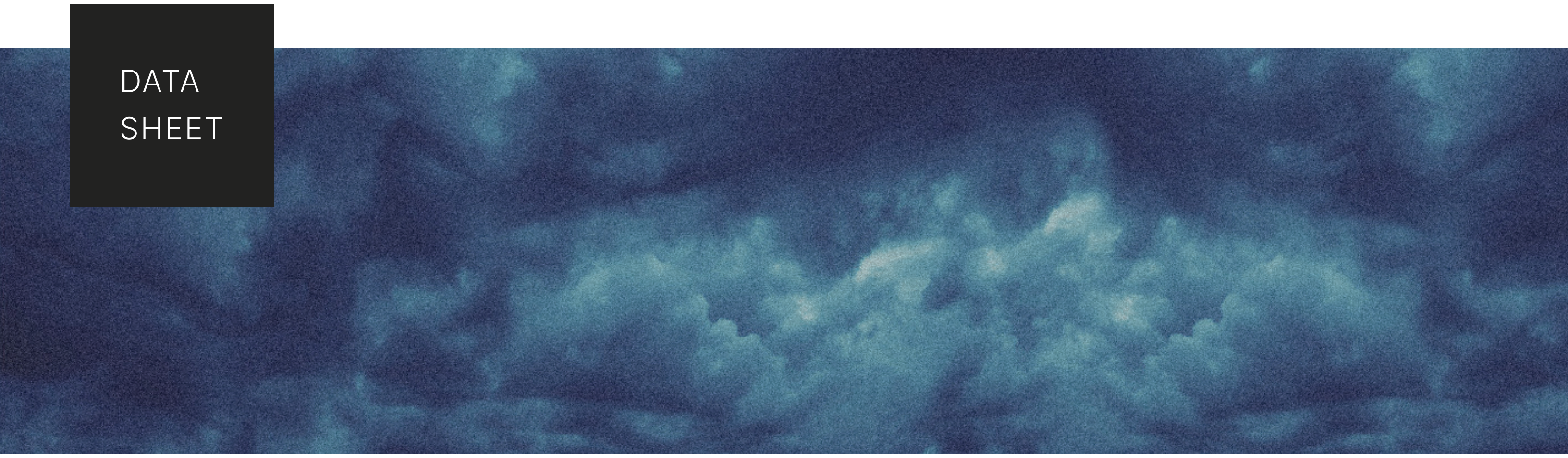
DATA SHEET



Recorded Future for Microsoft Sentinel

BENEFITS

- Automatically detect risky IOCs in your environment
- Triage alerts faster with elite, real-time intelligence
- Respond quickly with transparency and context around internal telemetry data
- Maximize your investment in Microsoft Sentinel

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 tiIndicators for native leverage
- Incident enrichment via dedicated Connector Actions and unprecedented intelligence from Recorded Future

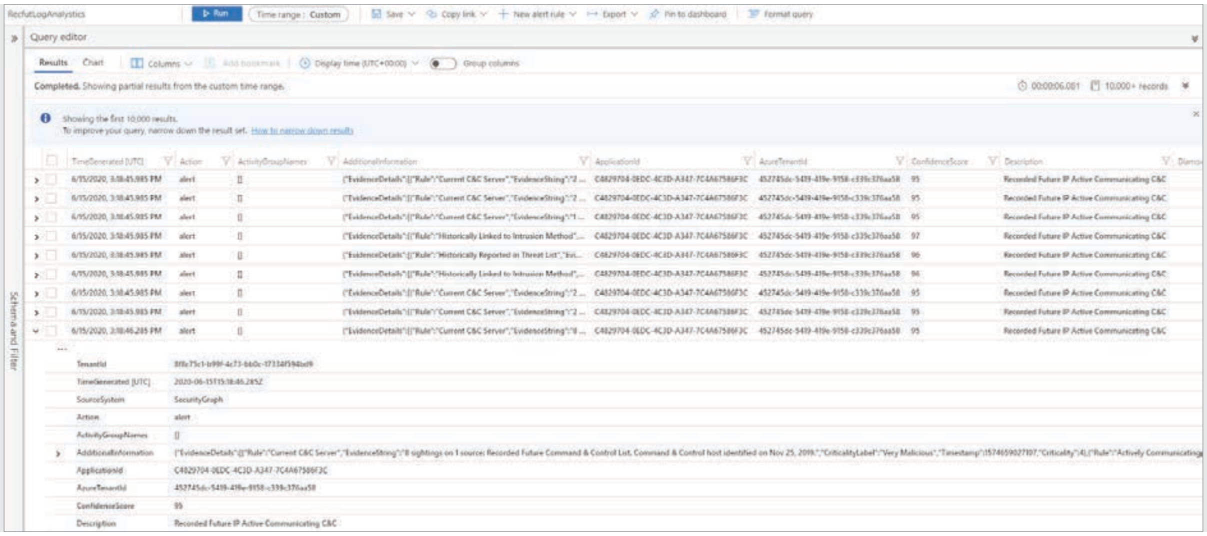
As the attack surface grows, security teams are seeing more and more events each day. However, with too little time and not enough context on the activity in their cloud environment, there's no way to connect the dots between data in Microsoft Sentinel and the external risk of any detected threats. This 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 Sentinel environment. This data is delivered 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

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 Sentinel. This provides analysts with visibility into technical indicators — and empowers them to make prioritization decisions based on a real-time Recorded Future risk score that is backed by transparent evidence.



