

## **View Threat Intelligence Dashboard**

The **Threat Intelligence** page lists the most up-to-date data set for the Secure Workload pipeline that identifies and quarantines threats by inspecting the data center workloads against externally known malware command and control addresses, and security flaws in processes and geographical location.

The **Threat Intelligence** page lists the most up-to-date data set for the Secure Workload pipeline that identifies and quarantines threats by inspecting the data center workloads against externally known malware command and control addresses, and security flaws in processes and geographical location. From this page, you can also identify communication from workloads to well-known malicious IPv4 addresses. The malicious IP addresses are updated every 24 hours. You can choose to automatically update the threat intelligence data sets or manually upload the data sets to Secure Workload.



Note

The feature to identify well-known malicious IP addresses is disabled by default. To enable this feature, see Visibility of Well-Known Malicious IPv4 Addresses.

To manage threat intelligence, from the navigation pane, choose **Manage** > **Service Settings** > **Threat Intelligence**.

The **Threat Intelligence** page displays the updated status of threat intelligence data sets. These data sets are updated automatically.



Note

The Threat Intelligence feature requires a connection to Cisco Secure Workload servers to automatically update. Your enterprise outbound HTTP request may require:

- Allow the following domain from the enterprise firewall outbound rules: uas.tetrationcloud.com
- Configure your outbound HTTP Connection.

In environments without an outbound connection, upload the data sets directly. For more information, see the **Manual Uploads** section.

#### Table 1: Data Sets

Data set	Description
NVD CVEs	Security related software flaws, CVSS base score, vulnerable product configuration, and weakness categorization
MaxMind Geo	Identification of the location and other characteristics of source IPs
NIST RDS	NIST Reference Data Set of digital signatures of known, traceable software applications
Team Cymru	Insight on 3,000+ botnet command and control IPs
Hash Verdict	Verdict of Secure Workload on process hashes (only available with the Automatic Updates section).



Note

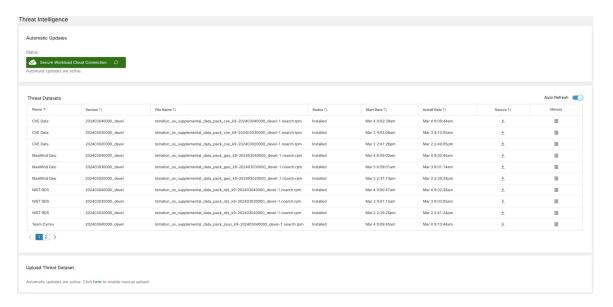
In case the MaxMind Geo data set is manually uploaded in an earlier release, you must reupload the corresponding RPM to view the location and related information on the Flow Visibility page.

- Automatic Updates, on page 2
- Manual Upload of Data Sets, on page 3

# **Automatic Updates**

Secure Workload updates threat data sets everyday between 3 to 4 a.m. UTC by synchronizing with the global data set available here. The global data set is refreshed weekly, on Fridays or Mondays. The Threat Intelligence dashboard lists the data sets and the date on which the data set was last updated.

Figure 1: Threat Intelligence



## **Manual Upload of Data Sets**



Note

**Scheduling Manual Uploads**: Data set RPM files are published to the Secure Workload Update Portal weekly. We recommend that you install the latest releases periodically by configuring a schedule for an administrator.

### **Download Updated Data Sets**

Download the latest threat data sets from here.

### **Upload Latest Data Sets**

#### Before you begin

Log in as a **Site Administrator** or **Customer Support Executive**.

### Procedure

- **Step 1** From the navigation pane, choose **Manage** > **Service Settings** > **Threat Intelligence**.
- Step 2 Under the Upload Threat Dataset section, enable manual upload.
- Step 3 Click Select Supplemental RPM and select the RPM files that are downloaded from the Secure Workload Update Portal.
- Step 4 Click Upload.

The RPM upload process is initiated and the status is displayed on a progress bar. After the upload, the RPM file is processed and installed in the background. The threat data sets are updated after the installation is complete.

Figure 2: Threat Data Sets

