Recorded Future® | DATA SHEET

SecOps Intelligence Module

Speed up alert triage with intelligence that's built for security workflows

Challenge

The ever-growing number and dynamic nature of threats are causing security operations teams to see more alerts each day. Researching thousands of raw data points is often a manual and human-constrained process, overwhelming for even the most seasoned security analyst. With too little time and lacking sufficient context within their security tools, it's difficult to determine which alert represents a critical incident and which may just be a redundancy or a false positive, while true positives may be slipping through the cracks. Too many alerts, a lack of resources, and limited context leave security operations teams burnt out and overwhelmed.

Solution

The Recorded Future SecOps Intelligence Module empowers security operations teams to confidently prioritize and resolve alerts, detect previously undetected threats, and block threats while avoiding business disruption. Engineered to integrate with existing security workflows and tools, the SecOps Intelligence Module puts comprehensive intelligence at an analyst's fingertips without adding needless complexity.

Recorded Future automates the collection, analysis, and production of intelligence from an unrivaled range of open source, dark web, and technical sources, and then combines it with world-class research to drive accelerated responses. With the Recorded Future SecOps Intelligence Module, users gain access to ready-to-use data sets of high-risk indicators that empower analysts to identify threats before they impact the business. The solution also adds invaluable context to internal network observables from firewalls, proxies, antivirus, and other security logs.

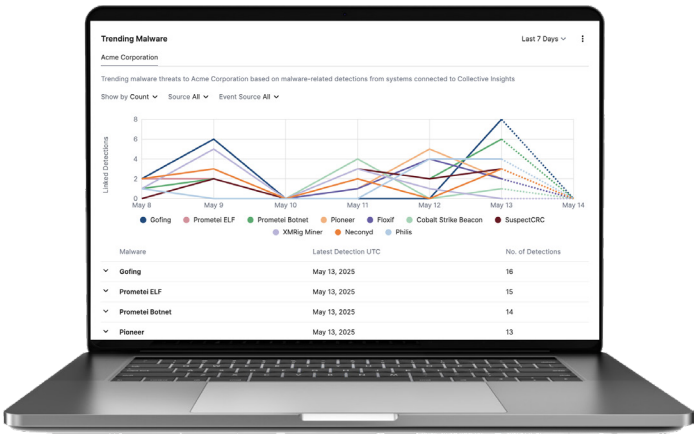
Integrated directly into SIEM, SOAR, EDR, or XDR tools for alert triage and threat detection use cases, SecOps Intelligence provides real-time Risk Scores and key evidence for indicators to help analysts quickly resolve false positives,determine alert prioritization, and easily access more information when further investigation is required. By minimizing the need to manually aggregate,correlate, and triage information, Recorded Future empowers analysts to dramatically reduce the amount of time it takes to detect, investigate, and respond to real threats.

Key Benefits

- Maximize investment in existing tools with out-of-the-box integrations
- Reduce time to respond to critical threats with real-time Risk Scores
- Streamline investigations for informed decision-making with the SecOps Intelligence Dashboard
- Automate security workflows and reduce security team workloads and complexity

Key Use Cases

- Prioritize critical threats and resolve alerts
- Integrate real-time Risk Scores and context into the existing tools and workflows of the security analyst
- Cut down alert triage and investigation time



Example SecOps Intelligence overview dashboard exposing trending malware overtime and the ability to view specific detections and pivot to Intelligence Cards™ as needed.

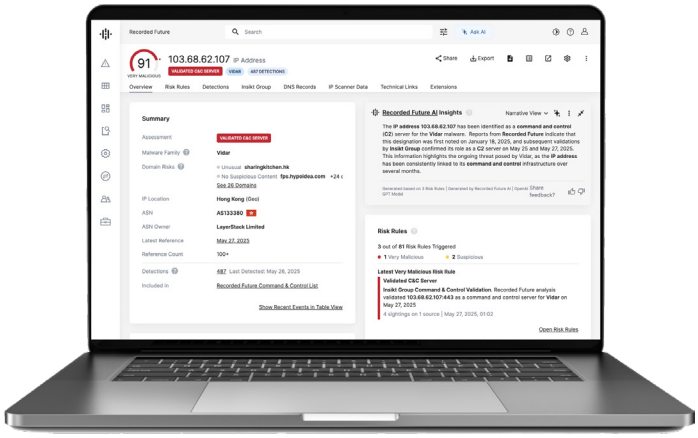
1.4x
increase in team capacity

~3x
decrease in time to identify a new threat

11
hours saved per team weekly on alert triage, investigation, and response effort

Features

Real-time Risk Scores and context	The SecOps Intelligence Module provides context on IPs, domains, URLs, hashes, and malware to help you filter relevant information from the noise, prioritize threats with confidence, and respond with speed, ultimately reducing risk.
Out-of-the-box SIEM, SOAR, EDR, and more integrations	Easily incorporate SecOps Intelligence into your existing tools and workflows with out-of-the-box integrations, including Splunk, Microsoft Sentinel, Cortex XSOAR, ServiceNow Security Incident Response, CrowdStrike, and SentinelOne.
Broadest source coverage available	SecOps Intelligence automates the collection, analysis, and production of intelligence from an unrivaled range of open, dark web, and technical sources. Then it combines that intelligence with world-class research to help you respond faster.
All-in-one view	See trending threat topics and expert research together in the SecOps Intelligence Dashboard.



Example Intelligence Card showing comprehensive intelligence on an IP address including risk score, expert analysis, transparency to original sources of intelligence, and more.

"We use the correlation dashboards in Recorded Future's app for Splunk to pull what's relevant and sort by severity. Surfacing one IP among billions is hard so being able to sort according to risk helps us triage faster."

Alex Minster
Security Engineer, Kyriba

Discover what your organization can do with the SecOps Intelligence Module.

Request a demo to learn how you can make fast, effective, data-driven decisions with Recorded Future.