

حذفصل إلى لقتنا، IBM QRadar في Cisco نم ةباحس إلى نام ق يبطت إلى لقتنلل
 رظن بيوبتلة مالع رهظت فوس. Cisco ةباحس نام بيوبتلة مالع قوف رقناو ةيسيئرلا
 Umbrella بيوبتلة تامالع إلى لوصولو كلذ دعب كنكمي. تامولعمل ءحولو ةباحس إلى لع ماع
 كئالچس ضرعل ذيقتنلل و CloudLock و قيقحتلل و

كنكمي. يضارثفا لكشب مايأ 7 رخآ نم تانايبلا راهظإل ةباحسلال نامأ قيبطت نييعت مت
نيميلال لىلأ دوجوملا خيراتلا قاطن قوف رقللاب ينمزللا راطلال رييغت:

ite Cloudlock Enforcement

2018-04-13 18:18 - 2018-04-19 18:18

2018-04-13 18:18

2018-04-19 18:18

18 : 18

18 : 18

< Apr 2018 >

Su	Mo	Tu	We	Th	Fr	Sa
25	26	27	28	29	30	31
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5

< May 2018 >

Su	Mo	Tu	We	Th	Fr	Sa
29	30	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2
3	4	5	6	7	8	9

Last 1 Day

Last 2 Days

Last 7 Days

Last 30 Days

This Month

Last Month

Custom Range

Apply

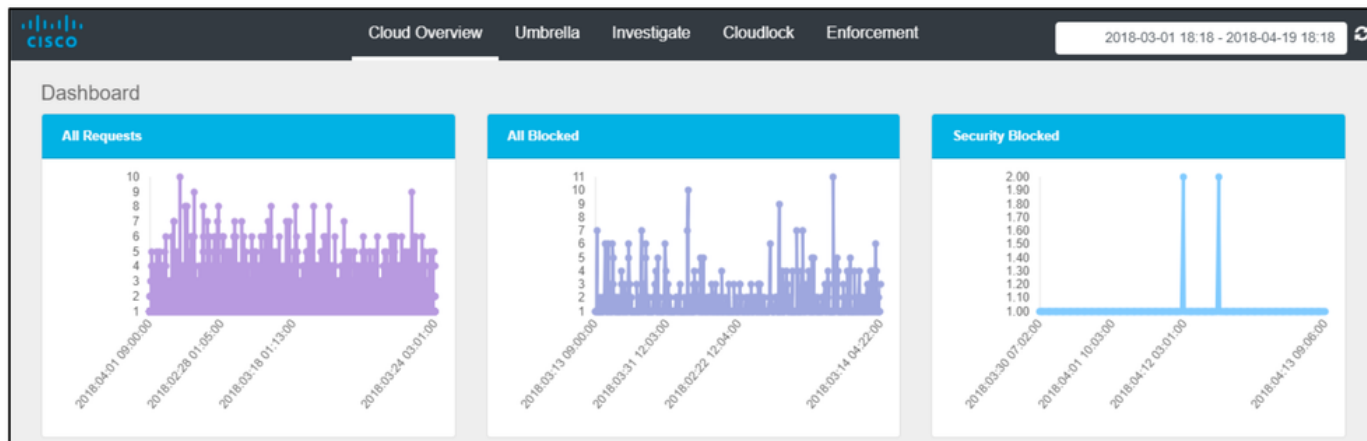
Cancel

360072030052

Cisco نم ةباحسلال نامأ قيبطت تانوكم

ةباحسلال لىلأ ةماع ةرظن

تايللمع لكو، تابللطال عيجم لثم تامولعم ةباحسلال لىلأ ةماع ةرظن بيوبتلا ةمالع ضرعت
ماع لكشب CloudLock ثداوحو، ةهوبشملا ةنمآلا ةبترللاو، DGA لامتحاو، نامألا عنمو، رطخال
ططخمالا لىلأ دننسملا ليئرملا ليثمتلا في فيزيومتلا نييتمملاو، ايلعلا هئلا



