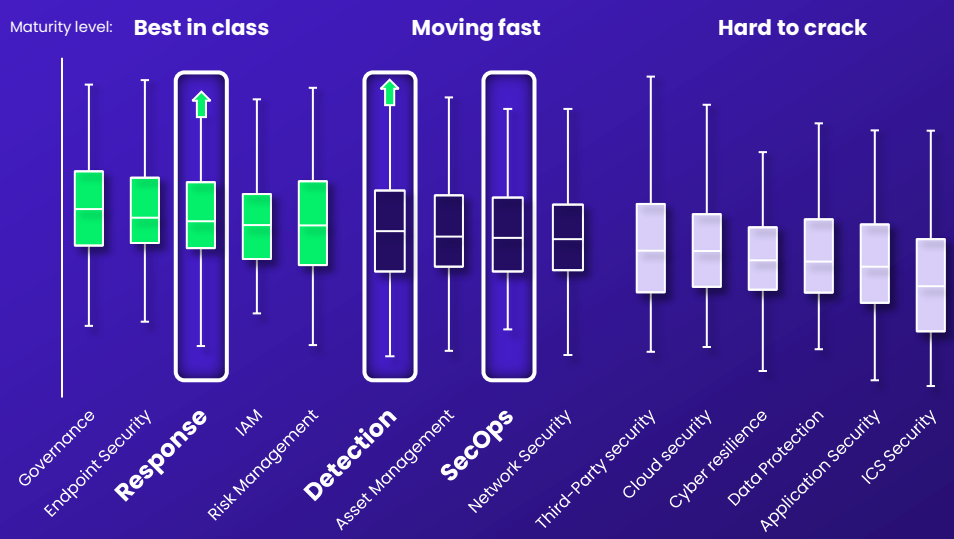
Run annually since 2019, the benchmark has surveyed 150+ Wavestone clients, representing more than 7 million employees. It is based both on the NIST CSF and ISO 27001/2. The benchmark itself consists of approximately 200 questions across 16 topics (highlighted below).

Each year, we collate the results and present high-level findings to the public. This year's headline? 'Measured progress, persistent challenges'. Overall, companies progressed by 1 percentage point, up to 54%. The chart below and the following pages highlight the key findings for SecOps specifically.

## Security Operations in context

**Box plot view** of maturity scores for every topic: Minimum / 1st quartile / Median / 3rd quartile / Maximum.

↑ *>3% YoY Increase*




**Source:** *Wavestone Cyber Benchmark 2025*

# What can the Benchmark tell us about our maturity?

### Response is becoming routine and well-practiced

**Incident response capabilities have shown clear improvement since 2024 (+3%)**, primarily driven by success in improving coordination between business units ahead of crises, and strengthening crisis management procedures.

This is a helpful by-product of recent regulatory compliance initiatives but also demonstrates increased understanding that effective incident response is a key factor in reducing the reputational and operational impact of critical incidents in particular.

### Detection is moving fast, but so are threats

**Detection capabilities also continued to improve (+4%) demonstrating increased efficiency**, particularly within large organizations with the capacity to run detection-as-code pipelines. Significant progress has also been observed in monitoring 'crown jewels', plus log coverage in cloud environments.

Having said this, with time-to-exploit down to a matter of minutes, increasingly advanced threat actors targeting private companies, and a rapidly expanding attack surface fuelled by non-human identities, these advances remain fragile.

### SecOps moves slower, reflecting broader trends

While process and technology advances since 2024 are not to be under-stated, this year's Cyber Benchmark tells us that **People advances are not to be overstated. Significant divergences between sectors remain** in the Security/Business FTE ratio, indicating that budget pressures and retention continued to be an issue this year.

Taking a step back, SecOps appears to be following the trend of consolidation. This is seen more directly when we look at sectoral trends.

## Detection: a constantly evolving challenge

Detection is a useful case to bring to life the themes highlighted in the Benchmark. Specifically, when we look to the percentage of large organizations surveyed (approx. 100 companies) that have implemented certain capabilities, we find ...

