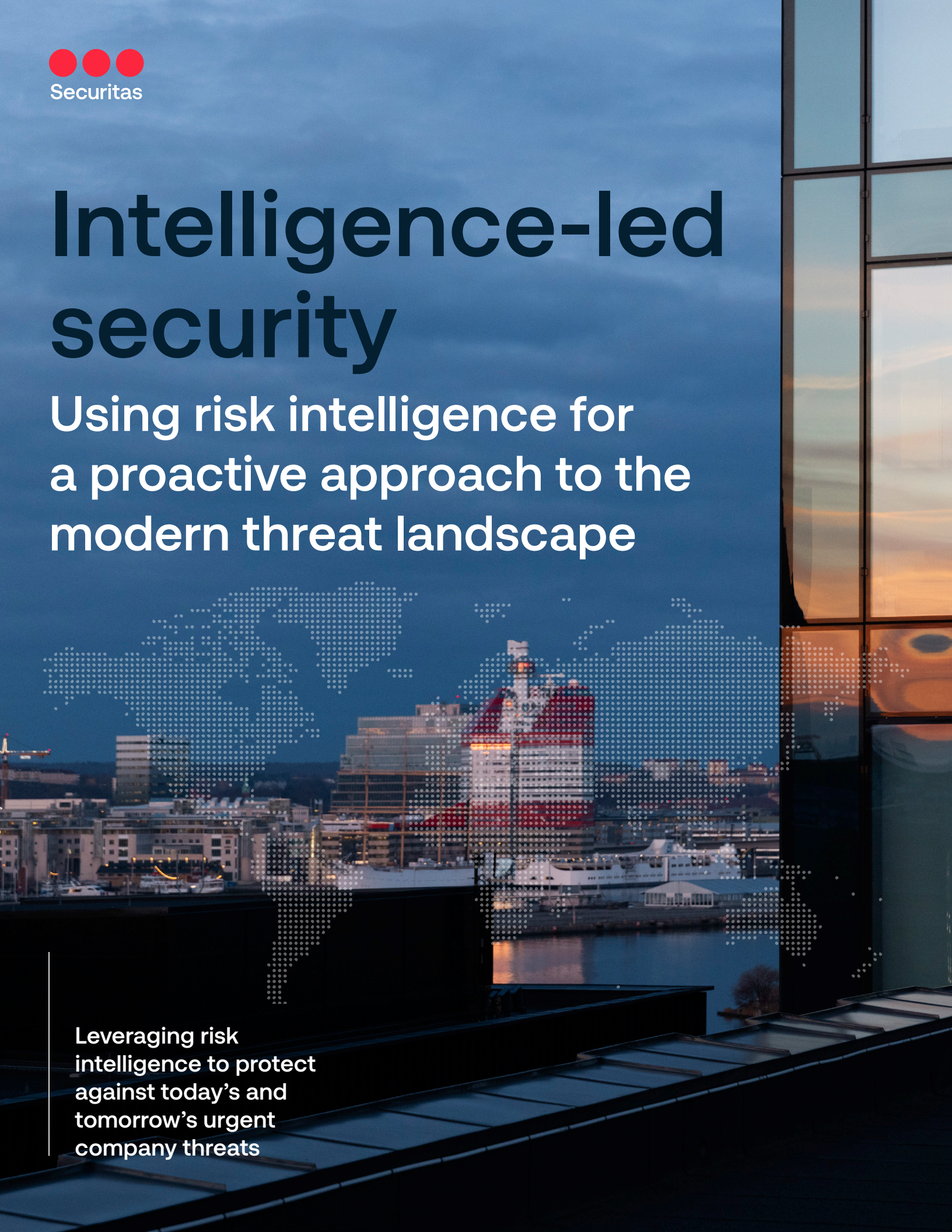
Securitas

Intelligence-led security

Using risk intelligence for a proactive approach to the modern threat landscape



Leveraging risk intelligence to protect against today's and tomorrow's urgent company threats

Contents

Welcome to the intelligent security era

Companies today navigate an increasingly complex and interconnected risk landscape that is evolving faster than ever. With the protection of people, assets, and reputation on the line, security programs must evolve with the times. This requires a shift in how companies approach security, from a reactive process focused only on incident response to a proactive security program integrating across the organization.

A crucial piece of this new security puzzle is risk intelligence. Risk intelligence is more than information — it's context. What does information mean, what will happen next, and what can you do? Risk intelligence powers an intelligence-led security program, allowing organizations to anticipate, detect, and mitigate threats and feel confident in their security decisions.

