

SlashNext Phishing IR Integration Guide (Splunk) Phantom SOAR

TABLE OF CONTENTS

1 OVERVIEW	2
2 DETAILED DESCRIPTION	2
3 INTEGRATION INSTALLATION	3
4 INTEGRATION ACTIVATION	4
5 ACTIONS	6
Host Reputation	7
Host Report	8
Host URLs	9
URL Scan	10
URL Scan Sync	11
URL Scan Report	13
Download Screenshot	14
Download HTML	15
Download Text	15
API Quota	16

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 allows employees to improve their recognition of 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

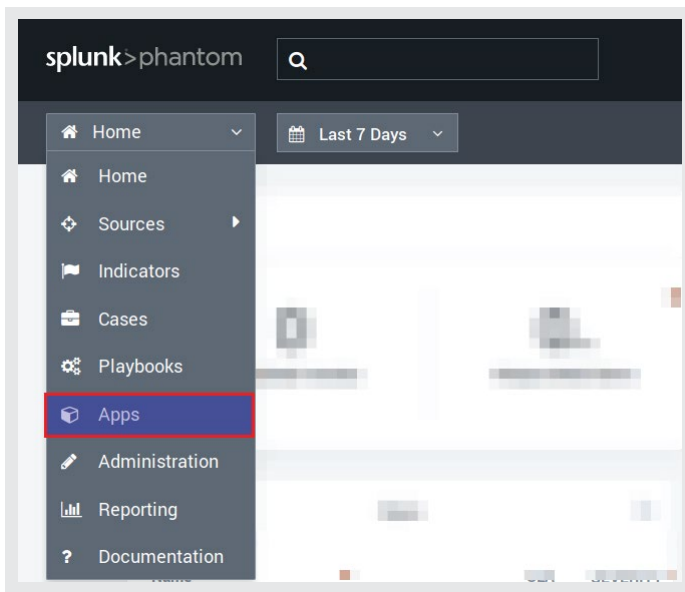
3 | INTEGRATION INSTALLATION

📌 Important Note

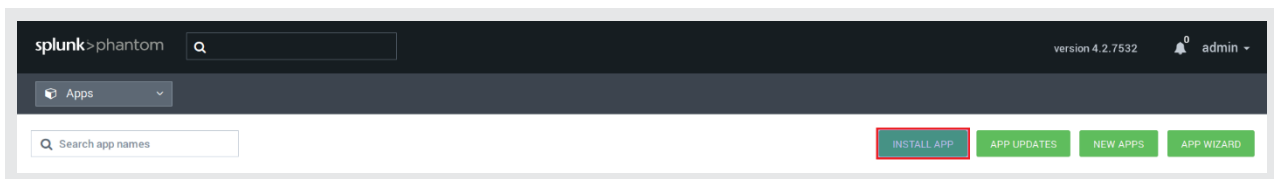
Please do note that you will only need to install the integration in case SlashNext has explicitly provided you a tarball file or if you download it from Phantom APP store.

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

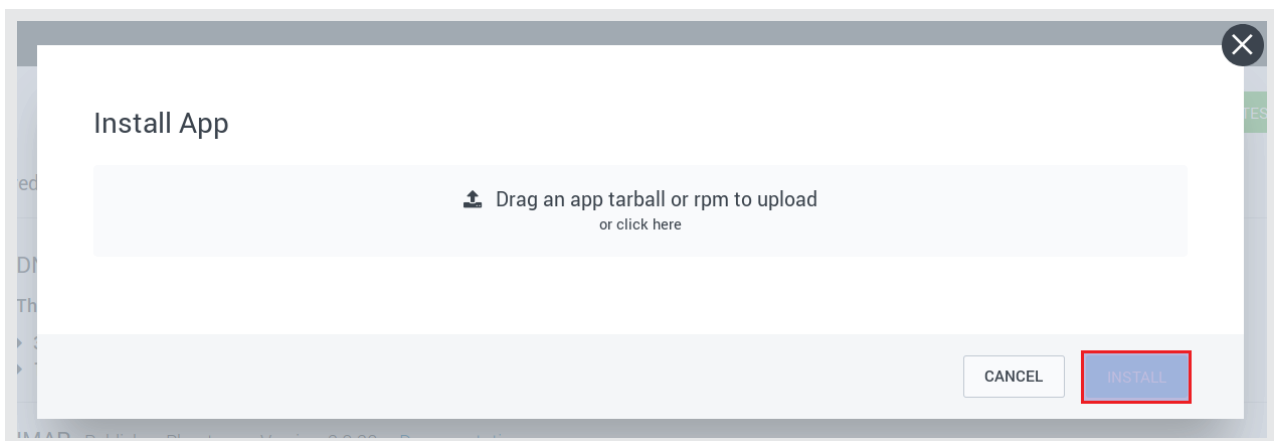
1. Login to the Phantom platform.
2. Go to Phantom **Apps** by clicking on the drop-down menu on the top left side of the Phantom UI as shown below.



