SLASHNEXT

USER GUIDE V1.0.0

SlashNext Phishing IR Integration Guide Demisto SOAR

TABLE OF CONTENTS

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.

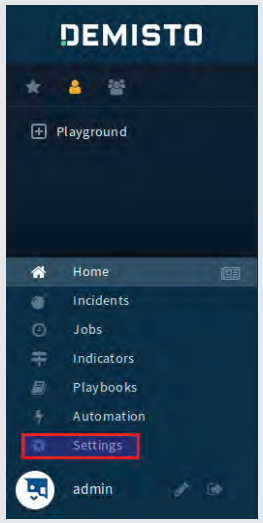
The SlashNext Phishing Incident Response integration app uses an API key to authenticate with SlashNext cloud. If you don't have a valid API key, contact the SlashNext team: support@slashnext.com

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 yml 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.



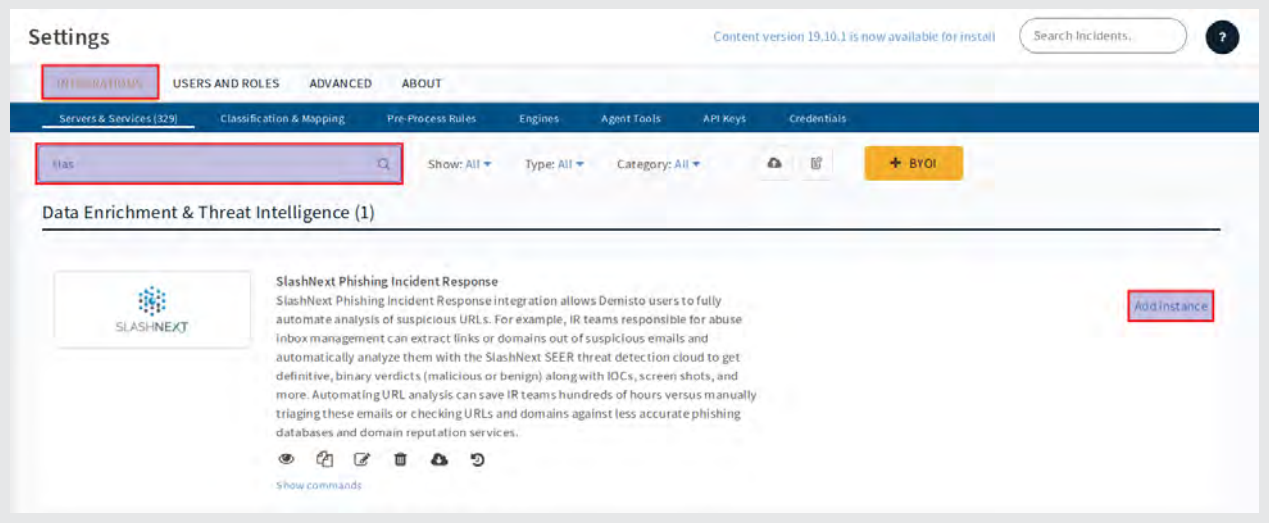
3. Select **INTEGRATIONS** tab on **Settings** page, and then select **Servers & Services** tab and click on **Upload Integration** button as shown in the snapshot below.

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

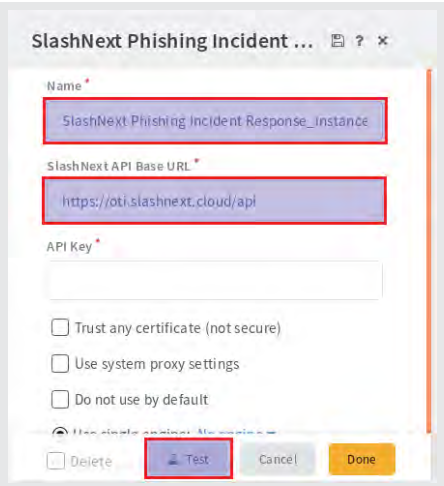
4 | INTEGRATION ACTIVATION

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

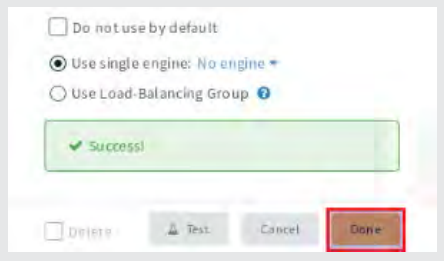
1. On the Demisto **Settings** page, select **INTEGRATIONS** tab and type slashnext in the **Search integration...** field and press Enter button as shown in the snapshot below.



