

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

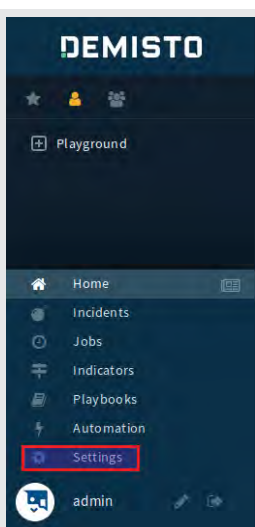
3 | INTEGRATION INSTALLATION

📌 Important Note

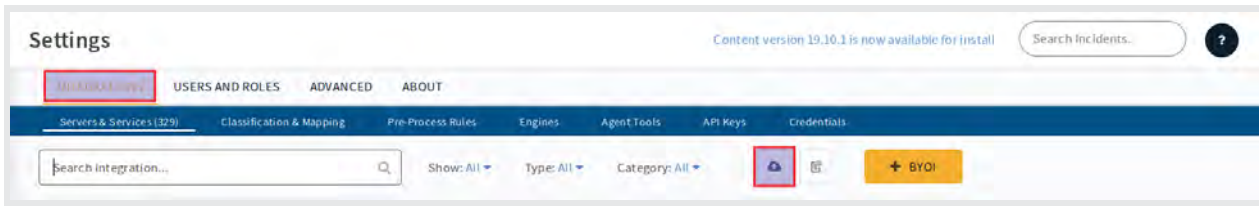
Please do note that you will only need to install the integration in case SlashNext has explicitly provided you a yaml file.

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.

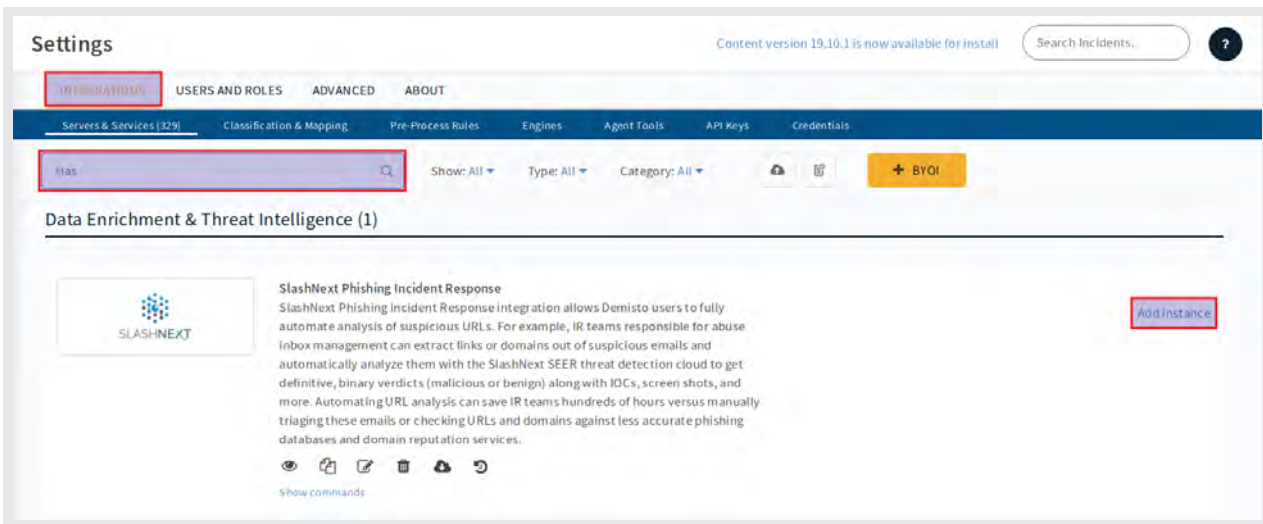


4. Input the provided **SlashNextPhishingIncidentResponse.yml** file in the pop-up **File Upload** window and click **Open**.

