Recorded Future®

Reducing Detection Time

How Threat Intelligence Finds the Signal in the Noise

Recorded Future®

Executive Summary

Recorded Future recently conducted numerous interviews with clients and security industry experts to hear about their goals and challenges in today's evolving cybersecurity landscape.

Interviewees told us that they're looking to enhance their security infrastructure, streamline operations, and proactively detect and defend against cyber threats. Whether they're currently using cybersecurity automation tools or not, they recognize the benefits of automated security solutions to help gather, monitor, and report on potential risks more efficiently and effectively.

> In this eBook, we'll share the top four challenges security teams face, and we'll show how automated threat intelligence solutions can help teams quickly collect external insights for faster decision-making, increased capacity, and more effective risk mitigation.

Recorded Future®

● CHALLENGE 1

Too much data, not enough context

Turning data into actionable insights is a top challenge

Security and threat intelligence teams are overwhelmed. They're inundated with more data than ever, but it lacks the necessary context to help them understand which threats to prioritize.

37%

of security professionals list "too much data, not enough information" as their top day-to-day challenge.[1]

More tools and more alerts can make teams less effective

When Recorded Future asked clients and industry experts about their pain points, many cited "alert overload" — the overwhelming volume of security alerts and notifications that can hinder productivity, create stress and anxiety, and lead to missed opportunities.

Interviewees consistently emphasized the importance of efficiently managing alert overload, staying informed about potential threats, and taking necessary actions. They recognized the need for comprehensive alert management solutions that streamline operations and improve the effectiveness of threat detection and response.

54%

of respondents in the 2024 *Cybersecurity Buyers Report* list alert fatigue as their top challenge[2]

6

is the average number of tools analysts interact with to investigate a single alert[3]

3

is the average number of hours analysts dedicate to resolving each investigation[3]

Tens of thousands to millions

is the number of alerts in a typical SOC each day[4]

10-20

is the number of alerts the typical analyst can triage each day[4]

25%

of alerts are false positives and

55%

go uninvestigated[4]

Security teams need to reduce alert overload

One Recorded Future client emphasized the need to triage and prioritize alerts more effectively, stating,

"We need a solution to filter out unnecessary alerts and focus on high-quality data for actionable insights."

Recorded Future®

SOLUTION 1

Enrich internal data with external threat intelligence

In order to prioritize and remediate the threats that matter most, security teams need to supplement internal alerts with external information and context so they can perform rapid triage and then scope and contain incidents.

Use external threat intelligence to prioritize and rank alerts based on risk

Risk-based decision-making is critical in alert prioritization. After integrating Splunk with the Recorded Future platform, one company reported saving "a huge amount of time" primarily through the use of risk scores.[5]

"The ability to prioritize alerts based on external threat intelligence and risk factors is crucial for our security operations."

— Recorded Future client

Improve mean time to investigate (MTTI) and triage processes while reducing false positives

Threat Intelligence gives security teams the context they need to triage alerts promptly and with significantly less effort. It prevents analysts from wasting hours pursuing alerts based on:

- Actions that are likely to be innocuous rather than malicious.
- Attacks that aren't relevant to their organization.
- Attacks for which defenses and controls are already in place.

Recorded Future users report that they're

48% faster

at identifying new threats than before[5]

"We use the correlation dashboards in Recorded Future's app for Splunk to pull up what's relevant and sort by severity," said one Recorded Future client. "Surfacing one IP among billions is hard, so being able to sort according to risk and work our way down the list definitely helps us start triaging faster."

An Insurance Organization has been using Recorded Future SecOps Intelligence to investigate malware such as DarkGate and Purple Fox. The team pulls IOCs from the Intelligence Cards to proactively block malware in their environment.

Focus on the risks that matter most to your organization

With Recorded Future threat intelligence, analysts can quickly identify the most significant threats and take immediate, informed actions to resolve them.

How a Manufacturing Organization uses Recorded Future

A security lead calls Recorded Future's risk scoring the most comprehensive and accurate of anything the company has used. He says the additional context allows him to save time by focusing on high-risk vulnerabilities for patching "instead of chasing everything with a high CVSS score."

