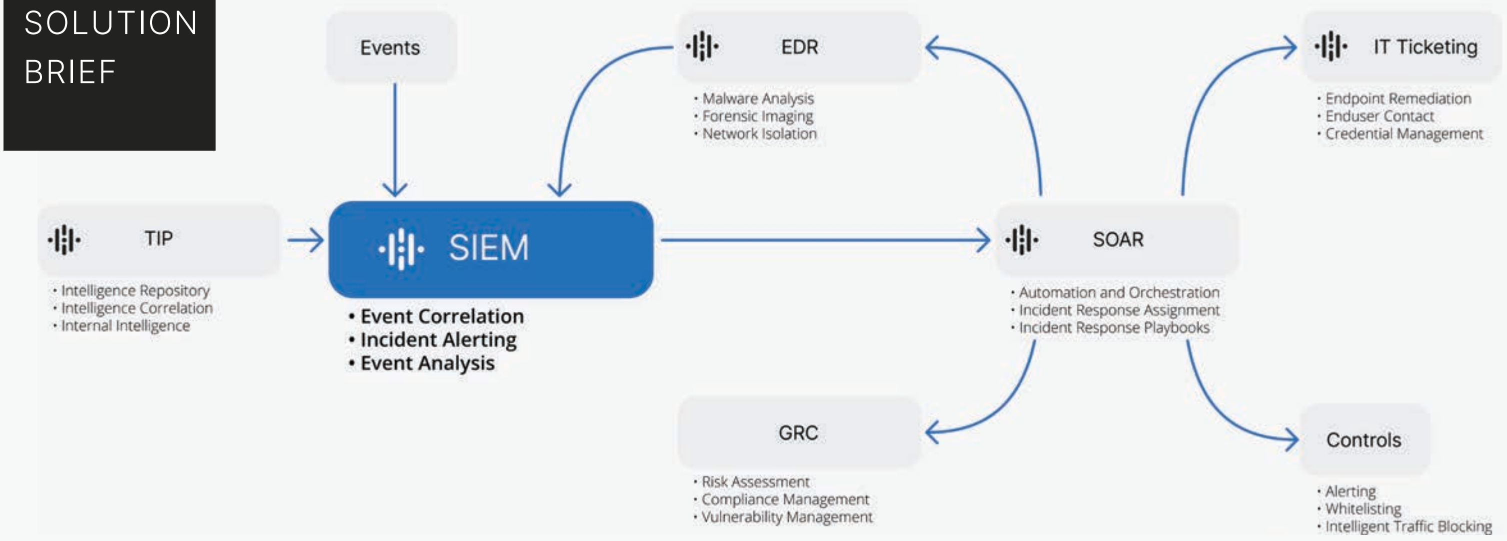
SOLUTION BRIEF



Supercharging SIEM Solutions With Threat Intelligence

The Challenge With SIEMs: Alert Fatigue

For years, security operations teams have relied on security information and event management (SIEM) technology to collect, correlate, and analyze security event logs from a variety of sources across their network environments. These tools were built to help them quickly detect and respond to threats, while streamlining compliance reporting and post-incident investigation. Yet as organizations continue to embrace new technologies to fuel digital transformation, the attack surface grows and the abundance of security alerts puts added stress on already overworked security professionals. Security operations center (SOC) Incident Response (IR) analysts are plagued by alert fatigue and face the following challenges with their SIEM technology:

- **Information Overload:** SIEMs generate thousands of security alerts each day. This is far too much information for SOC analysts to triage (research and process) manually. Studies show that nearly half of alerts go completely uninvestigated. (https://blogs.cisco.com/security/cisco-2017-annual-cybersecurity-report-the-hidden-danger-of-uninvestigated-threats)
- **No Outside View:** Without outside context, SIEMs only alert on internal data, leaving organizations unaware of external threats that could be targeting them.
- **Lack of Context:** While threat feeds can aid in uncovering new threats, the varying quality of feeds and lack of context often create unnecessary work when correlated with SIEM data. They may introduce a lot of false positive alerts and noise to an already noisy environment. To act effectively on these alerts, analysts often need to spend hours performing manual triage (research).

