

# **Recorded Future Integration with Microsoft Defender for Endpoint**

#### **BENEFITS**

- Proactively blocking of threats
   before they impact the business
- Continuous threat protection, by automatically keeping your Microsoft Defender for Endpoint instance updated with the latest security intelligence
- Maximize your investment in Microsoft Defender for Endpoint by utilizing your Microsoft Sentinel Services

#### **KEY FEATURES**

- Real-time intelligence on known
   Command and Control servers and
   recently weaponized domains
- Out-of-the-box integration for delivering indicators to Microsoft Defender for Endpoint

This integration requires the organization to have a Microsoft Sentinel account with the Microsoft Sentinel application enabled The ever-growing number and dynamic nature of threats make it extremely difficult to identify, triage, and prevent attacks. There's just too much information to analyze, too many security controls to update, and too little visibility to threat activity outside of your organization.

Recorded Future helps security teams reduce their risk exposure by collecting, analyzing, and delivering actionable security intelligence. With this integration, high confidence indicators are automatically sent to Microsoft Defender for Endpoint, so that security teams can proactively protect their organizations from emerging threats.

### **Proactive Threat Prevention**

Recorded Future continuously monitors hundreds of thousands of open, closed, and technical sources to determine where emerging threats are coming from. This security intelligence, in the form of high risk IP addresses and domains, can be automatically and continuously delivered into Microsoft Defender for Endpoint, formerly known as Microsoft Defender ATP, for alerting and blocking suspect network traffic. As a result, endpoints and their corresponding users will be automatically protected from malicious sites and potential damage to their organization.

The Recorded Future integration with Microsoft Defender for Endpoint provides out-of-the-box protection against known high risk Command and Control IP addresses, as well as newly registered domains that appear to have been weaponized. This is accomplished through Microsoft Sentinel Logic Apps, and relies on the Threat Intelligence capabilities of Microsoft Sentinel to deliver the indicators of compromise into the Defender for Endpoint indicator repository in real time.

## ·III Recorded Future®

⑦         Recurrence	ce	05	
Recorded Future - C2 IP download	0s	Recorded Future - Weaponized Domains download	2
$\downarrow$			
Parse JSON 2	0s	(e) Parse JSON	4
$\downarrow$			
Filter array 2	0s	(v) Filter array	2
$\downarrow$		↓ ·	
Send IPs to Defender	9s	Send Domains to Defender	
RecordedFuture-ImportToMGS 2	0s	RecordedFuture-ImportToMGS	0
IP Count	0s	(2) Domain Count	1
	0s	Domain Count      INPUTS      Show raw in	
INPUTS Show	raw inputs 🗲	INPUTS Show raw in Inputs	puts >
INPUTS Show	raw inputs 🗲	INPUTS Show raw in	puts >
INPUTS Show Inputs 387 - Number of C2 IPs sent to Microsoft Defender for Endpoi	raw inputs 🗲	INFUTS Show new in Inputs (463) - Number of weaponized domains sent to Nicrosoft Defender fo	puts > r Endpo
INPUTS Show Inputs 387 - Number of C2 IPs sent to Microsoft Defender for Endpoi	r raw outputs	INPUTS Show new in Inputs 4653 - Number of weaponized domains sent to Microsoft Defender fo	puts >

The integration uses a Microsoft Sentinel logic app to deliver high confidence indicators to Microsoft Defender for Endpoint, via the Microsoft Graph Security.

🖲 🔍 💿 indicators - Microsof	1 365 MC						•
iii Microsoft 365 security							
=		1547 (MARRIED)			_		ŶΨ×
<ul> <li>Home</li> <li>Incidents &amp; alerts</li> </ul>	~	Settings > Indusints				URL	
D Hunting	-	Endpoints			_	🛞 Open page 🔋 Delete	
Action center		Permission			_		
🕙 Dreat analytics		Roles	Indicators			Indicator defails	^
Secure score		Device groups	Available capacity: \$040/15000 indica	ron	_	Created by Domain	
🖗 Learning hab			File hathes IP addresses UR	Automains Certificate	8	Expires on May 2, 2021	
Endpoints		APtz	Participanti and an and a second			(utc)	
D Search		SHM	• Network protection custom feed is of	A To block specified IF address, 1	Upmains, or LELL Automation		
			1 Export () Import + Add	item	_	Response Action	0
Device Inventory		Rales	V URL/Domain	Application	Actor A	O Atow	
4 Vulnerability management	~	Custom dirtections	(A) (ADDRESS	Cardinates .	Alert and plock	O Alert only	
• Partners and APIs	~~~	Alert supprension	0		Ken and pipels	Alert and block	
Evaluation & tutorials	2	Indicators	•		1000100000	Alert sile *	
Configuration management		Process Methory Indicators			Alert and block	Indextor	
Imail & collaboration		Automation upleads			Alertand block in	Alert severity *	
		Automation fulder exclusions			Alert and block		
Submissions		And in the second se			Alert and Block	Category	
Acces		Device management			Alert and block	Description *	
🕰 Policies (k rules		Onboarding			Alertand Stock	Weaponind Domain	
< Reports		Offboarding			Aletand block		(C)
© Health		Contraction of the second			Alert and Stock	Sam	

Recorded Future indicators appear in Microsoft Defender for Endpoint and are preconfigured for "Alert and Block"

#### 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

