infoblox.

DEPLOYMENT GUIDE

Infoblox TIDE & MISP Integration

Table of Contents

Introduction	2
Requirements	2
Tested Hardware & Software	2
Deployment Summary	2
Deployment Instructions	3
CSP API Key Retrieval	3
TIDE Feed Filters	5
Limitations	7
MISP Configuration	8
MISP Events & Attributes with TIDE	11
Additional Resources	14

Introduction

This deployment guide demonstrates how to incorporate TIDE feeds into a MISP instance.

Infoblox Threat Intelligence Data Exchange (TIDE) leverages highly accurate machine-readable threat intelligence (MRTI) data to aggregate and selectively distribute data across a broad range of security infrastructure. The threat intelligence team curates, normalizes, and refines the high-quality threat data to minimize false positives. Our threat feeds begin with information gained from native investigations and harvesting techniques. We then combine them with verified and observed data from trusted partners including government agencies, academics, several premier Internet infrastructure providers, and law enforcement. The result is a highly refined feed with a low historical false-positive rate.

The MISP threat sharing platform is a free and open-source software for gathering, sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or counter-terrorism information.

Requirements

The following items are required to incorporate the Infoblox TIDE feeds into MISP:

- Access to an Infoblox BloxOne Threat Defense Advanced subscription
- Access to a MISP instance

Tested Hardware & Software

• MISP version 2.4.130 installed on an Ubuntu 18.04 Virtual Machine

Deployment Summary

- 1. Retrieve your BloxOne Threat Defense Advanced API key from the Cloud Services Portal.
- 2. Observe TIDE filters offered by Infoblox and retrieve API call.
- 3. Configure MISP to connect to the Infoblox Cloud Services Portal and download TIDE feeds.
- 4. Demonstrate functionality of MISP with TIDE.

Deployment Instructions

CSP API Key Retrieval

You will need a BloxOne Threat Defense Advanced API key to pull the TIDE feeds via the REST API in MISP. You can access this key through the Cloud Services Portal (CSP). API keys are unique identifiers found in many applications to both identify the application making the API calls and verify the application making the calls has access to do so.

To access your API key:

- 1. Log into the CSP at <u>https://csp.infoblox.com</u>.
- 2. Upon logging in, hover over your username in the bottom-left corner and select User Profile.



3. Navigate to the User API Keys tab. Click **Create** to create a new API Key.



4. In the Create User API Key dialog box, input a **Name** and an **expiration date** for the API Key.

ib	Create Use	er API Key	a
.7 [.]	*Name Expires at	Example-Key 01/09/23 07:57 am	
	Cancel	S	ave & Close

- 5. Click Save & Close to confirm the creation of the API Key.
- 6. A dialog box containing the new API Key will be shown. Click **Copy** to copy your API key to your clipboard. Paste it somewhere you can easily access and then copy from later, such as Notepad.

	API Access Key Generated Please copy this API Key as this is the only time you are able to view it.	
	4	c1
Close		Сору

TIDE Feed Filters

Infoblox TIDE provides many filters to choose from depending on your needs. This section of the demo shows you an overview of the filters and how to retrieve the appropriate API call to grab these feeds in MISP based on the desired filters.

1. In the left side menu of the CSP, navigate to Research \rightarrow Active Indicators.

infoblox. 🧷											
🕐 Dashboard											
🖽 Manage	Dashboards Security	•									
\Xi Policies											
🔟 Reports	Dellus Summers	×									
Research											
答 Administration	Active Indicators	DNS FIREWALL ACTIVITY									
	Resources Threat Lab	O O O Total Events 0% High 0% Medium 0% Low									
		🔝 THREAT ACTIVITY									
	0	0									
	Devices with Threat Activity	Unique Threat Indicators									
	STATES CONTRACTIVITY	DATA EXFILTRATION INCIDENTS									
	0	0									
	BloxOne Endpoints with Threat Activity	Total Incidents									
	CTION TAKEN	HIGH SEVERITY EVENTS NOT BLOCKED									
	0 0	0									
	Total Blocked Allowed/Logged	High Threats not Blocked									

- 2. Here you can see all active threat indicators based on Infoblox TIDE research. There are millions of indicators, so let's focus on incorporating only Host data types in the Phishing threat class.
 - a. Under DATA TYPE, click Clear to deselect each checkbox.
 - b. Select Host.

Data Type	
Select all	Clear
Email	(4)
🗌 Hash	(8,294)
🗹 Host	(19,574,291)
IP	(143,124)
URL	(240,667)

- c. Under THREAT CLASS/PROPERTY, click Clear to deselect each checkbox.
- d. Click Show more.
- e. Select Phishing.