### Measured Progress & Persistent Challenges


Have **alerts** for **anomalous activity**


Regularly **monitor & analyze IDP** configuration

Strong performance in ITDR and AD / Entra ID monitoring reflect a continued focus on detecting key indicators of ransomware, to avoid the most impactful incidents for firms.

More broadly, it reflects a move beyond atomic IOCs toward behaviour-led detection.


**Collect** and **analyze business** application logs


Create **custom use cases** to identify APTs

High-profile incidents (e.g. those affecting Salesforce, SAP, Sharepoint on-prem. customers) highlight the need to improve monitoring coverage for business applications. Similarly, campaigns (e.g. conducted by Volt, Salt, Flax Typhoon this year) are a warning of the coming need to implement custom detections for APTs.

***Source:*** *Wavestone Cyber Benchmark 2025*

# What does the Benchmark tell us about key sectors?

## Manufacturing firms

Integrating OT into a unified SOC Framework continues to be the key trend. While clients are feeling the benefits of a decentralised model (reduced latency and increased context), they are finding it challenging in a currently volatile market to maintain the same baseline of controls across geographies.

Therefore, clients are implementing scalable governance and robust metrics (e.g. continuous exposure scoring of OT zones) to support a consolidation of capabilities and performance.

## Financial Services

Following a cycle of transformation initiatives, primarily focused on compliance and implementing Intelligence-driven defence, FS firms are now focusing on how to optimise performance and enhance their detection & response workflows using the newly AI tools available.

This is partially a natural reaction to programmes ending, and budgetary pressures, but also reflects the need to solidify foundations and develop their technology stack, in response to the ever-accelerating threat landscape.

## Automotive OEMs

Automotive OEMs are facing the challenge of convergence head on, working to embed big data analytics that can handle product telemetry, correlate with traditional IT and OT log sources, and meet stringent compliance requirements (e.g. UNECE WP.29).

To do so, they are implementing novel solutions, such as custom visualisations of OTA Update lifecycles to identify suspicious activity, and correlation rules with CAN bus telemetry to detect impacts on vehicle performance earlier.

## Across sectors, the watchwords for 2025 are convergence and consolidation

Ultimately, we are touching on the two core trends we have observed in 2025: IT / OT / Product convergence & consolidation in Security Operations, but what about their consequences? Below we lay out four which have been of particular interest to our clients:

| | |
|---|---|
| **Developing Extended Fusion Centres** | Fusion centres are final bastions of consolidation & convergence – clients who have implemented this model are looking to incorporate third parties to improve visibility into this key perimeter, as a response to increasing regulatory pressure. |
| **Automating Detection Validation** | SOC teams are increasingly turning to automated validation frameworks to continuously test detection logic against observed TTPs, with the aim of improving their efficacy and the team's own efficiency, helping to match the pace of attackers. |
| **Co-Teaming for L1 Activities** | Agentic AI provides the technological capacity to overcome the surfeit of alerts SOC teams are facing, so it's not surprise that they are being deploying for alert enrichment, suppression and triage at L1. |
| **Organisational Transformation** | The most mature firms are now already looking ahead to the next transformation cycle, specifically, a more adaptive detection & response capability. The approaches taken vary but focus on a high level of automation to redirect analyst effort. |

**How to continue maturing a converge function is this year's central theme**, v section beginning with a discussion on evolving regulatory landscape...

# 02. What are the common challenges in 2025?

Turning from the strategic to the practical, this section focuses on three key challenges clients face in 2025, and how they are seeking to overcome them.

# Complying with pertinent regulations in 2025

Historically, SecOps has operated as a technical function focused on monitoring, detection, and response. Today, regulators expect these teams to be integrated with the whole of the business and contribute directly to a holistic security mindset. Consequently, the burden to demonstrate compliance by maintaining traceability, ensuring timely reporting, and supporting resilience has increased. Similarly, the scope of regulatory scrutiny has broadened to how incidents are classified, how quickly they are escalated, and whether appropriate logs and evidence are maintained. Security Operations teams must therefore be prepared to demonstrate that their processes are not only effective, but also aligned with legal and regulatory obligations.

