SLASHNEXT

USER GUIDE V1.0.0

SlashNext Automated Data Enrichment Guide Anomali

TABLE OF CONTENTS

1 | INTRODUCTION

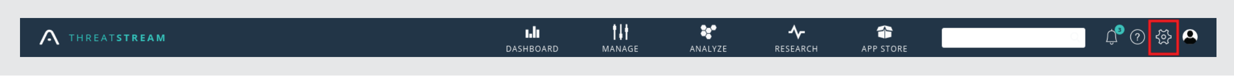
This document outlines the process to install the Enrichment Integration provided by SlashNext into the Anomali ThreatStream Platform and also provides details on how to efficiently use the integration to acquire detailed threat information from SlashNext for IPs, Domains and URLs.

SlashNext, Inc has developed a Context-Based Enrichment Integration for the Anomali ThreatStream platform so that SOC analysts and IR teams can leverage SlashNext's On-demand Threat Intelligence cloud platform within the ThreatStream platform to track down potentially malicious Indicators of Compromise (IoC).

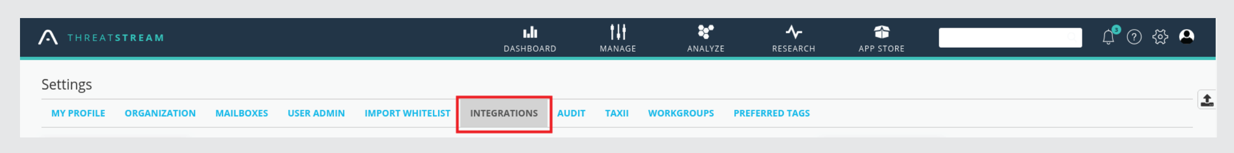
2 | CONFIGURATION

To configure and activate the SlashNext Enrichment bundle for ThreatStream platform, follow the steps mentioned below:

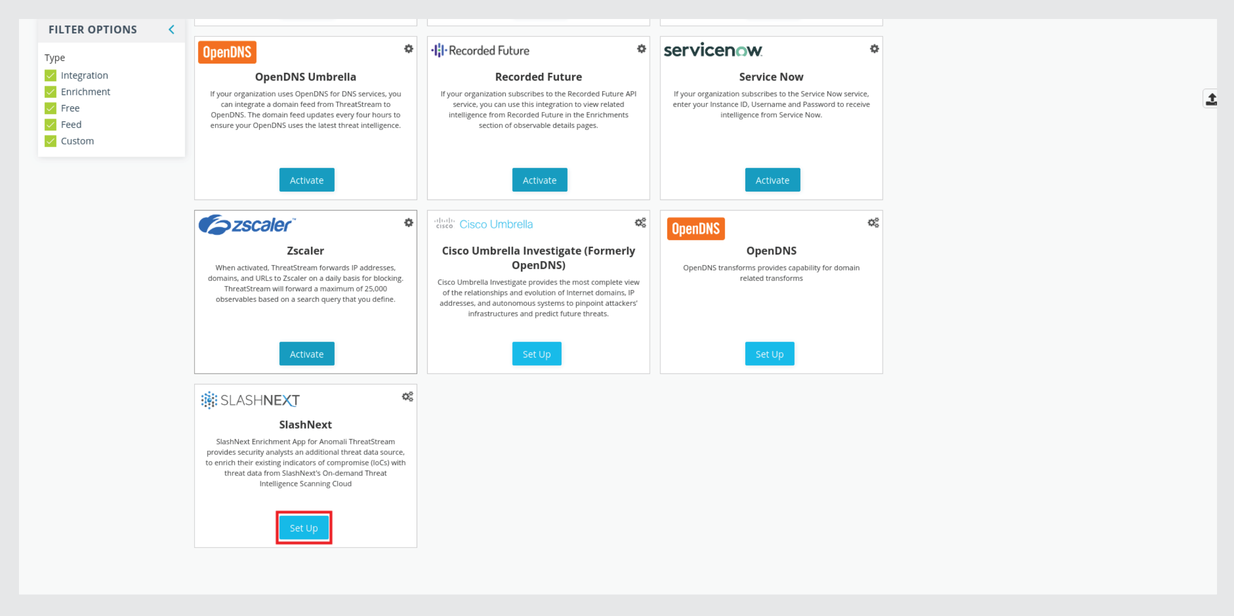
1. Click on **Settings** button on the top menu-bar to go to the Settings of Anomali ThreatStream



