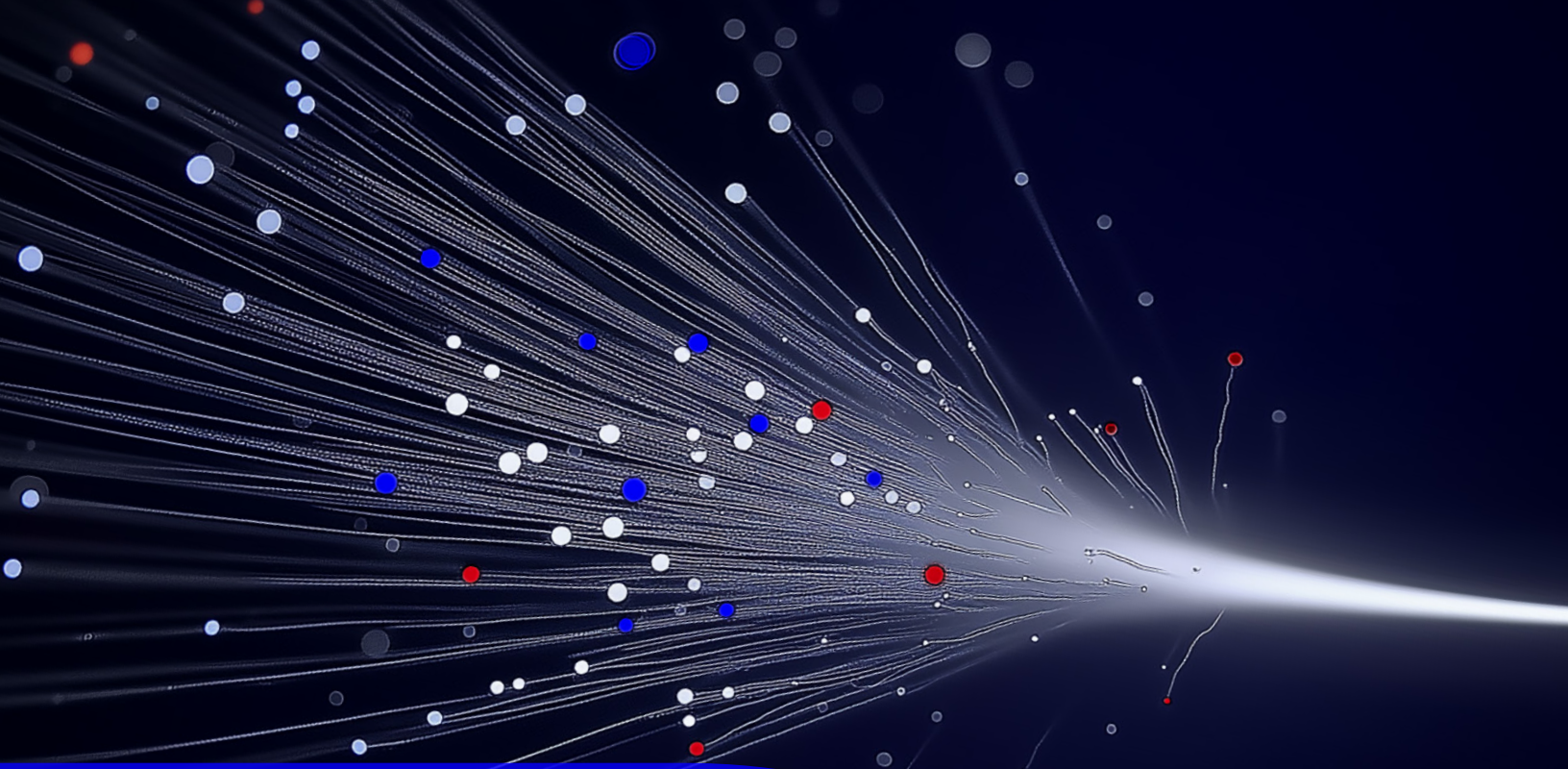


Recorded Future®

Reduce 27-step Threat Hunts to 5 Simple Steps.

Discover how to move from manual bottlenecks to 24/7 autonomous defense.

A Recorded Future eBook

FEBRUARY 2026

Manual security operations create a troubling gap.

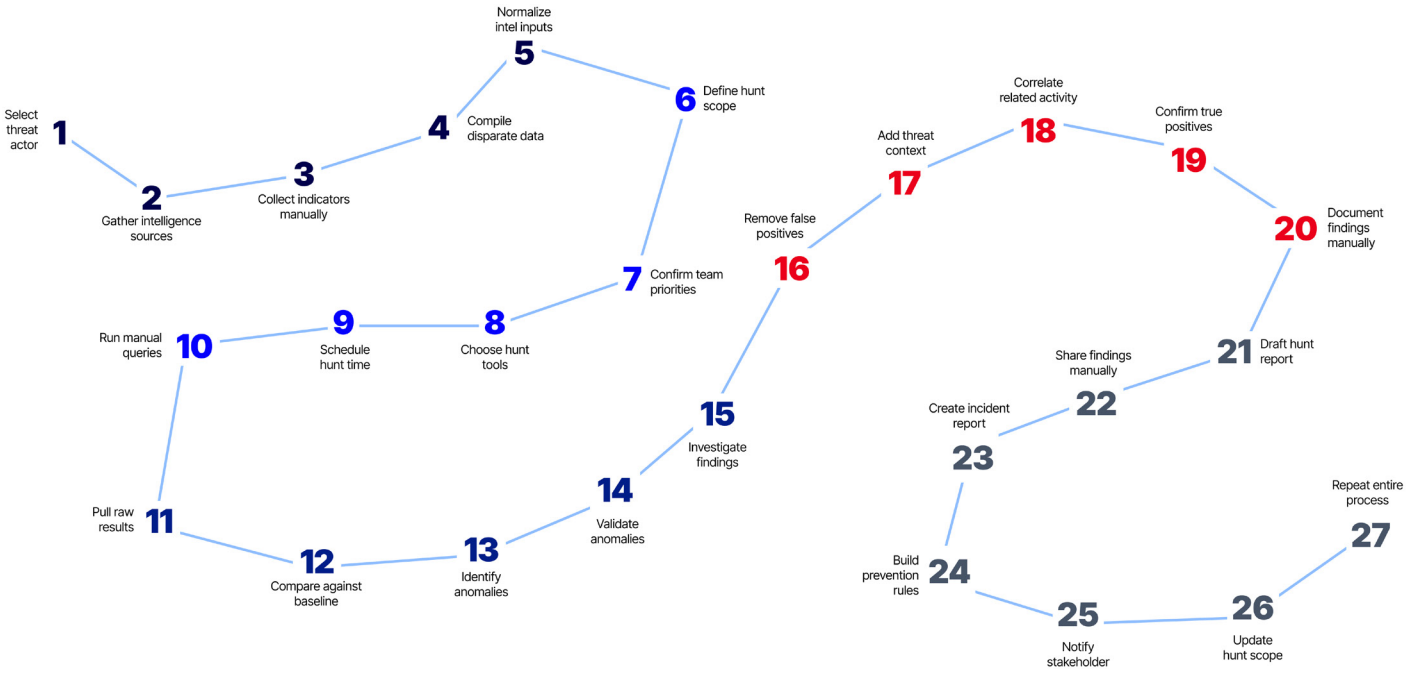
In organizations around the globe, threat hunting looks something like this: Every Monday morning, analysts kick off a new set of manual threat hunts, and they complete their investigation, review, and reporting processes on Friday afternoon.

