THREAT INTELLIGENCE FROM THE WEB, TAILORED FOR SECURITY OPS

Recorded Future offers both off-the-shelf and custom features that QRadar users can use to bring real-time threat intelligence into the security operations center. Through QRadar’s right-click functionality, analysts can access real-time Intel Cards that include:

• IP address, domain, file hash, and vulnerability risk scores
• Full transparency on risk evidence, including sources and sightings
• Related entities such as attack vectors, domains, and malware
• On-demand export to STIX and CSV

Real-Time Threat Intelligence for QRadar

Dramatically increase your speed to “no” verdicts. Rapidly understand true incidents in context.

Security operations center (SOC) teams are inundated with alerts and events. Threat intelligence from Recorded Future creates clarity by adding rich context. We surface and deliver threat intelligence in real time from the widest breadth of open, technical, and dark web sources, helping you make informed verdicts. SOC analysts can efficiently dismiss false positives and capture threat context for true incidents.

Detect important incidents in your network that you would otherwise have missed.

Recorded Future identifies indicators with elevated risk by analyzing web reporting, threat lists, and our own novel methods. And unlike IP or domain reputation lists, we deliver rich context so you can selectively apply indicators that match your security needs in event correlation and detection rules.
Through Recorded Future’s Enterprise Web application, alerts can be configured to monitor outside-the-network risks, including company name, domains, and key CIDR blocks.

Finally, security teams can incorporate Recorded Future’s context-rich threat feed into QRadar’s reference collections to expand the data available for analysis.

WHY RECORDED FUTURE

Faster Analysis
Spend less time collecting data and supercharge your analytic capacity.

Cut Out the Middleman
Direct access to real-time intel for monitoring and IR.

Relevant Intel
Tailored to your environment, infrastructure, and corporate profile.

Gain threat awareness beyond your network.

Be proactive with incident detection, as risks originate or are first reported outside your network. Monitor and alert on risks related to your IP ranges, domains, and company using Recorded Future as your sensor in the web. When alerting rules trigger, we deliver detailed notifications with provenance, links to sources, and cached access to ephemeral content.

Drill down from correlation to triage to investigation.

For a demo or quote, email us at info@recordedfuture.com.

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.