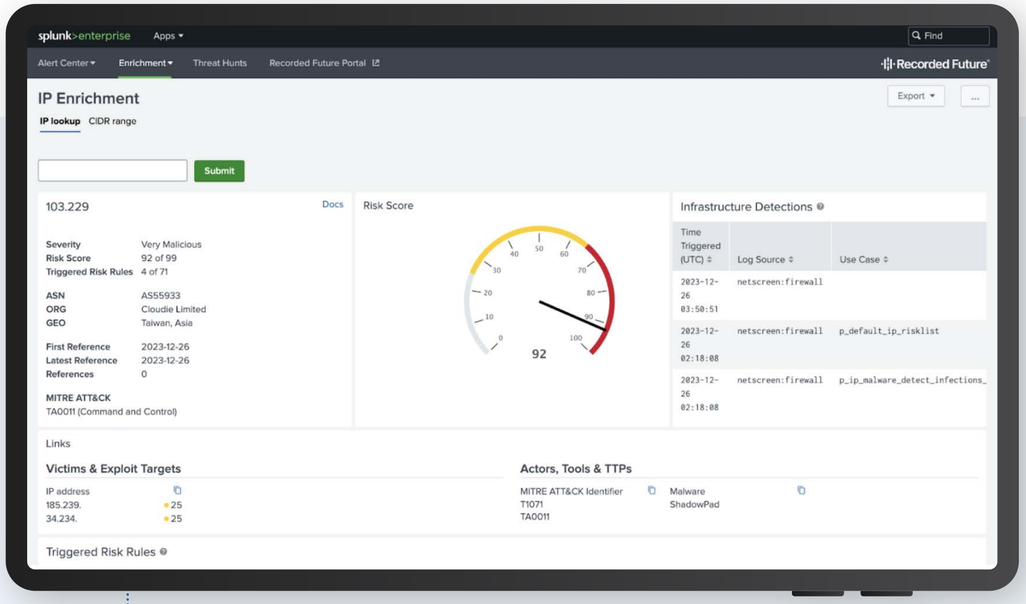
Recorded Future®

Enrich your internal data with Recorded Future solutions

Streamline security operations by automating security workflows with the context you need to identify and mitigate critical threats. Investigate high-risk IoCs, improve alert triage, and use our Threat Map to discover adversaries most likely to harm your organization.

Integrations provide access to robust intelligence optimized for use in the tools you already use, including Splunk, Palo Alto Networks, Microsoft, and ServiceNow.

▶ See Interactive Demo



IP Enrichment within Splunk Enterprise enables analysts to view all associated activity with a malicious IP, including infrastructure detections, victims of the ShadowPad C2 IP, and associated threat actors and TTPs. Take an interactive tour of the Recorded Future x Splunk integration.

Recorded Future®

● CHALLENGE 2

Security teams are overloaded

Resource constraints and a lack of skilled professionals create a vicious cycle for employees working on shorthanded teams. With too many responsibilities and not enough personnel, security staff are burning out and quitting their jobs at high rates.

The labor market isn't keeping up with demand

80%

of organizations are impacted by the shortage of security professionals in the labor market[3]

39%

of new security jobs remain open for weeks or months[3]

Workloads and burnout are on the rise

80%+

say their workloads have increased in the past year[1]

63%

of practitioners experience some level of burnout[1]

As a result, security teams struggle to be effective

When their teams are understaffed and overburdened, organizations are at higher risk of missing critical threat signals or addressing them too late.

46%

of CISOs strongly agree that their cyber threat intelligence programs are burdened by too many manual processes, most of which span the entire threat intelligence lifecycle and create multiple bottlenecks[6]

36%

of business leaders view resource and skill gaps as their highest barrier to cyber resilience[7]

36%

of surveyed security leaders said they've experienced an incident that could have been prevented had their team been more capable[3]

Recorded Future®

SOLUTION 2

Maximize team resources with actionable threat insights

Free up your security teams to spend more time on strategic projects and initiatives by automating the alert triage process.

Upskill junior and less-skilled analysts

With in-depth information about the latest threats, less-experienced analysts can make critical connections in threat intelligence data and build their skills more rapidly.