2. On the Settings page, click on **Integrations** tab as shown below to see all the installed Enrichment integrations



3. All the Enrichment Integrations installed in your Anomali ThreatStream integration will now appear. If you do not see **SlashNext** on the page, contact Anomali Support to install it in your instance. Click on the **Setup** button as shown below to configure SlashNext Enrichment



OpenDNS Umbrella

If your organization uses OpenDNS for DNS services, you can integrate a domain feed from ThreatStream to OpenDNS. The domain feed updates every four hours to ensure your OpenDNS uses the latest threat intelligence.

Recorded Future

If your organization subscribes to the Recorded Future API service, you can use this integration to view related intelligence from Recorded Future in the Enrichments section of observable details pages.

Service Now

If your organization subscribes to the Service Now service, enter your Instance ID, Username and Password to receive intelligence from Service Now.

Zscaler

When activated, ThreatStream forwards IP addresses, domains, and URLs to Zscaler on a daily basis for blocking. ThreatStream will forward a maximum of 25,000 observables based on a search query that you define.

Cisco Umbrella Investigate (Formerly OpenDNS)

Cisco Umbrella Investigate provides the most complete view of the relationships and evolution of Internet domains, IP addresses, and autonomous systems to pinpoint attackers' infrastructures and predict future threats.

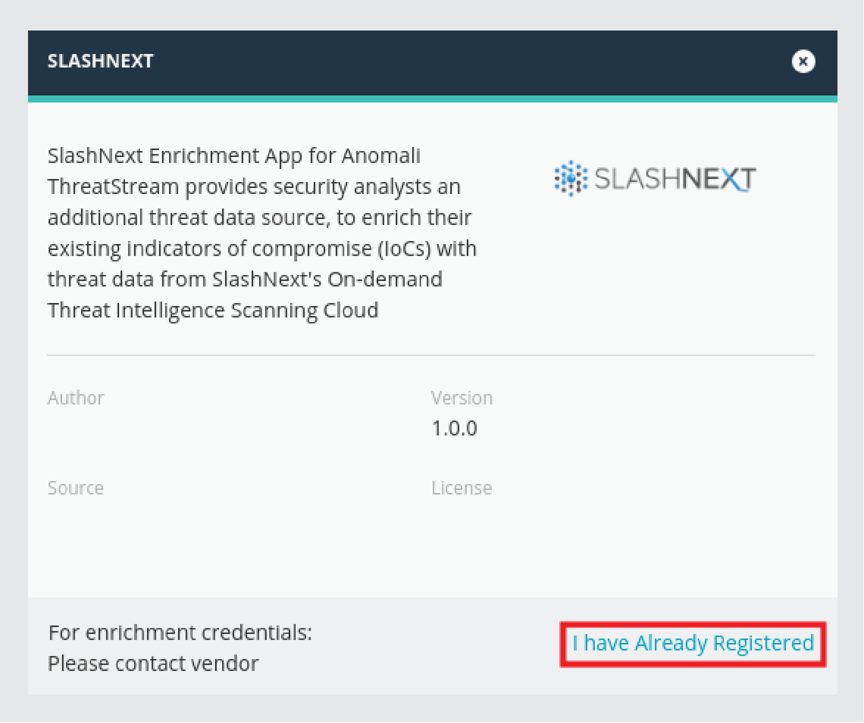
OpenDNS

OpenDNS transforms provides capability for domain related transforms

SlashNext

SlashNext Enrichment App for Anomali ThreatStream provides security analysts an additional threat data source, to enrich their existing indicators of compromise (IoCs) with threat data from SlashNext's On-demand Threat Intelligence Scanning Cloud

4. A dialog box will appear as shown below, click on **I have Already Registered** text if you have obtained an API key from SlashNext, otherwise contact support@slashnext.com to get your API key.



