

Recorded Future and LogPoint

PRODUCT OVERVIEW

LogPoint is a modern security information and event management (SIEM) solution that collects and analyzes event data from any device or application within your infrastructure. LogPoint automatically identifies and sends alerts about critical incidents in your system, helping companies respond quickly and precisely to security incidents.

JOINT INTEGRATION DESCRIPTION

The increasing number of security events can overburden analysts and lead to alert fatigue. With the LogPoint and Recorded Future joint solution, businesses can improve their security posture with a proactive defense that gives immediate insight into threat actors, tools, and techniques. Analysts gain real-time, cross-platform insight into potential threats, effectively eliminating false positives so they can focus on uncovering advanced threats.

CHALLENGES OVERCOME THROUGH INTEGRATION

By combining LogPoint's modern SIEM solution with Recorded Future's advanced TI reporting, we provide:

- An efficient way to detect and reveal any emerging threats, such as zero-day threats, APTs exploits within your infrastructure before they impact your business.
- Real-time insights on hundreds of thousands of IOCs to alert you about known attacks and proactively prompt action, such as blocking known bad IP addresses.

USE CASES

- LogPoint easily transforms data from Recorded Future into actionable intelligence, making it easier for SOC teams to protect your infrastructure.
- SOC teams can enrich log records using threat indicators such as IP, hash, URL, domain, or malware, providing a detailed overview of threat actors plus contextual information about why they are malicious.
- SOC teams can drill forward from a threat indicator to see all important artifacts associated with an IoC, making the incident management process more efficient.

BENEFITS:

- An efficient way to detect and reveal any emerging threats, such as zero-day threats, APTs exploits within your infrastructure before they impact your business.
- Real-time insights on hundreds of thousands of IOCs to alert you about known attacks and proactively prompt action, such as blocking known bad IP addresses.

LOGPOINT DASHBOARD SEARCH REPORT INCIDENT **SETTINGS** 08:34:50 admin

Recorded Future

Intelligence Card OVERVIEW THREAT LISTS RECENT REFERENCES SHODAN

General Information Settings Drill Forward Settings

Overview - IP 176.32.194.247 [Back to Search](#) [Recorded Future](#)

	6 of 52 Risk Rules observed	Very Malicious Criticality Label	Jul 2, 2019 First Reference	Jul 20, 2019 Latest Reference	AS197834 ASN	Armenia Country
--	--------------------------------	-------------------------------------	--------------------------------	----------------------------------	-----------------	--------------------

Triggered Risk Rules

Current C&C Server • 1 sighting on 1 source
RAT Controller - Shodan / Recorded Future. Threat listed on Jul 12, 2019.

Actively Communicating C&C Server • 1 sighting on 1 source
Recorded Future Network Traffic Analysis. Identified as C&C server for 1 malware family: Nanocore RAT Trojan. Communication observed on TCP-54984. Last observed on Jul 21, 2019.

USER ACCOUNTS CONFIGURATION KNOWLEDGE BASE SYSTEM RECORDED FUTURE

LOGPOINT DASHBOARD SEARCH REPORT INCIDENT **SETTINGS** 04:58:57 admin

Recorded Future

General Information Settings Drill Forward Settings

Total Records: 293522

S.N.	Name	Type	Last Successful Fetch	Status	Number of Records
1	IP Risklist	IP	2019-07-10 04:00:37	Completed	35091
2	Domain Risklist	Domain	2019-07-10 03:01:12	Completed	14845
3	URL Risklist	URL	2019-07-10 03:01:12	Completed	100000
4	Hash Risklist	Hash	2019-07-09 11:02:25	Completed	100000
5	Vulnerability Risklist	Vulnerability	2019-07-09 11:02:25	Completed	43586

USER ACCOUNTS CONFIGURATION KNOWLEDGE BASE SYSTEM RECORDED FUTURE

Recorded Future®

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.

© Recorded Future, Inc. All rights reserved. All trademarks remain property of their respective owners.

LOGPOINT

About LogPoint

LogPoint is committed to creating the best SIEM in the world. We enable organizations to convert data into actionable intelligence: supporting cybersecurity, compliance, IT operations, and business analytics.