

VMware vSphere Integration

This integration periodically fetches logs and metrics from vSphere vCenter servers.

Compatibility

The integration uses the Govmomi library to collect metrics and logs from any VMware SDK URL (ESXi/vCenter). This library is built for and tested against ESXi and vCenter 6.5, 6.7 and 7.0.

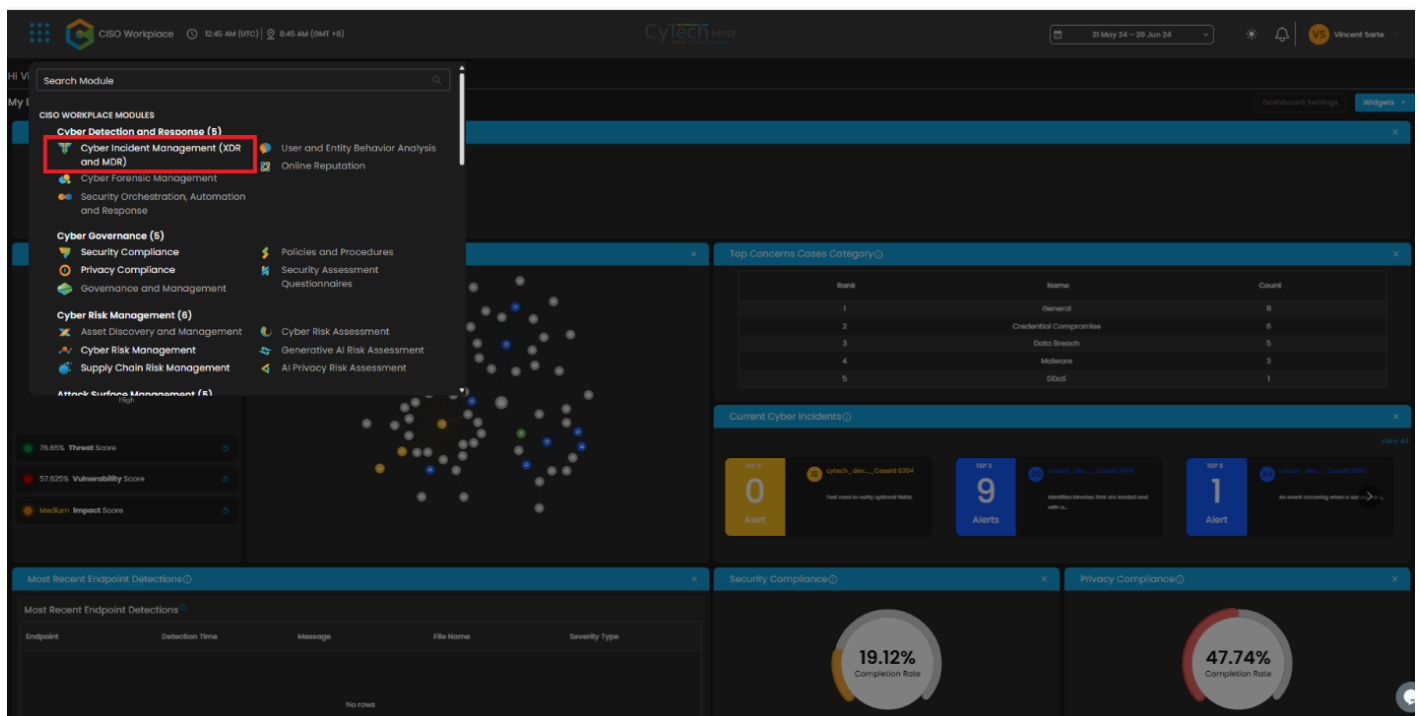
Installation Guide:

[VMware vSphere 7.0 Installation](#)

