Lastline Enterprise Tanium IOC Detect Integration

January 17, 2024

6950 Hollister Avenue, Suite 100
Goleta, CA 93117
lastline.com | 805.456.7076

1 Introduction

This guide describes the integration of Tanium IOC Detect into Lastline Enterprise.

The Tanium IOC Detect Integration allows Lastline Enterprise to verify infections reported by the Lastline Analysis Report, through the Tanium IOC Detect service, by matching IOCs generated by Lastline.

In the next sections this guide will explain how to configure and use Tanium IOC Detect Integration.

2 Overview of the Tanium IOC Detect Integration

2.1 Glossary

This section briefly explains the meaning of some of the terms that are used in this guide.

2.1.1 IOC

Indicator of compromise, is a forensic artifact observed on a network or on a host that, with high confidence, indicates a computer intrusion. Typical IOCs are virus signatures, IP addresses, MD5 hashes of malware files, URLs or domain names of botnet command and control servers, registry settings, process handles, name changes. IOCs are represented in a human-readable format, often XML. There exists several initiatives to standardize format of IOCs for more efficient automated processing.

2.1.2 OpenIOC

A threat information sharing standard that allows to logically group forensic artifacts and communicate this information in a machine readable format. OpenIOC can be defined as a language to describe IOCs and is written in XML.

2.1.3 STIX

Structured Threat Information Expression, is a structured language for describing cyber threat information so it can be shared, stored and analyzed in a consistent manner.

2.1.4 Tanium IOC Detect

Service offered by Tanium, Inc. that provides IOC detection, management and analysis capabilities that scale to the enterprise for real-time responses to intrusions. Currently, Tanium supports IOCs in OpenIOC and STIX format.

2.1.5 IOC Detection

The process of searching for IOCs on specified host machines on a network.

2.2 Architecture

When using Tanium IOC Detect Integration, it is possible to verify infections reported by the Lastline Enterprise Analysis Report on host machines, through the Tanium IOC Detect service. When a report is generated by Lastline Analysis Report after a successfull analysis of a submitted resource (currently supported for the integration are Windows executables) the user may choose to run a detection with Tanium IOC Detect on all host machines having Tanium IOC Detect installed. This process works by generating an IOC, in OpenIOC format, from the Lastline Analysis Report and using it as input for the Tanium IOC Detect service.

Once Tanium IOC Detect has completed the detection, a summary of the results will be displayed next to the analysis report tab on the user portal.

3 Requirements

- An updated version of the Tanium server needs to be installed (this integration works for version 6.5.314.4301 or later) on a server machine.
- The Tanium client must be deployed on the host machines on which the user wants to run the detection.
- The integrated Tanium IOC Detect workbench needs to be installed in the Tanium server console (current version used for the integration is 2.0.4.41)
- The Tanium IOC Detect tools needs to be deployed on the client machines.

4 Configuration

4.1 Tanium server and client installation

The first step consists in the installation of the Tanium server on the server machine and the deployment of the Tanium client on the host machines. Follow the guide at https://kb.tanium.com/Tanium_Server_Installation to complete this step.