Integration Partners

Recorded Future has existing SIEM integrations with the following security software partners. These integrations enable organizations to find more threats and triage alerts faster with real-time intelligence displayed directly in their existing SIEM dashboard.

splunk>
LogRhythm
exabeam
McAfee
IBM Security
RSA
LOGPOINT
MICRO FOCUS
DEVO
Microsoft

- **Timing is Off**: Correlation can be critical for discovering new threats, but because indicators of compromise (IOC) may only be valid for a certain amount of time, it's important to correlate threat feed data with internal logs in as close to real time as possible within the timeframe the threat intelligence is discovered. Given the current state of SIEM capabilities and threat feed information, this can be challenging to operationalize.

As the attack surface continues to grow and organizations monitor more and more events, SIEM solutions' limitations have become increasingly apparent. To effectively respond to the multitude of alerts generated each day, SOC analysts need a way to prioritize which alerts to focus on first so they can optimize their effort for maximum risk reduction.

Contextualized Threat Intelligence, Seamless Integration

Properly contextualized threat intelligence that correlates with internal alerts is a vital component of any proactive security strategy. Relevant insights, updated in real time, give security operations analysts, incident responders, and vulnerability management professionals the insights they need — when they need them — to make faster, more confident security decisions.

Real-time threat intelligence from Recorded Future is machine readable for frictionless integration with existing SIEM solutions — empowering analysts to better detect, prioritize, and contextualize threats in real time.

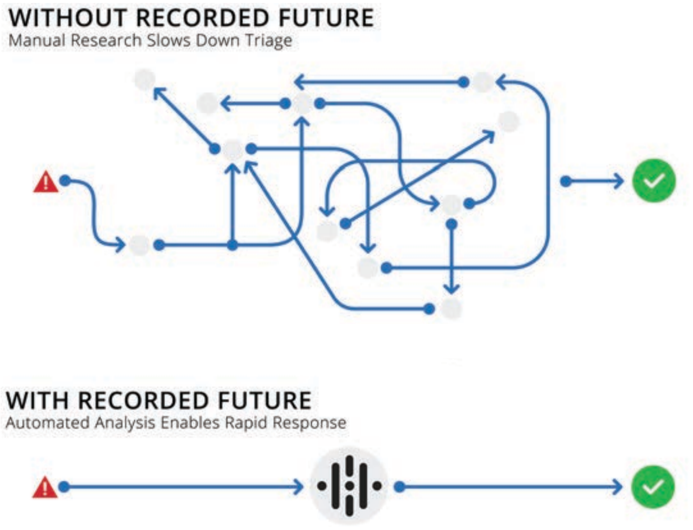
Enriching Alerts for Faster Response

Analysts are inherently limited by how much research they can perform for a given alert. There are only so many sources they can consult and so much time they can spend before needing to come to a verdict. Recorded Future arms analysts with vital information in real time, by using an automated approach for threat intelligence collection. We gather data from the broadest set of sources and use natural language processing and analytics to connect disparate data points across the web and aggregate them into intelligence that's surfaced in real time. Armed with real-time risk scores for indicators, SOC IR analysts can quickly determine which alerts should be prioritized first, and easily dive into more information if further investigation is required. By eliminating the need to manually triage and aggregate information, Recorded Future helps analysts dramatically reduce triage and investigation time, easily prioritize focus, and resolve more incidents faster.

Utilizing Real-Time Intelligence in SIEM Technology

- **Rapidly identify critical threats.** Teams can receive high-priority alerts on traffic to/from IP addresses known as "very malicious," while receiving lower-priority alerts on traffic to/from IPs considered "malicious."
- **Home in on specific activity types and timeframes.** Teams can identify high-priority alerts on traffic to IPs that are known as "current command and control," while assigning lower risk to IP traffic dubbed "historical command and control."
- **Identify the vulnerabilities that matter most.** By providing vulnerability management teams with additional context around how vulnerabilities reported to the SIEM are being exploited, they can prioritize patching and mitigation strategies to the riskiest vulnerabilities.

Alert Triage


WITHOUT RECORDED FUTURE
Manual Research Slows Down Triage
WITH RECORDED FUTURE
Automated Analysis Enables Rapid Response

Reducing False Positives With High-Fidelity Data

Recorded Future's unique combination of automated data collection and human analysis generates high-quality intelligence that can be correlated with SIEM data to identify high-risk threats before they impact the business. Recorded Future provides ready-to-use data sets of high-risk indicators, as well as related IOCs and contextualized vulnerability metadata, which can be fed directly into the SIEM. These data sets, called risk lists, include Risk Scores, which are assigned to each IP address, domain, URL, hash, and vulnerability based on risk rules sourced from over 800,000 web sources and over 60 external threat feeds. Risk lists can be correlated with the SIEM, adding valuable context to internal network observables from firewalls, proxies, antivirus, and other security logs. Using high-confidence data with clear risk rules that factor into the threat scores, rather than using black-box threat feeds, aids in identifying high-risk security events and minimizes false positives.