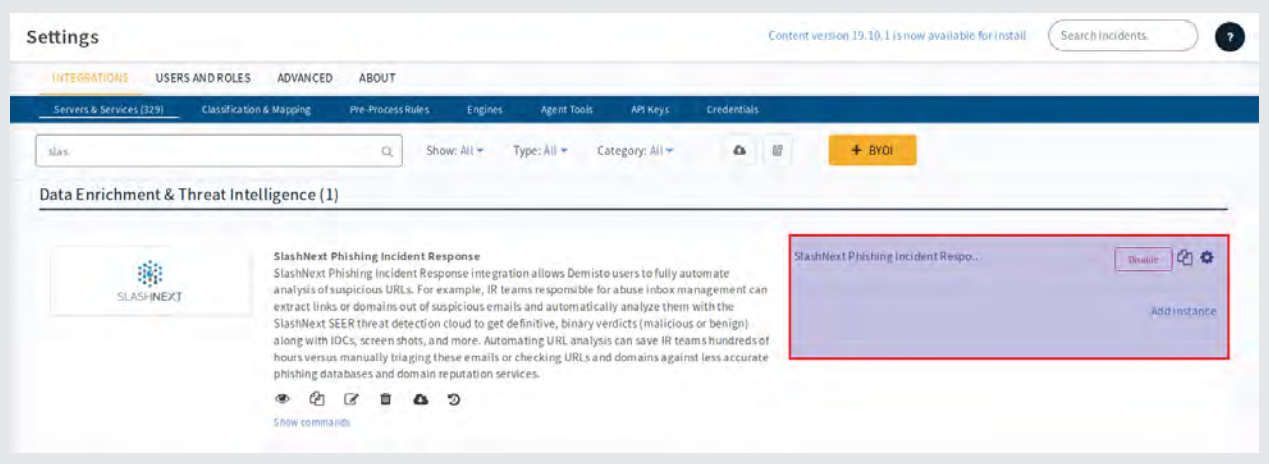
2. SlashNext Phishing Incident Response Integration will be listed, click on **Add instance** button as shown above.
3. Type the new instance **Name** (as you like), **Your API Key** (provided by SlashNext) and the **SlashNext API Base URL** (if specifically provided by SlashNext otherwise leave this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

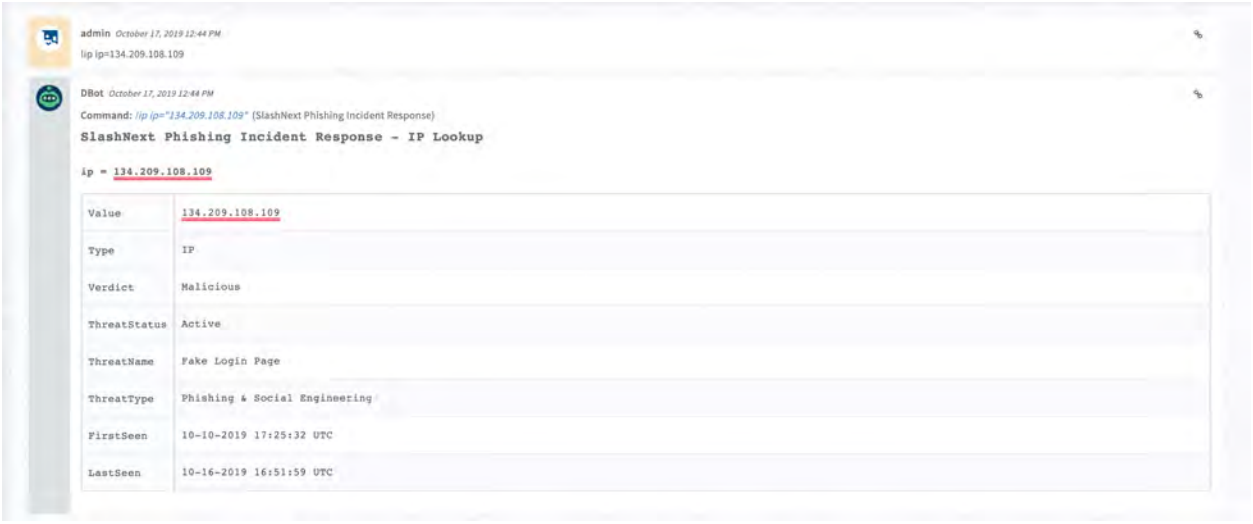
1. **ip -** Looks up an IP address indicator in the SlashNext Threat Intelligence database.
2. **domain -** Looks up a Fully Qualified Domain Name (FQDN) indicator in the SlashNext Threat Intelligence database.
3. **slashnext-host-reputation -** Queries the SlashNext Cloud database and retrieves the 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;

