Netsurion

Integration Guide

Integrate Azure Key Vault with the Netsurion Open XDR platform

Publication Date

March 21, 2023

Abstract

This guide provides instructions to configure and retrieve the Azure Key Vault events via the Azure Event Hub and then forward the logs to the Netsurion Open XDR platform.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Scope

The configuration details in this guide are consistent with Azure Key Vault and the Netsurion Open XDR platform version 9.3 or later.

Audience

This guide is for the administrators responsible for configuring and monitoring Azure Key Vault in the Netsurion Open XDR platform.

Product Terminology

The following terms are used throughout this guide:

- The term “Netsurion’s Open XDR platform” or “the Netsurion Open XDR platform” or “the Open XDR platform” refers to Netsurion open XDR.
- The term “Data Source Integrations” refers to Knowledge packs.

Table of Contents

1 Overview

Azure Key Vault cloud service offers a secure place to store and access secrets. API keys, passwords, certificates, and cryptographic keys can be managed in Azure key Vault.

The Netsurion Open XDR platform monitors events from Azure Key Vault. To increase the security of sensitive data and gain insights into the operations and usage of Azure Key Vault, Netsurion's Open XDR platform offers a solution for integrating Azure Key Vault. As a result, potential security threats could be simpler to recognize and address. It triggers alerts whenever an action critical to the service is carried out.

2 Prerequisites

- An Azure subscription and a user who is a global administrator.
- An Azure Resource group.

3 Integrating Azure Key Vault with Netsurion Open XDR

Integrate Azure Key Vault with the Netsurion Open XDR platform by streaming the logs to the Azure Event Hub, and from Azure Event Hub to the Netsurion Open XDR platform using the Function App.

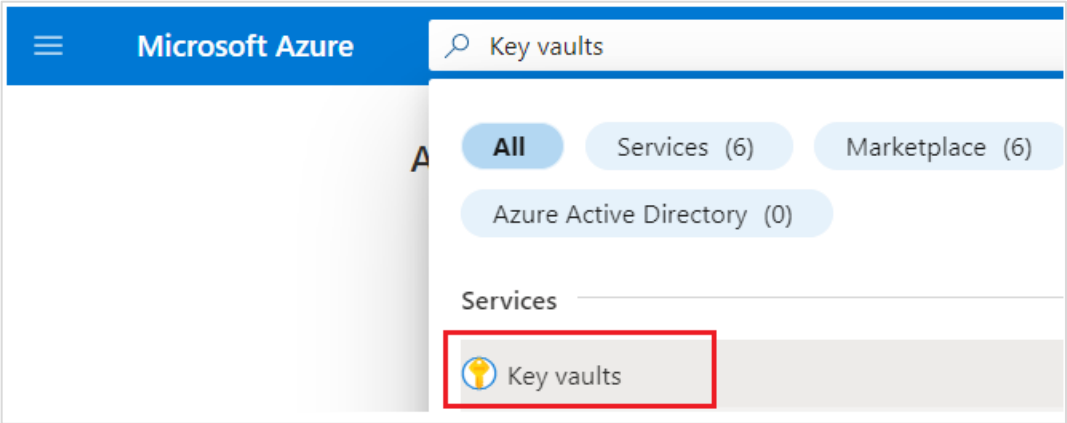
3.1 Create Event Hub and Function App

Refer to the configuration Event Hub and Function App to forward the logs to the Netsurion Open XDR platform.

