ESET Tech Center

Connecting ESET PROTECT to Microsoft Sentinel

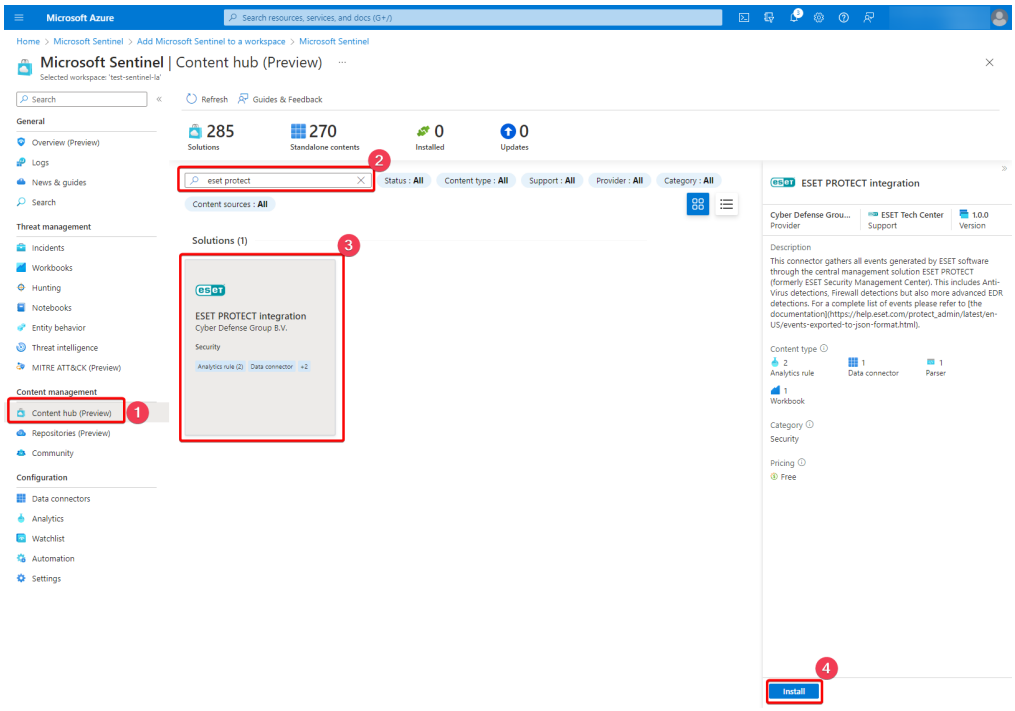
Mitchell | ESET Nederland - 2023-03-23 - Comments (0) - ESET PROTECT On-prem

Prerequisites:

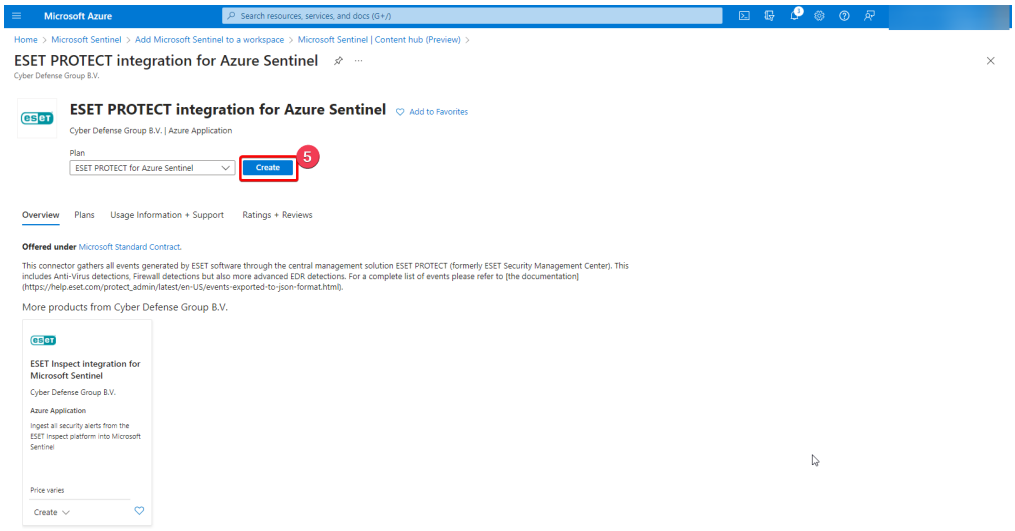
- ESET PROTECT installed
- Microsoft Sentinel
- A Linux server