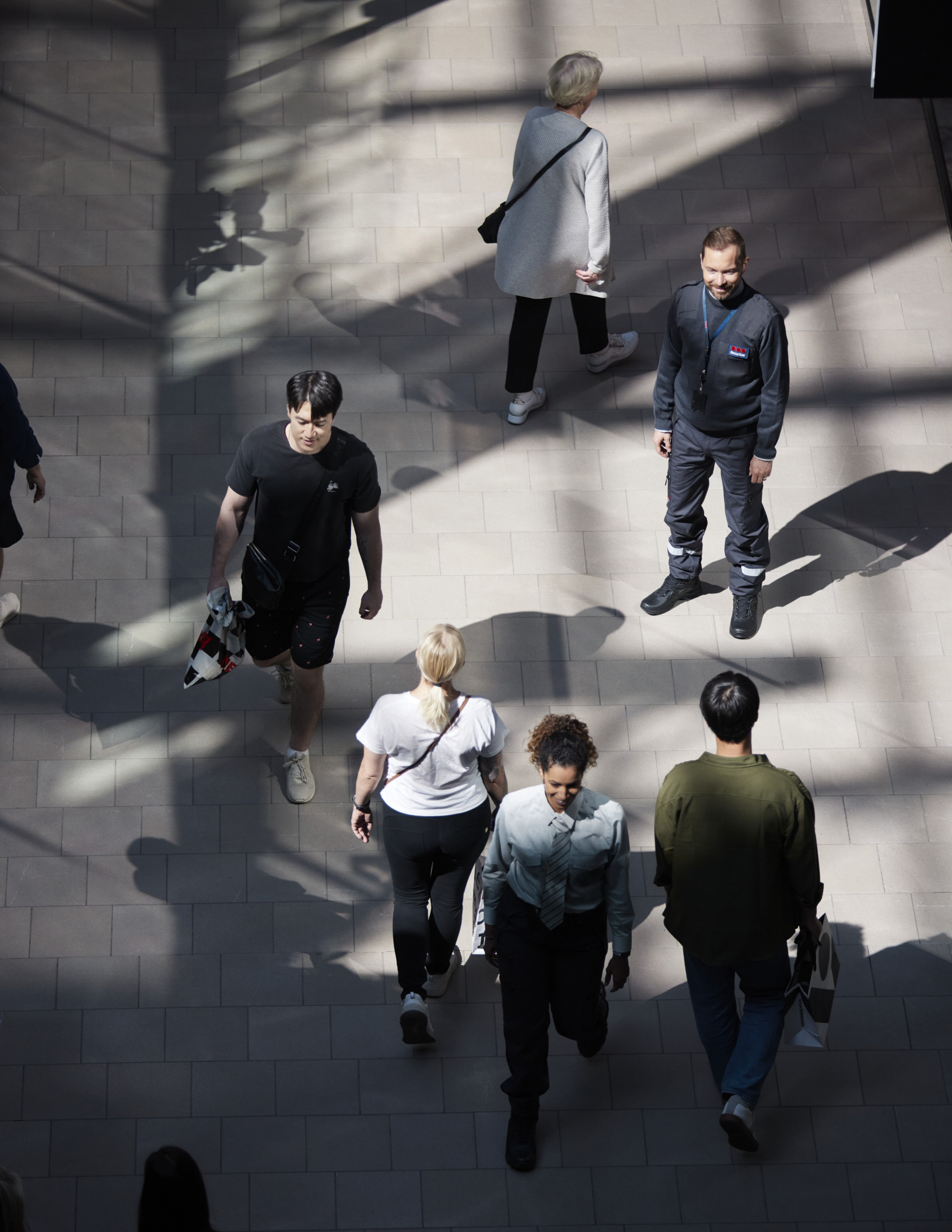
At Securitas USA, we help organizations prepare to meet today's and tomorrow's threats through comprehensive risk intelligence services. Our world-class Risk Intelligence Center monitors global threats and helps our clients have the insights they need for their intelligence-led security programs.

We invite you to learn about the benefits of intelligence and how a security program can protect and grow your organization. In this whitepaper, you'll enter the intelligent security era, where we cover the basics of risk intelligence and how a security program can detect threats earlier, mitigate incidents more effectively, and innovate on new opportunities otherwise unseen.

You'll discover the highest-impact global risks identified by Securitas USA in our latest Annual Intelligence Estimate and how security teams can respond. You can also see how we implement intelligence-led security with a client case study, helping them build resilience in the face of adversity — and how we can do the same for you.

Integrating intelligence into security programs is indispensable for businesses preparing to meet the unpredictable challenges of the future. The intelligence-led security approach, supported by a trusted partner like Securitas USA, can significantly enhance your capability to proactively manage risks, assisting sustained growth and resilience in an ever-evolving global landscape.

