SLASHNEXT

USER GUIDE V1.0.0

SlashNext Threat Intelligence Integration Guide Anomali TIP

TABLE OF CONTENTS

1 | INTRODUCTION

SlashNext threat intelligence provides three types of feeds as per the corresponding type of IoCs which are listed below.

1. SlashNext Intel – Phishing IPs as the name indicates contains IPv4 IoCs and are added with iType set to Phishing IP.
2. SlashNext Intel – Phishing FQDNs as the name indicates contains domain IoCs and are added with iType set to Phishing Domain.
3. SlashNext Intel – Phishing Wildcard URLs as the name indicates contains wildcard URL IoCs and are added with iType set to Phishing URL.

All the IoCs within SlashNext threat feeds have 4 attributes which have been added as tags to facilitate the filtering of feed to get a list of more desired IoCs as per threat nature or as per usage.

1. Threat Type as the name indicates contains the broad threat nature pose by the IoC.
2. Threat Name as the name indicates contains the exact threat name pose by the IoC.
3. First Seen as the name indicates contains the timestamp when the IoC was first observed to be active threat.
4. Last Seen as the name indicates contains the timestamp when the IoC was last observed to be active threat.

> **Note**
> The integration of SlashNext feeds is done by Anomali feeds team and customer don't need to worry about this. They can skip to List Specific IoCs.

2 | FEED INTEGRATION

This document should be accompanied by a SlashNext feeds integration python script which fetches the SlashNext threat feeds using a web API after authentication with SlashNext Cloud, parse the received IoCs as per Anomali requirements and then upload the feeds to Anomali platform.

2.1 | REQUIREMENTS

Following lists the requirements to run the SlashNext feeds integration python script and upload the IoCs provided by SlashNest to Anomali threat intelligence platform.

1. Access to an Anomali instance
2. Installed Anomali feeds SDK
3. Python version 2.7
4. Requests library for python 2.7

2.2 | EXECUTION

In order to execute the SlashNext feeds integration python, Anomali feed SDK virtual environment should be activated and Anomali environmental variables should be sourced.

There are three types of feeds provided by SlashNext;

1. SlashNextIntel – Phishing IPs
2. SlashNextIntel – Phishing FQDNs
3. SlashNextIntel – Phishing Wildcard URLs

Any of the above threat feed can be integrated using the following command.

```
python IntegrateSlashNext.py -a <api_key> -<feed_type><auto_expire>
```

Where

1. api_key = API key provisioned by SlashNext
2. feed_type = “i, d, u or w” to indicate one of the SlashNext feed type
3. auto_expire = “e” to enable the auto expiration of IoCs within 1 day

By default, Anomali expires the IoC after 90 days of last ingestion by enabling auto expiration the IoC shall expire within 1 day of last ingestion, this is required considering the highly dynamic nature of SlashNext feeds.
Specific feed integration example are given below.

SlashNextIntel – Phishing IPs feed can be integrated/updated by executing following command.

```
python IntegrateSlashNext.py -a XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX -ie
```

SlashNextIntel – Phishing FQDNs feed can be integrated/updated by executing following command.

```
python IntegrateSlashNext.py -a XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX -de
```

SlashNextIntel – Phishing Wildcard URLs feed can be integrated/updated by executing following command.

```
python IntegrateSlashNext.py -a XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX -we
```

For further information, please use the following command.

```
python IntegrateSlashNext.py -h
```

3 | LIST SPECIFIC IoCs

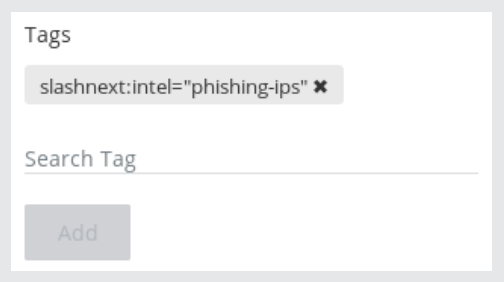
Within Anomali platform the user can filter the SlashNext feed to specifically list the IoCs as per requirements.

3.1 | FILTER FEED TYPES

Filtering can be performed by going to **ANALYZE** → **Observables** in ThreatStream instance as shown in the following snapshot.

If the user intends to get only the IP type IoC from SlashNext with Anomali threat intelligence platform, the user should look for following tag in the Filter Options pane as shown in the following snapshot.

Searched tag
slashnext:intel="Phishing-IPs"



Similarly for domain type IoCs the tag filtered should be.

Searched tag
slashnext:intel="Phishing-FQDNs"

And for wildcard URL IoCs the tag is

Searched tag
slashnext:intel="Phishing-Wildcard-URLs"

3.2 | FILTER ATTRIBUTES

SlashNext feed contains following values of **Threat Type**

Phishing & Social Engineering

Searched tag
slashnext:threat-type="Phishing-&-Social-Engineering"

Malware & Exploit

Searched tag
slashnext:threat-type="Malware-&-Exploit"

Callback/C2

Searched tag
slashnext:threat-type="Callback/C2"

Each of the above threat type is further divided based upon the Threat Name which are plentiful so only a few are listed below.

1. Fake Login Page (slashnext:threat-name="Fake-Login-Page")
2. Scareware (slashnext:threat-name="Scareware")
3. Rogue Software (slashnext:threat-name="Rogue-Software")
4. Internet Scam (slashnext:threat-name="Internet-Scam")
5. Exploit:Win32/MSDocs (slashnext:threat-name="Exploit:Win32/MSDocs")
6. BadObject:Multi/RogueBinary (slashnext:threat-name="BadObject:Multi/RogueBinary")
7. BadObject:Win32/InstallCore (slashnext:threat-name="BadObject:Win32/InstallCore")
8. Trojan:OSX/SearchJack (slashnext:threat-name="Trojan:OSX/SearchJack")
9. Trojan:Win32/Hijacker (slashnext:threat-name="Trojan:Win32/Hijacker")
10. Trojan:Multi/RogueExtension (slashnext:threat-name="Trojan:Multi/RogueExtension")
11. Trojan:Win32/Spigot (slashnext:threat-name="Trojan:Win32/Spigot")
12. BankingTrojan:Win32/Zbot (slashnext:threat-name="BankingTrojan:Win32/Zbot")
13. ... ...

User can perform IoC filtration based upon each and every one of the above threat type and threat name through their respective tags.