## Firstly, what are the key requirements teams need to be aware of?

Across jurisdictions, regulators have prioritized specific requirements, pulling SecOps teams in different directions...

**Prioritizing a minimum baseline of Operational Resilience**

**EU**

**NIS2** (*Critical Sectors*)
Mandates 24/7 detection, rapid incident reporting (within 24 hours), and **supply chain risk monitoring**

**DORA** (*Financial Services*)
Demands proof of operational resilience, including incident classification, **recovery testing**, and unified reporting

**Ensuring client and customer data is adequately protected**

**UK**

**UK NIS Regulations** (*Critical Sectors*)
Aligns closely with NIS2: mandates detection capabilities, incident response, and **threat intelligence sharing**

**UK GDPR / ICO Guidance** (*All organizations processing PII*)
Requires **data breach identification and reporting** within 72 hours, backed by logs and evidence

**Minimizing the financial/non-financial impacts of cyber incidents**

**US**

**SEC Cyber Rules** (*Publicly-listed Companies*)
Requires **disclosure of material cyber incidents** within 4 days - pushing for fast detection and escalation.

**GLBA / FFIEC** (*Financial Services*)
Enforces requirements for threat detection, **response procedures**, and control effectiveness.

**and pushing towards data sovereignty**

**China**

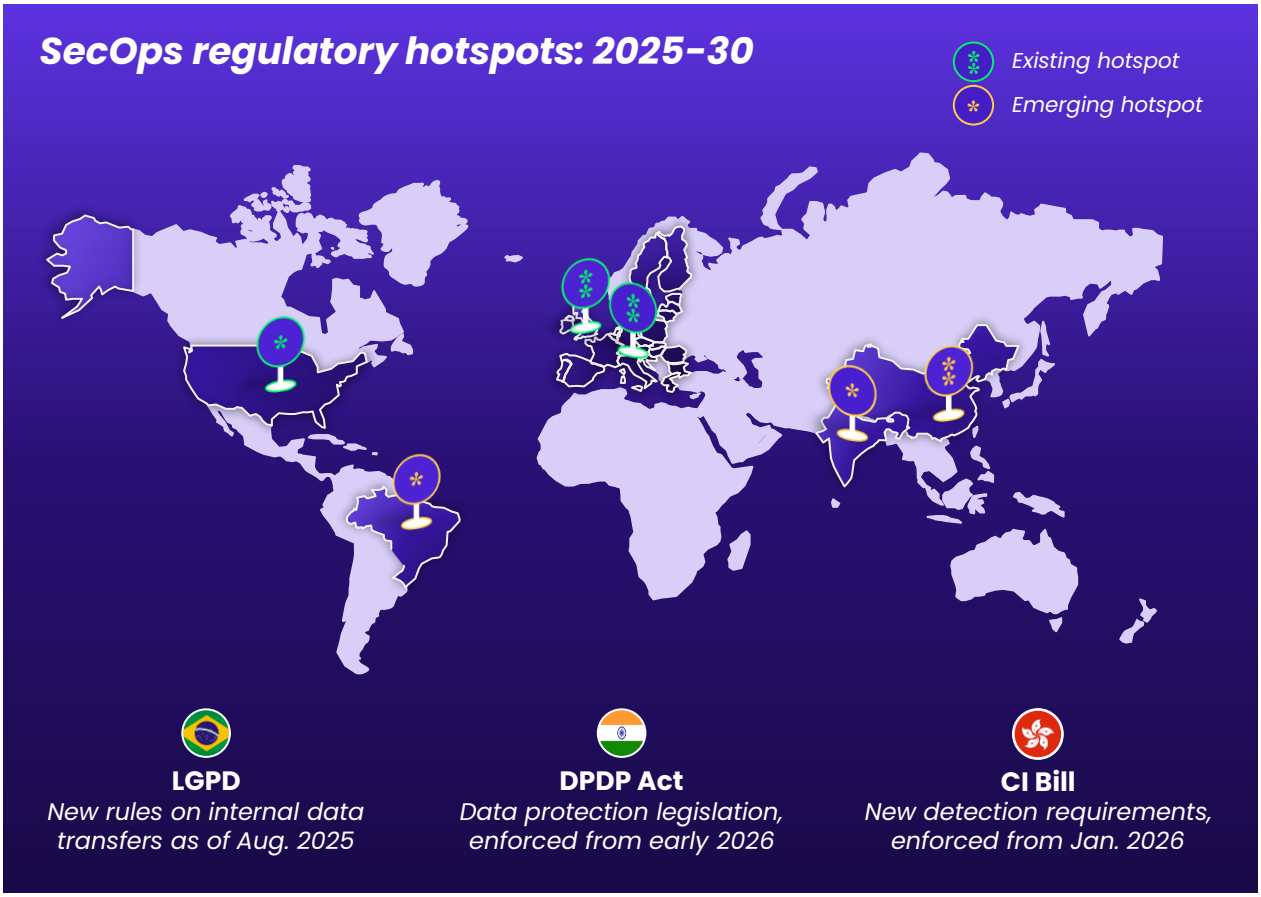
**Cybersecurity, Data Security, Personal Information Protection Laws** (*All network operators, CIIOs, entities processing PII*)
**Data localization**, real-time monitoring, incident reporting within 1–4 hours, **cross-border transfer security assessments**.