Mike Evans
Director, Risk Intelligence Center



Navigating the threat landscape with proactive risk intelligence

Companies today face a vast and complex web of risks[1], from cyber threats and industrial espionage to shifting markets and geopolitical unrest. Faster informational speeds, the global economy's interconnectedness, and rapid technological advances amplify the potential impacts these threats can cause.

Successfully navigating the always-evolving risk landscape demands more than mere vigilance. It requires a shift in security from a reactive process to a strategic, proactive, organization-wide approach.

The key to this new approach is integrating intelligence into security programs. Intelligence-led security transforms data collected from many sources into actionable intelligence[2] that defines current threats and anticipates future risks. Intelligence-led organizations can devise effective strategies to help manage a broad spectrum of internal and external risks.

How can an intelligence-led security program fortify your business against the unpredictable challenges of tomorrow?

1 Top 5 macro security risks European businesses faced in 2023
2 How modern security is driven by actionable intelligence

Who needs intelligence-led security?

At its core, an intelligence-led security program is about understanding and assessing what matters to you as an organization and a decision-maker. Risk intelligence supports this effort through a consistent flow of information from many sources to give organizations visibility and foresight into potential risks and make informed choices to manage risks and enhance resilience.

While risk intelligence can help any company improve its security program, it can significantly benefit specific industries. For instance, aerospace, defense, life sciences, and technology companies inherently possess a higher threat profile because they're attractive targets for malicious actors. Other risk–conscious sectors, like financial services, may not confront the same threat levels but hold vital information and services they need to protect. Robust security measures can help them prevent operational disruption.

Across all industries, smartly applied risk intelligence helps companies of all sizes and in every industry proactively manage their organizational security and unlock new paths to grow with their markets.

Risk intelligence: the basics

Intelligence is not some "dark art" relegated to police or military agencies. Useful information exists everywhere and offers the potential for incredible insights — if you know where to look and how to use it.

Sources of intelligence data

Intelligence relies on various sources operating together to view the entire threat landscape. A well-executed security program incorporates data from multiple sources, such as:

Open-source intelligence (OSINT)
OSINT is data collected from publicly available sources, such as newspapers, television, radio broadcasts, public reports, government documents, and websites. OSINT helps companies understand the public sentiment, media coverage, and industry and market trends.

Within this field is social media intelligence (SOCMINT), data pulled from social media sites. This helps security teams identify and analyze social signals that point toward emerging security incidents and larger trends.

Human intelligence (HUMINT)
HUMINT is information gathered through interpersonal contacts, such as interviews, meetings, and operations. HUMINT can provide insights into intentions, thoughts, and motivations not readily discernible from digital or document-based sources.

You can gather this data from your organization or lean on a partner to expand your information repository. Securitas USA's global HUMINT network offers an extensive dataset gathered from employees, sensors, and other technology.

Proprietary internal data
Security program components generate significant quantities of intelligence that companies can use. For instance, cameras capture critical intelligence data during physical security incidents; however, that makes up a tiny percentage of overall camera footage. Analyzing footage of regular operations for additional intelligence can help identify new vulnerabilities or improvement areas. Many opportunities like this live within the proprietary data your organization gathers.

Data's wide availability may imply that collecting intelligence is easy, but useful intelligence must also be accurate, timely, and relevant to your organization. An all-source approach that ingests data from many sources, coupled with internal subject matter expertise, can help you find and discern reliable and credible intelligence from noise.

Types of manipulated information

Security professionals should know how to screen incoming intelligence data for risks and identify the most relevant ones. This is extremely important today as organizations and their people, including executives, are increasingly connected to the online world.

Yet, malicious actors manipulate information and how it spreads to advance specific agendas. Manipulated information has become such a global phenomenon that the United Nations has stepped in to combat its spread[3].

Security teams need to know what manipulated information looks like. The most common types are:

Misinformation
Misinformation deals with the unintentional spreading of incorrect information by sharing stories believed to be accurate but are actually amplifying false information. Sharing a company story on social media that looked true but was fabricated is an example of misinformation.

Disinformation
Disinformation involves deliberately spreading false information where the original person sharing it knows it's not true or lacks context, intending to advance specific (often harmful) agendas. For instance, a threat actor could generate negative rumors about your company or its leadership, resulting in financial or reputational damage.

Malinformation
Malinformation uses legitimate information out of context or combines private data to draw false conclusions to harm individuals, groups, or organizations. For example, threat actors leaking your CEO's personal information publicly (aka "doxxing") is a form of malinformation.

An intelligence-led security program monitors and assesses threats like these to help so that your organization and its people are protected from the right risks.

The intelligence cycle

Intelligence is the linchpin of a proactive organizational security program. Effectively using it may require adjusting your operations to match how information should flow through an organization. We call this the "intelligence cycle," composed of four major steps.

