

SlashNext Phishing IR Integration Guide Demisto SOAR

TABLE OF CONTENTS

1 OVERVIEW	2
2 DETAILED DESCRIPTION	2
3 INTEGRATION INSTALLATION	2
4 INTEGRATION ACTIVATION	3
5 COMMANDS	4
IP	5
Domain	5
Host Reputation	6
Host Report	7
Host URLs	8
URL Scan	8
URL Scan Sync	10
URL Scan Report	11
Download Screenshot	12
Download HTML	12
Download Text	13

1 | OVERVIEW

SlashNext Phishing Incident Response Integration allows SOAR platform users to fully automate analysis of a suspected phishing URL. For instance, IR teams responsible for abuse inbox management can extract links or domains out of a suspicious email and scan them in real time with SlashNext's SEER™ threat detection cloud. This can save numerous hours of manual triaging and analyzing hundreds, even thousands of emails per day—allowing IR teams to be more efficient and stay lean.

2 | DETAILED DESCRIPTION

SlashNext Phishing Incident Response (SNX-PIR) Integration App allows SOAR users to fully automate analysis of a suspected phishing URL. Phishing awareness training for enterprise organizations has been a double-edged sword. On the one hand, it's allowed employees to be better at detecting potential phishing emails but, on the other hand it's led to overly crowded inboxes for IR teams.

With SNX-PIR app, security analysts in IR teams responsible for abuse inbox management can now fully automate extracting links or domains out of a suspicious email and scan them in real-time with SlashNext's proven cloud-powered, analysis engine. This integration provides valuable metadata such as detailed reputation of any host, real-time URL scanning at scale, and a complete download of various artifacts of scanned webpages—including screenshots, full html and the rendered text.

Built and run by an in-house team of talented software architects, data scientists, security researchers and cybersecurity experts, our massive cloud powers this IR automation app—resulting in lightning speed without compromising the effectiveness of phishing detection.

The SlashNext Phishing Incident Response integration app 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

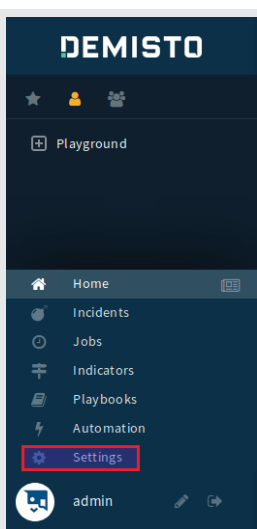
3 | INTEGRATION INSTALLATION

ⓘ Important Note

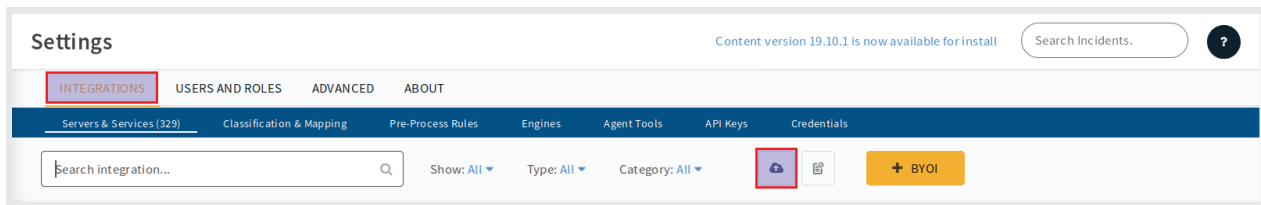
Please do note that you will only need to install the integration in case SlashNext has explicitly provided you a yaml file.

Follow the steps listed below to install the SlashNext Phishing Incident Response application in Demisto SOAR platform.

1. Login to the Demisto platform.
2. Go to Demisto settings by clicking on the **Settings** menu on the left side pane of the Demisto UI as shown below.



3. Select **INTEGRATIONS** tab on **Settings** page, and then select **Servers & Services** tab and click on **Upload Integration** button as shown in the snapshot below.

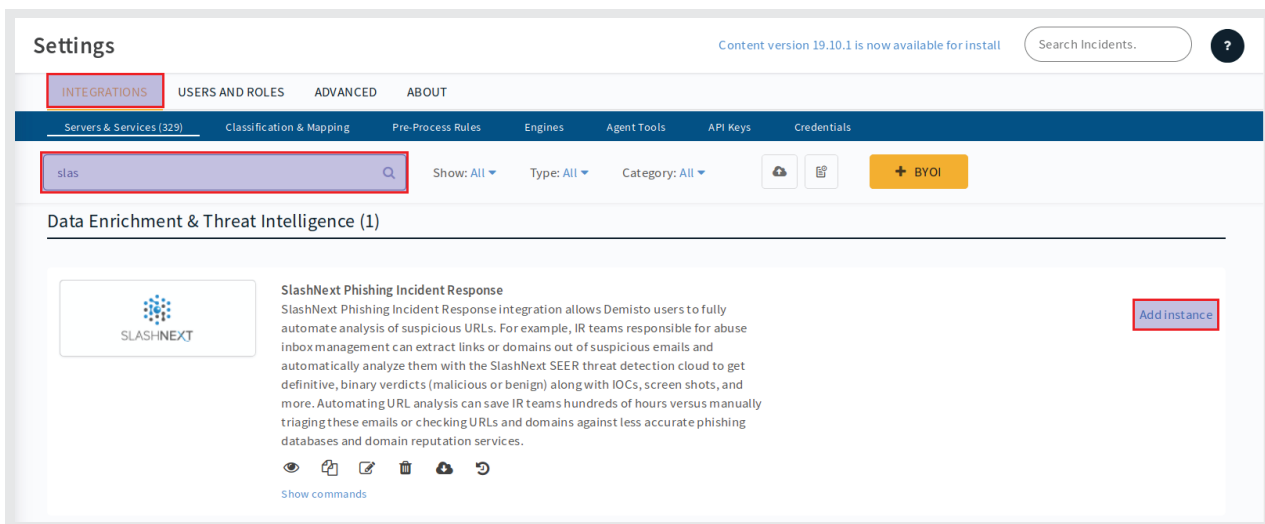


4. Input the provided **SlashNextPhishingIncidentResponse.yml** file in the pop-up **File Upload** window and click **Open**.

