Recorded Future®

Using SecOps Intelligence to Disrupt Adversaries

Defend Your Organization With Faster Investigation and Response

As the attack surface grows, security operations and incident response teams are seeing more and more security alerts each day. If you're like most analysts, you're plagued by alert fatigue and you struggle to pinpoint, triage, and respond to real threats targeting your organization using only information from your internal environment. You're dealing with:

TOO MANY ALERTS, TOO LITTLE TIME

Researching thousands of raw data points is overwhelming to even the most seasoned security analyst. With too little time and not enough information, it's difficult to determine which alert represents a critical incident and which may just be a redundancy or a false positive. Valuable time is wasted getting to "no" for irrelevant alerts, while true positives may be slipping through the cracks.

NO OUTSIDE VIEW

When internal alerts come from non contextual threat data feeds and disparate systems, they lack the vital information on external threats that enables good decision making. Even if you're using external threat indicators — like free feeds and unverified sources — many are unreliable, often resulting in additional false positives and dangerous blind spots.

MANUAL DETECTION

Manual searches for external threats related to your organization and industry are time consuming and ineffective. Analysts spend many valuable cycles looking for information on the open and dark web, only to find incomplete pieces of what they need — ultimately resulting in slower responses to real threats.

INEFFECTIVE BLOCKING PRACTICES

The ever-growing number and dynamic nature of threat indicators make it extremely challenging to confidently identify and block real threats at the perimeter with firewall, email security, and endpoint solutions. Meanwhile, false positives are routinely blocked, which disrupts business operations and hinders employee productivity.

Recorded Future: Unprecedented SecOps Intelligence

Recorded Future automates the collection, analysis, and production of elite security intelligence at scale to drive accelerated responses across vast amounts of data. By centralizing and continuously updating intelligence in real time, Recorded Future empowers security operations and incident response analysts to identify relevant, previously unknown threats. With Recorded Future, analysts are able to immediately access actionable context and respond confidently — without any manual research.

Using a sophisticated combination of our patented algorithm process and world-class human analysis, Recorded Future fuses an unrivaled range of open source, dark web, technical sources, and original research. This results in relevant, real-time insights, delivered in every language, and integrated with security systems to enable four primary uses cases for security operations and incident response:

ALERT TRIAGE

Recorded Future connects the dots between the broadest range of sources across every language. Unprecedented intelligence and critical context enable analysts to confidently prioritize alerts based on a risk score that updates in real time and is backed by transparent evidence. This empowers them to quickly discount false positives, identify the most significant threats, and take immediate action. Plus, more than 10 out-of-the-box SIEM and SOAR integrations position this real-time security intelligence directly within their existing security solutions.

RECORDED FUTURE IN ACTION.

Get real-time enrichment from Recorded Future integrated immediately into your SIEM or SOAR solution. This provides the context you need to prioritize and escalate incidents, accelerate remediation, and save analysts' time.

THREAT DETECTION

Security practitioners deal with countless alerts every day — many of which come out of external data that's correlated with internal network data. However, teams are left with more alerts than answers when the data lacks context or timeliness. Recorded Future's unmatched, machine-scale collection and analysis provides risk lists for IPs, domains, hashes, malware, and vulnerabilities with critical context to speed detection, automated responses, and risk reduction.

RECORDED FUTURE IN ACTION.

Quickly identify potential threats by automatically matching internal data with Recorded Future intelligence and risk scores. This enables you to detect threats earlier and respond faster by adding valuable context to internal network observables from firewall, email security, and endpoint solutions.

THREAT PREVENTION

The explosive growth of indicators means that threat feeds have to be high confidence and high fidelity in order to be actionable. Recorded Future Security Control Feeds are the quality indicators and context organizations need to automate actions and proactively prevent threats. Armed with proprietary, evidence-based findings, organizations are able to automatically block high-risk indicators at firewall, email security, and endpoint solutions without needing to do additional enrichment. Additionally, custom risk feeds integrated into third-party products empower analysts to block more threats at the edge, minimize false positive blocking, automate incident response, and improve overall security posture.

RECORDED FUTURE IN ACTION.

Integrate Recorded Future Security Control Feeds with existing perimeter security solutions to generate higher-quality alerts and block lists with fewer false positives. Be alerted via email or the Recorded Future mobile app when a malicious threat is detected, then block validated, active indicators at your endpoint or firewall.

Relevant insights, updated in real time, give security operations and incident response teams the right information at the right time to disrupt adversaries and prevent damage to their organization. Recorded Future's sophisticated algorithm combined with world-class human analysis enables analysts to easily detect and resolve alerts for maximum risk reduction.

Key Features

- More than 1 billion Intelligence Cards™
- Real-time risk scores and evidence from the open, dark, and technical web
- Proprietary, evidence-based detect-and-block grade indicators
- Relevant, real-time alerts for your organization from the Intelligence Goals Library
- 10+ out-of-the-box SIEM and SOAR integrations

Key Benefits

- Review 50% more alerts
- Improve MTTD by identifying threats 10X faster
- Improve MTTR by resolving threats 63% quicker
- Identify 22% more threats before impact
- Boost overall security team efficiency by 32%

Recorded Future®

www.recordedfuture.com

@RecordedFuture

About Recorded Future

Recorded Future delivers security intelligence to amplify the effectiveness of security and IT teams by informing decisions in real time with contextual, actionable intelligence. By analyzing data from open, dark, and proprietary sources, Recorded Future offers a singular, integration-ready view of threat information, risks to digital brand, vulnerabilities, third-party risk, geopolitical risk, and more.