Recorded Future®

DATA SHEET

Integrating Threat Intelligence Into Security

Challenge

Security teams across the organization are faced with challenging questions — which alerts represent real threats? How do I prioritize patching after a vulnerability scan? What external threats are targeting my organization? What is the extent of this incident and what was the goal? Internal context and manual research provide some insights, but it's not enough to make the fastest, most effective decisions

Solution

Recorded Future Connect Xchange is designed to provide access to rich threat intelligence directly in the security solutions teams are already using.

Direct access to threat intelligence where you need it

Recorded Future's structured threat intelligence can be accessed and displayed in real time directly in existing security solutions, empowering security teams to have the rich threat intelligence they need, when they need it.

Customized risk lists for correlation

Threat intelligence can be tailored to specific alert use cases. By selecting specific threat intelligence to include in a risk list before integration and correlation with internal data, organizations can support high-fidelity alerting.

External intelligence combined with internal

Centralization of all external threat intelligence enables security teams to see everything at once. For example, internal block lists can be combined with external threat intelligence for a single risk list.

Seamless integrations

The Recorded Future Connect API is an open RESTful API used to integrate threat intelligence with third-party security solutions such as SIEMs, incident management systems, ticketing systems, threat intelligence platforms, and more.

CAPABILITIES:

The Connect API integrates threat intelligence for:

Enrichment

Dive into external data for details and context for risk-based alert and incident prioritization.

Correlation

Identify relationships between internal activity logs and external risk and threat intelligence.

Monitoring and Alerting

Review and alert on company-specific entities found in external data.

Benefits

Faster, risk-based alert triage

Real-time access to rich external context empowers security operations teams to quickly triage alerts and uncover what's important faster.

Focus on strategic decisions

Automated collection and analysis combined with real-time delivery of threat intelligence means security teams are freed from manual research and able to focus on strategic, higher-value work.

Reduced dwell time

Faster triage and effective prioritization means attackers have less time to work before they are discovered — reducing business impact of an incident.

Unknown threats revealed

Tailored risk lists enable organizations to correlate with internal data to find specific threats. This ability to alert based on real threats reduces the mean time to response (MTTR) and business impact.

Connect Partners

Recorded Future Connect includes more than 30 integrations:

SIEM	Incident Response/SOAR	Vulnerability Management
IBM QRadar	Phantom	tenable
exabeam	SWIMLANE	Qualys
splunk>	resilient an IBM Company	RAPID7
LogRhythm The Security Intelligence Company	insightConnect	NOPSEC
McAfee	DEMISTO A PALO ALTO NETWORKS COMPANY	brinqa

And more

servicenow RSA Archer GRC SentinelOne

IBM i2 Analyze paloalto NETWORKS MALTEGO

Visit www.recordedfuture.com/integrations for more details.

Recorded Future®

www.recordedfuture.com

@RecordedFuture

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.