Meanwhile, attackers who breached the network on Tuesday have already compromised your systems and moved on.

This is the manual operations gap, and it represents one of the most dangerous vulnerabilities in enterprise security today.

Today's manual threat hunting workflow

In most SOCs, threat hunting involves 27 separate steps.



With such a time-consuming and resource-intensive process, the question security leaders should be asking isn't whether their team is working hard enough. It's whether this manual workflow can ever keep up with the speed of today's threats.

THE RECORDED FUTURE ADVANTAGE

Cut 27 steps down to 5.

Given the manual operations gap, security teams need intelligence that doesn't just inform—it acts.

Recorded Future empowers teams to operationalize high-quality, organization-specific, prioritized, and continuously validated intelligence while minimizing false positives and reducing significant operational burden from their threat hunters in the trenches.

With new Autonomous Threat Operations, teams can reduce 27 steps to just 5:

1. Let intelligence drive your hunt.
2. Architect your hunt at scale.
3. Activate autonomous threat hunting.
4. Review correlated findings.
5. See the impact with AI Reporting.

Read on to walk through the five steps of autonomous threat hunting and see how this new workflow reduces manual bottlenecks and delivers the continuous coverage that modern threats demand.

STEP 1

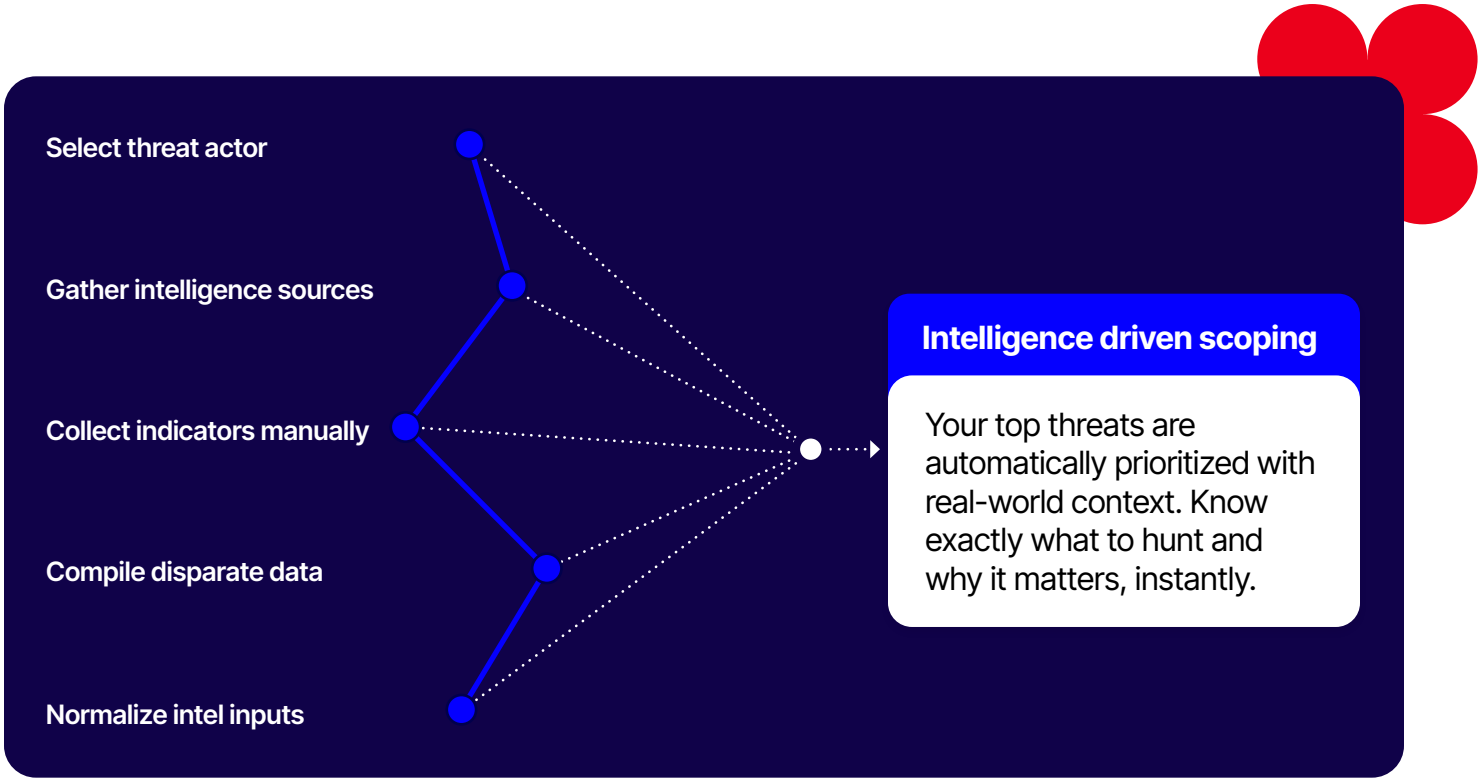
Let intelligence drive your hunt.