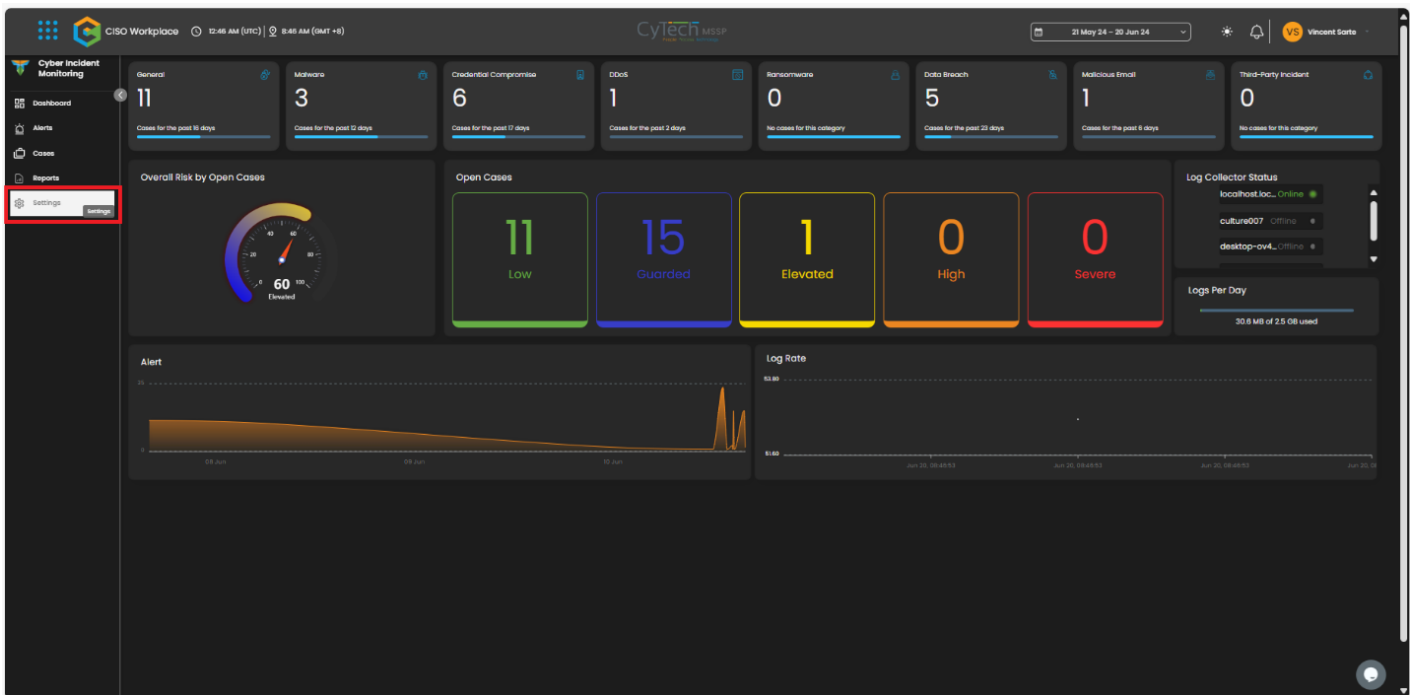
[Govmomi Library](#)

Integration Process

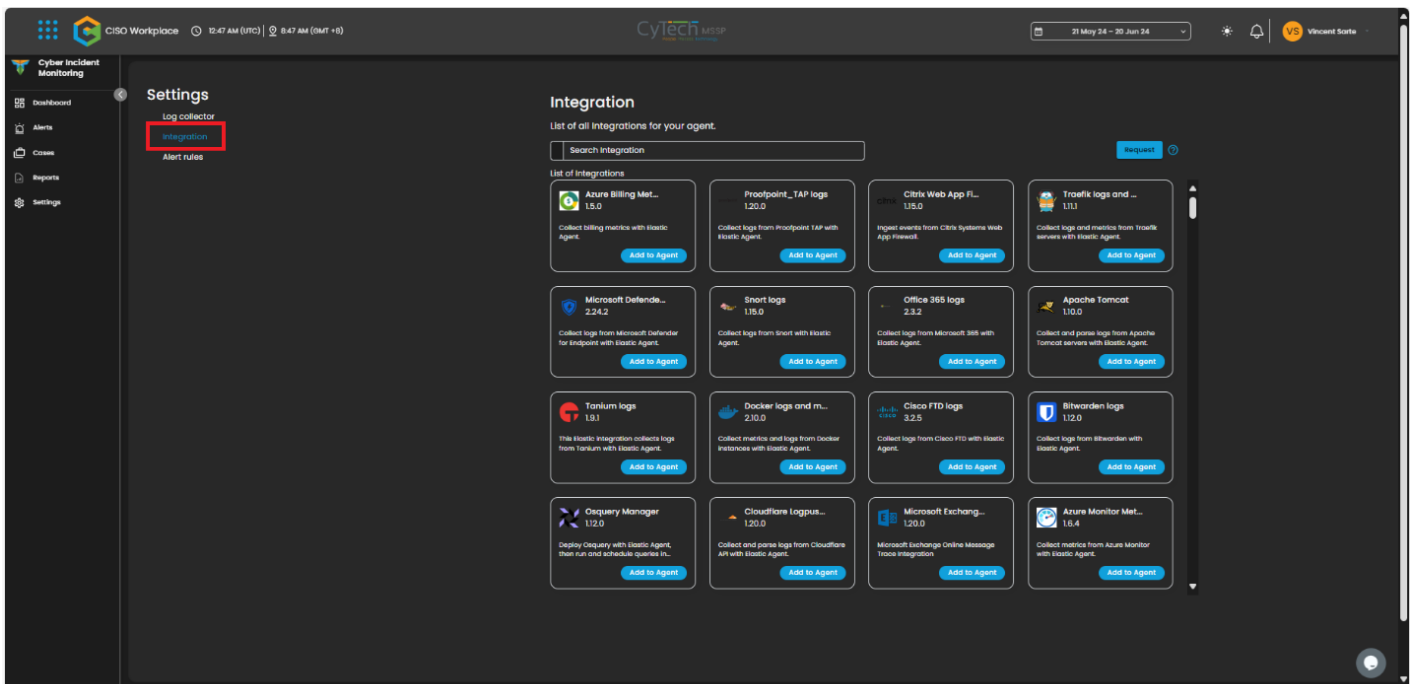
Go> Cyber Incident Management (XDR and MDR)



