ONTIC

Security Industry Trends, Insights, and Forecasts for 2026

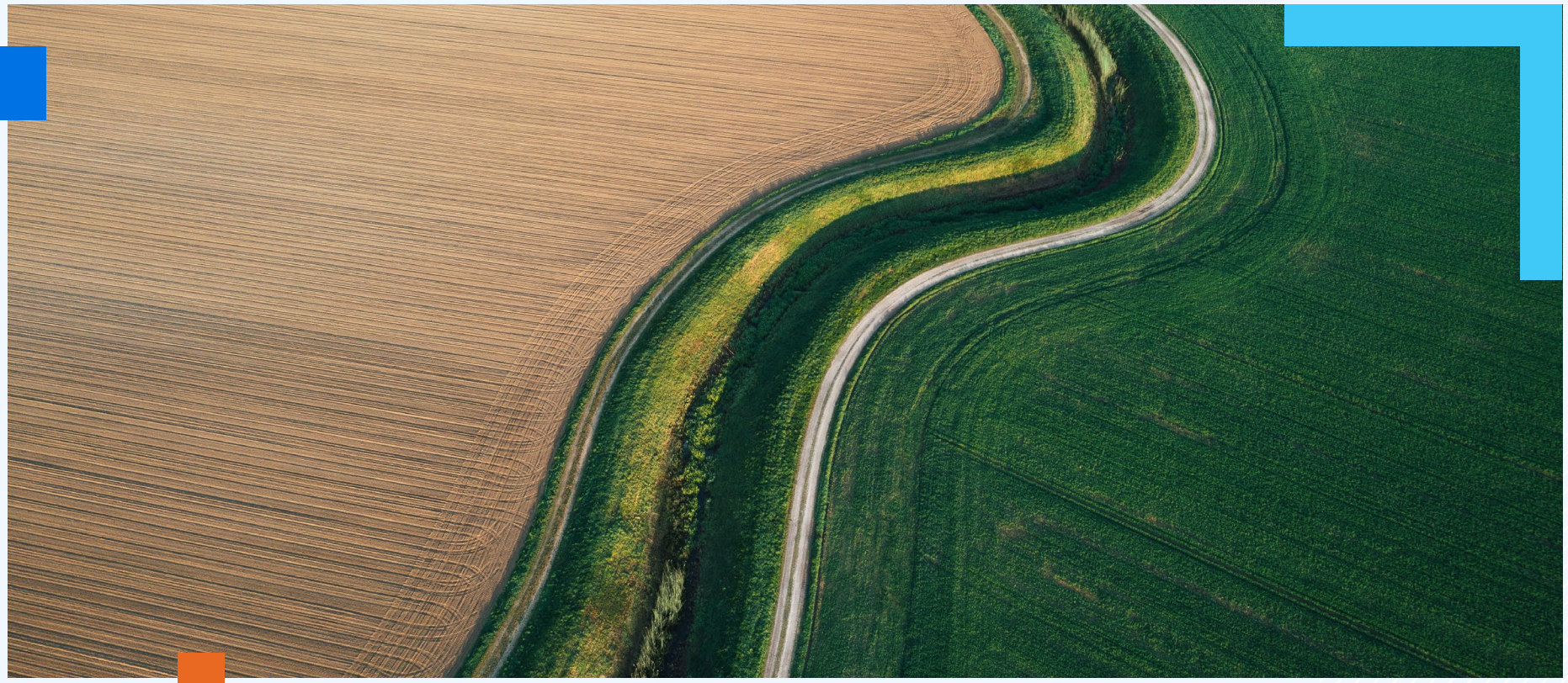

Table of Contents

Foreword from Ontic's Chief Innovation Officer

The pace of transformation within corporate security has accelerated over the past year. What began as cautious experimentation with AI and data integration in 2025 has become a reshaping of how organizations detect, interpret, and respond to risk. Security functions are now smarter, more connected, and strategically aligned with enterprise priorities.

This year's insights reflect that evolution. Experts across intelligence, investigations, and executive protection share a conviction: the future of security depends on integrating people, processes, and technology—guided by accountability and human judgment.