3. On the **Apps** page click on **INSTALL APP** button as shown below.



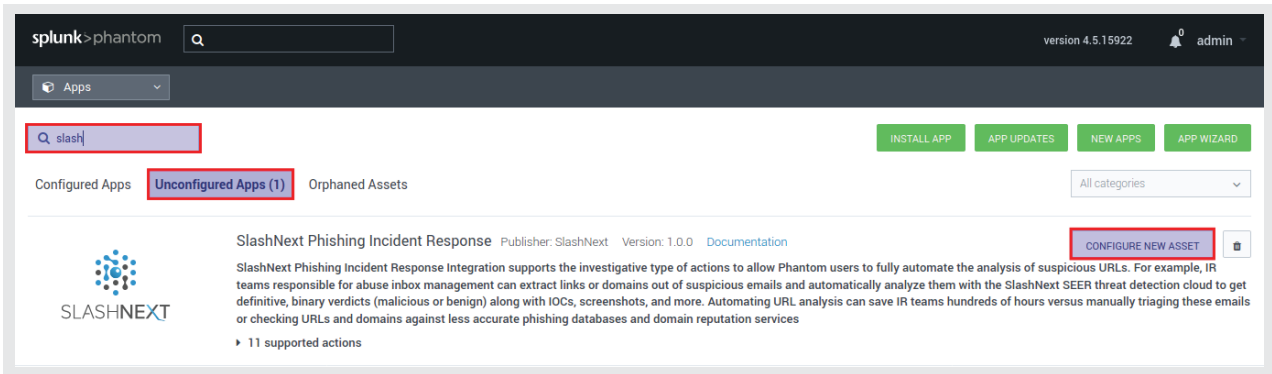
4. On the pop-up **Install App** menu, input the **phantom_slashnextphishingincidentresponse.tgz** package provided by SlashNext and click **INSTALL** as shown below.