For example, let's say an alert is generated when an unknown external IP address attempts to connect over TCP port 445. An experienced analyst would know that ransomware was used in a recent SMB exploit, and would identify the IP address as likely to be compromised based on the owner, location, and open source data.

A less experienced analyst might not make these connections unaided, but contextualized SecOps intelligence from Recorded Future would show them that other devices on the network use SMB on port 445 to transfer files and data between servers. It would also inform them that the new exploit and ransomware have been associated with that IP address, so they would immediately understand the need to investigate further.

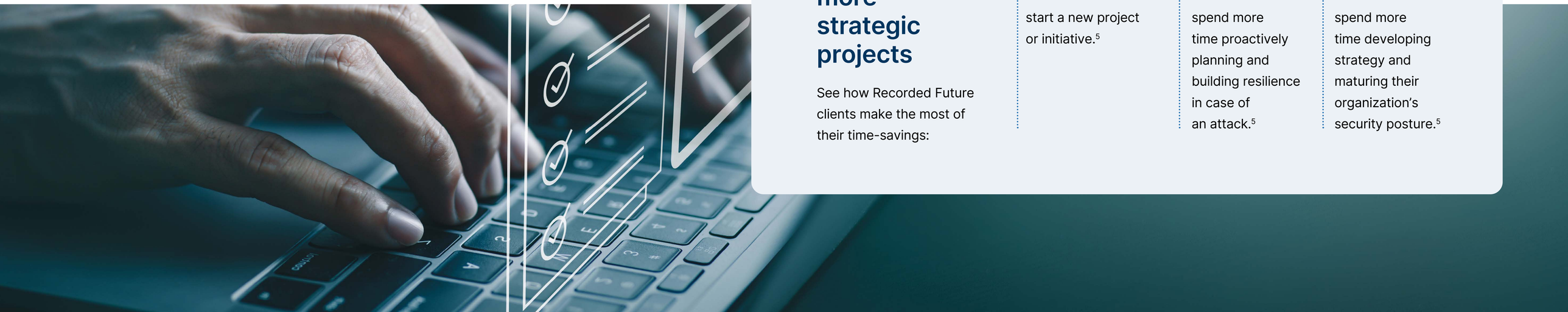
Take on more strategic projects

See how Recorded Future clients make the most of their time-savings:

27%
start a new project or initiative.[5]

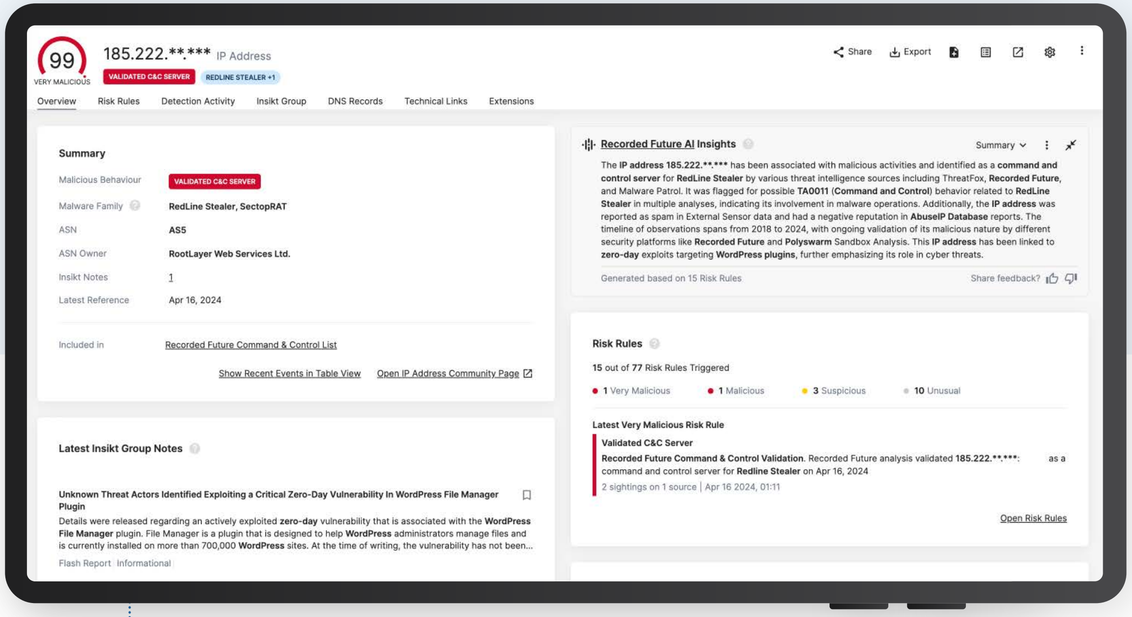
45%
spend more time proactively planning and building resilience in case of an attack.[5]

