USER GUIDE V1.0.0

SlashNext Phishing IR Integration Guide Swimlane SOAR

TABLE OF CONTENTS

1		3
2	REQUIREMENTS	3
3		3
4	ACTIONS	8
	SlashNext : Host Reputation	8
	Inputs	8
	Outputs	9
	SlashNext : Host Report	10
	Inputs	10
	Outputs	11
	SlashNext : Host URLs	12
	Inputs	12
	Outputs	12
	SlashNext : URL Scan	13
	Inputs	13
	Outputs	14

TABLE OF CONTENTS

SlashNext : URL Scan Sync	
Inputs	
Outputs	
SlashNext : Scan Report	
Inputs	
Outputs	
SlashNext : Download HTML	
Inputs	
Outputs	
SlashNext : Download Screenshot	
Inputs	
Outputs	
SlashNext : Download Text	
Inputs	
Outputs	
SlashNext : API Quota	
Inputs	
Outputs	
5 PLAYBOOKS	
Playbook - SlashNext Host Reputation	
Outputs	
Playbook - SlashNext URL Scan	
Outputs	

1 | INTRODUCTION

SlashNext Phishing Incident Response Integration for Swimlane SOAR platform is a bundle (swimbundle) which is a collection of Swimlane actions and assets that utilize SlashNext's On-demand Threat Intelligence (OTI) APIs to implement all the Phishing Incident Response (IR) actions.

2 | REQUIREMENTS

- 1. Swimlane Platform Version >= 10.0.1
- 2. Swimlane Server running
- 3. Swimlane Platform License
- 4. SlashNext Phishing Incident Response Plugin (swimbundle created using btb build server)
- 5. SlashNext On-demand Threat Intelligence (OTI) API Key provisioned by SlashNext to authenticate requests to SlashNext cloud

3 | INSTALLATION

To install SlashNext plugin into Swimlane platform, follow the steps below:

1. Log in to the Swimlane platform using the credentials created.

You can set up your Swimlane user profile by following the official docs at the following link: https://swimlane.com/knowledge-center/docs/introduction/welcome-to-swimlane

0	SWIM	ILANE	
0	Welcome to Swimlane Prioritize alerts, remediate threats and improve operational performance.	Usernane Password e	0
	Δ		

2. Once logged in and user profile is completed, go to the Integrations tab from the sidebar menu.



3. Then switch to the Plugins tab.

						+ New Task	
Ass			Plugins				
Plu	ugins en	nable you to peri	form out-of-the	-box integrations with thir	d-party vendors. Once installed, new options will be available in Assets and To	asks.	Upload Plugins

4. Click on Upload Plugins button and select the SlashNext plugin from the browse menu. Once successfully uploaded, the plugins tab would look something like this.

		Plugins						
Plugins end	able you to perfo	orm out-of-the-b	pox integrations with thir	d-party vendors. Once inst	alled, new options will	be available in Assets a	nd Tasks.	Upload Plugins
Name			Description		Version	Author	Python Version	
sw_slash	next_phishing	_incident_res	pon: SlashNext Phishir	ng Incident Response int	1.0.2	SlashNext	2.7	Î

5. Next, go to the Assets tab and click on New Asset.

					+ New Task	① Upload Tasks / Scripts	+ New Asset
Assets							
Assets har	ndle secure auth	entication and	l version mangement for e	xternal systems that are consumed by your tasks.			

6. A new asset popup screen would open. From there, select the asset type SlashNext Phishing Incident Response.

General Name Enter asset name Description Enter description for the asset
Name Enter asset name Description Enter description for the asset
Enter asset name Description Enter description for the asset
Description Enter description for the asset
Enter description for the asset
Asset Type
A
٩
Version: 1.0.3 Python: 2.7
SlashNext Phishing Incident Response Version: 1.0.4 Python: 2.7
Directory Server
Active Directory Python: 2.7
Email Server
IMAP Email Python: 2.7

7. Next, click on the Details tab and enter the SlashNext API Key and SlashNext API Base URL.

SlashNext API Base URL refers to the SlashNext endpoint URL. Do not changes its value from the default one until specified by SlashNext. Insert the SlashNext API key provided by SlashNext in the **SlashNext API Key** parameter.