	Threat Class/Property		
		Select all	Clear
		APT	(8,213)
		■ ▶ Bot	(5)
		CompromisedDomai	n (2)
		CompromisedHost	(9)
		Cryptocurrency	(1,988)
		DNSTunnel	(6)
Threat Class (Property		ExploitKit	(1,070)
Threat Class/Property		ICS	(1)
Select all	Clear	IllegalContent	(11)
APT	(8.213)	InternetInfrastructur	e(57,150)
	(-,)	MaliciousNameserve	r (64)
▶ Bot	(5)	MalwareC2	(10,972)
CompromisedDomair	n (2)	■ MalwareC2DGA (8	,794,616)
	$\langle 0 \rangle$	MalwareDownload	(444,900)
	(9)	Parked	(2,466)
Cryptocurrency	(1,988)	Phishing	(807,900)
+ Show more		Policy (2	,603,870)
		Proxy	(5,059)

f. Click **Apply Filter** at the top. Now you will only see Host data types of the Phishing class listed.

infoblox. 🗘				
 Dashboard Manage Policies 	Filter	Apply Filter	Export Genera	ate API Request
Reports Research	Data Type		INDICATOR	DATA TYPE
Dossier	Select all	Clear	config-panel.frge.io	HOST
 Active Indicators 	Email	(4)		

3. Click **Generate API Request** to view the API request you will need to copy into MISP to grab this data. The necessary request is highlighted in blue below. Copy and paste it somewhere you can easily copy from later, such as Notepad. Click **OK** to close the popup.



Limitations

There are several limitations to note when importing feeds into MISP.

- Importing millions of records from TIDE into MISP can take a very long time, potentially hours or even days on low end systems. It is highly recommended to use <u>filters</u> in your API calls, such as an *rlimit=100000* to reduce import time.
- 2. Importing multiple datatypes in the same feed can cause problems, including 400 errors returned by MISP. It is highly recommended to import one datatype (host, url, ip, hash or email) at a time within the same feed. If you want to use multiple datatypes, you can create multiple feeds in MISP that return each datatype, or use the *fields=* parameter in the TIDE call to return only one domain field from each datatype. This is due to the TIDE API returning different fields between datatypes. For example, hashes and ips do not have a 'domain' field like URLs, emails and hosts do; or that URLs contain an extra 'url' field for which the other types do not.
- 3. MISP has an easier time importing CSV over JSON. When using CSV, MISP parses the actual domains/hosts better without the extra characters returned by JSON. To return CSV, use the *data_format=csv* parameter in the TIDE call.

MISP Configuration

This section shows how to connect MISP to the Infoblox TIDE feeds.

1. Navigate to Sync Actions \rightarrow List Feeds.



2. Click Add Feed in the left menu.



3. Input the **parameters** for the new feed.

List Feeds	Add MISP Feed
Search Feed Caches	
Import Feeds from JSON Feed overlap analysis matrix Export Feed settings	Add a new MISP feed source. Enabled Caching enabled Lookup visible Name
	B1TD-Phishing
	Provider
	Infoblox
	Input Source
	Network 🗸
	URL
	lox.com/tide/api/data/threats?type=host&class=phishing.=30d
	Source Format
	Freetext Parsed Feed
	Any headers to be passed with requests (for example: Authorization)
	Authonzation: Token <yuur apt="" here="" key=""></yuur>
	Add Basic Auth
	Creator organisation
	ORGNAME 🗸
	Target Event
	Fixed Event
	Target Event ID
	Leave blank unless you want to reuse an existing event.
	Exclusion Regex
	Regex pattern, for example: "//https://myfeedurl/i
	Auto Publish Override IDS Flag Delta Merge
	Distribution
	All communities 🗸
	Default Tag
	None 🗸
	Filter rules: Modify Add

4. Click Add when done.

Check Enabled and Caching enabled.

Name: Enter a recognizable name.

Provider: Enter a recognizable provider.

Input Source: Select Network as we are accessing our source (the TIDE feeds) non-locally.

URL: URL of the TIDE feeds desired. You copied this URL from the CSP in the <u>TIDE Feed Filters</u> section in step 3. Copy that URL here, or as a reminder, input:

https://csp.infoblox.com/tide/api/da
ta/threats?type=host&class=phishing&
period=30d

Note the appended **&period=30d** at the end. This limits the dataset to the last 30 days, but you can omit it if you want to use all data from all time. You can also append **&rlimit=100** if you wish to limit the dataset to the first 100 entries, for example. Setting a limit will significantly shorten the time MISP will need to fetch this feed later.

Source Format: Select Freetext Parsed Feed.

Headers: This is where your API key is input. Enter "Authorization: Token <YOUR API KEY>" into the textarea. Do not include the <> symbols or quotes.

Creator Organization: Select a recognizable organization. You can add new organizations to MISP later.

- 5. If the feed is not already, enable it.
 - a. Click the **checkbox** on the left of the newly created feed.
 - b. Select Enable selected.
 - c. Select Enable caching for selected if you desire caching.