52%
spend more time developing strategy and maturing their organization's security posture.[5]



Recorded Future®

Make the most of your resources with Recorded Future solutions and products



IP Intelligence card for an active C2 IP address associated with the infostealer, RedLine Stealer

Automate Security Workflows to more effectively and efficiently manage security alerts.

Efficient Incident Management and Response

- **Situation:** The analysis confirms the IP's involvement in a broader campaign targeting financial institutions.
- **Action:** You use Splunk to generate actionable alerts and automate response workflows, such as blocking the IP at the firewall and isolating affected systems.
- **Benefit:** Streamlined incident response processes reduce manual tasks and response times, allowing you to focus on higher-level analysis and proactive threat hunting.
- Learn more by taking an interactive tour of Recorded Future's Splunk ES integration.

Recorded Future®

● CHALLENGE 3

Unintegrated security tools add more noise

When security organizations work with multiple tools that don't talk to each other, analysts spend a significant amount of time manually coordinating information to try to determine what matters and what doesn't.

Too many tools lead to frustration and other challenges

39%
of organizations use between 10–25 disparate tools for security operations.[3]

47%
use more than 25 incongruent security operations tools.[3]

49%
of security teams say that having too many different consoles or tools to investigate incidents is one of the top 5 things that frustrate them the most.[1]

Top 5 challenges related to security operations "tool sprawl"[3]

1. Cost and purchasing complexity from working with multiple vendors
2. Increased reliance on inefficient manual processes
3. Slower investigation and response times
4. Ineffective security risk assessment
5. Ineffective security workflow coordination

Security automation can help, but it comes with its own complexities

Automation can speed up investigations, provide valuable context around incidents, and trigger response actions. However, many security teams struggle to effectively use automation solutions such as security orchestration, automation, and response (SOAR).[8]

Recorded Future®

SOLUTION 3

Make your security tools more effective by integrating external threat intelligence

In ideal environments, security tools can be counted on to handle data collection and processing so that analysts can focus on analysis, remediation, and planning for the future.

1. **Score each alert according to importance.**
2. **Determine whether each alert should be dismissed as a false positive or triaged for further investigation.**
3. **Enrich each alert with valuable, real-time context and evidence.**

Together, integration and security automation are force multipliers

Organizations that effectively integrate their internal tools with external intelligence eliminate the need for analysts to manually compare each alert to information derived from their ecosystem of tools. And together, integrated solutions and automated processes can filter out a huge number of false positives without any analyst oversight, saving time and empowering analysts to focus on higher-value work.

Recorded Future use cases

Financial services organization

Less than a week after integrating their Endpoint Detection and Response (EDR) tool with Recorded Future Collective Insights, a financial services organization was able to easily conduct incident response on AsyncRAT. The SecOps dashboard in Recorded Future made it easy to see which C2 the malware connected to, and the security team was able to block it with minimal effort and time spent.

Kyriba
The financial software company uses the correlation dashboards in the Recorded Future Splunk app to save time:

“We pull up what’s relevant and sort by severity,” a Kyriba security engineer said. “Surfacing one IP among billions is hard, so being able to sort according to risk and work our way down the list definitely helps us start triaging faster.”

Recorded Future®

Boost your security tools' effectiveness with Recorded Future products and solutions

Enhancing situational awareness with Collective Insights and the Splunk Correlation Dashboard

Example scenario

A Level 2 SOC analyst at a large healthcare provider is responsible for overseeing the integration of threat intelligence across different platforms and ensuring that the organization's security posture is proactive and robust. Her challenge is to effectively visualize data from disparate sources to quickly detect and mitigate threats.