From AI integration to human oversight

AI is indispensable for data processing, threat detection, and predictive modeling. Yet machines alone can't make sense of complexity. In 2026, success will hinge on trustable AI guided by human oversight. The most resilient organizations will utilize AI to amplify expertise, enabling faster, more contextual, and reliable decisions when it matters most.

A Connected Intelligence ecosystem

The convergence of corporate functions — from physical security and cybersecurity to HR and legal — is redefining how enterprises anticipate and mitigate risk. Siloed information has become an operational weakness. The leaders shaping the future are building shared frameworks where intelligence flows freely and insights drive coordinated action.

Evolving threats, expanding accountability

Security faces new volatility driven by AI deception, insider risk, normalized violence, and activism-fueled disruption. As threats grow more complex, so do expectations of leadership. Protecting people and assets is no longer enough. Teams must show strategic value through transparency, defensibility, and measurable ROI.

Professionalization and preparedness

Corporate security is transforming. GSOCs are evolving into fusion centers, executive protection is a leadership priority, and risk management is embedded in daily operations. The focus is shifting from protection to performance — building proactive, data-informed programs that strengthen resilience and position security as a driver of growth.

As we enter 2026, the rise of AI, the convergence of functions, and the demand for security-driven value are redefining how organizations view protection and performance. Aligning people, technology, and process under a unified vision can turn risk into strategic advantage.

We invite you to explore this year's forecast, reflect on these insights, and consider how they may guide your organization's next chapter.

Thank you,

Manish Mehta

Manish Mehta
Chief Innovation Officer
Ontic

Chapter 1: Threat Intelligence

Harmony among data, AI, and human insight

As we look ahead to 2026, threat intelligence programs are evolving from reactive information gathering into unified ecosystems that integrate data, technology, and human expertise. The maturation of AI and machine learning is accelerating analysis and pattern recognition, yet the value of skilled analysts capable of interpreting, contextualizing, and prioritizing intelligence has never been greater. The future of intelligence will hinge on balancing speed with precision, leveraging threat intelligence platforms to break down silos, enable true cross-functional collaboration, and empower analysts to focus where human judgment matters most.

Harmony among data, AI, and human insight

"Intelligence's greatest strength is in reducing uncertainty and enabling sound decision-making. As the geopolitical volatility of 2025 extends into 2026, corporate intelligence teams will be more critical than ever. Security crises are liable to catch unprepared or reactive teams off guard, serving as a reminder of the importance of intelligence when it's too late. By contrast, effective security intelligence teams will engage in strategic scenario analysis, work closely with executive stakeholders to align with business priorities, and proactively identify and mitigate risks to the business."

Maria Robson-Morrow, Ph.D.
Chief Operating Officer
Belfer Center for Science and International Affairs, Harvard Kennedy School

"In 2026, Connected Intelligence will become even more important with a growth in social activism driven by geopolitical events. Security teams will not only have to keep travelers aware of protests and acts of violence resulting from social activism, they will also have to be aware of potential insiders, staff members with access to facilities, and systems that are driven to act against their employer. This "employee activism" will cross the lines of executive protection, insider threat, workplace violence, travel security, physical security, and cyber. The Ontic Platform can position security teams to work together to mitigate these evolving threats."

Tim Kirkham
Vice President, Investigations Practice
Ontic

Harmony among data, AI, and human insight

"In 2026, the weaponization of AI against executives will accelerate, and it won't remain confined to cyberspace. Deepfakes, synthetic voice calls, and generative misinformation campaigns will not only impersonate leaders but also trigger second and third-order effects. Security and intelligence practitioners must recognize this as an operational threat, not a technical one. AI-enabled targeting will fuse digital deception with physical consequences, altering travel plans, triggering crises, and shaping public narratives in real time. The organizations best prepared will treat this as a convergence issue, integrating cyber, intelligence, communications, and executive protection disciplines to detect, verify, and counter these operations before they spill into the real world. Protecting executives now means defending both their digital identities and their physical safety from AI-driven manipulation."