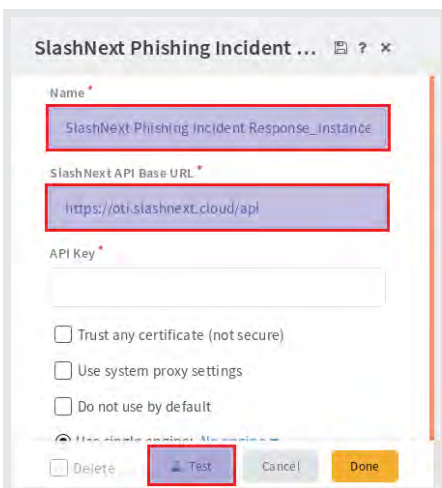
4 | INTEGRATION ACTIVATION

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

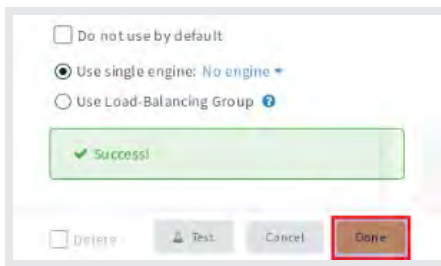
1. On the Demisto **Settings** page, select **INTEGRATIONS** tab and type slashnext in the **Search integration...** field and press Enter button as shown in the snapshot below.



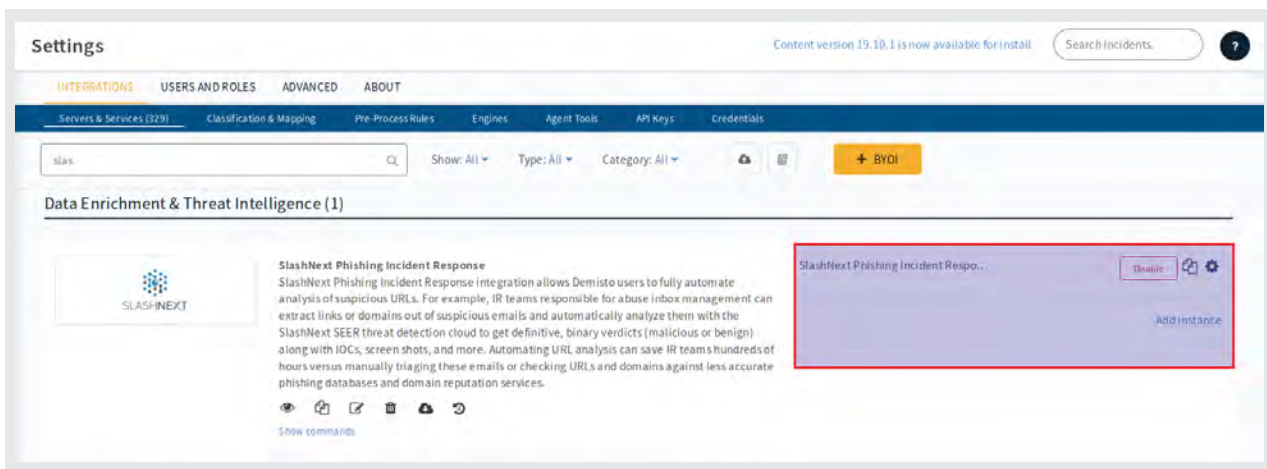
2. SlashNext Phishing Incident Response Integration will be listed, click on **Add instance** button as shown above.
3. Type the new instance **Name** (as you like), **Your API Key** (provided by SlashNext) and the **SlashNext API Base URL** (if specifically provided by SlashNext otherwise leave this 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;

Value	134.209.108.109
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;