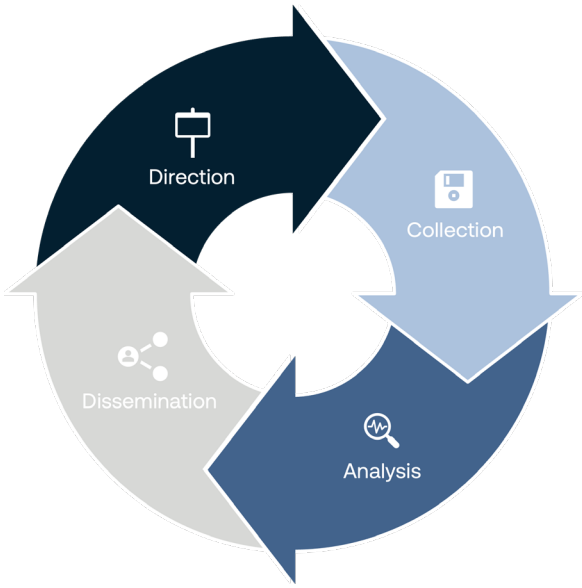
Direction
Direction involves identifying and prioritizing intelligence requirements across the business. Your leaders should define the organization's objectives and relevant context to guide the rest of the cycle.

Collection
During collection, you gather insights from multiple sources. An all-source intelligence approach[4], which includes sources unique to your organization, such as employees, partners, and suppliers, helps you avoid intelligence gaps.

Analysis
Security teams should then apply analytical techniques to interpret collected data. Many teams finish this phase by applying red-amber-green ratings in risk matrices. However, technological tools can offer more sophisticated analytical methods to produce comprehensive insights.

Dissemination
Dissemination is the sharing of intelligence findings across the company. Many organizations limit dissemination to security teams, but intelligence-led security needs valuable insights and recommendations to reach decision-makers across business functions.

Information flowing through this cycle shifts security from a reactive process to a proactive business function that adds value in multiple ways.



4 Risk Intelligence Advisory Service: Organization specific intelligence-led security

Approaching proactive intelligence-led security

Intelligence-led security programs can lead companies' approaches to security and strategic planning. Security practitioners must provide insights and recommendations to help combat potential risks and contribute to organizational improvement and growth avenues.

How do you set up and run this security program to help ensure your company is safe now and grows in the future?

Risk intelligence assists in early detection and mitigation

Risk intelligence can empower your organization with early detection mechanisms to identify potential threats before they escalate. Continuous monitoring and analysis of various intelligence sources allows you to discover, act, and mitigate threats faster.

For example, consider the worldwide upheaval in early 2020 because of the COVID-19 pandemic. Many businesses and people were caught off-guard by the pandemic's onset and severity, significantly affecting companies' operations[5] worldwide.

Yet, intelligence showed signs of an oncoming pandemic in late 2019. Stories appeared about "unknown viral cases" emerging in specific regions. Our intelligence teams drafted reports about a possible pandemic as early as December 2019, alerting our customers to these early warning signals.

Proactive monitoring for leading indicators of potential threats—in this case, COVID-19—helps companies better plan and prepare to mitigate business and operational challenges before risks fully materialize. It's a powerful upgrade to your organization's security operations: You guard against known threats, uncover the fuller threat landscape, pick out patterns, and act decisively to achieve better security outcomes.

How can security leaders gather and analyze intelligence for early signs of trouble? Start with a few key steps:

Leverage all appropriate intelligence sources, including internal organization insights and partnerships. Successful intelligence operations require a mix of data streams: OSINT, SOCMINT, HUMINT, and proprietary internal data. How much and what kind of insights you need depends on your company's size, industry, and security profile, but diversify beyond one channel.

Apply critical thinking during intelligence analysis to identify potential leading indicators in available information that could warrant further monitoring. It's easy to compile everything into blanket alert reports. However, using intelligence to drive business decisions means diving into the data, searching for patterns, and alerting teams on specific risks and their implications.

5 Impact of the coronavirus pandemic on businesses and employees by industry

Review and update intelligence requirements regularly to focus collection efforts on emerging risks. As the intelligence cycle runs, revisit the types of signals you seek and the sources you use. Hold a team leader accountable for this review process and invest sufficient time and resources into keeping your intelligence fresh and relevant to your needs. Since the risk environment changes quickly, we recommend reviewing and updating your objectives and risks at least every three months.

Tailor your incident response using intelligence

After establishing potential organizational threats, teams need to know the details: Who is behind a threat, why they're doing it, what they hope to achieve, and how they plan to attack. Risk intelligence analysis can generate the crucial context teams need to tailor response plans and resolve incidents.