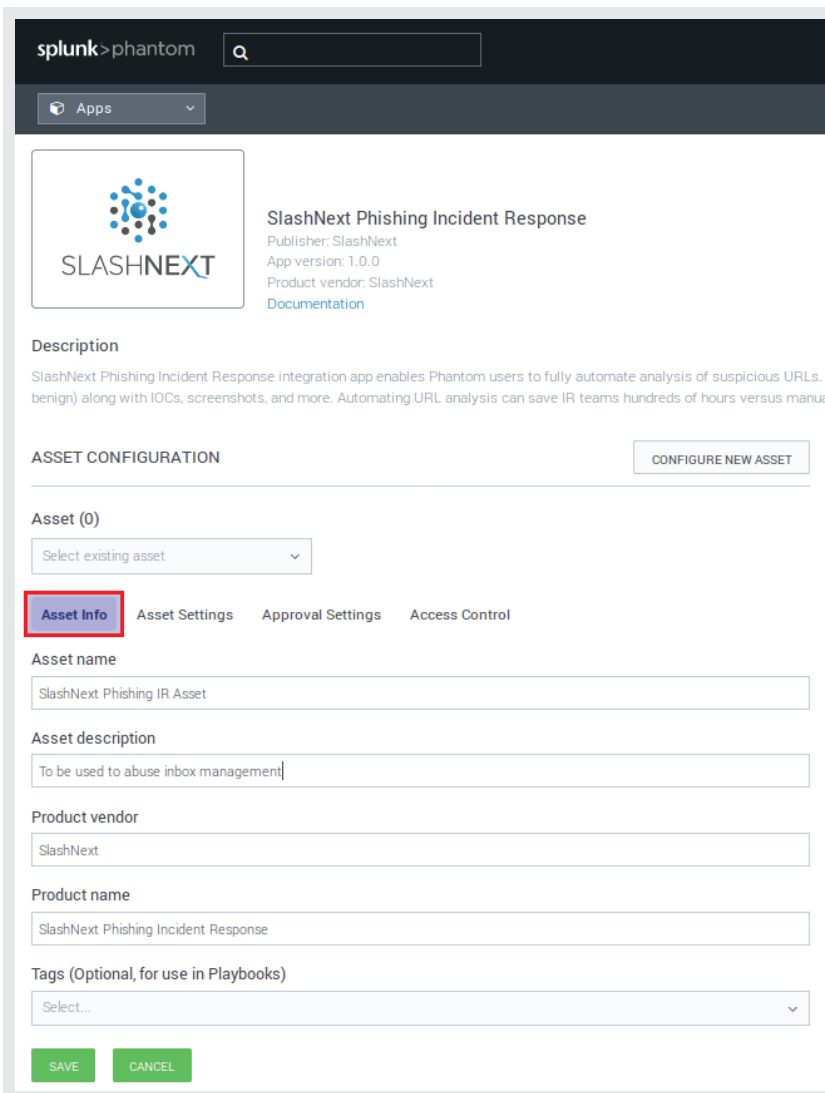
4 | INTEGRATION ACTIVATION

Follow the steps listed below to activate the SlashNext Phishing Incident Response integration in Splunk Phantom SOAR platform.

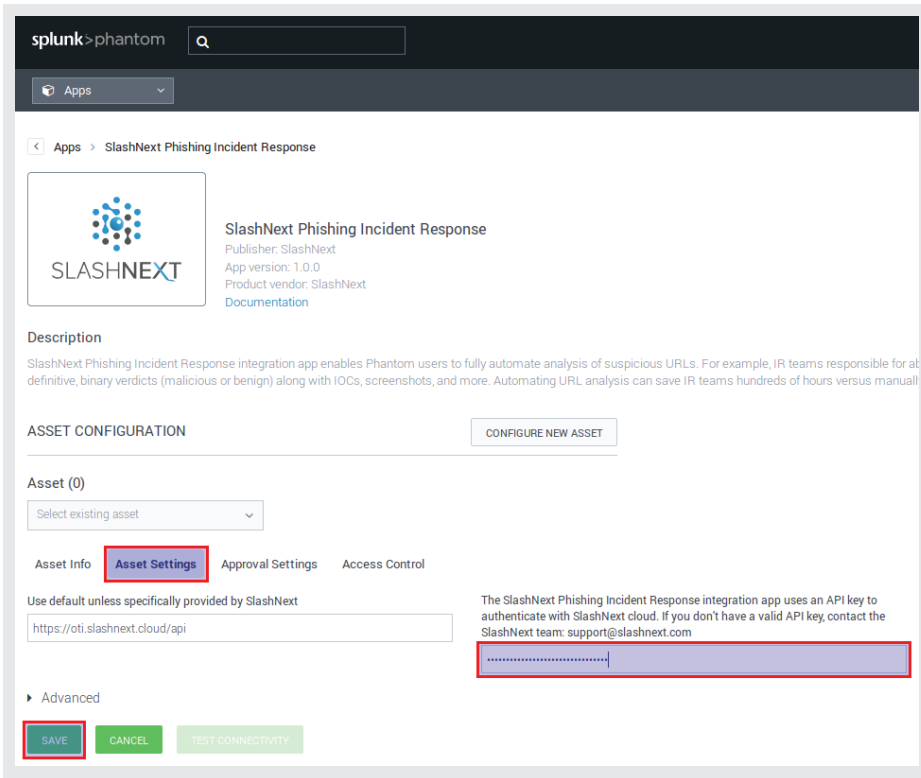
1. On the Phantom **Apps** page, select **Unconfigured Apps** tab and type 'slashnext' in the **Search...** field and press **Enter** button as shown in the snapshot below.



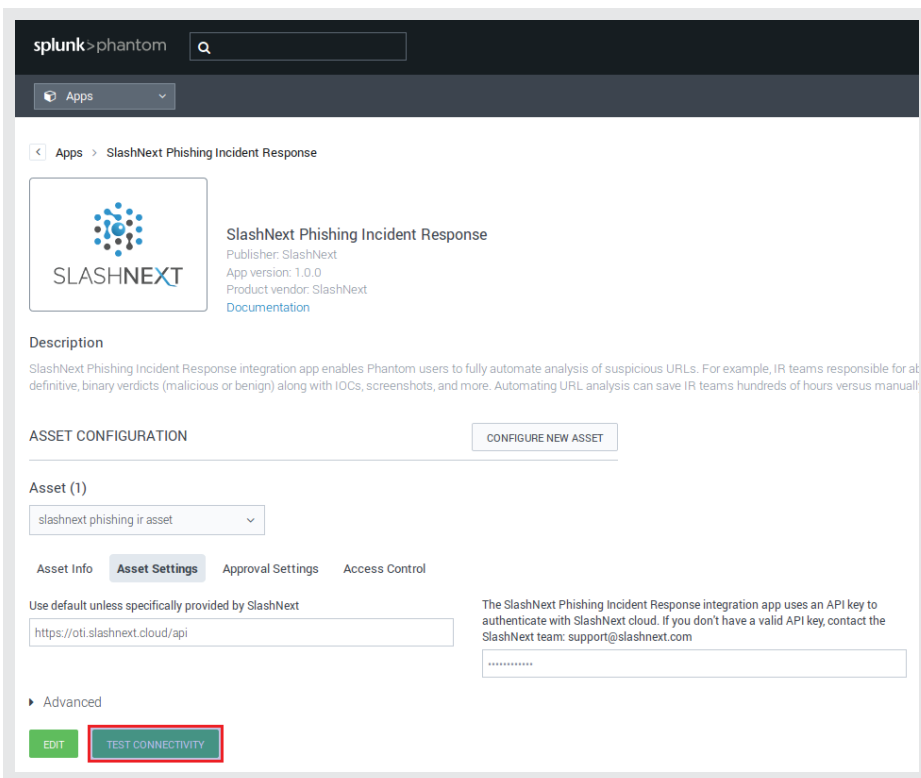
2. SlashNext Phishing Incident Response integration will be listed there, click on **CONFIGURE NEW ASSET** button as shown above.
3. On the **Asset Info** tab, input the new **Asset name** and **Asset description** (as you like) as shown below.



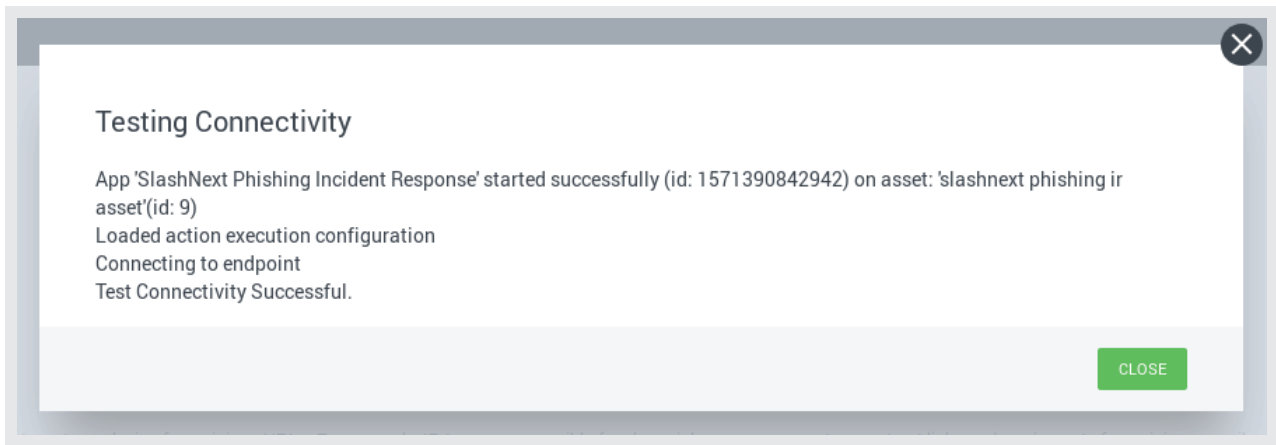
4. On the **Asset Settings** tab, input the **API Key** provided by SlashNext and click **SAVE** as shown below.