# Navigating regulatory compliance beyond 2025

## What are the emerging requirements to watch out for?

Despite regional differences, several consistent expectations are emerging. Regulators increasingly require documented incident response procedures, evidence of backup and retore capabilities, comprehensive logging, and visibility of 3rd party risks.

**Real-time reporting to internal and external stakeholders** is becoming a standard requirement across jurisdictions.




## Preparing for regulatory scrutiny

SecOps teams should assess their readiness against the operational requirements embedded in these regulations. This includes reviewing incident response workflows, ensuring logging infrastructure supports traceability, and validating that escalation procedures meet regulatory timelines.

**Integration with governance, risk, and compliance (GRC) functions is essential** to ensure alignment between technical operations and legal obligations.

Organisations should also evaluate their resilience posture, including the ability to recover from disruptions and maintain continuity. Third-party risk management must be embedded into security operations, with visibility into vendor controls and contractual obligations.

# Overcoming the SOC workforce challenge

## What's the problem?

Amidst an increasingly complex threat landscape, SOCs are under mounting pressure to stay one (*or even multiple*) steps ahead. This combined with various internal pressures SOCs to maintain proactiveness and efficiency.

Despite an increase of UK cybersecurity graduates, businesses lack advanced technical skills like penetration testing. This shortage limits SOCs' ability to work proactively and, meet performance targets. Crucially, heavy workloads drive analyst stress and turnover, threatening SOC effectiveness.

**30%**

of business report gaps in advanced technical skills *(UK Government, 2025)*

**4.8 M**

unfilled roles globally *(ICS2, 2024)*

**70%**

SOC analysts experiencing severe stress *(Cassetto, 2025)*

## What's the solution?

**1. Leveraging the technological opportunity**
Recent advances in automation and AI-enabled tooling are transforming the landscape of security operations, offering a powerful path forward for modern SOCs. By filtering noise, reducing false positives, and streamlining triage, these technologies encourage analysts to focus their attention on critical threats rather than getting buried in routine alerts. Automation not only accelerates response times but also creates opportunities for analysts to develop advanced skills such as threat hunting, incident investigation, and proactive defence strategy.

**2. Intensifying additional training & support**
While supportive of a proactive SOC, clear training pathways and career progression plans are essential for building a resilient SOC, faced with an increasingly complex threat landscape.

**3. Maximising Co-Teaming Benefits**
Analysts must be confident in interpreting AI-generated insights, identifying activities requiring their intervention. To do so, they must be supported through in-depth training and mentorship from senior leaders / CoEs. Creating a collaborative environment is also essential to encourage knowledge sharing during this intense period of up-skilling. Most importantly, fostering a supportive work environment, with mental health resources and flexible working, is vital to build resilient, motivated teams.