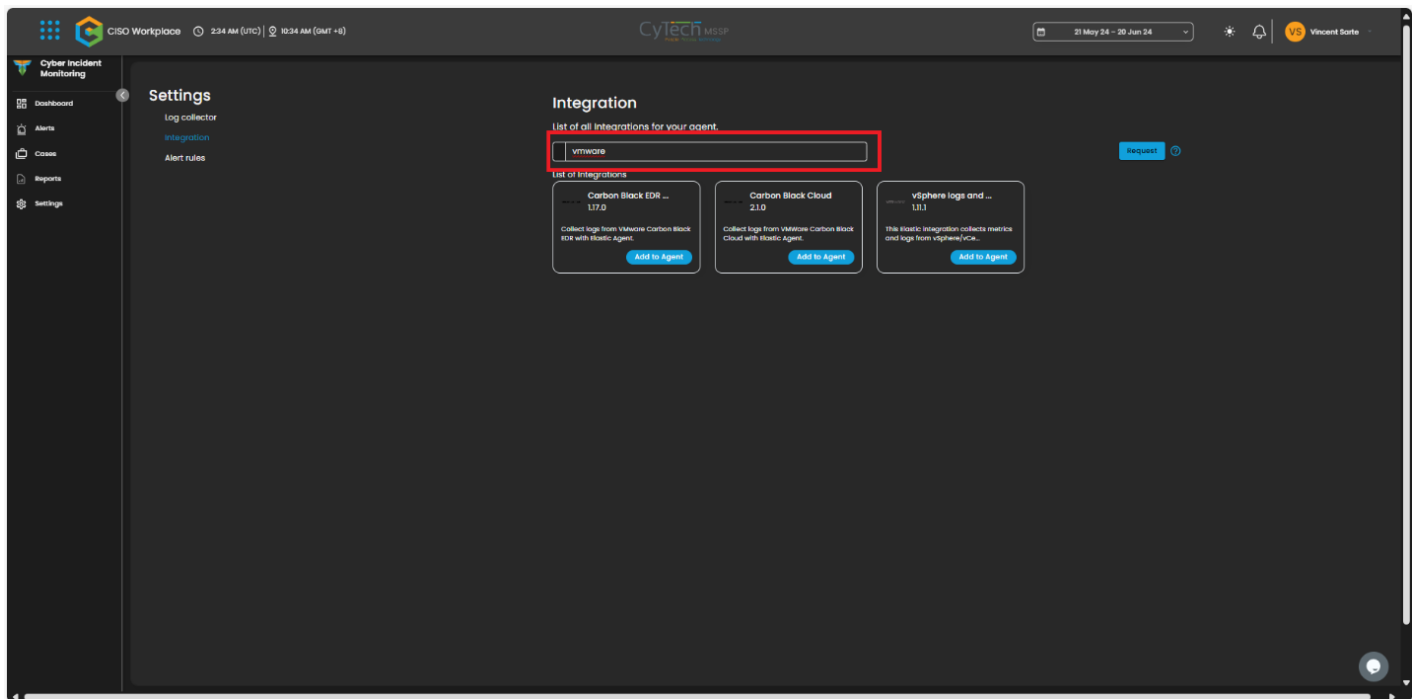
Go> Cyber Incident Management (XDR and MDR)> Settings



