BM Security

Cisco Umbrella with Enforcement API App for IBM Resilient

Boost network visibility and gain actionable insight

Benefits

- Single console simplicity combines threat visibility, detection, and quick response
- **Power and flexibility** to integrate containment response activities into your workflow
- **Reduced security risk** from accelerating incident response

Overview

IBM Security and Cisco Security have joined forces to deliver advanced integrations to improve network visibility and speed threat detection and response.

The Cisco Umbrella and IBM Resilient solution enhances customer security efficiency by providing data enrichment, threat analysis and suspicious domain containment in a single dashboard. Cisco Umbrella Enforcement API, included with Umbrella Platform, integrates directly with the IBM Resilient incident response platform.

Example: when tracking a suspicious domain in a security incident, analysts can add a DNS entry that will trigger an Umbrella evaluation, querying a list of domains. From the resulting table, analysts can drill down on a domain for investigation, remove good domains from the blacklist, and add malicious domains to the blacklist.

Key Capabilities

Threat analysis

Enriched data from Cisco Umbrella and IBM Resilient provides the intelligence to perform advanced threat analysis Suspicious domain containment
 Cisco Umbrella's enforcement API can take

action and block suspicious domains

Simple integration

Resilient administrators can easily add Umbrella Enforcement API functions to a Resilient activity from menu-item actions to complex automatic workflows

BM Security

Fast Threat Response

Security analysts are faced with the daunting task of detecting advanced threats, analyzing them to determine the severity, and conducting rapid incident responses. Many of these tasks are manual and labor intensive, causing missed threat indicators and delayed responses to the most severe events. The integration of Cisco Umbrella and IBM Resilient can accelerate incident response, helping the customer reduce risk and increase efficiency in their security operations.

The Cisco Security and IBM Security Advantage

The ongoing collaboration between Cisco Security and IBM Security helps organizations strengthen their security posture against increasingly sophisticated cyberattacks. Rather than working in silos, these two leading security providers are collaborating to build solutions and share threat information that will empower clients to act at extreme speed and scale to see a threat once – and protect everywhere.

asks Details Arti	facts Brea	ach GDPR	Notes & Attachmer	nts S	tats & Timeline			
rtifacts								E
						Add Artifact	Table	Gra
Search Q			Artifact	Type: Al	Date Crea	ated: All -	Has Attack	nment:
			Created	Delsta?				Actions
now 25 • entrie Type DNS Name	o Valu	e neexample.com	Created 09/17/2018	Relate?	cified in artifact	type settings		Actions
Туре	o Valu acm		09/17/2018		cified in artifact Add to QRad		· 1	
Type DNS Name	 Value acm Acc 	neexample.com	09/17/2018	As spec		ar Reference	· 1	

Cisco Enforcement		Search Q Print	Export
Name Ø	0 Id 0	Last Seen ()	
www.russianbear.ru	31857076	2018-06-19T15:45:38Z	
acmeexample.com	33642238	2018-09-17T12:55:55Z	

Next Steps

The Cisco Umbrella and IBM Resilient solution provides customers with more efficient solutions to rapidly detect and analyze threats. This application enables customers to protect their environments through orchestrating incident responses. These capabilities eliminate redundant and tedious tasks typically performed by security analysts which translates to more effective security operations. This app is now available on the IBM Security App Exchange. For more information visit http://cs.co/ibmsec.

© 2018 Cisco and/or its affiliates. All rights reserved. This document is Cisco Confidential. For Channel Partner use only. Not for distribution. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

[©] Copyright IBM Corporation 2018 IBM Security Solutions. IBM, the IBM logo, ibm.com, QRadar, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml This document is current as of the initial date of publication and may be changed by IBM at any time.