New Asset	✓ Save
General Details	
SlashNext API Key 🕐 Required	
SlashNext API Base URL 🕐 Required	
https://oti.slashnext.cloud/api	
Test Connection	

8. Make sure that the entered values are correct. Then, click on Test Connection button. If you entered the values correctly, a success message will be shown. Otherwise, an error message will be shown.



9. Once the connection is successful, Click on the New Task button. Now you would see that the SlashNext actions are available. Click on any of the SlashNext Tasks from them and click on Create button at the top right.

New Task		✔ Create 🔍 Fork
Filter types		
All Data Creation Investigation	Email Import Data Creation Import and update records from Emails	Network File Data Creation CSV & Excel files on network share
Misc Scripts	SlashNext URL Scan Sync Investigation (Python: 2.7) Performs a real-time URL scan with SlashNext cloud-based SEER Engine in a blocking mode.	SlashNext URL Scan Sync Investigation (Python: 2.7) Performs a real-time URL scan with SlashNext cloud-based SEER Engine in a blocking mode.
	SlashNext Scan Report Investigation (Python: 2.7) Retrieves the results of a URL scan against a previous scan request. If the scan is finished,	SlashNext Scan Report Investigation (Python: 2.7) Retrieves the results of a URL scan against a previous scan request. If the scan is finished,
	SlashNext Host Report Investigation (Python: 2.7) This action queries the SlashNext cloud database and retrieves a detailed report for a	SUSTINEXT Host Reputation Investigation (Python: 2.7) This action queries the SlashNext cloud database and retrieves the reputation of a
	SlashNext Host Report Investigation (Python: 2.7) This action queries the SlashNext cloud database and retrieves a detailed report for a	SlashNext Host Reputation Investigation (Python: 2.7) This action queries the SlashNext cloud database and retrieves the reputation of a
	SlashNext Host Urls Investigation (Python: 2.7) This action queries the SlashNext cloud database and retrieves a list of all URLs	SlashNext URL Scan Investigation (Python: 2.7) Performs a real-time URL scan with SlashNext cloud-based SEER Engine. If the specified

10. Select your related Swimlane application and click Save on the top right.

New Task \ SlashNext Host Reputation	✓ Save
Task Name	
Host Reputation	
Related Application	

Name:				
SNX Host	Reputation (QA)			
Descriptio	on:			
Task Type:	:			
Task Type: Investigatio	: on: SlashNext Host	t Reputation		
Task Type: Investigation Asset: Requ	: on: SlashNext Host uired	t Reputation		
Task Type: Investigatio Asset: Requ SNX Ass	: on: SlashNext Host uired Set	t Reputation		× ×
Task Types Investigation Asset: Require SNX Ass	: on: SlashNext Host vired set	t Reputation		x * Q
Task Type Investigation Asset: Require SNX Ass	: on: SlashNext Host uired set	t Reputation		× . વ
Task Type Investigatio Asset: Requ SNX Ass SNX Ass Version:	: on: SlashNext Host vired set 1.0.0 PythonVersio	t Reputation	nishing Inciden	× × Q ent Response
Task Type Investigatid Asset: Requ SNX Ass (SNX Ass Version:	: on: SlashNext Host uired Set Set 1.0.0 PythonVersio	t Reputation	hishing Inciden	ent Response
Task Type: Investigati Asset: Requ SNX Ass SNX Ass Version:	: on: SlashNext Host wired set set 1.0.0 PythonVersio	r Reputation on: 2.7 Type: Slash Next Pl	ishing Inciden	× م م ent Response

11. Then, from the General Tab, click on the Asset dropdown and select the SlashNext Asset that you created earlier.

12. Save the task. Now you can add the Input Configurations, Outputs and Triggers based on your Application requirements.

4 | ACTIONS

SlashNext Integration Plugin for Swimlane contains the following actions as elaborated below:

4.1 | SLASHNEXT : HOST REPUTATION

Host Reputation

This action queries the SlashNext cloud database and retrieves the reputation of a host.

4.1.1 | INPUT

PARAMETER	REQUIRED	DESCRIPTION
host	True	The host to look up in the SlashNext Threat Intelligence database. It can be either a domain name or an IPv4 address

Description: The host to look up in the SlashNext Threat Intelligence database. Can be either a domain name or an IPv4 Field: Host Example:	Option:	host Required	Туре:	Record	
address. Example:		Description: The host to look up in the SlashNext Threat	Field:	Host	
Example:		intelligence database. Can be either a domain name or an IPv4 address.	Tield.		
		Example:			

4.1.2 | OUTPUT

eneral Configuration Output Parameters Output	ts Triggers					
8 Output Parameters Defined This action queries the SlashNext cloud database and retrieves the reputation of a host.						
Parameter		Name	Description			
host_errorNo		Error Number				
host_errorMsg		Error Message				
host_threatData_verdict						
host_threatData_threatStatus		Threat Status				
host_threatData_threatName		Threat Name				
host_threatData_threatType		Threat Type				
host_threatData_firstSeen		First Seen				
host_threatData_lastSeen		Last Seen				

4.2 | SLASHNEXT : HOST REPORT

Host Report

This action queries the SlashNext cloud database and retrieves a detailed report for a host and associated URL.

4.2.1 | INPUT

PARAMETER	REQUIRED	DESCRIPTION
host	True	The host to look up in the SlashNext Threat Intelligence database. It can be either a domain name or an IPv4 address

General	Configur	ation Output Parame	ters Outputs	Triggers					
SlashNe	SlashNext Host Report Configuration								
	Option:	host Required			Туре:	Record			
		Description: The host to lo Intelligence database. Car			Field:	Host			
		address.							
		Example:							

4.2.2 | OUTPUT

This function will report the threat information of the Host in the notes section. Additionally, it will show the threat information of the latest URL associated with that Host along with its webpage's forensics (Screenshot, HTML and Text), if available:

out Parameters Defined n queries the SlashNext cloud database and retrieves a detailed report for a host and associated URL.		
er -	Name	Description
rorNo		
rorMsg		
reatData_verdict		
reatData_threatStatus		
reatData_threatName		
reatData_threatType		
reatData_firstSeen		
reatData_lastSeen		
r1_errorNo		
r1_errorMsg		
rl_urlDataList_url		
rl_urlDataList_scanId		
rl_urlDataList_threatData_verdict		
rl_urlDataList_threatData_threatStatus		
rl_urlDataList_threatData_threatName		
rl_urlDataList_threatData_threatType		
rl_urlDataList_threatData_firstSeen		
rl_urlDataList_threatData_lastSeen		
rl_normalizeData_normalizeStatus		
rl_normalizeData_normalizeMessage		
hot_errorNo		
hot_errorMsg		
hot_scData_scName		
hot_scData_scContentType		
hot_scData_scBase64		
rorNo		
rorHsg		
mlData_htmlName		
mlData_htmlContentType		
mlData_htmlBase64		
rorNo		
rorMsg		
xtData_textName		
utbata tautbasa64		

4.3 | SLASHNEXT : HOST URLS

Host URLs

Search in SlashNext Cloud database and retrieve list of all URLs associated with the specified host.

4.3.1 | INPUT

PARAMETER	REQUIRED	DESCRIPTION
host	True	The Host to look up in the SlashNext Threat Intelligence database, for which to return a list of associated URLs. It can either be a domain name or an IPv4 address
limit	False	The maximum number of URL records to fetch. Default value is "10"



4.3.2 | OUTPUT

rral Configuration Output Parameters Outputs Triggers		
21 Output Parameters Defined This action queries the SlashNext cloud database and retrieves a list of all URLs associated with the specified host.		
Parameter	Name	Description
urls_errorNo		
urls_errorMsg		
urls_urlDataList_url		
urls_urlDataList_scanId	Scanned URL Scan ID	
urls_urlDataList_threatData_verdict		
urls_urlDataList_threatData_threatStatus		
urls_urlDataList_threatData_threatName		
urls_urlDataList_threatData_threatType		
urls_urlDataList_threatData_firstSeen		
urls_urlDataList_threatData_lastSeen		
urls_urlDataList_finalUrl		
urls_urlDataList_landingUrl_url		
urls_urlDataList_landingUrl_scanId		
urls_urlDataList_landingUrl_threatData_verdict		
urls_urlDataList_landingUrl_threatData_threatStatus		
urls_urlDataList_landingUrl_threatData_threatName		
urls_urlDataList_landingUrl_threatData_threatType		
urls_urlDataList_landingUrl_threatData_firstSeen		
urls_urlDataList_landingUrl_threatData_lastSeen		
urls_normalizeData_normalizeStatus		
urls_normalizeData_normalizeMessage		

4.4 | SLASHNEXT : URL SCAN

URL Scan

Performs a real-time URL 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 action 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 "SlashNext Scan Report" anytime after 60 seconds using the returned Scan ID.