Value	www.dhl-services.ga
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

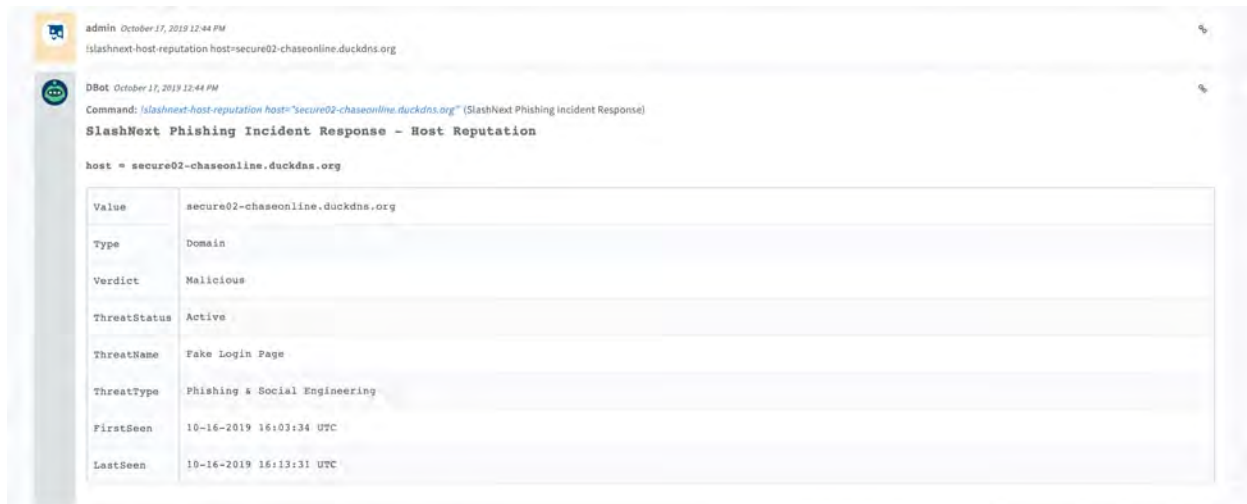
slashnext-host-reputation

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:

The screenshot shows a Demisto console window with the following content:

Command: `slashnext-host-report host="virtualsemarketing.pk"` (SlashNext Phishing Incident Response)

SlashNext Phishing Incident Response - Host Report

Host: virtualsemarketing.pk

Value	virtualsemarketing.pk
Type	Domain
Verdict	Malicious
ThreatStatus	Active
ThreatName	Fake Login Page
ThreatType	Phishing & Social Engineering
FirstSeen	10-18-2019 15:41:19 UTC
LastSeen	10-18-2019 15:53:44 UTC

Command: `slashnext-host-report host="virtualsemarketing.pk"` (SlashNext Phishing Incident Response)

SlashNext Phishing Incident Response - Latest Scanned URL

Host: virtualsemarketing.pk

Value	https://virtualsemarketing.pk/venom/Chase2019/myaccount/index.php
Type	Scanned URL
Verdict	Malicious
ScanID	87389975-c6c4-42ef-8674-f73e4648d9
ThreatStatus	Active
ThreatName	Fake Login Page
ThreatType	Phishing & Social Engineering
FirstSeen	10-18-2019 15:41:19 UTC
LastSeen	10-18-2019 15:53:44 UTC

Command: `slashnext-host-report host="virtualsemarketing.pk"` (SlashNext Phishing Incident Response)

Uploaded and commented on an image: `slashnext_87389975-c6c4-42ef-8674-f73e4648d9.jpg`

Host Preview:

Forensics: Webpage Screenshot for the Scanned URL: `https://virtualsemarketing.pk/venom/Chase2019/myaccount/index.php`

Command: `slashnext-host-report host="virtualsemarketing.pk"` (SlashNext Phishing Incident Response)

Uploaded file: `slashnext_87389975-c6c4-42ef-8674-f73e4648d9.html` (Download)

Forensics: Webpage HTML for the Scanned URL: `https://virtualsemarketing.pk/venom/Chase2019/myaccount/index.php`

Property	Value
Type	text/html; charset=utf-8
Size	6,627 Bytes
Info	HTML document, UTF-8 Unicode text, with very long lines
MD5	8f6e711a8b9c78c39f3a1e81121e5e
SHA1	083c308771c3a05050ac6029931c1c5d78c
SHA256	4d33b48bc5644174053e434498270b3089925c24c250d6d7311e5f
SHA512	08baef5677ac7e6730ca3e950481927bc77c4c42d8017944f3124c049e1c151170a45a547d32c0e0374e64408149b2385a119f93e948d0
SSDeep	f92:zmh4CQyZNF8ACQjcm0mY-H4J8H-Ljpe2HavTSLA8j0mmY4A3M3uT58

Open HTML view

Command: `slashnext-host-report host="virtualsemarketing.pk"` (SlashNext Phishing Incident Response)

Uploaded file: `slashnext_87389975-c6c4-42ef-8674-f73e4648d9.txt` (Download)

Forensics: Webpage Rendered Text for the Scanned URL: `https://virtualsemarketing.pk/venom/Chase2019/myaccount/index.php`

Property	Value
Type	txt
Size	375 bytes
Info	UTF-8 Unicode text
MD5	8786c336a13e8d9d642ac321781d444
SHA1	2371e3902d78f9e23bda75e5970142d27630
SHA256	2bc3f2424206a980b54545f722d61318c3c009af2c11652306e4d77938
SHA512	722945d4f30e8132e91745532a007d4f0e4f7013192370f98b0b44417949e7f72bc43432a3abb98b0e9413d87e7d873000266b0149f2d42c
SSDeep	6:WZ3v3Bz3Kc0K0:rk0eWwRv3S8QW3a1JcZw6w8thJJ3sp9ekJgLoM0Uy5-MRv5ub0v0m0k0z0wJg0el0dy0r0

Open HTML view

5.5 | HOST URLS

slashnext-host-urls

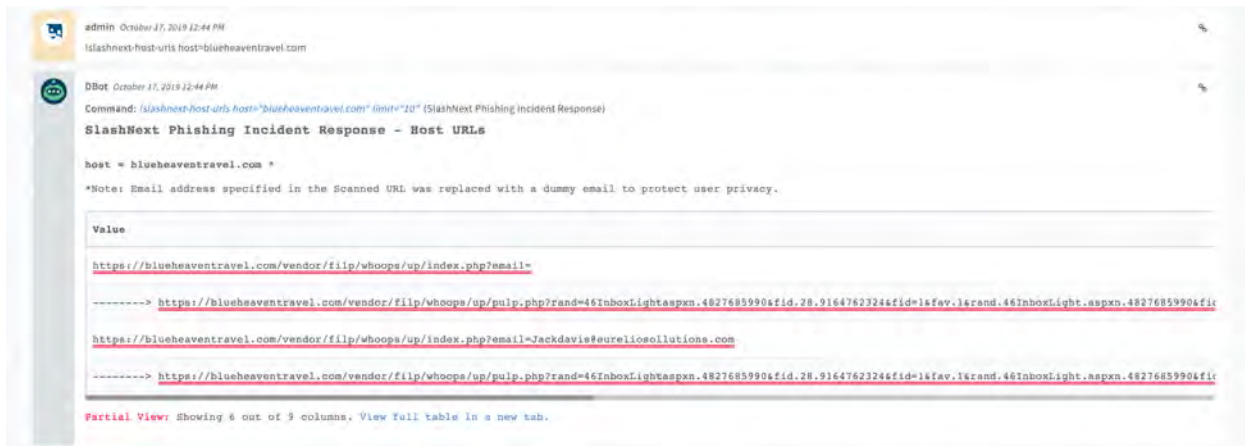
Queries the SlashNext Cloud database and retrieves a list of all URLs.

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=blueheaventravel.com

DBot October 17, 2019 12:44 PM
Command: !slashnext-host-urls host="blueheaventravel.com" limit="20" (SlashNext Phishing Incident Response)
SlashNext Phishing Incident Response - Host URLs

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

Value
-----
https://blueheaventravel.com/vendor/filip/whoops/up/index.php?email=
-----> https://blueheaventravel.com/vendor/filip/whoops/up/pulp.php?rand=46InboxLight.aspx.4827685990&fid.28.9164762324&fid=1&fav.1&rand.46InboxLight.aspx.4827685990&fid.
https://blueheaventravel.com/vendor/filip/whoops/up/index.php?email=Jackdavis@eureliocollutions.com
-----> https://blueheaventravel.com/vendor/filip/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 = bb526bd3-0ea4-44f4-b40e-6ca1d4db7fd6 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



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	83f2e7c7a306da14c0b9c974a04a8c39b6a573c2
SHA256	aebca0b5f0366f8e11d0744846b2026257b5f0c864114b56b62df49805d6bf37
SHA512	85d6f413ea5690c1cfb03f6b85ed1ac70d7aad76d3bb4ac43995fa12e1aedc3f0144f3a5060dfee01e138c9da56d395c9d60c69a1a1b27afa65e10e631f5fad
SSDeep	3072:5:5eT10xCJUZPeQJNzYjB5QJ99//BqyTk3nXVBA9xPguCtQTKPcQAAf8dI//SdimCOZPeQzBqyT2FG91jXqSpLcQAAs

Open HEX view

Command: slashnext-url-scan url="http://www.compassok.tk/vilo/nsw/data/UntitledNotebook2.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	5805b308aa9c727254ac0b7a8b7ec25b
SHA1	130855905d71dbcf4f062db86f73d141bcf4be6a
SHA256	b06029c325fe5789f1c7a4dad73eb003a35418c8c1307e35aec91646bd1d5121
SHA512	b9bc83d1517f0c876d3a1901b12fc5642eb907589e6deaa92365591aed88b08977f0be654b213421aa08715b41d429ef750b6f3009d0cb25a67d74467441c251
SSDeep	6:1Dg7iwzptzx7ENe4rSLWCKWny/RoB3JKrQLLu5yhFEW6MKA9iIMlFv:JgiwzpjTEwLjKah8SQLLhFEYMH3Gld

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;

The screenshot shows a Demisto console window with the following content:

```

Command: slashnext-url-scan-sync url="http://www.khoppingwo.com/js/hqop/1718.php?timeout=60" extended_info="true" (SlashNext Phishing Incident Response)
Updated and commented on an image: slashnext_c2122371-3689-4751-8c6b-e61a4976d33 (SlashNext Phishing Incident Response)
Hide Forensic
64 Forensic: Webpage Screenshot for the Scanned URL = http://www.khoppingwo.com/js/hqop/1718.php
Command: slashnext-url-scan-sync url="http://www.khoppingwo.com/js/hqop/1718.php?timeout=60" extended_info="true" (SlashNext Phishing Incident Response)
Updated and commented on an image: slashnext_c2122371-3689-4751-8c6b-e61a4976d33.html Download
64 Forensic: Webpage HTML for the Scanned URL = http://www.khoppingwo.com/js/hqop/1718.php
Open HTML image
64 Forensic: Webpage Rendered Text for the Scanned URL = http://www.khoppingwo.com/js/hqop/1718.php
Open HTML page
  
```

The scan results table is as follows:

Value	http://www.khoppingwo.com/js/hqop/1718.php
Type	Reassess URL
Verdict	Malicious
ReassID	02122371-3689-4751-8c6b-e61a4976d33
ThreatStatus	Active
ThreatName	Fake Login Page
ThreatType	Phishing & Social Engineering
FirstSeen	19-17-2019 07:50:54 UTC
LastSeen	19-17-2019 07:50:17 UTC

The screenshot shows a login page with the text "Mit dem Testkom Login anmelden".

The HTML properties table is as follows:

Property	Value
Type	text/html; charset=utf-8
Size	9,504 bytes
Info	HTML document, UTF-8 Unicode text, with very long lines
MIME	text/html; charset=utf-8
SHA1	4be0588443e16c2013e6e9f0c6c18d4c5c3a
SHA256	8c6e4d9f66e6d979664e48080d47033c4a5c3c13e7f712267c1478
SHA512	8744e0396778e3a3c04776e32e09d2c977f5c1341a461212af65c06e5e3a7e278a6e14521338b07d8d88c3a24095a044528093758
DDoSip	66.NL.BC.MA.QA.RK.VAWK@Uw.JSM14500j4k4K7kx.B5M4TV9w4v8.M8GqTQ70rcunV9Bjv8

The rendered text table is as follows:

Property	Value
Type	text
Size	112 bytes
Info	UTF-8 Unicode text
MIME	text/html; charset=utf-8
SHA1	6d3041c17ee8e201909f9a29e079b5d5c09
SHA256	4364a7e2875e170468929f8d4c1d54677436310b4815d9e902aa02371
SHA512	80ee419038cc060161090771a072a8b1312429f970a143224f65d9f215dca4144da75e633e541c40b8a72028f9c5a4710304c480f
DDoSip	6.EE.E8.f0.c4.c2777e.H.z0jy4tUg9fHxK.Z0MPLA.LAS5Yv6X75LQY-CFv08H-Du3d0RkxwM8aGd16X7Z

