Recorded Future®

Building Cyber Resilience

Four Strategies for Taking a Proactive Approach with Threat Intelligence

Recorded Future®

Table of Contents

Recorded Future®

Executive Summary

In the past year, there's been a notable rise in ransomware attacks from groups including REvil, Conti, BlackBasta, and Lockbit. The CL0P MOVEit campaign affected 2,750 organizations and 94 million individuals, making it the biggest hack of 2023. Additionally, the rapid growth of AI has created new opportunities for threat actors, and the Israel-Hamas and Russia-Ukraine wars have led to high levels of global unrest and uncertainty.

Amidst this turmoil, it's no wonder that the term "cyber resilience" is everywhere in the security community. Enterprises want to build resilience in order to combat emerging threats, meet compliance and regulatory requirements, deal with cyberattacks and service disruptions, manage increasingly complex operations, and mitigate the risks associated with their reliance on third-party software providers.

In this eBook, we'll explore four ways that security teams can use Recorded Future to build the resilience they need to achieve these critical goals and help drive business forward.

Recorded Future®

CHAPTER 1

Know Your Adversary

CHALLENGES

Lack of clarity on which threats to prioritize

Attackers come from all over, target different industries, and have different methods and motivations

- ✓ **Attack critical infrastructure**
- ✓ **Spread disinformation**
- ✓ **Steal assets**

Top three aims of the "Big Four" APT groups backed by Russia, China, Iran, and North Korea. (The Record)

$1.1 billion

is the 'known' amount companies, individuals, and other ransomware victims paid in 2023. (The Record)

Security teams struggle to determine which adversaries have the intent and opportunity to target them

1,000s

of threat actor groups operate around the world at any given time →

Including:

- State-sponsored threat actors
- Ransomware groups
- Advanced persistent threat (APT) groups
- Hacktivists
- And more

Security teams cite 2 top obstacles to clarity

Potential clients have told Recorded Future that their investigations are hampered by these key issues:

1. **Noisy open-source threat intelligence feeds**

   40% of CISOs strongly agreed it is hard to sort through threat intelligence noise to determine what's relevant to their organization (Tech Target)

2. **Time-consuming manual research processes**

   According to the Tines Voice of the SOC report, spending time on manual work is the most frustrating aspect of the job (Tines)

Recorded Future®

OUTCOMES

Focus on the threats that matter most

With proactive threat mitigation strategies that include threat intelligence and automation, security teams can make informed decisions about critical threats and enhance their security processes.

4 steps to building resilience against threat actor groups

1. Focus on threats specific to your organization

Use threat intelligence to build your defenses against the threat actors that have:

- **The highest intent** (i.e., they're targeting other organizations in your industry)
- **The highest opportunity** (i.e., they're targeting the tech and tools you use)

Prioritize groups that are targeting your industry and tech, and de-prioritize any others.

> "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 ealy 'heads up' so we can get out in front when something bubbles up."
>
> — Alex Minster, Security Engineer at Kyriba

2. Reduce risk from initial access vectors

Focus on the top initial access vectors — including phishing, valid credentials, and exploitation of public-facing applications — and improve your defenses there.

Identify and remediate compromised credentials, vulnerabilities, and brand impersonation opportunities.

> "The timeliness is a big win with Identity Intelligence. Being able to automate the response after seeing an alert to our active directory allows us to feel confident that the account is secure."
>
> – Curtis Hartsell, Senior Cyber Threat Intelligence Manager at Toyota Motors North America

3. Deploy pre-built hunting packages

Implement these open-source detection mechanisms in your local environment to hunt for adversaries, malware, or traffic of interest.

Run hunting packages like YARA, Sigma, and Snort rules to detect threat actor activity in your network.