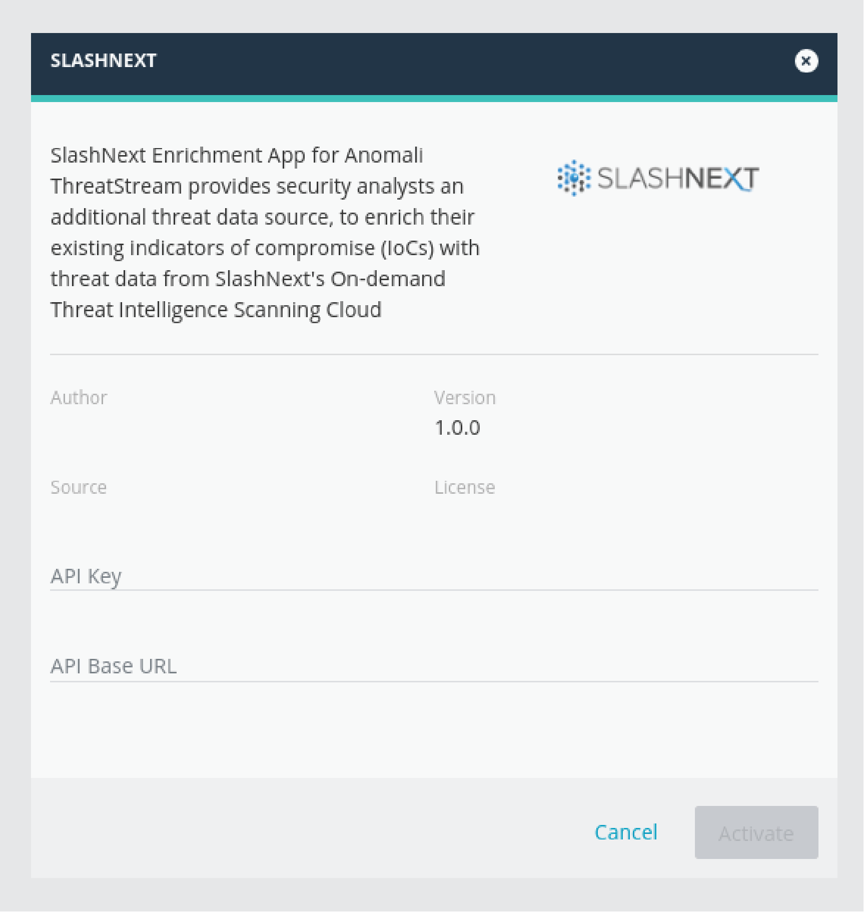
SLASHNEXT

SlashNext Enrichment App for Anomali ThreatStream provides security analysts an additional threat data source, to enrich their existing indicators of compromise (IoCs) with threat data from SlashNext's On-demand Threat Intelligence Scanning Cloud

Author	Version 1.0.0
Source	License

For enrichment credentials:
Please contact vendor

4. Insert your SlashNext **API key** in the API Key text-field. Optionally, you can also specify an alternate API Base URL, if and only if, specifically specified by SlashNext otherwise leave it empty. Finally, click on the **Activate** button to finish your configuration.



SLASHNEXT

SlashNext Enrichment App for Anomali ThreatStream provides security analysts an additional threat data source, to enrich their existing indicators of compromise (IoCs) with threat data from SlashNext's On-demand Threat Intelligence Scanning Cloud

Author	Version 1.0.0
Source	License

API Key

API Base URL

If you leave **API Base URL** empty, SlashNext Enrichment will use the default base URL of: https://oti.slashnext.cloud/api

