

WHITE PAPER

# Security Intelligence: Driving Security from Analytics to Action

## Solve Your Security Challenges With Elite Intelligence

Security intelligence brings automation and insights to the forefront to solve every security challenge. Recorded Future combines analytics with human expertise to produce superior security intelligence that disrupts adversaries at scale.



### CHALLENGES:

#### Vulnerability Management:

Thousands of new high and critical vulnerabilities expose your organization to potential threats each year — but there's no way to know which ones to patch first, and it's impossible to patch them all.

#### Third-Party Risk:

Static, point-in-time vendor assessments provide only limited visibility into the risk profiles of the third-parties your organization depends on.

#### Geopolitical Risk:

Attacks, protests, natural disasters, and other localized events threaten your physical assets around the globe as shifting political climates and language barriers complicate your security efforts.

#### Brand Protection:

Phishing campaigns, data and credential leaks, and domain abuse like typosquatting all put your organization's reputation in jeopardy.

#### Threat Analysis:

Manually collecting, analyzing, and sharing vast amounts of information leads to data overload, communication breakdown, and analysis paralysis — as well as dead ends on the dark web.

#### SecOps and Incident Response:

The rapidly expanding threat landscape, time constraints, and lack of context about threats make it impossible to connect the dots across a high volume of disparate data and information.



### SOLUTIONS:

#### Vulnerability Intelligence:

Reduce the actual risk to your organization with external content that empowers you to prioritize patching based on the likelihood of vulnerability exploitation — not just the severity.

#### Third-Party Intelligence:

Continuously assess the third parties throughout your entire supply chain in real time for an unbiased, ongoing view of the risk they represent to your organization.

#### Geopolitical Intelligence:

Receive clear warnings before events occur and as they happen — so you'll be always prepared to take immediate action and protect your assets in the locations that matter to your organization.

#### Brand Intelligence:

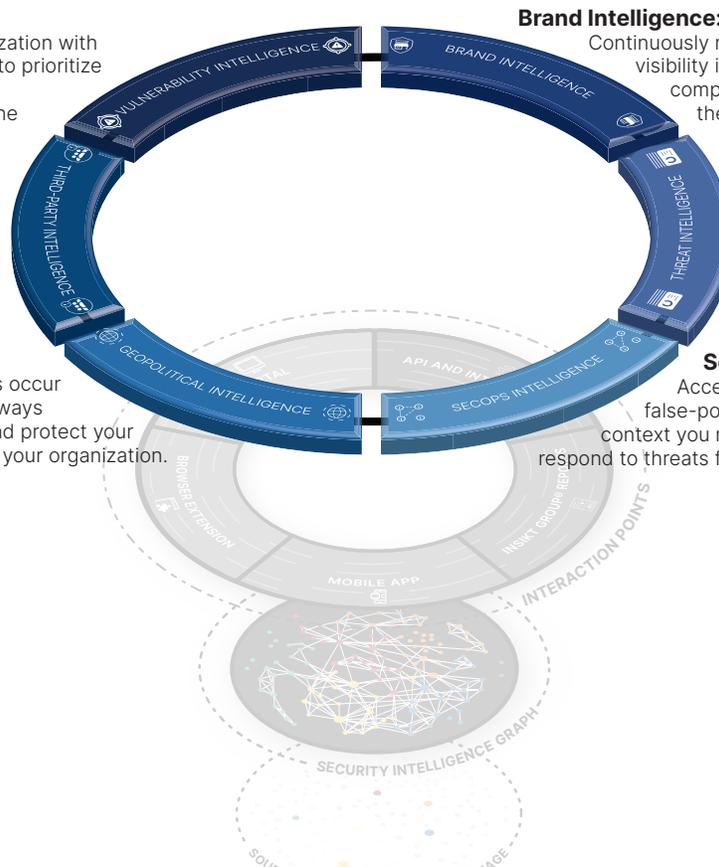
Continuously monitor the internet at scale for visibility into fraudulent mentions of your company and products — and quickly take them down.

#### Threat Intelligence:

Eliminate manual research and interact with elite intelligence in real time for a comprehensive view of your threat landscape that empowers you to focus on disrupting your adversaries.