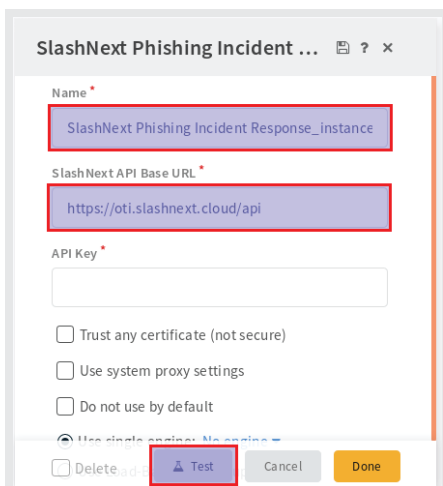
4 | INTEGRATION ACTIVATION

Follow the steps listed below to activate the SlashNext Phishing incident response integration in Demisto SOAR platform.

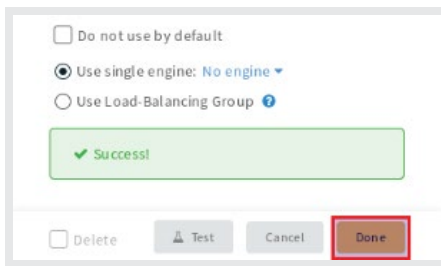
1. On the Demisto **Settings** page, select **INTEGRATIONS** tab and type slashnext in the **Search integration...** field and press Enter button as shown in the snapshot below.



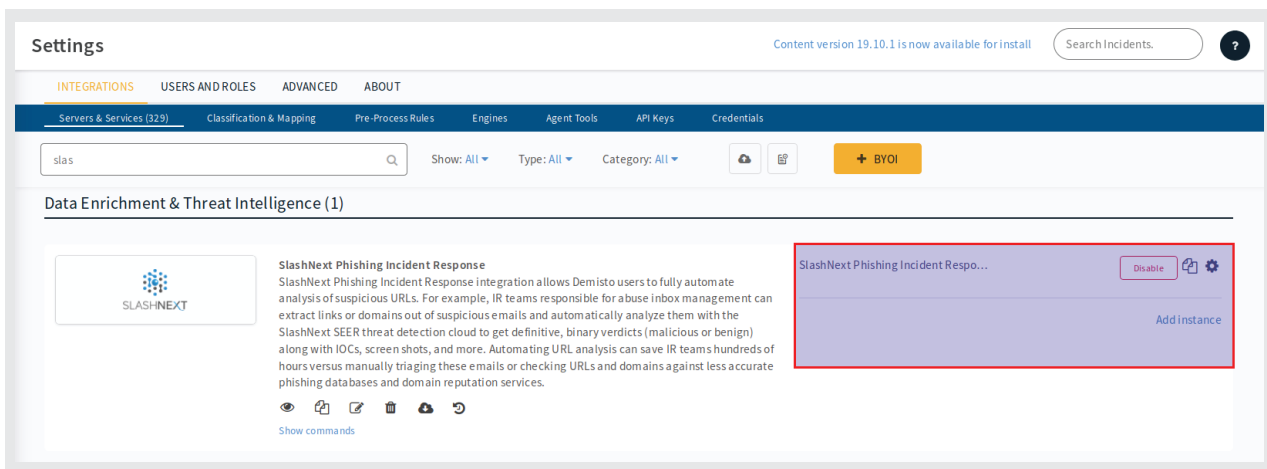
2. SlashNext Phishing Incident Response Integration will be listed, click on **Add instance** button as shown above.
3. Type the new instance **Name** (as you like), **Your API Key** (provided by SlashNext) and the **SlashNext API Base URL** (if specifically provided by SlashNext otherwise leave this as it is) in the pop-up menu and click on the **Test** button as highlighted in the snap below.



4. In case test is successful, there will be a Success message, which means the integration is activated, click on the **Done** button as shown.



5. The activated instance will also appear against the listed Integration on the **Settings** page.



5 | COMMANDS

SlashNext Phishing Incident Response integration app supported commands and outputs are listed below.