## What's the result?

A more efficient, resilient SOC where workloads are balanced, backlogs are minimised, and burnout risks are significantly reduced. However, SOC's must ensure these tools are configured correctly and ensure analysts are trained to use them effectively.

# Building a business case for SOC transformation

As regulatory expectations become more defined, organizations must justify SOC investments in terms that align with executive priorities.

## Estimating cost vs value: the incident avoidance lens

SOC investment involves both upfront and ongoing costs, including technology, personnel, and process development. However, the value of a SOC is best measured by its ability to reduce the financial impact of cyber incidents. Early detection and rapid response can prevent significant losses from data breaches, ransomware, and system outages. Estimating avoided incident costs provides a tangible metric for return on investment. Operational efficiency is another key benefit. SOCs improve resource utilisation by automating alert triage, prioritising threats, and centralising visibility. These capabilities allow teams to manage more risk with fewer resources.

## Aligning SOC with board level concerns

To gain board-level support, SOC benefits must be framed in terms of resilience, compliance, and reputation. Faster threat detection supports business continuity. Centralised monitoring simplifies audit preparation and regulatory reporting. Proactive defence reduces the likelihood of reputational damage from public incidents.

Metrics such as mean time to detect and respond, downtime reduction, and regulatory fines avoided help translate technical performance into business value.

## Deriving business value from the SOC's data

Modern SOCs generate data that can support broader risk management. Fusion Centres, or Joint SOC, which integrate IT security with fraud, insider threat, and physical security, offer richer context and faster response. SOC data can also reveal operational trends and performance insights that inform strategic decisions.

A strong business case for SOC transformation reflects the organisation's risk profile, regulatory obligations, and strategic goals. It should demonstrate how the SOC mitigates risk, supports compliance, and delivers measurable value. The cost of investment must be weighed against the cost of inaction, which can be far greater in today's threat landscape.

> **"To gain board-level support, SOC benefits must be framed in terms of resilience, compliance, & reputation."**
>
> **Saaid Mohamoud**
> Senior Consultant

# 03. What's next for SecOps?

Looking towards the horizon, this last section discusses several emerging trends that indicate how Security Operations' role will continue to evolve into the future.

# XDR: considerations for sustainable implementation

Since 2018, Extended Detection and Response (XDR) has gained traction in the security operations landscape, backed by compelling promises: proactive detection and unified security capabilities (two key challenges highlighted in our 2024 Whitepaper).

However, perceptions of what XDR vary. Several definitions are used colloquially, with no shortage of marketing jargon.

At its core, **XDR is an architectural model designed to break down silos** and link previously isolated security tools.

In practice, this approach consolidates security operations capabilities, with XDR acting as a central platform that ingests and correlates data from multiple sources, enriches it, identifies threats, and automates responses, reducing the number of portals, platforms and licenses to manage.

Gartner defines two types ...

**Open XDR** offers connectors to multiple vendor solutions, fully embracing the XDR philosophy by breaking down silos.

**Closed XDR** provides a single platform with all security tools, enabling seamless integration between solutions and simplifying commercial processes, however, this risks vendor lock-in.

XDR platforms can be invaluable to achieve high levels of maturity and significantly reduce detection and response times in an ever-evolving landscape.

However, Identifying whether an XDR is needed in your organisational context and if so, which type is appropriate is fraught with challenges. Here we summarise some of those challenges.

## Key questions to consider when deciding on methods for implementing XDR

| Do you have the right foundation? | What should your strategy for change be? | Is this magnitude of change necessary? |
|---|---|---|
| Whilst XDR platforms represent a significant opportunity to simplify and increase operational efficiency, it requires several underlying capabilities to already be mature to be effective. The maturity of Data management, Threat Intelligence and Organizational integration have a significant impact on the operational effectiveness of an XDR platform. | In the long-term, open XDR platforms offer many of the intended XDR benefits without the need for a complete overhaul and transition of your technology stack, but a 'Spanners' approach more complex operational management requirements. Conversely, Closed XDR platforms have a complex and significant initial change period, with multiple tool transitions required in parallel, but operational simplification and value are realised faster. | Regardless of which type is selected, careful analysis, planning and then lengthy technical and operational change are unavoidable. When considering tool selection, the business and financial elements must be weighed against the Security Operations goals, and framed by clear definitions of Key performance/Risks/ Compliance Indicators with associated targets. |

# Agentic AI in SecOps: setting out the problem(s)

With Google's 'Big Sleep' AI now autonomously patching vulnerabilities before humans even wake up, **the urgency to balance machine precision with human oversight in security operations has reached a critical inflection point**.