#### SecOps Intelligence:

Accelerate alert triage with fewer false-positive alerts, and instantly get the context you need to make informed decisions and respond to threats fast.



# TABLE OF CONTENTS

<b>Embedding Intelligence for a Security Advantage.....</b>	<b>4</b>
Security Intelligence: By Design.....	6
The Single Source of Truth Across Your Organization.....	6
Shared Approach, Meaningful Outcomes.....	6
<b>Supercharge Six Critical Security Solution Areas.....</b>	<b>8</b>
One Plus One Equals Three.....	12
<b>Security Intelligence That Fits Your Organization.....</b>	<b>13</b>
Think Big, Start Smart.....	15
Advance When and How You Want.....	15
<b>Kick off With Quick Wins.....</b>	<b>16</b>
Reach Higher With Security Intelligence.....	18

# Embedding Intelligence for a Security Advantage

**Too often, intelligence and security are out of sync. Teams and objectives are siloed, analysis lacks relevance, and the response is slow and reactionary — resulting in lost time and resources. Of course, the alignment of intelligence and security is precisely where organizations see some of their most dramatic operational gains, whatever the security or risk initiative may be. When we take a unified approach by embedding analytics and automation into the core of everyday security workflows and decision-making, [security intelligence](#) and its outputs transform security and make the greatest impact.**

## Security Intelligence: By Design

Functionally, security intelligence is a method by which data and insights are collected, analyzed, and automated to accelerate distinct security systems and functions. More than that, it's a mindset; a philosophy for [how intelligence drives every security initiative and strategic decision](#). In the same vein as other “by design” doctrines, security intelligence brings [automation and insight](#) to the forefront of every facet of security, including strategic planning, technical design and architecture, and implementation and execution.

More concretely, Recorded Future uses this definition:

**Security Intelligence:** *An outcomes-centric approach to reducing risk that fuses external and internal threat, security, and business insights across an entire organization.*

## The Single Source of Truth Across Your Organization

Security intelligence is applicable to practically any security, threat, or risk initiative you manage. Take for example, [phishing prevention](#) and [vulnerability management](#): These two distinct functions share little in common in terms of technology, experience, and task execution. Yet, both benefit from security intelligence and the tailored data collection, analysis, and workflow automation that it produces.

Rather than starting from scratch each time, security intelligence enables organizations to build, store, and reapply common insights and operational workflows wherever possible. As security intelligence expands to additional functions and stakeholders, the organization maintains institutional knowledge and the data and insights grow more robust for every security initiative.

## Shared Approach, Meaningful Outcomes

With a common process and framework underlying security intelligence, the business benefits and security outcomes also share similarities for any security, risk, or threat initiative it supports. In particular, security intelligence benefits fall into three primary categories:

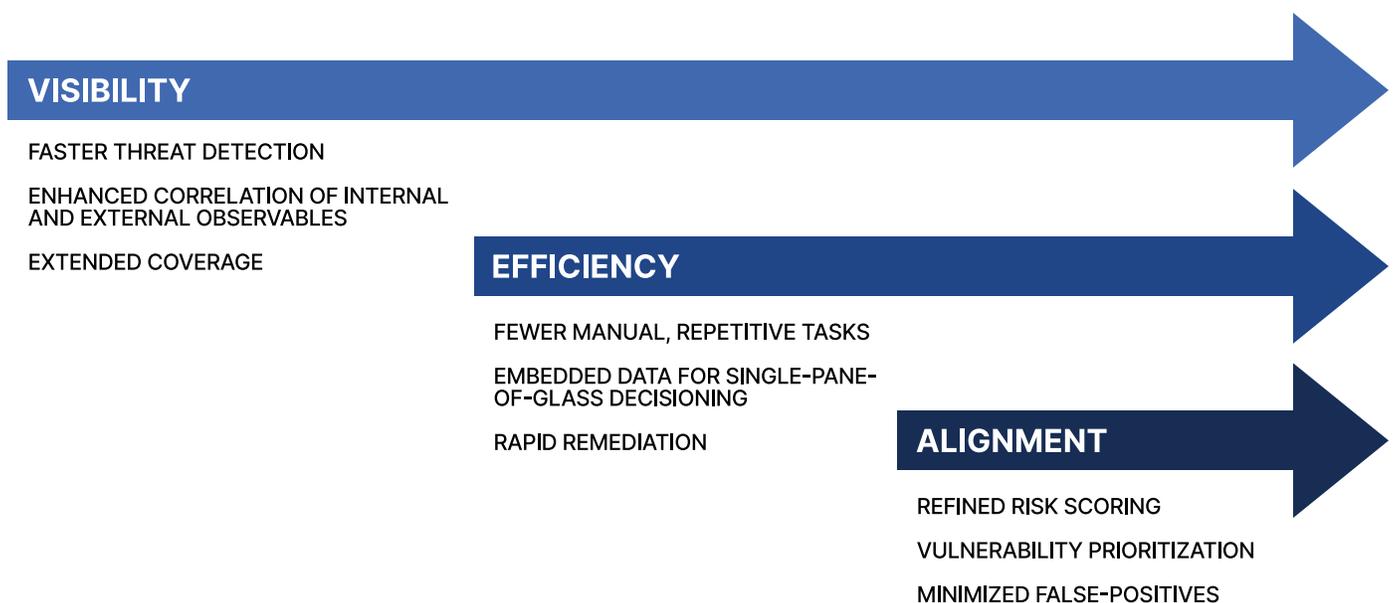
**Dynamic, 360-degree visibility.** Across [every security intelligence use case](#), visibility benefits are a constant. With a contextualized, real-time understanding of your internal and external threat environments, once-vulnerable blindspots become tactical advantages in your ongoing efforts to disrupt adversaries. Success hinges on the quality of the insight you generate — specifically its reach, speed, and relevance to the business — making security intelligence all the more important. With security intelligence powering your strategic initiatives, you will detect threats faster, develop a more intricate and actionable understanding of your threat environments, and better track your attack surface, overall.

**Operational efficiency, integration, and automation.** Security intelligence [integrates with your existing security technology stack](#) to reduce manual and resource-intensive processes. For example, rather than researching individual security events with information spread across multiple dashboards, Recorded Future's intelligence is easily inserted directly into your SIEM, or any security application (e.g., SOAR, NGFW, VRM, among others). Efficiency gains from technical integration and automation ultimately mean fewer tasks and [faster resolutions for your security operations team](#), intuitive decision-making, and standardized processes to expedite remediation.

**Business, risk, and stakeholder alignment.** Security intelligence ensures that your data and operational outputs are specifically tailored and relevant to you: Your organization, your people, your processes and procedures, and your assets, threats, and risk tolerance. Among the scores of metadata, security intelligence relies on three contextual lenses that appropriately set its scope and purpose:

- a) Links and associations to the business
- b) Threat and risk severity
- c) Stakeholder and functional relevance

When applied and analyzed from this perspective, security intelligence enables you to accurately assess and respond to risk, automatically prioritize CVEs based on threat severity, and filter out noisy threat feeds and hacker chatter to minimize false-positives and enrich more important investigation and response.



*Figure 1: Security Intelligence Converts Your Data Into Business Value*

# Supercharge Six Critical Security Solution Areas

Intelligence is no longer a side project or siloed within a threat intelligence team. [Security intelligence supports a wide range of roles and functions](#) across all security activities, including physical and information security, fraud, IT, risk, compliance, executive reporting, and more.

Given the diverse array of [security intelligence use-cases](#), you need to treat security intelligence not as one tool, but as a modularized solution capable of extending to distinct security activities. The core capabilities of each solution lay a common foundation for security intelligence, including the collection, analysis, scoring, automation, integration, and dashboards and reporting. Then, [solution-specific functionality augments the platform](#) and tailors it to the unique needs and activities of one or more distinct security areas. These modularized solutions are listed alphabetically here:

**Brand Intelligence Module.** From phishing attacks, to stolen PII, to fake mobile apps and social media accounts — how far does your attack surface extend and where has your data leaked? Brand intelligence equips organizations with [continuous visibility to monitor and detect](#) new cases of unsanctioned mentions, data leaks, and impersonations of your corporate brand. However, brand intelligence doesn't end at the detection of brand threats — it also streamlines the takedown and remediation steps on your behalf.

