ESET Tech Center

Connecting ESET PROTECT to Microsoft Sentinel

Mitchell | ESET Nederland - 2023-03-23 - Reacties (0) - ESET PROTECT

Prerequisites:

- ESET PROTECT installed
- Microsoft Sentinel
- A Linux server

Deploy ESET PROTECT integration to Microsoft Sentinel

1. Navigate to Microsoft Sentinel > Content Hub
2. Search for ESET PROTECT
3. Select the ESET PROTECT integration by Cyber Defense Group B.V.
4. Click on “install”

5. Click “create” in the next window:

6. Select the appropriate Log Analytics workspace to deploy the integration to and click “review + create”

7. After the validation has passed, click “create” to start the deployment.

Configure ESET PROTECT to send events to Microsoft Sentinel

Install OMS-Agent

1. After deploying the solution you can find the “ESET PROTECT (Preview) Data Connector” in the Data connectors section:

2. After opening the connector page, you will find the instructions to install the Log Analytics agent, because Syslog is only collected by the Linux agent, you will have to install the agent on a linux machine. (for example, the ESET PROTECT Server)

3. Download & install the agent using the command provided:

4. After installing the agent the Agents management overview should report that 1 Linux computer is connected:

Configure OMS-Agent to collect syslog data

1. Open the Log Analytics workspace
2. navigate to “Legacy Agent Management” > Syslog
3. Click on “add facility”
4. select the facility name “user”
5. save the changes by clicking “apply”

6. Note: If you installed the OMS-agent on a different computer, you will need to do some additional config because the OMS agent only listens on 127.0.0.1 by default.

1. change the bind adress in the following file/etc/opt/microsoft/omsagent/conf/omsagent.d/syslog.conf

```
/etc/opt/microsoft/omsagent/conf/omsagent.d/syslog.conf

<source>
  type syslog
  port 25224
  bind 0.0.0.0
  protocol_type udp
  tag oms.syslog
</source>

<filter oms.syslog.**>
  type filter_syslog
</filter>
```

2. restart the agent

```
/opt/microsoft/omsagent/bin/service_control restart
```

Configure ESET PROTECT to export syslog data to the OMS Agent.

7. Login to ESET PROTECT
8. Navigate to more > Admin > Settings
9. Configure the syslog settings based on the screenshot below:

1. All ESET PROTECT event data should now be sent to Sentinel, you can generate some audit events by logging out and back in to ESET PROTECT for example. confirm that the events reached Sentinel by running the following query:

2. Alternatively you can open the workbook that was created after deploying the solution:

Enable analytics rules to create incidents from ESET detections

1. Navigate to Microsoft Sentinel > Configuration > Analytics
2. Select the 2 ESET analytic rules
3. Click “Enable”

4. Triggering threat detections will now create an incident: