Please use the email template below to request the API token from the internal team that manages your EDR. Simply copy the text into a new email, fill in any bracketed details, make any other necessary edits, and send it to the appropriate contact / distribution list.

Subject: Request: Microsoft Defender Read-Only API Key Generation for Recorded Future Integration

Hi Team,

I am requesting your assistance to enable a high-value feature within our Recorded Future platform called **Collective Insights®**. This feature is included in our current license at no additional cost.

What is the Goal?

The purpose is to connect our security tools (starting with our EDR) to Recorded Future's intelligence. This will give our security team a unified view of threats and help us:

- **Uncover stealthy threats** potentially missed by Microsoft Defender's native detection engine.
- **Automate MITRE ATT&CK® heatmaps** to visualize the specific adversary tactics being used against our environment.
- **Generate summary reports** across our entire security stack to save analysis and reporting time.

What is Needed from You?

To enable this, we need a **read-only** API token generated from our SentinelOne instance.

How to Generate the Token:

Recorded Future has provided a step-by-step video walkthrough guide for this process and it should take less than 15 minutes to complete.

- **Link to Instructions:** https://reachsuite.app/go/exp-7ecd314e

Security & Data Privacy: (Follow link for detailed PDF)
https://support.recordedfuture.com/hc/en-us/article_attachments/44049994449299

- **Permissions:** The API key only requires **read-only** access. It has no write or administrative privileges.
- **Data Scope:** The integration ingests detection **metadata** only (e.g., timestamps, process names, file hashes, command lines). It **does not** access or ingest sensitive file contents, user data, or other forms of Personally Identifiable Information (PII).

- **Platform:** All data is securely transmitted, processed, and stored within our dedicated Recorded Future instance.

Next Steps:

Once the API token is generated, please securely provide it to me so I can complete the configuration within the Recorded Future platform.

Please let me know if you have any questions or concerns that I can relay back to our Recorded Future contacts.