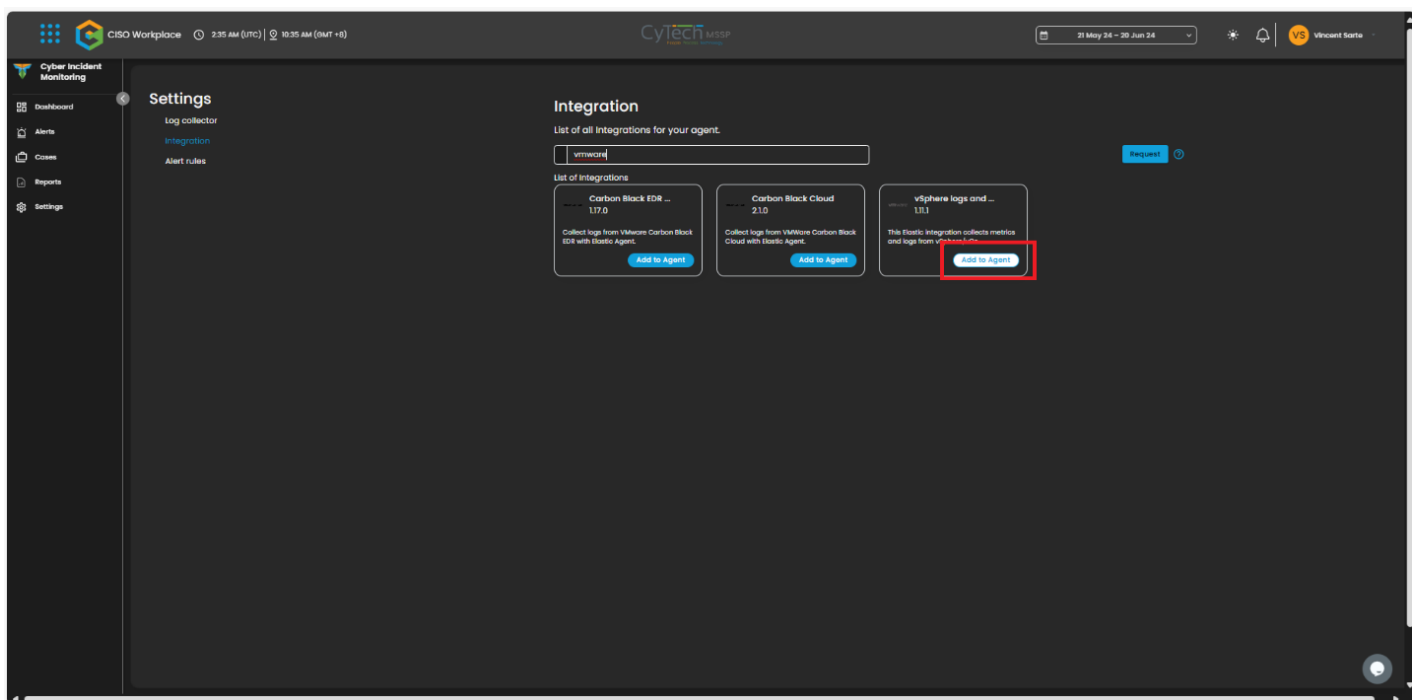
Go> Cyber Incident Management (XDR and MDR)> Settings> Integration



Go> Cyber Incident Management (XDR and MDR)> Settings> Integration>
In search bar type "Vmware"