Completed. Showing partial results from the custom time range.

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	ActivityGroupNames	AdditionalInformation	ApplicationId	AzureTenantId	ConfidenceScore	Description	Diamo
6/15/2020, 3:18:45.985 PM	alert	[]	{"EvidenceDetails":[{"Rule":"Current C&C Server","EvidenceString":"2 ...	C4829704-0EDC-4C3D-A347-7C4A67586F3C	452745dc-5419-419e-9158-c339c376aa58	95	Recorded Future IP Active Communicating C&C	
6/15/2020, 3:18:45.985 PM	alert	[]	{"EvidenceDetails":[{"Rule":"Current C&C Server","EvidenceString":"2 ...	C4829704-0EDC-4C3D-A347-7C4A67586F3C	452745dc-5419-419e-9158-c339c376aa58	95	Recorded Future IP Active Communicating C&C	
6/15/2020, 3:18:45.985 PM	alert	[]	{"EvidenceDetails":[{"Rule":"Current C&C Server","EvidenceString":"1 ...	C4829704-0EDC-4C3D-A347-7C4A67586F3C	452745dc-5419-419e-9158-c339c376aa58	95	Recorded Future IP Active Communicating C&C	
6/15/2020, 3:18:45.985 PM	alert	[]	{"EvidenceDetails":[{"Rule":"Historically Linked to Intrusion Method",...	C4829704-0EDC-4C3D-A347-7C4A67586F3C	452745dc-5419-419e-9158-c339c376aa58	97	Recorded Future IP Active Communicating C&C	
6/15/2020, 3:18:45.985 PM	alert	[]	{"EvidenceDetails":[{"Rule":"Historically Reported in Threat List","Evi...	C4829704-0EDC-4C3D-A347-7C4A67586F3C	452745dc-5419-419e-9158-c339c376aa58	96	Recorded Future IP Active Communicating C&C	
6/15/2020, 3:18:45.985 PM	alert	[]	{"EvidenceDetails":[{"Rule":"Historically Linked to Intrusion Method",...	C4829704-0EDC-4C3D-A347-7C4A67586F3C	452745dc-5419-419e-9158-c339c376aa58	94	Recorded Future IP Active Communicating C&C	
6/15/2020, 3:18:45.985 PM	alert	[]	{"EvidenceDetails":[{"Rule":"Current C&C Server","EvidenceString":"2 ...	C4829704-0EDC-4C3D-A347-7C4A67586F3C	452745dc-5419-419e-9158-c339c376aa58	95	Recorded Future IP Active Communicating C&C	
6/15/2020, 3:18:45.985 PM	alert	[]	{"EvidenceDetails":[{"Rule":"Current C&C Server","EvidenceString":"2 ...	C4829704-0EDC-4C3D-A347-7C4A67586F3C	452745dc-5419-419e-9158-c339c376aa58	95	Recorded Future IP Active Communicating C&C	
6/15/2020, 3:18:46.285 PM	alert	[]	{"EvidenceDetails":[{"Rule":"Current C&C Server","EvidenceString":"8 ...	C4829704-0EDC-4C3D-A347-7C4A67586F3C	452745dc-5419-419e-9158-c339c376aa58	95	Recorded Future IP Active Communicating C&C	

TenantId	8f8c75c1-b99f-4c73-bb0c-17334f594bd9
TimeGenerated [UTC]	2020-06-15T15:18:46.285Z
SourceSystem	SecurityGraph
Action	alert
ActivityGroupNames	[]
AdditionalInformation	{"EvidenceDetails":[{"Rule":"Current C&C Server","EvidenceString":"8 sightings on 1 source: Recorded Future Command & Control List. Command & Control host identified on Nov 25, 2019.","CriticalityLabel":"Very Malicious","Timestamp":1574659027107,"Criticality":4},{"Rule":"Actively Communicating
ApplicationId	C4829704-0EDC-4C3D-A347-7C4A67586F3C
AzureTenantId	452745dc-5419-419e-9158-c339c376aa58
ConfidenceScore	95
Description	Recorded Future IP Active Communicating C&C

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

Results*

Resolve Security Threats 63% Faster

Relevant insights, updated in real time, and integrated with Microsoft Sentinel 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, *Organizations React to Security Threats More Efficiently and Cost Effectively with Recorded Future*

ABOUT RECORDED FUTURE

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

www.recordedfuture.com   @RecordedFuture