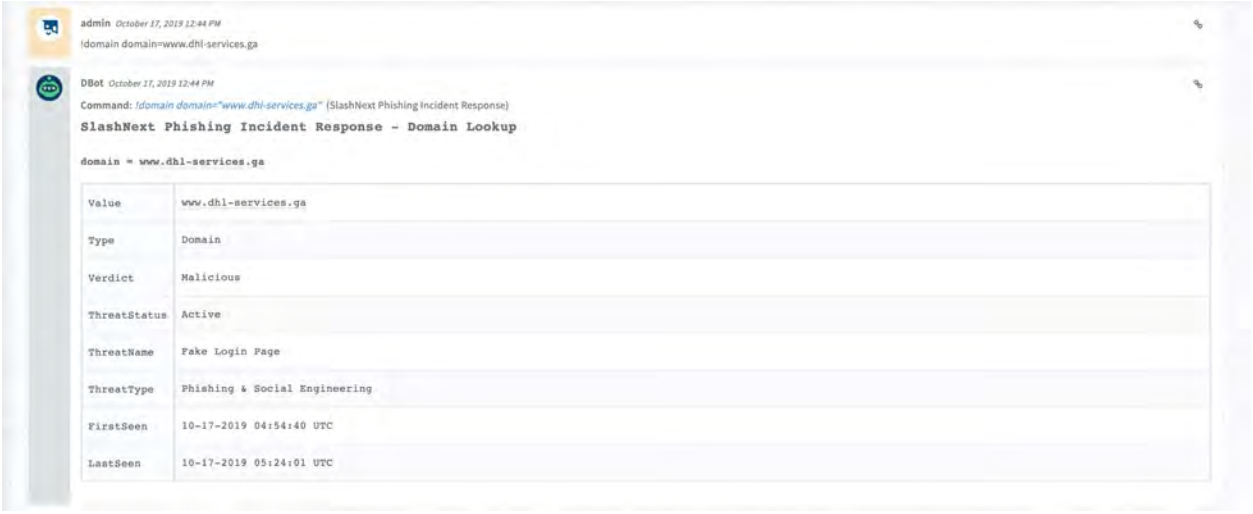


5.2 | DOMAIN

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;

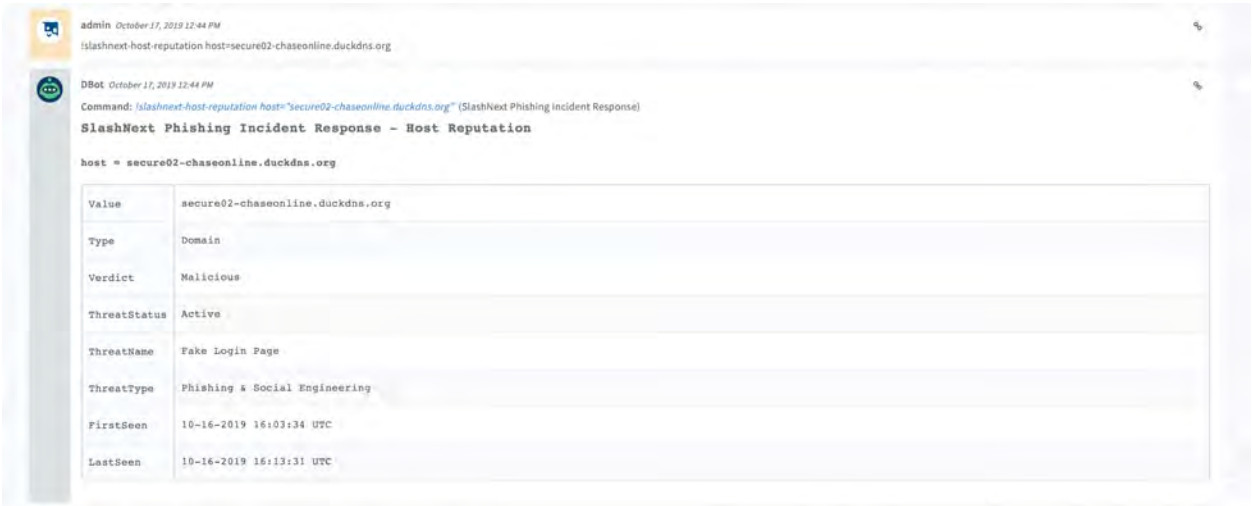


5.3 | HOST REPUTATION

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;

