cisco SECURE

Radware and SecureX Integration Demo Guide







Cisco SecureX[™] is a cloud-native, built-in platform that connects our Cisco[®] Secure portfolio and your infrastructure, providing a consistent experience that provides visibility, enables automation, and enhances security across network, endpoint, cloud, and applications. SecureX simplifies security and integrates into the solutions that customers have already deployed.

In order to demo the features and functionality of Cisco solutions as well as Cisco solutions integrated with Radware solutions, Cisco has developed a portal that allows configuration, testing, and demoing of Cisco and Cisco-Radware solutions. This environment, known as dCloud, is accessible via the following weblink: https://dcloud.cisco.com/

Please note that a valid Cisco Connection Online (CCO) account is required to access Cisco's dCloud environment. Please speak with your local Cisco account team if you do not have a CCO account or create one here: https://www.cisco.com/c/en/us/about/help/login-account-help.html.

One of the dCloud demo environments is called Cisco SecureX and Secure Endpoints with Orbital v1. In this environment, it is possible to view a wide breadth of SecureX integrations, including integration with the Cisco Cloud Web Application Firewall (WAF) solution. Cisco DDoS, WAF, and other solutions are available through Cisco's OEM partnership with Radware.

To learn more about this demo environment, please visit the following link:

https://dcloud-docs.cisco.com/c/r/dcloud-docs/sites/en_us/Security/ secure_x_v1_output/b_secure_x_w_secure_endpoints_w_orbital_v1_ bookmap1.html?dc=rtp





 \bigcirc

SecureX is a collection of cloud tools that integrate with other cloud services, including Radware-enabled solutions for Cisco Cloud DDoS and WAF services, and on-prem devices such as Cisco FMC, WSA, etc. SecureX pulls in threat and event type of information, correlates it between various security devices, and enriches it with Cisco security threat research and forensics.



Figure 1. SecureX - dCloud demo environment: architecture

* Cisco Cloud WAF is powered by Radware.

Cisco SecureX with the Cloud WAF demo environment consists of a single web application (<u>www.ciscowaf.com</u>) that is protected by the Cisco Cloud WAF solution against attacks such as crosssite scripting, brute force attacks, and SQL attacks, as shown in the diagram below:



Figure 2. Cisco Advanced WAF - dCloud demo environment



Security Events in the Cloud WAF portal show the source IP of the attacker and the type of vulnerability they were trying to exploit. The attacker, whose IP address is **54.162.202.67**, is launching a series of application-level attacks such as URL violations in an attempt to browse the website's directory. Cloud WAF is stopping the attempted exploit.

Cisco	ណ៍ Dashboard 🛛 🗘	Monitor 💮 Assets	Account							Ε ζ) 0 🌘	
← Back to Applicati	Security Eve	ents										
WAF DI	DoS			Sort by Time	•	€↓	25 per page	•	Page 1	V = =1	S 🖓	-0-
Action	Time Last week	Destination × Cisco-WAF-Demo	Source			Se	curity		Severity		More	
Blocked 623819313 🗐	25 Jun 2021 13: 02: 02	Cisco-WAF-Demo www.ciscowaf.com	54.162.202.6 United	7 d States of America - US		All	L Access Violat	nsion ion	High		\odot	Î
Blocked 610663214	25 Jun 2021 13: 02: 02	Cisco-WAF-Demo www.ciscowaf.com	54.162.202.6	7 d States of America - US		Vu Co	I nerabilities de Injection		High		\odot	
Blocked 610663213	25 Jun 2021 13: 02: 02	Cisco-WAF-Demo www.ciscowaf.com	54.162.202.6 United	7 d States of America - US		Vu Sei	I nerabilities ver Misconfigu	ration	High		\odot	
Blocked 610663212	25 Jun 2021 13: 02: 02	Cisco-WAF-Demo www.ciscowaf.com	54.162.202.6	7 d States of America - US		All UR	owed File Exte L Access Violat	nsion ion	High		⊘	
Blocked 623819312	25 Jun 2021 13: 02: 02	Cisco-WAF-Demo www.ciscowaf.com	54.162.202.6 United	7 d States of America - US		Vu Co	Inerabilities de Injection		High		\odot	
Blocked 610662910	25 Jun 2021 12: 47: 02	Cisco-WAF-Demo www.ciscowaf.com	54.162.202.6	7 d States of America - US		All UR	wed File Exte L Access Violat	nsion ion	High		⊘	
Blocked 623819009	25 Jun 2021 12: 47: 02	Cisco-WAF-Demo www.ciscowaf.com	54.162.202.6	7 d States of America - US		Vu Soi	I nerabilities ver Misconfigu	ration	High		\odot	
Blocked 610662909	25 Jun 2021 12: 47: 02	Cisco-WAF-Demo www.ciscowaf.com	54.162.202.6	7 d States of America - US		Vu Co	Inerabilities de Injection		High		\odot	
Blocked 623819008 []	25 Jun 2021 12: 47: 02	Cisco-WAF-Demo www.ciscowaf.com	54.162.202.6 United	7 d States of America - US		All	wed File Extern L Access Violat	nsion ion	High		\odot	

