

JOINT SOLUTION BRIEF

Infoblox and ThreatQ[™] Technology Segment: Enrichment & Analysis

INTEGRATION HIGHLIGHTS

- Enhance IP address and DNS visibility for TIP administrators.
- · Accelerate responses to emerging threat vectors by using Infoblox contextual data.
- Integrate threat intelligence feeds from the ThreatQ platform with Infoblox DNS security solutions
- Download Infoblox threat intelligence from the Infoblox Threat Intelligence Data Exchange (TIDE) into the ThreatQ database.
- Monitor lookalike domains.

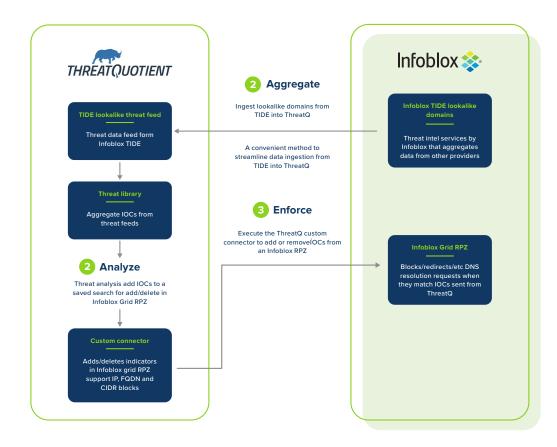
With the combination of Infoblox contextual data and the ThreatQ threat intelligence platform, your organization can categorize, manage and respond to threats with greater speed and efficacy by activating cyberintelligence in Infoblox DNS and importing Infoblox threat intelligence.

ThreatQ by ThreatQuotient™

ThreatQ is an open and extensible threat intelligence platform (TIP) to provide defenders the context, customization and collaboration needed for increased security effectiveness and efficient threat operations and management. ThreatQ accelerates the transformation of threat data into actionable threat intelligence by giving defenders unmatched control through a threat library, an adaptive workbench and an open exchange to ensure that intelligence is accurate, relevant and timely to their business. With ThreatQ, customers can automate much of what is manual today and get more out of existing security resources, both people and infrastructure.

Silobreaker

Infoblox is the leading global provider of DNS, DHCP and IP address manage-ment services. Infoblox DNS can put more than 45 million threat indicators to work in real time within the Infoblox Grid[™] and BloxOne[™] Threat Defense, which provides advanced DNS security as SaaS-based services from the cloud. Infoblox solutions automate network control functions to reduce costs and maximize uptime while protecting against a flood of malware and DDoS attacks. From discovery, configuration and compliance, Infoblox automates and simplifies network and security processes.



Integration Use Cases:

Integrating Infoblox IP and DNS contexts with ThreatQuotient supports a variety of use cases, such as:

- Allow joint customers to assess, categorize and manage security incidents
- Eliminate unnecessary, duplicate and irrelevant indicators before they enter your network
- Enforce security and automate changes

THREAT() 🤇 🔹	副 Threat Library 人 Investigations Lat	Analytics		+ Create	Q A # ®			
S Indicators 330	infoblox, add				Load Search + @ Saint			
					ns 💌 Actions 💌			
	Type * Status * Score	* Expiration	*					
	VALUE 0	TYPE #		DATE CREATED . LAST MODIFICO				
	 87.87.87.8 76.76.7.6 	IP Address IP Address		06/08/2020 04:12pm 06/08/2020 04 06/08/2020 04:12pm 06/08/2020 04				
	@ 65.65.6.5	IP Address		06/08/2020 04:12pm 06/08/2020 04 06/08/2020 04:12pm 06/08/2020 04				
	• 23.23.2.3	IF PARENT	PAM VLANs	Super Host DHCP DNS File Dakibution	- open			
	bim.bam.com		Contract Contraction					
	blah.bloh.com	4			Response Policy Zones Subscriber Services Deployment NXDOMAIN Rulesets B			
	blah-blah.com	** + + • +	Response Policy Zer					
	paypalservice.net-suga-size-vpn.hd.devel opment.grandrounds.com paypal.info.airteimail.com		threatqrpz	ê 🗡 🖪				
			Oulck Filter None	Filter On Show Filter				
	 psypalcenterlocal.deskpro.com 	+	+ • (12) 8	• (± • (0	Go to 🔤 😡	Edwalder Attibuter		
				OR ADDRESS	POLICY DATA COMMENT SITE	Order Response Policy Zones		
	 paypalsupportLcom 		□ = 23.23		Passihru Doma	Policy Zones		
	 paypal-confirm.info 		E = 65.65		Passthra Domai,	C Theat insight in the Cloud Client		
	 paypalloginsftp.flexporterraform-wx221. sandbox.flexport.com 		E 76.7		Passtwu Domai			
	 paypal.com-accountslimited.app.acorns. 			1878	Passihra Doma	Manage Dynamic Update Groups		
	• com			10.140.163	Passihru Domai	🛓 Import Zone		
				unt-paypal.org				
				ant-replypaypal-serventtp.com	Connection Settines			
				accountpaypel us	Connection Settings			
					API IP/Hostname			
				into paypal into	10.13.0.169		9	
			E = accp	aypal.com	Hostname or IP address of the Infoblox Grid Instance.			
			🗐 🗐 admi	nistration paypat.biz	- Username			
			🗐 🗏 apps	piypal.com.aitelmail.com	admin	admin		
			E asad	spaypelsignon.us.metrics.powerchs.org	Username for logging to infoldox Grid.			
				al028ptn-manage-paypal us-confluence 3p music dec-staging periscopedata	com			
				asadabbilgin-manage pageal us-iya atg corp periocopedita.com asadabbilgin-manage pageal us-iya h doc periocopedita.com N 2		Former for larging on inflution SAL		
					Password for logging to infoliox Grid.			
					- Savert search with indicators to add to an infolder 897			
					infoblox_add			
					The name of the saved search in the ThreatQ instance with indicators to be	added to an infoliox RPZ.		
					- Saved search with indicators to delete from an Infoblox RPZ			
					infoblox_remove			
					The name of the saved search in the ThreatQ instance with indicators to be	deleted from an infobilist RP2.		
						r The name of the Infoblox RP2 -		
					threatorpz			
				The name of the Response Policy Zone created on the Infablox Grid apptiance.				
					Name of the DNS view default			
					The name of the DNS view in which the record resides. The default value for	r DNS view is "default".]	
					Save Changes			

About ThreatQuotient

ThreatQuotient[™] understands that the foundation of intelligence-driven security is people. The company's open and extensible threat intelligence platform, ThreatQ[™], and cybersecurity situation room solution, ThreatQ Investigations, empower security teams with the context, customization and prioritization needed to make better decisions, accelerate detection and response, and advance team collaboration.

Leading global companies use ThreatQuotient solutions as the cornerstone of their security operations and threat management system. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe and APAC.

For more information, visit threatquotient.com.



Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent of the Fortune 500.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054

+1.408.986.4000 | info@infoblox.com | www.infoblox.com



© 2021 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).