infoblox.

DEPLOYMENT GUIDE

Integrating BloxOne Threat Defense TIDE IoC into Cisco Firepower Management Center

Table of Contents

Introduction	2
Requirements	2
BloxOne TD Instructions	.2
Cisco Firepower Instructions	5

Introduction

Cisco Firepower Management Center manages the following Cisco network security solutions:

- Firepower Next-Generation Firewall
- Firepower Next-Generation IPS
- ASA with Firepower Services
- Firepower Threat Defense for ISR
- Advanced Malware Protection (AMP) for Networks

A <u>Cisco Firepower Management Center</u> feature, Threat Intelligence Director, ingests third-party threat feeds and correlates enriched observations from Cisco security solutions to detect and alert on security incidents. By converting intelligence into actionable indicators of compromise, you can block or monitor more threats, reduce the number of alerts you must review, and improve your overall security posture.

This deployment guide shows you how to upload the Infoblox BloxOne Threat Defense TIDE indicators into Cisco Firewall Management Center.

Requirements

- Access to Infoblox Cloud Services Portal TIDE (Threat Intelligence Data Exchange).
- Cisco Firepower Management Center version 7.2.1 or above.

BloxOne TD Instructions

- 1. Log into the csp.infoblox.com website to acquire a Service API key to access the threat indicators.
- 2. Navigate to Administration \rightarrow User Access.



- 3. Under Users tab, click on Create, this opens the Create User window. Input the following:
 - Name: Input a name for this user.
 - **Type**: Select **Service** in the dropdown menu.
 - Available User Groups: In this section, select the appropriate user group/s which will inherit the permissions and roles to this service user. Click Save and Close.

Create User				
*Name	demo_service_user			
Туре	Service	-		
Email]	
	Search			Search
AVAILABLE USER GROUPS		»	SELECTED USER GROUPS	1
ib-ddi-admin		U	ib-td-user	×
ib-td-admin		\odot		
ib-ddi-user		\odot		
ib-trusted-partner		\odot		
act_admin		\odot		

4. Click on the Service API Keys tab.

infoblox.	¢	Users Roles	User Groups Access Policies	Service API Keys
🐵 Dashboard				
🖽 Manage		Create Enabl	le Disable Delete	
듣 Policies				
🔟 Reports			∧ NAME	STATE

5. Click on **Create**. Type in a **name**, select the **Service User** you created earlier and select an **expiration date**. Click **Save and Close**.

Create Ser	vice API Key
*Name	Key_for_demo
*Service User	demo_service_user
Expires at	08/31/23 12:06 pm

6. Copy the API key and save it to a file. This will be your only time that you can do so.



7. You are now ready to create the URL to download the IOCs that you request. Navigate to Research \rightarrow Active Indicators.

infoblox. 🧳									x 🝳
 Dashboard Manage Policies 	Filter	Apply Filter	Export Generate AF	Pl Request			Search		
Reports	Data Type		INDICATOR	DATA TYPE	THREAT CLASS	DETECTED	DATA PROVIDER	THREAT	≡
Dossier Active Indicators	Select all	Clear (1)	hrcbishtek.com	HOST	UncategorizedThreat	2023-07-17T11:23:00.000Z	AISCOMM	80	•
Resources	Hash	(11,225)	ber6vjyb.com	HOST	UncategorizedThreat	2023-07-17T11:23:00.000Z	AISCOMM	80	
Administration	✓ Host ✓ IP	(17,763,930) (1,028,367)	nitutdra.com	HOST	UncategorizedThreat	2023-07-17T11:23:00.000Z	AISCOMM	80	
		(139,101)	guerdofest.com	HOST	UncategorizedThreat	2023-07-17T11:23:00.000Z	AISCOMM	80	
	Threat Class/Prope	Clear	secretsdump.py	HOST	UncategorizedThreat	2023-07-17T11:23:00.000Z	AISCOMM	80	
	 APT Bot 	(5,461) (5)	ecorfan.org	HOST	UncategorizedThreat	2023-07-17T11:23:00.000Z	AISCOMM	80	
	 Compromised Compromised 	IDomain (3) IHost (5)	compromisedhost.eicar.network	HOST	CompromisedHost	2017-07-24T17:22:40.053Z	AISCOMM	100	
	 Cryptocurrent + Show more 	cy (2,279)	fuanshizmo.com	HOST	UncategorizedThreat	2023-07-17T11:23:00.000Z	AISCOMM	80	