4.4.1 | INPUT

PARAMETER	REQUIRED	DESCRIPTION
url	True	The URL that needs to be scanned.
extended_info	False	Whether to download forensics data, such as Screenshot, HTML, and rendered text. If "true", forensics data will be returned. If "false" (or empty) forensics data will not be returned.

General	Configuration Ou	put Parameters Outputs Triggers							
SlashNe	SlashNext URL Scan Configuration								
	Option: url Required	urf Required	Type:	Record × *					
		Example:	Field:	URL × *					
				During and					
	Option:	extended_into Description: Whether to download forensics data, such as screenshot, HTML, and rendered text. If\"true\", foramice data will be anterand. If "felded" for another formatice data will not be assumed. Default in "felded"	Type: Field:	Extended info					
		антераси или и или селециянски л. (. накот, тре спраду литерализиони или пос се лечиллесь резионала (. накот, . Example:							
L									

4.4.2 | OUTPUT

34 Output Parameters Defined Performs a real-time URL 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 action 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 "slashnext-scan-report" action anytime after 60 seconds using the returned Scan ID.					
Parameter	Name Description				
url_errorNo					
url_errorMsg					
url_urlData_url					
url_urlData_scanId					
url_urlData_threatData_verdict					
url_urlData_threatData_threatStatus					
url_urlData_threatData_threatName					
url_urlData_threatData_threatType					
url_urlData_threatData_firstSeen					
url_urlData_threatData_lastSeen					
url_urlData_landingUrl_url					
url_urlData_landingUrl_scanId					
url_urlData_landingUrl_threatData_verdict					
url_urlData_landingUrl_threatData_threatStatus					
url_urlData_landingUrl_threatData_threatType					
url_urlData_landingUrl_threatData_threatName					
url_urlData_landingUrl_threatData_firstSeen					
url_urlData_landingUrl_threatData_lastSeen					
screenshot_errorNo					
screenshot_errorMsg					
screenshot_scData_scName					
screenshot_scData_scContentType					
screenshot_scData_scBase64					
html_errorNo					
html_errorMsg					
html_htmlData_htmlName					
html_htmlData_htmlContentType					
html_htmlData_htmlBase64					
text_errorNo					
text_errorMsg					
text_textData_textName					
text_textData_textBase64					
url_normalizeData_normalizeStatus					
url_normalizeData_normalizeMessage					

4.5 | SLASHNEXT : URL SCAN SYNC

URL Scan Sync

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 action will submit a URL scan request and wait for the scan to finish. The scan may take up to 60 seconds to finish.

4.5.1 | INPUT

PARAMETER	REQUIRED	DESCRIPTION
url	True	The URL that needs to be scanned.
extended_info	False	Whether to download forensics data, such as Screenshot, HTML, and rendered text. If "true", forensics data will be returned. If "false" (or empty) forensics data will not be returned.
timeout	False	A timeout value in seconds. If the system is unable to complete a scan within the specified timeout, a timeout error will be returned. The default timeout value is 60 seconds.

SlashNext URL Scan Sync Configuration Option: uf leveled Description: the color Descr	General Configuration Output Parameters Outputs Triggets									
Option: uit leaded Description:: The URL to scon. Example: Type: Record * * Option: ctended_info Description:: Mether to download formisic data, such as screenshot, HTML, and reindered tast. If true, formisic data will be returned. If facts (or empty) formisic data, such as screenshot, HTML, and reindered tast. If true, freed: Type: Record * * Option: timeout: timeout: freeder Example: Example: * * Option: timeout: timeout: timeout: timeout: timeout: * * Option: timeout: timeout: timeout: timeout: * * * Option: timeout: timeout: timeout: timeout: timeout: * * Example: timeout: timeout: timeout: timeout: timeout: * * Field: timeout: timeout: timeout: timeout: timeout: * * Field: timeout: timeout: timeout: timeout: timeout: * * Example: timeout: timeout: timeout:	SlashNext URL Scan Sync G	SlashNext URL Scan Sync Configuration								
Option: extended_info Type: Record * * Description: Infaste for empty) forensics data will not be returned. If faste for empty) forensics data will not be returned. Deduit is faite. Field: Extended info * * Field: Extended info * * * * * Option: timeout timeout timeout * * Description: A inteaut value in is seconds: If the system is unable to complete a scon within the specified timeout. If no * * * timeout timeout value is specified, a default timeout value is 60 seconds. timeout a different timeout. If no * * Field: Tumeout * * * Description: A inveout value is specified, a default timeout value is 60 seconds. timeout a different timeout. If no * * Example: Tomout * * *	Option:	urt sevene Description: The URL to scan. Example:	Type: Field:	Record × ×						
Description: Whether to downised dransies data, such as screenshot, HTML, and rendered text. If true, forensics data will be returned. If fabe (or empty) forensics data will not be returned. Default is false. Field: Extended Info x x Example: Example: Record x v Option: timeout timeout stabel to complete a scon within the specified timeout value is 60 seconds. Type: Record x v Field: Tuneout timeout value is 50 seconds. the specified automout value is 60 seconds. to attrave to so and the stabel to complete a scon within the specified timeout. If no x v timeout timeout value is 50 seconds. Example: Tuneout x v	Option:	extended_info	Туре:	Record x v						
Option: timeout Type: Record x x Description: A fineout value in seconds. If the system is unable to complete a scon within the specified timeout, allowate error will be extanned. You can run the action again with a different timeout. If no timeout value is specified, a default timeout value is 60 seconds. Field: Timeout Timeout x x		Description: Whether to download forensics data, such as screenshot, HTML, and rendered text. If true, Iorensics data will be returned. If faibe (or empty) forensics data will not be returned. Default is faibe. Example:	Field:	Extended Info × v						
imeout, a imeout error will be teturned. You can run the action again with a different timeout. If no Field: Tmeout timeout value is so seconds. Example:	Option:	timeout Description: A timeout value in seconds: If the system is unable to complete a scan within the specified	Туре:	Record × v						
		timeout, a timeout error will be teturned. You can run the action again with a different timeout. If no timeout value is specified, a default timeout value is 60 seconds. Example:	Field:	Timeout × ×						

4.5.2 | OUTPUT

35 Output Parameters Defined Performs a real-time URL scan with SlashNext cloud-based SEER Explane in a blocking mode. If the specified URL already exists in the cloud databa	ise, scan result will be returned immediately. If not, this action will submit a URL scan request
and wait for the scan to finish. The scan may take up to 60 seconds to finish.	
Parameter	Nama Description
scan_sync_errorNo	
scan_sync_error#sg	
scan_sync_urlData_url	
scan_sync_arlData_scanId	
scan_sync_urlData_threatData_verdict	
scan_sync_urlData_threatData_threatStatus	
scan_sync_urlData_threatData_threatName	
scan_symc_urlData_threatData_threatType	
scan_sync_urlData_threatData_firstSeen	
scan_sync_urlData_threatData_lastSeen	
scan_sync_urlData_firalUrl	
scan sync urlData landingUrl url	
scan_sync_urlData_lardingUrl_scanId	
scan_sync_urlData_lardingUrl_tnreatData_verdict	
scan_sync_urlData_landingUrl_threatOata_threatStatus	
scan_sync_urlData_landingUrl_threatData_threatName	
scan_sync_urlData_landingUrl_threatData_threatType	
scan_sync_urlData_lardingUrl_threatData_firstSeen	
scan_symc_urlData_landingUrl_threatData_lastSeen	
screenshot_errorNo	
screenshot_errorMsg	
screenshol_scDala_scName	
screenshot_scData_scContentType	
screenshot_scData_scBase64	
html_errorNo	
html_errorMsg	
html_htmlData_htmlName	
html_htmlData_htmlContentType	
html_htmlDxta_htmlBase64	
text_errorNo	
text_errorMsg	
text_textData_textName	
text_textData_textBase64	
scan_sync_normalizeDeta_normalizeStatus	
scan_sync_normalizeData_normalizeMessage	

4.6 | SLASHNEXT : 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

4.6.1 | INPUT

PARAMETER	REQUIRED	DESCRIPTION
scanid	True	Scan ID of the scan for which to get the report. It can be retrieved from the "URL Scan" function or "URL Scan Sync" function.
extended_info	False	Whether to download forensics data, such as Screenshot, HTML, and rendered text. If "true", forensics data will be returned. If "false" (or empty) forensics data will not be returned.