Instead of chasing down data, count on contextualized intelligence to show you the most relevant hunts to run.

Recorded Future offers two key capabilities that work together to keep your hunts aligned with your threat landscape in real time:

Threat Maps provide dynamic visualization of threat actors relevant to your organization based on your industry, geography, and technology stack. They automatically surface the actors most likely to target your environment, and they update continuously as the threat landscape evolves.

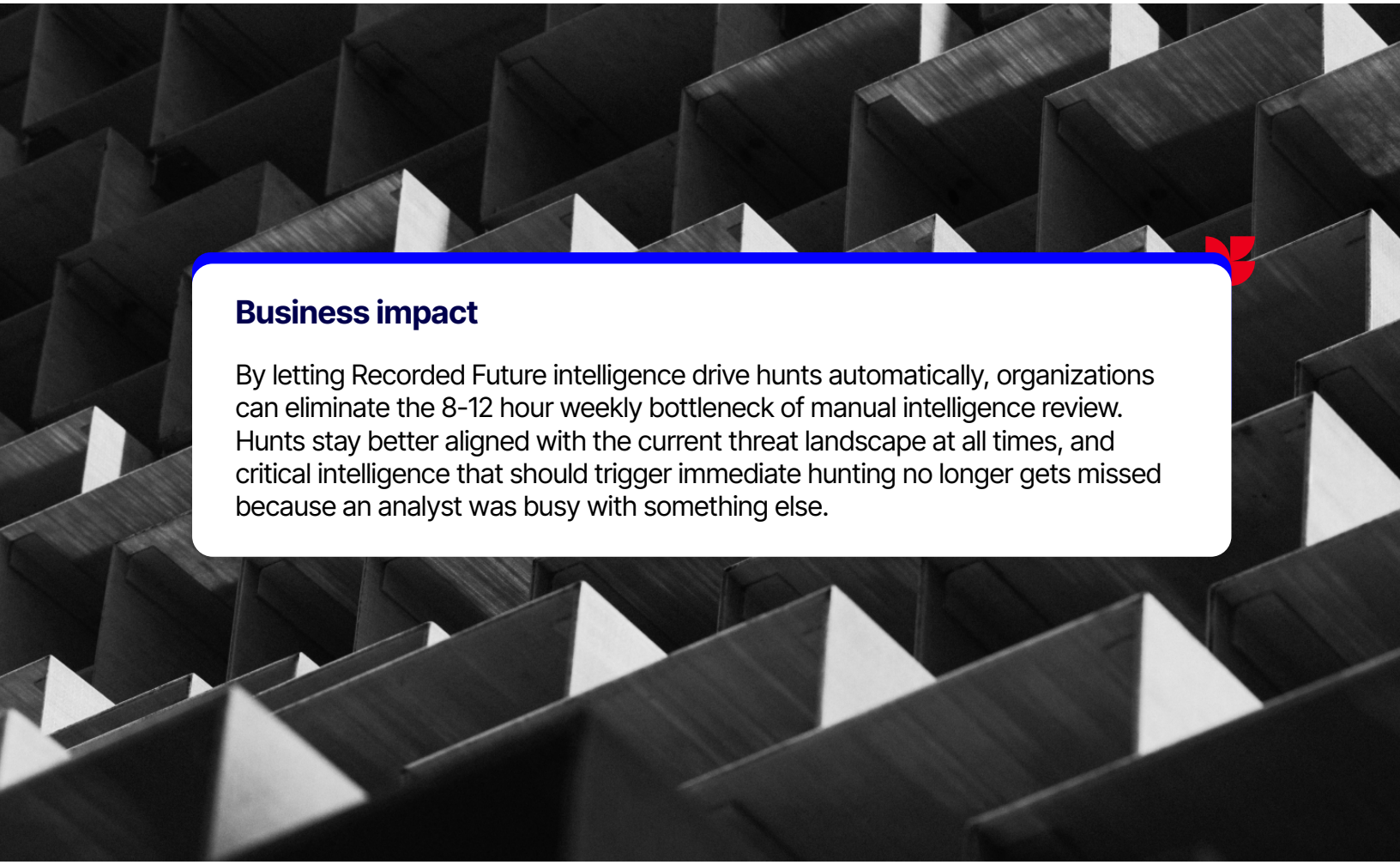
Threat intelligence from Insikt Group®, Recorded Future's elite research team, flows directly into Threat Maps and triggers hunt updates automatically.



How it works

Threat actors are automatically mapped to your organization's risk profile based on targeting patterns, capabilities, and intent. When new intelligence emerges—whether from Insikt Group research, third-party feeds, or the 1M+ sources automatically indexed by Recorded Future—it's contextualized and prioritized for you. That makes it fast and easy to determine what's most relevant so you know what to hunt.

Once hunts are running, they'll update dynamically in the Threat Map without analyst intervention.