For instance, a Securitas USA client recently identified a particularly disruptive protest planned for the next three months. While the client's leadership respected the right to protest, they needed a strategy to help so that protest actions did not lead to danger against people and assets.

They gathered risk intelligence through multiple sources to determine the groups behind the protest and their intended actions. Equipped with this information, the company planned its incident response, taking steps like:

- Monitoring for suspicious behavior
- Posting signs to deter trespassing
- Obtaining a court injunction to allow police to intervene should protest actions turn disruptive
- Coordinating external efforts between HR, operations, legal, and communications

The company tailored its response strategy and successfully mitigated millions of dollars in potential disruption risks. Security teams using risk intelligence help so that their incident response efforts are proactive and strategic, addressing root causes and helping to prevent future occurrences. Preparing more informed incident responses requires a few critical steps:

Conduct an inventory of critical assets and risks, walking through security requirements to identify priority areas to help protect during an incident or recover post-incident. Intelligence data can help determine what qualifies as a "high-value" asset and warrants additional attention or protection.

Conduct incident response planning within security teams and across the organization to align expectations and build a seamless plan before, during, and after incidents. HR, operations, legal, and communications leaders will likely influence an incident's outcome. Solicit their ideas and feedback and include them in regular security operations and reports.

Leverage partnerships with security experts to review an all-source intelligence collection strategy and get assistance analyzing security event data.

A partner's expertise will help you accurately and timely identify and contain vulnerabilities and emerging threats.

Discover market-changing innovations

Intelligence plays a critical role in security's future; however, the information you gather can also help catalyze a culture of innovation within your organization. Detailed information on potential threats can highlight emerging opportunities, turning risk intelligence into a wellspring of insights to develop fresh strategies, solutions, products, and services.

For instance, reviewing and analyzing SOCMINT helps companies understand emerging threats and protect people and assets. The tools and techniques to evaluate SOCMINT for threats can also identify emerging market opportunities. Intelligence can track customers' needs and competitors' activities to offer new, lucrative paths.

Intelligence should also help teams identify improvements to a security program's operations and outcomes. The holistic integration of technology, data, and human resources leads to insights into new components, capabilities, and training. With a security program integrated across organizational departments, intelligence can support the company's suite of operations and drive value in myriad ways.

This results in a culture of foresight that encourages teams to innovate, explore new avenues, and pivot strategies to help address challenges more effectively. To implement this type of forward-thinking culture, consider:

Utilizing security tools that track market trends, competitor activities, and shifts in the geopolitical and economic landscape affecting your industry and markets. This tool should ingest intelligence data from many sources and derive insights that lead to actionable steps and improvements in your operations.

Including more than security teams in regular intelligence reporting. Consistently share these emerging opportunities with leaders throughout your company. Regular, positive exposure to this information helps reinforce an organizational culture that reflects security best practices and forward-thinking innovation.

Embrace intelligence-led security with a trusted partner

Given the evolving threat landscapes and the need to differentiate, risk intelligence will play an ever-increasing role in organizational success. Security's role will expand from solely reactive protection to proactive business support, development, and growth. Companies equipped to gather, analyze, and deploy intelligence and insights stand to gain the most from this future.