Option:	scan_id_inquinted Description: Scan ID. Con be retrieved from the SlashNext URL Scan oction or the SlashNext URL Scan Sync action. Example:	Type: Field:	Record Scan ID	
Option:	extended_info Description: Whether to download forensics data, such as screenshot, HTML, and rendered text. If true, forensics data will be returned. If false, (or empty) forensics data will not be returned. Default is false. Example:	Type: Field:	Record Extended Info	

4.6.2 | OUTPUT

35 Output Parameters Defined 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 to check back later will be returned.			
Parameter	Name	Description	
scan_report_errorNo			
scan_report_errorMsg			
scan_report_urlData_url			
scan_report_urlData_scanId			
scan_report_urlData_threatData_verdict			
scan_report_urlData_threatData_threatStatus			
scan_report_urlData_threatData_threatName			
scan_report_urlData_threatData_threatType			
scan_report_urlData_threatData_firstSeen			
scan_report_urlData_threatData_lastSeen			
scan_report_urlData_landingUrl_url			
scan_report_urlData_landingUrl_scanId			
scan_report_urlData_landingUrl_threatData_verdict			
scan_report_urlData_landingUrl_threatData_threatStatus			
scan_report_urlData_landingUrl_threatData_threatType			
scan_report_urlData_landingUrl_threatData_threatName			
scan_report_urlData_landingUrl_threatData_firstSeen	Redirected URL First Seen		
scan_report_urlData_landingUrl_threatData_lastSeen			
scan_report_urlData_finalUrl			
scan_report_normalizeData_normalizeStatus			
scan_report_normalizeData_normalizeMessage			
screenshot_errorNo			
screenshot_errorMsg			
screenshot_scData_scName			
screenshot_scData_scContentType			
screenshot_scData_scBase64			
html_errorNo			
html_errorMsg			
html_htmlData_htmlName			
html_htmlData_htmlContentType			
html_htmlData_htmlBase64			
text_errorNo			
text_errorMsg			
text_textData_textName			

4.7 | SLASHNEXT : DOWNLOAD HTML

Download HTML

This action downloads a web page HTML against a previous URL scan request.

4.7.1 | INPUT

PARAMETER	REQUIRED	DESCRIPTION
scanid	True	The Scan ID is a unique ID assigned by SlashNext Cloud to each scanning request and can be retrieved using the "URL Scan" or the "URL Scan Sync" functions.



4.7.2 | OUTPUT

5 Output Parameters Defined This action downloads a web page HTML against a previous URL scan request.		
Parameter	Name	Description
html_errorNo		
html_errorMsg		
html_htmlData_htmlName		
html_htmlData_htmlContentType		
html_htmlData_htmlBase64		

4.8 | SLASHNEXT: DOWNLOAD SCREENSHOT

Download Screenshot

This action downloads a screenshot of a web page against a previous URL scan request.

4.8.1 | INPUT

PARAMETER	REQUIRED	DESCRIPTION
scanid	True	The Scan ID is a unique ID assigned by SlashNext Cloud to each scanning request and can be retrieved using the "URL Scan" or the "URL Scan Sync" functions.
resolution	False	Resolution of the web page screenshot. Default value is "high".



5.8.2 | OUTPUT

General Configuration Output Parameters Outputs Triggers		
5 Output Parameters Defined This action downloads a screenshot of a web page against a previous URL scan request.		
Parameter	Name	Description
screenshot_errorNo		
screenshot_errorMsg		
screenshot_scData_scName		
screenshot_scData_scContentType		
screenshot_scData_scBase64		

4.9 | SLASHNEXT : DOWNLOAD TEXT

Download Text

This action downloads the text of a web page against a previous URL scan request.

4.9.1 | INPUT

PARAMETER	REQUIRED	DESCRIPTION
scanid	True	The Scan ID is a unique ID assigned by SlashNext Cloud to each scanning request and can be retrieved using the "URL Scan" or the "URL Scan Sync" functions.

General	Configuration Ou	put Parameters Outputs Triggers			
SlashNext	t Download Text C Option:	onfiguration scan_id required	Туре:	Record	
			Field:	Scan ID	

4.9.2 | OUTPUT

General Configuration Output Parameters Outputs Triggers		
4 Output Parameters Defined This action downloads the text of a web page against a previous URL scan request.		
Parameter	Name	Description
text_errorNo		
text_errorMsg		
text_textData_textName		
text_textData_textBase64		

4.10 | SLASHNEXT : API QUOTA

API Quota

This action queries the SlashNext cloud database and retrieves the details of API quota.

4.10.1 | INPUT

This action has no inputs. Instead, it uses the API Key defined in the asset to get the API quota details.

4.10.2 | OUTPUT

Paiameter	Name	Description
api_quota_errorNo		
api_quols_errorMsg		
api_quota_quotaDetails_remainingQuota		
api_quota_quotaDetails_licensedQuota		
api_quota_quotaDetails_expiryDate		
api_quota_quotaDetails_isExpired		
api_quota_quotsDotails_pointsConsumptionRate_hostReputation		
api_quota_quotaDetails_pointsConsumptionRate_hcstUrls		
api_quota_quotaDetails_pointsConsumptionRate_urlReputation		
api_quota_quotaDetails_pointsConsumptionRate_uRLScan		
api_quots_quotsDetails_pointsConsumptionRate_uRLScanSync		
api_quota_quotaDetails_pointsConsumptionRate_downloadScreenshot		
api_quota_quotaDetails_pointsConsumptionRate_downloadText		
api_quota_quotaDetails_pointsConsumptionRate_downloadHTNL		
api_quota_quotaDetails_pointsConsumptionRate_customerApiQuota		
api_quota_quotaDetails_pointsConsumptionRate_urlScanWithScanId		
api_quota_quotaDetails_pointsConsumptionRate_urlScanSyncWithScanId		
api_quota_quotaDetails_consumedAPIDetail_hostReputation		
api_quota_quotaDetails_consumedAPIDetail_hostUrls		
api_quota_quotaDetails_consumedAPIDetail_urlReputation		
api_quota_quotaDetails_consumedAPIDetail_uRLScan		
api_quota_quotaDetails_consumedAPIDetail_uRLScanSync		
api_quota_quotaDetails_consumedAPIDetail_downloadScreenshot		
api quota quotaDetails consumedAPIDetail downloadText		
api quota quotaDetails consumedAPIDetail downleadHTML		
api quota quotaDetails consumedAPIDetail customerApiQuota	Consumed Api Customer Ani Ounta	
api quota quotaDetails consumedAPIDetail scanReportWithScanId		
ani nuota nuotaDetails consumedAPIDetail scanSyncBenortWithScanId	Consumed Ani Scan Sync Research Althe Scan 10	
api quota quotaDetalis consumedenintsGetali bostReputation	Consumed York's Host Reputation	
ani nuota nuotaDetails consumedPointsDetail bosturis		
api guota guotaDetalis consumedPointsDetali uriReguitation	Consumed Points Lid Resultations	
ani munta nuntaDetaile consumedDointeDetail uPIScan		
ani quota quotaDetalle consumedEninteEntali uEtConscue	Costuped Initia Ini Sea Car	
api_quota_quotaDetalla_consumedDeisteRetall_uktScanSync	Consumed Points Off Juli and Synth	
api_quota_quotaDetalle_consumedPointsDetall_dowhicad3creenshot		
api_quota_quotaUs_consume0PointSDetali_dowhicadText	consumed rounds provintibad lext	
api_quota_quotadetaiis_consumedPointSDeftaii_downloadHTML		
api_quota_quotaDetails_consumedPointSDetail_customerApiQuota		
api_quota_quotaDetails_consumedPointSUetail_scankeportwithScanid		
api_quota_quotaDetails_consumedPointsDetail_scanSyncPoportWithScanId		
api_quota_quotaDetails_note		

5 | PLAYBOOKS

SlashNext Phishing Incident Response also provides two playbooks that defines the business logic to automate URL and Host scanning for an incoming email in Abuse Inbox.

- First, set up and IMAP Email Asset as described in the official Swimlane documentation.
 - 1. Log in to Swimlane with your Chrome browser. From the global navigation menu, select Integrations.



Important! Contact your Swimlane support or sales representative if you do not have log in credentials for Swimlane.