Home E	vent Actions	Galaxies	Input Filters	Global Actio	ns Sync A	ctions A	dministration	Audit			
Feed added.											
List Feeds Search Feed Car Add Feed Import Feeds froi Feed overlap an Export Feed setti	ches m JSON alysis matrix ings	Feec Generate Load def « previc	S feed lookup ca auit feed meta bus next »	data Cache	i data (enabled all feeds Cact	feeds only) ie freetext/CS	SV feeds Ca	caching fo	eeds Fetch and store all feed data	All foods E	nabled foods
		ld	Enabled (Caching Name	Format	Provider	Org	Source	URL	Headers	Target
		□ 1	×	 CIRCL OSINT Feed 	misp	CIRCL		network	https://www.circl.lu/doc/misp/feed-osint		Feed not enabled
		2	×	✔ The Botvrij. Data	misp eu	Botvrij.eu		network	https://www.botvrij.eu/data/feed-osint		Feed not enabled
		6	× ·	 B1TD- Phishir 	freetext	Infoblox	ORGNAME	network	https://csp.infoblox.com/fide/api/data/threats? type=host&class=phishing.=30d	Authorization: Token xxx	Fixed event 1201
		Page 1 of	1, showing 3 r	ecords out of 3 to	al, starting on	ecord 1, end	ling on 3				

- 6. Fetch the feed.
 - a. On the right end of the feed row, click the ${}^{m V}$ icon to fetch all feed events.

Caching	Actions
Not cached 🎞	Q 🕑 14
Not cached 🃟	Q 🗹 🖬 🕰
Not cached 🋲	001 10

- 7. Verify the feed fetch was executed.
 - a. In the top bar, navigate to Administration \rightarrow Jobs. Verify the fetch Completed.

Jobs]
Purge j	Purge job entries:																											
Complete	d All																											
« previo	us 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	next »						
All	Default	Email	Ca	che																								
ld î	Date o	reated		Da	te mo	dified	ł	Pr	ocess	i ID				v	Vorker	Job	type		Inpu	t	Messa	ge Org	anisation	Status	Retries	s Progress		-
1216	2020-	09-22 16	8:01:19	20	20-09-	-22 16	6:21:42	2 07	'dee36	34e238	17f9cd	384f37	5a57bb9	9 d	efault	fetcl	n_feeds		Feed	1:6	Job	SYS	STEM	Completed	0	00	ompleted	╏
																					done.							T

MISP Events & Attributes with TIDE

Here is where we will add a new MISP event and attribute to demonstrate they are being checked against our new TIDE feed.

- 1. Navigate to Home.
- 2. Add a new **Event**.
 - a. Click Add Event in the left menu.

	Home	Event Actions	Galaxies	Input Fi	lters	GI	obal A	ctions	;	Sync A	ctions	\$	Adminis	stration	Aı	udit	
\langle	List Events Add Event	>	Even	ts													
	Import from… REST client		« previou	us 1	2	3	4	5	6	7	8	9	10	11	12	13	14

- b. Give the event **recognizable Event Info**. This could be a name, description, or anything otherwise distinguishable.
- c. Click **Submit** when finished.

List Events	Add Event		
Add E∨ent			
Import from			
REST client	Date	Distribution 😈	
	2020-09-14	This community only	/ ~
List Attributes	Threat Level 🕕	Analysis 🕕	
Search Attributes	High	∽ Initial	~
View Proposals	Event Info		
Events with proposals	This is a recognizal	ble description	
View delegation requests	Extends Event		
Export	Event UUID or ID. L	eave blank if not applicable.	
Automation			

- 3. MISP will automatically open the new event for you. MISP events are populated with attributes, such as domain names, IPs, indicators, etc. **Add** a new attribute to the event.
 - a. Scroll down and **click** the Plus button to add a new attribute. A popup will appear.

