Recorded Future®

DATA SHEET

Recorded Future® Integration with Microsoft Defender for Endpoint

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 Logic Apps to deliver indicators of compromise into the Defender for Endpoint indicator repository.

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 Azure Logic Apps

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 an Azure Logic Apps subscription and a connection to the Microsoft Graph Security API

Results*

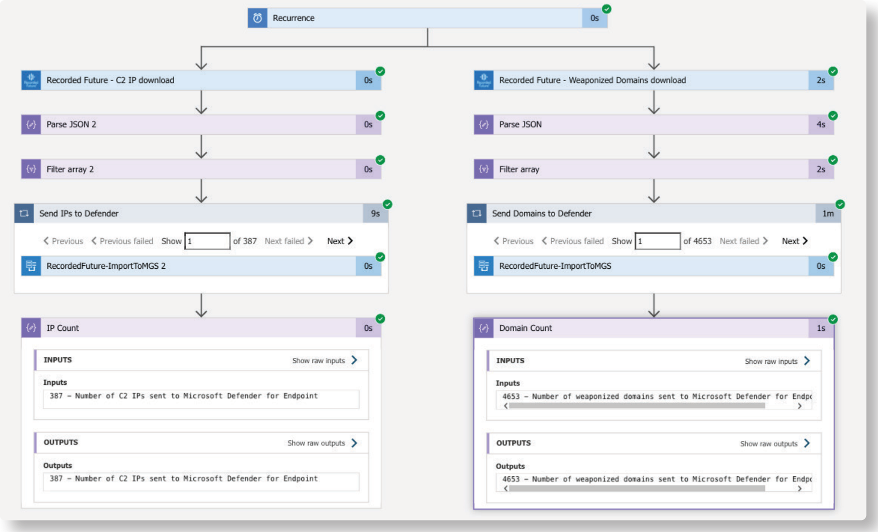
Identify 22% more security threats before impact

Recorded Future continuously monitors hundreds of thousands of open, closed, and technical sources to determine where emerging threats

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*


Recurrence 0s
Recorded Future - C2 IP download 0s
Parse JSON 2 0s
Filter array 2 0s
Send IPs to Defender 9s
< Previous < Previous failed Show 1 of 387 Next failed > Next >
RecordedFuture-ImportToMGS 2 0s
IP Count 0s
Recorded Future - Weaponized Domains download 2s
Parse JSON 4s
Filter array 2s
Send Domains to Defender 1m
< Previous < Previous failed Show 1 of 4653 Next failed > Next >
RecordedFuture-ImportToMGS 0s
Domain Count 1s
Show raw inputs >
Show raw outputs >

INPUTS

Inputs

```
387 – Number of C2 IPs sent to Microsoft Defender for Endpoint
```

OUTPUTS

Outputs

```
387 – Number of C2 IPs sent to Microsoft Defender for Endpoint
```

INPUTS

Inputs

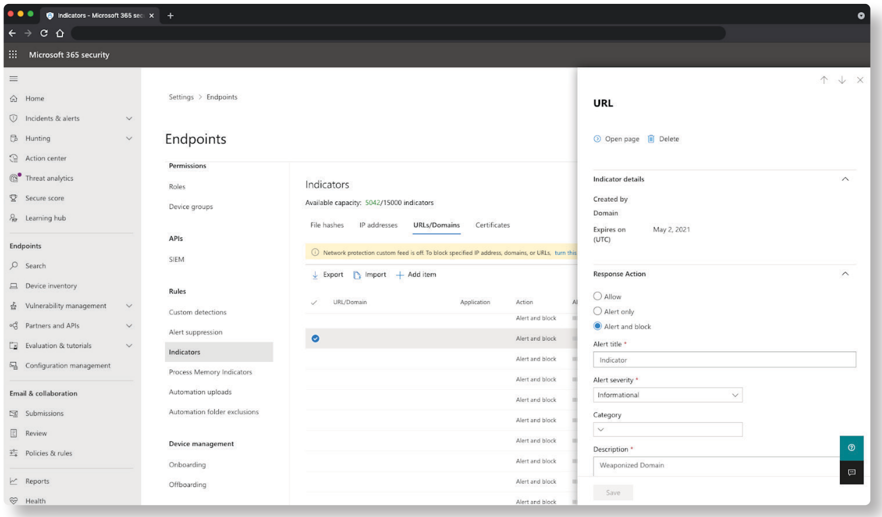
```
4653 – Number of weaponized domains sent to Microsoft Defender for Endpc
```

OUTPUTS

Outputs

```
4653 – Number of weaponized domains sent to Microsoft Defender for Endpc
```

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



Endpoints

Indicators

Available capacity: 5042/15000 indicators

Network protection custom feed is off. To block specified IP address, domains, or URLs, turn this

URL/Domain	Application	Action
		Alert and block
		Alert and block
		Alert and block
		Alert and block
		Alert and block
		Alert and block
		Alert and block
		Alert and block
		Alert and block
		Alert and block

URL

Indicator details

Created by

Domain

Expires on (UTC) May 2, 2021

Response Action

○ Allow
○ Alert only
● Alert and block

Alert title * Indicator

Alert severity * Informational

Category

Description * Weaponized Domain

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 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 1,700 businesses and government organizations across more than 75 countries.

www.recordedfuture.com @RecordedFuture