Recorded Future®

Collective Insights for Microsoft Defender

Data Privacy & Security Overview

What Data is Collected?

The integration is designed with a policy of data minimization, collecting only the necessary metadata from your Microsoft Defender services

- **Read-Only Access:** The integration uses **read-only permissions** in your Microsoft environment (`SecurityAlert.Read.All`). It cannot make any changes to your systems.
- **Specific Fields:** The connector collects only the following incident metadata from the Microsoft Defender suite:
  - `createdDateTime`: The time the incident was created.
  - `title`: The title of the incident.
  - `Id`: The unique ID of the incident.
  - `serviceSource`: The Defender tool the incident originated from.
  - `detectionSource`: The technology or sensor that identified the activity.
  - `mitreTechniques`: Associated TTPs for the incident.
  - `IOC type` and `IOC value`: The indicator type and value (e.g., hash, IP, URL).
- **No Sensitive Content:** The integration **does not** collect or store sensitive file contents, user data, or Personally Identifiable Information (PII).

How is your Data Secured?

We employ a multi-layered security strategy to protect your data, which is stored and processed within our secure Intelligence Cloud Platform, hosted on Amazon Web Services (AWS).

- **Encryption:** All of your data is encrypted both in transit and at rest.
  - **In Transit:** We use Transport Layer Security (TLS) 1.2 or higher.
  - **At Rest:** We use Advanced Encryption Standard (AES) 256-bit encryption.
- **Access Control:** Access to customer data is strictly limited to authorized personnel with a valid business purpose. We enforce role-based access with hardware token-based multi-factor authentication for production infrastructure. All access is extensively logged and audited.

Secure & Minimized Data Collection

- Integration uses read-only API permissions
- Only security event metadata is collected, not sensitive content
- Data is encrypted in transit using TLS 1.2+

Private & Anonymized Data Usage:

- Your data powers your private Collective Insights dashboards and other Recorded Future features
- Metadata is anonymized for platform and product improvement
- Collected metadata is encrypted at rest using AES-256

- **Vulnerability Management:** Our platform is continuously monitored. We conduct regular external penetration tests and run a robust Bug Bounty Program managed by HackerOne to identify and remediate potential vulnerabilities.

How Is Your Data Used?

Your data is used for two primary purposes, with strict privacy controls in place.

1. **To Power Your Collective Insights:** The collected metadata is used to provide the service directly to you. This includes generating your organization's unique Detection Trends dashboards, MITRE ATT&CK® heatmaps, and custom reporting.
2. **To Improve Our Intelligence:** We use **unattributed and anonymized** customer data to improve our products and services. This metadata, once stripped of any identifying customer information, helps our research teams identify broader threat trends and enhance our detection capabilities for all clients. Your data is never shared with third parties in an attributable form.

Our Commitment to Compliance and Trust

Recorded Future's security and privacy programs are validated by rigorous third-party audits and certifications to ensure we adhere to the highest global standards. Our certifications include:

- **SOC 2 Type 2** and **SOC 3**
- **ISO 27001** (Information Security Management)
- **ISO 27701** (Privacy Information Management)
- **ISO 9001** (Quality Management)
- **NIST 800-218** and **NIST 800-200** Frameworks
- **GDPR** Compliance

For additional details, please see: https://www.recordedfuture.com/legal/faq