

DATA
SHEET

Recorded Future for Rapid7 InsightIDR

Detect and respond to threats faster with actionable context at your fingertips. Recorded Future delivers security intelligence to arm security and IT teams that use Rapid7 InsightIDR with the real-time information they need to detect incidents earlier and prioritize their findings with confidence.

Contextualized Intelligence

Contextualized intelligence is a crucial component of any truly proactive security strategy. Recorded Future empowers faster, more informed security decisions with relevant insights that are updated in real time and integrated with your existing infrastructure. Security intelligence from open, technical, and dark web sources helps reduce security risk by automatically correlating against telemetry data within your Rapid7 environment for real-time detection of potential threats.

The explosive growth of indicators makes finding the needle in the haystack extremely resource-intensive for already overwhelmed security teams. With Recorded Future intelligence, security teams using Rapid7 InsightIDR can easily discover and validate findings. Real-time natural language processing automatically summarizes information on more than a billion threat-related entities while providing full access to the original sources of intelligence.

BENEFITS

- Detect previously unknown threats within Rapid7 InsightIDR
- Respond to findings faster with real-time, high-confidence context
- Maximize investments in Rapid7 InsightIDR and accelerate SecOps workflows

RESULTS*

- Identify 22% more security threats before impact
- Improve response times by 63%

**Learn more about the business value Recorded Future brings to clients in our [IDC Report](#)*

KEY FEATURES

- Recorded Future's risk lists for IPs, hashes, domains and URLs
- Out-of-the-box correlation against the client's raw logs, endpoint data, and network traffic

Utilizing the Recorded Future browser extension over Rapid7 InsightIDR allows users to enrich findings with evidence-based, real-time risk scores and risk rules — all without having to leave Rapid7 InsightIDR. This empowers users to confidently prioritize the most important findings in their environment, simplify workflows, and maximize the ROI of existing cybersecurity solutions.

The screenshot displays the 'Investigation Details' page for the finding 'Account cpna visited a suspicious link'. The interface includes a left sidebar with a list of findings, a central timeline view, and a right-hand pane for evidence and context.

Timeline:

- Mar 24, 2021 7:55 AM: Account cpna visited a suspicious link
- Mar 24, 2021 7:49 AM: Account cpna visited a suspicious link
- Mar 24, 2021 7:05 AM: Account cpna visited a suspicious link
- Mar 24, 2021 6:12 AM: Account cpna visited a suspicious link

Evidence:

- HTTP Request:** Fortinet Fortigate FW recorded 10.0.1.144 performing an HTTP GET request to http://morrishttu.ddns.net/ on at Mar 24, 2021 7:55:38 AM. 84 byte(s) were sent.
- Community Threat:** http://morrishttu.ddns.net/ belongs to the tracked community threat(s): Recorded Future Dynamic Threat Feed.
- User Account:** cpna (7insightidr.com) is associated with user Christopher Pena (7insightidr.com) by ACTIVE_DIRECTORY.

ABOUT RECORDED FUTURE

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,300 businesses and government organizations across 60 countries. Learn more at recordedfuture.com.



www.recordedfuture.com



@RecordedFuture