Likely DGA's		Suspicious Secure Rank ⓘ			
Destination	Last Queried	Destination	Securerank	Status Label	Last Queried
...	2018:06:05 01:11	...	5.64000	safe	2018:06:05 04:16
...	2018:06:02 09:01	...	-0.03000	malicious	2018:06:01 01:06
...	2018:06:05 01:15	...	-0.01000	malicious	2018:06:04 09:20
...	2018:06:02 11:04	...	-18.92000	malicious	2018:06:03 12:03
...	2018:06:08 11:05	...	-0.01000	malicious	2018:06:05 01:10
...	2018:06:02 01:09	...	...	...	...
...	2018:06:06 03:20	...	...	...	...
...	2018:06:04 01:07	...	...	...	...
...	2018:06:08 12:05	...	...	...	...

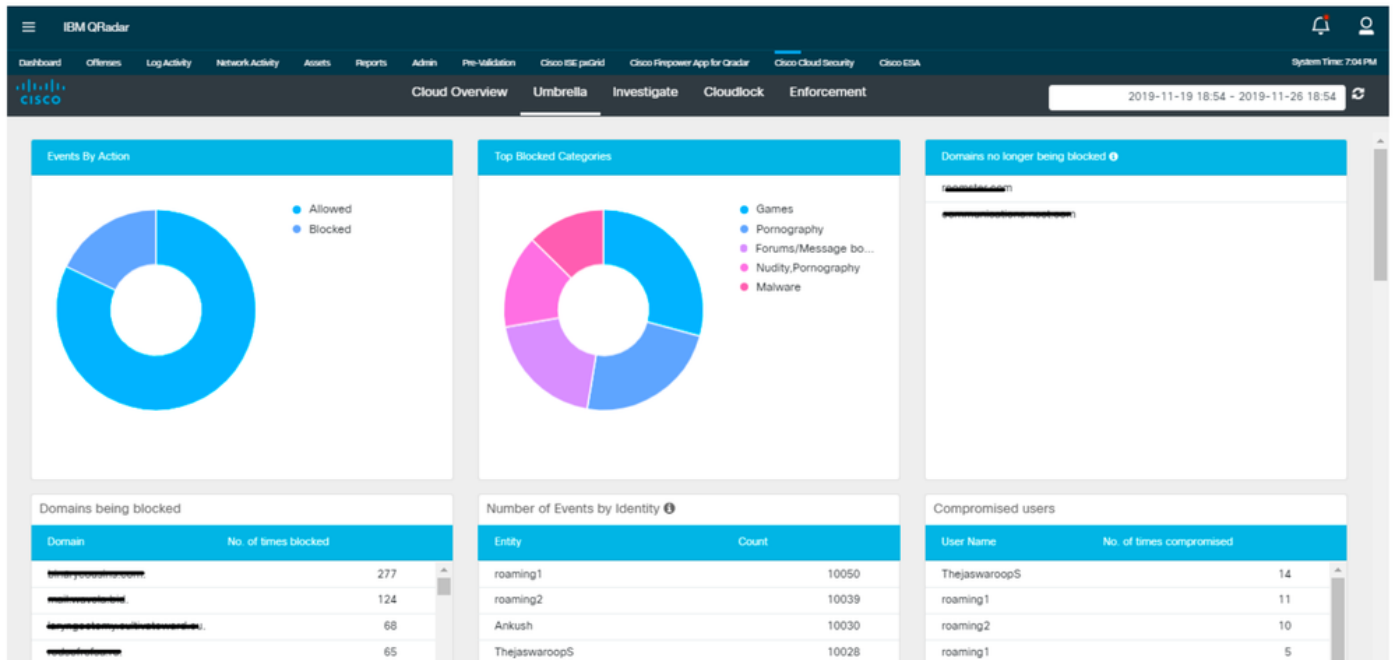
360072257631

Cloudlock Incidents		Cloudlock Top Policies		Cloudlock Top Offenders	
Status	Count	Policy	Count	User Name	Count
New	102548	Social Security Number	1	unknown user	3549
In Progress	12	New Unclassified App Installs	120	Sarat Kumar	3061
Dismissed	3	AppTest	102441	Anuraj C	2205
Resolved	2			Mohit Vaish	2002
				Kedar Bhat	1937
				Touseef Jagirdar	1893
				Rajeev Menon	1818
				Sameer Shelke	1814