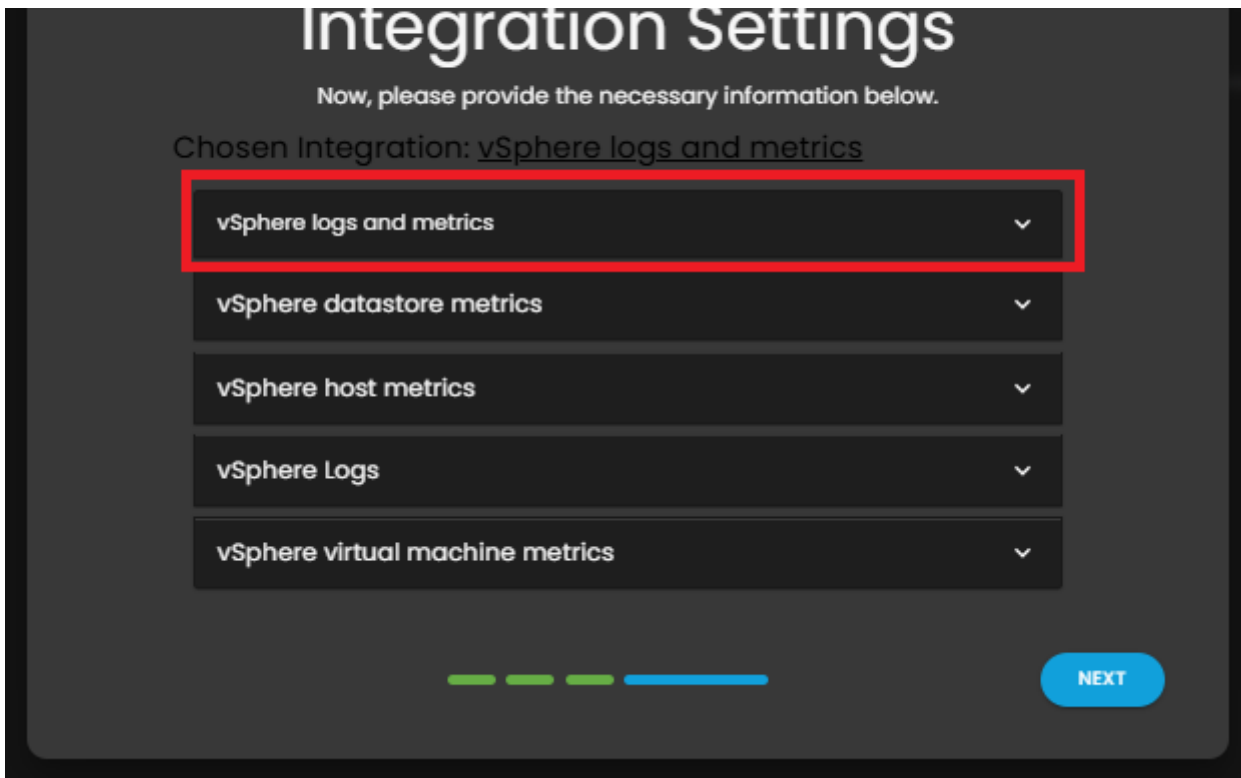
Click Add Agent



Choose your Log Collector

A screenshot of a log collectorDescription automatically generated

Click the vSphere logs and metrics



Keep it as is

A screenshot of a computerDescription automatically generated

Enter the IP address and port

A screenshot of a computerDescription automatically generated

Example: https://127.0.0.1:8989/sdk

127.0.0.1: This is the IP address of the local machine (localhost).

8989: This is the port number on which the SDK service is running. (Keep it as is)