Ryan Long
Founder + CEO, Protective Intelligence
INTELAB Ventures

"After a period of increased executive attention to geopolitical and security risks, the intelligence space seems to be entering a maturation phase. The last couple of years have seen a lot of new entrants – of varying quality – into the intelligence market offering geopolitical and security insights, and a lot of confusion among executives about who to turn to for support. This now seems to be winding down, and executives are beginning to have a clearer view of where to find relevant expertise and guidance within their companies. This is not universal, however, and security teams must actively help this maturation through laser-focused mission delivery and messaging on the risks they are responsible for."

Lewis Sage-Passant, PhD
Global Head of Intelligence
Novo Nordisk

Harmony among data, AI, and human insight

"As the use of AI and AI agents within corporate security organizations becomes more prevalent, one of the areas that CSOs will explore with interest is the use of AI to reduce (or ultimately replace) the number of 'human' intelligence analysts within their team. While replacing all human analysts is unlikely in the near term, CSOs will thoughtfully explore a new threat intelligence model that focuses on AI mining the threat data, creating the intelligence and threat reports, and then using a much smaller group of experienced intelligence analysts to provide oversight and information rationalization."

Dave Komendat
Chief Security Officer
Corporate Security Partners | Ontic Advisor

"Threat intelligence is at a turning point in 2026. Organizations are moving beyond cataloging past threats and shifting toward anticipating what's next. This evolution demands the integration of tactical, operational, and strategic insights across cyber, physical, and geopolitical domains to create a unified view of threats and risks. Predictive analytics and AI-driven automation are becoming embedded in decision-making systems, enabling faster and more resilient responses. Yet judgment cannot be automated — human tradecraft remains essential for nuance, context, and ethical oversight. The next era of threat intelligence will be defined by augmented foresight: the seamless fusion of machine speed and human judgment that allows organizations to anticipate and act decisively before threats materialize."

Nicolas Reys
Partner
Control Risks

Harmony among data, AI, and human insight

"Silos of information will persist, and the perfect information sharing process will remain the unicorn everyone is seeking. There will be some functions within organizations that remain reluctant to consider any AI-driven information sharing due to privacy concerns. Intelligence platforms with strong governance abilities to define roles and access will prove their value."

Cynthia Marble
Senior Director of Executive Protection Practice
Ontic

"While I am sure others are going to focus on the impact of AI on threat intelligence, I believe 2026 will again illustrate the importance of competent analysts. AI tools are helpful, but they are just that, tools—and tools can only be as effective as the person that uses them. Today's threat environment is more diverse and complex than ever. Threat actors have a wide range of grievance narratives to choose from, and a rising number of them are motivated by more than one grievance narrative. "Extremist influencers" have been able to use the increasing number of social media apps and other communication channels to reach, recruit, radicalize and operationalize potential attackers. AI-enabled tools can help analysts cut through some of the noise and chatter and they are good research tools. That said, a good/skilled analyst is still required to focus AI tools on the right actors and channels, and to then provide the context and situational understanding needed to produce actionable intelligence that can mitigate threats."

Scott Stewart
Vice President of Protective Intelligence
TorchStone Global

Chapter 2: Executive Protection

Intelligence-led, data-driven protection

In 2026, executive protection will continue its evolution from a purely physical function to an intelligence-driven discipline. The expanding threat landscape — marked by social polarization, online targeting, and the weaponization of information — demands that protection programs become more adaptive and integrated. Strong EP teams will adopt scalable, data-informed models that align protection posture with credible risk rather than optics. Ultimately, success will come down to defensibility and agility: protecting executives wherever they operate while showing that decisions are rooted in data and contribute directly to business continuity.

Intelligence-led, data-driven protection

"The Clarity Factory 2025 Annual CSO Survey — sponsored by Ontic — found that 77% of CSOs think poor understanding of security among business executives is the biggest obstacle to their effectiveness.

Many CSOs respond with efforts to educate the C-Suite, but this misses the point. Executives don't need to understand security and what it does — they need to trust you. A CSO's communication objective is not to educate executives about the specific threats or the functions of security — instead, they must use stories to build trust and influence, conveying meaning, impact, and value-add in terms that senior leaders will understand.