In what follows, we seek to prove that while intelligent automation is advancing rapidly in security operations, human oversight remains vital.

Analysts provide contextual judgment that AI lacks but may yet still support. As a result, current hypotheses across academia and security practitioners support a 'calibrated autonomy' approach, which scales machine control against trust and task sensitivity.

## AI will not replace, but support through co-teaming

AI may be a necessary means for alleviating SOC Analyst burnout, but it need not be so deterministic, rather a 'learning partner' with which SOCs can open new pathways toward adaptive, context aware functions. Namely, academics refer to a 'co-teaming' paradigm aimed at narrowing the vectors of analyst decision making, as opposed to debasing them entirely.

In this, AI agents augment SOC workflows by internalising and transmitting tacit knowledge which in turn supports dynamic and, crucially, proactive decision making by their human counterparts. For example, the Sony attack attributed to North Korea in retaliation to the movie, The Interview, began with a phishing campaign that compromised Sony's network. Albanese et al. (P. 16, 2025) argue that the co-teaming method would have been effective in "incorporating geopolitical threat signals into SOC workflows, harmonising disparate data sources, and leveraging LLM-based AI for real-time contextual analysis… provide[ing] analysts with actionable intelligence" well before the attacks would have escalated to the late stage, static, detection typically attributed to an automated SOC deployment. Wavestone has witnessed first-hand how LLMs are being leveraged to append, as opposed to replace, holistic security operations. Explicitly, the deployment of Copilot Agents to mobilise internal security guidelines and lessons learned, thereby refining a dynamic defence posture.

As such, co-teaming models offer a pragmatic avenue for organizations seeking to integrate AI without resorting to an all-or-nothing approach. They may benefit from piloting these models iteratively using internal threat intelligence and historical incident data to train AI agents in context-specific decision support, ensuring operational relevance while accelerating trust-building through demonstrable value.

The fact is that **human analysts remain crucial for enacting a 'proactive' defence strategy**, namely making the larger, evidence-based, and crucially nuanced decisions. Through this lens, AI co-teaming represents a strategic enabler for proactive defence, not just reactive triage, which can help organizations align AI initiatives with board-level resilience and risk appetite.

The question remains, though, how do we achieve a 'calibrated autonomy' approach that can effectively scale machine control against trust and sensitivity…

# Agentic AI in SecOps: driving towards a solution

## How are firms charting a course for the use of Agentic AI in their SOCs?

### Nothing is set in stone; AI involvement depends on trust and use case

Further perspectives have framed the adoption of AI into a 'tiered autonomy framework' (Mohsin et al., 2025) which redirects the debate away from bipolar adoption to a modal variant. Specifically, one that accounts for human-in-the-loop roles, trust levels, and a variety of use cases, ranging from 'manual' to 'fully autonomous'.

To illustrate this, a SOC simulation under the Augmenting Cyber Defence Capability (ACDC) project recently demonstrated the integration of **CyberAlly** (an AI augmented virtual analyst built on GPT models and enhanced with Retrieval-Augmented Generation) which was embedded in Blue Team operations during simulated wargames. The agent **performed triage, contextual enrichment, ticket creation, and supported analysts via Slack**, which had a significant reduction impact on alert fatigue. With this, CyberAlly was gradually elevated from full human-in-the-loop (HITL) validation to conditional autonomy for routine tasks, **demonstrating up to 67% faster investigations and over 60% reduction in response times.**

The study shows that trust in AI deployments is contextually tied to merit and autonomy, scaled proportionally. Organisations may support a targeted AI deployment by mapping SOC tasks along dimensions of complexity and trust to better understand where conditional autonomy can be introduced with confidence. To support this, developing internal trust metrics for AI agents (e.g. on accuracy, explainability and transparency) is key.