3.2 Configuring Azure Key Vault to stream events to Event Hub

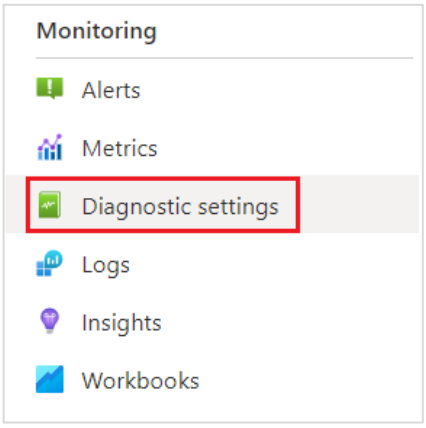
To configure Microsoft Azure Key Vault to stream events to Event Hub, as an Administrator,

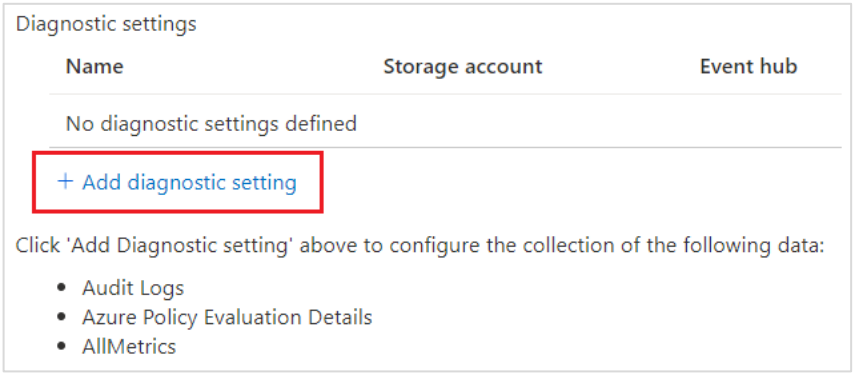
1. Log in to Microsoft Azure and create an event hub namespace.
2. In the **Microsoft Azure** console, click **All** services, then search and click **Key Vaults**.



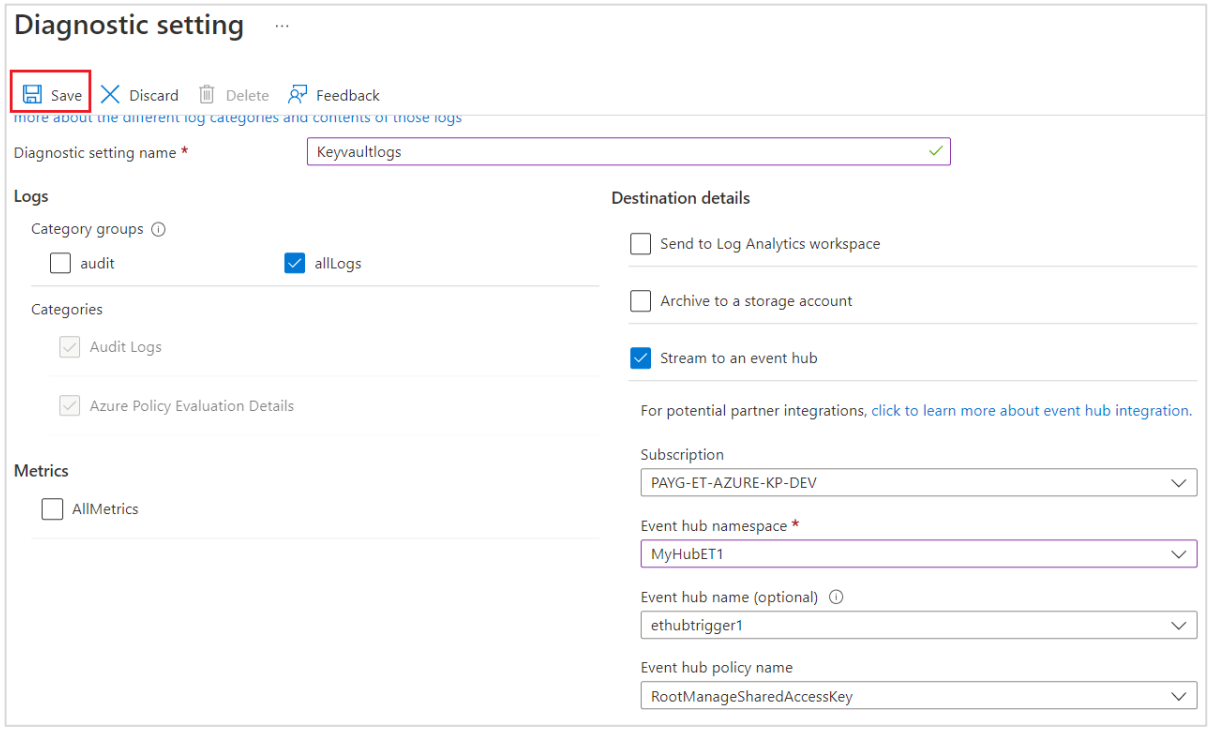
3. Then, select the appropriate Key Vault from the available lists to monitor.