Figure 3. Cisco Advanced WAF - Customer Portal

With the attacker's IP information, we can now leverage the power of Cisco's SecureX portal to help further investigate this attacker.

Connect to Cisco dCloud SecureX demo cloud:

https://dcloud2-rtp.cisco.com/content/instantdemo/cisco-securex-threat-response-v1-instant-demo? returnPathTitleKey=content-view

Click on the View button, as shown in the screenshot below:

CISCO dCloud My Hub Catalog Support	News Community Collections		▲ (10) ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○
Back			
Cisco SecureX Threat F	Response v1 - Instant De	mo	View
Information Resources			
Documentation Cisco SecureX Thifeat Response v1 - User Guide			
About Consta Us Des Agreement Relates Notes In Memorial	Related Resources Conco on macroart Canco paina/concort Proposed Expert Services Registre for Bid Management Readmaps	Follow Us Facebook Instagram Twitter YouTube	
D 2021 Cisco and/or its affiliates. All rights reserved.			

Figure 4. dCloud demo environment access







As mentioned earlier, SecureX is a collection of security tools. The tool that is leveraged to investigate an attacker is the SecureX Threat Response. Click "View," as shown in the screenshot below:





Once connected to the SecureX Threat Response, go to the top left of the page where there is a box with the words "Paste log entry, IP address, domain, etc" and enter the IP address of the attacker seen earlier in this document, **54.162.202.67**.

← → C ⓐ visibility.amp.cisco.com/investigate	 Q ☆ ⊕ ℙ 𝔄 ★ ❷ : nce ● ? Demo User ∨ 	
Paste log entry, IP address, domain, etc Investigate Upload Snapshot What can I search for?	Auto Omit	
Getting Started	My First Investigation	Speed up your investigations with SecureX Orchestration
Bird by confugation integration modules in Class Security, which allows Thread Response to grave your whiching Class beachmarks.	Puede exceptionation of DSC. (IP deviation, SMA, etc.) have accurable balance, advect here your SMM, kyy lines, and may other wanter-balance balance	No can add Lastern expanses enders his Te solet mens a seamheady on a data and ensuite entrifunct on and exemption have not experiment. The seamon and Clark do this new 2 mends when to see this is a data and each how to get stanted with Orchestration body.
	Need Help?	
Unitaritia Web Society Appliance Don't own these products? Spin sp for a free full. AMP for Exceptions Evail Society Appliance Prepare SMA Email StatSmatch Enterprise Tread: Ddr Unitaritia	Browse the help taplet, which hotald definitions, FAGs, and much more the transmission of	

Figure 6. Threat Response - Entering IP address information required to launch an investigation



Then click the Investigate button:

← → C
cisco Threat Response Investigate Snapshots Incidents Intelligence
54.162.202.67
Investigate Upload Snapshot What can I search for?
Getting Started
Start by configuring integration modules in Cisco SecureX, which allows Threat Response to guery your existing

Figure 7. Threat Response - Launching a new investigation

SecureX using API calls will retrieve information from the Cloud WAF and other Cisco Security solutions like Cisco Umbrella[®], Talos[®], FMC, etc., and will correlate all information regarding this attacker's IP from all of its services and sources.

Note: Because these are live feeds, you may not see exactly the same messages or attacks shown in the example below. This is normal and depends on the attacks which are occurring at the time of your lab and the Cisco Cloud Security threat information at the time of the demo. However, all the steps will be the same in investigating an attacker.



Figure 8. Threat Response - Active investigation





SecureX provides this enriched and correlated data view of an attacker and its attack vectors. Moving from left to right, we can see that this attacker IP targeted five systems. There is one investigation, with three indicators and by two modules.

Looking at the five targets, click on the down arrow to view these targets.