> "The workflow for downloading YARA and Sigma rules from interested threat actors and malware on our Threat Map has been a huge time saver. It has eliminated manual rule-building and enabled our staff to focus on more critical operational issues."
>
> — Recorded Future client

4. Integrate threat intelligence into your security workflows

Create an intelligence-driven response to threats. Enrich internal logs with external threat intelligence to separate the signal from the noise, accelerate alert triage, and improve visibility into relevant threats.

> "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."
>
> — Alex Minster, Security Engineer at Kyriba

Recorded Future®

CHAPTER 2

Understand Your Weak Points

CHALLENGES

Unknown and unmanaged attack surface risks

Attack surface exposures are difficult to identify

As organizations embrace digital transformation and cloud-based assets, their external attack surface grows and shifts. Lack of visibility into exposures like critical vulnerabilities and end-of-life software puts them at greater risk of attack.

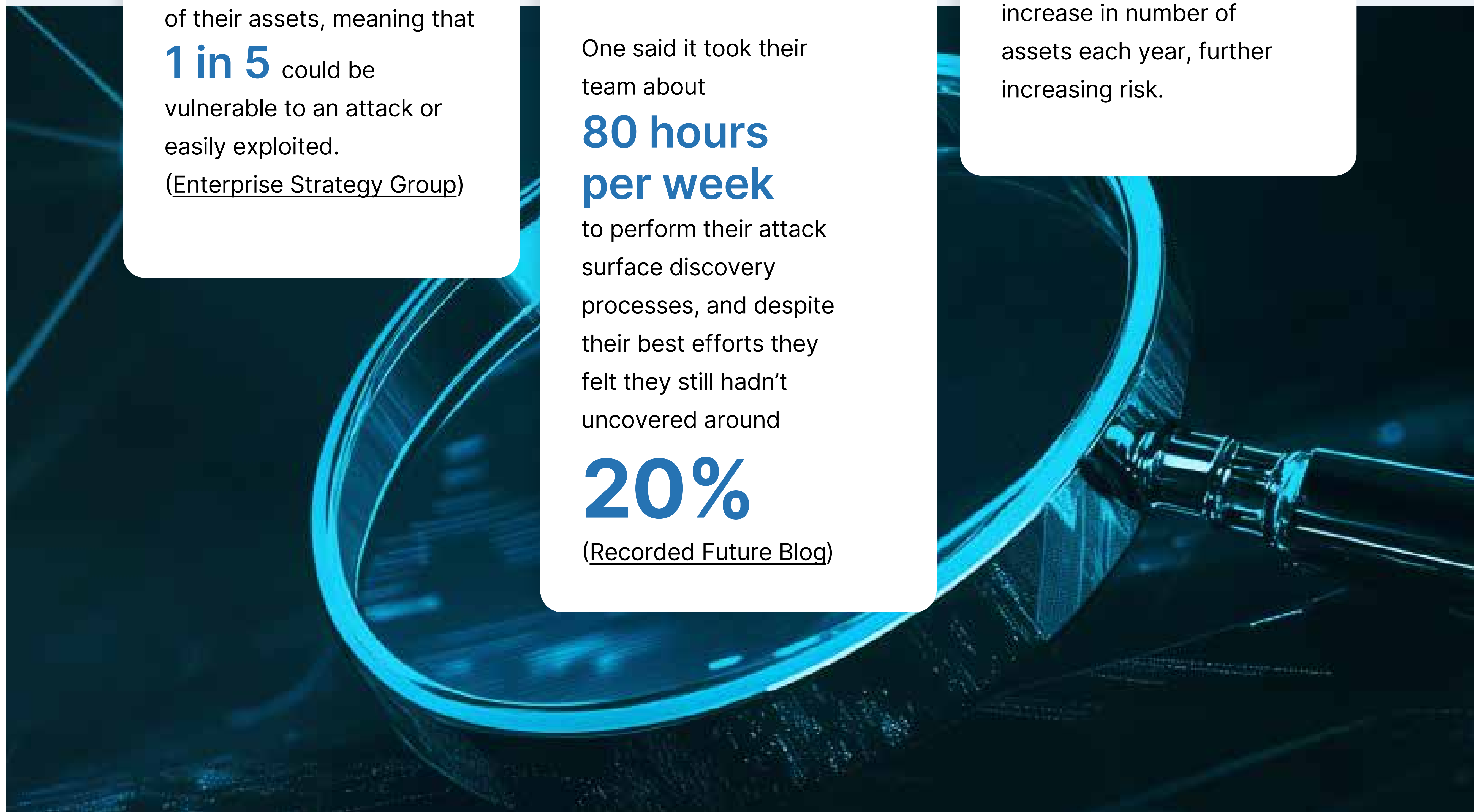
76%

of organizations say they've experienced a cyberattack due to an unknown or poorly managed internet-facing asset (Enterprise Strategy Group)

Managing exposures requires core cyber hygiene tenets:

- ✓ **Knowing where our assets are**
- ✓ **Securing what's vulnerable**

Security teams struggle with 3 key challenges



1 Asset blind spots

73%

of organizations believe they have strong awareness of **less than 80%** of their assets, meaning that **1 in 5** could be vulnerable to an attack or easily exploited. (Enterprise Strategy Group)

2 Resource-intensive discovery processes

Prior to using our solutions, many Recorded Future clients felt hampered by lengthy discovery processes.

One said it took their team about **80 hours per week** to perform their attack surface discovery processes, and despite their best efforts they felt they still hadn't uncovered around **20%**

(Recorded Future Blog)

3 Growing and changing attack surfaces

Recorded Future's data shows that the average enterprise sees about an **18%** increase in number of assets each year, further increasing risk.

OUTCOMES

Reduce attack surface risks and exposures

To help manage exposures, security teams need to be able to identify external assets, understand associated risks, and prioritize remediations.

4 steps to building resilience against attack surface exposures

1. Identify new assets

It's easy to miss things because you weren't looking, you weren't told, or standard protocols weren't followed.