One area where this can be especially impactful is executive protection. Over the past year, many boards have sought reassurance that C-Suite members are protected from threats to their physical safety. Yet some leaders push back, assuming it will be a heavy-handed approach that inconveniences them or their families.

CSOs can use stories not to explain program details that won't be remembered, but to convey balance, sensitivity, and a nuanced approach — reassuring leaders that executive protection efforts will be proportionate and well-judged.

Storytelling is now a non-negotiable skill for senior business leaders, and CSOs can expect a positive response. They should build their story, invest in communications and storytelling training, and create a functional narrative to build trust, awareness, and influence.

One storytelling client recently told me that he's started to hear his stories come back to him — that's the power of a story over a slide deck. Stories are sticky — they're more likely to be remembered and retold than org charts or service catalogs.

While C-Suite interest remains high, stories offer a powerful bridge between the concerns of executives and the capabilities of the security team. It's storytelling — not executive education — that secures the focus, resources, and buy-in corporate security teams need to be effective."

Rachel Briggs OBE
CEO and Founder
The Clarity Factory

Author of *The 2025 Annual CSO Survey*, *Holistic Security*, and *The Business Value of Corporate Security*

More from Rachel: The Clarity Factory's Storytelling for Security Leaders workshop

Intelligence-led, data-driven protection

"Attacks on politicians and executives are driving a new era of investment and standardization in executive protection. Rising threats – from targeted harassment and doxxing to high-profile physical attacks – have increased both visibility and spending for organizations responsible for safeguarding key personnel. Boards are recognizing that protecting executives is not just a compliance or HR issue, but a business imperative that directly impacts operational continuity, brand trust, and employee confidence. In 2026, standardization and data-driven metrics will elevate the executive protection profession. Just as cybersecurity teams measure dwell times, breach costs, and vulnerability exposure, executive protection teams will increasingly quantify risk reduction and operational impact: how many threats were identified, potential losses avoided, or disruptions mitigated. Organizations that connect these outcomes to clear business value will strengthen credibility, justify investment, and enhance performance across the security function."

Michael Evanoff
Chief Security Officer and Strategic Advisor
Verkada

"I don't think we've seen the end of targeted violence in our current 'Days of Rage.' Recent attacks such as those in Butler and West Palm and against Charlie Kirk and the ICE facility in Dallas indicate that the sniper threat will persist to haunt protectors. For VIPs speaking, outdoor public venues remain vulnerable to line of sight and the high ground (rooftops) used by copycat threat actors. To mitigate the sniper threat, rooftops should be pre-posted by event staff, combined with drone sweeps. Consideration should also be given to move speaking events into controlled indoor environments."

Fred Burton
Executive Director of Protective Intelligence
Ontic

Intelligence-led, data-driven protection

"As I contemplate the threats facing executive protection (EP) teams in 2026, I am reminded of Solomon's admonition, 'there is nothing new under the sun.' Domestically, and indeed globally, we have entered another cycle of internal polarization and societal friction that is reminiscent of the 'days of rage' we experienced during the 1960s and 1970s. This is resulting in a surge of attacks directed against prominent individuals like those seen during that turbulent period. The recent assassinations of Brian Thompson, Minnesota State Senator Melissa Hortman, and Charlie Kirk also serve to highlight the effectiveness of simple, time-tested methods of attack. As EP teams begin to implement measures to mitigate the impact of emerging attack tactics, such as the use of drones, they must not allow their concern for the future to eclipse their memory of the past. Attention must remain focused on protecting against danger posed by simple attacks conducted by a lone gunman armed with a pistol or long gun. EP teams must not neglect fundamental security practices such as conducting thorough advance work and protective intelligence assessments that can prevent simple attacks."

Scott Stewart
Vice President of Protective Intelligence
TorchStone Global

"In 2026, both external and internal threats targeting executives and enterprises are expected to intensify. From lone actors driven by personal grievances to ideologically-motivated activists and nation-state-sponsored operations, the threat spectrum is expanding. The need for integrated physical-digital programs that enhance visibility and layered protection against workplace violence and insider exploitation has never been greater. Investment in robust prevention capabilities — including technology-driven threat monitoring, structured triage and assessment processes, cross-functional insider-risk teams, and sustained workforce awareness — is essential to move from reactive defense to proactive threat prevention."