Step 1: Consolidating data for a unified view

Situation: She begins her analysis by addressing alerts from multiple sources, including EDR solutions and cloud security platforms.

Action: She uses Recorded Future's Collective Insights to aggregate and visualize these alerts on a unified dashboard. This dashboard is configured to pull in data from Splunk, SentinelOne, and CrowdStrike, offering a comprehensive view of the security landscape.

Benefit: This consolidation allows the analyst to quickly identify trends and anomalies across platforms without switching between different systems, improving her reaction time to potential threats.

Step 2: Analyzing trends with MITRE ATT&CK framework

Situation: Amidst the flood of data, she notices an uptick in alerts related to ransomware attempts.

Action: Using the Collective Insights dashboard, she applies the MITRE ATT&CK framework to categorize and analyze these threats. This helps her understand the tactics and techniques being used, and the extent of the potential impact.

Benefit: By contextualizing the data within a well-known framework, she enhances her analytical capabilities, allowing for targeted and effective countermeasures.

▶ Take an interactive tour of Recorded Future to see how a Level 2 SOC analyst could accomplish both steps outlined above.

Recorded Future®

● CHALLENGE 4

Ineffective collaboration hinders business growth

When security teams are burdened with heavy manual workloads, they don't have time to share intelligence and collaborate effectively with other internal teams like Marketing, Finance, Legal, Product Development, and more.

> That lack of insight and collaboration can affect strategic plans and the bottom line. For example, threat actors can damage a brand's reputation, causing challenges for Marketing as well as loss of revenue. Or they can attack a company's software vendors, interfering with key tools that multiple departments rely on to accomplish their day-to-day work.

A Perspective from Citizens Financial Group, Inc.

"We get so much information and we do our best to disseminate it out to our internal stakeholders, but there are only so many people that we can reach. We only have so many resources to do that…and so I think that's a big thing for us this year — just increasing that visibility on our intelligence and ensuring that we're not just sending information to teams, but we're actually sending intelligence. We're assessing risk and communicating why it's relevant and important to us and why people should care about it."

— Lea Cure, CTI Manager, Citiziens Financial Group, Inc.

Recorded Future®

SOLUTION 4

Improve cross-team collaboration with relevant insights and recommended actions

Keep business moving forward by providing internal partners with relevant insights on external threats and critical risks as well as clear steps for improving defenses.

How a commercial banking client's security team boosts collaboration

This security team shares intelligence with multiple departments across their organization, including:

- Marketing Communications for brand monitoring
- Third-party Risk Management to mitigate third-party breaches and securely onboard new vendors
- Business Development teams to evaluate acquisition targets
- Facilities Operations teams for disaster planning

"There are many different teams across an organization that can benefit from threat intelligence."

— Christopher Martinkus, Threat Intelligence Manager for a North American commercial bank

How Kyriba's security team works across departments

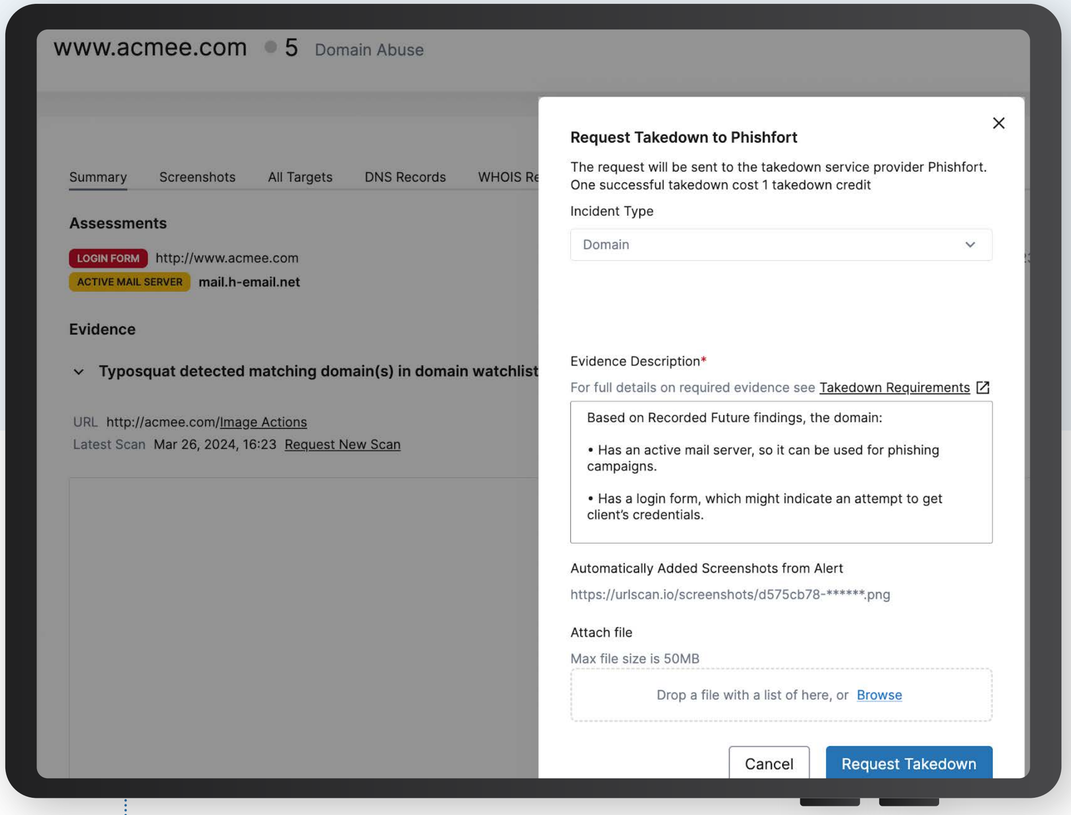
Homing in on the most relevant threats helps security analysts forewarn company leaders so they can take appropriate action. Kyriba credits Recorded Future's proactive intelligence with highlighting new cyber threats on the front end and helping to flag dangerous exposures like hijacked domains and stolen credentials on the back end.

"Threat intelligence from Recorded Future makes our team look prophetic. We're able to say, 'Here's something we need to be worrying about so let's raise awareness around that,' and sure enough, it starts to land on our shores a month or so later. It's been a great boost to our organization to have Recorded Future provide that early heads-up so we can get out in front when something bubbles up."

— Kyle Minster, Security Engineer, Kyriba

Recorded Future®

Improve collaboration with Recorded Future products and solutions



Auto-populated Evidence for Domain Takedown Request Associated with a Login Form. Learn more in an interactive tour.

Digital Risk Protection helps you protect your digital assets, brand image and data by automating risk detection, reducing investigation time, and improving response and mitigation efforts.

▶ See Interactive Demo

Recorded Future®

Strengthen your defenses with Threat Intelligence

Threat Intelligence is a critical component of the cybersecurity arsenal. With threat actors quickly evolving, IT environments growing more complex, and vulnerabilities continuing to increase, defenders need actionable context to prioritize response efforts and make informed decisions about actions to take.

Recorded Future helps organizations elevate existing security defenses by enhancing the depth and breadth of protection with insights into external threats and attacks before they impact. Enabling defenders to stay a step ahead of attackers, at the speed and scale of today's threat environment.

Recorded Future is the most comprehensive and independent threat intelligence cloud platform on the market, named a leader in The Forrester Wave™ External Threat Intelligence Service Providers, Q3 2023 report.

To learn more about the Recorded Future Intelligence Cloud Platform and how we can help secure your organization and enable faster decision-making, request a demo or talk to your customer success representative.

Recorded Future®

Endnotes

1 https://www.tines.com/reports/voice-of-the-soc-2023

2 https://www.actualtechmedia.com/wp-content/uploads/2023/12/cybersecurity-buyers-report-final.pdf

3 https://www.splunk.com/en_us/form/esg-soc-market-trends-report.html

4 https://www.picussecurity.com/how-to-improve-alert-management

5 Recorded Future Client Survey (April 2023)

6 https://www.techtarget.com/searchsecurity/opinion/Threat-intelligence-programs-need-updating-and-CISOs-know-it

7 https://www.weforum.org/publications/global-cybersecurity-outlook-2024/

8 https://www.forrester.com/report/best-practices-for-automating-security-operations-workflows/RES179705

Recorded Future®

About Recorded Future

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com