With automated discovery and a real-time inventory of internet-facing assets, security teams can understand what's new and what's changed to ensure that all assets are accounted for and in a defensible position.

> "Recorded Future saves our team a week's worth of time each month, freeing us up to focus on more proactive practices like vulnerability management and threat hunting."
>
> — Recorded Future client

2. Prioritize exposures

If assets have associated risks such as vulnerabilities, misconfigurations, or end-of-life software, organizations need to be able to prioritize these exposures with actionable scoring and evidence.

> "The Exposure section of Recorded Future Attack Surface Intelligence helps us zero in on the critical and high-risk vulnerabilities that are out there for our organization. It really helps us to quickly identify things like vulnerable databases or CVEs associated with WordPress plugins on specific sites."
>
> — Recorded Future client

3. Track software vulnerabilities

Clients have highlighted the importance of prioritizing vulnerabilities based on severity, impact, and exploitability rather than solely relying on CVSS scores.

They recognize the need for comprehensive vulnerability management and risk assessment, aiming to minimize noise and gain control over scan results. They also value timely reporting, accurate vulnerability assessments, and a proactive approach to identifying and addressing potential threats.

> "When you're looking at two different vulnerabilities that are possibly both critical per the CVSS score, which one's more important? Well, probably the one [associated with] the APT who's interested in your type of organization or industry and it's a part of their TTPs, or it's being actively used in your threat landscape. We really want to go after that first. When you can show how in a resource-constrained environment where you need to rack and stack your priorities, I think that's key. I'm sure there's nobody...who feels like they have enough resources."
>
> — Matt Bittick, Attack Surface Risk Reduction Analyst, Cummins

4. Enforce policies

While organizations spend a lot of time creating effective policies to keep their business, people, and assets secure, employees often knowingly or, more likely, accidentally bypass these policies.

Security teams need a way to spot out-of-policy assets, such as assets hosted with unapproved cloud providers or in unapproved locations, and admin panels that are accessible on the internet.

> "The team was able to surface several assets that were out of policy, such as admin pages that should never have been exposed... One of the best things Recorded Future's Attack Surface Intelligence is doing that the traditional tools are not good at is finding exposed admin pages."
>
> — Recorded Future client

CHAPTER 3

Monitor Digital Risks

CHALLENGES

Unknown digital risks

As organizations grow their digital presence and interact with customers and partners through new channels, they become more vulnerable to external threats such as brand and executive impersonation, account takeovers, and data leakage. In particular, they struggle to defend the initial access vectors that threat actors use to bypass defenses, such as valid credentials and phishing.

Digital risks are difficult to identify and investigate

There are too many hard-to-reach sources to monitor for brand mentions and leaked data. And even in easy-to-reach sources like social media and app stores, investigations are overwhelmingly manual and time-consuming, and they can still result in missed threats.

Top 2 reasons organizations need to manage digital risks:

1 Brand Image

Enterprises need to maintain a strong brand image, particularly in industries like healthcare and financial services where reputation and trust are critical.

46% of businesses have experienced brand impersonation over the past two years

(Splunk)

2 Vulnerable Credentials

Enterprises have large numbers of employee credentials to monitor in a threat landscape where emails and passwords are often leaked and then used in account takeovers.

86% of breaches involve the use of stolen credentials

(Verizon DBIR 2022)

Valid Accounts are the #1 initial access vector used by cybercriminals

(Recorded Future)

Recorded Future®

OUTCOMES

Monitor digital risks in real time

With actionable intelligence, security teams can better defend common initial access vectors. For example, by enabling automatic alerts when their brand or compromised credentials appear on the dark web, they'll have more time to focus on a response.

4 steps to building resilience against digital risks

1. Automate discovery

Unknown threats to your brand can include domain abuse, chatter on the dark web, executive impersonation on social media, and creation of fake apps.

With Recorded Future, you can automate monitoring processes to quickly surface threats and investigate them more effectively.

"We monitor and triage typosquatting and masquerading using automated systems, detecting new domains/certificates and changes to risk of previously detected domains. We can analyze and triage a new detection fully within 3-5 minutes, versus 20+ prior to Recorded Future and automation."

— Recorded Future client

2. Identify stolen credentials

Compromised credentials were the top initial access vector in 2023, and IBM X-Force has seen a 266% increase in the use of infostealer malware to aid threat actors in stealing more credentials.

By detecting credentials stolen via infostealer malware or being sold on dark web shops and forums, security teams can proactively reset accounts before threat actors use the stolen keys to bypass security systems.

One Recorded Future client noted that they've been seeing great value from identifying compromised employee accounts.
The intelligence within the exposed credential alert allows them to quickly act by resetting accounts, identifying the specific malware family, and educating the user.

3. Access helpful context

Timely alerts are helpful, but added context makes the difference. Context helps users make fast, effective, data-driven decisions, while eliminating the noise that leads to wasted time and inefficiencies.

"Recorded Future's optical character recognition (OCR) capabilities have helped us identify phishing and fake partnership sites. With a combination of the alerts and additional context, we've been able to quickly take the sites down."

— Recorded Future client

4. Remediate digital risks

Until taken down or mitigated, digital risks pose a serious threat to an organization's reputation, people, and assets.

Timely alerts and helpful context can help security teams request takedowns of fraudulent sites and/or reset stolen credentials before the brand suffers any harm.

"A great way for us to show the value the intelligence brings is to produce results. With the Identity Intelligence module we're able to do that pretty easily by seeing the compromised credentials show up, force password resets, and then see those immediate attempted logins using the stolen credentials, followed by thankfully a bunch of failures."

— Curtis Hartsell, Senior Cyber Threat Intelligence Manager at Toyota Motors North America

Recorded Future®

CHAPTER 4

Prevent supply chain risks

CHALLENGES

Assessing and monitoring supply chain vendors

Supply chain attacks and third-party risks are on the rise

It's difficult for security teams to get visibility into vendor breaches and to understand which vendors are susceptible to breaches.

