SLASHNEXT

USER GUIDE V1.0.0

SlashNext Phishing IR Integration Guide Tines SOAR

TABLE OF CONTENTS

1 | INTRODUCTION

This document outlines the process to using the phishing incident response APIs provided by SlashNext into Tine SOAR platform and also provides details on how to efficiently use these on-demand threat intelligence APIs to request reputation and real-time scan of specific IoCs.

SlashNext Phishing Incident Response integration APIs/Agents enables Tines users to fully automate analysis of suspicious URLs. For example, IR teams responsible for abuse inbox management can extract links or domains out of suspicious emails and automatically analyze them with the SlashNext SEER™ threat detection cloud to get definitive, binary verdicts (malicious or benign) along with IOCs, screenshots, and more. Automating URL analysis can save IR teams hundreds of hours versus manually triaging these emails or checking URLs and domains against less accurate phishing databases and domain reputation services.

The **SlashNext Phishing Incident Response** integration app enables Tines users to fully automate analysis of suspicious URLs in phishing emails, network logs, and more. Stories/Playbooks that require URL or Domain analysis can automatically analyze them with the **SlashNext SEER™** threat detection cloud to get definitive, binary verdicts (malicious or benign) along with IOCs, screenshots, and more.

SlashNext threat detection uses browsers in a purpose-built cloud to dynamically inspect page contents and site behavior in real-time. This method enables SlashNext to follow URL re-directs and multi-stage attacks to more thoroughly analyze the final page(s) and makes a much more accurate, binary determination with near-zero false positives. It also detects all six major categories of phishing and social engineering sites. These include credential stealing, rogue software / malware sites, scareware, phishing exploits (sites hosting weaponized documents, etc.), and social engineering scams (fake deals, giveaways, etc.).

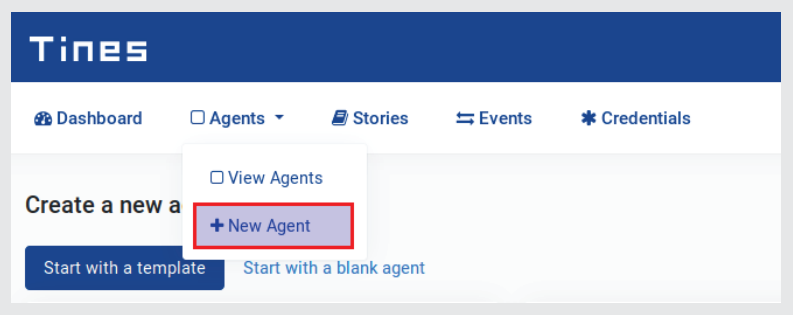
Use cases include abuse inbox management where SOC teams can automate URL analysis in phishing emails to save hundreds of hours versus more manual methods. Stories/Playbooks that mine and analyze network logs can also leverage SlashNext URL analysis on demand.

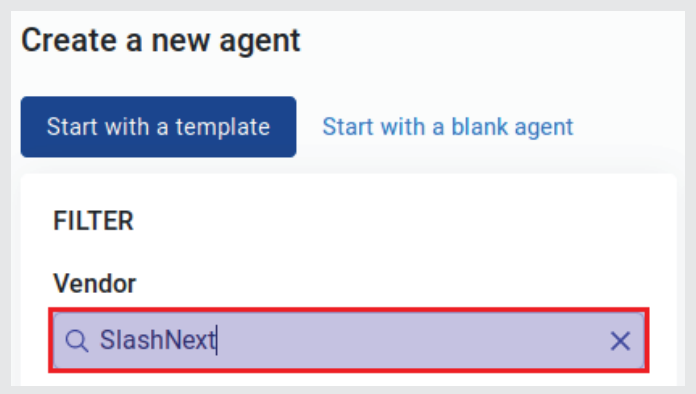
SlashNext not only provides accurate, binary verdicts (rather than threat scores), it provides IOC metadata and screenshots of detected phishing pages. These enables easier classification and reporting. Screenshots can be used as an aid in on-going employee phishing awareness training and testing.

The SlashNext Phishing Incident Response integration APIs/Agents uses an API key to authenticate with SlashNext cloud. If you don't have a valid API key, contact the SlashNext team: support@slashnext.com

2 | AGENT TEMPLATES

SlashNext provides HTML agent templates that corresponds to SlashNext Phishing Incident Response APIs within Tines to ease the process of developing a playbook/story or integrating these to an existing story/playbook which can be found under "Agents → New Agent" and then search for "SlashNext" under "FILTER → Vendor" as shown below.





SlashNext Phishing Incident Response integration provides following eight agent templates;

2.1 | GET HOST REPUTATION FROM SLASHNEXT

Search in SlashNext Cloud database and retrieve reputation of a host. Host can be either be a domain name or an IPv4 address. For an API Key contact support@slashnext.com

Template Details

```
{
        url: https://oti.slashnext.cloud/api/oti/v1/host/reputation
        content_type: json
        method: post
        payload:
        {
                authkey: {% credential SlashNext %}
                url: {{.host}}
        }
        expected_update_period_in_days: 1
}
```

SlashNext = SlashNext API key added to credentials section of Tines
.host = Host can either be a domain or an IPv4, can be either passed as direct value or a parameter from any above connected agents

2.2 | GET HOST'S URLS FROM SLASHNEXT

Search in SlashNext Cloud database and retrieve list of all URLs associated with the specified host. Host can be either be a domain name or IPv4 address. By default, a maximum of 10 associated URLs records will be fetched. For more records pagination is in place with page and rpp parameters.