Jackie Day
Partner
Control Risks

Intelligence-led, data-driven protection

"The targeting of high-profile individuals will redefine executive protection not by proximity, but by exposure. As executives live increasingly digital lives, their online personas have become extensions of their physical presence, complete with vulnerabilities that can be mapped, weaponized, and monetized. What once lived in fringe corners of the Internet—doxxing, data brokerage, digital impersonation—has now entered the mainstream risk portfolio.

This evolution redefines the concept of duty of care. Protectors and security leaders must now treat digital exposure as a core dimension of personal risk management, on par with travel or residential security. The organizations that thrive will be those that approach exposure management as a discipline, identifying, modeling, and reducing the digital attack surface before threat actors exploit it.

In the years ahead, defensibility will become the new differentiator: not merely 'Was the executive safe?' but 'Was their digital life defensible?' That is where executive protection is heading, and where the profession must evolve."

Chuck Randolph
Senior Vice President, Strategic Intelligence and Security
360 Privacy

Chapter 3: Investigations

From silos to coordinated prevention

The future of corporate investigations will be defined by collaboration, transparency, and early intervention. As insider risk becomes intertwined with privacy and compliance, investigative teams must partner closely with HR, legal, and cybersecurity to identify threats before they escalate. In 2026, mature programs will formalize data-sharing frameworks that protect confidentiality while enabling proactive action. The emphasis will shift from punitive outcomes to preventive culture — building organizational trust and treating investigations as integral to business continuity and resilience.

From silos to coordinated prevention

"As threats increasingly originate from the digital area and those digital threats hold potential to cross into the physical realm, geolocation signals are likely to play an increasingly significant role in identifying, assessing, and mitigating risk. For example, IP address tracking, mobile device location data, and geotagged social media posts can provide actionable intelligence that bridges the gap between online activity and physical presence.

While analysts and investigators already rely on tools like license plate readers and social media geotagging, a new wave of emerging technologies and datasets promises to further advance location-based intelligence. For instance, Bluetooth beacons, Wi-Fi triangulation, and wearable devices can generate granular location data. Some of these technologies are already widely used in industries such as marketing, where consumer movement and behavior are tracked to deliver targeted advertising, or in life/safety applications, to monitor user location for emergency response purposes.

As the convergence of digital and physical risk continues, the demand for advanced location-based technologies in security and investigations is likely to grow, offering the potential to detect threats earlier, respond more effectively, and safeguard assets and people with greater precision. However, this increased reliance on location data brings significant privacy concerns to the forefront. The collection, storage, and analysis of geolocation information — especially when combined with other personal data — raises questions about consent, surveillance, and data protection. For the security industry, balancing the benefits of enhanced situational awareness with the imperative to respect individual privacy will be a critical challenge.

Lou Silvestris
Risk Intelligence and Investigations Team Lead
American Family Insurance

From silos to coordinated prevention

"Corporate investigations and insider risk teams have begun to realize that most insider threat investigations have a nexus to privacy. In the coming year, we will see greater collaboration between insider risk teams and privacy teams to ensure all regulatory requirements are met during corporate investigations to include timely escalations to the privacy team."

Tim Kirkham
Vice President, Investigations Practice
Ontic

"In 2026, corporate security teams will increasingly rely on AI-driven systems to detect unusual behavior and surface potential insider risks hidden within massive data sets. These tools will transform how organizations identify early warning signs, shifting detection from reactive to proactive. However, success will depend on understanding how these models learn and where their blind spots lie. The most advanced programs will pair AI efficiency with human oversight to ensure accuracy, fairness, and trust in every decision."