Nonetheless, Agentic AI is going mainstream with leading vendors embedding autonomous agents that reason, write rules, parse data, and take actions with pilots already underway. Recently, Google Cloud announced SecOps Labs pilots for AI agents that auto-generate detection rules, playbooks, and data parsers.

**Evidence from live SOC operations using Gen AI correlated with a ~30% reduction in mean-time-to-resolution of security incidents**. (Bono et al., 2024)

Invariably, Agentic AI is quickly becoming a staple of Security Operations, despite continued apprehension regarding the absence of human oversight.

To conclude, despite the push to embed intelligent automation as the next logical step in security operations, existing trends suggest that human oversight and decision-making will remain a staple of SOC deployments. Further, increasingly recognised perspectives frame the deployment of AI in ways that emphasise context-sensitive levels of autonomy based on trust. As organizations continue to explore intelligent automation within their SOC environments, it may be prudent to approach AI integration not as a binary shift, but as a calibrated evolution. By aligning autonomy with task sensitivity and trust maturity, clients can preserve the strategic value of human oversight while unlocking operational efficiencies.

**Ultimately, the issue is not whether AI can replace human judgment, but how it can responsibly extend it.**

# Harnessing security data for strategic advantage

As Data continues to be the most valuable commodity in business, SecOps teams are mining their natural resources for insight and value.

The use of large data models, as well as increasingly complex data collection and management architectures continues to be a trend across our clients. Whilst we often focus on the challenges this presents to security teams: principally, grappling with the logistics of hosting and processing such large volumes of data to monitor new business workloads like GenAI Tooling, Industrial Robotics, and of course Connected Products, we miss a truism:

**The SOC is the largest data repository in almost scenarios.**

## But, what are SecOps teams doing with all this data?

**1. Seizing the opportunity to consolidate disparate monitoring services into a Global Joint SOC (JSOC):** Many organizations are choosing to consolidate monitoring services such as; Physical Security, Fraud and Operational Technology under one roof. This allows them to mutualise the underlying data infrastructure, leading to new opportunities to derive insights that will boost efficiency and reduce cost. It also promotes closer working between teams, opening exciting opportunities for correlation and enrichment, as well as drawing on a wider breadth of skillsets in investigations. Convergence can progress from a mere organisational efficiency to a distinct security advantage.

**2. Leveraging this unique data asset to provide business value, not just security value:** With such a wealth of data from both technology and business systems, the application of proper data science techniques and skills can lead to new business insights and a range of benefits including identifying:

- Commercial trends to help develop products or customer behaviour trends to help improve customer facing services
- Efficiency gains in business and operational processes
- Provide greater levels of automated assurance for security controls and business performance

**Benefits don't arrive overnight, but issues can.**

## So, what do we need to ensure?

- **Consistent data quality across all sources** the outputs of any process are only as good as the inputs they receive
- **Strong collaboration between teams** Context is crucial, and this can only come from proper integration of the SOC and business teams working on their data daily
- **Skills-Matching** Ensuring your teams are well-placed to support such complex processes is essential

The future belongs to organizations that see security data not as a vault, but as a lens, revealing patterns, predicting risks, and unlocking new opportunities.

**Henry James**
SecOps Consultant

# Concluding thoughts

In closing, we return to the vexing question of how the market will evolve in the longer term, and what might we need to consider that's currently over the visible horizon...

# The future of SecOps, in 2026 and beyond

We highlight three emerging trends and what the most mature firms are currently focused on implementing.

## 1. Dynamic Risk Management

### A move towards agentic detection & response capabilities

In 2024, we said that firms would begin to feel the benefits of detection-as-code; since then, it has matured into a well integrated engineering discipline.

What's new is the rise of agentic detection engineering: GenAI is now capable of proposing detection logic based on analysis of natural and programmatic language threat intelligence, while AI Agents can integrate with BAS tooling to test them, and ultimately deploy rules autonomously.