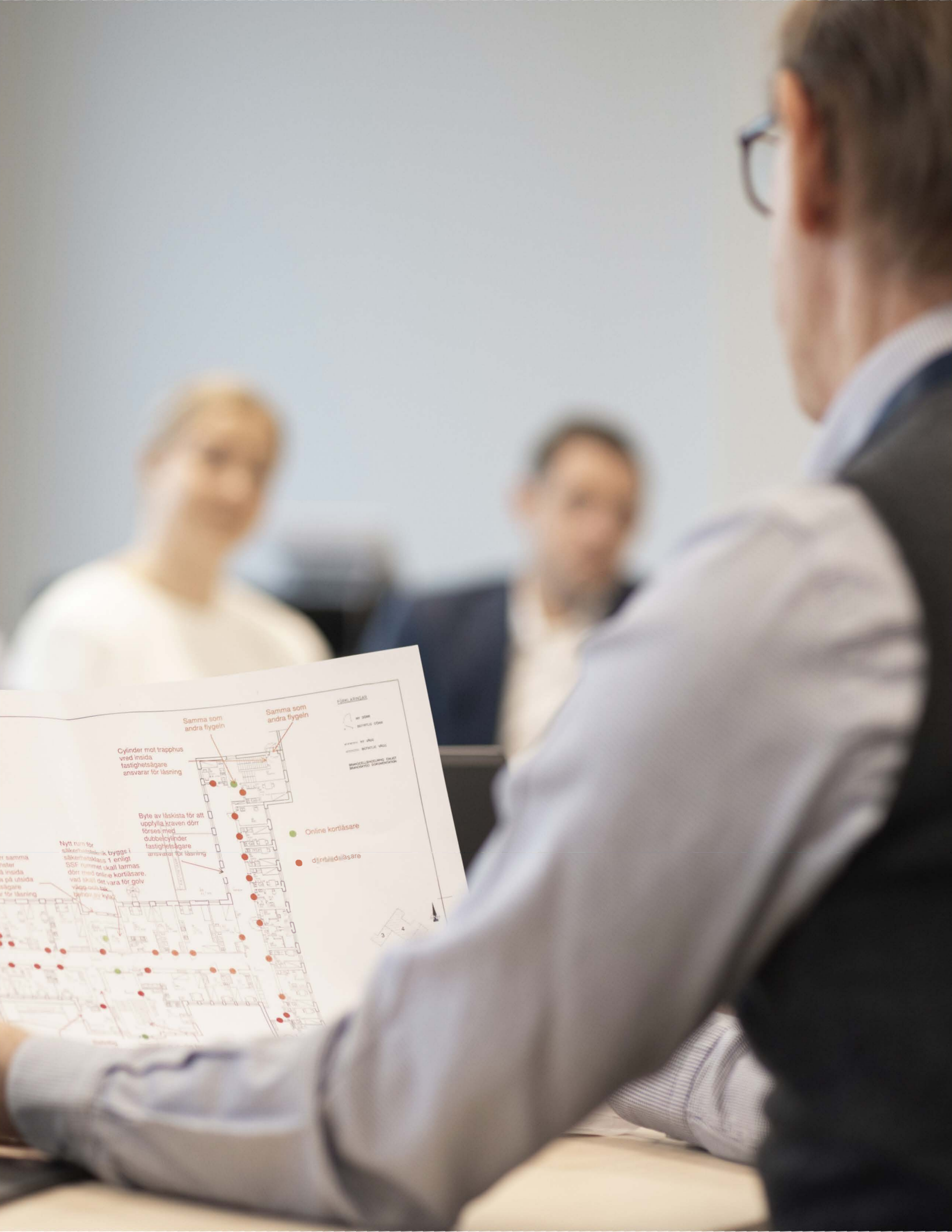
Everybody can access high-quality intelligence: From small businesses to global enterprises, Securitas USA helps companies of all sizes successfully deploy intelligence through our Risk Intelligence Center[6].

Our approach champions producing finished intelligence with insights and recommendations using an all-source approach so our clients can act quickly and decisively. We help integrate intelligence into our client's operations, ensuring on-site officers and account teams can identify and act upon potential threats. On-the-ground teams can mitigate threats before they emerge, supported by Securitas USA's suite of protective services.

The world will keep turning, and every day will bring new risks and challenges to your environment. Armed with risk intelligence and the services to contextualize and act upon insights, you'll be better prepared, informed, and in control to mitigate threats and take advantage of opportunities.

Contact us today to discuss your intelligence needs and how we can help transform intelligence into action[7].

6 Risk intelligence: Securitas' team drives resilience
7 RIC


Samma som andra flygeln
Samma som andra flygeln
Cylinder mot trapphus vred insida fastighetsägare ansvarar för låsning
Byte av låskista för att uppfylla kraven dörr försedd med dubbelcylinder fastighetsägare ansvarar för låsning
Online kortläsare
dörrautomatläsare

The Risk Intelligence Center's 2024 Annual Intelligence Estimate in brief

Influence and interference will define global security in 2024: influence to achieve an outcome, and interference to disrupt it. The key to succeeding in this threat landscape is information and the power to use it wisely.

Securitas USA's Risk Intelligence Center combines its all-source data approach with the vast network of security professionals at Securitas USA to develop the highest-quality finished intelligence. We share more details on the most pressing regional and global risks in our Annual Intelligence Estimate.

What major risks do businesses face in 2024?

Based on our analyses, here are the highest-level risks in today's world:

Climate and environmental risks

Climate change and rising global temperatures increase extreme weather events that disrupt business operations and negatively affect global food, energy systems, and infrastructure. As climate change takes center stage in global politics, expect additional pressure from environmental activist groups to interfere with operations. Companies should develop and test resilience plans to mitigate extreme weather impacts and review their ESG guidelines.

Increasing corporate espionage and the need for counterintelligence

More threat actors will infiltrate corporate operations, leading to significant data loss and damage to assets and reputation. Counter-intelligence will become a more prominent part of company operations, though this will take time. Meanwhile, companies should develop effective insider threat identification and detection programs and establish clear reporting processes.

Increasing security and stability challenges in Africa

Elections in the largest countries and increased influence from Russia and China are shifting geopolitics in Africa. Companies want to engage with Africa for its abundant natural resources and large market opportunities. Still, they must be wary of potential conflicts, coups, and corruption across large parts of the continent, so companies should prepare resilience plans and routes to evacuate personnel in case of incidents.