Adrienne Galbrecht
Sr. Team Lead, Strategic Services
Ontic

From silos to coordinated prevention

"In 2026, corporate investigation programs will increasingly rely on relationship building and organizational trust as force multipliers. Effective teams will recognize that early trigger awareness — spotting behavioral or environmental cues before they escalate — depends on open communication between employees, HR, Legal, and Security. The challenge will be maintaining this collaboration while respecting each function's privilege and autonomy. Mature organizations will formalize joint-review protocols and shared data models that protect confidentiality yet enable appropriate disclosure. The result is a system that values prevention over punishment, reinforces fairness and consistency, and supports the broader goals of employee safety, workplace integrity, and organizational resilience."

Jon Mangum
Chief Security Officer
Huntington Ingalls

"Targeted violence will be a persistent threat in 2026. It will continue to be driven primarily by lone actors motivated by perceived grievances and the desire to air them publicly. In this high-risk environment, proactive threat management will fundamentally shift from a tactical function to a strategic imperative discussed at the board level.

Geopolitical volatility, brand politicization, deep ideological polarization, and public mistrust in technology and institutions, coupled with an unpredictable job market, means the world will see more targeted violence. Countries around the world and US states will continue to enact laws mandating workplace violence prevention programs focused on early detection and behavioral threat assessments. These programs will go from nice-to-have to a core pillar of physical and enterprise security."

Robin Welch Stearns
President and Founder
Pacific Resilience Group

From silos to coordinated prevention

"The drive to include AI tools within workflows during the past 12 months has overshadowed the focus on developing and strengthening solid investigative practices. Teams in 2026 would benefit from a "return to basics" to hone their skillset. This includes re-examining workflows, source type, how to validate and vet sourcing, what is relevant versus related. Teams should be able to articulate clearly and in agreement what they are looking for and why, which factors matter in their investigative workflow and why it matters. Investigations aren't conducted as an exercise, the outcome is used to inform a decision to mitigate risk to the business–its people, places, IP, reputation, and products. The development of the people on a team is the best indicator for successful use of tools, whether AI-empowered or not. Tech is only as good as the people using them and continued training and development of people is essential."

Karna McGarry
Vice President, Managed Services
Red5

Chapter 4: GSOCs

The command hub for operational risk and intelligence

Tomorrow's GSOCs will serve as the nerve center for organizational risk intelligence — bringing together human expertise, smart automation, and connected data into one operational picture. In 2026, leading programs will move beyond traditional monitoring by integrating threat intelligence, business data, and contextual analysis to deliver real-time insights that guide decisions across the enterprise. Additionally, automation will help GSOCs scale globally while staying precise and responsive at the local level.

The command hub for operational risk and intelligence

"Converged GSOCs and Fusion Centers are essential for safeguarding people, property, and organizational reputation. Without the integration of cybersecurity, insider risk management, physical security, and advanced technologies, GSOCs will fall short of meeting future threat mitigation standards. A siloed approach creates vulnerabilities that adversaries can exploit, whereas convergence enables a unified threat picture, streamlined decision-making, and proactive risk management. Organizations that embrace this model will be better positioned to protect their assets, personnel, and brand integrity in an increasingly complex threat landscape."

Jacob Valdez
Head of Global Security Operations
Applied Materials

"The value of a well-designed, highly functioning GSOC cannot be underestimated. Forward-leaning CSOs will be working to integrate non-traditional security partners (Facilities, HR, Transportation and Logistics, Supply Chain, and others) within their GSOCs to create an intelligence center that provides a real-time operational risk picture. The added value of embedding these organizations within the GSOC is the speed at which a crisis management response can be deployed in the event of a major event. Including IT within the GSOC has been the norm for several years now, but more CSOs are expanding their operational risk capabilities by adding additional critical internal partners."

Dave Komendat
Chief Security Officer
Corporate Security Partners | Ontic Advisor

The command hub for operational risk and intelligence

"In 2026, GSOCs will become the true risk intelligence hub of the organization. With more accurate intelligence in the hands of the security teams, organizations make decisions faster with more confidence. AI-driven automation will move from experimental to essential within GSOCs and threat intelligence programs. Successful programs will determine the best way to optimize new technology using both people and computers, forming a human-computer system. With access to numerous information streams, GSOCs will be in the state of hyperconnectivity, providing organizations with valuable insight and information, and therefore supporting their growth.

