

Cyber Operations

Anticipate, prevent, and disrupt threats proactively. Hunt, detect, and respond autonomously.



Challenge

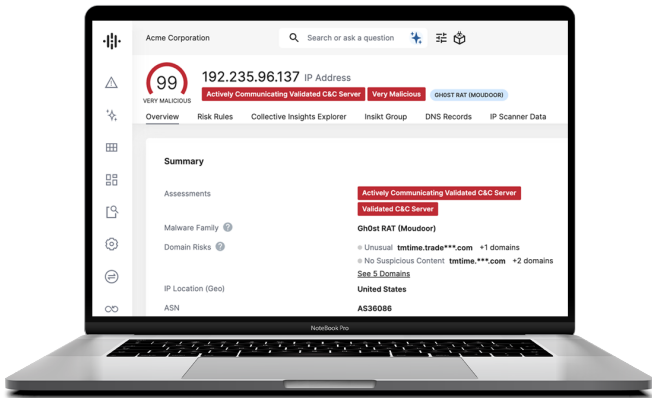
CTI, SOC, and Vulnerability teams are under pressure to stay ahead of adversaries who are faster, better resourced, and growing more sophisticated every day. Most teams are stuck reacting — spending hours manually correlating data per incident, running scheduled threat hunts long after adversaries have moved, and working through endless vulnerability backlogs without the context to know what’s actually being exploited right now. Let’s change that.

Solution

Recorded Future Cyber Operations brings together actionable intelligence, threat intelligence workflows, and autonomous capabilities that allow security teams to move from reactive to proactive defense. It provides threat visibility, alert triage, vulnerability prioritization, and autonomous response at machine speed — all powered by the Intelligence Graph® and integrated with your SIEM, EDR, and SOAR platforms.

What Your Team Can Do with Cyber Operations

| Benefits | Our Advantage |
|--|---|
| <p>See and Prioritize Threats</p> <p>Real-time monitoring across 200+ Network Intelligence points of presence</p> | <ul style="list-style-type: none"> • Surface threats that matter with Threat Maps tailored to you • Prioritize vulnerability patching based on exploitation data and ransomware activity • Generate detailed threat reports in minutes to keep stakeholders intelligence-led |
| <p>Investigate and Analyze</p> <p>Predict what comes next with MITRE ATT&CK mapping, natural language search, and a high-volume sandbox</p> | <ul style="list-style-type: none"> • Analyze 1.5M+ daily malware samples to see how malware actually operates • Map 350+ malware families at the sub-procedure level with MITRE ATT&CK mapping • Deploy detections faster with Insikt Group® finished intelligence and pre-written YARA, Snort, and Sigma rules |
| <p>Detect and Prevent</p> <p>Stop adversaries proactively from their objectives with intelligence and integrations</p> | <ul style="list-style-type: none"> • Correlate detections across your security stack automatically with Collective Insights® • Enrich telemetry with automatic TTP, malware, and threat actor tagging • Get real-time alerts on new exploits, malware, and campaigns targeting your industry |
| <p>Respond and Remediate</p> <p>Intelligence that enables you to act confidently and swiftly</p> | <ul style="list-style-type: none"> • Cut false positives with Risk Scores and Intelligence Cards® consolidating all IOC context • Auto-enrich alerts across your SIEM, SOAR, and EDR/XDR without leaving existing workflows • Understand adversary tactics and infrastructure for rapid, targeted remediation |



Autonomous Threat Operations Always-on defense that moves at machine speed.

When paired with Cyber Operations, intelligence-led autonomous threat operations execute hunting, detection, and response continuously, with minimal human intervention and your team in full control.

Hunt While You Sleep. Autonomously hunt threats across your entire security stack with built-in guidance for IoCs, malware, and threat actor TTPs, that dynamically updates to the changing threat priorities

Intelligence Everywhere. Continuously push validated threat indicators to all security controls, updating blocklists across every tool instantly

All Your Sources, All Together. Unify threat analysis across Intelligence Graph® data, ISACs, and third-party feeds through multi-source ingestion and correlation

Integrations with Intelligence

When intelligence lives inside the tools your team is already using, every decision the SOC and business makes becomes an intelligence-driven one. Recorded Future connects with your SIEM, EDR, SOAR, and vulnerability management platforms through bi-directional integrations, connectors, and APIs.



The outcomes of intelligence-driven security

| | |
|--|---|
| Increased Threat Visibility | 73% average increase in visibility into potential threats by using Recorded Future |
| Reduced Time to Awareness | 65% average increase users report in speed to identify a new threat compared to prior to using Recorded Future |
| Reduced Time to Action & Response | 32% average time savings in alert triage, investigation, and response efforts with Recorded Future (equates to 1.5x faster) |
| Reduced Security Workload & Low-Value Activity | 43% average increase in security team's capacity when using Recorded Future (equates to 1.4x team capacity) |
| Improved Defensive Alignment & Risk Posture | 64% of users say their team now has a significantly better understanding of their organization's threat landscape by using Recorded Future |

*Source User Evidence

“
Tasks that previously relied on the judgment of security experts have been automated, dramatically improving threat analysis times.”
Masato Kagotani
Director of Security Operations Division,
Panasonic Holdings Corporation

See Cyber Operations in Action

[Request a demo](#) to learn how to proactively defend and act against threats like never before with Cyber Operations.