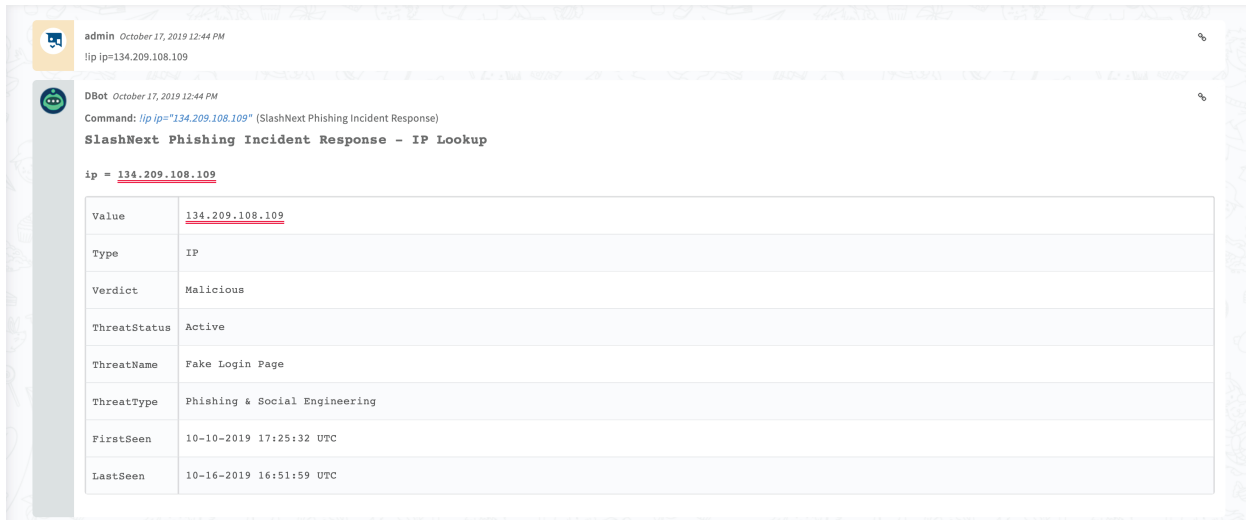
1. **ip** - Looks up an IP address indicator in the SlashNext Threat Intelligence database.
2. **domain** - Looks up a Fully Qualified Domain Name (FQDN) indicator in the SlashNext Threat Intelligence database.
3. **slashnext-host-reputation** - Queries the SlashNext Cloud database and retrieves the reputation of a host.
4. **slashnext-host-report** - Queries the SlashNext Cloud database and retrieves a detailed report.
5. **slashnext-host-urls** - Queries the SlashNext Cloud database and retrieves a list of all URLs.
6. **slashnext-url-scan** - Perform a real-time URL reputation scan with SlashNext cloud-based SEER Engine
7. **slashnext-url-scan-sync** - Perform a real-time URL scan with SlashNext cloud-based SEER Engine in a blocking mode.
8. **slashnext-scan-report** - Retrieve URL scan results against a previous Scan request.
9. **slashnext-download-screenshot** - Downloads a screenshot of a web page against a previous URL Scan request.
10. **slashnext-download-html** - Downloads a web page HTML against a previous URL Scan request.
11. **slashnext-download-text** - Downloads the text of a web page against a previous URL Scan request.

5.1 | IP

ip
Looks up an IP address indicator in the SlashNext Threat Intelligence database.

Input Arguments:
ip - required - IPv4 address to look up in the SlashNext Threat Intelligence database.

Output of command execution in Demisto;



admin October 17, 2019 12:44 PM
!ip ip=134.209.108.109

DBot October 17, 2019 12:44 PM
Command: !ip ip="134.209.108.109" (SlashNext Phishing Incident Response)
SlashNext Phishing Incident Response - IP Lookup

ip = 134.209.108.109

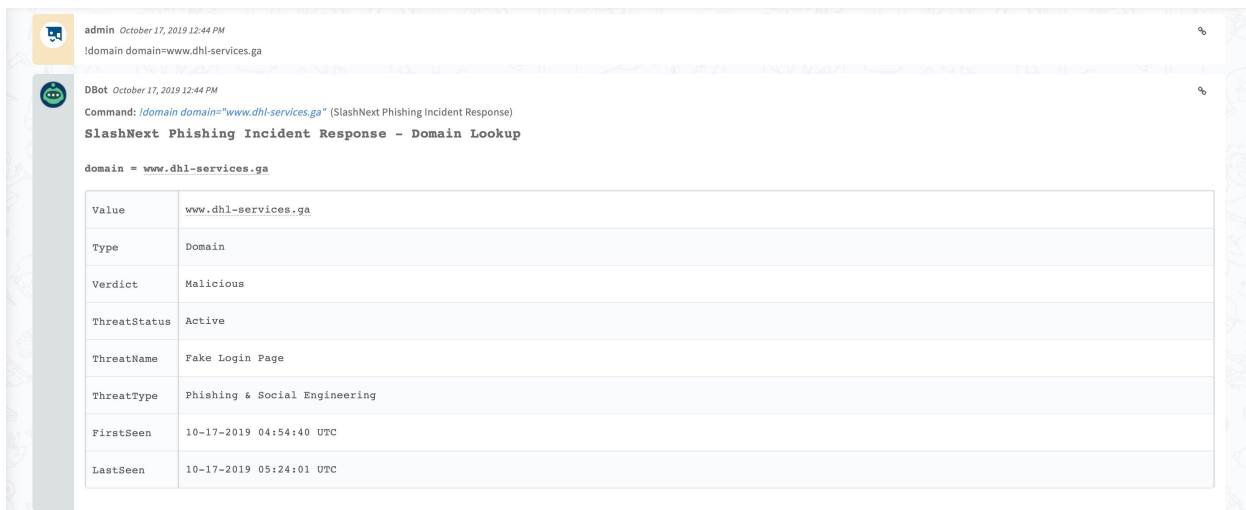
Value	<u>134.209.108.109</u>
Type	IP
Verdict	Malicious
ThreatStatus	Active
ThreatName	Fake Login Page
ThreatType	Phishing & Social Engineering
FirstSeen	10-10-2019 17:25:32 UTC
LastSeen	10-16-2019 16:51:59 UTC

5.2 | DOMAIN

domain
Looks up a Fully Qualified Domain Name (FQDN) indicator in the SlashNext Threat Intelligence database.

Input Arguments:
domain - required - The FQDN to look up in the SlashNext Threat Intelligence database.

Output of command execution in Demisto;



admin October 17, 2019 12:44 PM
!domain domain=www.dhl-services.ga

DBot October 17, 2019 12:44 PM
Command: !domain domain="www.dhl-services.ga" (SlashNext Phishing Incident Response)
SlashNext Phishing Incident Response - Domain Lookup

domain = www.dhl-services.ga

Value	<u>www.dhl-services.ga</u>
Type	Domain
Verdict	Malicious
ThreatStatus	Active
ThreatName	Fake Login Page
ThreatType	Phishing & Social Engineering
FirstSeen	10-17-2019 04:54:40 UTC
LastSeen	10-17-2019 05:24:01 UTC