Security teams will rely more on AI to filter noise from massive data streams, risk intelligence and proximity alerts, social media, access control, and incident logs, to identify credible threats faster. The real transformation will come from integrating these insights directly into incident management workflows, reducing response time, and improving decision-making accuracy across the enterprise. Lastly, with the power of intelligence, GSOCs move beyond providing traditional safety and security incident response and triage, they become the heartbeat of the organization, providing a slate of various non-safety and security services to add even more value to the organization."

Farhad Tajali, Ed.D.
SVP, Global Head of Safety and Security
Creative Artists Agency

"GSOCs will face growing pressure to do more — and do it faster — with leaner teams and tighter budgets. To keep pace, security operations will lean heavily on automation and integrated platforms that centralize data, streamline workflows, and enable real-time collaboration. The most valuable partners will be those that deliver timely, actionable intelligence and provide a unified space for teams to connect insights, manage cases, and make faster decisions."

Adrienne Galbrecht
Sr. Team Lead, Strategic Services
Ontic

Chapter 5: Incident Management

Turning incident response into a strategic advantage

In 2026, incident management will be defined by speed, precision, and foresight. Effective teams will use predictive analytics, AI-driven triage, and digital workflows to detect and respond to threats faster than ever. This shift will move organizations from a reactive recovery mindset to proactive prevention. Strong programs will focus on skilled people, clear playbooks, and seamless communication across teams. The most resilient organizations will treat every incident not as a setback, but as a chance to strengthen readiness and improve coordination across the business.

Turning incident response into a strategic advantage

"I think in the year ahead we'll see GSOC and incident management teams refocus on people, process, and technology. Too often, repurposed guards are placed in GSOC roles without proper training — well-intentioned, but it limits their impact. In 2026, I expect more investment in upskilling and recognizing that people are the foundation of effective security operations.

Processes will also get leaner. Long, 10-page SOPs don't work in fast-paced environments; teams will move toward concise, actionable playbooks that can actually be used in the moment.

And when it comes to technology, not every solution needs AI. I think we'll see teams double down on using what's already available — especially OSINT tools and social platforms like X or Instagram — to detect threats faster and act smarter without breaking the budget."

Michael Civitano
Senior Security Manager, Intelligence and GSOC
ServiceNow

"In 2026, incident management programs will emphasize speed of recognition and early intervention as key determinants of resilience. The ability to detect emerging disruptions—before they escalate into critical events or full-scale crises—will define maturity. Organizations will continue integrating data from safety, cyber, and facilities systems to shorten the time between detection, decision, and deployment. Playbooks will evolve into dynamic digital workflows, guiding responders with real-time situational context and embedded communications. The focus will move from reactive recovery to proactive containment—transforming incidents into learning opportunities that reinforce preparedness, strengthen cross-functional coordination, and protect business continuity."

Jon Mangum
Chief Security Officer
Huntington Ingalls

Turning incident response into a strategic advantage

"In 2026, threat management programs will evolve from reactive case handling to predictive risk prevention. AI and data analytics will play a pivotal role in connecting signals across investigations, incident reports, and behavioral patterns to identify emerging risks earlier. Threat detection takes on an entirely new meaning, using machine learning, and a perfect combination of human expertise and AI threat detection capabilities, leading to cyber-human learning loop, both machines and humans evolving and learning from each other.

Rather than responding to isolated threats, security teams will use predictive modeling and cross-functional data sharing (HR, Legal, Risk, etc.) to assess intent, capability, and escalation potential in real time. This shift in predictive threat management approach will enable organizations to intervene sooner, reduce insider risk, and strengthen the overall safety and security of organizations."

Farhad Tajali, Ed.D.
SVP, Global Head of Safety and Security
Creative Artists Agency

"Incident management will continue to be focused on predictive intelligence, especially with insider risk, geopolitics, and activism driving greater complexity and faster escalation cycles. The organizations who thrive will be those that shift from "responding quickly" to "seeing ahead," using data, cross-functional alignment, and industry partnerships to identify weak signals before they become headlines. AI will also be a key player in incident management, not as a replacement for judgment but as a multiplier for human capability. Tools that allow us to identify anomalies in behavior, accelerate signal-to-noise filtering, and summarize complex event streams in seconds will be differentiators in the ability to prepare before the sirens sound. That said, equal investment needs to also be paid in the wellbeing of the teams who carry the weight of responding to incidents. Without care for those who stand watch, resilience is temporary."

