# Recorded Future®

Automate Security Workflows

Streamline security operations with the context needed to identify and mitigate critical threats

Problem

Threat actors have an advantage, they only need to get it right once. On the other hand, security teams are buried in alerts, burdened with manual workflows, and lacking sufficient context, leaving them scrambling to stay ahead of attackers. Many alerts received by security operations teams are never even investigated leading to potential risks slipping through the cracks.

Only **33%** of alerts received by SOC teams are investigated
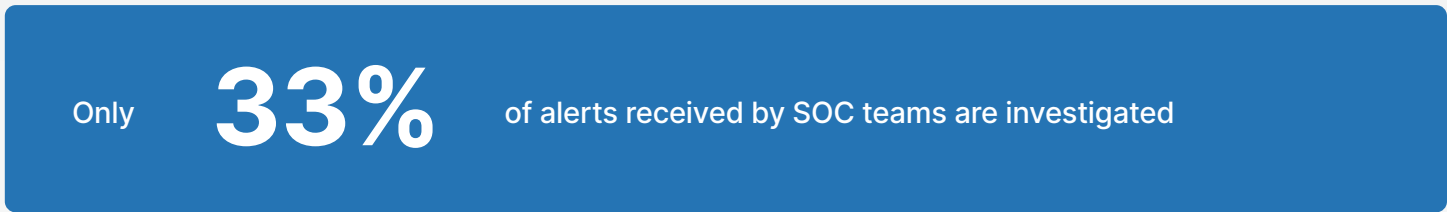
The most important element in cybersecurity is time, for both defenders and attackers.

The current state of affairs leaves defenders playing catch up. With threat intelligence, security teams can quickly separate the signal from the noise to ensure they can concentrate their efforts where they're most needed.

Solution

Recorded Future's Security Workflows Automation Solution enables security teams to respond to threats faster and more efficiently by automating the collection and distribution of intelligence in an actionable format. Integrated into your security tools and workflows, Recorded Future correlates and enriches internal data with external insights to accelerate threat identification, prioritization, and remediation.

Drivers

Sophisticated attackers	Lack of resources	Security stack complexity

Challenges

Dynamic indicators	Lack of context	Alert fatigue

Threat Intelligence Outcomes

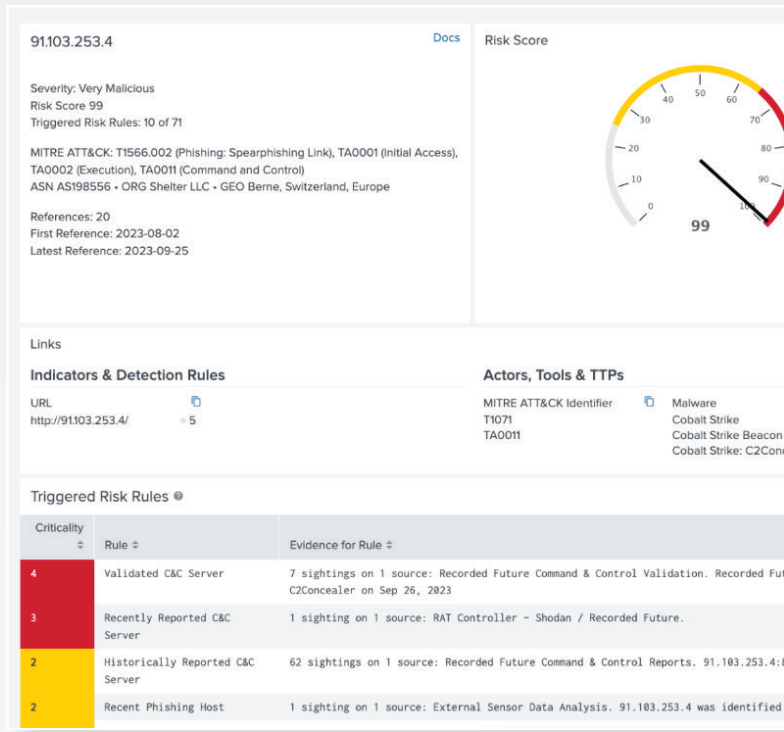| Reduce noise	Improve detection and response time	Enhance analyst efficency

Benefits

Focus on what matters

Empower security teams to efficiently prioritize alerts for investigation, eliminate the need to navigate between multiple tools, and streamline workflows to make informed decisions with ease.

Context at your fingertips

Get the information you need integrated into the tools your team uses today, including the severity of an indicator, related IOCs, linked malware, and expert research on the indicator in question.

Enhance efficiency
and take proactive action

Achieve reliable and trusted outcomes with intelligence as the foundation of your security operations automation strategy. Reduce the burden of manual tasks, whether it involves automating file detonation, conducting threat hunts, or by setting alerts to prevent future attacks.

FORRESTER®

WAVE LEADER 2023

External Threat Intelligence Service Providers

Request a Demo

recordedfuture.com/ demo-security-workflows-automation-solution

91.103.253.4 Docs   Risk Score

Severity: Very Malicious
Risk Score 99
Triggered Risk Rules: 10 of 71

MITRE ATT&CK: T1566.002 (Phishing: Spearphishing Link), TA0001 (Initial Access), TA0002 (Execution), TA0011 (Command and Control)
ASN AS198556 • ORG Shelter LLC • GEO Berne, Switzerland, Europe

References: 20
First Reference: 2023-08-02
Latest Reference: 2023-09-25

Links

Indicators & Detection Rules   **Actors, Tools & TTPs**

URL   MITRE ATT&CK Identifier   Malware
http://91.103.253.4/   5   T1071   Cobalt Strike
                                    TA0011   Cobalt Strike Beacon
                                                               Cobalt Strike: C2Con...

Triggered Risk Rules

Criticality ⇕	Rule ⇕	Evidence for Rule ⇕
4	Validated C&C Server	7 sightings on 1 source: Recorded Future Command & Control Validation. Recorded Fut... C2Concealer on Sep 26, 2023
3	Recently Reported C&C Server	1 sighting on 1 source: RAT Controller – Shodan / Recorded Future.
2	Historically Reported C&C Server	62 sightings on 1 source: Recorded Future Command & Control Reports. 91.103.253.4:8...
2	Recent Phishing Host	1 sighting on 1 source: External Sensor Data Analysis. 91.103.253.4 was identified...

Client Success Stories

"Threat intelligence helps prioritize my team's 'go forward' — our journey, if you will — to a Zero Trust North Star. Visibility and analytics is one foundational component, orchestration and automation is another. "

- John McLeod, CISO, NOV

32%   increase in team capacity

9.2 hours   per user per week saved on investigation & threat hunting activities

20%   of previously manual workflows automated