This is a recognizable description Event D 1202 UUD 9999412-449-432-4886-37/79956900 • Corector org 0604046 Corector org 0604046 Enail admin@admin.test Tops Corector org Date 2020-09-22 Triced Lovel High Analysis Initial Distribution This community only This community only • • • • Pathale 00 00 ec0 First recorded change Last change 0202-09-22 182207 Modification map Sightings 00 on - restricted to own organisation only. * Corection organisation only. *	This is a recognizable description Event D 1002 UD 99998412-449-432/sead-3279999698 € Creator org ORGANAE Ovener org ORGANAE Ovener org ORGANAE Tags Comedication (Sediminised) Tags Comedication (Sediminised) Tags Comedication (Sediminised) Date 2020-0-22 Threat Level High Analysis Initial Distitution This is a recognizable description Validadid No Mathed No Mathed No Mathed Comediation only I Extender conneg 2020-09-22 18:22.07 Mathed No Mathed No Mathed Comediation only I Extender conneg Comediation only I Extender conneg <th>This is a recognizable description Serve 0 1202 Uito 0999412-464-42-6660.000 0000000 00000000 00000000 00000000 000000000 000000000 000000000000000000000000000000000000</th> <th></th> <th></th> <th></th>	This is a recognizable description Serve 0 1202 Uito 0999412-464-42-6660.000 0000000 00000000 00000000 00000000 000000000 000000000 000000000000000000000000000000000000			
Finite is a recognize description Event ID 1202 UUID 9999412+489-4828-4884-36772995680 • Creator org OR ON AME Owner org OR ON AME Email admin@admin.test Tags Control Date 2020-09-22 Threat Level High Analysis Initial Distribution This community only Published No Wattributes 0.0 object0 First recorded change 2020-09-22 18-2207 Modification map Image: Control of the Controlation graph Sightings 0.0 object0 First recorded to own organisation only Image: Controlation graph	Times is a recognized bescription Event io 1202 Uulo 99998412-4429-4429-4429-4425-6490-3072995660 • Creator org ORONAME Owner org ORONAME Tags Image	Intersection Event 0 1202 Uso 99984124640-4226480-3272995600 Creator org ORONAME Owner org ORONAME Date 2020-06-22 Traces Owner org Date 2020-06-22 Traces High Acadysis Imal Detribution This is a recognizable description Print recorded change 0.0 Object Print recorded change 2020-02-21 (Size on the stription) Spiritive 0.0 Object Print recorded change 2020-02-21 (Size on the stription) Last change 2020-02-21 (Size on the stription) Spiritives 0.0 Object Print recorded change 2020-02-21 (Size on the stription) Last change 2020-02-21 (Size on the stription) Spiritives 0.0 Object Print recorded change 2020-02-21 (Size on the stription) Last change 2020-02-21 (Size on the stription) Spiritives 0.0 Object Print recorded change Correlation on printsation on to formation	This is a re	additable description	
Event t0 1202 UUD 9993412-e4e6-4a2Kaead-3772995660 € Creator org ORONAME Dwiner org ORONAME Tags Contract of the state of the	Event ID 1202 UUID 9999812-2e489-422.sead-3:772995680 € Creator org ORONAME Owner org ORONAME Tags Control of C	Event 0 99994412-9469-4925-8ee9-3:7729956600 1 Creater org ORGMANE Owner org ORGMANE Email admin@admin.test Tags Org Date 020-09-22 Thread Level High Analysis Initial Distribution This community only Pathtindets 0 (0 0bjec) First change 2020-09-22 1 Thread Level High Analysis Initial Distribution This is a recognizable description Pathtindets 0 (0 0bjec) First change 2020-09-22 16 22 07 Modification map	This is a re	sognizable description	
UUD 9999412:449:449:449:449:469:660 € Creator org ORCNAME Owner org ORCNAME Tags ORCNAME Tags Common of the state sta	UUb 9999412+4494-432+4ead-3:7729956690 Creator org OR0-NME Owner org OR0-NME Email admin@admin.test Tags Image: Imag	ULD 999994124494942745849357729956809 Creator org 0F601A442 Enail admin@gdmin.test Taps 0 2020-09-22 Threat Level High Analysis Initial Detitination This community only 0 4 1 Info This is a recognizable description Published No 00 elect First recorded change Lest change 2020-09-22 16 22:07 Modification map Sightings 0 0 0) - restricted to own organisation only 0 - Puolos = 0 diary # Elect graph # Elect graph # ATT2CK/matter = Abitudes = Discussion First new all in 202 These Construction of the construction of the constructio	Event ID	1202	
Creator org ORGNAME Owner org ORGNAME Email admingadmin last Tags Colored administ Threat Level High Analysis Initial Distribution This community only This is a recognizable description This is a recognizable description Phdistohd No Adtributes 0 (0 Object) First recorded change 2020-09-22 16 :22:07 Modification map	Creator org ORGRAME Owner org ORGRAME Email admin@admin.test Tags Comparison Date 2020-09-22 Threat Level High Anabysis Initial Distribution This community only Paulistated No RAttributes 0 (0 Object) First recorded change 2020-09-22 18-22.07 Modification map	Creator org ORONAUE Orener org ORONAUE Email adminigadminitest Tags Olive 2020-09-22 Threat Level High Analysis Indial Detribution This community only O C Info This is a recognizable description Published No RATE that is a recognizable description Published 00 Objecto First recorded change List change Sightings 0 (0) Objecto 1210-2207 Modification map Sightings 0 (0) - restricted to own organisation only A - Priors = Galaxy + Event timestine + Correlation graph + ATT&OK madix = Attributes = Objecussion * 1202 The E Calaxy is Stope bagie O Letters 12 Decky Store A SightingDB O Content * Related Tags * Filtering fool Crig Category Type Value Tags Gatacies & Comment Correlate Attributes warring: This own utilitable. It's streegy labeled the event with attributes warks descrubing to prevale a maximplic description Attributes warring: This own utilitable. It's streegy labeled the event with attributes werks estermation to prevale a maximplic description Attributes warring: This own utilitable. It's streegy labeled the event with attributes werks estermation top prevale a maximplic description Attributes warring: This own utilitable. It's streegy labeled the event with attributes werks estermation top prevale a maximplic description Attributes warring: This own utilitable. It's streegy labeled the event with attributes werks estermation top prevale a maximplic description Attributes warring: This own utilitable. It's streegy labeled the event with attributes (weice streegy labeled to event with attributes of the event with attributes werks estermation top prevale a maximplic description Attributes and the avent of the event with attributes (weice streegy labeled to event with attributes (weice streegy labeled	UUID	9999a412-e4e9-4a2Faead-3c7f2995e690 +	
Owner orig OPENAME Final admin@admin.test Tags Image: Imag	Owner org ORGNAUE Email admin@admin.test Tags Simple Date 2020-09-22 Threat Level High Anabysis Initial Distribution This community only Distribution This is a recognizable description Published No First recorded change 2020-09-22 16-22 07 Modification map	Overed or g Or Created Email admin@admin.test Tags Image Date 2020-09-22 Tread Lovel High Analysis Indial Distribution This community only Info This is a recognizable description Paldiabled No Paldiabled Paldiabled Paldiabled Paldiabled Paldiabled Paldiabled Paldiabled Paldiabled Paldiabled Paldiabled <t< td=""><td>Creator org</td><td>ORGNAME</td><td></td></t<>	Creator org	ORGNAME	
Email admingdommites Tags Image adminites Tags Image adminites Date ed. 2020-09-22 Image adminites Tardet Level High Analysis Initial Distribution This community only Image adminities Image adminities Photoshold No #Attributes 0 (0 Object) First recorded change 2020-09-22 18-22.07 Modification map Image adminities Sightings 0 (0) - restricted to own organisation only. Provisiting = Galaxy Executing adminities Image = Correlation graph #Attributes Image = Correlation graph #Attr	Final administration Tigs Image: administration Date 2020-09-22 Threat Level High Analysis Initial Distribution This community only Tife at level No Mathematication Image: administration Published No Attributes 0 (0 Object) First recorded change Last change Last change 2020-09-22 18-22 07 Modification map	Email adminingatominist Tags Imail Date 2020-09-22 Threat Level High Analysis Initial Distribution This community only If it is a recontractible description Padashand 80 Antifuence 0.00 Objecto First recorded change Lest change 2020-09-22 to 22:07 Modification map Sightings 0.00 - restricted to own organisation only / Pate 1:002: This is	Owner org	ORGNAME	
Tage Call and set Date 2020-09-22 Thread Level High Analysis Initial Distribution This community only Thread Level No #Attributes 0 (0 Object) First recorded change 2020-09-22 16-22 07 Modification map	rags View sil Date 2020-09-22 Threat Level High Analysis Initial Distribution This community only Threat Level N #Attributes 0 (0 Object) First recorded change Its community only Last change 2020-09-22 16 22 07 Modification map	Target 2020-09-22 Thread Level High Analysis initial Definituation This community only This community only Image: Community only Image: Community only Image: Community only Perification This is a recognizable description Published No Rathrows 0 (00 Object) First recorded change Last change Last change 2020-09-22 18:22:07 Modification map Image: Community only Sightings 0 (0) - restricted to own organisation only First recorded change Image: Community only Last change 2020-09-22 18:22:07 Modification map Image: Community only Sightings 0 (0) - restricted to own organisation only First recorded change Image: Community only Last change Image: Community only Sightings 0 (0) - restricted to own organisation graph First recorded change Image: Community only Image: Community only Image: Community only Image: Community only Image: Community only Image: Communit Stephe	Tarra	admin@admin.test	
Date 2020-09-22 Threat Level High Analysis Initial Distribution This community only Info This is a recognizable description Published No #Attributes 0 (0 object) First recorded change 2020-09-22 16-22 07 Modification map	Date 2020-09-22 Threat Level High Analysis Initial Distribution This community only Threat Level This is a recognizable description Published N #Attributes 0 (0 Object) First recorded change Last change 2020-09-22 16 22 07 Modification map Sightings 0 (0) - restricted to own organisation only First recorded change Last change 2020-09-22 16 22 07 Modification map Sightings 0 (0) - restricted to own organisation only Sightings 0 (0) - restricted to own organisation only Sightings 0 (0) - restricted to own organisation only Findex Contraction graph Findex Contraction graph Calaxies Contraction graph Calaxies Contraction graph Calaxies Contraction graph	Date 2020-09-22 Thread Level High Analysis Initial Distribution This community only Info This is a recognizable description Padashad No #Attributes 0 (0 Object) First recorded change	- Tays		
Interactions night Analysis Initial Distribution This community only This is a recognizable description Published No #Attributes 0 (0 Opiect) First recorded change Last change 2020-09-22 16 22:07 Modification map Sightings 0 (0) - restricted to own organisation only ♪ = Rivet = -Cataxy + Event graph + ATT&CK matrix = -Attributes = -Discussion ¥ 1202-This L	Interact Looke Fig.1 Analysis Intitial Distribution This community only This is a recognizable description Published No #Attributes 0 (0 Object) First recorded change Last change 2020-09-22 18 22:07 Modification map Sightings 0 (0) - restricted to own organisation only. Pixet second seco	In teal Looke Puglin Analysis Indial Distribution This community only ● < Info This is a recognizable description Published No PAttributes 0 (0 Object) First recorded change Lest change 2020-09-22 16-22.07 Modification map Sightings 0 (0) - restricted to own organisation only / Sightings 0 (0) - restricted to own organisati	Date Threat Level	2020-09-22	
Autors unital Distribution This community only • <	Autops minor Distribution This community only • Info This is a recognizable description Published No #Attributes 0 (0 Object) First recorded change 2020-09-22 16 22 07 Modification map	Autopics minutes Distribution This community only Info This is a recognizable description Published No #Attributes 0 (0) Objecto First recorded change Last change 2020-09-22 16 22:07 Modification map Sightings 0 (0) - restricted to own organisation only - Photos — Galaxy + Event graph + Event timeline + Correlation graph + ATT&CK matrix - Attributes - Discussion X 1202 This Calaxy + Event graph + Event timeline + Correlation graph + ATT&CK matrix - Attributes - Discussion X 1202 This Calaxy is view all Calaxy is scope toggle • Detected to Decay score * SightingDB • Context * Related Tags * Filtering tool Org Category Type Value Tags Galaxies of information) to provide a meaningful event Attributes varings This event doesn't contain any attribute. R's strongly solvised to populate the event with attributes (indicators, observables or information) to provide a meaningful event	Anabacia		
This community only If is Info This is a recognizable description Published No #Attributes 0 (0 object) First recorded change Last change Last change 2020-09-22 16:22:07 Modification map	This community only Info This is a recognizable description Published No #Attributes 0 (0 Object) First recorded change Last change Last change Sightings 0 (0) - restricted to own organisation only First recorded to own organisation only * Revisition of the state o	This community only	Distribution	11NVM	
Info This is a recognizable description Published No #Attributes 0 (0 Object) First recorded change Last change Last change 0 (00-restricted to own organisation only /* Sightings 0 (0) - restricted to own organisation only /* Pixt 1202_This L	Info This is a recognizable description Published No PAttributes 0 (0 Object) First recorded change Last change Last change 2020-09-22 16 22:07 Modification map Image: Comparison only image: Comparison	Info This is a recognizable description Public No Statubutes 0 (0) Object) First recorded change Last change Last change 2020-09-221 6:22:07 Modification map		This community only	
Published No PAttributes 0 (0 Object) First recorded change 2020-09-22 16:22:07 Modification map	Polisikad No FAxt induces 0 (0 Object) First recorded change 2020-09-2216:22:07 Modification map - Sightings 0 (0) - restricted to own organisation only /* - Pixots - Galaxy + Event timeline * 1202: This L	Published No PAttributes 0 (0 Object) First recorded change	Info	This is a recognizable description	
PAtributes 0 (0 Object) First recorded change 2020-92-215/22.07 Last change 2020-92-215/22.07 Modification map	PAtributes 0 (0 Object) First recorded change 2020-09-22 16:22:07 Modification map	#Attributes 0 (0 Object) First recorded change 2020-09-22 18:22:07 Modification map	Published	No	
First recorded change 2020-09-2218/22.07 Modification map	First recorded change 2020-09-22 16:22:07 Modification map	First recorded change Last change 2020-09-22 16 22:07 Modification map Sightings 0.(0) - restricted to own organisation only Phots - Galaxy + Event graph + Event graph + ATTRCK matrix - Attributes - Discussion Instal Galaxies Instal + previous next> Y New all - previous - previous	#Attributes	0 (0 Object)	
Last change 2020-09-2218:22:07 Modification map	Last change 2020-09-22162207 Modification map	Lest change 2020-09-22 16:22.07 Modification map Sightings 0 (0) - restricted to own organisation only A PRVots - Galaxy + Event graph + Event timeline + Correlation graph + ATTSCK matrix - Attributes - Discussion x 1202: This L. Galaxies Calaxies Calaxies Calaxies Correlate New all Correlate Correlate Attribute warning: This event doesn't contain any stribute. It's strongly advised to populate the event with attributes (indicators, observables or information) to provide a meaningful event	First recorded change		
Modification map Sightings 0 (0) - restricted to own organisation only. - Phots - Galaxy + Event graph + Event timeline + Correlation graph + ATT&CK matrix - Attributes - Discussion (* 1202 This L Galaxies (* 2 * * *	Modification map Sightings 0 (0) - restricted to own organisation only. - Prvots - Galaxy * 1202 This L Calaxies C+ previous next = View all	Modification map Sightings 0 (0) - restricted to own organisation only.	Last change	2020-09-22 18:22:07	
Sightings 0 (0) - restricted to own organisation only / - Pixots - Galaxy + Event graph + Event graph + Correlation graph + ATT&CK matrix - Attributes - Discussion X 1202 This L Galaxies	Sightings 0 (0) - restricted to own organisation only. ► - Pixots - Galaxy + Event graph + Event timeline + ATT&CK matrix - Attributes - Discussion Image: Signiful and Sign	Sightings 0 (0) - restricted to own organisation only. A - Pwots - Galaxy + Event graph + Event timeline + Correlation graph + ATT&CK matrix - Attributes - Discussion 1 1202:This Galaxies Galaxies Galaxies Correlate view all Correlate Correlate Correlate Correlate Correlate Correlate Attributes to populate the ovent with attributes (indicators, observables or information) to provide a meaningful event	Modification map		
- Phots - Galaxy + Event graph + Event timeline + Correlation graph + ATT&CK matrix - Attributes - Discussion 1202 This L Galaxies G+ = +		PRvots - Galaxy + Event graph + Event timeline + Correlation graph + ATT&CK matrix - Attributes - Discussion It 1202:This t Galaxies Galaxies very all Correlate Yeliated Tags ▼ Filtering tool Org Category Type Value Tags Galaxies Comment Correlate Attribute warning: This event doesn't contain any attribute. It's strongly atMsed to populate the event with attributes (indicators, observables or information) to provide a meaningful event	Sightings	0 (0) - restricted to own organisation only. F	
x 1202: This I Galaxies Image:	Galaxies Cell Cell Ceprevious nexts View all	Image: Second state of the second s	- Pivots - Galaxy •	Event graph + Event timeline + Correlation graph + ATT&CK matrix - Attributes - Discussion	
Galaxies Cel 2014	Calaxies C C C C C C C C C C C C C C C C C C C	Calaxies Calaxies Correlate			
Galaxies Cr 24	Galaxies C = 2+ < previous next > view all	Galaxies Image: Second state in the secon	X 1202: This I		
	<pre>contacted c previous next > View all </pre>	Image: sprewhous ned.s view all Image: sprewhous ned.s view all Image: sprewhous ned.s view all Image: sprewhous org Deleted MEDecsy score Image: sprewhous org Category Type Value Tags Galaxies Comment Correlate Attribute warning: This event doesn't contain any stribute. It's strongly advised to populate the event with attributes (indicators, observables or information) to provide a meaningful event	Galaxies		
	<pre>c previous next > Vfew all</pre>				
	<pre>c previous next > view all</pre>	e previous next-s vew all e previous next-s vew all e previous e previe previous			
<pre>revious next > view all</pre>		Image: State in the second state in	« previous next »	view all	
		Image: Second contraction of the second contresecond contraction of the second contraction			
		Attribute warning: This event doesn't contain any attribute. It's strongly advised to populate the event with attributes (indicators, observables or information) to provide a meaningful event		Scope toggle Velated 22 Decay score A Sighting DB Context Related Tags Y Filtering tool	Canadata
+ JE E Scope toggle + Peleted 12 Decay score A SightingDB O Context * Related Tags Y Filtering tool	+ E 🛪 Scope toggle 🕈 Deleted 🗠 Decay score 🖌 SightingDB 🛛 Context 🥆 Related Tags 🍸 Filtering tool	Attributes warning: This event doesn't contain any attribute. It's strongly advised to populate the event with attributes (indicators, observables or information) to provide a meaningful event		rg category lype Value Tags Galaxies Comment	correlate
Image: Scope toggle > Toleted Image: Decay score M SlightingDB O Context Tributing tool Org Category Type Value Tags Galaxies Comment Correlate	Image: State in the state i				d overt
Image: State in the state	Image: State in the second		Attribute warning: This	went doesn't contain any attribute. It's strongly advised to populate the event with attributes (indicators, observables or information) to provide a meaningfd	a event

- b. Category: Select Network activity.
- c. Type: Select domain.
- d. Value: Enter "tv-powiat24.h2g.pl". This is a known malicious domain in the TIDE feed.
- e. Click Submit.

Add Attribute		×
Category 🚯	Туре	î
Network activity *	domain 💌	- 8
Distribution		- 8
Inherit event ~		
Value		
tv-powiat24.h2g.pl		
	Å	
Contextual Comment		. 8
		10
For Intrusion Detection System		
Batch Import		- I 🗄
Disable Correlation		
Eirst soon data 🚔		
First seen date		
		- 1
Last seen date 苗		
First seen time O		
HH:MM:SS.sssss+TT:TT		
	Submit	Cancel
	Subline	Gancer

4. You will see the event ID of our new feed appears under Related Events for this attribute. Hover over the ID to verify.

l	+ 🗉	≣ ≭	Scope toggle 🕶	👕 Deleted	🗠 Decay score	👫 SightingD	B 🚯 Conte	ext 📲 Related Tags	▼ Filtering tool			
I	□ Date ↑	Org	Category	Type V	alue	Tags	Galaxies	Comment	Correlate	Related	Orgc: ORGNAME	Distrit
	2020-09-22		Network activity	domain ty	-powiat24.h2g.pl	3 + +	3+ +			<u>1201</u>	Date: 2020-09-22 Info: B1TD-Phishing feed	nherit
											Correlating Value: tv-powiat24.h2g.pl	

5. Click on the **ID** to view the feed event info.

+		È	*	Scope toggle 👻	👕 Delet	ed 🗠 Decay score	i SightingD	B 🚯 Conte	xt 📲 Related Tags	▼ Filtering tool	
Dat	e î	Or	g	Category	Туре	Value	Tags	Galaxies	Comment	Correla	te Related Events
202	0-09-2	2		Network activity	domain	tv-powiat24.h2g.pl	⊗ + ≗ +	⊗ + ≗ +			(1201)

a. Shown is the feed event info.

Home EventActions																	
View Event View Correlation Graph	B1TD-Phishi	ng feed											Related Eve	nts			
View Event History	Event ID	1201											This is a re-	onnizable descrip	tion sy Phis	hing Sites	sy One IP hosting
Edit Event	UUID	44669284-04d0-404c-90d3-d	d49700a45fe 🕴										^{oR} 2020-09-22	ognizatio descri	1 Fix 201	3-01-03 3	Fn 2018-06-01
Delete Event	Creator org	ORONAME											CH OSINT Fand	y Bear Pens the V	Vorst Blog Posts	Ever by Thre	atConnect
Add Attribute	Owner org	ORONAME											MIM-Loris	2017-10-02 46	-2 offina "skr		C-16 122458
Add Object	Email	admin@admin.test											2017-10-03				1
Add Atlachment	Tags	🔇 + 🚢 +											M2M - Lock	2017-09-05 : Affi	I=3 : "Voice Mes	age from D1	1234567890
Enrich Event	Date	2020-09-22											 05NT, Th 	Curinus Case of	Notenard and CI	othonic: Evol	nsing a Maligin
Merge attributes from	Threat Level	Undefined											2017-08-15	Composiçõese or	realized and on	monte, Expe	2
	Analysis	Completed											ce Pivot on oth	er email address	es found by using	g the same p	hysical addre
Publish Event	Distribution	All communities 🛛 🔒	<										2016-06-28				1
Contact Reporter	Info	B1TD-Phishing feed											2016-04-21	king mo a cyser-	Adatik Patilitator	In the rooting	narios by men
Download as	Published	No											CH OSINT Phis	ning sites and exp	loit kits decemb	er 2015 - pa	rt 2 by TechHel
	#Attributes	203962 (0 Object)											2010-12-13 Show (5 more)				1
List Events	First recorded change	2020-09-22 16:03:26											anon (a more)				
Add Event	Last change	2020-09-22 16:21:42															
	Modification map																
	Sightings	$\boldsymbol{0}\left(\boldsymbol{0}\right)$ - restricted to own organi	sation only. 🗡														
	- Pivots - Galaxy + E	ventgraph + Eventämeline +	Correlation gra	ph +ATT&CK matrix = Attributes = Discuss	sion												
	X 1202: This I	1201: B1TD-P.,															
				<u>,</u>													
	Galaxies																
	Ø+≛+			J													
	<previous 1="" 2<="" th=""><th>3 4 5 6 7 8</th><th>9 10</th><th>11 12 13 14 15 16 17</th><th>18 19 20 21</th><th>1 22 2</th><th>23 24 25</th><th>26 27 28</th><th>29 30</th><th>31 32 33 3</th><th>4 35 36 37</th><th>38 39 40</th><th>41 42 43</th><th>44 45</th><th>46 47 4</th><th>8 49</th><th>50 51 52</th></previous>	3 4 5 6 7 8	9 10	11 12 13 14 15 16 17	18 19 20 21	1 22 2	23 24 25	26 27 28	29 30	31 32 33 3	4 35 36 37	38 39 40	41 42 43	44 45	46 47 4	8 49	50 51 52
	60 61 next>	New all															
						_											
	+ = = ×	Scope toggle + Deleted	🗠 Decay sco	re 🖌 SightingDB 🚯 Context 🦙 Related	d Tags 🛛 🕇 Filtering tool												E
	Date † Or	G Category	Туре	Value	Tag	s	Galaxies	Comment			Correlate	Related Even	Is	Feed hits		IDS	Distribution
	2020-09-22	Payload delivery	filename	anazom buzz	8	+ 2 +	🚯 + 🗮 +									2	All
	2020-09-22	Payload delivery	filename	esitffnylomygzqt-dat-millinium.eyz.appspat	com 📀	+ 🛎 +	😵 + 🚨 +									2	All
	2020-09-22	Payload delivery	filename	jsgeqoliqvanucce-dob-millinium.eyr.appspol	Lcom 😵	+ 🛓 +	🔇 + 🚨 +										All

Additional Resources

There are several ways to download MISP. Find instructions here.

MISP offers many optional modules for additional functionality. Find a summary of available modules and their installation instructions <u>here</u>.

For all things MISP, find the detailed administrative user guide <u>here</u>.

For more information about Infoblox's BloxOne Threat Defense, see the guide here.

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters 2390 Mission College Blvd, Ste. 501 Santa Clara, CA 95054 +1.408.986.4000 www.infoblox.com

@ 2023 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc. All other marks are the property of their respective owner(s).