Arian Avila
VP, Technology and Security Operations Executive
CapitalOne

Chapter 6: Risk and Vulnerability Assessments

A unified view of organizational risk

In 2026, the process of identifying and mitigating risk will be fully embedded into enterprise strategy — aligning security priorities with strategic, operational, and reputational goals. Breaking down functional silos will create a unified understanding of organizational exposure and strengthen collaboration across teams. While AI-driven tools will enhance predictive capabilities, human judgment will remain essential for interpreting insights and guiding action. The most effective programs will emphasize continuous evaluation, cross-departmental alignment, and a culture of preparation that makes resilience part of everyday operations.

A unified view of organizational risk

"By 2026, physical security risk and vulnerability assessments will evolve from static audits to dynamic, intelligence-driven models that fuse physical, cyber, and operational risks. AI and predictive analytics will play a central role, enabling organizations to anticipate threats rather than simply document them. As a result, assessments will not only catalog vulnerabilities but will eventually model what could happen next. As the line between digital and physical infrastructure disappears, leading programs will focus on resilience, ecosystem dependencies, and measurable business impact — redefining how security and strategy intersect."

Manish Mehta
Chief Innovation Officer
Ontic

"In 2026, enterprise risk management must break free out of its silos. Physical, cyber, and geopolitical threats can no longer be treated separately — they are interconnected challenges demanding unified, agile responses to cascading effects across business operations. Success will rely on leaders being fluent across all threat domains, empowered by adaptive structures and communication flows that move as fast as today's information cycles. To stay ahead and drive innovation, organizations will need integrated frameworks that assess and quantify cross-domain risk and apply AI-enabled insight to anticipate, adapt, and respond in real time."

Lianne Kennedy-Boudali
Partner
Control Risks

A unified view of organizational risk

"Companies today face an ever-growing number of risks and vulnerabilities that they need to prepare for, and this is a certainty in 2026. These risks include executive protection, workplace violence, cyber attacks, labor unrest, civil unrest, geopolitical tensions, government regulations, economic downturns, active shooters, terrorism, and many others. Due to high risk volume, it is essential that companies conduct a continuous review of them and identify what their top fifteen or twenty risks are. It is also crucial that security leaders and their teams are thoroughly prepared for these risks to actually occur. A comprehensive understanding of your company's risks and vulnerabilities leads to a thorough Enterprise Risk Management (ERM) system so your leadership fully understands what is needed to protect its people, assets, and financials. One of my favorite sayings has always been - Proper Preparation Prevents Poor Performance."

Rich Davis
Senior Security Advisor
Richard C Davis Security Consulting

"Leadership will push, and security professionals will continue to search for, the perfect AI-driven solution to help them determine, or "predict" risk. AI will help surface the "so what?" but the "now what?" action will still require human judgment and a hands-on approach. This will leave those who are seeking full automation frustrated."

Cynthia Marble
Senior Director of Executive Protection Practice
Ontic

A unified view of organizational risk

"Uncertainty requires security to anticipate what may be on the horizon and prove their ability to be adaptable and anticipate change. Risk assessments as the type of documents that can provide companies this guidance. It's an opportunity to provide legal, human resources, sales, marketing, policy, compliance, and other business units with a framework for coordination and communication with actionable outcomes to navigate through 2026 and beyond. A strong Risk Assessment should go beyond physical assessment of cameras, badging, and access control and provide a holistic approach to security and its support to each business unit. It can provide the connection between an outdated business continuity plan, threat to supply chain, and changes in labor laws in another country. These products not only provide a roadmap for security and identify gaps and changes in the threat landscape, but if done correctly, they serve a conduit for security to take the lead in guiding other stakeholders through the process of minimizing risk for the company."

Karna McGarry
Vice President, Managed Services
Red5