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;

The screenshot shows a Demisto console with the following content:

```

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=ca9886755e017b27aa4c81f3b53cbf4ca9886755e017b27aa4c81f3b53cbf4
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-c5e-44a5-a09f-9cf078285299.jpg
Hide Preview

[Image: Screenshot of a PayPal login page with fields for email and password, and a 'Submit' button.]

Forensics: Webpage Screenshot for the Final URL = https://caservice.ml/paypal/a931ca/en/season.php?country.x=ca9886755e017b27aa4c81f3b53cbf4ca9886755e017b27aa4c81f3b53cbf4

Command: !slashnext-url-scan url=https://caservice.ml/paypal/extended_info=true [SlashNext Phishing Incident Response]
Uploaded file: slashnext_39cb08a3-c5e-44a5-a09f-9cf078285299.html Download

Forensics: Webpage HTML for the Final URL = https://caservice.ml/paypal/a931ca/en/season.php?country.x=ca9886755e017b27aa4c81f3b53cbf4ca9886755e017b27aa4c81f3b53cbf4
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           f1c6418d32e73cf0f044837794e838
SHA1          34816a30b436944e93e6e243e53f60f91269
SHA256        5dd13904a6e095fe4f8cc1d01eb2c1ba5f0bea91c0cee0359818e467d58972
SHA512        d16960440f5db01a28857452b96321cfa7cd1d244c10b8856e2f69604ca01adad8ca78894cbeeafa101d1f69f2d7a73725ada727c7d168b34ab998268039a
SSDeep        768:3q/bfCRieS43Gwzh1bdKAwI6RP+Wk.JfksDip;KzTCRlee3jD6VJ0Bz

Open HEX view

Command: !slashnext-url-scan url=https://caservice.ml/paypal/extended_info=true [SlashNext Phishing Incident Response]
Uploaded file: slashnext_39cb08a3-c5e-44a5-a09f-9cf078285299.txt Download

Forensics: Webpage Rendered Text for the Final URL = https://caservice.ml/paypal/a931ca/en/season.php?country.x=ca9886755e017b27aa4c81f3b53cbf4ca9886755e017b27aa4c81f3b53cbf4
File may be malicious

Property      Value
-----
Type          txt
Size          94 bytes
Info          UTF-8 Unicode text
MD5           91d8bb86d78e47f0894bf5105845a360f
SHA1          95c14f8cd252772daaf664db60e073963e542015
SHA256        589e362239bb7150289010831f643806d2dc39e1629fa8162fbd91b0e9293d6
SHA512        2821966d67fab3ce5af97a7d36c0e86dd1d3f5cebb38c231b87f9adcf0e7fc4080e072e05b417980b0dfc92db05c35500a91aa1fd19df0527d2fbc0bd047a0
SSDeep        3:DRKpB+BX6cFutI+XMT6Fulte7vHrBn;OehkoAMvbNn

Open HEX view
    
```