5. After saving asset configuration, **TEST CONNECTIVITY** button will become active. Click on it to verify connectivity with SlashNext cloud.



6. In case of successful connection, you will see following message in the **Testing Connectivity** pop-up menu. Click on **CLOSE** and integration app is ready to be used.



5 | ACTIONS

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

1. **host reputation** - Queries the SlashNext cloud database and retrieves the reputation of a host.
2. **host report** - Queries the SlashNext cloud database and retrieves a detailed report.
3. **host urls** - Queries the SlashNext cloud database and retrieves a list of all URLs.
4. **url scan** - Perform a real-time URL reputation scan with SlashNext cloud-based SEER Engine.
5. **url scansync** - Perform a real-time URL scan with SlashNext cloud-based SEER Engine in a blocking mode.
6. **scan report** - Retrieve URL scan results against a previous scan request.
7. **download screenshot** - Downloads a screenshot of a web page against a previous URL scan request.
8. **download html** - Downloads a web page HTML against a previous URL scan request.
9. **download text** - Downloads the text of a web page against a previous URL scan request.
10. **slashnext api quota** - Find information about your API quota, like current usage, quota left etc.

5.1 | HOST REPUTATION

host reputation

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

Action Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
host	Required	The host to look up in the SlashNext Threat Intelligence database. Can be either a domain name or an IPv4 address.	string	domain / IP

Action Output

SLASHNEXT				
<p>SlashNext Phishing Incident Response - Host Reputation</p> <p>action = host reputation host = www.lineageedcx.ru</p>				
Host www.lineageedcx.ru				Verdict Malicious
Threat Status Active	Threat Name Fake Login Page	Threat Type Phishing & Social Engineering	First Seen 10-18-2019 12:44:41 UTC	Last Seen 10-18-2019 12:48:19 UTC

5.2 | HOST REPORT


host report

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

Action Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
host	Required	The host to look up in the SlashNext Threat Intelligence database. Can be either a domain name or an IPv4 address.	string	domain / IP

Action Output



SlashNext Phishing Incident Response - Host Report

action = host report
host = virtualmarketing.pk

Host virtualmarketing.pk				Verdict Malicious
Threat Status Active	Threat Name Fake Login Page	Threat Type Phishing & Social Engineering	First Seen 10-16-2019 15:41:09 UTC	Last Seen 10-18-2019 01:47:15 UTC

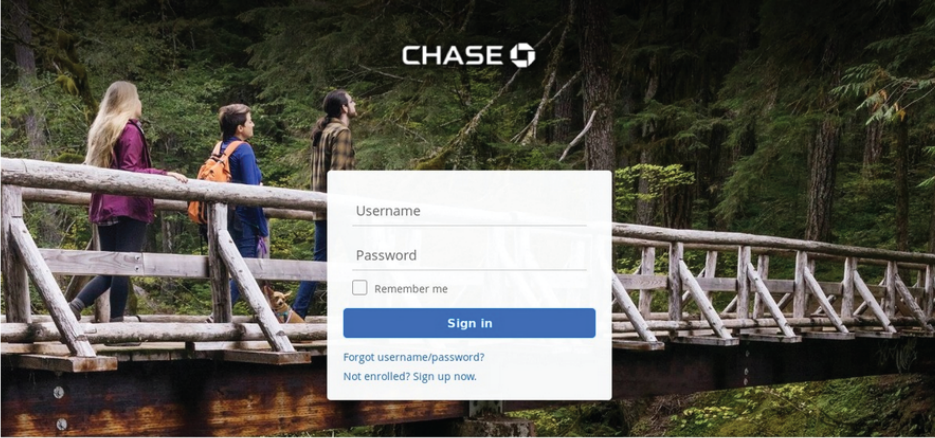
SlashNext Phishing Incident Response - Latest URL

host = virtualmarketing.pk

Scanned URL https://virtualmarketing.pk/voixm/Chase2019/myaccount/index.php			Verdict Malicious
Threat Status Active	Threat Name Fake Login Page	Threat Type Phishing & Social Engineering	
Scan ID 873d9975-c6c4-42ef-9674-ff3ee4a44ed9	First Seen 10-16-2019 15:41:09 UTC	Last Seen 10-16-2019 15:53:44 UTC	

SlashNext Phishing Incident Response - Webpage Screenshot

Download Screenshot



SlashNext Phishing Incident Response - Webpage HTML

Download HTML

SlashNext Phishing Incident Response - Webpage Text

Download Text

5.3 | HOST URLS


host urls

Queries the SlashNext Cloud database and retrieves a list of all URLs associated with the specified host.