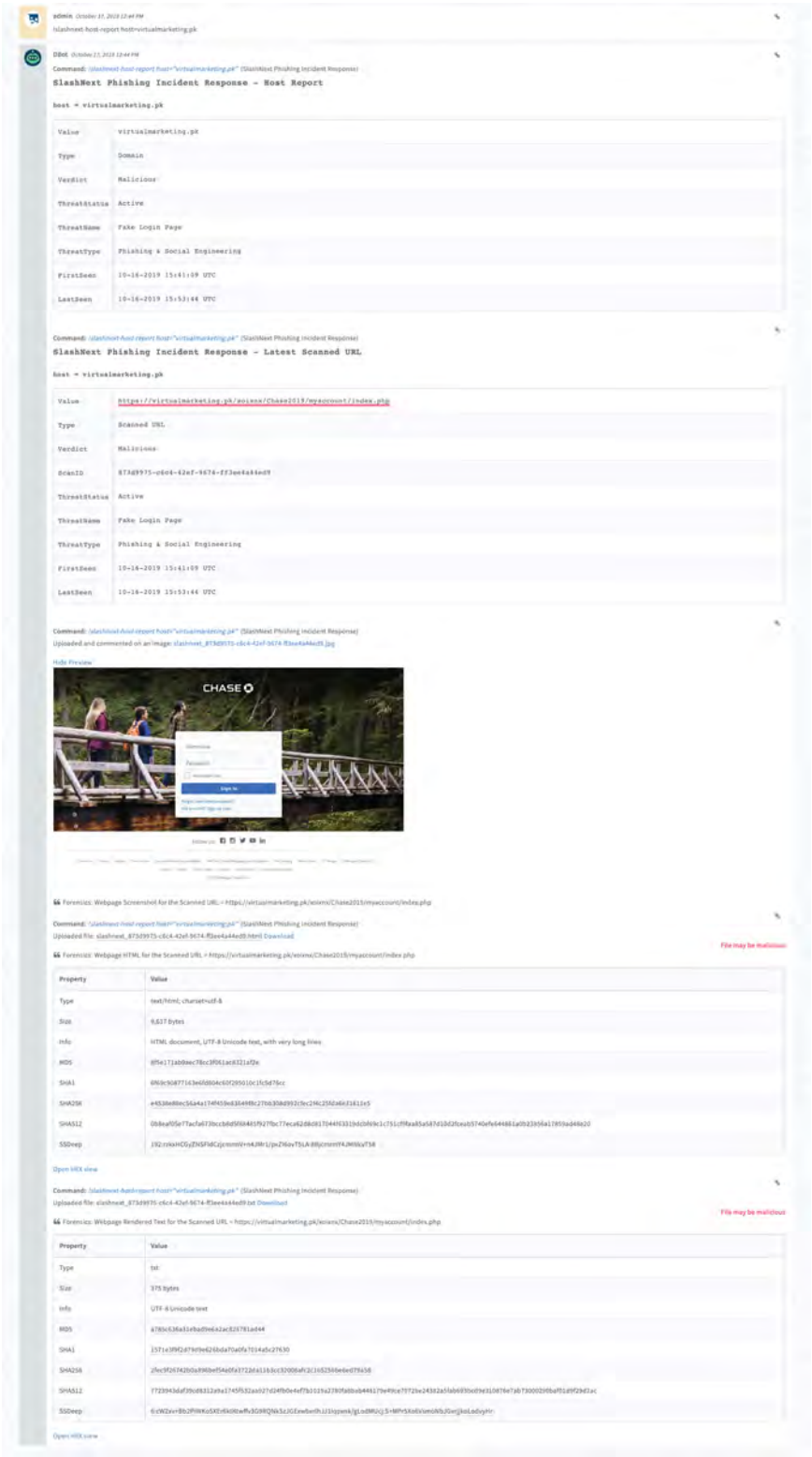


5.4 | HOST REPORT

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;

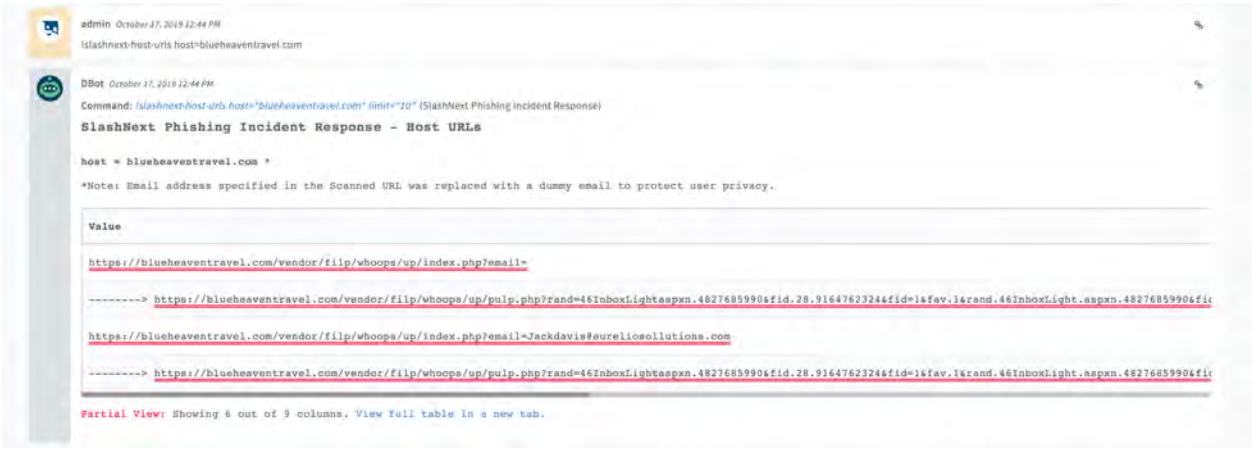


5.5 | HOST URLs

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;



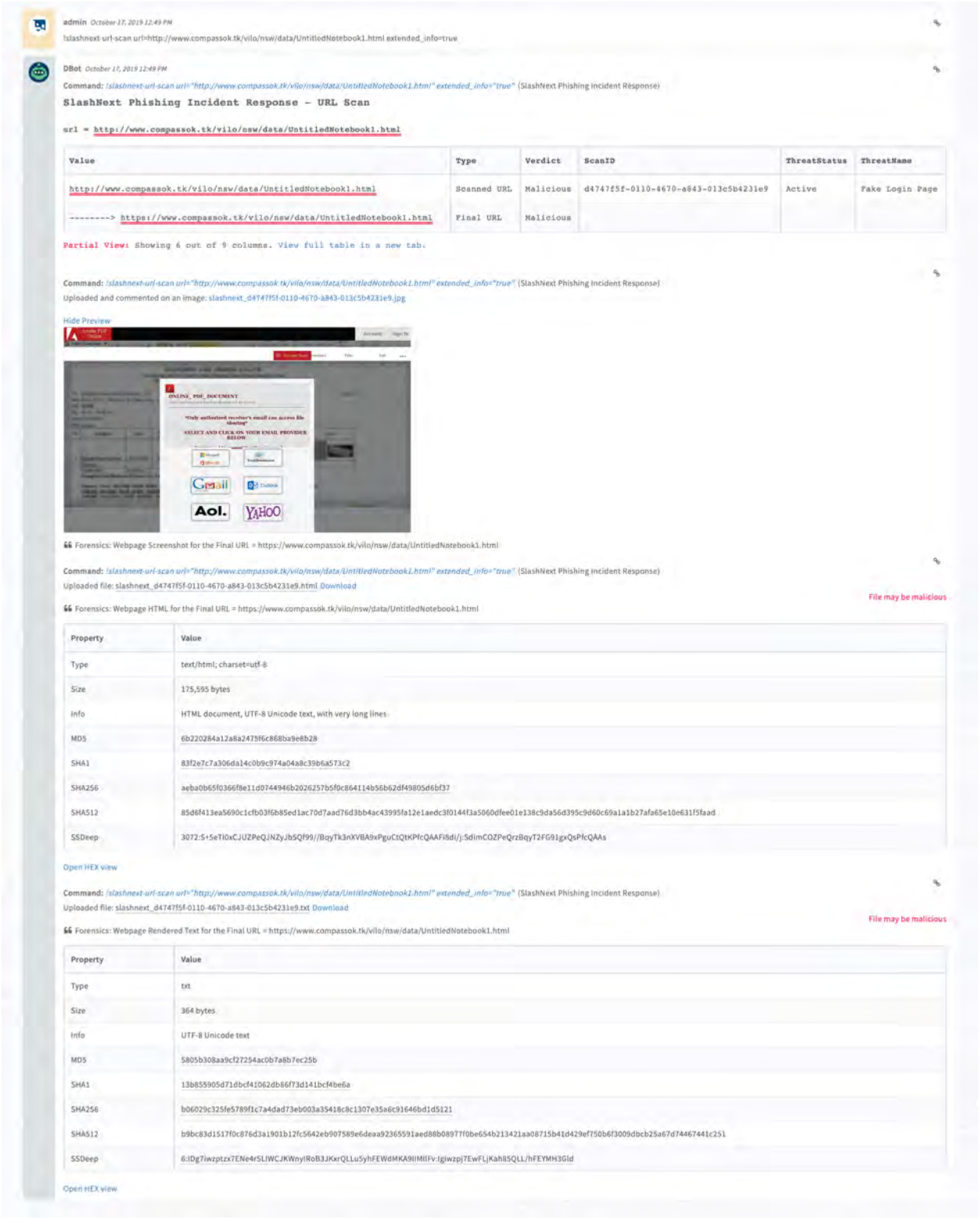
5.6 | URL SCAN

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 extented_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;