Deploy ESET PROTECT integration to Microsoft Sentinel

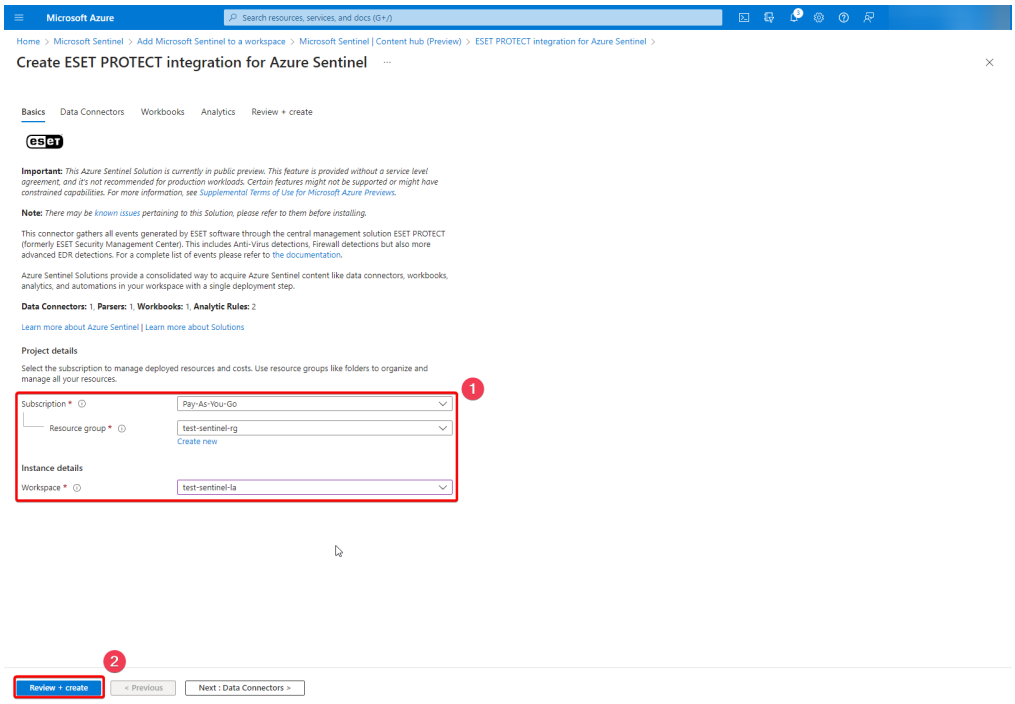
1. Navigate to Microsoft Sentinel > Content Hub
2. Search for ESET PROTECT
3. Select the ESET PROTECT integration by Cyber Defense Group B.V.
4. Click on “install”



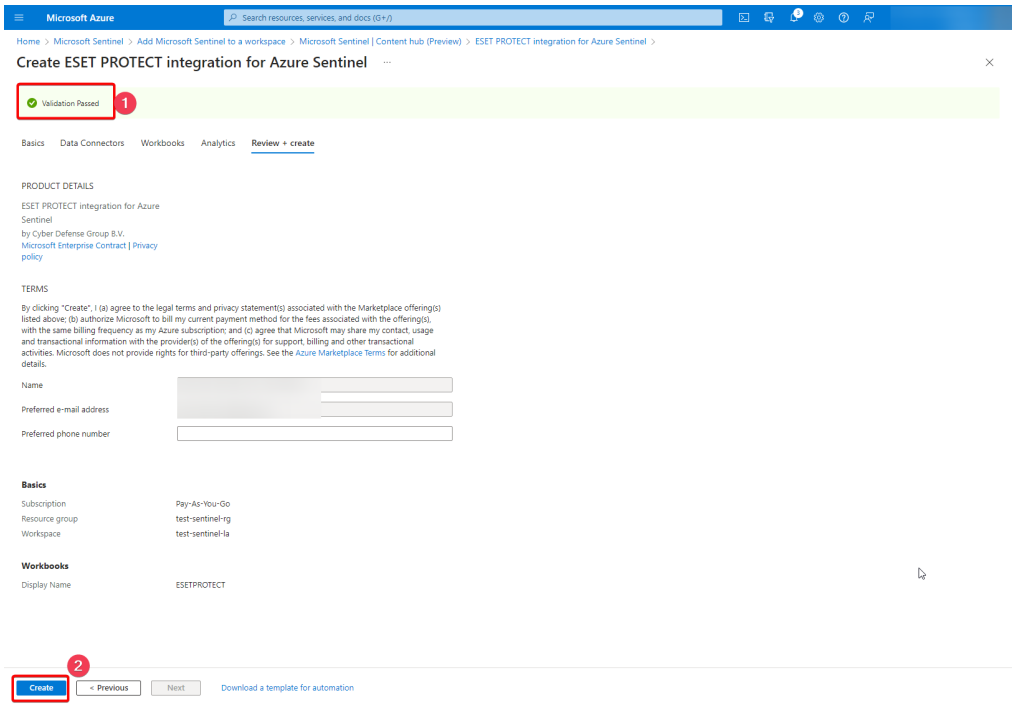
5. Click “create” in the next window:



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



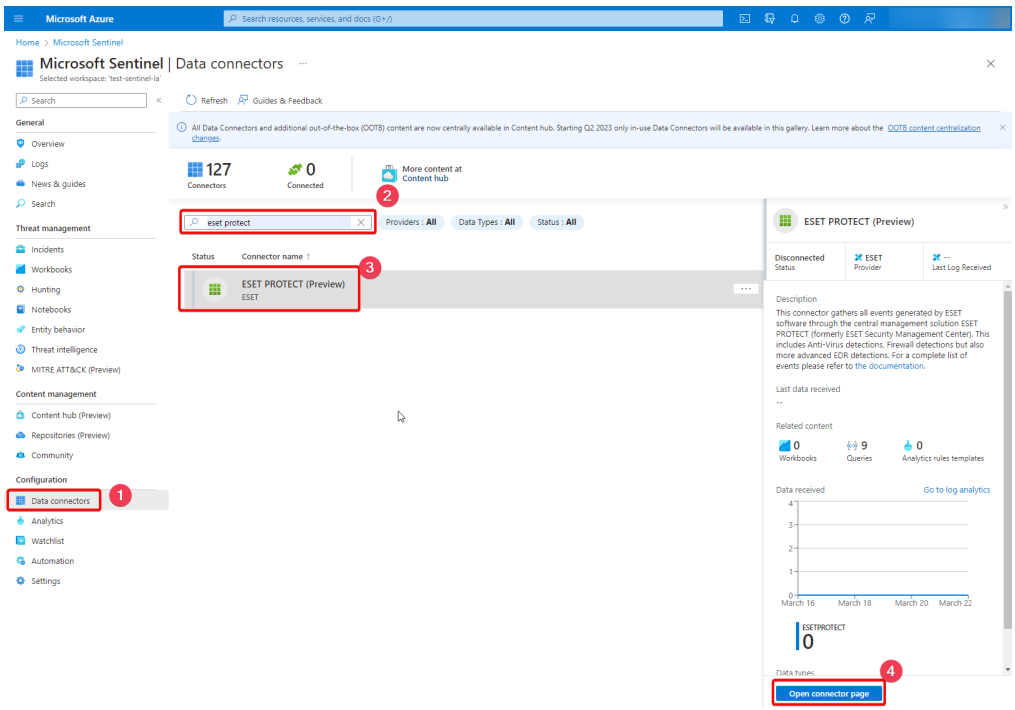
7. After the validation has passed, click “create” to start the deployment.