	5 Targets 🗸	
5 w	eb application	
	urL www.ciscowaf.com/test.php	
	URL www.ciscowaf.com/zuoss.php	
	URL www.ciscowaf.com/vendor/phpunit/phpunit/src/Util/PHP/e	\sim
	url www.ciscowaf.com/xmlrpc.php	
	uRL open.ciscowaf.com/test.php	
	1	

Figure 9. Targeted URLs

We can see the five URLs that were targeted.

For the Indicators, click on the down arrow.

³ Indicators →	
Code Injection Code Injection	
URL Access Violation URL Access Violation	
Server Misconfiguration Server Misconfiguration	

Figure 10. Indicators





We can see the three types of security threats that were launched by this attacker: Code Injection, URL Access Violation, and Server Misconfiguration.

The two modules that provided information for this attacker were the Radware Cloud WAF service and Cisco Umbrella.



Figure 11. Modules

By clicking on the IP address in the middle of the screen, we get another perspective of this data.

b b 1



Figure 12. Investigation details



In the Judgement tab, we can see that Umbrella provided a Neutral judgement for this IP address.

By clicking the Indicators tab, we can see all the indicators for this attacker's IP. In each indicator, we can see the confidence of the attack. In this example, it is High.



Figure 13. Indicators

By clicking the JSON button for a given indicator, the API response information in JSON format can be analyzed.

Code	Injection
▼ "i	ndicator" : {
	description" : "Code Injection"
•	"tags" : []
•	"valid_time" : {}
	producer" : "Radware Cloud WAF"
"	schema_version" : <mark>"1.0.16"</mark>
	type" : "indicator"
	short_description" : "Code Injection"
	title" : "Code Injection"

Figure 14. Indicator in JSON format

Additionally, SecureX is able to push configuration out to the Cloud WAF. For example, if an IP is deemed malicious, the SecureX administrator can block that IP by adding it to the block list in the Cloud WAF service. This prevents this IP from accessing the website altogether.

Click on the down arrow next to the IP address and a menu will open with the option to Add IP to block list.



Figure 15. Adding an IP address to a block list

The action of "Add IP to block for the app" will fail as the API credentials do not have write permission and we don't want to block this IP as it will affect others' experiences with the demo.

Note: In this dCloud SecureX demo for Cloud WAF, there was not a lot of correlated information because the Attacker IP is not a real-world attacker. This IP is only attacking this website under our control, and Talos, Umbrella, and AMP are real environments that are only collecting real threat information. In a real-world attack, there would be much richer and correlated events that can be viewed in SecureX. This is why SecureX is better experienced in a real-world environment than in a demo.

As mentioned, dCloud SecureX and Cloud WAF provided in this demo are a real environment; however, the attackers are not real world. What this means is you can test it by launching your own nonmalicious attack that will be detected and blocked by Cloud WAF from your PC.







First determine your internet IP address by googling "What's my IP."

Google	what is my ip address	× 🕴 ९
	Q All I News ▶ Videos ⊘ Shopping ♀ Maps I More	Settings Tools
	About 1,790,000,000 results (0.47 seconds)	
	What's my IP	:
	184.147.53.64 Your public IP address	
	→ Learn more about 184.147.33.33	

Figure 16. What's my IP address?

From your web browser's URL box, enter the following:

www.ciscowaf.com/zuoss.php

You should get the following message: "Unauthorized Activity Detected"

\leftarrow	C	Not secure www.ciscowaf.com/zuoss.php	
			Unauthorized Activity Detected
			You are seeing this page because we have detected unauthorized activity. If you believe that there has been some mistake, please contact our support team with the case number below.
			Case Number: 623823070







Wait a couple of minutes, and then go back to the SecureX Threat Response window.

Figure 18. SecureX Threat Response window

Enter your IP address and click "Investigate."

\leftrightarrow \rightarrow C $ ightarrow$ visibility	amp.cisco.com/ii	nvestigate				
threat Response	Investigate Snaps	nots Incidents	Intelligence			
184.147.33.33						
Investigate Upload Snaps	hot What can I	search for?				
	Ge	ting Started				

Figure 19. Investigate on an IP address





You should be able to see your IP address and the type of attack you attempted on the www.ciscowaf.com website.

Figure 20. Investigation in Threat Response

Investigate further by looking through all the options within the SecureX Threat Response window.

If you would like further information, reach out to your Cisco or Radware account team (cisco.alliance.team@radware.com), who will be happy to provide further information.

Thank you for your interest in the Radware and SecureX integration demo.

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: 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. 07/21