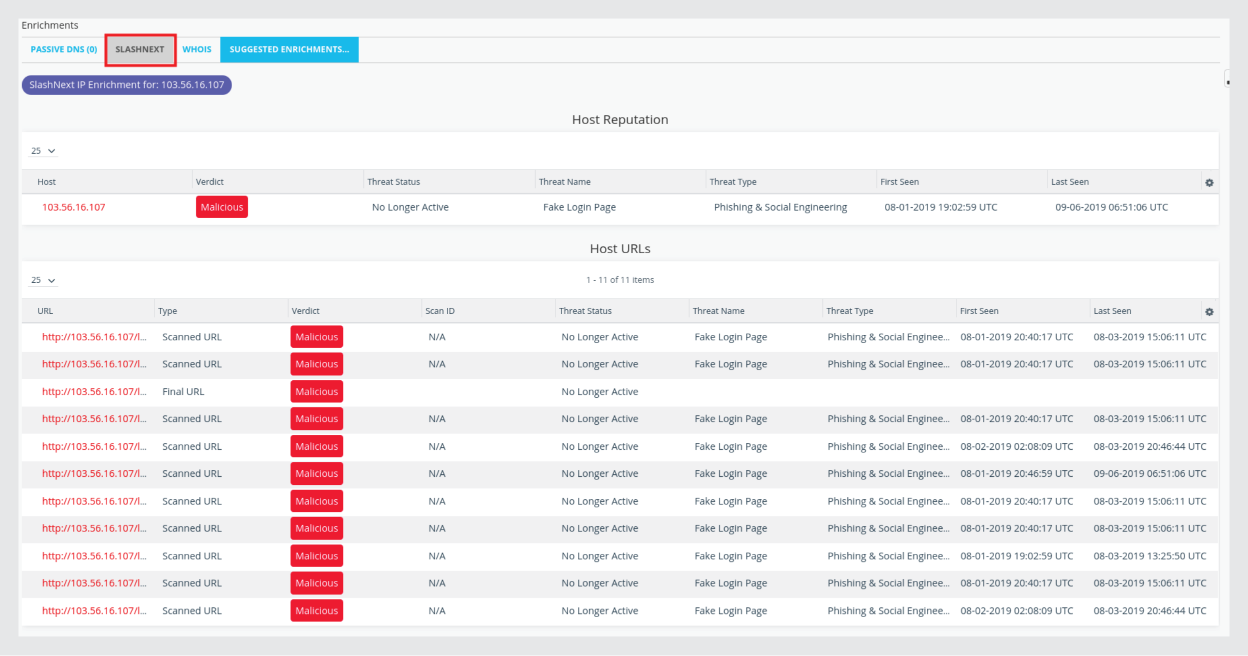
At this point, the configuration for your SlashNext Enrichment is complete and is ready to be used. In case any error occurs, contact Anomali Support for further assistance.

3 | SUPPORTED ENRICHMENTS

When activated, SlashNext Enrichment for ThreatStream supports enrichment for three types of indicators as shown below:

3.1 | IP ENRICHMENT

On the details page of an IP, click on **SLASHNEXT** tab under the **Enrichments** sections (as shown below) to fetch the enrichment data for that particular IP



Host Reputation

Host	Verdict	Threat Status	Threat Name	Threat Type	First Seen	Last Seen
103.56.16.107	Malicious	No Longer Active	Fake Login Page	Phishing & Social Engineering	08-01-2019 19:02:59 UTC	09-06-2019 06:51:06 UTC