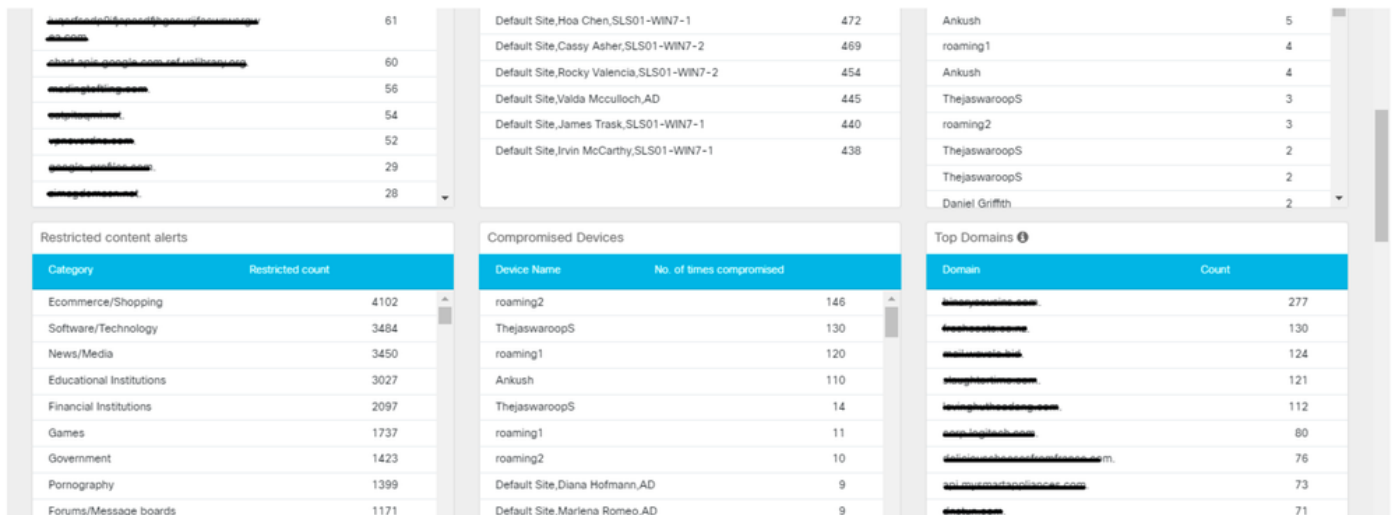
360072257611

Umbrella

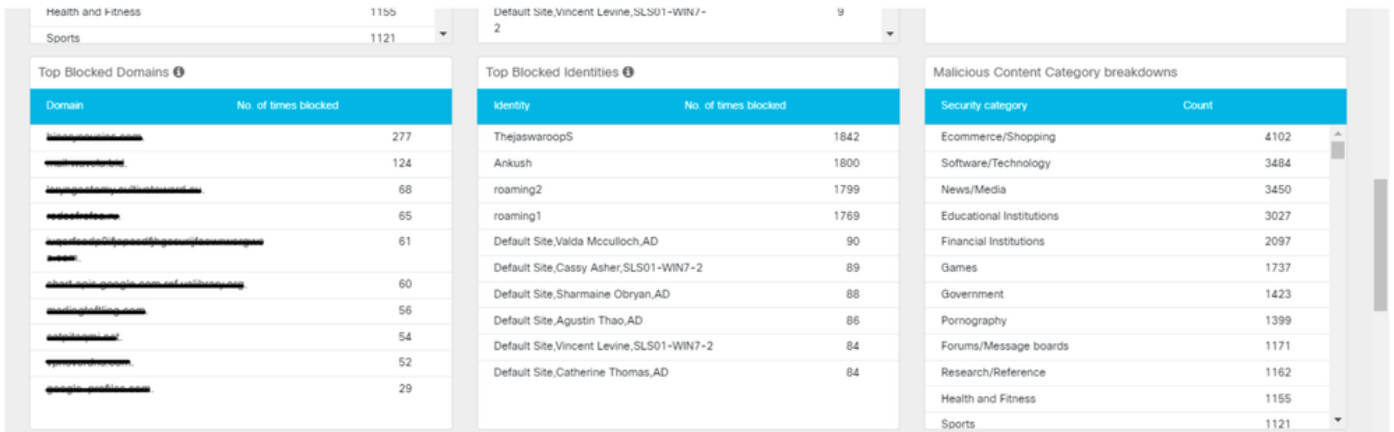
ةروطحم ل تائفلاو ،ءارجإل بسح ثادحألا لثم تامولعم "ةلظملا" بيوبتلا ةمالع ضرعت ةروطحم دعت مل يتي تالاجملاو ،اهرظح متي يتي تالاجملاو ،ةيوهلا بسح ثادحألا ددعو ،ايلعلا م يتي تالاجملاو ،ديقملا يوتحملا تاهيبننو ،رطخلل مهضيرعت مت نيذلا نيمدختسملو يوتحملا تائفلاطأو ،ايلعلا ةروطحملا تايوهلاو ،ةروطحملا ايلعلا تالاجملاو ،اهقارتخإ إلا دنتسم يئرمل ليثمت ي فمدختسمل لوصو هاجتاو طاشنلاو ،ايلعلا تائفلاو ،ةراضلا ططخملا.