Action Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
host	Required	The host to look up in the SlashNext Threat Intelligence database, for which to return a list of associated URLs. Can be either a domain name or an IPv4 address.	string	domain / IP
limit	Optional	The maximum number of URL records to fetch. Default is "10".	numeric	

Action Output



SlashNext Phishing Incident Response - Host URLs

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

Scanned URL		Verdict	
https://blueheaventravel.com/vendor/filp/whoops/up/index.php?email=		Malicious	
Threat Status	Threat Name	Threat Type	
No Longer Active	Fake Login Page	Phishing & Social Engineering	
Scan ID	First Seen	Last Seen	
N/A	10-16-2019 17:39:54 UTC	10-18-2019 03:48:20 UTC	
Final URL		Verdict	
https://blueheaventravel.com/vendor/filp/whoops/up/pulp.php?rand=46inboxlightaspxn.4827685990&fid.28.9164762324&fid=1&fav.1&rand...		Malicious	

Scanned URL		Verdict	
https://blueheaventravel.com/vendor/filp/whoops/up/index.php?email=Jackdavis@eureliosollutions.com		Malicious	
Threat Status	Threat Name	Threat Type	
No Longer Active	Fake Login Page	Phishing & Social Engineering	
Scan ID	First Seen	Last Seen	
N/A	10-16-2019 15:21:56 UTC	10-18-2019 01:28:09 UTC	
Final URL		Verdict	
https://blueheaventravel.com/vendor/filp/whoops/up/pulp.php?rand=46inboxlightaspxn.4827685990&fid.28.9164762324&fid=1&fav.1&rand...		Malicious	

5.4 | URL SCAN


url scan

Performs 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 be returned immediately. If not, this command will submit a URL scan request and return with the message "check back later" and include a unique Scan ID. You can check the results of this scan using the "scan report" command anytime after 60 seconds using the returned Scan ID.

Action Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
url	Required	The URL that needs to be scanned.	string	URL
extended_info	Optional	Whether to download forensics data, such as screenshot, HTML, and rendered text. If "checked", forensics data will be returned. If "unchecked" (or empty) forensics data will not be returned.	boolean	

Action Output



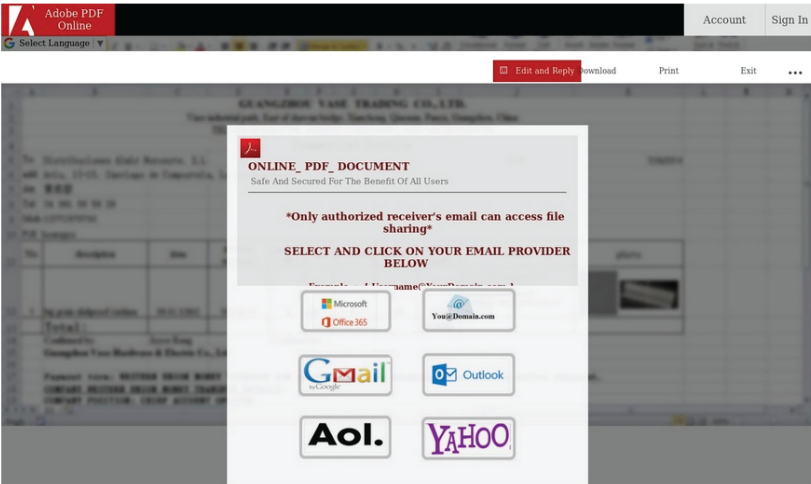
SlashNext Phishing Incident Response - URL Scan

action = url scan
url = http://www.compassok.tk/vilo/msw/data/UntitledNotebook1.html

Scanned URL http://www.compassok.tk/vilo/msw/data/UntitledNotebook1.html		Verdict Malicious
Threat Status Active	Threat Name Fake Login Page	Threat Type Phishing & Social Engineering
Scan ID d4747f5f-0110-4670-a843-013c5b4231e9	First Seen 10-16-2019 23:56:48 UTC	Last Seen 10-17-2019 00:00:16 UTC
Final URL https://www.compassok.tk/vilo/msw/data/UntitledNotebook1.html		Verdict Malicious

SlashNext Phishing Incident Response - Webpage Screenshot

[Download Screenshot](#)



SlashNext Phishing Incident Response - Webpage HTML

[Download HTML](#)

SlashNext Phishing Incident Response - Webpage Text

[Download Text](#)

5.5 | URL SCAN SYNC


url scansync

Performs 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 be 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.

Action Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
url	Required	The URL that needs to be scanned.	string	URL
extended_info	Optional	Whether to download forensics data, such as screenshot, HTML, and rendered text. If "checked", forensics data will be returned. If "unchecked" (or empty) forensics data will not be returned.	boolean	
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. You can run the command again with a different timeout. If no timeout value is specified, a default timeout value is 60 seconds.	numeric	

Action Output




SlashNext Phishing Incident Response - URL Scan Sync
 action = url scansync
 url = http://www.shoppingwo.com/js/shop/171B.php

Scanned URL http://www.shoppingwo.com/js/shop/171B.php		Verdict Malicious
Threat Status Active	Threat Name Fake Login Page	Threat Type Phishing & Social Engineering
Scan ID c2122371-3669-4751-8c0c-e61a6a907d33	First Seen 10-17-2019 07:50:04 UTC	Last Seen 10-17-2019 07:50:17 UTC

SlashNext Phishing Incident Response - Webpage Screenshot

Download Screenshot


ERLEBEN, WAS VERBINDET.

KUNDENCENTER


Mit dem Telekom Login
anmelden


Angemeldet bleiben [Benutzername oder Passwort vergessen?](#)

LOGIN

[Brauchen Sie Hilfe?](#)

Noch keinen Telekom Login? [Telekom Login erstellen und Kundencenter nutzen.](#)



© Telekom Deutschland GmbH
20.11.1.
Impressum  Datenschutz

SlashNext Phishing Incident Response - Webpage HTML

Download HTML

SlashNext Phishing Incident Response - Webpage Text

Download Text

5.6 | URL SCAN REPORT


scan report

Retrieves the results of a URL scan against a previous scan request. If the scan is finished, results will be returned immediately; otherwise the message "check back later" will be returned.

Action Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
scanid	Required	Scan ID of the scan for which to get the report. Can be retrieved from the "url scan" action or "url scansync" action.	string	snx scan id
extended_info	Optional	Whether to download forensics data, such as screenshot, HTML, and rendered text. If "checked", forensics data will be returned. If "unchecked" (or empty) forensics data will not be returned.	boolean	

Action Output



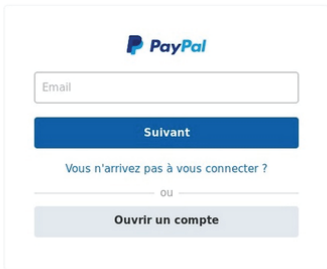
SlashNext Phishing Incident Response - Scan Report

action = scan report
scan id = 39cb08a3-c5ea-44a5-a097-9cfd78285299

Scanned URL https://caservice.ml/paypal		Verdict Malicious
Threat Status Active	Threat Name Fake Login Page	Threat Type Phishing & Social Engineering
Scan ID 39cb08a3-c5ea-44a5-a097-9cfd78285299	First Seen 10-16-2019 19:19:18 UTC	Last Seen 10-16-2019 19:29:18 UTC
Final URL https://caservice.ml/paypal/a931ca/en/season.php?country.x=ca988675e017b27aa4c81f3b53c8bf4ca988675e017b27aa4c81f3b53c8bf4		Verdict Malicious

SlashNext Phishing Incident Response - Webpage Screenshot

Download Screenshot



SlashNext Phishing Incident Response - Webpage HTML

Download HTML

SlashNext Phishing Incident Response - Webpage Text

Download Text

5.7 | DOWNLOAD SCREENSHOT


download screenshot

Downloads a screenshot of a web page against a previous URL scan request.

Action Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
scanid	Required	Scan ID. Can be retrieved from the "url scan" action or the "url scansync" action.	string	snx scan id

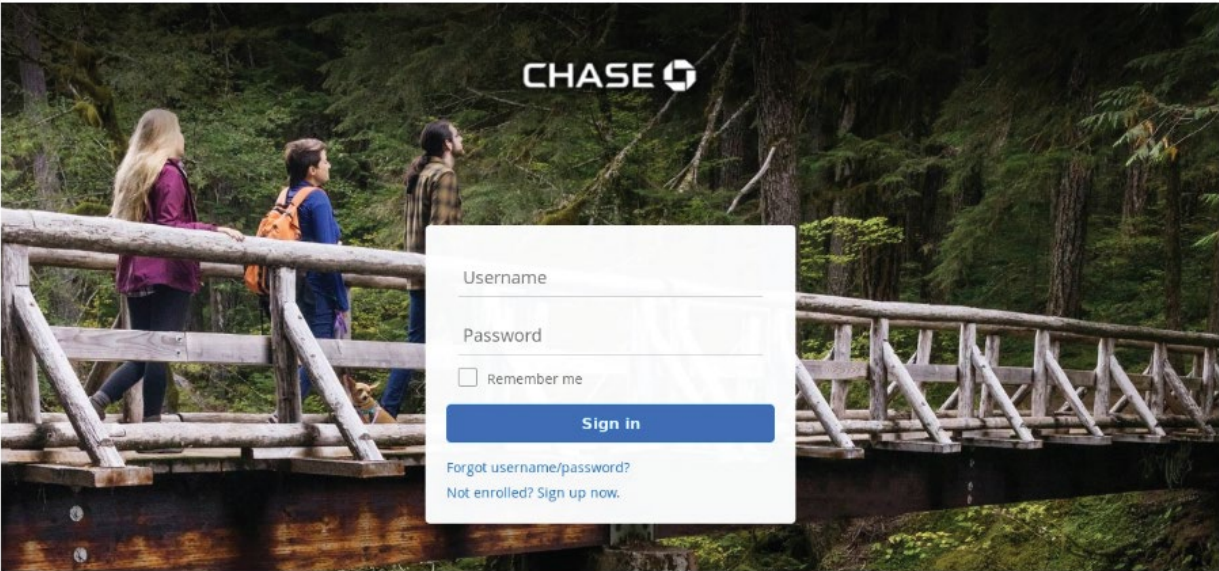
Action Output



SlashNext Phishing Incident Response - Download Screenshot

action = download screenshot
 scan id = 873d9975-c6c4-42ef-9674-ff3ee4a44ed9

[Download Screenshot](#)



Follow us: [f](#) [i](#) [t](#) [y](#) [in](#)

[Contact us](#) [Privacy](#) [Security](#) [Terms of use](#) [Our commitment to accessibility](#) [SAFE Act: Chase Mortgage Loan Originators](#) [Fair Lending](#) [About Chase](#) [J.P. Morgan](#) [JPMorgan Chase & Co.](#)
[Careers](#) [Español](#) [Chase Canada](#) [Site map](#) [Member FDIC](#) [Equal Housing Lender](#)
 © 2019 JPMorgan Chase & Co.

5.8 | DOWNLOAD HTML


download html

Downloads a web page HTML against a previous URL scan request.

Action Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
scanid	Required	Scan ID. Can be retrieved from the "url scan" action or the "url scansync" action.	string	snx scan id

Action Output



SlashNext Phishing Incident Response - Download HTML

action = download html
scan id = 873d9975-c6c4-42ef-9674-ff3ee4a44ed9

Download HTML

5.10 | DOWNLOAD TEXT


download text

Downloads the text of a web page against a previous URL scan request.

Action Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
scanid	Required	Scan ID. Can be retrieved from the "url scan" action or the "url scansync" action.	string	snx scan id

Action Output



SlashNext Phishing Incident Response - Download Text

action = download text
scan id = 873d9975-c6c4-42ef-9674-ff3ee4a44ed9

Download Text

5.11 | API QUOTA

api quota

Find information about your API quota, like current usage, quota left etc.

Action Parameters

No parameters are required for this action

Action Output



SlashNext Phishing Incident Response - API Quota

action = api quota
Coming soon...