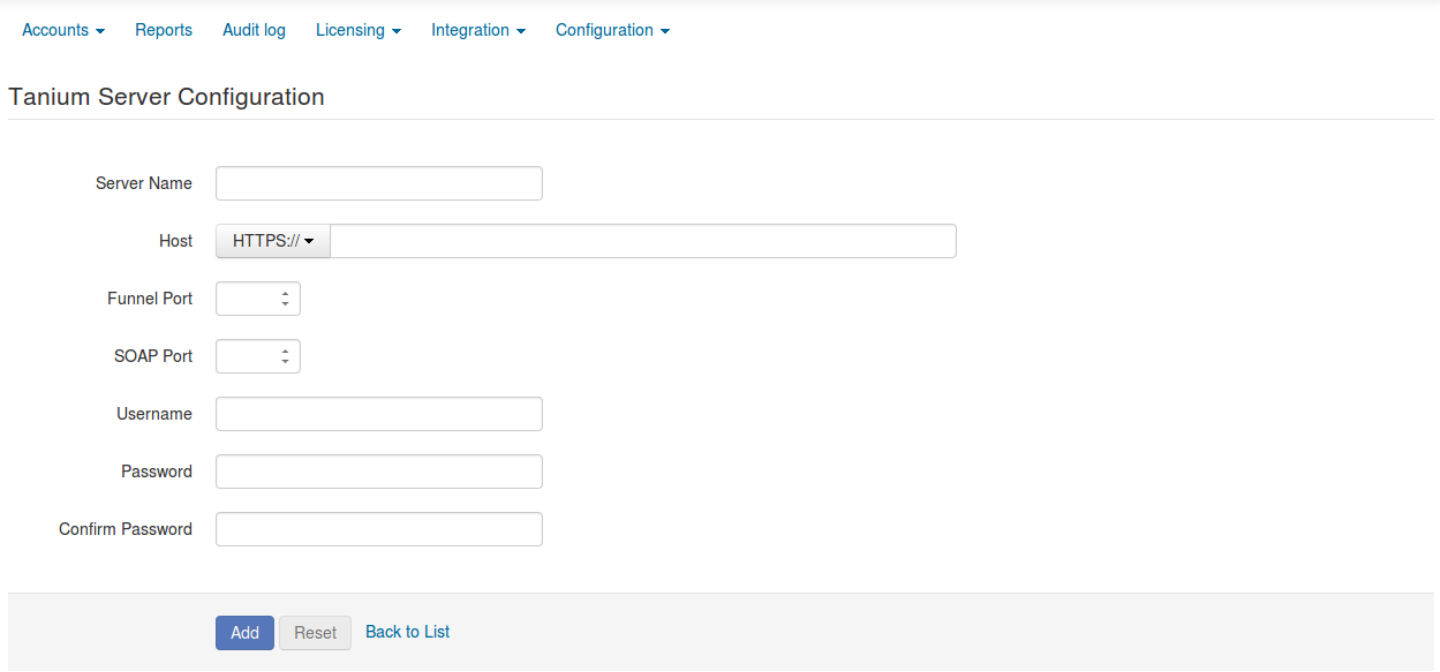
4.2 Tanium IOC Detect installation

The next step consists in the installation of the Tanium IOC Detect workbench inside the Tanium Console and the distribution of the IOC Detect tools on the client machines. Follow the guide at https://kb.tanium.com/IOC_Detect_Install_Guide, to perform this procedure.

4.3 Tanium server configuration

Once the Tanium server and IOC Detect service are operational on the server machine, and the client and IOC Detect tools are deployed on he host machines, the user needs to insert on the Lastline portal the configuration to allow the interaction with the server. From the user portal go to "Admin" → "Integration" → "Tanium Server Configuration".

Click on the "+" button on the right side to enter the server configuration screen.



Insert the Tanium server configuration

The user will then be asked to fill a form specifying:

- name of the server
- HTTP protocol (either "HTTP" or "HTTPS")
- IP address or hostname of the server
- port on which the the Tanium IOC Detect service is listening on (443 by default)
- port on which the Tanium SOAP API is listening on (443 by default)
- username and password needed for authenticating to the Tanium server

4.4 Lastline Analysis Report

To be able to launch a detection using Tanium IOC Detect, the user needs to start from a successful Lastline analysis of a windows executable, like the one shown in the example image below.

Overview Report

Analysis Overview for 6062fdc71440cb97db32c645627e181f

Comments (0)

Analysis Overview

MD5	6062fdc71440cb97db32c645627e181f
SHA1	1b6fc019b91a304f3d39dcba19b570aa91f69a63
MIME Type	application/x-pe-app-32bit-i386
Submission	2015-07-29 02:56:49 UTC

Threat Level

The file 6062fdc71440cb97db32c645627e181f was found to be malicious.

Risk Assessment

Maliciousness score 75/100
Risk estimate High Risk - Malicious behavior detected

Analysis Overview

Type	Description
File	Modifying executable in Windows directory

Third-party tools

VirusTotal link report.

A successful Lastline analysis overview

From the analysis overview go to the "Report" section and click on the laptop icon on the top-right corner of the page.

Overview Report Timeline

Artifacts Subject 1 (awree.exe)

Analysis information ?

Analysis subject 3dcf90df1aab266f52251cf463ee337f
Analysis type Dynamic analysis on Microsoft Windows 10

Events Report

Artifacts

Analysis Subject 1 (awree.exe)

Name	awree.exe

Lastline Analysis Report page

Select a sensor license to associate with the IOC matching result (which will be needed as network identifier), then select one of the previously inserted Tanium server configurations and click "submit" to start the Tanium IOC Detect detection.

Once the detection has started, the user will be taken to a page showing the progress of the process.

When Tanium completes the detection on the host machines, the page will be updated with the results. In case one or more of the host machines were identified as compromised by Tanium IOC Detect, the results will show the name of the host machine and its IPv4 and IPv6 adresses.

Overview | Report | IoC Tanium

Tanium IoC Request Information

Task UUID	0a715016f66a46949017ba313f057b1a
Report	View Report Download IOC in OPENIOC Format for Tanium

Tanium IoC Task Information

Progress	completed
Start Time	2015-07-29 19:04:19
End Time	2015-07-29 19:06:13
Result	Success

Detection concluded and the following hosts were identified as compromised: [CompromisedHost(name='win8-1.lastline-test.com', ip_v4='10.2.72.12', ip_v6='fe80::64e1:1022:2930:628b')]

Page showing the results of a successful detection