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

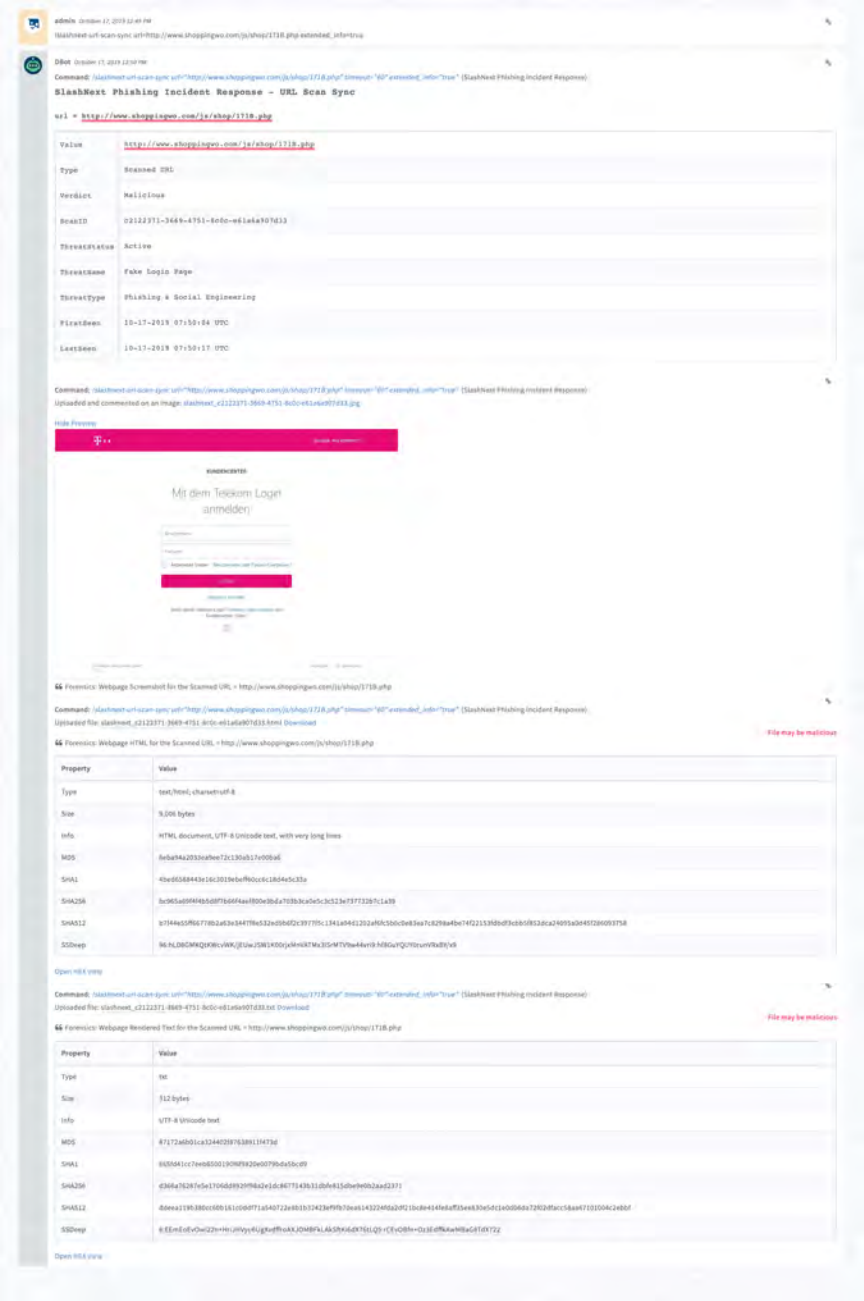


5.7 | URL SCAN SYNC

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 extented_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;

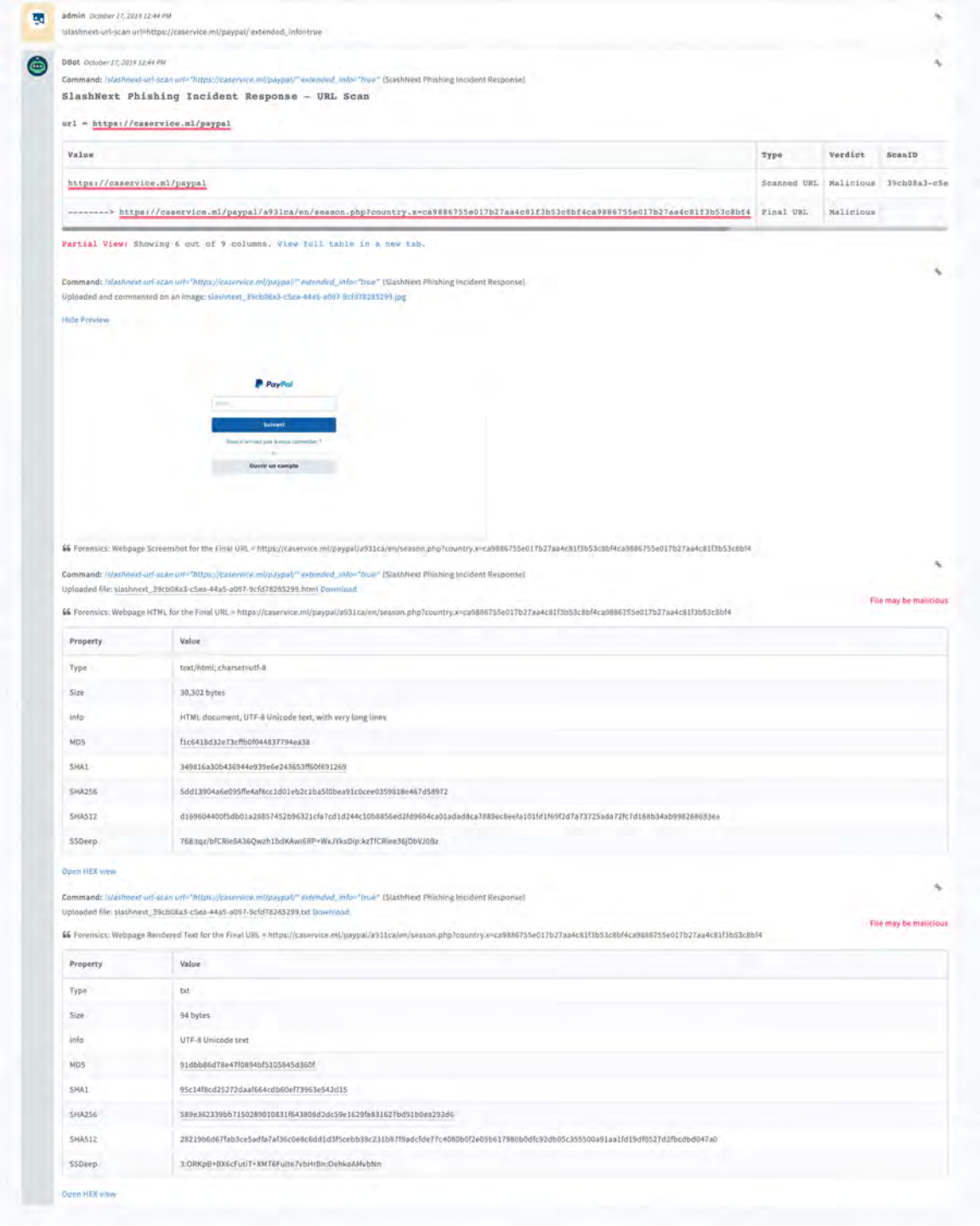


5.8 | URL SCAN REPORT

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 extented_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;