Business impact

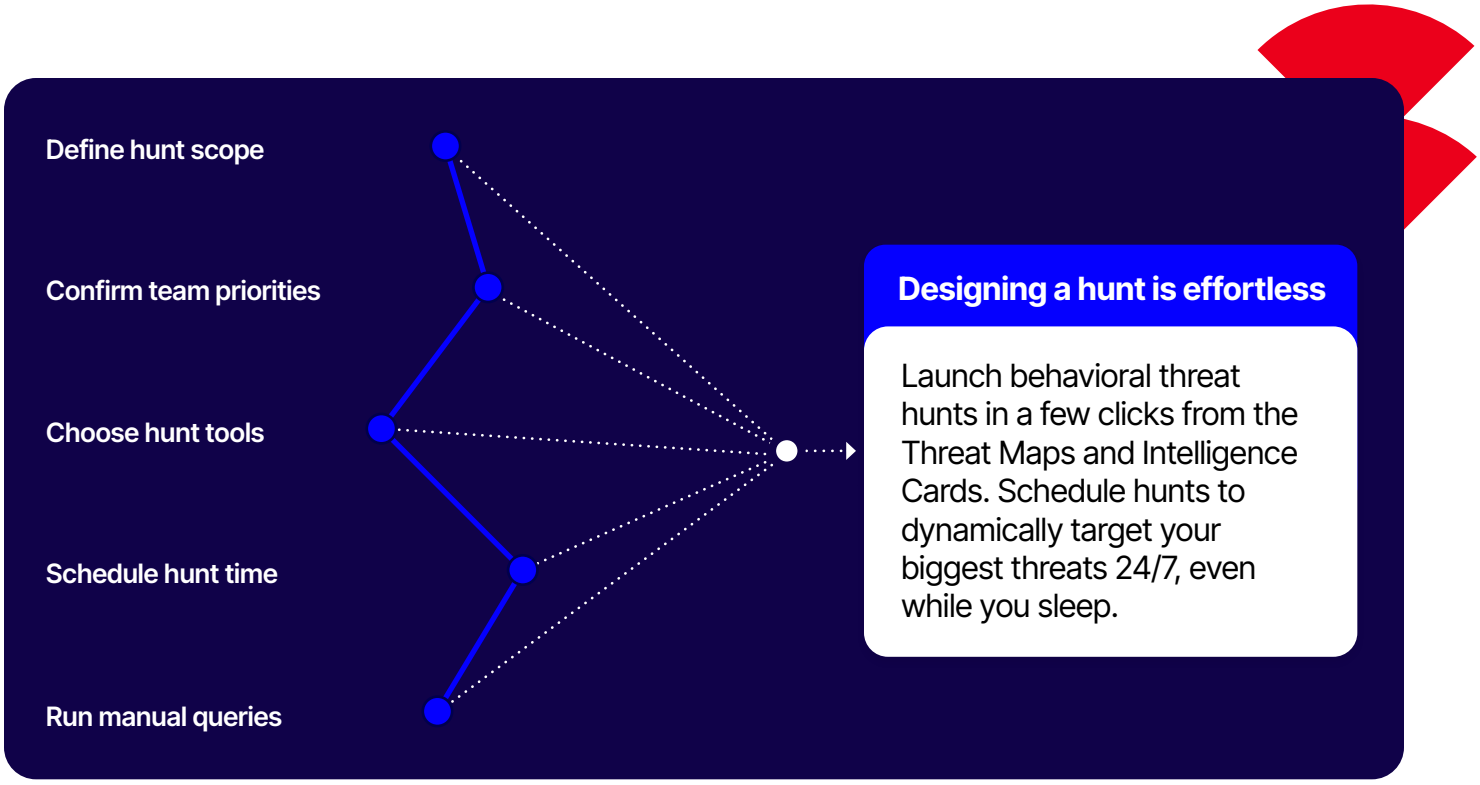
By letting Recorded Future intelligence drive hunts automatically, organizations can eliminate the 8-12 hour weekly bottleneck of manual intelligence review. Hunts stay better aligned with the current threat landscape at all times, and critical intelligence that should trigger immediate hunting no longer gets missed because an analyst was busy with something else.

STEP 2

Architect your hunt at scale.

Rather than logging into multiple tools, translating IOCs into different query languages, and running searches one platform at a time, design your hunt once and execute it everywhere.

Recorded Future centralizes hunt design and execution within a unified platform while maintaining deep integration with your existing security tools. You can seamlessly hunt across your tech stack, including your SIEM, SOAR, firewalls, and endpoint protection solutions.



How it works

Initiate hunts from almost anywhere, including:

Threat Map

Start hunts based on threat actors targeting your sector, with relevant IOCs, TTPs, and detection rules pre-loaded.

Malware Map

Hunt for specific malware families, including associated infrastructure and behavioral indicators.

Intelligence Cards

Dive deep into specific IOCs, malware variants, or threat actors with one-click hunt initiation.

Insikt Group Notes

Convert research findings directly into active hunts, ensuring that new intelligence translates immediately into defensive action.

Autonomous Threat Operations Homepage

Get visibility into all active hunts across your environment and hunt configuration.

Hunt across many tools at once

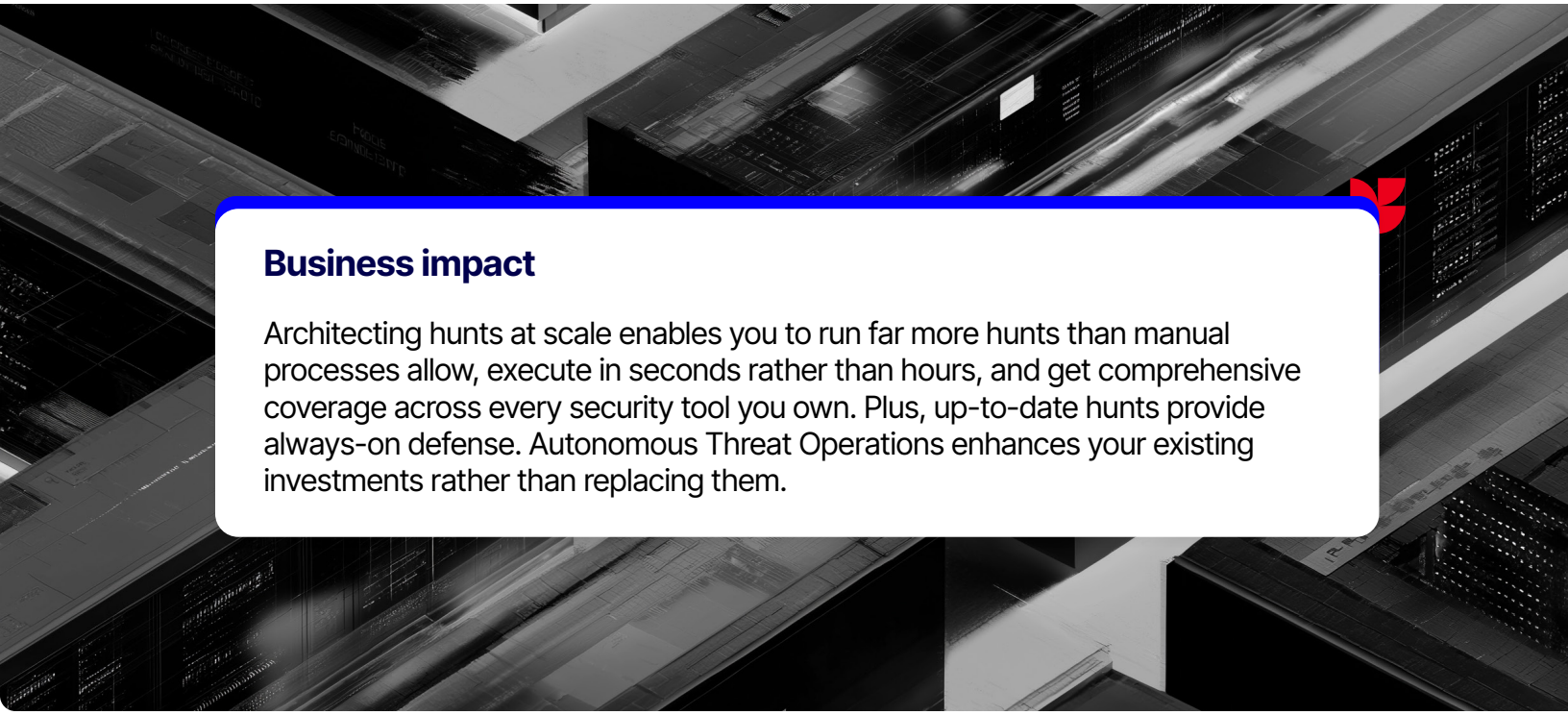
Autonomous Threat Operations ingests intelligence from across your ecosystem—ISAC feeds, 1M+ Recorded Future sources, and your own internal sources—and then enriches and prioritizes it within the Intelligence Graph®, which contains over 200 billion nodes of threat data.

