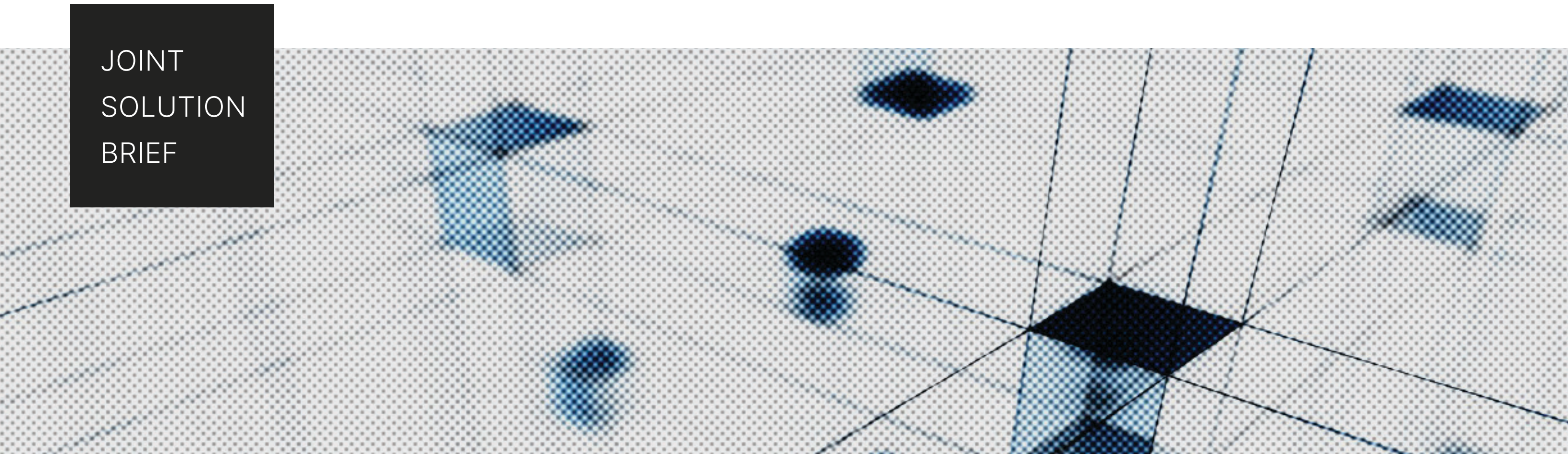
JOINT SOLUTION BRIEF



Recorded Future and Splunk Threat Intelligence Management

Benefits

- Build processes to identify the most relevant threats, proactively protect your network
- Quickly respond to incidents in a measurable way
- Ability to layer external threat data on top of internal telemetry data

Use Cases

The integration between Splunk Threat Intelligence Management and Recorded Future allows security responders to:

- Detect and gain context on threats with real-time external intelligence
- Proactively block threats before they impact the business

Product Overview

Splunk Threat Intelligence Management is an Intelligence Management Platform that helps you operationalize data across tools and teams, helping you prioritize investigations and accelerate incident response. This allows analysts to fully integrate their security technologies, teams, and processes with actionable threat intelligence resulting in reduced detection to response time and enhanced asset protection.

Joint Integration Description

The integration between Splunk Threat Intelligence Management and Recorded Future allows users to bring high-fidelity threat intelligence into their workflows to reduce the MTTR (mean time to response). The integration makes use of the following Recorded Future Risk List for correlation and detection:

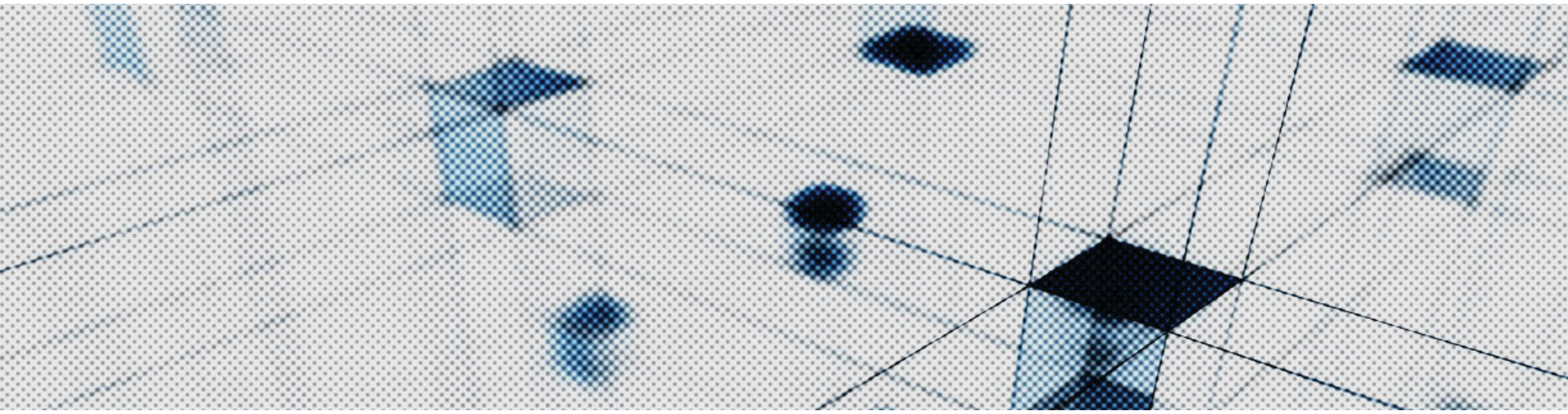
- IP
- URL
- Hash
- Vulnerability

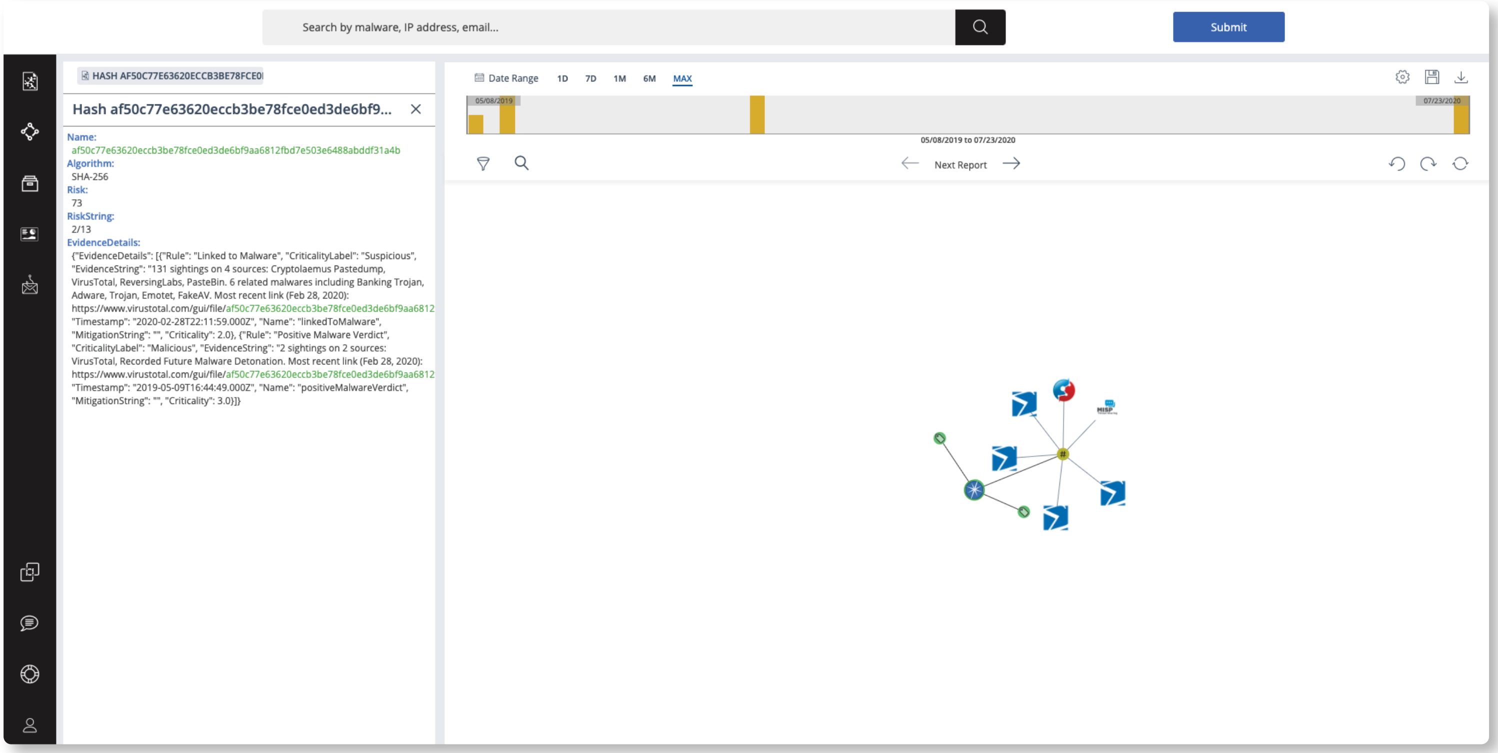
These datasets contain malicious indicators that can be used for correlation against internal telemetry data.

Challenges Overcome Through Integration

When security teams don’t collaborate and tools don’t communicate, critical gaps emerge. By making Recorded Future data available in Splunk Threat Intelligence Management, you’re able to:

- Build processes to identify the most relevant threats, proactively protect your network
- Quickly respond to incidents in a measurable way
- Ability to layer external threat data on top of internal telemetry data





Hash af50c77e63620eccb3be78fce0ed3de6bf9...

Name:
af50c77e63620eccb3be78fce0ed3de6bf9aa6812fbd7e503e6488abddf31a4b
Algorithm:
SHA-256
Risk:
73
RiskString:
2/13
EvidenceDetails:

```
{"EvidenceDetails": [{"Rule": "Linked to Malware", "CriticalityLabel": "Suspicious",
"EvidenceString": "131 sightings on 4 sources: Cryptolaemus Pastedump,
VirusTotal, ReversingLabs, PasteBin. 6 related malwares including Banking Trojan,
Adware, Trojan, Emotet, FakeAV. Most recent link (Feb 28, 2020):
https://www.virustotal.com/gui/file/af50c77e63620eccb3be78fce0ed3de6bf9aa6812
"Timestamp": "2020-02-28T22:11:59.000Z", "Name": "linkedToMalware",
"MitigationString": "", "Criticality": 2.0}, {"Rule": "Positive Malware Verdict",
"CriticalityLabel": "Malicious", "EvidenceString": "2 sightings on 2 sources:
VirusTotal, Recorded Future Malware Detonation. Most recent link (Feb 28, 2020):
https://www.virustotal.com/gui/file/af50c77e63620eccb3be78fce0ed3de6bf9aa6812
"Timestamp": "2019-05-09T16:44:49.000Z", "Name": "positiveMalwareVerdict",
"MitigationString": "", "Criticality": 3.0}]}
```

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 1,600 businesses and government organizations across more than 70 countries.

www.recordedfuture.com @RecordedFuture