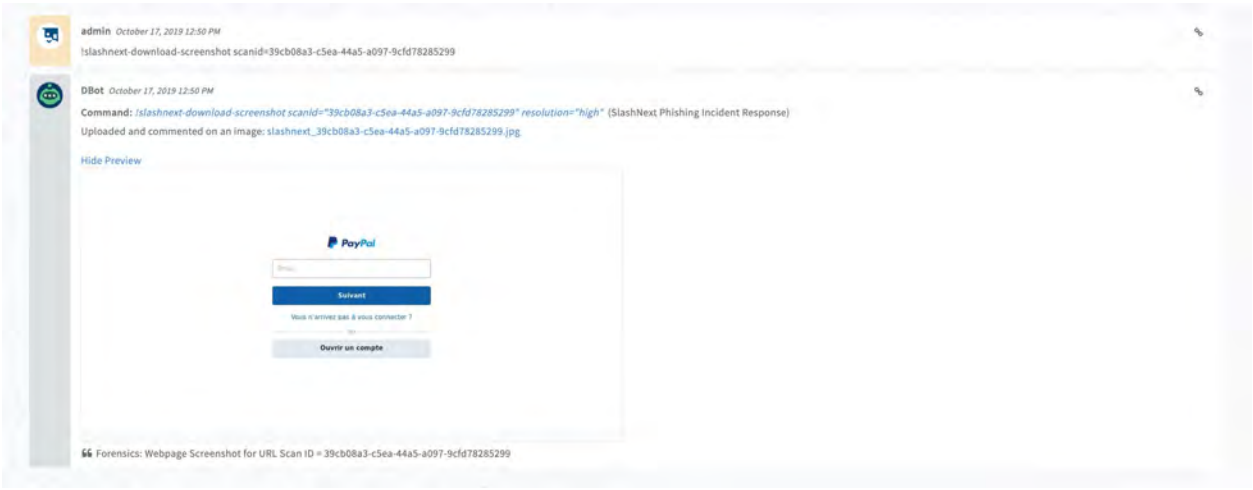


5.9 | DOWNLOAD SCREENSHOT

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;

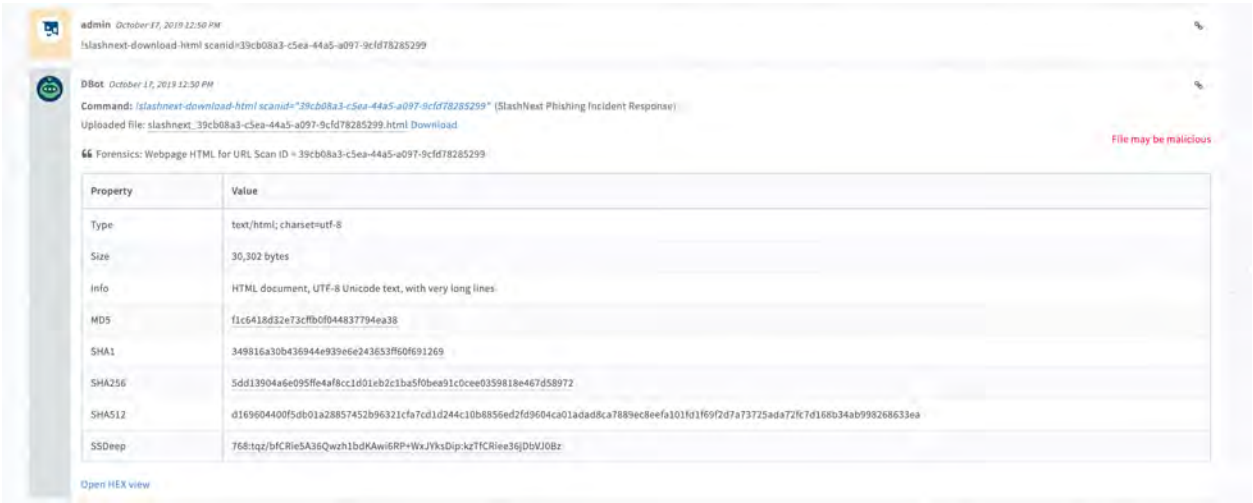


5.10 | DOWNLOAD HTML

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;