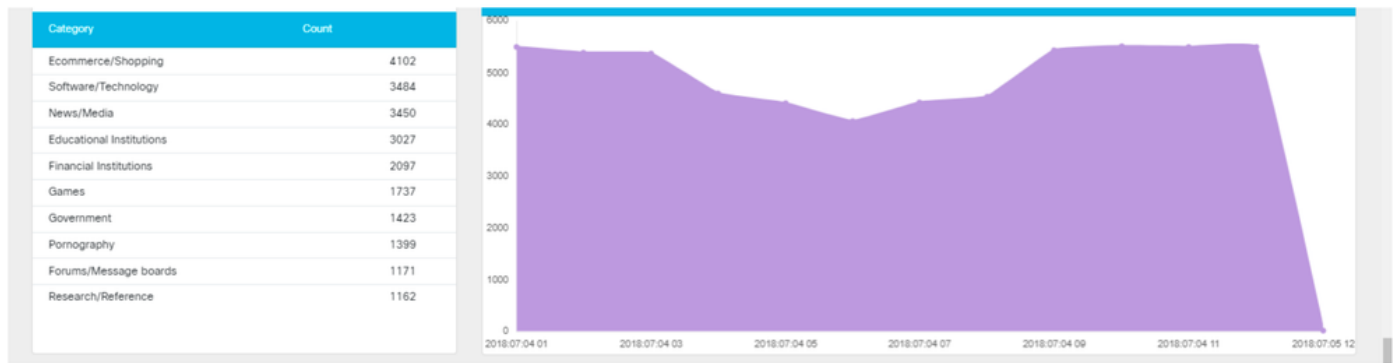
360072263411



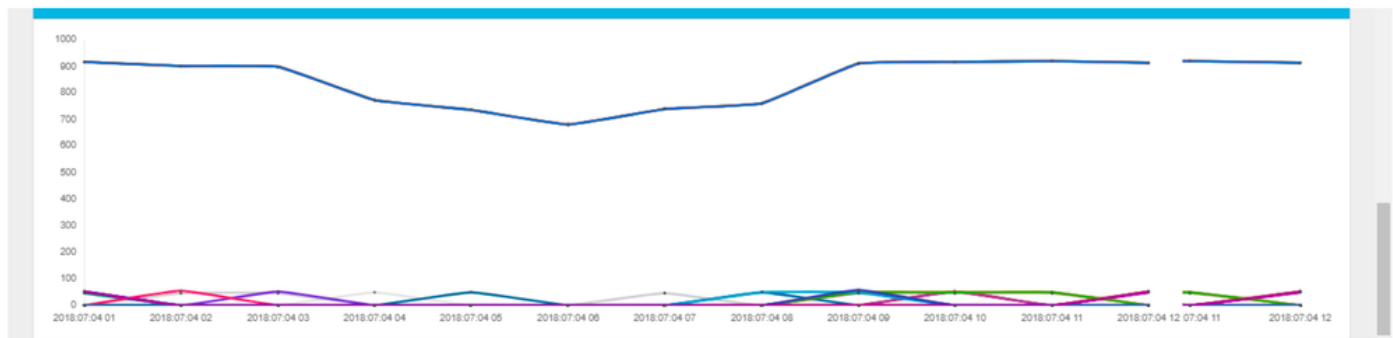
360072263391



360072037372



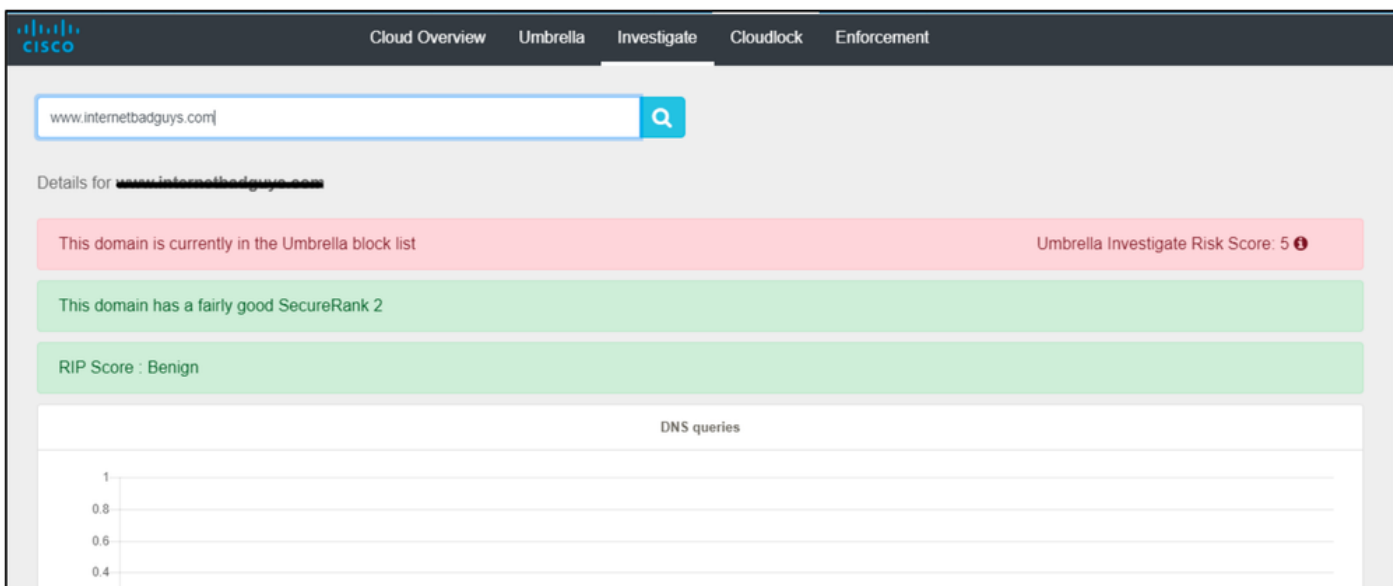
360072263331



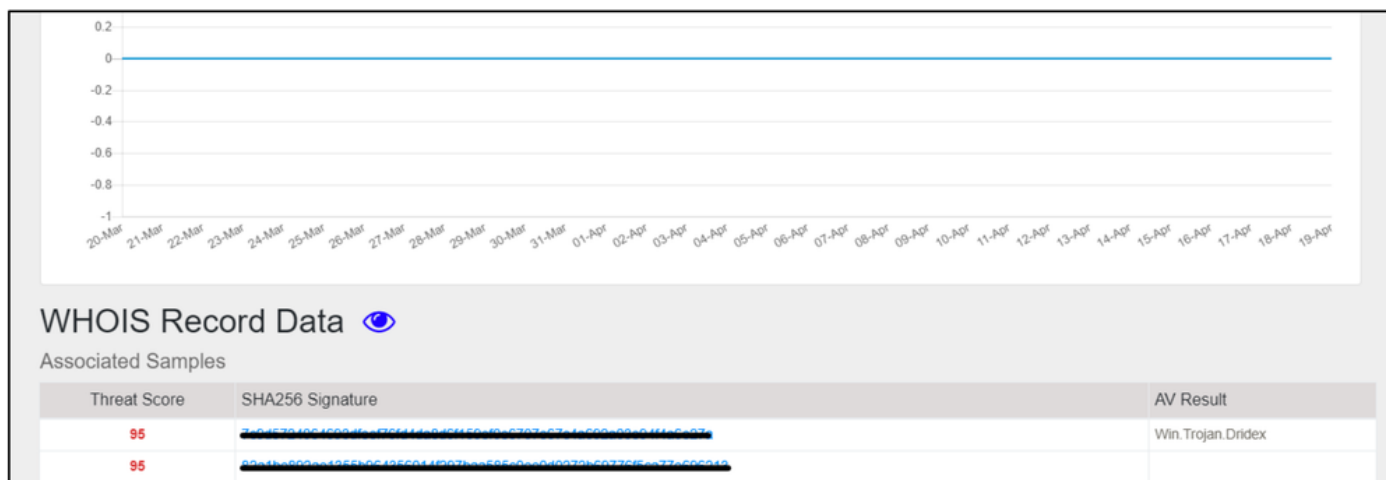
360072263351

ربختسن

مسابقة قلعتم الامولعمل الي ف شحبل نم مدختسم ال "ققيحتل" بيوبتل الةمالع نكمت يوتحي هنا امك .ينورتكلال دي ربل ناووع وةئجتل و IP و ASN و URL ناووع و ا فيضم ال كلذى الى امو DGA تامولعمو ،WHO لجس لثم تامولعملع



360072263511



Features	
TTLs min	1
TTLs max	1
TTLs mean	1
TTLs median	1
TTLs standard deviation	0
Country codes	US
Country count	1
ASNs	AS 36692
ASNs count	1
Prefixes	67 215.88.0
Prefixes count	1

CloudLock

Incidents									
Incident ID									
Q									
Id	Platform	Matches	Policy	Detected	Source	Owner	Severity	Status	Actions
132352847	office365	1	AppTest	Jun 03, 2018 5:20:13 pm	AzureActiveDirectory User Login Failed	unknown user	CRITIC	IN PRO	Update