When you launch a hunt, it executes across your connected tools simultaneously. Current integrations include Splunk, CrowdStrike Falcon XDR, CrowdStrike NG-SIEM, Google SecOps, SentinelOne, Zscaler ZIA, Microsoft Unified SecOps, and Palo Alto Networks Panorama—and more are added all the time.

This means a single hunt for a threat actor's infrastructure can query your SIEM logs, endpoint telemetry, network traffic, and cloud environments in one operation. No context-switching, no manual correlation, and no tools left unchecked.

Automatically stay up to date

When intelligence changes, your hunts update automatically. External intelligence merges with your internal data into a closed-loop system that strengthens prevention and detection at every signal, and a single interface lets you manage hunts across your entire security stack.



Business impact

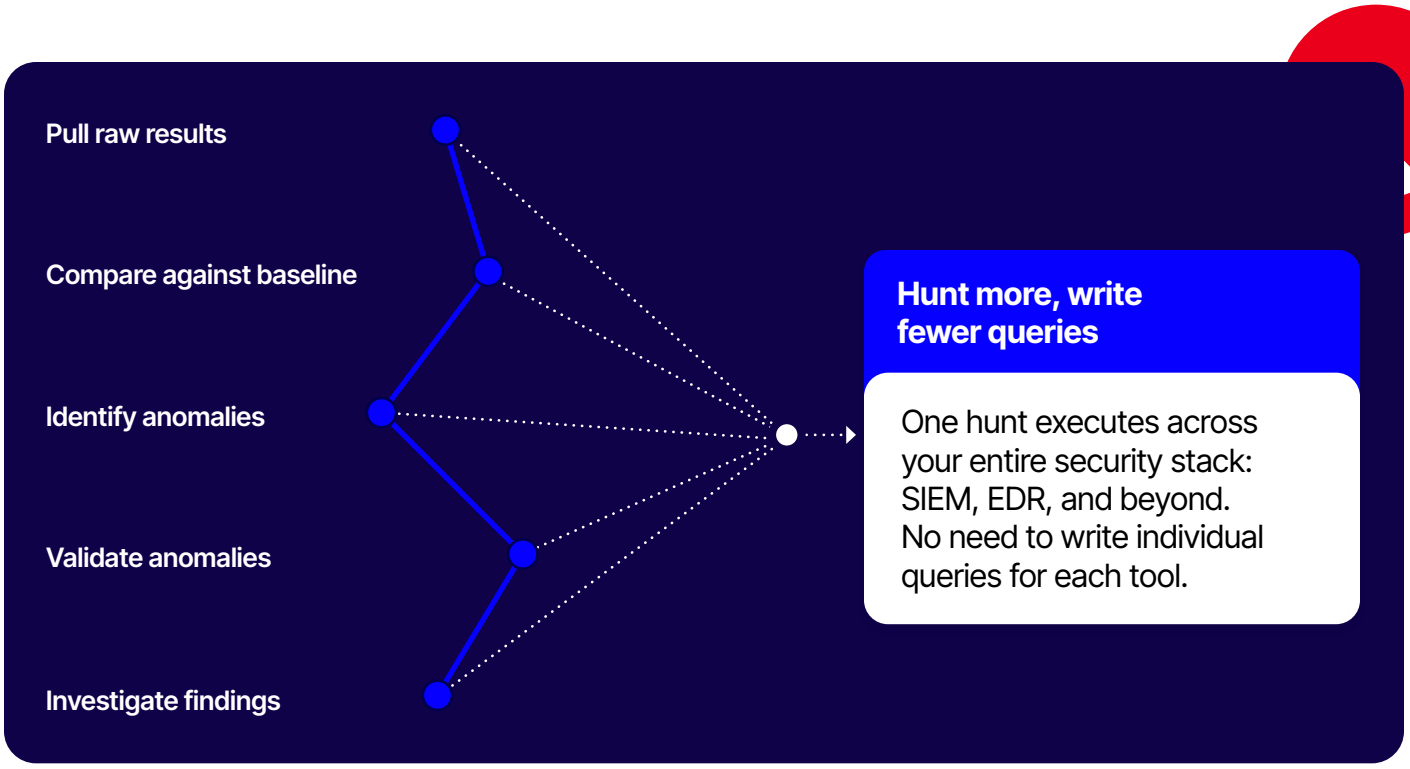
Architecting hunts at scale enables you to run far more hunts than manual processes allow, execute in seconds rather than hours, and get comprehensive coverage across every security tool you own. Plus, up-to-date hunts provide always-on defense. Autonomous Threat Operations enhances your existing investments rather than replacing them.