**Geopolitical Intelligence Module.** Discover how physical threats manifest, and often mirror, online threat activity. [Applying OSINT, geodata, and other location-based analytics](#), geopolitical intelligence acts as your eyes and ears online. It keeps watch of your physical assets and facilities, providing early signals of planned attacks, protests, acts of terror, and more. Geopolitical intelligence also serves as a physical protection layer, delivering real-time alerts about your physical assets when local and regional events may put them at risk.

**SecOps Intelligence Module.** Accelerate alert triage. Minimize false-positives. Automate response workflows. When you [advance security operations and incident response-related activities](#) with security intelligence in these three areas, you are all but guaranteed to uplevel your teams' outputs in significant ways. SecOps intelligence works across all three. Your teams work faster and more efficiently when equipped with the unique context and powerful analytics of security intelligence. Investigations are more comprehensive, so analysts spend less time on meaningless alerts and see even fewer false positives. SecOps intelligence also accelerates the response by automating the corresponding action, alerting, and orchestration to your connected systems and applications.

**Third-Party Intelligence Module.** Even the best, most-exhaustive vendor questionnaires and controls are not enough to [manage third-party risk](#) today. The data becomes obsolete after it's returned, and gaps in responses and evidentiary materials turn risk prioritization and heat map exercises into a game of darts. Third-party intelligence fills these gaps. It supplements what you know about your third-parties with deeper, primary-sourced data and risk analysis. With this information at your fingertips, you are empowered to make immediate, better-informed decisions about third-party risk and what to mitigate when it's needed — without waiting weeks for responses or guessing about whether the information is still correct.

**Threat Intelligence Module.** Security intelligence empowers [threat intelligence analysts](#) to focus on adversaries and the broader threat environment at large. When applied to the threat intelligence function, security intelligence uses [extensive collection and human and machine analysis of threat data](#) to generate valuable insights, which are used to:

- a) Understand the tactics, techniques, and procedures (TTPs) of various threat actors
- b) Determine attacker motives
- c) Track pertinent macro trends from various industry, region, and geopolitical vantage points

With these objectives in mind, threat intelligence further enhances threat analysis by adding crucial business and security context. As a result, threat analysts reduce time spent researching irrelevant threats and gain deeper, more detailed information on the events they do research.

**Vulnerability Intelligence Module.** An excruciating activity for security professionals, [vulnerability management](#) continues to hamper security efforts, as well as the IT teams who perform the actual patching. The crux of the issue is there are too many high and critical CVEs — but there is no risk contextualization for the specific organization and its IT environment. Vulnerability intelligence provides this vital context to CVEs, making it possible to assess how actively they're being exploited, and by whom. Armed with this information, security teams are able conduct more complete, risk-based prioritization of their CVEs — empowering them to address the vulnerabilities most gravely exposing the organization first.

## One Plus One Equals Three

It's important to note that all six security intelligence modules operate entirely independent of the other five. So, no matter which solutions you put into action, you get the same high-quality capabilities and alerts. Even better, when you extend security intelligence to additional solution areas, they feed into each other by sharing the data, context, and integration across multiple solutions.

Implementing additional solutions increases the value of your security intelligence exponentially. For instance, here's how you may find that your [third-party intelligence](#) solution augments the capabilities and insight provided by your [brand intelligence](#) activities: Let's say you're conducting a third-party risk review and you identify a particularly concerning risk event for one of your strategic partners. You discover that they had a data breach that could damage your company's reputation because the incident resulted in your partner leaking sensitive data that your customers entrusted to your organization. The complementary nature of the two security intelligence solutions adds value both as a discrete solution and as an aggregate, resulting in new economies of scale as it expands.

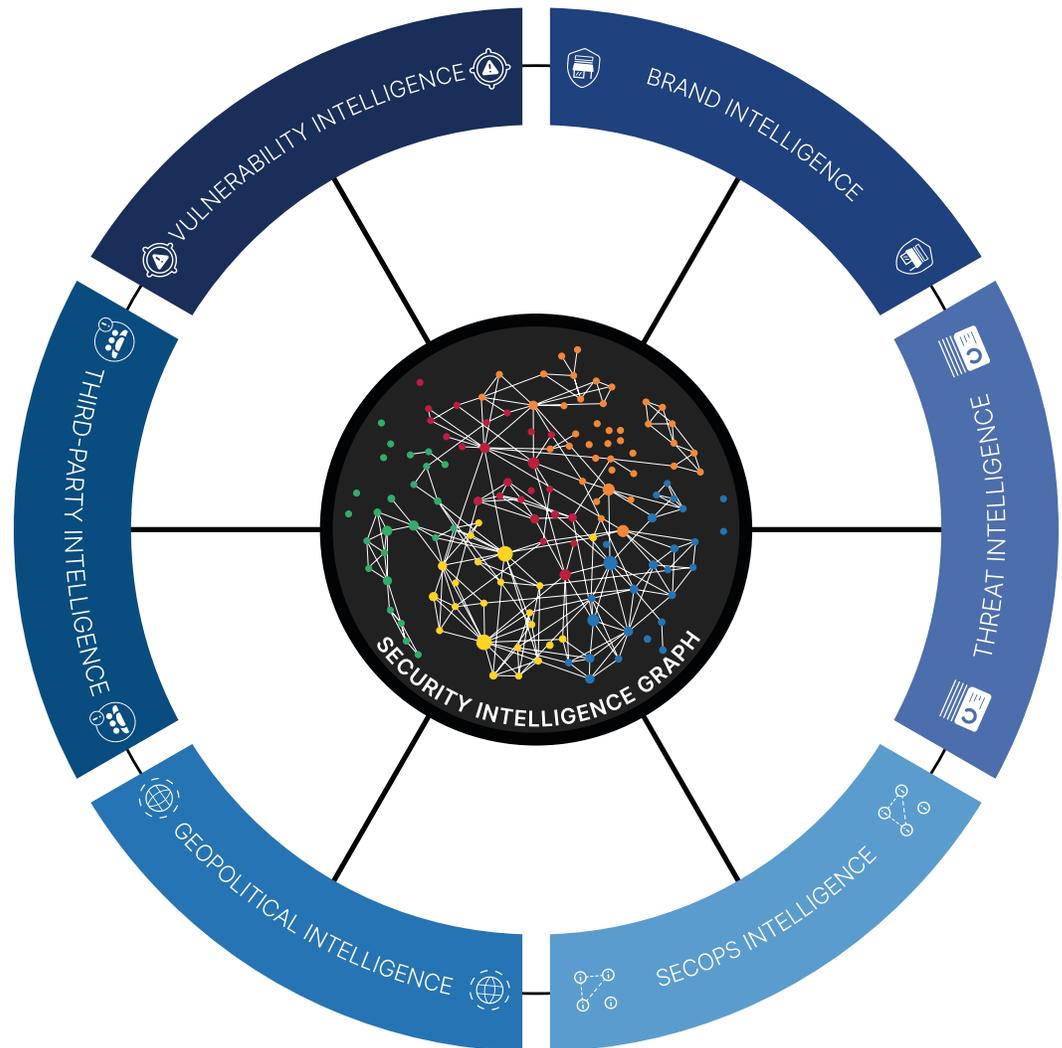


Figure 2: The Six Strategic Solution Areas of Security Intelligence

# Security Intelligence That Fits Your Organization

**Security intelligence easily scales up and down to match the size, maturity, and specific needs of any organization. Whether you're new to the technology and still identifying your goals, or you're a longstanding proponent with aggressive expansion plans, security intelligence adapts to your needs and priorities. [Recorded Future's modular security intelligence solutions](#) ensure it's easy to adopt additional solutions to adapt over time without arduous implementations or steep learning curves.**

## Think Big, Start Smart

Practically every security function is able to extract value from the exponential benefits and technical advantages of a robust security intelligence program. Take this into account as you determine your implementation strategy with clear priorities in mind and ideas for who will benefit the most right out of the gate. Six, 12, 18 months from now, how do you want your organization to be using security intelligence? What will it take to get there?