132352852	office365	1	AppTest	Jun 03, 2018 5:24:23 pm	AzureActiveDirectory User Login Failed	Mohit Vaish	CRITIC	NEW	Update
132352856	office365	1	AppTest	Jun 03, 2018 5:24:39 pm	AzureActiveDirectory User Logg ed In	Khiladi Bayal	CRITIC	IN PROGRESS	Update
132490696	office365	1	AppTest	Jun 04, 2018 4:39:22 pm	AzureActiveDirectory User Logg ed In	Anil Kumar Yarl apalli	CRITIC	IN PRO	Update

٣. شَدَحْ لَ لَوْح لِي صَافَتِ لَ نَم دِي زَمِ ضَرَعَل شَا دَحْ أَلَا نَم يَا تَقُو دِي دَحَت نِي مَدَحَت سَمَلَل نَكَمِي

Incident Details

Objective Type

Name	Codesign Production
Platform	office365
Owner	██████████@aujas.com
Policy	New Unclassified App Installs
Time	
IP Address	
Status	NEW
Severity	ALERT

Detected	Match Type	Match
	New Unclassified App Install	s

360072042332

ضرف بي وبت ةمالع

نيم دخت سملل نكمي .اهرظح م تي تي تال تالاجملا نع تامولعم ظرف بي وبت تال ةمالع ضرعت ةهجالا هذه نم اهرظح ءاغلل ةروطح م تال تالاجملا ديحت اضيأ

cloud

CISCO

Cloud Overview

Umbrella

Investigate

Cloudlock

Enforcement

2018-04-13 18:18 - 2018-04-19 18:18

Blocked Domains

☐	Domain	Last Seen
☐	aujasdigital.com	Mar 16, 2018 9:46 AM
☐	havanacubanrealestate.co	Mar 28, 2018 11:47 AM

1 - 2 < >

Unblock

360072038472

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م ج ر ت
م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م ج ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م م ج ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م ج ر ت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا ة ا د ع و ج ر ل ا ب ي ص و ت و ت ا م ج ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems
(ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا