

Recorded Future for Microsoft Azure

As the attack surface grows, security teams are seeing more and more events each day. However, with too little time and not enough context on the activity in their cloud environment, there's no way to connect the dots between data in Microsoft Azure services and the external risk of any detected threats. This slows responses and potentially enables relevant threats to slip through the cracks.

Contextualized Intelligence

Relevant insights, updated in real time, and integrated with your existing infrastructure drive faster, more informed security decisions. Recorded Future's unprecedented intelligence reduces security risk by automatically positioning threat data in your Microsoft Azure environment. This data is delivered to popular services like Microsoft Azure Sentinel and Microsoft Defender ATP to provide context and empower analysts to identify and triage alerts faster, proactively block threats, and reduce time spent on false positives to improve analyst efficiency.

Faster Threat Detection and Triage in Microsoft Azure Sentinel

Enables analysts to spend less time researching and more time remediating by correlating external threat intelligence against internal telemetry data by layering elite security intelligence on top of internal activity in Microsoft Azure Sentinel. This provides analysts with visibility into technical indicators — and empowers them to make prioritization decisions based on a realtime Recorded Future risk score that is backed by transparent evidence.

Proactive Threat Prevention With Microsoft Defender ATP

The ever-growing number and dynamic nature of threat indicators make it extremely difficult to confidently identify, block, and prevent real threats. By providing known malicious indicators identified across open, closed, and technical sources, Recorded Future security intelligence enables Microsoft Defender ATP users to validate known risky indicators currently living on endpoints and proactively block threats in their Microsoft cloud environment.

BENEFITS:

- Proactively block threats before they impact the business
- Automatically detect risky IOCs in your environment
- Triage alerts faster with elite, realtime intelligence
- Respond quickly with transparency and context around internal telemetry data
- Maximize your investment in Microsoft Azure

KEY FEATURES:

- Recorded Future IOC risk scores, risk rules, and evidence
- Recorded Future security intelligence via a dedicated Logic App Connector
- Recorded Future indicators available as Microsoft Graph Security API tilndicators for native leverage
- Incident enrichment via dedicated Connector Actions and unprecedented intelligence from Recorded Future

Results*

Resolve Security Threats 63% Faster

Relevant insights, updated in real time, and integrated with Microsoft Azure drive faster, more informed security decisions. Recorded Future eliminates laborious manual collection by providing contextual intelligence on internal telemetry data — empowering teams to quickly and confidently respond to incidents.

Identify 22% More Security Threats Before Impact

Using a sophisticated combination of patented machine and expert human analysis, Recorded Future fuses an unrivaled set of open source, dark web, technical sources, and original research to deliver relevant cyber threat insights in real time — empowering you to identify threats faster.

Improve Security Team Efficiency by 32%

Use the world's most advanced security intelligence platform to easily access the information you need, when you need it, to disrupt adversaries and reduce risk to your organization.

*Learn more about the business value Recorded Future brings to clients in our IDC Report, <u>Organizations React to Security Threats More Efficiently and Cost Effectively with</u> <u>Recorded Future</u>

