Data Collectors in Taegis XDR

tanyazehnder
Secureworks Employee

10-26-2022 02:22 PM - edited 10-27-2022 01:09 PM

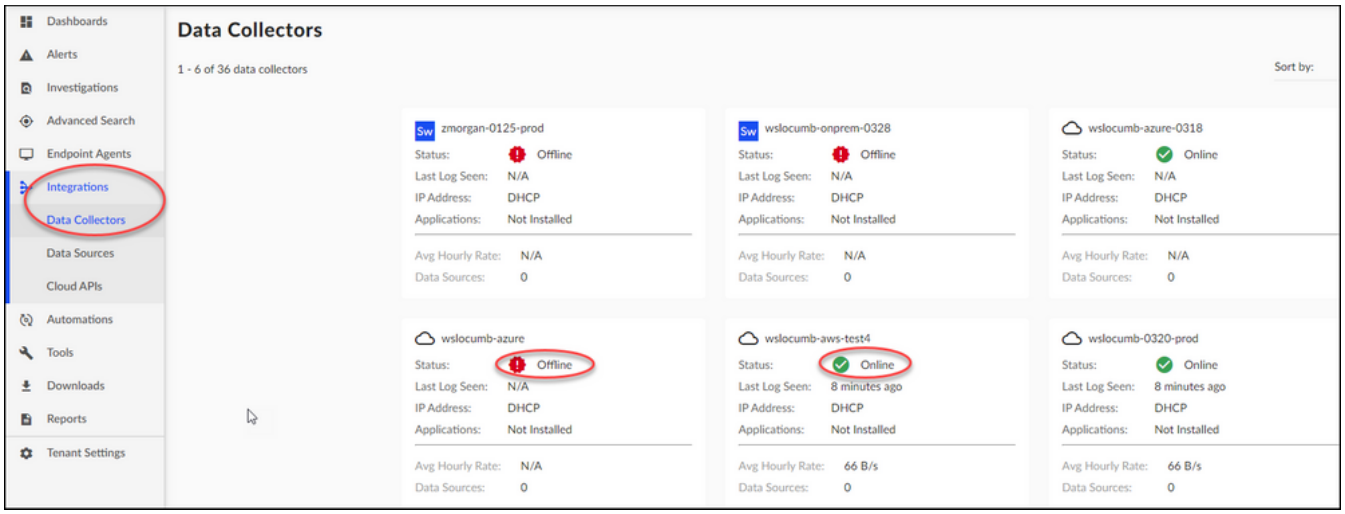
Summary

Integrating data collectors and APIs is key to leveraging Taegis™ XDR's full monitoring capabilities. Taegis XDR supports a whole host of integrations, including network integrations, cloud integrations, and endpoint integrations. Secureworks® also offers our own Taegis XDR on-premises data collector.

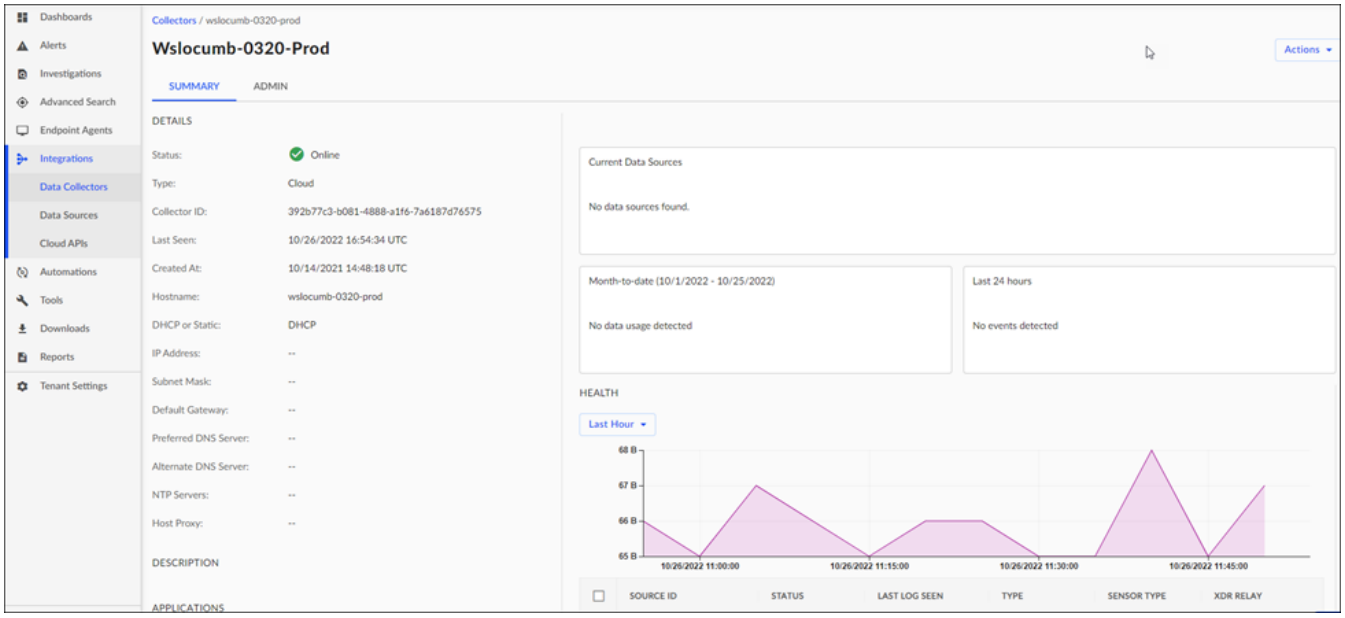
Solution

Managing Data Collectors

View your organization's current integrated collectors and monitor their health on the Data Collectors page in Taegis XDR, accessed by choosing **Integrations, Data Collectors** in the left navigation menu.



Click a collector's tile to view more detailed information.



Installing the On-Premises Data Collector

The On-Premises Data Collector is a virtual machine appliance that must be installed in your hypervisor environment to collect data and transmit it to the Taegis XDR Infrastructure. **When installing the data collector, it is important you follow the steps in On-Premises Data Collector in order.**

The Data Collector can be preconfigured and downloaded in XDR from **Integrations** > **Data Collectors** and installed in a vsphere and/or hyperv environment. Once the appropriate information is provided, the collector will be customized, built, and configured to DHCP or static IP addressing depending on your selection.

Note: Recommended virtual environment versions for the XDR On-Premises Data Collector are **vSphere ESXi 6.7 or later** or **Hyper-V 8.0in Windows Server 2016 or later**.

Once complete, an .iso cdrom image containing your client certificate/credentials and disk image in the form of .ova (vsphere) or .vhdx (hyper-v) will be available for download from XDR. Attach the .iso (cdrom image) to the collector VM on boot. Once booted, the appliance registers with XDR, and the status of the connection will be displayed in the XDR Console.

FAQ

Can I Log Into My Data Collector?

You may wonder if you can log into your data collector to investigate network connectivity issues. The answer is no. Please work with Product Support for this type of assistance.

How Can I Make Sure My Data Collector Was Deployed Correctly?

If you can see the name you provided for the collector, and NOT "ctpx login", the collector was deployed properly.

If the collector was not properly deployed, you will need to redeploy it.

Does XDR Collect Data and Alert Locally if There Is No Internet Connection?

Provided there is connectivity between the security or network appliance and an on-premise XDR Collector, the logs will continue to be forwarded to the data collector until the storage limit is reached. This limit would be subjected to the 200GB of space, which was dedicated to the data collector when provisioned. The logs would be forwarded to the Taegis platform once internet connectivity is restored.

In the case of cloud-based data collection, internet connectivity is required for the collector to receive the data from the security or network appliance. Because XDR has not received those events, alerting would not be possible until the data is ingested and processed through the detectors.

What Is the Expected Time Frame for New Network Integrations To Appear in Taegis XDR?

Expect a time variable between three and 10 minutes for new network integrations to appear on the Data Source page and the Collector page, depending on network resourcing and communications with Taegis XDR.

Troubleshooting

Issues When Creating XDR Integrations

If you experience issues when creating XDR Integrations, verify that your role is set to Tenant Admin (not Tenant Auditor). Creating XDR integrations requires Tenant Admin rights. Any other role usage may cause the process to stall.

My Network Integration Apperaws on the Collectors Page but Not on the Data Sources Page

If data received by a data collector can be attributed to an integration, it is visible on the Collectors page. It may take some time for that data to appear on the Data Sources page as the data is sent to Taegis XDR in 50GB data blocks. Consequently, an integration which is not very verbose would populate at a slower rate than another data source which may be a bit more verbose.

If the Data Sources page is not populating collected data at all, it could be because the delivery of the data source information was interrupted. This happens when a network appliance interrupted the communication between a collector and XDR.

Resources

Manage Data Collectors

Integrating Taegis XDR with Third-Party Ticketing Systems: Use Case-ServiceNow

Secureworks Taegis XDR Basic Application Support

XDR Collector Implementation and Data Confirmation

Data Collectors **Informational** **Integrations** **Taegis XDR**

0 Kudos

COMMENT

Powered by Khoros