Pathlock Cloud - Event Logging Solution

Purpose

This document is intended for Pathlock Cloud customers. It provides detailed instructions for installing and using the Sentinel Connector. By following the steps outlined here, you can seamlessly ingest Pathlock Cloud event logs into Microsoft Sentinel, enabling advanced analysis and threat detection.

Overview

This solution provides a comprehensive framework for collecting, analyzing, and visualizing event logs from Pathlock Cloud Application. It ingests PLC event data into a custom log table in Microsoft Sentinel, enabling security teams to monitor application activity and detect security threats and anomalies..

Key Features

- **Custom Log Ingestion**: Ingests PLC event data into a custom log table in Microsoft Sentinel using a dedicated Data Collection Endpoint (DCE) and Data Collection Rule (DCR).
- **Advanced Threat Detection**: Enables security teams to analyze user and application event logs to identify and investigate a wide range of security risks and behavioral anomalies.
- **Intuitive Visualization**: Includes a pre-built workbook to visualize PLC event data for advanced analysis and informed incident response.
- **Seamless Integration**: Designed to work with the Pathlock Cloud Solution to easily collect and forward event logs to your Sentinel workspace.

Prerequisites

Before deploying this solution, ensure you have the following:

- **Pathlock Cloud Solution**: Pathlock Cloud integrates with Sentinel to log the event information. This is an external dependency and is not included in this solution package. You must have a Pathlock Cloud license and access to the Pathlock Cloud application.
- **Connector Configuration**: You must configure the Sentinel Connector in Pathlock Cloud application to send event logging information to Sentinel.

  Learn More:

  ```
     - Pathlock cloud Sentinel connector implementation documentation:
  https://help.pathlock.com/pathlock-cloud-documentation/pathlock-cloud/integrations/microsoft-sentinel
  ```

- **Registering a client application for integration**:

  - Sign in to the Microsoft Azure admin center https://portal.azure.com/#home
  - If you have access to multiple tenants, use the Settings icon in the top menu to switch to the tenant in which you want to register the application from the Directories + subscriptions menu.
  - Click on App registrations and select New registration.
  - Enter a display Name for your application.
  - Choose an option for Specify who can use the application in the Supported account types section.
  - Don't enter anything for Redirect URI (optional).
  - Select Register to complete the initial app registration.
  - When registration finishes the Microsoft Azure admin center displays the app registration's Overview pane. On this page the app was assigned values for the Application (client) ID and Directory (tenant) ID. Copy and securely save these values.

- **Create a client secret**:

  - Select Certificates and secrets > Client secrets tab.
  - Click New client secret button.
  - Enter a description and set the Expiry days/months.
  - Click Add button and Copy the secret from 'Value' column. This is the Application (client) secret. Copy and securely save the secret.

- **Assign Permissions to the client application**:

  - Select API permissions > Add permission > Azure Service Management > Delegated permissions
  - Select these permissions
    - user_impersonation
  - Click Add permissions.
  - Click the 'Grant admin consent for [your tenant]' button and then click Yes to finish.

- **Create a resource group**:

  - Sign in to the Microsoft Azure admin center https://portal.azure.com/#home
  - Click on + Create
  - Search for Resource groups in the search bar at the top type Resource groups and select it.
  - Click on Create
  - Fill in Details
    - Subscription Choose your active Azure subscription.
    - Resource group name e.g. plcsentinelrg
    - Region Choose the same region where your Log Analytics Workspace will be (e.g. East US)
    - Click Review + Create then Create.
  - Select the newly created Resource Group. You will be redirected to Overview page

Note:

```
    Make sure Monitoring Metrics Publisher and Log Analytics Contributor Access is
provided to the registered application.
    To provide access >
        - Click on Access Control (IAM).
        - Click on + Add > Add Role Assignment.
        - Select the role "Monitoring Metrics Publisher".
        - Click Next.
        - Select the radio button User, group, or service principal.
        - Click on +Select Members.
        - Search by application name (See → [*Registering a client application for integration*](#registering-a-client-application-for-integration) section.)
        - Select the application.
        - Click Review + assign.
        - Repeat these steps for the next role (Log Analytics Contributor)
```

- **Log Analytics Workspace**: An active Microsoft Sentinel workspace with the required permissions.
    - Go to Azure Portal https://portal.azure.com/#home
    - Search for Log Analytics workspaces Click on Log Analytics workspaces
    - Click + Create
    - Fill in the Workspace Details
        - Subscription Select your Azure subscription
        - Resource Group Use existing (e.g.plcsentinelrg)
        - Region Match with your DCR/DCE (e.g. East US)
    - Note down Parent Management Group Value by clicking on Subscription link.
    - Click Review + Create
    - Click Create to deploy

- **Add Log Analytics Workspace in Microsoft Sentinel**:
    - Go to Microsoft Sentinel
    - Click on + Create
    - Search for Log Analytics workspace using Filter By Name.
    - Click on the created Log Analytics workspace.
    - Click on Add.

Deployment Instructions

This solution is deployed through a single ARM template that orchestrates the deployment of all necessary components.

- From the Microsoft Sentinel Content Hub, locate and select this solution.

- Click "Install" and follow the guided wizard.

- Enter the required parameters, such as the solution name and resource group location.

- Once the deployment is complete, navigate to your workspace to see the deployed components.

Configuration

After successful deployment, you must configure PLC connector to send data to your new Data Collection Endpoint.

- In your Azure portal, navigate to your deployed Data Collection Rule (DCR).

- Go to the "*Endpoints*" section to find the URI for your DCE.
- Locate the DCR's "*Immutable ID*" in the properties section.
- Use these two values to configure your third-party API as per its documentation. The API should be configured to send data to the DCE URI using the DCR's immutable ID.

Included Content

This solution package includes the following content:

- **Data Connectors**: A Data Collection Endpoint (DCE) and a Data Collection Rule (DCR) for custom log ingestion *(PLCSentinel-DCE.json, PLCSentinel-DCR.json)*
- **Workbooks**: A pre-built workbook for visualizing PLC event data *(PLCEventLoggingWorkbook.json)*.
- **Deployment Templates**: The *mainTemplate.json* and *createUiDefinition.json* files for guided deployment.
- **Documentation**: A comprehensive README.md file (this document) for guidance.

Data Schema

The solution ingests data into a custom log table. The schema of this table is defined in the DCR. For a detailed breakdown of the fields, please refer to the *PLCSentinel-DCR.json* file.

Troubleshooting

If you encounter issues during deployment or data ingestion, check the following:

- **Permissions**: Ensure your user account has the necessary permissions to deploy resources in the selected subscription.

Note:

```
    Make sure Monitoring Metrics Publisher and Log Analytics Contributor Access is provided to the registered application.
    To provide access >
        - Click on Access Control (IAM).
        - Click on + Add > Add Role Assignment.
        - Select the role "Monitoring Metrics Publisher".
        - Click Next.
        - Select the radio button User, group, or service principal.
        - Click on +Select Members.
        - Search by application name (See → [*Registering a client application for integration*](#registering-a-client-application-for-integration) section.)
        - Select the application.
```

```
          - Click Review + assign.
          - Repeat these steps for the next role (Log Analytics Contributor)
```

- **DCE/DCR Configuration**: Double-check that you have correctly copied the DCE URI and DCR Immutable ID when configuring your third-party API.
- **Note:**

  ```
    Click on Access Control (IAM). Make sure Log Analytics Contributor and
  Monitoring Metrics Publisher Access is inherited.
  ```

Support

For technical support and questions, please contact us at:

- **Email**: customersupport@pathlock.com
- **Link**: https://pathlock.com/support/