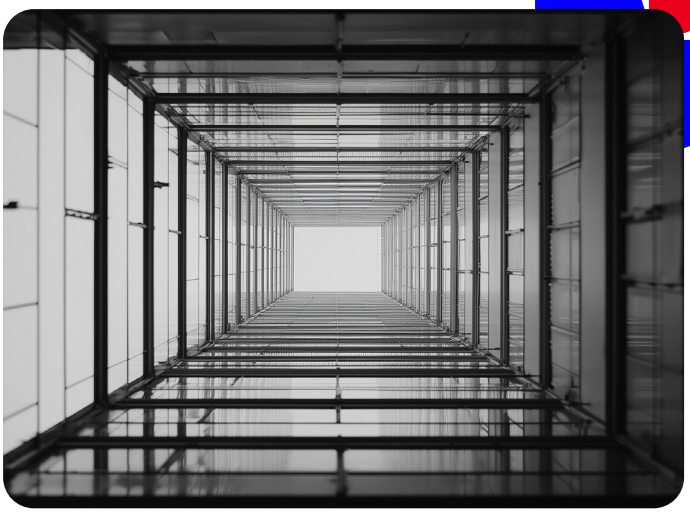
Recorded Future® | DATA SHEET

Collective Insights®

Powered by the Intelligence Cloud

Your entire environment gets smarter the moment you connect. **Included in your Threat Intelligence or SecOps license. No additional cost.**



What Is Collective Insights®?

Recorded Future Collective Insights® bridges the gap between what is happening inside your network and what is happening outside in the wild. By connecting telemetry from your existing security controls (SIEM, EDR, SOAR, email security, and more), we transform raw detection data into a proactive defense strategy.

The result: a holistic, organization-specific view of your threat landscape, enriched with the world's best external threat intelligence and community insights, all presented in one consolidated view.

How It Works

Collective Insights® ingests security events from your existing tools, normalizes them, and enriches each detection with Recorded Future intelligence. The more integrations you connect, the more precise your threat landscape becomes.

What gets smarter the moment you connect your telemetry:

- Threat Maps and Intelligence Cards are automatically enriched with your organization-specific sightings.
- Recorded Future AI generates custom reports from your enriched detection data.
- The Threat Detection Dashboard becomes your single source of truth for relevant threats.
- MITRE ATT&CK heatmaps are automatically built and updated over time.

Insight. Validation. Foresight.

Three capabilities that turn fragmented intelligence into decisive action.

INSIGHT
Prioritize what matters

Connect your internal telemetry to Recorded Future's real time intelligence to see the malware, actors, and techniques behind your detections and find the needle in the haystack.

VALIDATION
Validate your defenses

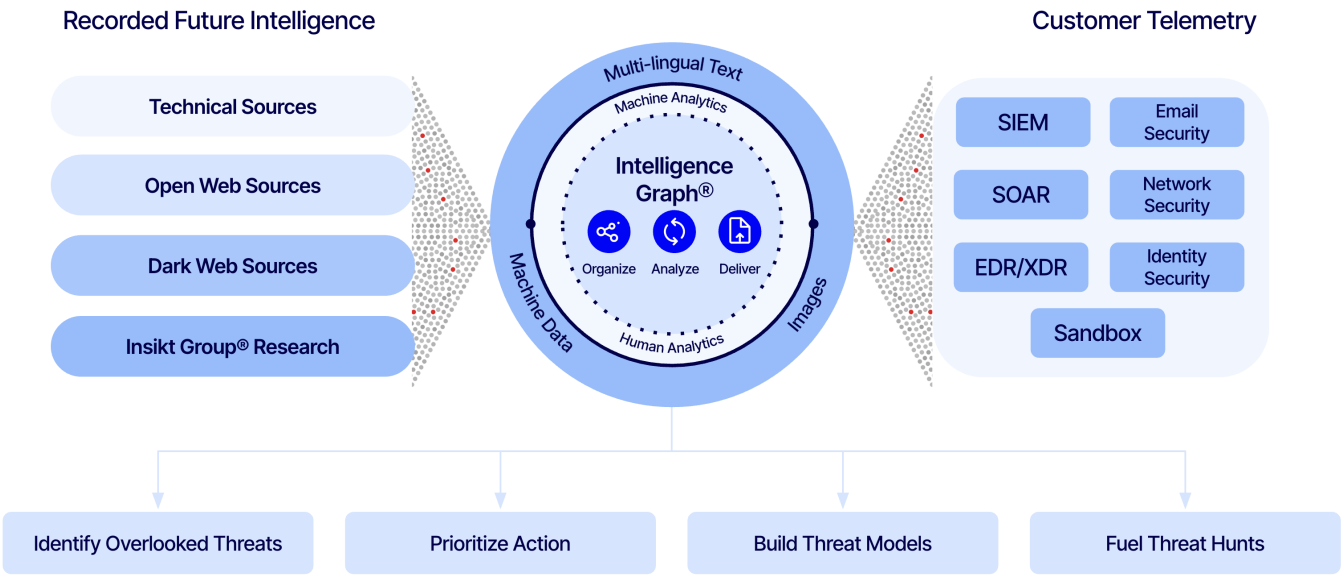
Automatically map your detections to the MITRE ATT&CK framework to see exactly where you are protected and where gaps remain. Prove the ROI of your security stack.

FORESIGHT
Stay ahead of attacks

Compare your threat landscape to industry peers to identify trending attacks before they reach your perimeter. Deploy YARA, SIGMA, or Snort rules proactively.

Privacy by Design

Collective Insights® is built on a zero-leak architecture. No PII ever leaves your control. Threat sightings are shared non-attributably within the community. Your organization's identity is never exposed to other customers or third parties. ISO 27701 and SOC2 compliant.



Key Capabilities

Identify overlooked threats

Visualize security events to spot threats your native tools miss, and identify deviations from baseline behavior.

Prioritize action

Get a second opinion on low-severity detections. Identify new malware and use quick reporting tools to act with confidence.

Inform threat hunts

Hunt related threats using automated playbooks, detection rules, TTPs, and intelligence context.

Build threat models

Automatically tag security events and map them to the MITRE ATT&CK framework to build a more resilient organization over time.

Discover how Recorded Future clients are using Collective Insights® today.

Gain a comprehensive view

The security team appreciated how easy it was to set up Collective Insights® with CrowdStrike, and they find the data to be highly useful. They reported that Collective Insights® is the only place their analysts can go to see MITRE ATT&CK data compiled for both their Splunk and CrowdStrike environments in one place.

Identify overlooked threats

Collective Insights® capabilities are used to normalize detections across their security tools, including ProofPoint. Recently when using the visualizations on the Threat Detection Dashboard, the security team noticed a large spike in hash values coming from ProofPoint and were able to identify over 4,000 emails related to a phishing campaign. Armed with this information, they were able to use the sandbox to validate.

Augment internal playbooks

The security team uses information from the Threat Detection Dashboard to prioritize their responses based on severity. The team also uses Recorded Future's recommended actions in their existing internal playbooks.