5.9 | DOWNLOAD SCREENSHOT

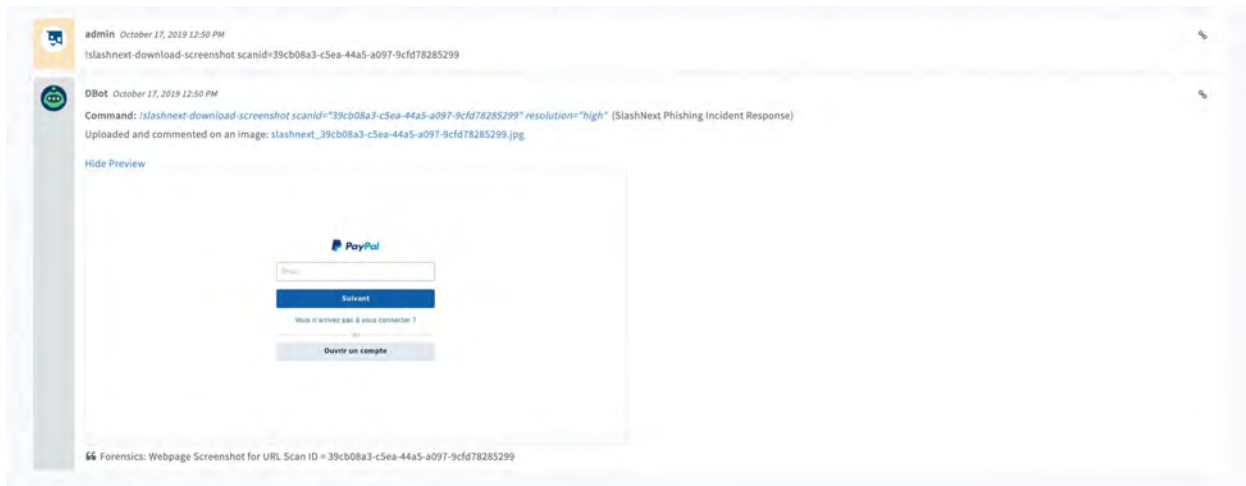
slashnext-download-screenshot

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

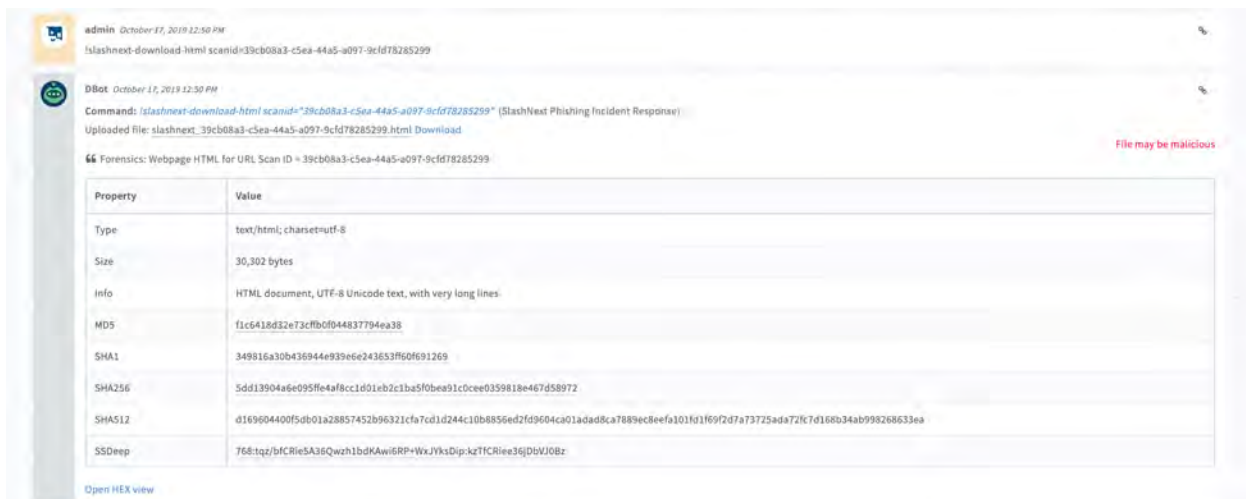
slashnext-download-html

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 Demisto interface with the following details:

- User:** admin (October 17, 2019 12:50 PM)
- Command:** slashnext-download-text scanid="39cb08a3-c5e4-44a5-a097-9cfd78285299" (SlashNext Phishing Incident Response)
- Uploaded file:** slashnext_39cb08a3-c5e4-44a5-a097-9cfd78285299.txt
- Forensics:** Webpage Rendered Text for URL Scan ID = 39cb08a3-c5e4-44a5-a097-9cfd78285299
- Warning:** File may be malicious

Property	Value
Type	txt
Size	94 bytes
Info	UTF-8 Unicode text
MD5	91d8b86d78e47f0894bf5105845d360f
SHA1	95c14f8cd25272daaf64cdeb0ef73963e542d15
SHA256	589e362339bb7150289010831f643808d2dc59e1629fab31627bd91e0ea293d6
SHA512	28219b6d67fab3ceadfa7af36c0e8c6dd1d3f5cebb38c231b87f9adcfde77c4080b0f2e05b617980b0dfc92db05c35500a91aa1fd19df0527d2fbcdbd047a0
SSDeep	3:ORKpB+BX6cFutIT+XMT6FulteTvHrBn:OehkoAMvbnN

Open HEX view