Configure ESET PROTECT to send events to Microsoft Sentinel

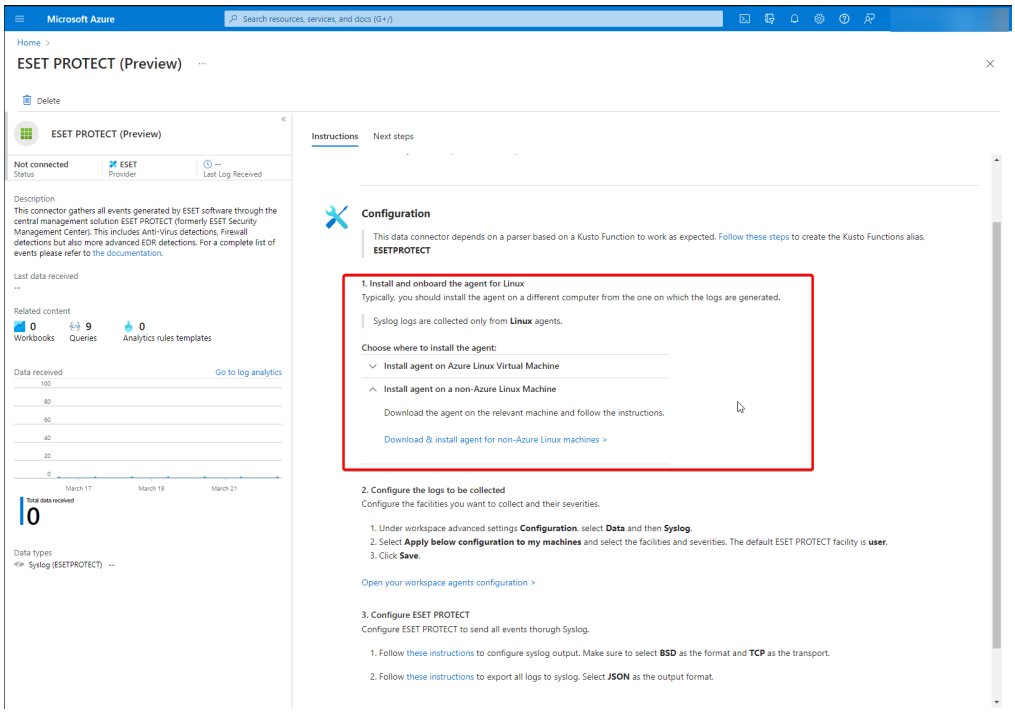
Install OMS-Agent

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

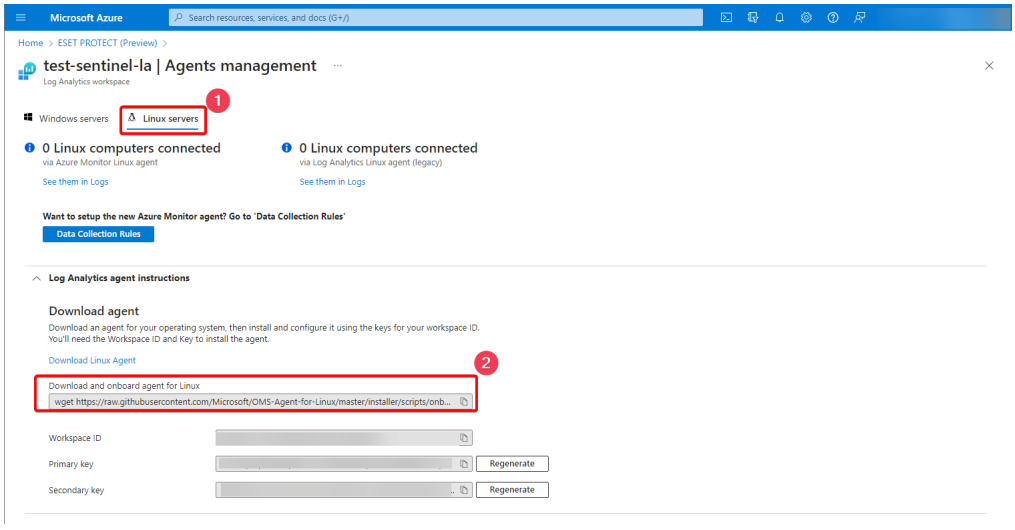


2. After opening the connector page, you will find the instructions to install the Log

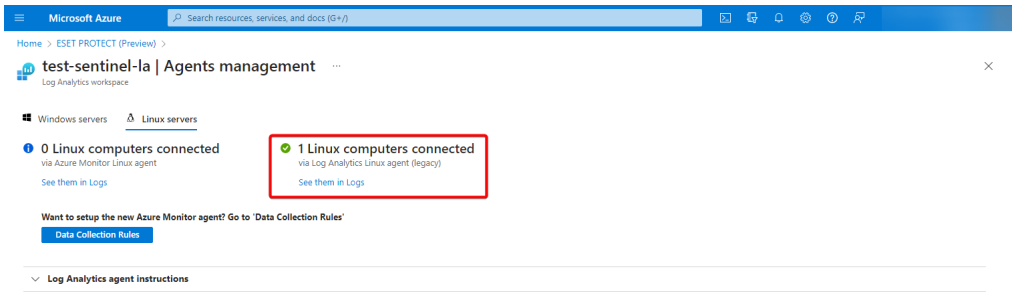