STEP 3

Activate autonomous threat hunting.

Since even well-resourced security teams can only hunt during working hours, continuous and autonomous defense is the way forward.

Once configured, Recorded Future's Autonomous Threat Operations lets you launch ad-hoc hunts on emerging campaigns in minutes, or schedule dynamic hunts targeting your highest-priority threat actors. And it can operate 24/7 without human intervention—not because it follows rigid schedules, but because it adapts autonomously to the threat landscape.



How it works

It hunts while you sleep.

Set up a recurring hunt to happen at night when there's less business activity in security tools, and your findings will await your review when you start work.

It offers 24/7 autonomous coverage.

Hunts execute around the clock, matching the velocity of modern attacks.

It adapts autonomously.

Unlike automated systems that follow pre-programmed rules, autonomous systems work independently using AI, adapting to new intelligence and making decisions with minimal human intervention. When a new threat emerges at midnight, autonomous hunting can respond immediately.

It offers prevention at scale.

Get unified threat protection across all your security controls, with blocks and detections automatically pushed to firewalls, EDRs, SIEMs, and web proxies. Prevention policies enforce consistently without manual intervention.

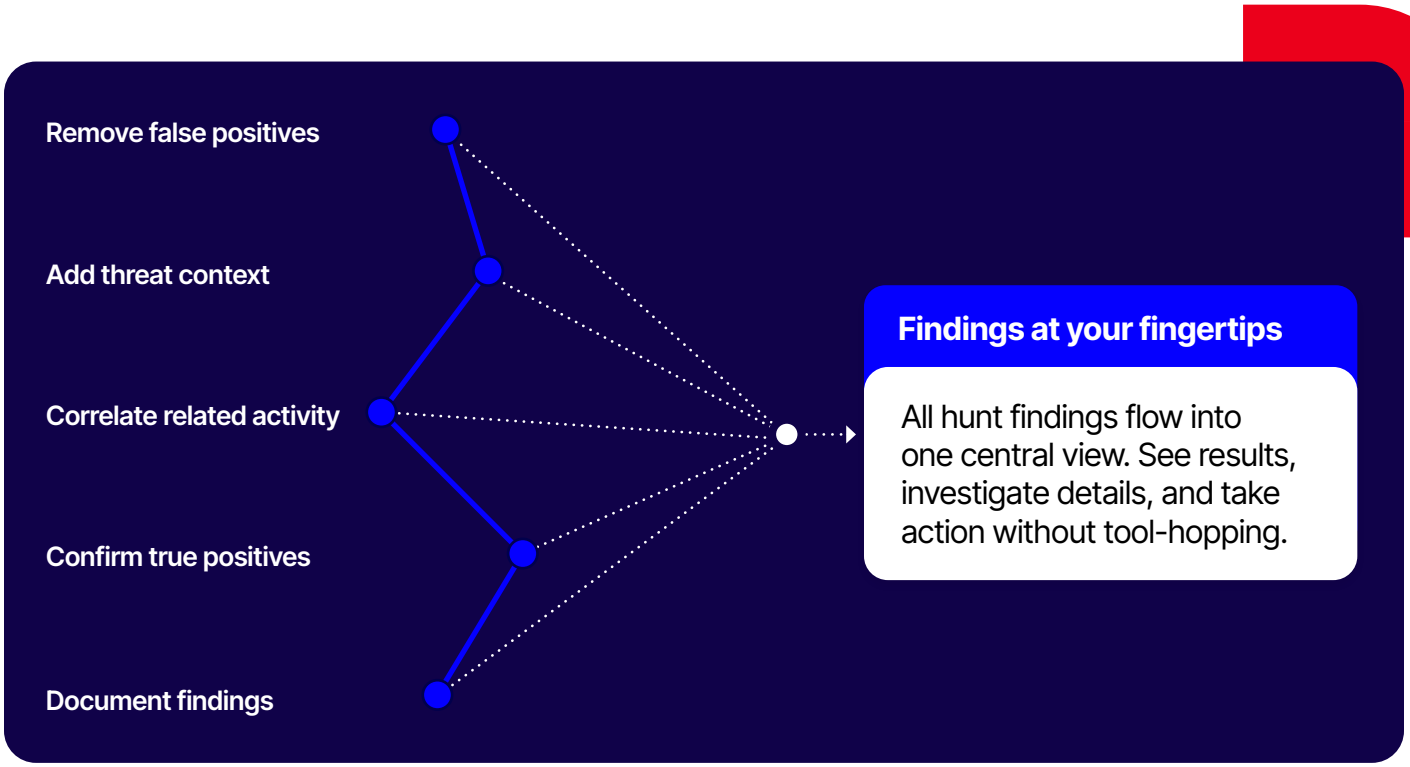
Business impact

Continuous monitoring delivers what manual processes never could: true 24/7 coverage. Organizations using Recorded Future can identify new threats 65% faster and save over 100 hours per week, per team (~$290K annually), as detailed in our ROI Report.

STEP 4

Review correlated findings.

No need to manually put findings in a usable format, clean up false positives, and correlate results across tools. Recorded Future's Autonomous Threat Operations delivers consolidated, correlated findings that are ready for action.



How it works

Single-location visibility

eliminates the need to go into multiple tools. View results in the Recorded Future Platform to quickly see hunt findings and identify and remove false positives.