> **"Our Recorded Future integration helps us answer critical questions such as 'Where else has this alert been seen?' and 'What's the risk really like on this particular IOC?' This allows us to speed up the triage process, make faster decisions, and automate processes."**
>
> **Zachary Hinkel**
> Hogan Lovells

Recorded Future: Faster, More Confident Decision-Making

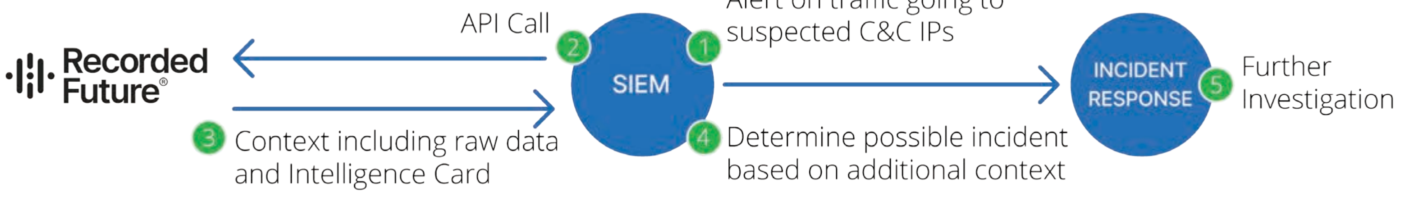
Recorded Future helps organizations reduce risk with the industry's only complete threat intelligence solution powered by patented machine learning and artificial intelligence. The solution delivers more context than threat feeds, updates in real time so intelligence stays relevant, and integrates seamlessly with SIEM solutions to provide:

Enrichment. Rapidly contextualize alerts by enriching them with the broadest set of external data sources — technical, open web, and dark web sources — ensuring all detection gaps are closed.

Correlation. Identify correlations between internal SIEM data and external threat intelligence to drive rapid response — reducing the burden on IT security.

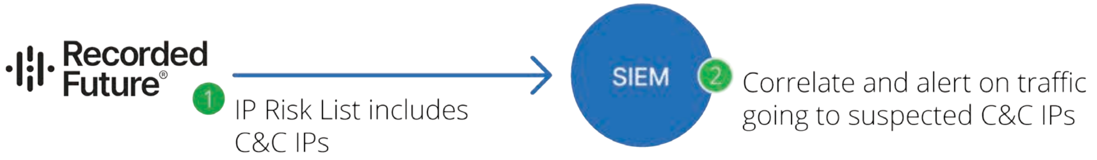
Targeted Alerts. Use Recorded Future to continuously monitor for intelligence directly relevant to the organization and receive contextualized, risk-prioritized alerts in real time that can be added to your SIEM.

ENRICHMENT



Recorded Future
API Call
2
SIEM
1
Alert on traffic going to suspected C&C IPs
3
Context including raw data and Intelligence Card
4
Determine possible incident based on additional context
INCIDENT RESPONSE
5
Further Investigation

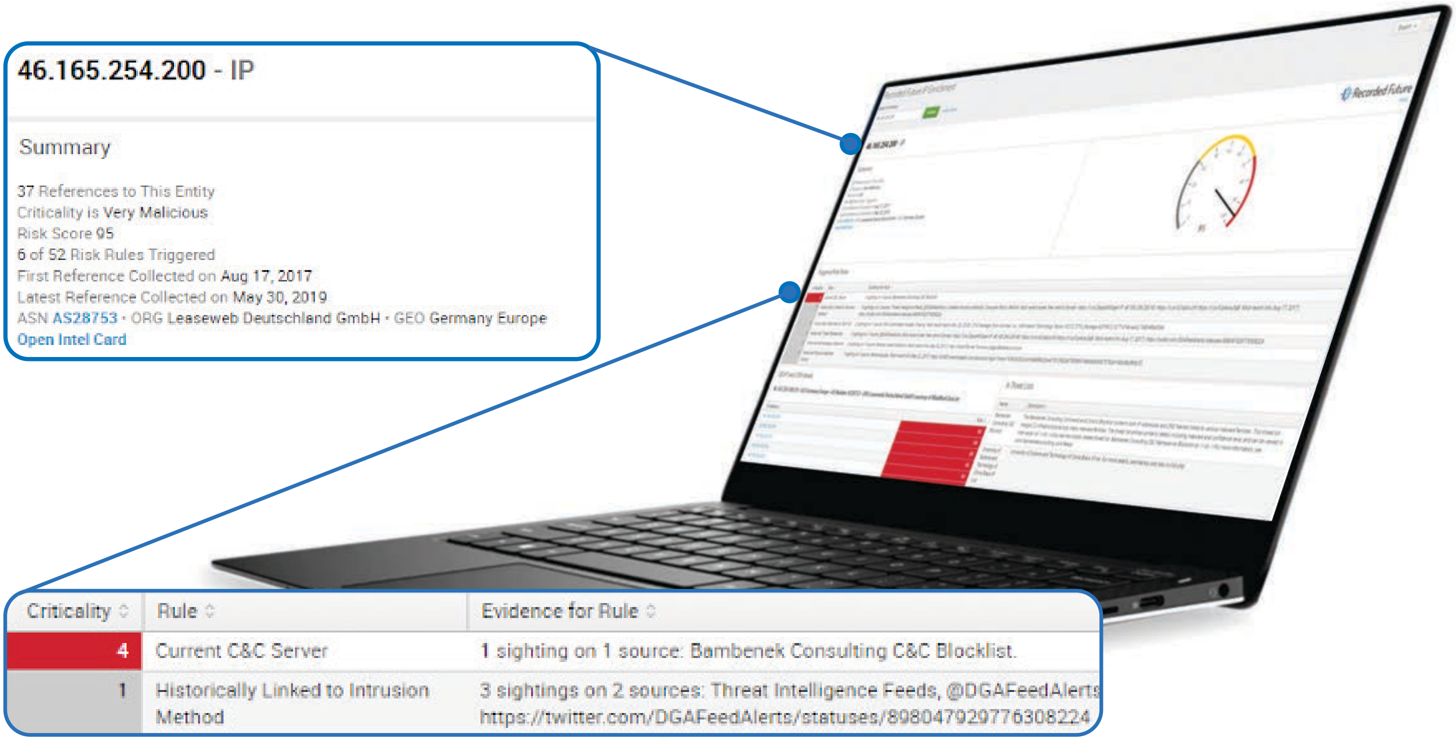
CORRELATION



Recorded Future
1
IP Risk List includes C&C IPs
SIEM
2
Correlate and alert on traffic going to suspected C&C IPs

Recorded Future SIEM Integration in Action: Splunk

1. There's increased traffic to a suspicious IP address — what should you do?
2. Investigate that alert directly from your SIEM and discover it's a command and control server
3. Take quick, decisive action to block that IP address



46.165.254.200 - IP

Summary

37 References to This Entity
Criticality is Very Malicious
Risk Score 95
6 of 52 Risk Rules Triggered
First Reference Collected on Aug 17, 2017
Latest Reference Collected on May 30, 2019
ASN AS28753 · ORG Leaseweb Deutschland GmbH · GEO Germany Europe
Open Intel Card

Criticality	Rule	Evidence for Rule
4	Current C&C Server	1 sighting on 1 source: Bambenek Consulting C&C Blocklist.
1	Historically Linked to Intrusion Method	3 sightings on 2 sources: Threat Intelligence Feeds, @DGAFeedAlerts https://twitter.com/DGAFeedAlerts/statuses/898047929776308224

Don't Take Our Word for It

Zachary Hinkel of Hogan Lovells explains how integrating Recorded Future into the company's security stack speeds up alert triage and decision-making:

"The Recorded Future Connect integration helps us answer critical questions such as 'Where else has this alert been seen?' and 'What's the risk really like on this particular IOC?' This allows us to speed up the triage process, make faster decisions, and automate processes. Without threat intelligence, you're playing a guessing game on whether an indicator is useful or not. You could end up guessing something is really bad – and causing downtime trying to triage it — when in reality, it is something very outdated."

Key Benefits

By integrating existing SIEM solutions with Recorded Future, organizations can:

- Research events **4X** faster
- Increase overall efficiency by **32%**
- Identify **22% more** threats before impact

EXPLORE OTHER RECORDED FUTURE INTEGRATIONS | RECORDEDFUTURE.COM/INTEGRATIONS

ABOUT RECORDED FUTURE

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based 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 1,400 businesses and government organizations across more than 60 countries. Learn more at recordedfuture.com.

www.recordedfuture.com   @RecordedFuture