Rect	futLogAn	alustics	▶ Run (Time range : 0	Custom	Vew alert rule ∨ → Export ∨ 🔗 Pin to o	ashboard 🔄 Format query			
		,	Time range .						
Schema and Filter	2 Query editor								*
	Results Chart 🛄 Columns 🗸 🕺 Add bookmark 🕥 Display time (UTC+0000) 🗸 💽 Group columns								
	Completed. Showing partial results from the custom time range.							ا 00:00:06.081	‴ 10,000+ records 🛛 🛠
	Showing the first 10,000 results. To improve your query, narrow down the result set. How to narrow down results								×
		TimeGenerated [UTC]	Action V ActivityGroupNames			√ AzureTenantId	√ ConfidenceScore		☑ Diamo
	>	6/15/2020, 3:18:45.985 PM	alert []	{"EvidenceDetails":[{"Rule":"Current C&C Server","E	videnceString":"2 C4829704-0EDC-4C3D-A34	-7C4A67586F3C 452745dc-5419-419e-9158-c	339c376aa58 95	Recorded Future IP Active	Communicating C&C
	>	6/15/2020, 3:18:45.985 PM	alert []	{"EvidenceDetails":[{"Rule":"Current C&C Server","E	videnceString":"2 C4829704-0EDC-4C3D-A34	-7C4A67586F3C 452745dc-5419-419e-9158-c	339c376aa58 95	Recorded Future IP Active	Communicating C&C
	>	6/15/2020, 3:18:45.985 PM	alert []	{"EvidenceDetails":{{"Rule":"Current C&C Server","E	videnceString":"1 C4829704-0EDC-4C3D-A34	-7C4A67586F3C 452745dc-5419-419e-9158-c	339c376aa58 95	Recorded Future IP Active	Communicating C&C
	>	6/15/2020, 3:18:45.985 PM	alert []	{"EvidenceDetails":[{"Rule":"Historically Linked to In	ntrusion Method", C4829704-0EDC-4C3D-A34	-7C4A67586F3C 452745dc-5419-419e-9158-c3	339c376aa58 97	Recorded Future IP Active	Communicating C&C
	>	6/15/2020, 3:18:45.985 PM	alert []	{"EvidenceDetails":[{"Rule":"Historically Reported in	n Threat List", "Evi C4829704-0EDC-4C3D-A34	-7C4A67586F3C 452745dc-5419-419e-9158-c3	339c376aa58 96	Recorded Future IP Active	Communicating C&C
	>	6/15/2020, 3:18:45.985 PM	alert []	{"EvidenceDetails":[{"Rule":"Historically Linked to In	ntrusion Method", C4829704-0EDC-4C3D-A34	-7C4A67586F3C 452745dc-5419-419e-9158-c	339c376aa58 96	Recorded Future IP Active	Communicating C&C
	>	6/15/2020, 3:18:45.985 PM	alert []	{"EvidenceDetails":[{"Rule":"Current C&C Server","E	videnceString":"2 C4829704-0EDC-4C3D-A34	-7C4A67586F3C 452745dc-5419-419e-9158-c	339c376aa58 95	Recorded Future IP Active	Communicating C&C
	>	6/15/2020, 3:18:45.985 PM	alert []	{"EvidenceDetails":[{"Rule":"Current C&C Server","E	videnceString":"2 C4829704-0EDC-4C3D-A34	-7C4A67586F3C 452745dc-5419-419e-9158-c	339c376aa58 95	Recorded Future IP Active	Communicating C&C
	× 🗆	6/15/2020, 3:18:46.285 PM	alert []	{"EvidenceDetails":[{"Rule":"Current C&C Server","E	videnceString":"8 C4829704-0EDC-4C3D-A34	-7C4A67586F3C 452745dc-5419-419e-9158-c	339c376aa58 95	Recorded Future IP Active	Communicating C&C
		Tenantid 8/8c75c1-b994-4c73-bb0c-17334/594bd9							
	TimeGenerated [UTC] 2020-06-1515:18-46.285Z SourceSystem SecurityGraph								
		Action	alert						
		ActivityGroupNames [
	AdditionalInformation ["EvidenceDetails": "["Rule": "Current C&C Server", "EvidenceString": 8 sightings on I source: Recorded Future Command & Control List. Command & Control Nov 25, 2019.", "CriticalityLabel": "Very Malicious," Timestamp": 1574559027107, "CriticalityLabel": "Very Malicious," Timestamp: 157459027107, "CriticalityLabel": "Very Malicious," Timestamp: 1574559027107, "CriticalityLabel": "Very Malicious," Timestamp: 15745590271							np":1574659027107,"Criticality":4},{"	'Rule":"Actively Communicating
	Applicational C482704-0EDC-4C3D-A347-7C4A6758693C Azure Tenantid 4527456c-5419-4198-9158-c339c376aa58 ConfidenceScore 95								
		Description	95 Recorded Future IP Active Communicati	ng (%)					
		Description	Recorded Future in Active Communication	ng cac					

Recorded Future's integration with Microsoft Azure enables Recorded Future risk lists to detect threats found within internal logs in Microsoft Azure Sentinel.



www.recordedfuture.com

@RecordedFuture

About Recorded Future

Recorded Future delivers security intelligence to amplify the effectiveness of security and IT teams by informing decisions in real time with contextual, actionable intelligence. By analyzing data from open, dark, and proprietary sources, Recorded Future offers a singular, integration-ready view of threat information, risks to digital brand, vulnerabilities, third-party risk, geopolitical risk, and more.

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