Analytics agent, because Syslog is only collected by the Linux agent, you will have to install the agent on a linux machine. (for example, the ESET PROTECT Server)



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

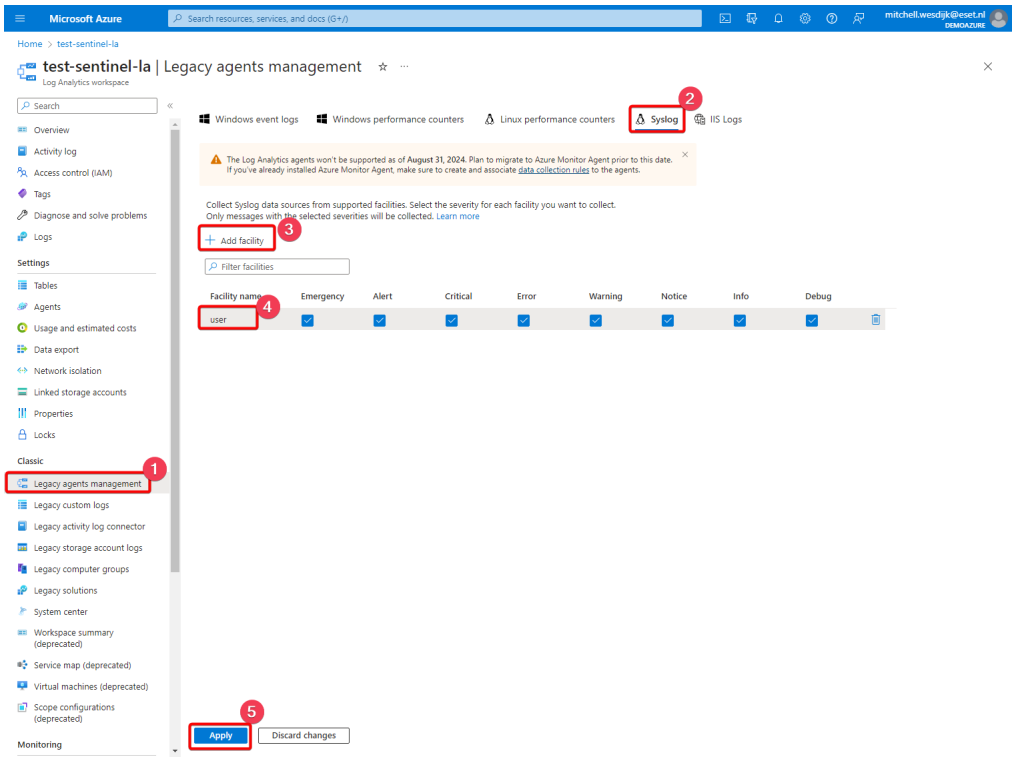


4. After installing the agent the Agents management overview should report that 1 Linux computer is connected:



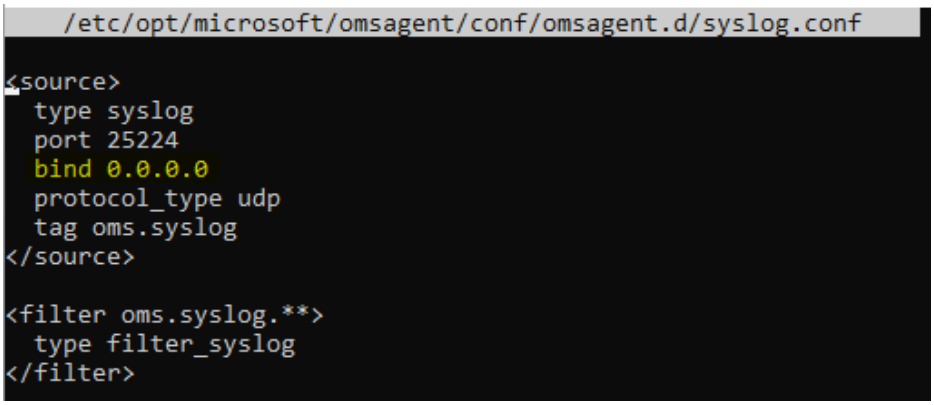
Configure OMS-Agent to collect syslog data

