Thycotic Docs - ssi - 1.0.0

Connect your Thycotic Secret Server to Azure Sentinel

This article explains how to connect your Thycotic Secret Server appliance to Azure Sentinel. The Thycotic Secret Server data connector allows you to easily connect your Thycotic Secret Server logs with Azure Sentinel, to view dashboards, create custom alerts, and improve investigation. Integration between Thycotic and Azure Sentinel makes use of the CEF Data Connector to properly parse and display Secret Server Syslog messages.

NOTE: Data will be stored in the geographic location of the workspace on which you are running Azure Sentinel.

Configure Logs and Connect Thycotic Secret Server to the Syslog Agent

Configure Thycotic Secret Server to forward Syslog messages in CEF format to your Azure workspace via the Syslog agent. If you don't have such a log forwarding server, see these instructions to get one up and running.

1. In the Azure Sentinel portal:
    1. Click Data connectors.
    2. Select Thycotic Secret Server.
    3. Open the connector page.
2. Follow the configure Secret Server instructions to configure sending syslog data to the log forwarding server.
3. Validate your connection and verify data ingestion using these instructions. It may take up to 20 minutes until your logs start to appear in Log Analytics.

Thycotic Software, LLC
1101 17th Street, N.W., Suite 1200
Washington, D.C., 20036 USA
Main: +1 202.802.9399
Fax: +1 202.315.3315
www.thycotic.com

Find Your Data

After a successful connection is established, the data appears in Logs, under the Azure Sentinel section, in the **CommonSecurityLog** table.

To query the Thycotic logs in Log Analytics, enter **CommonSecurityLog** at the top of the query window.

Next Steps

In this document, you learned how to connect Thycotic Secret Server to Azure Sentinel. To learn more about Azure Sentinel, see the following articles:

- Learn how to get visibility into your data, and potential threats.
- Get started detecting threats with Azure Sentinel.
- Use workbooks to monitor your data.