Host URLs

1 - 11 of 11 items

URL	Type	Verdict	Scan ID	Threat Status	Threat Name	Threat Type	First Seen	Last Seen
http://103.56.16.107/l...	Scanned URL	Malicious	N/A	No Longer Active	Fake Login Page	Phishing & Social Enginee...	08-01-2019 20:40:17 UTC	08-03-2019 15:06:11 UTC
http://103.56.16.107/l...	Scanned URL	Malicious	N/A	No Longer Active	Fake Login Page	Phishing & Social Enginee...	08-01-2019 20:40:17 UTC	08-03-2019 15:06:11 UTC
http://103.56.16.107/l...	Final URL	Malicious		No Longer Active				
http://103.56.16.107/l...	Scanned URL	Malicious	N/A	No Longer Active	Fake Login Page	Phishing & Social Enginee...	08-01-2019 20:40:17 UTC	08-03-2019 15:06:11 UTC
http://103.56.16.107/l...	Scanned URL	Malicious	N/A	No Longer Active	Fake Login Page	Phishing & Social Enginee...	08-02-2019 02:08:09 UTC	08-03-2019 20:46:44 UTC
http://103.56.16.107/l...	Scanned URL	Malicious	N/A	No Longer Active	Fake Login Page	Phishing & Social Enginee...	08-01-2019 20:46:59 UTC	09-06-2019 06:51:06 UTC
http://103.56.16.107/l...	Scanned URL	Malicious	N/A	No Longer Active	Fake Login Page	Phishing & Social Enginee...	08-01-2019 20:40:17 UTC	08-03-2019 15:06:11 UTC
http://103.56.16.107/l...	Scanned URL	Malicious	N/A	No Longer Active	Fake Login Page	Phishing & Social Enginee...	08-01-2019 20:40:17 UTC	08-03-2019 15:06:11 UTC
http://103.56.16.107/l...	Scanned URL	Malicious	N/A	No Longer Active	Fake Login Page	Phishing & Social Enginee...	08-01-2019 19:02:59 UTC	08-03-2019 13:25:50 UTC
http://103.56.16.107/l...	Scanned URL	Malicious	N/A	No Longer Active	Fake Login Page	Phishing & Social Enginee...	08-01-2019 20:40:17 UTC	08-03-2019 15:06:11 UTC
http://103.56.16.107/l...	Scanned URL	Malicious	N/A	No Longer Active	Fake Login Page	Phishing & Social Enginee...	08-02-2019 02:08:09 UTC	08-03-2019 20:46:44 UTC

Host Reputation

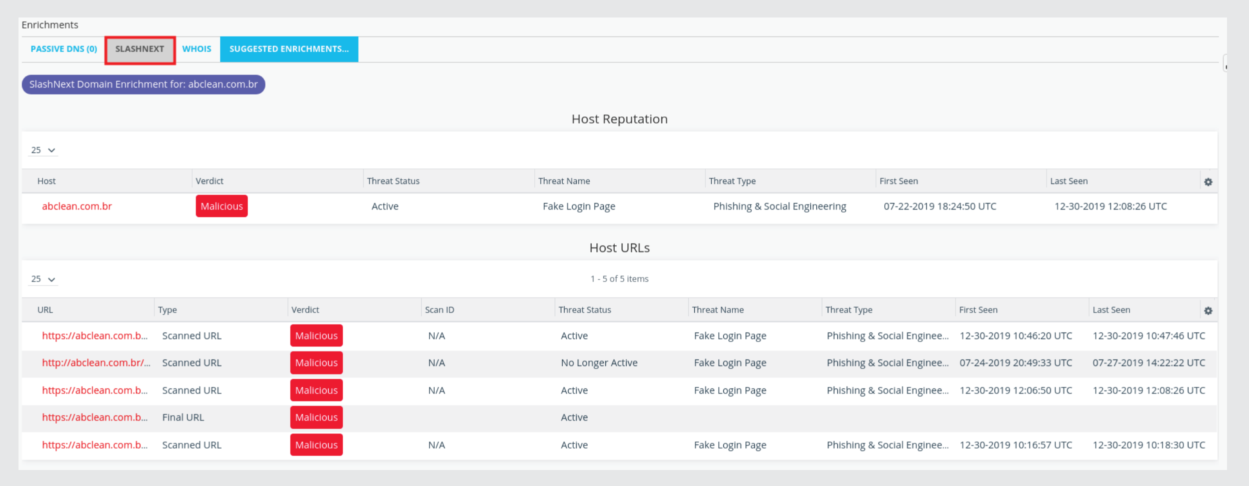
The **Host Reputation** table provides details on whether the IP is Malicious or Benign and, if malicious, the detailed information about the threat posed by the particular IP.

Host URLs

The **Host URLs** table provides a list of all the URLs scanned under that particular IP and their detailed threat information, respectively.

3.2 | DOMAIN ENRICHMENT

Similarly, on the details page of a Domain indicator, click on **SLASHNEXT** tab under the **Enrichments** sections to fetch the enrichment data for that particular Domain



SlashNext Domain Enrichment for: abclean.com.br

Host Reputation

Host	Verdict	Threat Status	Threat Name	Threat Type	First Seen	Last Seen
abclean.com.br	Malicious	Active	Fake Login Page	Phishing & Social Engineering	07-22-2019 18:24:50 UTC	12-30-2019 12:08:26 UTC

Host URLs

1 - 5 of 5 items

URL	Type	Verdict	Scan ID	Threat Status	Threat Name	Threat Type	First Seen	Last Seen
https://abclean.com.b...	Scanned URL	Malicious	N/A	Active	Fake Login Page	Phishing & Social Enginee...	12-30-2019 10:46:20 UTC	12-30-2019 10:47:46 UTC
http://abclean.com.br/...	Scanned URL	Malicious	N/A	No Longer Active	Fake Login Page	Phishing & Social Enginee...	07-24-2019 20:49:33 UTC	07-27-2019 14:22:22 UTC
https://abclean.com.b...	Scanned URL	Malicious	N/A	Active	Fake Login Page	Phishing & Social Enginee...	12-30-2019 12:06:50 UTC	12-30-2019 12:08:26 UTC
https://abclean.com.b...	Final URL	Malicious		Active				
https://abclean.com.b...	Scanned URL	Malicious	N/A	Active	Fake Login Page	Phishing & Social Enginee...	12-30-2019 10:16:57 UTC	12-30-2019 10:18:30 UTC

Host Reputation

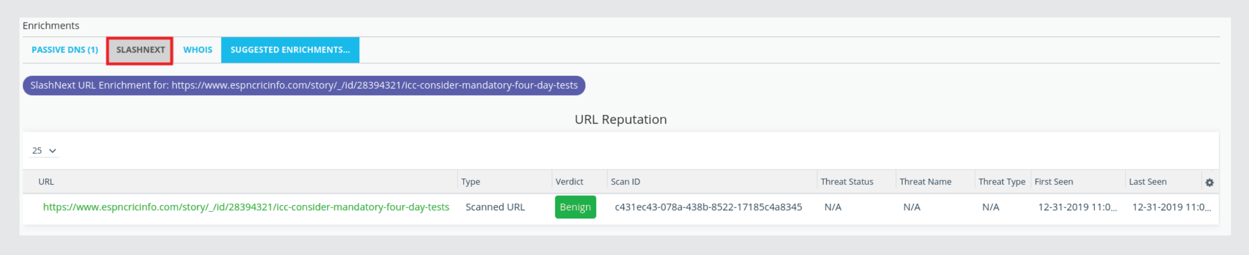
The **Host Reputation** table provides details on whether the Domain is Malicious or Benign and, if malicious, the detailed information about the threat posed by the particular Domain.

Host URLs

The **Host URLs** table provides a list of all the URLs scanned under that particular Domain and their detailed threat information, respectively.

3.3 | URL ENRICHMENT

Enrichment for a URL can be fetched on the details page of a URL by clicking on **SLASHNEXT** tab under **Enrichments** section



SlashNext URL Enrichment for: https://www.espncricinfo.com/story/_/id/28394321/icc-consider-mandatory-four-day-tests

URL Reputation

URL	Type	Verdict	Scan ID	Threat Status	Threat Name	Threat Type	First Seen	Last Seen
https://www.espncricinfo.com/story/_/id/28394321/icc-consider-mandatory-four-day-tests	Scanned URL	Benign	c431ec43-078a-438b-8522-17185c4a8345	N/A	N/A	N/A	12-31-2019 11:0...	12-31-2019 11:0...

URL Reputation

URL Reputation table provides details on whether the scanned URL is Malicious or Benign and the exact details of the threat posed by the URL (if any)