8. Clear all of the check marks and then check the items that you want and then click on **Apply Filter**. For example, select **URL**.

infoblox. 🧳					R 🕢
 Dashboard Manage Policies 	Filter Apply Filter	Export Cenerate API Request		Searc	:h
Reports	Data Type	INDICATOR DATA TYPE	THREAT CLASS DETECTED	D DATA PROVIDER	THREAT
Dossier Active Indicators	Select all Clear	https://imsagentes.pe/dgrjfj/ URL	UncategorizedThreat 2023-07-	-17T11:23:00.000Z AISCOMM	80
Resources Threat Lab	Hash (11,225)	https://ecorfan.org/base/sj/docu URL	UncategorizedThreat 2023-07-	-17T11:23:00.000Z AISCOMM	80
뽄 Administration	IP (1,028,367)	https://nomoresense.com/checki URL	UncategorizedThreat 2023-07-	-17T11:23:00.000Z AISCOMM	80
	VRL (139,101)	https://beróvjyb.com/dns.php URL	UncategorizedThreat 2023-07-	-17T11:23:00.000Z AISCOMM	80
	Select all Clear	https://snowboardspecs.com/nai URL	UncategorizedThreat 2023-07-	-17T11:23:00.000Z AISCOMM	80
	→ APT (5,461) → Bot (5)	https://hrcbishtek.com/%7B5 URL	UncategorizedThreat 2023-07-	-17T11:23:00.000Z AISCOMM	80
	CompromisedDomain (3) CompromisedHost (5)	https://www.meditimespharma.c URL	UncategorizedThreat 2023-07-	-17T11:23:00.000Z AISCOMM	80
	Cryptocurrency (2,279) Show more	https://corporacionhardsoft.com URL	UncategorizedThreat 2023-07-	-17T11:23:00.000Z AISCOMM	80

9. Click on **Generate API Request**. This button will show you the basis of the API URL that you will add to the sources in Cisco Firewall Management Center. The screenshot below is an example.



- 10. Take the segment starting with HTTPS and do the following:
 - https://<Service API Key>@csp.infoblox.com/tide/api/data/state/threats?type=url&rlimit=<# of IOCs>&data_format=STIX
 - In the line above in bold, you add the service API key that was previously generated, the state parameter which provides the IOCs that are currently active, the number of IOCs, and the data format which is STIX.

Cisco Firepower Instructions

1. Log into the Cisco Firewall Management Center.

Firewall Managem Overview / Dashboards /	nent Center Dashboard	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	0	₽	🕜 admin 🔻	cisco SECUP	ŧ
													Reportin	g
Summary Dashboar Provides a summary of activity on the app	rd (switch dashboard) pliance													
Network × Threats	Intrusion Events S	Status G	deolocation	QoS	+			Show t	he Last	11	hour		¥	11
												[Add Widgets	ו

2. Click on Integration \rightarrow Intelligence \rightarrow Sources.

Firewall Management Center	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy Q	🔮 🌣 🔞 admin 🔻	cisco SECURE
Sources Indicators Observables										
٩									C 0 Sources	+
\$ Name					‡ Type	Delivery Acti	tion Publish	▼ Last Updated	Status	

- 3. Click on the '+' button on the right side of the screen to add a source. Select delivery type of URL. Add the URL that was created in step 9. Here is an example:
 - https://<service api key>
 @csp.infoblox.com/tide/api/data/threats/state?type=url&rlimit=100&data_format=stix
 - $\circ~$ This URL will access 100 URL IOCs and output them in STIX format.

- Input the **username** of the api key.
- The **password** is the service api key.
- Input a **name** of the feed.
- Optionally, input a **description**.
- Input an **update interval**. This tells Firewall Management Center how often to query csp.infoblox.com for updates.
- Click 'Save'.

Add Source	Ć	? ×									
DELIVERY	TAXII URL Upload										
ТҮРЕ	STIX 🗸										
URL*	'oblox.com/tide/api/data/threats/state?type=url&rlimit=100&data_format=sta	*									
	SSL Settings	×									
USERNAME	apikey										
PASSWORD											
NAME*	URL										
DESCRIPTION	URL feed										
ACTION	Monitor										
UPDATE EVERY (MINUTES)	1440 Never Update										
TTL (DAYS)	90										
PUBLISH											
	Save	ancel									