4. From the left panel, go to **Monitoring** > **Diagnostics settings** and click **Add diagnostics setting.**





5. In the **Diagnostic setting** interface, specify the following details.



- Provide the **Diagnostics settings name**, such as **Netsurion open XDR_Key Vault**.

- From the left of the interface, in the **Logs** section, select **allLogs**.
- From the right of the interface, in the **Destination details** section, select **stream to an event hub** and then choose the following.
  - **Subscription:** Select the preferred Azure subscription from the drop-down list.
  - **Event Hub namespace:** Select the Event Hub namespace from the drop-down list.
  - **Event Hub name:** Select Event Hub created under Event Hub namespace from the drop-down list.
  - **Event Hub policy name:** Select the Event Hub policy from the drop-down list.

6. After providing all the details, click **Save.**

4 Data Source Integrations (DSIs) in the Netsurion Open XDR platform

After the logs are received by the Netsurion Open XDR platform, configure the Data Source Integrations in the Netsurion Open XDR platform.

The Data Source Integrations package contains the following files for the Azure Key Vault.

- Categories_Azure Key Vault.iscat
- Alerts_Azure Key Vault.isalt
- Reports_Azure Key Vault.etcrx
- KO_Azure Key Vault.etko
- Dashboards_Azure Key Vault.etwd
- MITRERules_Azure Key Vault.etmr

Note

MITRERules_Azure Key Vault.etmr is applicable only for the Netsurion Open XDR platform version 9.4 or later.

Note

Refer the How To Configure DSI guide for the procedures to configure the above DSIs in the Netsurion Open XDR platform.

Data Source Integrations Details

Alerts

Name	Description
Azure Key Vault: Delete/update activity detected	This alert is triggered whenever a delete(s) or update(s) activity related to the Azure Key Vault is detected.
Azure Key Vault: Potential brute force detected	This alert is triggered whenever an unauthorized access to the Azure Key vault is detected.
Azure key Vault: Policy changes detected	This alert is triggered whenever a modification to policy configuration to Azure Key Vault is observed.
Azure key Vault: Suspicious activities detected	This alert is triggered whenever any suspicious events are identified on Azure Key Vault.

Reports

Name	Description
Azure Key Vault - Activities overview	This report contains information related to all activities concerning the Azure Key Vault service.

Dashboards

Name	Description
Azure Key Vault – Unauthorized events by source IP	This dashlet displays the source IP of the unauthorized events occurred on Azure Key Vault.
Azure Key Vault – Activities overview	This dashlet displays the different activities that occurred on Azure Key Vault.
Azure Key Vault – Http response methods	This dashlet displays the Http response methods of the request accessing Azure Key Vault.

Saved Search

Name	Description
Azure Key Vault - Activities overview	This saved search allows parsing events that are specific to the activities detected by Azure Key Vault.

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's managed offering includes our 24x7 SOC that operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers Managed Threat Protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection and Response (MDR) and a Top 25 Global MSSP. Learn more at netsurion.com.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

Direct Enterprise	SOC@Netsurion.com	1 (877) 333-1433 Option 1, Option 1
MSP Enterprise	SOC-MSP@Netsurion.com	1 (877) 333-1433 Option 1, Option 2
Essentials	Essentials-Support@Netsurion.com	1 (877) 333-1433 Option 1, Option 3
Self-Serve	EventTracker-Support@Netsurion.com	1 (877) 333-1433 Option 1, Option 4

https://www.netsurion.com/eventtracker-support