Middle East security and stability undermined by US-Iran competition

Following the escalation of the Gaza-Israel conflict, multiple wide-ranging flashpoints could potentially ignite in 2024. As the US-Iran relationship maintains significant tension, pressure could boil over into unrest or conflict, such as the Houthi disruptions to shipping in the Red Sea. Companies operating or with supply chains operating in the region will likely experience disruptions, so develop contingency plans in case instability increases.

Persistent heightened threat of extremism and terrorism

Foreign and domestic extremism and terrorism threats will stay heightened in 2024 as such groups increase clashes with authorities and potentially plan acts of sabotage. Europe is especially vulnerable, as major events like parliamentary elections, the 2024 Paris Olympics, and the European football championships present appealing targets for hostile actors. Companies with international operations should assess their exposure and prepare proper safety protocols.

Europe's diversifying activist landscape

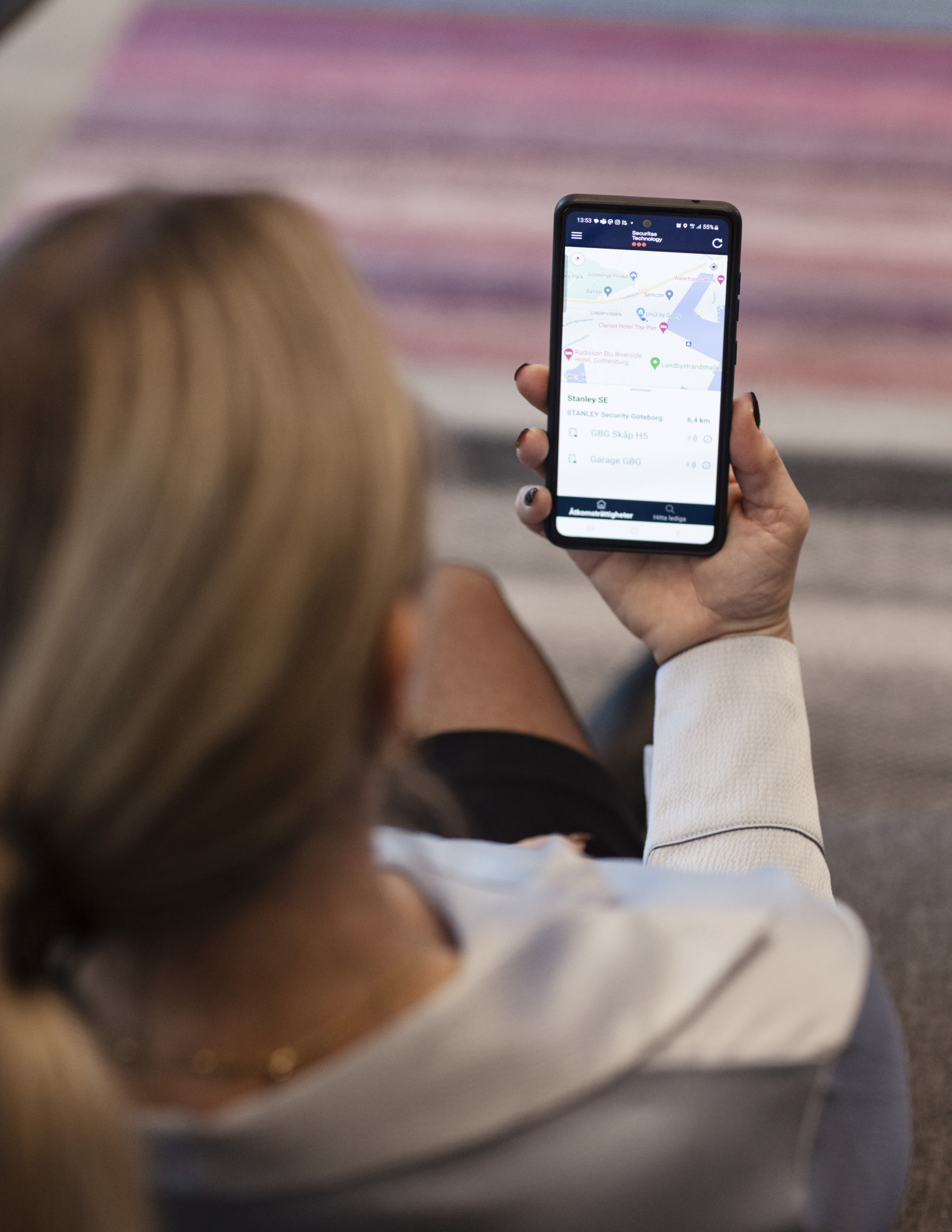
In addition to extremism, activist groups have honed more potent tactics, techniques, and procedures (TTPs) to target companies and disrupt their operations. Increased media and public coverage of activist actions may embolden groups to impose larger risks on their targets. Companies should develop specific response plans for activist groups and monitor their partner network for other targets.