4. Refresh the Sources screen and click on the status for results of the download.

[Firewall Management Center Integration / Intelligence / Sources	Overview	Analysis	Policies	Devices	Objects	Integration				Deploy	م	0	\$ (🗿 admin 🔻	cisco SECURE
	Firewall Management Center Integration / Intelligence / Sources Sources Indicators Cotenvables Cotenvables	Overview	Analysis	Policies	Devices	Objects + Type STIX	Integration + Datwery URL	Action Monitor	Pu	Status Message Last Updated Nast Update Total Indicators Consumed Discarded Observables Consumed Unsupported Invalid	Deploy Operation comp 2 minutes ago in 23 hours 100 Last Update 100 Last Update 100 0 Last Update 0 0	Q leted su	. C	☆ (C Stat	admin ▼ 1 Source us 2completed	thethe secure + ♪ □

5. Click on the Observables tab to get the results.

Fi Int	Firewall Management Center Overview Analysis Policies Devices Objects Integration Deploy Q 📀 🌣 🚱 admin 🔻 端 SECURE											
Sources	Indicators Observables											
۹											C 100 Observables	
¢ Type Value								Action	Publish	▼ Updated At	\$ Expires	
URL	translogistixgroup.com/adobereasdt/Adol	eReader/					1	S Monitor -		Nov 15, 2022 2:37 PM EST	Feb 13, 2023 2:37 PM EST	Ø
URL po-trackd4k.com/Address.php?session=T0Xf90s30pjDtjeOQ2yIBPHDXgymTxr0MPdCsB48v49UnfGiqy9wftVLjcUz/								Monitor -		Nov 15, 2022 2:37 PM EST	Feb 13, 2023 2:37 PM EST	D
URL	off.fbook-90801813.almajd.ps/nextVRF.ht	nl?location=3D3e99	3cc4461511d=/				1	🕤 Monitor 🗸		Nov 15, 2022 2:37 PM EST	Feb 13, 2023 2:37 PM EST	Ð
URL	load.cofry.com/www.apple.com/nz/						1	S Monitor -		Nov 15, 2022 2:37 PM EST	Feb 13, 2023 2:37 PM EST	Ø
URL	pages.lemlist.com/api/page-templates/pt	p_skXbWCaXNfp4M	17Sii?=5994trwits/				1	Monitor -		Nov 15, 2022 2:37 PM EST	Feb 13, 2023 2:37 PM EST	D
URL	labp655.tmweb.ru/50e5fd93239c40e5e65	837ff0b4de4c3/					1	📀 Monitor 🗸		Nov 15, 2022 2:37 PM EST	Feb 13, 2023 2:37 PM EST	D
URL	lloydsbank.security-personal-devices.com	n/Login.php/					1	S Monitor -		Nov 15, 2022 2:37 PM EST	Feb 13, 2023 2:37 PM EST	ß
URL	parcel.emiratespost.ae.bangerpickleball.c	om/uae/09fc3a2643	3a523ca257b5d43	6e6d21a1/zlatan	.php/		1	Monitor -		Nov 15, 2022 2:37 PM EST	Feb 13, 2023 2:37 PM EST	D
URL	www.isupport.com-w3t.co/i/sing/H4Qj/						1	S Monitor -		Nov 15, 2022 2:37 PM EST	Feb 13, 2023 2:37 PM EST	Ø
URL	oneyog.com/wp-admin/usr/af6f2/						1	😔 Monitor 🗸		Nov 15, 2022 2:37 PM EST	Feb 13, 2023 2:37 PM EST	D
URL	garderobsbrickor.se/eds/?client-request-	id=Y2hhaXlhcG9ybi	5wYWxhbm9uZEB	dm9uaWsuY29t/			1	📀 Monitor 🗸		Nov 15, 2022 2:37 PM EST	Feb 13, 2023 2:37 PM EST	Ø
URL	services.runascape.com-vc.ru/m%3Dweb	login/loginform5889	%2C943%2C238%2	C69188411%2C2	2497/		1	📀 Monitor 🗸		Nov 15, 2022 2:37 PM EST	Feb 13, 2023 2:37 PM EST	Ø
URL	catechumenical-alli.000webhostapp.com	'link/english/crypt/ir	ndex.html/				1	S Monitor -		Nov 15, 2022 2:37 PM EST	Feb 13, 2023 2:37 PM EST	ß
URL	rmidtracking-a4cabf.ingress-erytho.easy	wp.com/rm/5741582	21762206628/				1	🕤 Monitor 🕶		Nov 15, 2022 2:37 PM EST	Feb 13, 2023 2:37 PM EST	ß

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).