Historical context

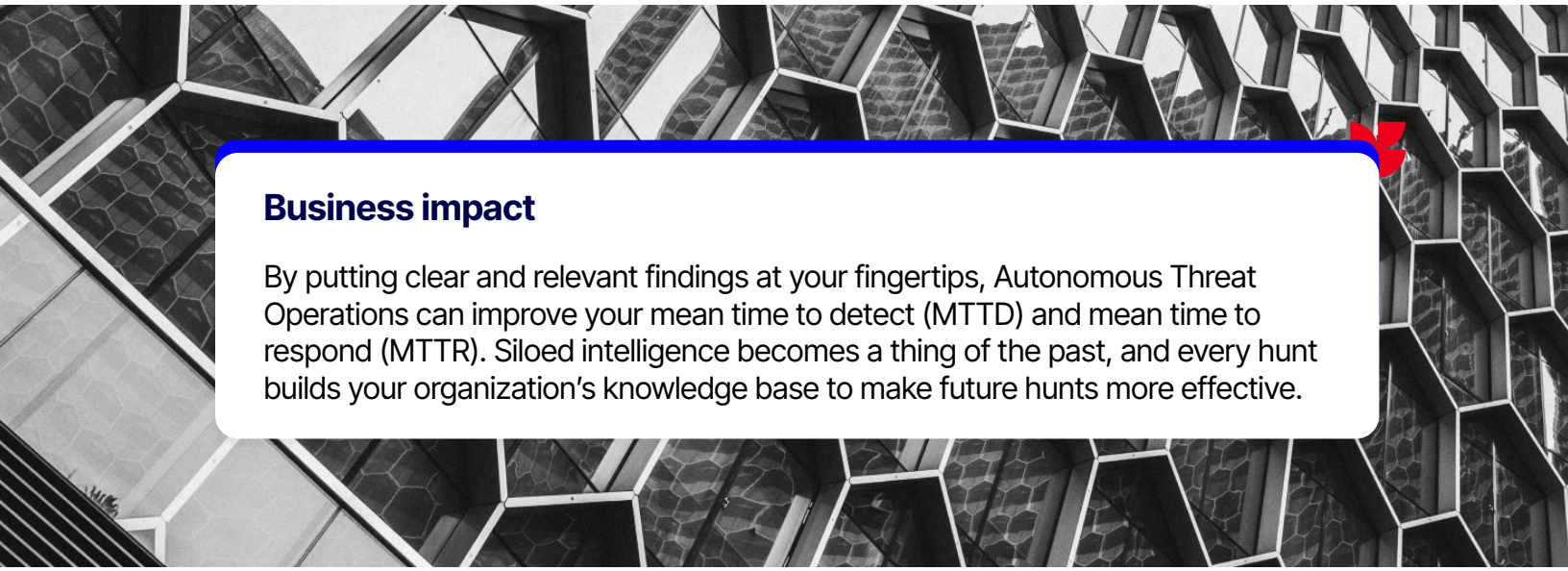
from the Intelligence Graph® shows whether an indicator appeared in previous campaigns, which threat actors have used similar infrastructure, and how the threat has evolved over time.

Automatic enrichment

adds context the moment findings are identified. Every result correlates automatically with the Intelligence Graph®, connecting IOCs to known threat actors, active campaigns, and documented TTPs. Risk Scores reflect relevance to your specific environment, not generic severity ratings.

A collective defense model

means that threat patterns identified across Recorded Future's customer base inform the intelligence that drives your hunts. You benefit from those global insights, while source attribution ensures that you maintain full control over your own data.



Business impact

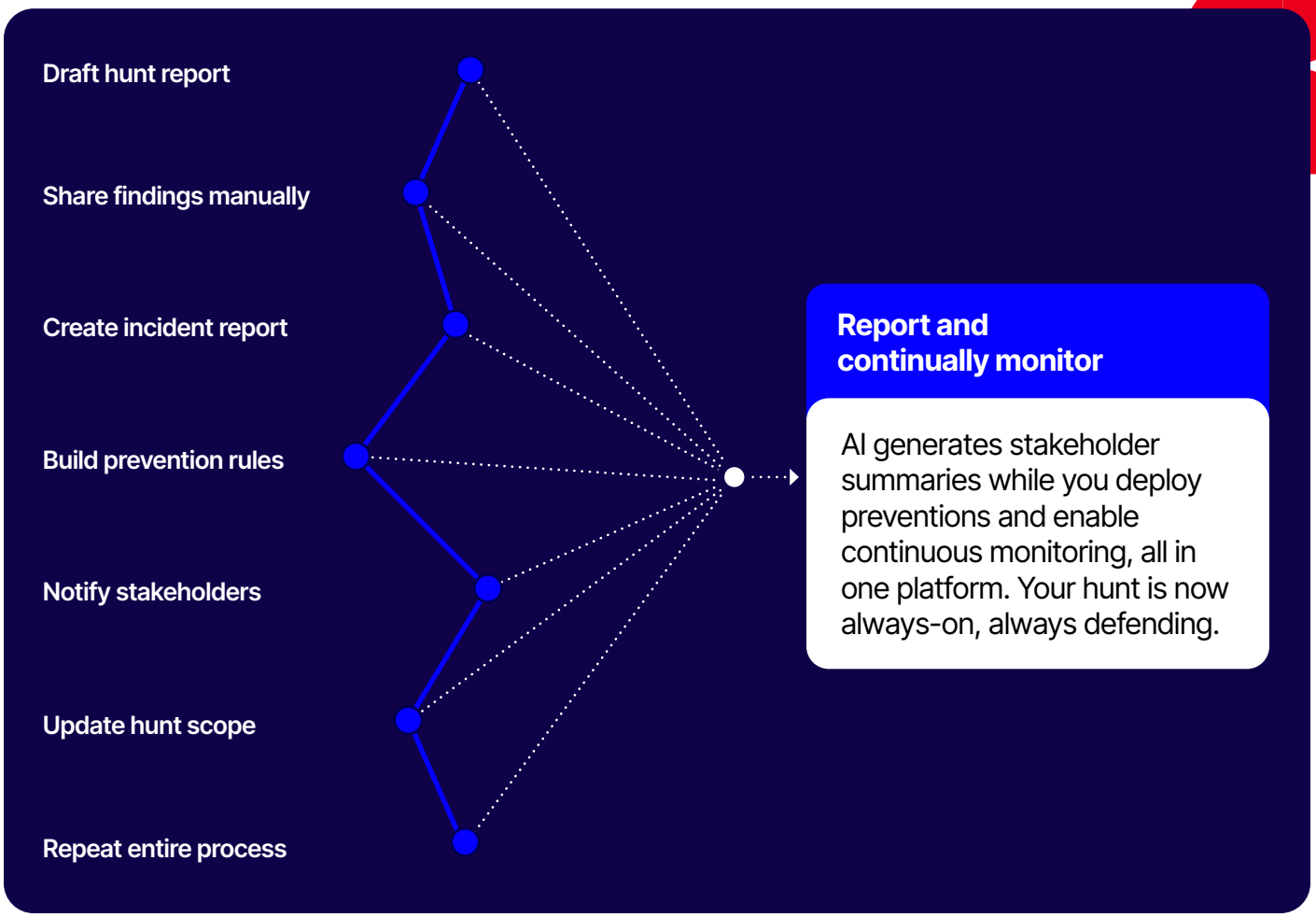
By putting clear and relevant findings at your fingertips, Autonomous Threat Operations can improve your mean time to detect (MTTD) and mean time to respond (MTTR). Siloed intelligence becomes a thing of the past, and every hunt builds your organization's knowledge base to make future hunts more effective.