Organized criminal groups and their expanding reach

Organized criminal groups (OCGs) are expanding into more industries throughout Latin America and beyond. OCGs are exploiting mining operations, increasing global fentanyl production and distribution, extorting organizations with ransomware, and laundering money through cyberspace. Companies should review physical and cyber security measures to help protect assets, people, and property from potential OCG threats.

As risks multiply, safeguard your operations by developing and maintaining intelligence monitoring capabilities to mitigate threats like these and more.

What about other critical risks, such as cybercrime, critical infrastructure, and doing business with China? To help prepare your plan of action, review the full Annual Intelligence Estimate 2024 report.


13:53
55%
Securitas Technology
Göteborgs moske
Banzai
Semcon
Waterfront Cabins
LUNDBYVASSEN
Uni3 by Geely
Clarion Hotel The Pier
Radisson Blu Riverside Hotel, Gothenburg
Lundbystrandshallen
Stanley SE
STANLEY Security Göteborg
6,4 km
GBG Skåp H5
Garage GBG
Hitta lediga

How can the RIC help clients prepare for risks today and tomorrow?

Leveraging advanced technology and vast experience, Securitas' Risk Intelligence Center delivers insights to mitigate complex threats from cybercrime, terrorism, and other emerging global challenges. We equip businesses and security teams with the knowledge needed for safer decisions.

Our work helps tailor your intelligence-led security program powered by technology and timely intelligence data.

Leveraging advanced technology and vast experience, Securitas USA's Risk Intelligence Center delivers insights to mitigate complex threats from cybercrime, terrorism, and other emerging global challenges. We equip businesses and security teams with the knowledge needed for safer decisions. Our work helps tailor your intelligence-led security program powered by technology and timely intelligence data.

Securitas USA provides intelligence services like reports, alerts, and investigations to help clients make informed decisions and protect their operations. We identify threats daily, like insider threats, criminal activity, and emerging trends affecting clients.

For instance, Securitas USA's RIC collects, analyzes, and shares vast intelligence, producing more than 14,000 global alerts per month and 350 reports per year. One of these routine reports recently led to a significant success for intelligence-led security. The report documented a Securitas USA guarding client, a multinational manufacturing company with a global supply chain, as a target for disruptive protests. Thanks to risk intelligence, the company learned the protest group's goals were to interfere with processing and distribution centers and stop the supply of perishable goods.

Before the client signed up for intelligence services, Securitas USA's RIC analysts proactively addressed the threat with them. The company's security manager revealed they had suffered a similar incident beforehand, incurring nearly £1.2 million in losses due to supply chain disruptions.

To prevent this potential outcome, they initiated a comprehensive response, including increased awareness and communication with suppliers, updated security and resilience measures based on specific threats, and an injunction obtained from the High Court in London to prevent trespassing.

With heightened preparedness, enhanced security, and an injunction, the company proactively protected its people and assets. This incident helped the client realize the importance of using intelligence for baseline threat assessments and ongoing risk monitoring, and they signed on with the RIC afterward.

Want to know more details and action steps the client took? See the full story[8].

8 Risk intelligence helps prevent potential losses for client

Tailored risk intelligence services

No matter what your threat landscape looks like, risk intelligence can help you contextualize data and make informed decisions to protect your organization. Securitas USA provides many services to put intelligence to work, including:

- Asset and location security
- Security risk management and investigations
- Brand and reputation protection
- Crisis and incident management
- Travel security and executive protection

Securitas USA approaches security on an individual basis. Every client has unique needs, so we spend considerable time understanding your company and goals. Typically, working with us involves:

- Determining your business requirements, like real-time world event alerts, location-specific data, company-specific information, or personalized analysis.
- Choosing a plan that suits your needs, including customized alerts.
- Accessing our services through a safe and secure process.
- Accessing round-the-clock support from our analysts on potential threats or challenges.

We tailor our plans to meet your specific intelligence objectives and expectations, including services like:

- Situational awareness reporting services, providing intelligence on threats worldwide
- Targeted alerting notifying clients of incidents or threats near them
- Individualized intelligence services to meet your specific needs and concerns
- Embedded analyst services, with an RIC analyst equipped to deliver customized intelligence

The intelligent security era starts with actionable intelligence. Let us help you find the most crucial information and use it to protect your organization and grow into the future of security.

Reach out to us today to talk about your intelligence goals and objectives.