

**Azure Sentinel Playbook - Defender for IoT**

Block Azure IoT Hub Device Automation

Table of Contents

1. Getting Started
   * Prerequisites
   * Installation
2. Usage
3. Contact

**Getting Started**

Use the following steps to correctly configure Block-Hub-Device Automation in your Azure Sentinel instance

**Prerequisites**

These detections require you have Syslog data connector enabled and parser installed.

* Please refer to the data connector content here.
* Generate SAS token using Azure CLI

az iot hub generate-sas-token -n "MyHubName" --policy registryReadWrite

**Installation**

Block-Hub-Device can be used to **disable** device communication to Azure IoT Hub.

Graphical user interface, application

Description automatically generated

1. Download Block-Hub-Device.json file
2. Navigate to Azure-> [Deploy A Custom Template](https://portal.azure.com/#create/Microsoft.Template)
3. Click ‘Build your own template in the editor’ and upload json file
4. Provide the IoT Hub Name and SAS token generated in the Prerequisites section.
5. Click “Review and Create.”

Graphical user interface, text, application, email

Description automatically generated

1. After deployment navigate to Azure->Logic App->Block-Hub-Device to inspect the logic app created.

Graphical user interface, application, Teams

Description automatically generated

**Usage**

SOC can execute the Playbook on-demand from Azure Sentinel.

To run a playbook on-demand:

1. In the **Incidents** page, select an incident and click on **View full details**.
2. In the **Alerts** tab, click on the alert you want to run the playbook on, and scroll all the way to the right and click **View playbooks** and select **Block-Hub-Device** to **run** from the list of available playbooks on the subscription.

**Contact**

Email: [MicrosoftTeam@criticalstart.com](mailto:MicrosoftTeam@criticalstart.com)

**About**

Add Something Here