

**Azure Sentinel Analytics Rules - Defender for IoT**

Advance detection rules for Defender for IoT

Table of Contents

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

**Getting Started**

Use the following steps to correctly configure Defender for IoT detection rules 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.

**Installation**

1. Download analytics rules
2. Navigate to Azure Sentinel -> Analytics -> Import rules
3. Import all the provided rules

A screenshot of a computer

Description automatically generated with medium confidence

**Usage**

The rules will execute every 5mins against the previous 5mins data providing near real time detection and alerting.

**Contact**

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

**About**

Add Something Here