- 2. Select the Assets tab and then, from the Integrations taskbar, select + New Asset.
- 3. On the New Asset, General tab, provide a name and description (optional) for your asset, and then select IMAP Email from the Asset Type pull-down field.

Swimlane Email	🗸 Save
General	
Name	
Swimlane Email	
Description	
Asset Type	
	٩
McAfee Data Exchange Layer Asset Version: 1.0.0	
Directory Server	
Active Directory	
Email Server	
IMAP Email	
POP3 Email	
SMTP Email	

4. Click the **Details** tab and fill out the required **Host** and **Port** fields. In addition, complete the **User** and **Password** fields and ensure that the **Use SSL** field is enabled.

Swimlane Email	✓ Save
General Details	
Host Required	
imap.gmail.com	
Port Required	
993	
Use SSL	
User	
swimlanetest@gmail.com	
Password	
Test Connection	

Note: The User and Password you use here need to be real assets that you have access to!

5. Next, click **Test Connection**.

Swimlane Email	🗸 Save
General Details	
Host Required	
imap.gmail.com	
Port Required	
993	
Use SSL	
User	
swimlanetest@gmail.com	
Password	
Test Connection	

6. Once you receive a message that the connection test has succeeded, click Ok, and then click Save to save your new asset.



You can now see your asset listed under the Assets tab.



• After creating an Email Asset, go on to create a related Email task which uses the Asset created in the first step by following the official Swimlane documentation here.

The details for both playbooks are mentioned below:

5.1 | PLAYBOOK - SLASHNEXT HOST REPUTATION

This section demonstrates the complete business logic to scan Hosts (IPv4/Domain) from an incoming email in Swimlane platform via SlashNext Phishing Incident Response playbook application.

A new Swimlane record is created for each of the host present in the email body.

SE-1155	🔒 Delete 🚦
Scanned Host: estelasplantrental.com	
Host Verdict: Malicious	
Host Threat Status: No Longer Active	Host Threat Name: Fake Login Page
Host Threat Type: Phishing & Social Engineering	Host First Seen: 03-10-2020 12:38:56 UTC
Host Last Seen: 03-20-2020 22:14:52 UTC	
Latest URL: http://estelasplantrental.com/amexx/login	
Latest URL Scan ID: 1d5e0b40-0cbe-40d2-9cc4-9ad973e9b67f	Latest URL Verdict: Malicious
Latest URL Threat Status: No Longer Active	Latest URL Threat Name: Fake Login Page
Latest URL Threat Type: Phishing & Social Engineering	Latest URL First Seen: 03-16-2020 12:38:45 UTC
Latest URL Last Seen: 03-19-2020 23:51:24 UTC	Latest URL Normalized Status: 0
Latest URL Normalized Message:	
Host Screenshot: Name	
658195936CAC 6228201F10C62462060F1FD5D9B1759E158294B00B3044595C5F	
Host Html File:	
Name	
A34F3CC26CD9F644981749272DDA95649F52FBC389AC321223F371AE88495517	
Host Text File:	
Name	
16A5DE2FD7212587DDFD804F4E90DE50B15E81BC3069A4B46D16F7F439975C72	

5.2.1 | OUTPUT

5.2 | PLAYBOOK - SLASHNEXT URL SCAN

This section demonstrates the complete business logic to scan URLs from an incoming email in Swimlane platform via Slash-Next Phishing Incident Response playbook application.

A new Swimlane record is created for each of the URLs found in the email body.

CAN RESULTS SECTION		
Scanned URL:	Scanned URL Scan ID: and 2000 0.001 and 14 (5072-601 8and 2010)	
incps.//poin-group-crooces.ooowebioscapp.com	66073031-3976;474(-00);4-1319647979)	
Scanned URL Verdict: Malirious	Scanned URL Threat Status:	
Scanned URL Threat Name: Fake Login Page	Scanned URL Threat Type: Phishing & Social Engineering	
03-09-2020 08:30:12 UTC	Scamed OKL Last Seen: 03-09-2020 09:17:58 UTC	
Redirected URL:		
Screenshot:		
Name		
0C238AD6C22BF887012D9F59052D5E03CFBE841C5EA13C1888C18E3FF65993BD		
Html File:		
Name		
Text File:		
Name		
44E97A49F6D8755CD7035EE7527F84A42986D9E7D8E272B4ACE385025FA1E733		