Connecting ESET PROTECT to Microsoft Sentinel

Mitchell | ESET Nederland - 2025-04-16 - Comments (0) - ESET PROTECT On-prem

The added value

ESET PROTECT is an XDR cybersecurity platform that combines next-gen prevention, detection, and proactive threat-hunting capabilities. ESET's highly customizable solutions include local support and have minimal impact on performance, identify and neutralize known and emerging threats before they can be executed, support business continuity, and reduce the cost of implementation and management.

ESET Cloud Office Security provides advanced protection for Microsoft 365 and Google Workspace apps against malware, spam or phishing attacks with ultimate zero-day threat defense.

Integrating the ESET PROTECT Platform with Microsoft Sentinel empowers users to efficiently monitor and manage threat detections while enhancing overall organization security. The ESET PROTECT Platform data connector uses Azure Functions to connect to the ESET PROTECT, ESET Inspect and ESET Cloud Office Security via ESET Connect API to pull detection logs into Microsoft Sentinel.

Integration type

- Combination of the log-based and API-based integration

How to enable the integration

The ESET PROTECT Platform solution takes a dependency on the following technologies:

- Logs Ingestion API in Azure Monitor
- Azure Functions

Important

Pulling detection logs from the ESET PROTECT Platform into Microsoft Sentinel using Azure Functions can result in additional data ingestion costs. See the details on the Azure Functions pricing page.

Ensure you have the required permissions and follow the configuration steps below.

Required permissions

- Read and write permissions on the Azure Log Analytics workspace.
- Read permissions to shared keys for the Azure Log Analytics workspace. See the documentation about the workspace keys.
- Read and write permissions on Azure Functions to create a Function App. See the documentation about Azure Functions.
- Sufficient permissions to register an application with the Microsoft Entra tenant.
- Permission to assign the Monitoring Metrics Publisher role to the registered application in Microsoft Entra ID.

Configuration steps

1. Create an ESET Connect API User account.

2. Create a Microsoft Entra ID registered application by following the steps in the Register a new application instruction.

3. Install the ESET PROTECT Platform connector from the Azure Marketplace or the Azure portal. When installed, select the ESET PROTECT Platform data connector in Azure Portal > Configuration > Data Connectors > ESET PROTECT Platform data connector and click Open Connector Page.

4. Deploy the ESET PROTECT Platform data connector using the Azure Resource Manager template; on the ESET PROTECT Platform data connector page, click Deploy to Azure. The system will redirect you to the customized template page.

5. Complete the Project details and Instance details fields:

    1. Subscription—Your Azure subscription.

    2. Resource group—Your previously created Resource group. It must be the same as your Log Analytics workspace Resource group.

    3. Region—The location of your previously created Resource group. This field is automatically populated when you select the Resource group.

    4. Workspace Name—The name of your Log Analytics workspace associated with your Microsoft Sentinel instance.

    5. Table Name—The name of the table that will store the detection logs data after the deployment. This field is pre-defined for you. It is recommended to keep the default Table Name, as features like the parsing function use it.

    6. Data Collection Endpoint Name—The name of the data collection endpoint. This field is pre-defined for you.

    7. Data Collection Rule Name—The name of the collection rule. This field is pre-defined for you.

    8. Application Name—The name of the Azure Function App that will be created as a result of the deployment. The name must be unique. Therefore, the system will add additional characters from your Resource group ID to the name you provide to ensure its uniqueness.

    9. Application Run Interval—The time interval (in minutes) for the application to run and pull the detections. This field is pre-defined for you, but you can select a different option.

    10. Object ID—The Object ID of the registered application in Microsoft Entra ID. To get the required Object ID value, follow this path: Azure Portal > Microsoft Entra ID > Manage menu option > Enterprise applications > the value in the Object ID column next to your registered application name.

    11. Azure Client ID—The Application (client) ID of the registered application in Microsoft Entra ID.

    12. Azure Client Secret—The Client Secret of the registered application in Microsoft Entra ID.

    13. Azure Tenant ID—The Directory (tenant) ID of the registered application in Microsoft Entra ID.

14. Login—The ESET Connect API user login username obtained in step one.

15. Password—The ESET Connect API user password obtained in step one.

16. ESET PROTECT instance—The ESET product that Microsoft Sentinel uses to gather detection data. The available options are Yes/No; Yes is set by default, but you can change it. You can select more than one ESET product if they are located in the same region.

17. ESET Inspect instance—The ESET product that Microsoft Sentinel uses to gather detection data. The available options are Yes/No; No is set by default, but you can change it to Yes if you have an ESET Inspect instance and it is located in the same region as your other ESET instances.

18. ESET Cloud Office Security instance—The ESET product that Microsoft Sentinel uses to gather detection data. The available options are Yes/No; No is set by default, but you can change it to Yes if you have an ESET Cloud Office Security instance and it is located in the same region as your other ESET instances.

19. Instance Region—The location of your ESET PROTECT/ESET Inspect/ESET Cloud Office Security instance.

20. Key Base—This field is pre-defined for you; do not change it.

6. Click Review + create to validate your configuration, then click Create to finalize it.

The new Function App will be created when the configuration and deployment are finished. The app will pull the detections data from the ESET PROTECT Platform and push it to Microsoft Sentinel.

Integration verification

To verify the integration and review the detection logs:

1. Go to Azure Portal > Microsoft Sentinel > your Log Analytics workspace > General > Logs.

2. Select the table created during deployment. The table will store detections pulled from the ESET PROTECT Platform and their details.