STEP 5

See the impact with AI Reporting.

Finally, you need an efficient way to connect hunting activity to business impact.

Recorded Future uses AI to automate the entire reporting workflow, making it easy for you to earn trust by showing proven security outcomes and demonstrating consistent threat prevention.



How it works

Automated report generation

produces summaries of top findings and actions taken with a single click. AI-powered analysis identifies the most significant results, threat actors, and business risks. Custom templates let you tailor reports for different audiences, such as technical detail for SOC teams and strategic summaries for the board.

Measurable intelligence ROI

is revealed, with AI Reporting tracking every prevented incident, documenting blocked threats and the intelligence that identified them, and calculating tangible ROI. When the CFO asks what the threat intelligence budget actually delivered, you can report the number of threat hunts conducted, active threats identified, malicious indicators blocked, and estimated cost savings through the prevention of potential breaches.

Executive-ready insights

translate technical hunting activity into business terms. Board-level summaries show threat landscape evolution and organizational defense posture. Trend analysis demonstrates improvement over time. And auditors can use documentation to confirm continuous monitoring activities.

Business impact

Organizations using AI Reporting demonstrate 350% ROI on intelligence investments and 57% reduction in overall cyber risk. Security leaders can justify investments with concrete metrics rather than activity reports, transforming threat intelligence from a cost center into a measurable risk-reduction function.

Enter the era of the autonomous SOC.

The shift from manual to autonomous operations isn't about replacing human expertise; it's about removing the manual processes that prevent that expertise from scaling and delivering real business impact.

In an autonomous SOC, you can transform your security economics to:

1.

Force-multiply your team.

One analyst can accomplish what previously required a team, and enable everyone to focus on more strategic investigations and other priorities.

2.

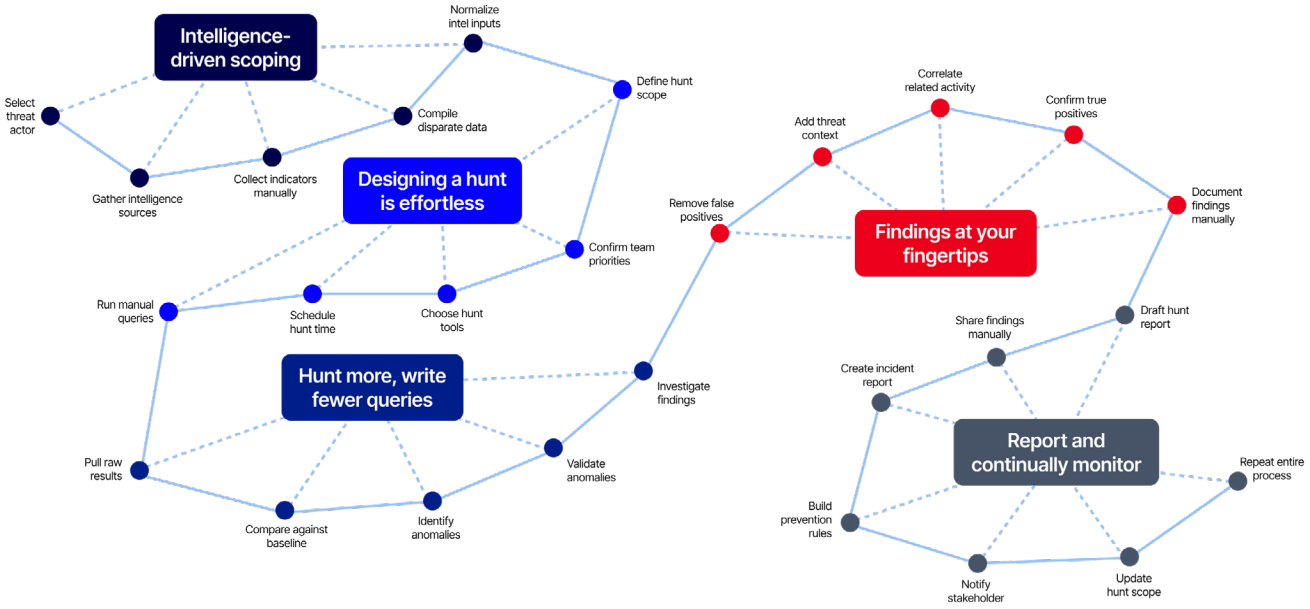
Prove intelligence value.

Track every prevented incident, blocked threat, and avoided incident to show the board exactly what you've stopped and why it matters.

3.

Maximize existing investments.

No rip-and-replace. Your current tools become more effective when they work together autonomously.



Defend at machine speed with Autonomous Threat Operations.

Recorded Future's Autonomous Threat Operations represents a fundamental shift in how organizations defend against threats.

Rather than today's reality of:

- **Manually** hunting threats across tools
- Spending **hours** correlating data from silos
- Responding **reactively** after detection
- **Updating** blocklists by tool

Autonomous Threat Operations offers tomorrow's advantage, with:

- **Autonomous**, 24/7 threat hunting
- **Instant**, multi-source data ingestion and correlation
- Predictive defense **before impact**
- Automated and measurable **prevention** across security tools

It's one platform for every tool and every threat. Unlike other solutions, it orchestrates your entire security stack—SIEM, EDR, SOAR, and more—to turn disparate tools into a unified, autonomous defense system.

Getting started.

The path from manual bottlenecks to autonomous defense is clear. Ready to see Autonomous Threat Operations in action?

Book a customized demo

Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining Intelligence Graph®-powered AI with the world's largest collection of specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact business.

Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.