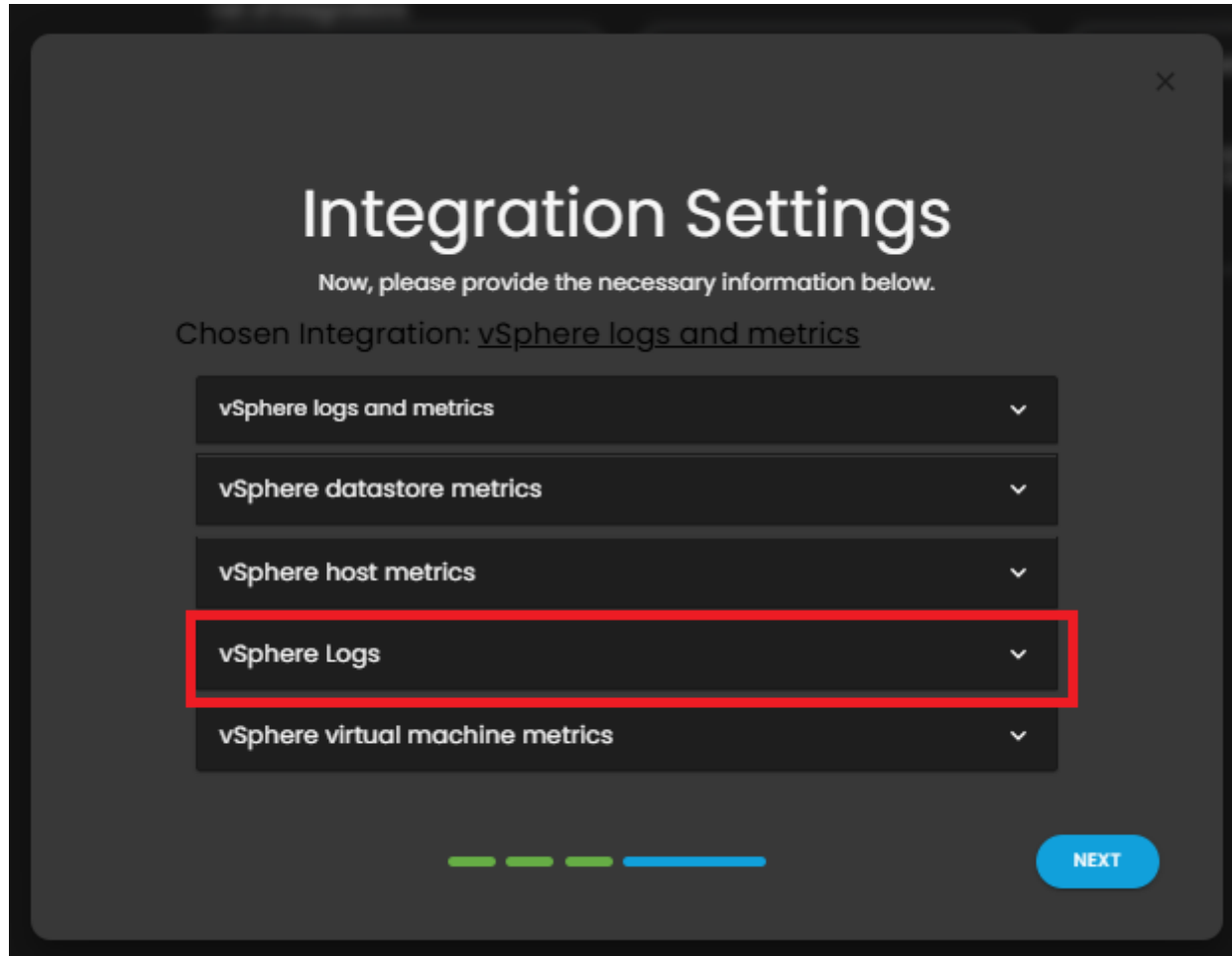
/sdk: This indicates that the SDK is accessible at this path. (Keep it as is)

Notes: To add multiple hosts, enter each IP address following the same format (https://<IP_or_hostname>:port/sdk) and press enter.

Enter the Username and password of vSphere account

A screenshot of a computer screenDescription automatically generated

Notes: The insecure option bypasses the verification of the server's certificate chain, which can be used to use this

A screenshot of a dark-themed 'Integration Settings' dialog box. The title 'Integration Settings' is at the top in large white font. Below it, a subtitle says 'Now, please provide the necessary information below.' The main content area shows 'Chosen Integration: vSphere logs and metrics' in a light gray font. Below this, there is a list of five integration options, each in a dark gray box with a white dropdown arrow on the right. The options are: 'vSphere logs and metrics', 'vSphere datastore metrics', 'vSphere host metrics', 'vSphere Logs' (which is highlighted with a red rectangular border), and 'vSphere virtual machine metrics'. At the bottom of the dialog, there is a progress indicator consisting of four horizontal bars: the first three are green and the fourth is blue. To the right of the progress indicator is a blue rounded button labeled 'NEXT' in white capital letters. A small 'X' icon is in the top right corner of the dialog box.

Integration Settings

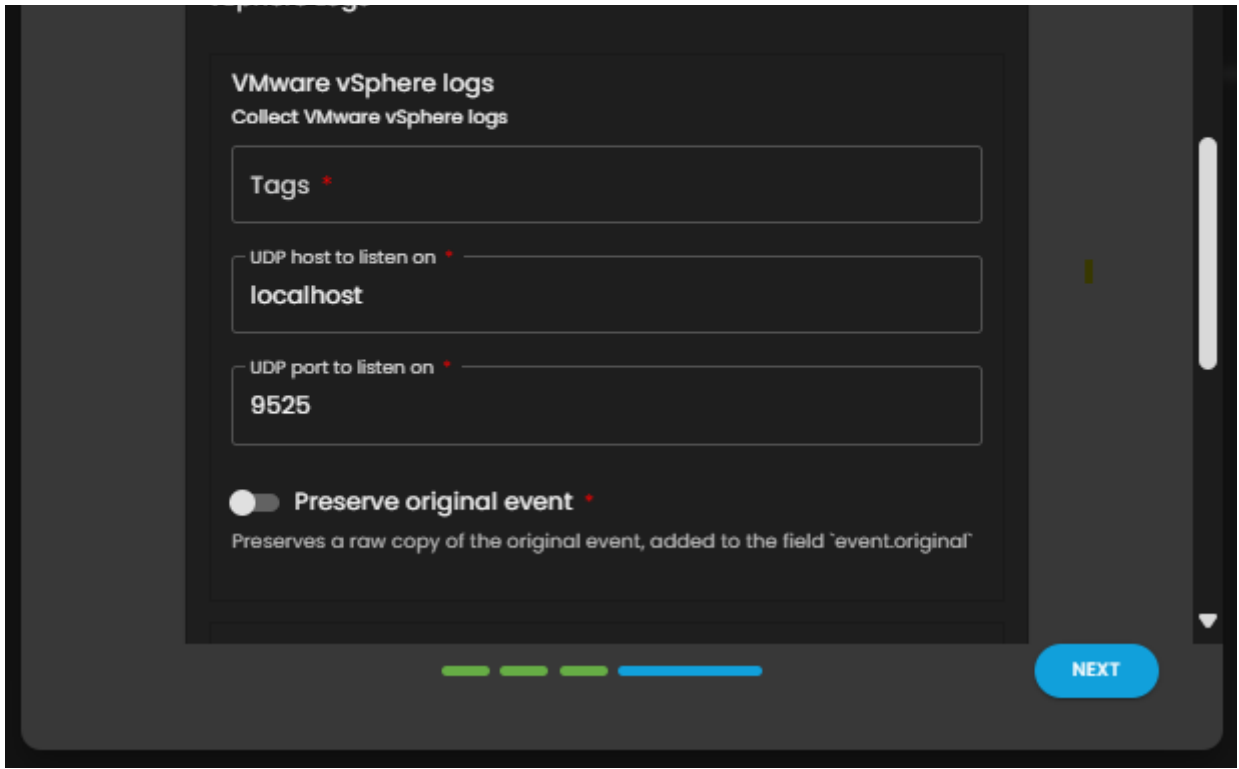
Now, please provide the necessary information below.

Chosen Integration: vSphere logs and metrics

- vSphere logs and metrics
- vSphere datastore metrics
- vSphere host metrics
- vSphere Logs**
- vSphere virtual machine metrics

NEXT

Collect logs from vSphere via UDP



Tags: Click the given tags

UDP host to listen on: This is the IP address of the machine where the log collector is running.

UDP port to listen on: This is the port on which the log collector will listen for incoming log data. (Keep it as is)

Notes: Enabling "Preserve original event" ensures raw log data is always available, crucial for troubleshooting, compliance, and verifying log accuracy. It adds raw data to event.original, doubling storage needs and potentially slowing processing if storage isn't scaled, impacting efficiency.

Collect logs from vSphere via TCP

A screenshot of a computerDescription automatically generated

Tags: Click the given tags

TCP host to listen on: This is the IP address of the machine where the log collector is running.

TCP port to listen on: This is the port on which the log collector will listen for incoming log data. (Keep it as is)

Notes: Enabling "Preserve original event" ensures raw log data is always available, crucial for troubleshooting, compliance, and verifying log accuracy. It adds raw data to event.original, doubling storage needs and potentially slowing processing if storage isn't scaled, impacting efficiency.

Click Next to complete the integration.

Revision #2

Created 23 April 2024 14:15:24

Updated 26 June 2024 09:26:03 by Reut Rubinstein