When paired with a GRC Engineering approach, clients can go further. Risk scores can be dynamically adapted based on live telemetry, and alerts raised or action taken to tune preventive or mitigating controls.

## 2. Preparing for Q-Day

### Developing a quantum-ready SOC

With quantum computing moving closer to reality, mature clients are assessing their exposure to quantum threats.

Security Operations will have a key role in this transition, not only by monitoring for data exfiltration activity which is indicative of a "harvest now, decrypt later" strategy, but also by future-proofing the SOC's own architecture and data pipeline against security threats.

The most prepared clients are already exploring the requirements for PQC readiness as they deploy ZTNA, and conducting threat modelling to identify scenarios they may encounter in future.

## 3. Security Operations or cyber resilience?

### CISOs considering converging SecOps, OpRes & GRC

With the lines between these teams beginning to dissolve, mature organizations are starting to consider how they might want to consolidate and / or converge these functions into unified cyber resilience teams in future.

As a first step, clients are embedding GRC engineers into their SecOps teams.

The most advanced organizations establishing shared capability hubs, supported by unified platforms, shared data models, and common incident taxonomies, enabling faster decision-making and more consistent execution across the security lifecycle.

# Conclusion

## So, where *is* the market heading?

It's clear that detection & response will continue to be key topics as we look towards 2030. As we've alluded to throughout this paper, we believe that we are currently in a Sattelzeit (saddle period), managing the transition from one transformation cycle to the next.

This is reflected in the first of our key themes: consolidation. It can be seen not only internally within SecOps teams, but also in broader M&A dynamics (see LevelBlue's acquisitions of Trustwave, and latterly Stroz Friedberg). This phase is certainly not yet over and will continue to shape trends for the foreseeable (assuming continued business, trade and policy volatility).

This change in market behaviour is indicative of a broader change in attitude amongst corporations of all sizes. With many now proactively considering the implications of new technology offerings and growing investment in Agentic and Generative AI especially, to review their operating models and technology stacks, to keep pace with the growing sophistication of Cyber attacks and not be the next big headline.

Looking beyond this, the natural question is: ***what will this next transformation look like?***

The mantra of the next five years is speed. Everything is getting faster: business interactions, technological development, and threat actors…

Building on their strong foundations and success, Security Operations teams will need to match this pace and dynamism. Consequently, we firmly believe there will be a need to transform towards a more resilient approach.

Strategic objectives to simplify, evolve and demonstrate return on investment provide the impetus; the business imperative to become more customer-centric will provide the energy to break down siloes further and force the SOC to look beyond the triage board to become more than just a cost centre.

**We believe now is the time to push for truly dynamic SecOps capabilities; the questions is, how will you approach it?**

**Francesca Kempster**
**Manager**
UK SecOps Lead

**We are entering an exciting time of opportunity for Security Operations, now more than ever we have the tools and motivation to make fundamental changes. Let's seize this moment to push for bold transformation!**

**Benoît Marion**
**Senior Manager**
Global SecOps SME

# Editors

**Francesca Kempster**

**Manager**

**James Maidment**

**Senior Consultant**

# Acknowledgments

Each of the topics covered here originally appeared as individual LinkedIn posts which were researched and drafted by the SecOps team in the UK.

Particular thanks goes to the individual writers listed below, whose invaluable input has shaped the insights throughout this paper.

**Fatima Azim**

**Consultant**

**Henry James**

**Consultant**

**Matthew Hood**

**Consultant**

**Euan Fairweather**

**Consultant**

**Saaid Mohamoud**

**Senior Consultant**

**Martin Gregoire**

**Analyst**


## *About Wavestone*

Wavestone is a consulting powerhouse, dedicated to supporting strategic transformations of businesses and organizations in a world that is undergoing unprecedented change, with the ambition to create positive and long-lasting impacts for all its stakeholders.

Drawing on more than 5,500 employees in 17 countries across Europe, North America and Asia, the firm offers a 360° portfolio of high-value consulting services, combining seamlessly first-class sector expertise with a wide range of cross-industry capabilities.

Wavestone is listed on Euronext Paris and recognized as a Great Place to Work®.

**www.wavestone.com**