

Microsoft Defender

Microsoft Defender → Coralogix Via Azure Event Hubs

At a glance (architecture)

- Microsoft Defender (Defender for Cloud and/or Defender XDR / Endpoint)
- → **Azure Event Hubs** (central streaming bus)
- → **Azure Function (Event Hub trigger)** using Coralogix template
- → **Coralogix** (logs/alerts analytics)

Prerequisites

- Azure subscription with permission to:
 - Create & configure **Event Hubs** namespace/event hub
 - Configure **Defender** export (Defender for Cloud and/or Defender XDR)
 - Deploy **Azure Functions** from template

Step 1 — Create Event Hubs namespace & event hub

1. In Azure Portal → **Event Hubs** → + **Create** namespace.
 - Pricing tier: **Standard** (recommended)
 - Throughput units: start with **1** (scale later)
 - Networking: public or private as per policy
2. Inside the namespace → + **Event Hub**
 - Name: `defender-stream`
 - Partitions: **2-4** (scale with volume)
 - Message retention: 1-7 days (align to recovery needs)
3. Create a **Shared access policy** with **Listen** rights (for the Function) and copy the connection string.

Step 2 — Export from Defender for Cloud → Event Hubs

Use **Continuous export** to stream alerts and recommendations.

1. Azure Portal → **Defender for Cloud** → *Environment settings* → choose subscription.

Microsoft Azure

Search resources, services, and docs (G+/I)

Copilot

Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Environment settings

Showing 2 subscriptions

Search

+ Add environment | Refresh | Create custom recommendation | Guides & Feedback | Cost calculator | Defender Plans Coverage

You may be viewing limited information. To get tenant-wide visibility, click here →

Azure subscriptions: 0
AWS accounts: 0
GCP projects: 0
GitHub connectors: 0
AzureDevOps connectors: 0

0 Total issues

GCP Projects 0 | AWS Accounts 0 | AzureDevOps ADO 0

Search by name

Environments == All | Standards == All | Coverage == All | Connectivity status == All

Collapse all

Name ↑↓	Total resources ↑↓	Connectivity status
▼ Azure		
▼ Tenant Root Group (1 of 1 subscriptions)	4	
▼ Coralogix-CSP	4	
EventHub-dugotjq3jmjy6		
EventHub-oinvnb2wkyyqg		
Coralogix-CSP 2		

Microsoft Azure

Search resources, services, and docs (G+/I)

Copilot

Home > Microsoft Defender for Cloud | Environment settings > Settings

Settings | Continuous export

Coralogix-CSP

Search

Save

Settings

Defender plans

Security policies

Email notifications

Workflow automation

Continuous export

Continuous export

Configure streaming export setting of Defender for Cloud data to multiple export targets. Exporting Defender for Cloud's data also enables you to use experiences such as integration with 3rd-party SIEM and Azure Data Explorer. [Learn More >](#)

Event hub Log Analytics workspace

Export enabled ☒ On ☐ Off

Exported data types

☒ Security recommendations All recommendations selected

Recommendation severity * Low,Medium,High

Include security findings ☒ Yes

☒ Secure score Overall score,Control score

Controls All controls selected

☒ Security alerts Low,Medium,High,Informational

Continuous export → + Add export

1. **Export target: Azure Event Hubs**
2. **Data types:** select **Security alerts** and/or **Security recommendations** (add resource state changes if needed)
3. **Event Hub:** choose your namespace and the `defender-stream` hub
4. Save.

Resulting payloads: JSON per alert/recommendation with keys such as `alertId`, `severity`, `resourceId`, `description`, `compromisedEntity`, `tactics`, `firstSeen`, `lastSeen`.

Step 3 — Deploy the Coralogix Azure Function (Event Hub → Coralogix)

We'll use Coralogix's ARM template to create a Function App that triggers on your Event Hub and forwards events to Coralogix.

1. Open the Coralogix **Azure Functions** deployment link (ARM template).

Learn more about Coralogix ARM in our [documentation](#).

1. Fill parameters:
 - **EventHub connection string** (with `Endpoint=...;EntityPath=defender-stream` or supply hub name separately if template asks)
 - **Consumer group**: `$Default` or a dedicated `coralogix-cg`
 - **CORALOGIX_PRIVATE_KEY**: from Coralogix UI → Data Ingestion
 - **CORALOGIX_REGION**: e.g., `EU1`, `AP1`, `US1` (exact value per account)
 - **APPLICATION_NAME**: e.g., `microsoft-defender`
 - **SUBSYSTEM**: e.g., `alerts` or `xdr-events`
 - (optional) **COMPANY_ID** if required by your region
2. **Plan**: Consumption or Premium (P1 for high throughput). Enable **Always On** if using Premium.
3. **Networking**: if Event Hub is private, integrate the Function with the VNet and grant access.
4. Deploy. Confirm the Function is bound to the Event Hub trigger.

Step 4 — Validate ingestion in Coralogix

- In Coralogix → **Logs** → filter by `application:microsoft-defender`.
- You should see JSON logs arriving within a minute of new alerts/events.
- Example search (Lucene):
 - `severity:High AND (tactics:CredentialAccess OR tactics:DefenseEvasion)`

Support

Need help?

Our world-class customer success team is available 24/7 to walk you through your setup and answer any questions that may come up.

Feel free to reach out to us **via our in-app chat** or by sending us an email to support@coralogix.com.

 Last updated: October 9, 2025

Was this helpful?

Leave your feedback here.

☐ **Yes** ☐ **No**

Send

© 2025 Coralogix. All rights reserved.

Generated on: November 20, 2025

Source: <https://coralogix.com/docs/integrations/security/microsoft-defender/>