Starting smart is about beginning with purpose — not just speed — in mind. Whether you want to [implement a single security intelligence solution area or all six](#), the most successful organizations we work with begin in similar fashion — with a clear, concerted approach based on a set timeline. Adopt an agile mindset for both your security intelligence rollout and ongoing activities. Doing so will keep you dynamic and poised to shift as quickly as your adversaries.

## Advance When and How You Want

Since security intelligence is modular, your adoption of it can be too. For instance, maybe you're [using security intelligence to monitor the dark web](#) and you begin to realize the value it would bring as a correlation and enrichment source for your [incident response and security operations](#), as well. Within a short timeframe, you're able to have your [security intelligence inserted directly into your SIEM](#), to keep the bulk of your work on the analytics platform your team already knows inside and out. From that point on, it's up to you. With the flexibility Recorded Future enables, security intelligence quickly becomes an in-demand security capability across your security teams and your organization.

# Kick off With Quick Wins

Wherever you are in your [security intelligence journey](#), there are easy, practical steps that will ensure you get the most from security intelligence. When you begin your next security intelligence project, make sure you:

**Identify success metrics and reports early on.** Assign performance metrics for security intelligence prior to launching new capabilities. You may elect to benchmark your mean-time-to-remediate (MTTR) new threats, the number of alerts that are enhanced with intelligence, or how many feeds are being ingested. Alternatively, you could measure analyst efficiency. For example, one study shows that [Recorded Future improved customers' security workflows by 50%](#). If you expect similar efficiency gains given the size and scope of your [security intelligence and automation plans](#), you may want to track a similar percentage gain for your organization. As long as the metrics you set are based on realistic assumptions, you will have a valuable barometer to continuously mature your program over time.

**Recognize the ROI.** You will see nearly instantaneous returns on your initial investments into security intelligence. In fact, an independent analysis conducted by Forrester found that [Recorded Future customers have seen 328% ROI](#) on their security intelligence improvements. With a short, 3-month payback period and high ROI, articulating the [value in terms of business benefit](#) should help you gain internal buy-in.

**Identify opportunities with the security tools you already use.** [Integrating security intelligence into your existing technologies and applications](#) is an excellent first step. This minimizes the disruption to existing work streams and adds net-new capabilities that accelerate or enhance the outputs of the existing work being done. Recorded Future works with all of the leading [security technology providers](#) to offer quick, templated integrations for solutions in categories like SIEM, SOAR, IR, EDR, GRC, and many more. For even further integration and system customization, Recorded Future provides robust, bi-directional RESTful APIs to support your work the way you need it.

**Loop security intelligence back in for continuous feedback.** Insights from security intelligence [empower security decision-makers](#) with an unbiased lens into many facets of their operations and external threat environment. During your strategic planning, it's worth analyzing recent reports and detected events for emerging trends in attack vectors that may influence the projects and strategies you choose to prioritize.

## Reach Higher With Security Intelligence

Security intelligence is the cyber fuel you need to [power and propel your security forward](#). Use it to extend your visibility, to elevate your output, and to automate your response for any or all [six solution areas](#).

As you embed security intelligence more broadly throughout your organization, the returns you see will begin to grow exponentially within and across each solution. Whatever your priorities, security intelligence will evolve with them to amplify your risk reduction efforts and drive you — your team, your objectives, your business — to reach even higher echelons of performance and efficiency.



 [www.recordedfuture.com](http://www.recordedfuture.com)

 [@RecordedFuture](https://twitter.com/RecordedFuture)

### About Recorded Future

Recorded Future delivers the world's most technically advanced security intelligence to disrupt adversaries, empower defenders, and protect organizations. Recorded Future's proactive and predictive platform provides elite, context-rich, actionable intelligence in real time that's intuitive and ready for integration across the security ecosystem.

© Recorded Future, Inc. All rights reserved. All trademarks remain property of their respective owners.