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

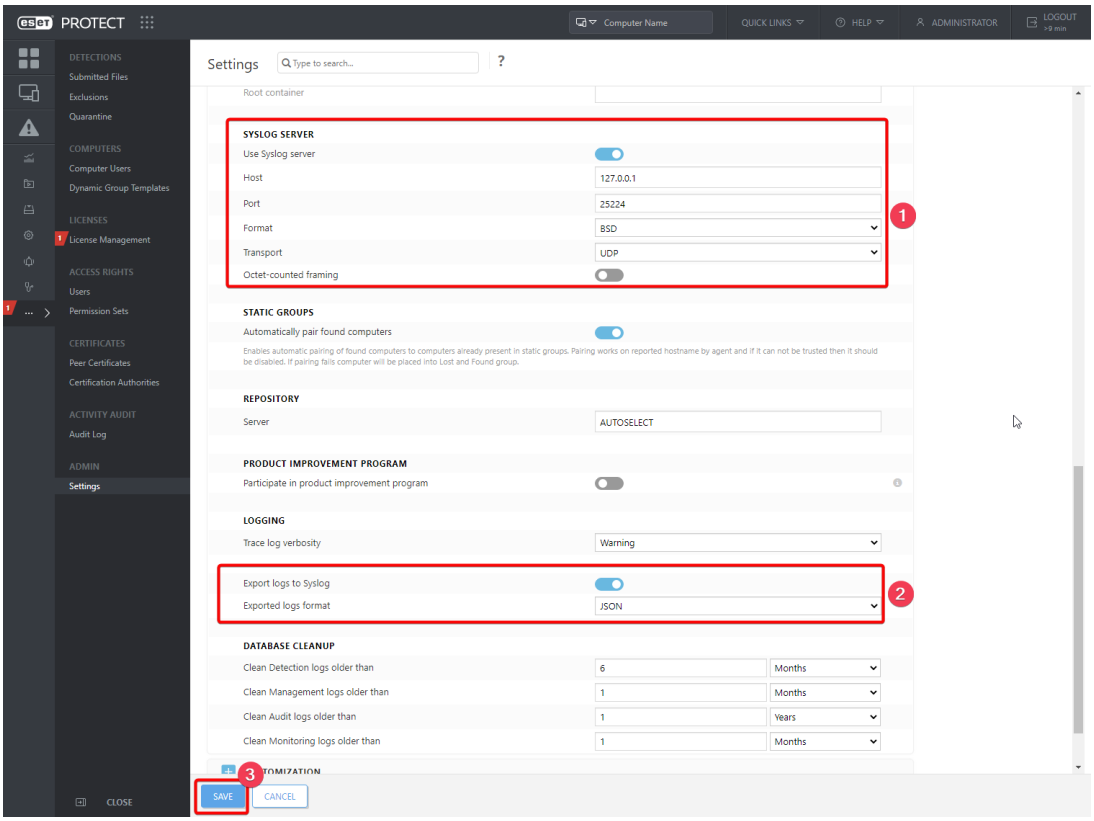


2. restart the agent

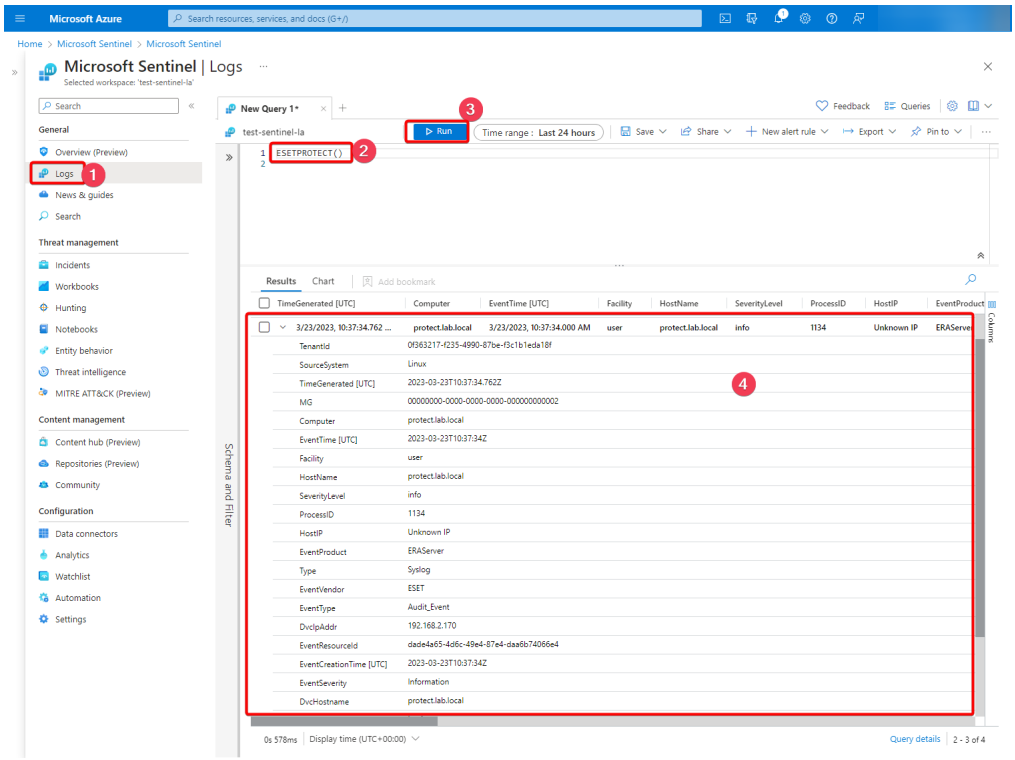
   ```
   /opt/microsoft/omsagent/bin/service_control restart
   ```

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:

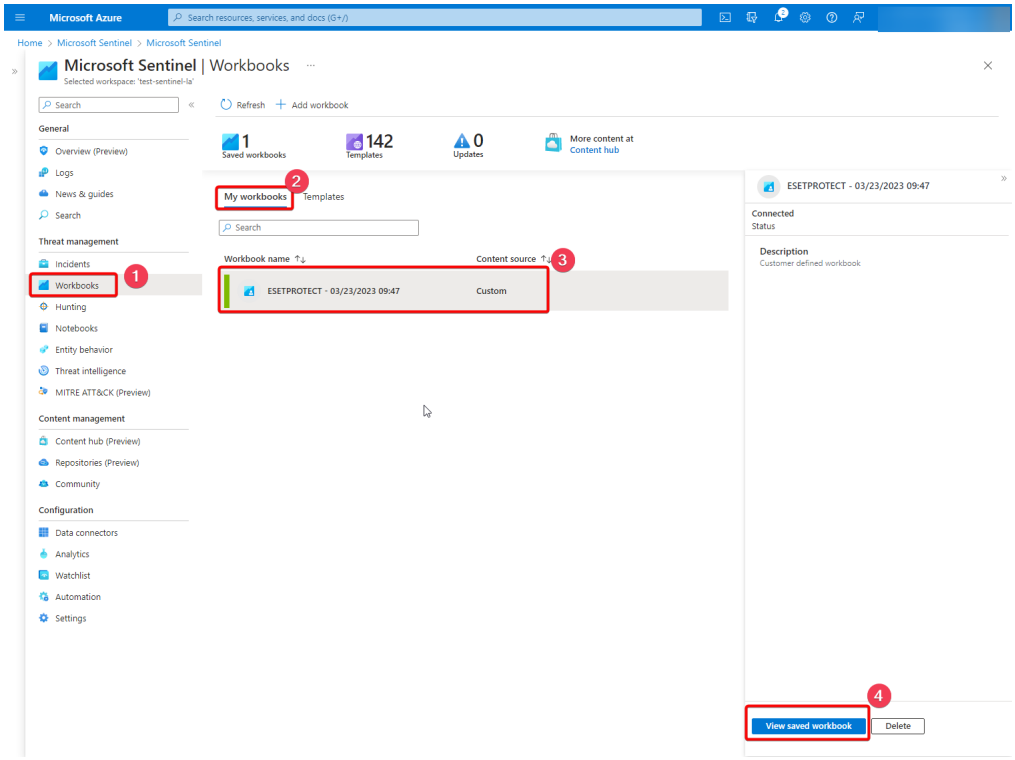


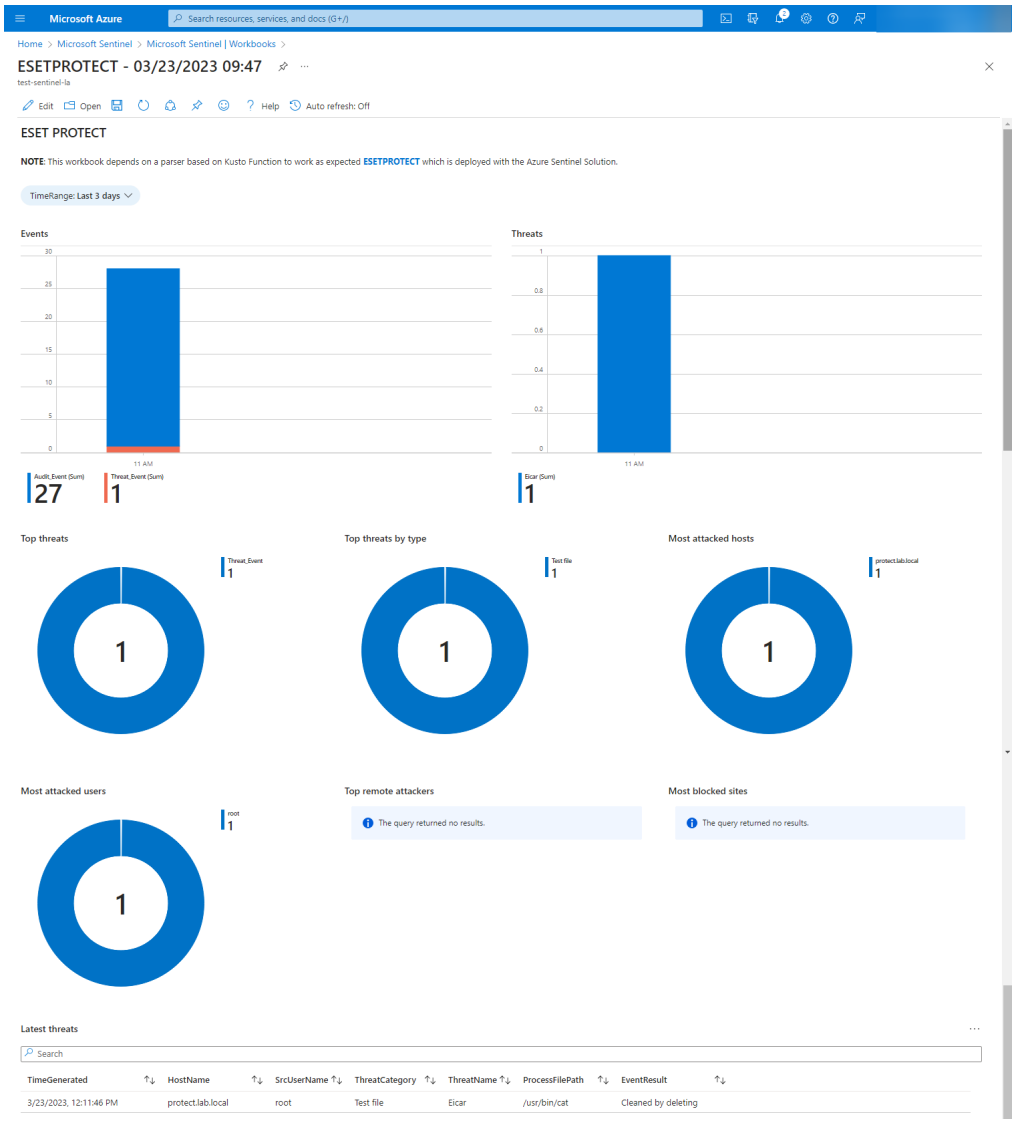
1. All ESET PROTECT event data should now be sent to Sentinel, you can generate some audit events by logging out and back in to ESET PROTECT for example. confirm that the events reached Sentinel by running the following query:



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

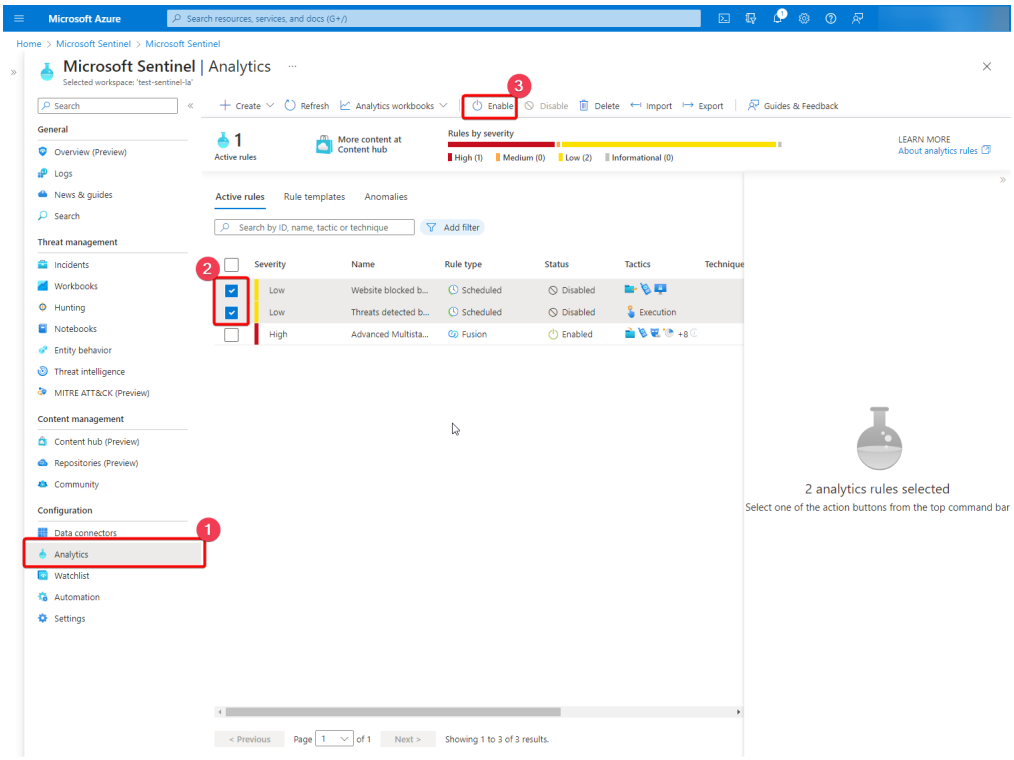
solution:


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel > Microsoft Sentinel
Microsoft Sentinel | Workbooks
Selected workspace: 'test-sentinel-la'
Search
General
Overview (Preview)
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub (Preview)
Repositories (Preview)
Community
Configuration
Data connectors
Analytics
Watchlist
Automation
Settings
Refresh
Add workbook
1
Saved workbooks
142
Templates
0
Updates
More content at
Content hub
My workbooks
Templates
Search
Workbook name
Content source
ESETPROTECT - 03/23/2023 09:47
Custom
ESETPROTECT - 03/23/2023 09:47
Connected
Status
Description
Customer defined workbook
View saved workbook
Delete
1
2
3
4

