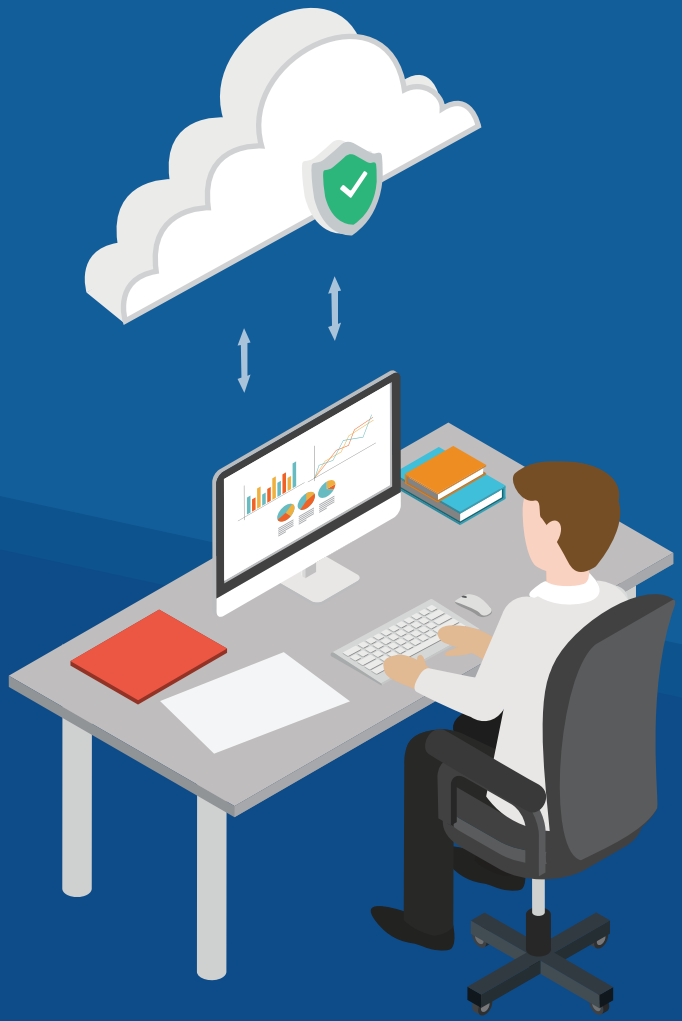
ManageEngine
Log360

Detecting network intruders with **STIX/TAXII feed processing**

A Guide



www.manageengine.com/products/log360/

Introduction

In today's evolving threat landscape, the key to efficient threat mitigation is early detection. The Structured Threat Information Expression (STIX), a structured language for describing threats, and the Trusted Automated Exchange of Indicator Information (TAXII) protocol, a collaborative threat sharing platform, both emerged as community-driven ways to defend against cyberthreats. Since STIX and TAXII provide global standards for identifying and sharing threat information, threat feeds based on these protocols are widely used and always provide the latest, most reliable threat information.

The ideal way to secure your organization's network would be to constantly update your threat database with these feeds. However, as any security administrator knows, updating your threat database frequently takes a lot of work. Log360, a log management and IT compliance solution with a built-in STIX/TAXII feed processor, makes it easy for you to detect threats in real time.

The STIX/TAXII feed processor updates the global threat database on local Log360 instances every day to ensure your threat feeds remain up-to-date. The global threat database also contains over 600 million blacklisted IP addresses that are collected from other trusted open sources and updated daily. Log360 sends alerts in real time whenever a blacklisted source tries to interact with your network, helping you detect threats early on.

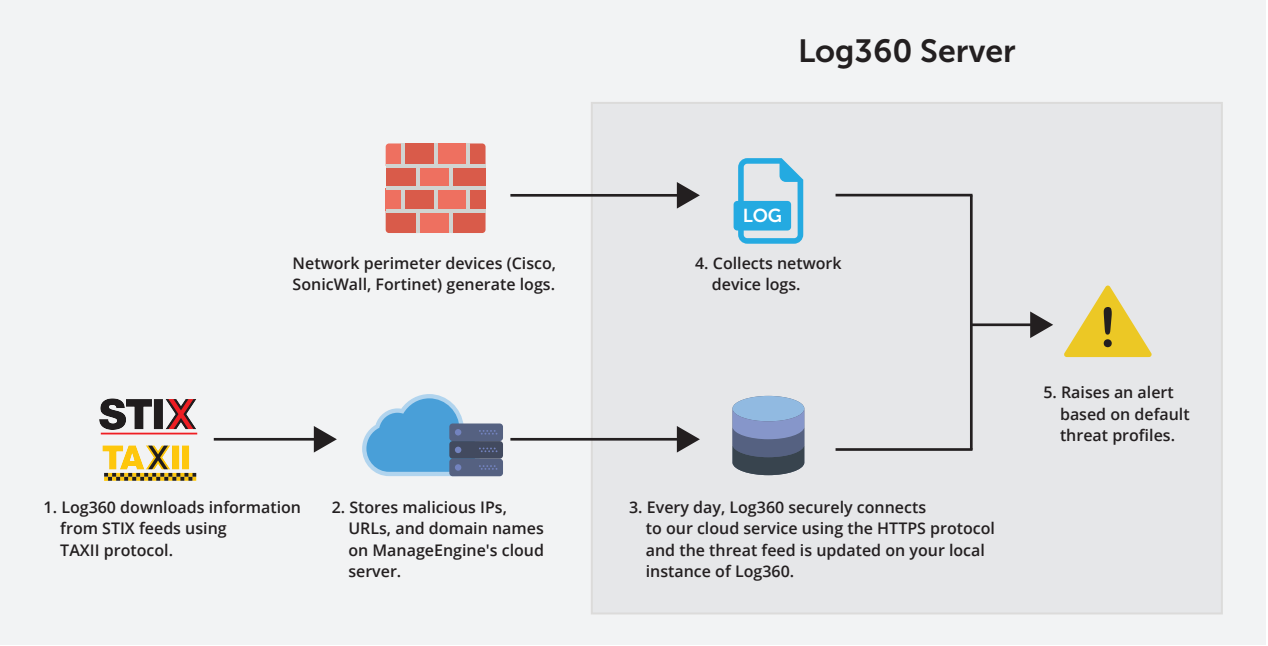
Threat detection with EventLog Analyzer

- **Access to a comprehensive knowledge base:** Log360 processes some of the most prominent threat feeds, including those based on the STIX/TAXII protocols.
  You can also add custom STIX/TAXII based feeds which your organization subscribes to.

- **Dynamic threat information:** Log360 automatically pulls the latest information from threat feeds, making sure you stay up-to-date.

- **No configurations required:** Log360 starts processing the feeds immediately after deployment.

How it works



1 Log360 downloads the threat feeds on a daily basis from two STIX/TAXII based feeds, **Hail A TAXII** and **AlienVault OTX.** If you have added any other custom feeds, it collects threat information from them as well.

2 The downloaded threat feeds (comprised of malicious IPs, URLs, and domain names) are stored in our cloud service so the Log360 server's resources, memory, and performance aren't affected.

3 Every day at 7am, Log360 securely connects to our cloud service using the HTTPS protocol and the threat feed is updated on your local instance of Log360. The files are named STIXdn.txt, STIXip4.txt, STIXsub.txt, and STIXurl.txt, and stored in <Home>/data/za/threatfeeds, where <Home> is the location where you've installed Log360.

4 Log360 collects the logs from all devices on your network.

5 It then correlates the log data with the threat feeds in real time, detects intrusion attempts from malicious domain names, URLs, or IPs if any, and sends out email or SMS notifications to the required security professionals.

Best of all, Log360 entire threat detection process listed above requires no configuration on your end. As soon as you've deployed Log360, its threat feed processor starts working automatically.

At a glance

- **What objects does the STIX/TAXII feed processor support?** Malicious IP addresses, URLs, and domain names that get reported in the STIX feeds are stored in Log360 global threat database.

- **What other information does the global threat database have?** It also contains over 600 million blacklisted IP addresses collected from other trusted open sources.

- **What protocol is used to transfer feeds from the cloud to local instance?** The local instance of Log360 connects to ManageEngine's cloud service using the secure HTTPS protocol.

- **How often is the threat data on the local instance updated?** The global threat database on the local instance is updated with the latest information every morning at 7am.
  If you have added custom threat feeds, information is retrieved and stored as per the schedule you've specified.

- **What gets correlated to detect threats instantly?** Log360 correlates logs from your network with the global threat database to detect threats.

Adding custom threat feeds to Log360

To add a new threat feed server,

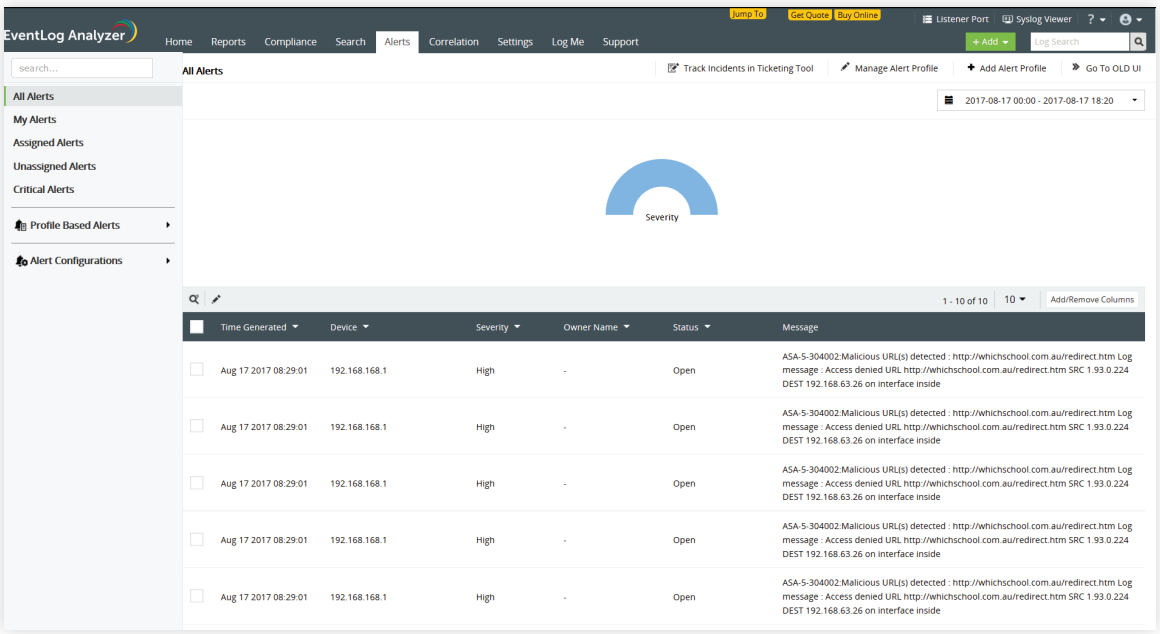
1. Go to **Settings > Threat Management > Add New Server.**
2. In the Add Server box, enter the desired Display name, URL, Username and Password.
3. In the "Schedule" drop down list, select the desired type of schedule and the exact time for the TAXII server feed collection.
4. In the "Poll from" box, pick a date from when the past feeds should be collected.
5. To save the server configuration click on Add Server.

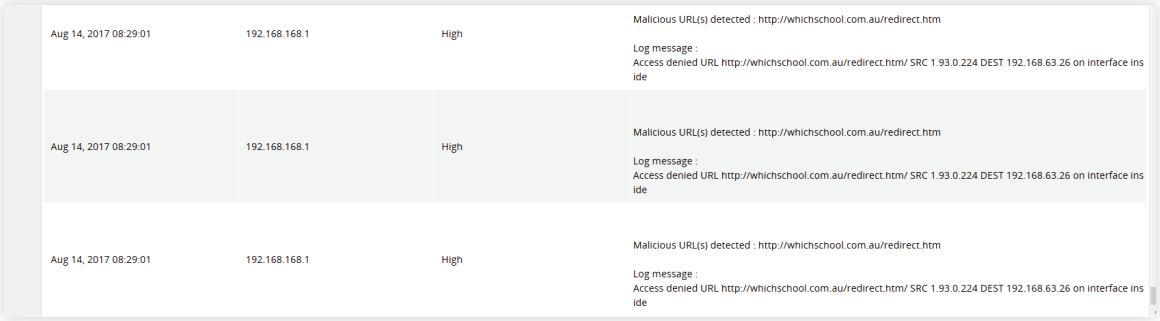
You can also edit, delete, or manage the added threat feeds from the **Settings > Threat Management** page.

Accessing alert notifications for Log360 threat intelligence platform

All the alerts that get triggered from Log360 threat intelligence platform can be found in Alerts -> Profile-based alerts -> Default threats.

To change the notification settings for these alert profiles, click on the Manage Alert Profile button or the edit icon ( ).





Log360 allows you to take advantage of a global knowledge base of threats and ensure no malicious intruder can breach your network. Apart from real-time alerts, the solution also allows you to manage the alerts as tickets by assigning owners, updating their status, and more. All this requires no additional setup, so you get to add an extra layer of security with virtually no effort.