5.3 | HOST REPUTATION

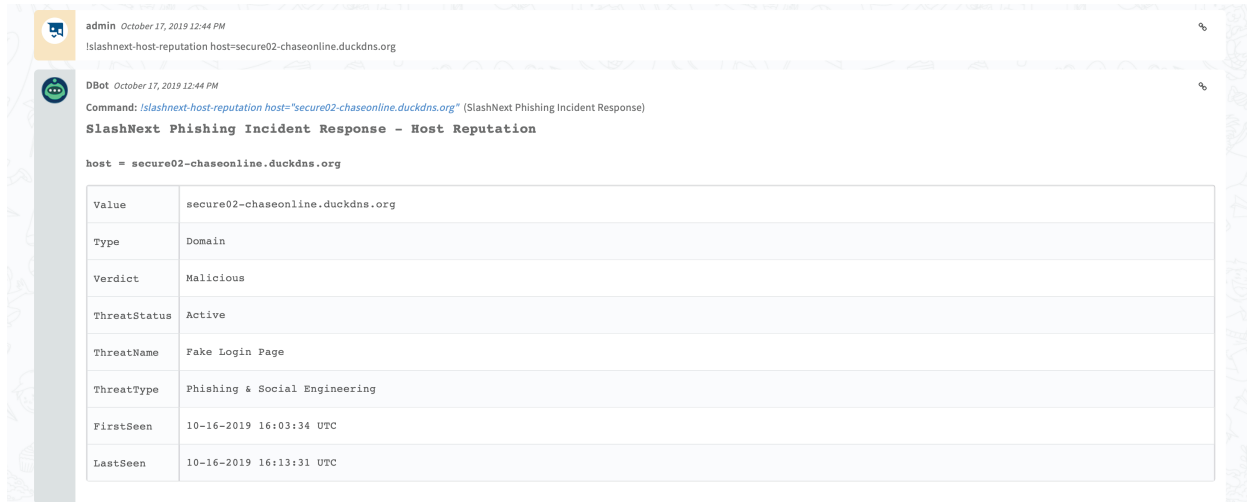
slashnext-host-reputation

Queries the SlashNext Cloud database and retrieves the reputation of a host.

Input Arguments:

host - required - host can be either be a domain name or IPv4 address.

Output of command execution in Demisto;



admin October 17, 2019 12:44 PM
!slashnext-host-reputation host=secure02-chaseonline.duckdns.org

DBot October 17, 2019 12:44 PM
Command: `!slashnext-host-reputation host="secure02-chaseonline.duckdns.org"` (SlashNext Phishing Incident Response)

SlashNext Phishing Incident Response - Host Reputation

host = secure02-chaseonline.duckdns.org

Value	secure02-chaseonline.duckdns.org
Type	Domain
Verdict	Malicious
ThreatStatus	Active
ThreatName	Fake Login Page
ThreatType	Phishing & Social Engineering
FirstSeen	10-16-2019 16:03:34 UTC
LastSeen	10-16-2019 16:13:31 UTC

5.4 | HOST REPORT

slashnext-host-report

Queries the SlashNext Cloud database and retrieves a detailed report for a host and associated URL.

Input Arguments:

host - required - host can be either be a domain name or IPv4 address.

Output of command execution in Demisto:

admin October 17, 2019 12:44 PM
 slashnext-host-report host=virtualmarketing.pk

DBot October 17, 2019 12:44 PM
 Command: slashnext-host-report host="virtualmarketing.pk" [SlashNext Phishing Incident Response]
SlashNext Phishing Incident Response - Host Report

host = virtualmarketing.pk

Value	virtualmarketing.pk
Type	Domain
Verdict	Malicious
ThreatStatus	Active
ThreatName	Fake Login Page
ThreatType	Phishing & Social Engineering
FirstSeen	10-16-2019 15:41:09 UTC
LastSeen	10-16-2019 15:53:44 UTC

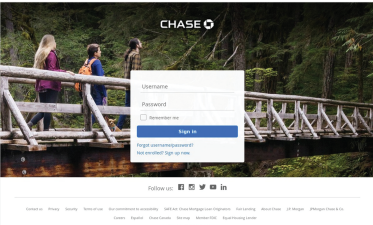
Command: slashnext-host-report host="virtualmarketing.pk" [SlashNext Phishing Incident Response]
SlashNext Phishing Incident Response - Latest Scanned URL

host = virtualmarketing.pk

Value	https://virtualmarketing.pk/soinxn/Chase2019/myaccount/index.php
Type	Scanned URL
Verdict	Malicious
ScanID	873d9975-c6c4-42ef-9674-f33e444ed9
ThreatStatus	Active
ThreatName	Fake Login Page
ThreatType	Phishing & Social Engineering
FirstSeen	10-16-2019 15:41:09 UTC
LastSeen	10-16-2019 15:53:44 UTC

Command: slashnext-host-report host="virtualmarketing.pk" [SlashNext Phishing Incident Response]
 Uploaded and commented on an image: slashnext_873d9975-c6c4-42ef-9674-f33e444ed9.jpg

Hide Preview



Forensics: Webpage Screenshot for the Scanned URL = <https://virtualmarketing.pk/soinxn/Chase2019/myaccount/index.php>

Command: slashnext-host-report host="virtualmarketing.pk" [SlashNext Phishing Incident Response]
 Uploaded file: slashnext_873d9975-c6c4-42ef-9674-f33e444ed9.html Download

Forensics: Webpage HTML for the Scanned URL = <https://virtualmarketing.pk/soinxn/Chase2019/myaccount/index.php>

Property	Value
Type	text/html, charset=utf-8
Size	9,617 Bytes
Info	HTML document, UTF-8 Unicode text, with very long lines
MDS	8f5e171ab9aec78c3f061ac3211af2e
SHA1	689c90877163e86804e60f29501c1fc5d76cc
SHA256	e538e88ec5644174f45e8e849bc27bb308d992fec24c25fdaf631811e5
SHA512	0b6ea0f5677ac7a673bc8b8584859277bc77eac2db817044f6319d0b0bc1c151c7faa85a581d1d2f2e6b5740e464861a0b2385fa17859ad48a20
SSDeep	192:zrkxHC0jZNSF4cJmmmmV+H4JM1jppz26uvTSLA8BjcnmmY4JMNkvT58

Open HEX view

Command: slashnext-host-report host="virtualmarketing.pk" [SlashNext Phishing Incident Response]
 Uploaded file: slashnext_873d9975-c6c4-42ef-9674-f33e444ed9.txt Download

Forensics: Webpage Rendered Text for the Scanned URL = <https://virtualmarketing.pk/soinxn/Chase2019/myaccount/index.php>

Property	Value
Type	txt
Size	375 bytes
Info	UTF-8 Unicode text
MDS	a785c396d31ebd9642ac326781ad44
SHA1	1571e39f2d798e2c0bd10a701485c27930
SHA256	26c3f267420ba896be54e0f3722da113cc3006afcc1616256bede73a58
SHA512	7723943d4f39c8112a9147225a9274b04e4f7b119d192780f8b0ba448179e4ce7072bc4382a5ab693bd0f1308767ab73002290ba01d9d29d24c
SSDeep	6:cw2xv8b2pWwK0cXrkkXwflv3GSRQhK5zJGzwbxthJ11gpxmKjg0dMUj5+MPV5x06Vom0hX0rj0e0dy0tr

Open HEX view

5.5 | HOST URLS

slashnext-host-urls

Queries the SlashNext Cloud database and retrieves a list of all URLs.

Input Arguments:

host - required - host can be either be a domain name or IPv4 address.

limit - optional - maximum number of URL records to fetch. This is an optional parameter with default value of 10.

Output of command execution in Demisto;

```
admin October 17, 2019 12:44 PM
!slashnext-host-urls host=blueaeventravel.com

DBot October 17, 2019 12:44 PM
Command: !slashnext-host-urls host="blueaeventravel.com" limit="10" (SlashNext Phishing Incident Response)
SlashNext Phishing Incident Response - Host URLs

host = blueaeventravel.com *
*Note: Email address specified in the Scanned URL was replaced with a dummy email to protect user privacy.

Value
-----
https://blueaeventravel.com/vendor/filp/whoops/up/index.php?email=
-----> https://blueaeventravel.com/vendor/filp/whoops/up/pulp.php?rand=46InboxLight.aspx.4827685990&fid.28.9164762324&fid=1&fav.1&rand.46InboxLight.aspx.4827685990&fid
https://blueaeventravel.com/vendor/filp/whoops/up/index.php?email=Jackdavis@eureliosolutions.com
-----> https://blueaeventravel.com/vendor/filp/whoops/up/pulp.php?rand=46InboxLight.aspx.4827685990&fid.28.9164762324&fid=1&fav.1&rand.46InboxLight.aspx.4827685990&fid

Partial View: Showing 6 out of 9 columns. View full table in a new tab.
```

5.6 | URL SCAN

slashnext-url-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 'slashnext-scan-report' command after 60 seconds or later using the returned Scan ID.

Input Arguments:

url - required - The URL that needs be scanned.

extended_info - optional - If *extended_info* is set 'true' the system along with URL reputation also downloads forensics data like screenshot, HTML and rendered text. If this parameter is not filled, the system will consider this as 'false'.

Output of command execution in Demisto in case result is not readily available;

```
admin October 17, 2019 12:51 PM
!slashnext-url-scan url=https://app.slack.com/client/TN71J00AG/DP2N38E91 extended_info=true

DBot October 17, 2019 12:51 PM
Command: !slashnext-url-scan url="https://app.slack.com/client/TN71J00AG/DP2N38E91" extended_info="true" (SlashNext Phishing Incident Response)
SlashNext Phishing Incident Response - URL Scan

url = https://app.slack.com/client/TN71J00AG/DP2N38E91

Your Url Scan request is submitted to the cloud and may take up-to 60 seconds to complete.
Please check back later using "slashnext-scan-report" command with Scan ID = bb528bd3-0ea4-44f4-b40e-4ca1d4db7fd6 or running the same "slashnext-url-scan" command one more time.
```


Output of command execution in Demisto in case result is readily available with `extended_info=false`;

admin October 17, 2019 12:49 PM
 slashnext-url-scan url=http://www.compassok.tk/vilo/nsw/data/UntitledNotebook1.html extended_info=true

DBot October 17, 2019 12:49 PM
 Command: `slashnext-url-scan url="http://www.compassok.tk/vilo/nsw/data/UntitledNotebook1.html" extended_info="true"` (SlashNext Phishing Incident Response)

SlashNext Phishing Incident Response - URL Scan

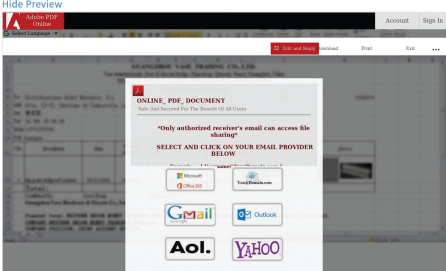
url = <https://www.compassok.tk/vilo/nsw/data/UntitledNotebook1.html>

Value	Type	Verdict	ScanID	ThreatStatus	ThreatName
http://www.compassok.tk/vilo/nsw/data/UntitledNotebook1.html	Scanned URL	Malicious	d4747f5f-0110-4670-a843-013c5b4231e9	Active	Fake Login Page
-----> https://www.compassok.tk/vilo/nsw/data/UntitledNotebook1.html	Final URL	Malicious			

Partial View: Showing 6 out of 9 columns. [View full table in a new tab.](#)

Command: `slashnext-url-scan url="http://www.compassok.tk/vilo/nsw/data/UntitledNotebook1.html" extended_info="true"` (SlashNext Phishing Incident Response)
 Uploaded and commented on an image: [slashnext_d4747f5f-0110-4670-a843-013c5b4231e9.jpg](#)

Hide Preview



Forensics: Webpage Screenshot for the Final URL = <https://www.compassok.tk/vilo/nsw/data/UntitledNotebook1.html>

Command: `slashnext-url-scan url="http://www.compassok.tk/vilo/nsw/data/UntitledNotebook1.html" extended_info="true"` (SlashNext Phishing Incident Response)
 Uploaded file: [slashnext_d4747f5f-0110-4670-a843-013c5b4231e9.html](#) [Download](#)

Forensics: Webpage HTML for the Final URL = <https://www.compassok.tk/vilo/nsw/data/UntitledNotebook1.html> File may be malicious

Property	Value
Type	text/html; charset=utf-8
Size	175,595 bytes
Info	HTML document, UTF-8 Unicode text, with very long lines
MDS	6b220284a12a8a2475f6c868ba9e8b28
SHA1	83f2e7c7a306da14c0b9c974a048c39b6a573c2
SHA256	aeba0b6f0366f8e11d0744946b2026257b5f0c864114b56b62df49805d6bf37
SHAS12	85d6f413ea5690c1cfb03f6b85ed1ac70d7aad76d3bb4ac43995fa12e1aedc3f0144f3a5060dfee01e138c9da56d395c9d60c69a1a1b27afa5e10e631f5faad
SSDeep	3072:5+5eT10xJUZPeQJNzYJb5QJ99//BqyTK3nXVBA9xPguCtQtkPcQAafi8d/jj;SdlmCOZPeQzrBqyT2FG91gXqSpfcQAAs

[Open HEX view](#)

Command: `slashnext-url-scan url="http://www.compassok.tk/vilo/nsw/data/UntitledNotebook1.html" extended_info="true"` (SlashNext Phishing Incident Response)
 Uploaded file: [slashnext_d4747f5f-0110-4670-a843-013c5b4231e9.txt](#) [Download](#)

Forensics: Webpage Rendered Text for the Final URL = <https://www.compassok.tk/vilo/nsw/data/UntitledNotebook1.html> File may be malicious

Property	Value
Type	txt
Size	364 bytes
Info	UTF-8 Unicode text
MDS	5805b308aa9c27254ac0b7a8b7ec25b
SHA1	13b85905d71dbcf41062db86f73d141bcf4be6a
SHA256	b06029c325fe5789f1c7a4dad73eb003a35418c8c1307e35a6c91646bd1d5121
SHAS12	b9bc83d1517f0c876d3a1901b12f:5642eb907589e6dea92365591.aed88b08977f0be654b213421aa08715b41d429ef750b6f3009dcb25a67d74667441c251
SSDeep	6:lDg7wzptz7ENe4rSLIWCJKWny/RoB3JKrQLLu5yhFEWdMKA9iIMlFv:lgwzpj7EwFLjKah8SQLL/hFEYMH3Gld

[Open HEX view](#)

5.7 | URL SCAN SYNC

slashnext-url-scan-sync

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.

Input Arguments:

url - required - The URL that needs be scanned.

timeout - optional - A timeout value in seconds. 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.

extended_info - optional - If extended_info is set 'true' the system along with URL reputation also downloads forensics data like screenshot, HTML and rendered text. If this parameter is not filled, the system will consider this as 'false'.

Output of command execution with extended_info=true in Demisto;

admin October 17, 2019 12:49 PM
 !slashnext-url-scan-sync url=http://www.shoppingwo.com/js/shop/1718.php?extended_info=true

DBot October 17, 2019 12:50 PM
 Command: !slashnext-url-scan-sync url="http://www.shoppingwo.com/js/shop/1718.php?extended_info=true" [SlashNext Phishing Incident Response]
SlashNext Phishing Incident Response - URL Scan Sync

url = http://www.shoppingwo.com/js/shop/1718.php

Value	http://www.shoppingwo.com/js/shop/1718.php
Type	Scanned URL
Verdict	Malicious
ScanID	c2122371-3669-4751-8c0c-e61a6a907d33
ThreatStatus	Active
ThreatName	Fake Login Page
ThreatType	Phishing & Social Engineering
FirstSeen	10-17-2019 07:59:04 UTC
LastSeen	10-17-2019 07:59:17 UTC

Command: !slashnext-url-scan-sync url="http://www.shoppingwo.com/js/shop/1718.php?extended_info=true" [SlashNext Phishing Incident Response]
 Uploaded and commented on an image: slashnext_c2122371-3669-4751-8c0c-e61a6a907d33.jpg

Hide Preview

66 Forensics: Webpage Screenshot for the Scanned URL = http://www.shoppingwo.com/js/shop/1718.php

Command: !slashnext-url-scan-sync url="http://www.shoppingwo.com/js/shop/1718.php?extended_info=true" [SlashNext Phishing Incident Response]
 Uploaded file: slashnext_c2122371-3669-4751-8c0c-e61a6a907d33.html Download

66 Forensics: Webpage HTML for the Scanned URL = http://www.shoppingwo.com/js/shop/1718.php File may be malicious

Property	Value
Type	text/html; charset=utf-8
Size	9,006 bytes
Info	HTML document, UTF-8 Unicode text, with very long lines
MDS	6eba9a2033ea3ee72c1330ab17e02ba6
SHA1	4be9d588443e1c3019eb0ff0cc6c18d4e5c33a
SHA256	bc95a69f465d68f7b64ef80e3bd703b13ca5c3c323e73732b7c1a39
SHA512	074ae50f6778ba3e34474b632e919f02c397775c1341a04d12022f0f5c0b0c63ea7cd298a8e747221538b0f73cb59853dc44095a0645286093758
SSDeep	96.NLDGMKQKwVWVWVJEUwJ5W1K00pMvATk3i5r4TV9w4v9r3H8Gv1QP0rurvR8Yv9

Open HEX view

Command: !slashnext-url-scan-sync url="http://www.shoppingwo.com/js/shop/1718.php?extended_info=true" [SlashNext Phishing Incident Response]
 Uploaded file: slashnext_c2122371-3669-4751-8c0c-e61a6a907d33.txt Download

66 Forensics: Webpage Rendered Text for the Scanned URL = http://www.shoppingwo.com/js/shop/1718.php File may be malicious

Property	Value
Type	txt
Size	312 bytes
Info	UTF-8 Unicode text
MDS	87172a681ca324402f87638911f413d
SHA1	665941cc7eeb65001909f9820e077bda5cd9
SHA256	d366a76287e5e1706d68929f98a2e1d4877143b31d0f815d0be0b2aad2371
SHA512	d6ea1190380c60161c0d071a54072a8b132423a9b70ea143224562d713c8e41468a8f5ee33e5d1e0d96d47202fac58ae7101004c2a00f
SSDeep	6.EEmEeVw2z2wHrJHYvUeUgVdfuAXJOM8FLASR0K6X7H1LQ2:rcv0Bh+Oz3EdmAwWBg8T8X722

Open HEX view

5.8 | URL SCAN REPORT

slashnext-scan-report

Retrieve URL scan results against a previous Scan request. If the scan is finished, result will be returned immediately; otherwise a 'check back later' message will be returned.

Input Arguments:

scanid - required - Scan ID returned by an earlier call to 'snx-url-scan' or 'snx-url-scan-sync' commands.

extended_info - optional - If extended_info is set 'true' the system along with URL reputation also downloads forensics data like screenshot, HTML and rendered text. If this parameter is not filled, the system will consider this as 'false'.

Output of command execution without extended_info or with extended_info=true in Demisto:

admin October 17, 2019 12:44 PM
 !slashnext-url-scan url=https://caservice.ml/paypal/ extended_info=true

DBoT October 17, 2019 12:44 PM
 Command: !slashnext-url-scan url="https://caservice.ml/paypal/" extended_info="true" (SlashNext Phishing Incident Response)
SlashNext Phishing Incident Response - URL Scan

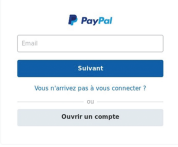
url = <https://caservice.ml/paypal/>

Value	Type	Verdict	ScanID
https://caservice.ml/paypal/	Scanned URL	Malicious	39cb08a3-c5e
-----> https://caservice.ml/paypal/a931ca/en/season.php?country.x=ca9886755e017b27aa4c81f3b53c8bf4ca9886755e017b27aa4c81f3b53c8bf4	Final URL	Malicious	

Partial View: Showing 6 out of 9 columns. View full table in a new tab.

Command: !slashnext-url-scan url="https://caservice.ml/paypal/" extended_info="true" (SlashNext Phishing Incident Response)
 Uploaded and commented on an image: slashnext_39cb08a3-c5ea-44a5-a097-9cfd78285299.jpg

Hide Preview



Forensics: Webpage Screenshot for the Final URL = <https://caservice.ml/paypal/a931ca/en/season.php?country.x=ca9886755e017b27aa4c81f3b53c8bf4ca9886755e017b27aa4c81f3b53c8bf4>

Command: !slashnext-url-scan url="https://caservice.ml/paypal/" extended_info="true" (SlashNext Phishing Incident Response)
 Uploaded file: slashnext_39cb08a3-c5ea-44a5-a097-9cfd78285299.html Download

Forensics: Webpage HTML for the Final URL = <https://caservice.ml/paypal/a931ca/en/season.php?country.x=ca9886755e017b27aa4c81f3b53c8bf4ca9886755e017b27aa4c81f3b53c8bf4> File may be malicious

Property	Value
Type	text/html; charset=utf-8
Size	30,302 bytes
Info	HTML document, UTF-8 Unicode text, with very long lines
MD5	f1c6418d32e73c7fb0f044837794ea38
SHA1	349816a30b436944e939e6e243653f60f691269
SHA256	5dd13904a6e095fefa4f8cc1d01eb2c1ba5f0bea91c0ccee0359818e467d58972
SHA512	d169604400f5db01a28857452b96321cfa7cd1d244c10b8856ed2fd9604ca01adad8ca7889ec8eeafa101fd1f6972d7a73725ada72fc7d168b34ab998268633ea
SSDeep	768:tzq/bfCRieSA3Gqwh1bdKAwIGRP+Wx.JYksDlp:kzTfCRlee3jDblUj0Bz

Open HEX view

Command: !slashnext-url-scan url="https://caservice.ml/paypal/" extended_info="true" (SlashNext Phishing Incident Response)
 Uploaded file: slashnext_39cb08a3-c5ea-44a5-a097-9cfd78285299.txt Download

Forensics: Webpage Rendered Text for the Final URL = <https://caservice.ml/paypal/a931ca/en/season.php?country.x=ca9886755e017b27aa4c81f3b53c8bf4ca9886755e017b27aa4c81f3b53c8bf4> File may be malicious

Property	Value
Type	txt
Size	94 bytes
Info	UTF-8 Unicode text
MD5	91d8bb86d78e47f0894bf5105845d360f
SHA1	95c14f8cd25272daaf664cd60e73963e542d15
SHA256	589e36239bb7150289010831f643808d2dc59e1629fa831627bd91b0ea293d6
SHA512	28219b6d67fab3ce5adfd7af96c0e86dd1d3f5cbb38c231b87f9adcfd77c4080b0f2e05b617980bdfc92d805c35500a91aa1fd19df0527d2fbcdbd047a0
SSDeep	3:ORkpB+BX6cFutiT+XMT6Fulte7vbHrBn:OehkoAMvbNn

Open HEX view

5.9 | DOWNLOAD SCREENSHOT

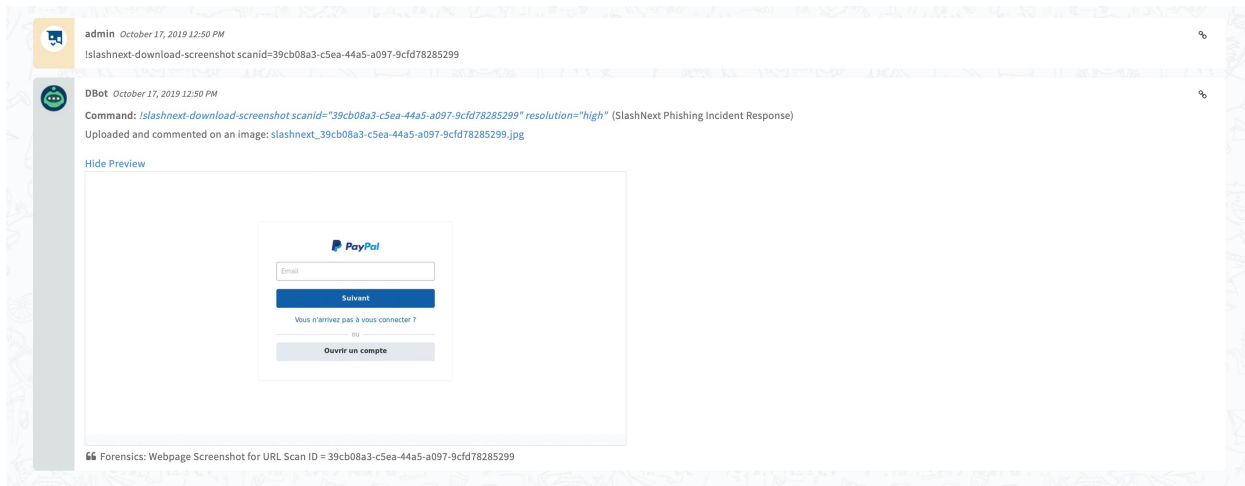
slashnext-download-screenshot

Download webpage screenshot against a previous URL Scan request.

Input Arguments:

scanid - required - Scan ID returned by an earlier call to 'slashnext-url-scan' or 'slashnext-url-scan-sync' commands.

Output of command execution in Demisto:



5.10 | DOWNLOAD HTML

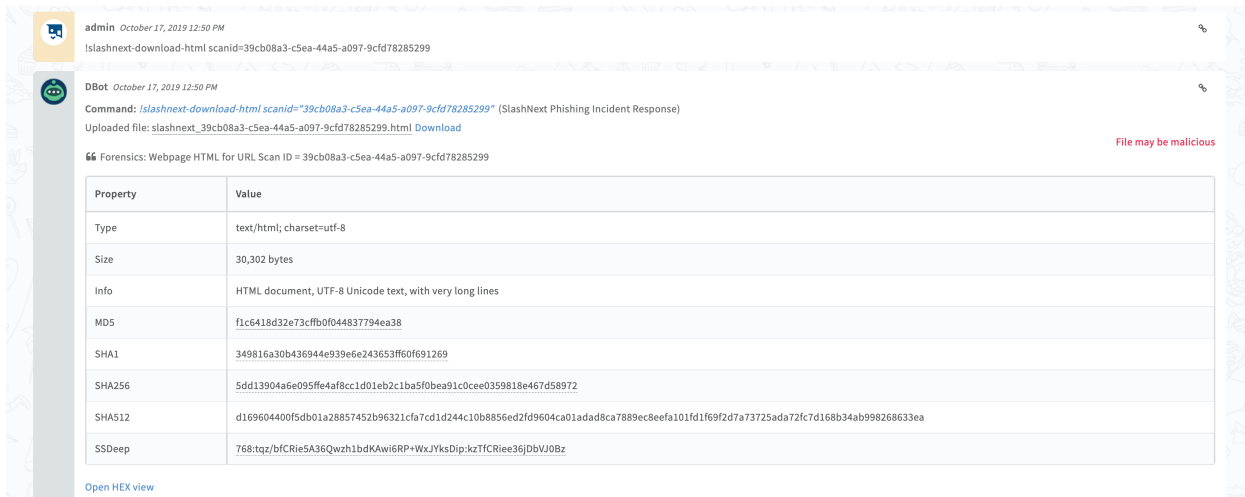
slashnext-download-html

Download webpage HTML against a previous URL Scan request.

Input Arguments:

scanid - required - Scan ID returned by an earlier call to 'slashnext-url-scan' or 'slashnext-url-scan-sync' commands.

Output of command execution in Demisto:



5.11 | DOWNLOAD TEXT

slashnext-download-text

Download webpage text against a previous URL Scan request.

Input Arguments:

scanid - required - Scan ID returned by an earlier call to 'slashnext-url-scan' or 'slashnext-url-scan-sync' commands.

Output of command execution in Demisto;

The screenshot shows a chat interface with two messages. The first message is from 'admin' at 12:50 PM, showing the command 'slashnext-download-text scanid=39cb08a3-c5ea-44a5-a097-9cfd78285299'. The second message is from 'DBot' at 12:50 PM, showing the command execution details and a table of file properties.

Command: *slashnext-download-text scanid="39cb08a3-c5ea-44a5-a097-9cfd78285299"* (SlashNext Phishing Incident Response)
 Uploaded file: slashnext_39cb08a3-c5ea-44a5-a097-9cfd78285299.txt [Download](#)

Forensics: Webpage Rendered Text for URL Scan ID = 39cb08a3-c5ea-44a5-a097-9cfd78285299 File may be malicious

Property	Value
Type	txt
Size	94 bytes
Info	UTF-8 Unicode text
MD5	91d8b86d78e47f0894bf5105845d360f
SHA1	95c14f8cd25272daaf664cdb0ef73963e542d15
SHA256	589e362339bb7150289010831f643808d2dc59e1629fa831627bd91b0ea293d6
SHA512	28219b6d67fab3ce5adfa7af36c0e8c6dd1d3f5cebb38c231b87f9adcfd77c4080b0f2e05b617980b0dfc92db05c355500a91aa1fd19d0527d2fbcdbd047a0
SSDeep	3:ORKpB+BX6cFutIT+XMT6Fulte7vbHrBn:OehkoAMvbNn

[Open HEX view](#)