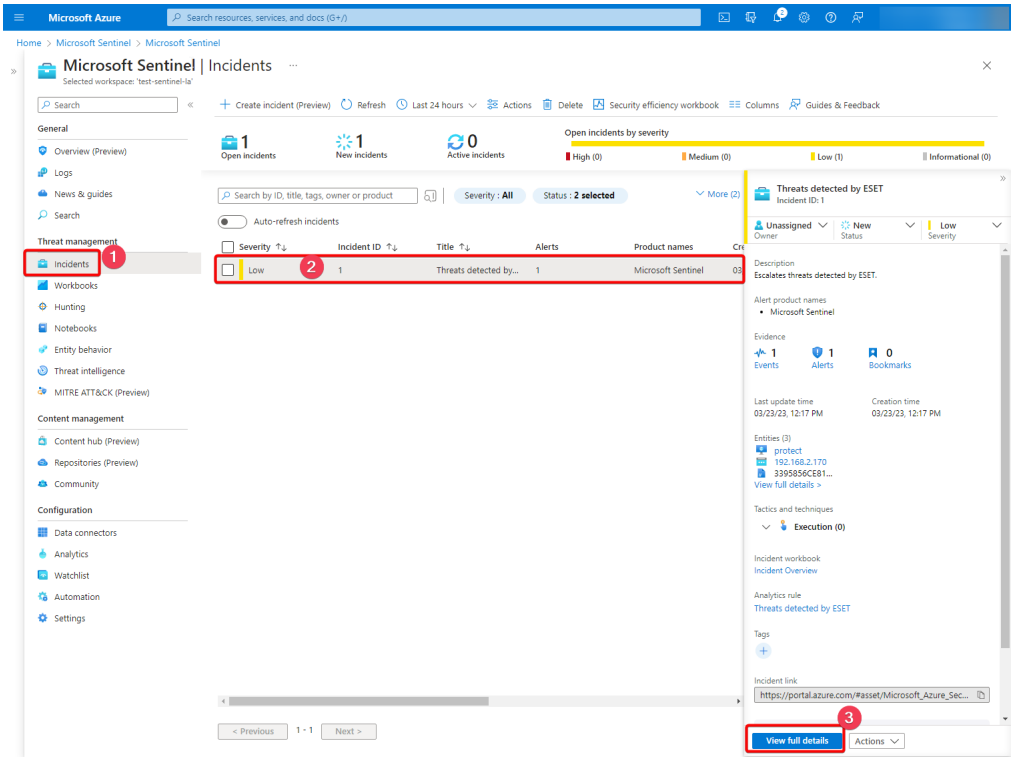


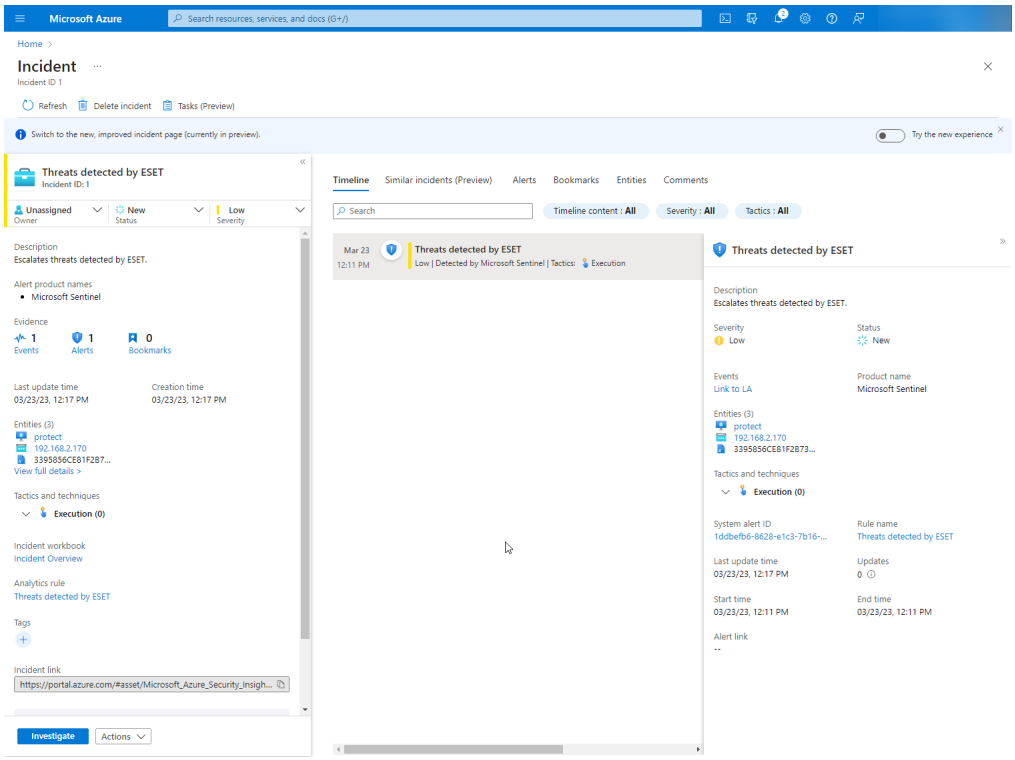
Enable analytics rules to create incidents from ESET detections

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:




Microsoft Azure
Search resources, services, and docs (G+/)
Home
Incident
Incident ID 1
Refresh
Delete incident
Tasks (Preview)
Switch to the new, improved incident page (currently in preview).
Try the new experience
Threats detected by ESET
Incident ID: 1
Unassigned
Owner
New
Status
Low
Severity
Description
Escalates threats detected by ESET.
Alert product names
Microsoft Sentinel
Evidence
1
Events
1
Alerts
0
Bookmarks
Last update time
03/23/23, 12:17 PM
Creation time
03/23/23, 12:17 PM
Entities (3)
protect
192.168.2.170
3395856CE81F2B7...
View full details >
Tactics and techniques
Execution (0)
Incident workbook
Incident Overview
Analytics rule
Threats detected by ESET
Tags
Incident link
https://portal.azure.com/#asset/Microsoft_Azure_Security_Insigh...
Investigate
Actions
Timeline
Similar incidents (Preview)
Alerts
Bookmarks
Entities
Comments
Search
Timeline content : All
Severity : All
Tactics : All
Mar 23
12:11 PM
Threats detected by ESET
Low | Detected by Microsoft Sentinel | Tactics: Execution
Threats detected by ESET
Description
Escalates threats detected by ESET.
Severity
Low
Status
New
Events
Link to LA
Product name
Microsoft Sentinel
Entities (3)
protect
192.168.2.170
3395856CE81F2B73...
Tactics and techniques
Execution (0)
System alert ID
1ddbefb6-8628-e1c3-7b16-...
Rule name
Threats detected by ESET
Last update time
03/23/23, 12:17 PM
Updates
0
Start time
03/23/23, 12:11 PM
End time
03/23/23, 12:11 PM
Alert link
--