> "The thing that keeps me up at night is supply chain attacks. We can have a lot of control over a lot of different things. We can put mitigations in place to defend against them and hope that it catches it. But with supply chain attacks, a lot of the time, especially with vendors there's not a whole lot that you can do to prevent them."
>
> — Recorded Future client

Supply chain attacks involve 3 common targets

1. Suppliers and vendors

59% of organizations have experienced a data breach caused by a third party due to a lack of visibility. (Opus & Ponemon)

2. Software technologies

54% of organizations have an insufficient understanding of cyber vulnerabilities in their supply chain. (World Economic Forum)

3. Physical locations

"Geopolitical risks arising from supply chain issues, regional tensions, and expanding regulation all lead to strategic risks for enterprises, so they need to develop more efficient and effective technical security programs." (Gartner)

OUTCOMES

Proactive visibility into supply chain risks

Security teams can reduce risk by improving the way they assess threats and risks to vendors as well as vendor products and partners. They can help ensure that customer and employee data isn't stolen in a third-party breach or vulnerability exploit. And they can put measures in place to help keep supply chain and geopolitical risks from impacting company performance.

Improve monitoring with real-time insights into third-and fourth-party vendors

With proactive threat mitigation strategies that include threat intelligence and automation, security teams can make informed decisions about critical threats and enhance their security processes.

> "Recorded Future is invaluable, as it helps us determine whether something is an active threat or a past threat, something to prioritize or not give as much importance. We also use it for research purposes, such as for vendor selection and management. As the company continues to expand quickly, we need to make sure that we're staying nimble and on top of things — and Recorded Future enables us to do so."
>
> — Security analyst, Hughes Federal Credit Union

Recorded Future®

4 steps to building resilience against supply chain risks

1. Improve real-time visibility

With the right tools, your security team can immediately assess both cyber and physical threats to your suppliers and vendors.

For example, Recorded Future sends alerts when a supplier is mentioned on a ransomware extortion site, or when a key part of their physical supply chain has been disrupted.

"We've had instances where an alert came through from Recorded Future that a third party of ours was listed on a ransomware site, and we were actually notifying that vendor before they even knew that they were listed on there."

— Recorded Future client

2. Streamline investigations

Empower your security team to quickly evaluate new vendors, review products prior to procurement, see changes in the risk exposure of a third party, and evaluate fourth-party exposures.

Speed up investigations with the ability to simultaneously compare risks across a number of vendors.

A Recorded Future client noted they were alerted of a ransomware incident at one of their third party providers hours before they were notified by some of their other sources.

3. Track software vulnerabilities in your tech stack

Track vulnerabilities in your tech stack, from disclosure to exploitation in the wild. When your security team can understand the weaponization stage of specific vulnerabilities, they can be more proactive about reducing risk.

Use solutions that offer guidance on the severity of each vulnerability as well as recommended actions to help inform patching cycles.

One Recorded Future client says the separation of vulnerabilities into lifecycle stages, particularly exploit likely, helps them get left of boom.

4. Continuously monitor supply chain vendors

Solutions that provide alerts as well as context enable security teams to quickly mobilize to mitigate attacks.

For example, Recorded Future's playbook alerts for high-impact third-party cyber events help organizations stay ahead of critical risks. Clients often tell us that they're able to notify their vendors before the vendor even knows they've been victimized.

"Recorded Future Third-Party Intelligence provides a different perspective on the profile of a vendor that we're working with. We can see past incidents that they've had, and spot check their security hygiene in real-time. It helps to give the risk assessor a different perspective, and some additional questions, that they can probe into with their points of contact at the vendor."

— Recorded Future client

·|¦|· Recorded Future®

Build Resilience 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 and the Frost Radar™: Cyber Threat Intelligence, 2024 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 account manager.

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