Template Details

```
{
        url: https://oti.slashnext.cloud/api/oti/v1/host/report
        content_type: json
        method: post
        payload:
        {
                authkey: {% credential SlashNext %}
                url: {{.host}}
                page: 1
                rpp: 10
        }
        expected_update_period_in_days: 1
}
```

SlashNext = SlashNext API key added to credentials section of Tines
.host = Host can either be a domain or an IPv4, can be either passed as direct value or a parameter from any above connected agents

2.3 | SUBMIT URL TO SLASHNEXT FOR SCAN

Perform a real-time URL reputation scan with SlashNext cloud-based SEER Engine. If the specified URL already exists in the cloud database, scan results will get returned immediately. If not, this command will submit a URL scan request and return with 'check back later' message along with a unique Scan ID. User can check results of this scan with same API after 60 seconds or later using the returned Scan ID. For an API Key contact support@slashnext.com

Template Details

```
{
        url: https://oti.slashnext.cloud/api/oti/v1/url/scan
        content_type: json
        method: post
        payload:
        {
                authkey: {% credential SlashNext %}
                url: {{.url}}
        }
        expected_update_period_in_days: 1
}
```

SlashNext = SlashNext API key added to credentials section of Tines
.url = URL to be scanned, can be either passed as direct value or a parameter from any above connected agents

2.4 | SUBMIT URL TO SLASHNEXT FOR BLOCKING SCAN

Perform a real-time URL scan with SlashNext cloud-based SEER Engine in a blocking mode. If the specified URL already exists in the cloud database, scan result will get returned immediately. If not, this command will submit a URL scan request and wait for the scan to finish. The scan may take up to 60 seconds to finish. If the system is unable to complete a scan within the specified timeout, a timeout error will be returned. User may try again with a different timeout. If no timeout value is specified, a default value of 60 seconds will be used.

Template Details

```
{
        url: https://oti.slashnext.cloud/api/oti/v1/url/scansync
        content_type: json
        method: post
        payload:
        {
                authkey: {% credential SlashNext %}
                url: {{.url}}
                timeout: 60
        }
        expected_update_period_in_days: 1
}
```

SlashNext = SlashNext API key added to credentials section of Tines
.url = URL to be scanned, can be either passed as direct value or a parameter from any above connected agents

2.5 | GET URL SCAN RESULT FROM SLASHNEXT

Perform a real-time URL reputation scan with SlashNext cloud-based SEER Engine. If the specified URL already exists in the cloud database, scan results will get returned immediately. If not, this command will submit a URL scan request and return with 'check back later' message along with a unique Scan ID. User can check results of this scan with same API after 60 seconds or later using the returned Scan ID. For an API Key contact support@slashnext.com

Template Details

```
{
        url: https://oti.slashnext.cloud/api/oti/v1/url/scan
        content_type: json
        method: post
        payload:
        {
                authkey: {% credential SlashNext %}
                scanid: {{.scanid}}
        }
        expected_update_period_in_days: 1
}
```

SlashNext = SlashNext API key added to credentials section of Tines
.scanid = Scan ID from an earlier scan or blocking scan request, can be either passed as direct value or a parameter from any above connected agents

2.6 | GET SCANNED URL'S FORENSIC SCREENSHOT FROM SLASHNEXT

Download webpage screenshot against a previous URL Scan request. Scan ID returned by an earlier API call for scan submission. For an API Key contact support@slashnext.com

Template Details

```
{
        url: https://oti.slashnext.cloud/api/oti/v1/download/screenshot
        content_type: json
        method: post
        payload:
        {
                authkey: {% credential SlashNext %}
                scanid: {{.scanid}}
                resolution: high
        }
        expected_update_period_in_days: 1
}
```

SlashNext = SlashNext API key added to credentials section of Tines
.scanid = Scan ID from an earlier scan or blocking scan request, can be either passed as direct value or a parameter from any above connected agents

2.7 | GET SCANNED URL'S FORENSIC HTML FROM SLASHNEXT

Download webpage HTML against a previous URL Scan request. Scan ID returned by an earlier API call for scan submission. For an API Key contact support@slashnext.com

Template Details

```
{
        url: https://oti.slashnext.cloud/api/oti/v1/download/html
        content_type: json
        method: post
        payload:
        {
                authkey: {% credential SlashNext %}
                scanid: {{.scanid}}
        }
        expected_update_period_in_days: 1
}
```

SlashNext = SlashNext API key added to credentials section of Tines
.scanid = Scan ID from an earlier scan or blocking scan request, can be either passed as direct value or a parameter from any above connected agents

2.8 | GET SCANNED URL'S FORENSIC TEXT FROM SLASHNEXT

Download webpage rendered text against a previous URL Scan request. Scan ID returned by an earlier API call for scan submission. For an API Key contact support@slashnext.com

Template Details

```
{
        url: https://oti.slashnext.cloud/api/oti/v1/download/text
        content_type: json
        method: post
        payload:
        {
                authkey: {% credential SlashNext %}
                scanid: {{.scanid}}
        }
        expected_update_period_in_days: 1
}
```

SlashNext = SlashNext API key added to credentials section of Tines
.scanid = Scan ID from an earlier scan or blocking scan request, can be either passed as direct value or a parameter from any above connected agents