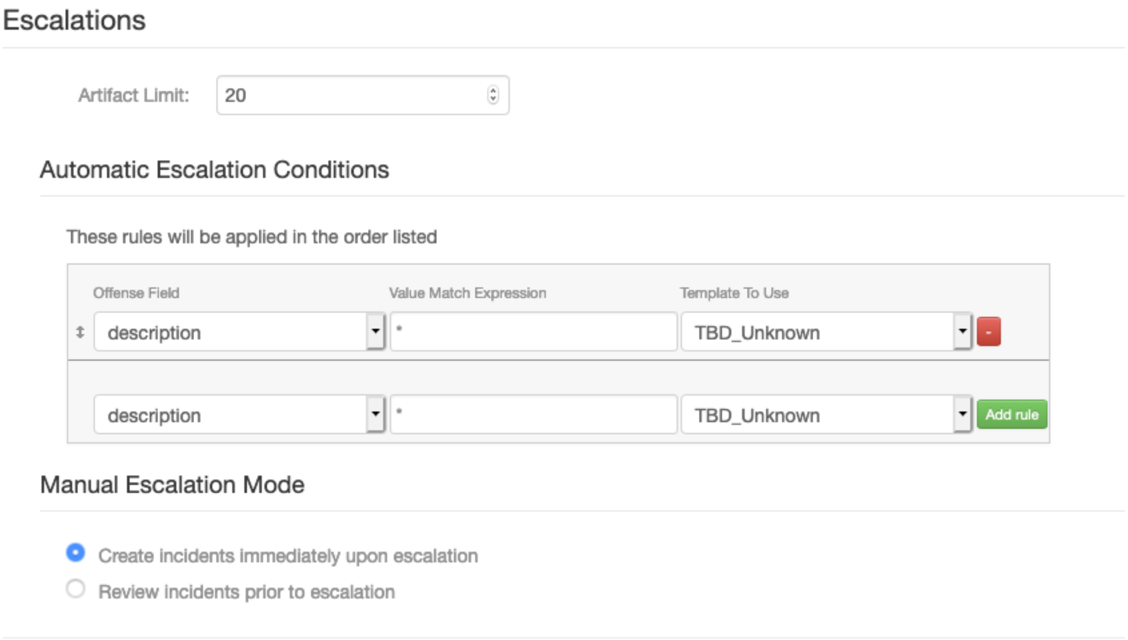
QRadar QROC – Resilient

Table of Contents

Alerte Escalation

Alert are transmitted automatically from QRadar to Resilient using the following configuration:



Escalations

Artifact Limit: 20

Automatic Escalation Conditions

These rules will be applied in the order listed

Offense Field	Value Match Expression	Template To Use	
description	*	TBD_Unknown	-
description	*	TBD_Unknown	Add rule

Manual Escalation Mode

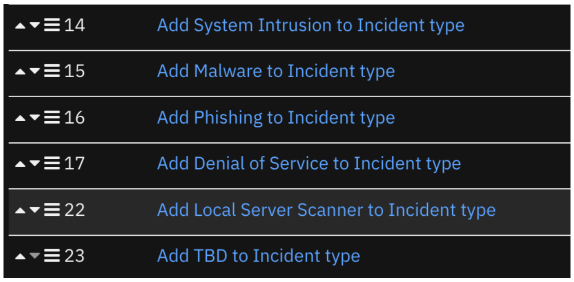
● Create incidents immediately upon escalation

○ Review incidents prior to escalation

The offense field must be set to: Name, or: Description
The value match expression must be set to: *
The Template To Use must be set to: TBD_Unknown

Incident assignment to correct Incident Type

A set of rules will assign the incident to a correct incident type based on keywords matching on field Description:



14	Add System Intrusion to Incident type
15	Add Malware to Incident type
16	Add Phishing to Incident type
17	Add Denial of Service to Incident type
22	Add Local Server Scanner to Incident type
23	Add TBD to Incident type

Out of the Box playbooks on default Incident Type:

- System Intrusion: CnC, exploit, Intrusion
- Malware: Virus, Malware
- Phishing: Spam, Phishing, Spear
- Denial of Service: Denial of Service, DOS, DDOS

Specific Playbook on Offense type:

- Local Server Scanner: Scan
- (More to come)

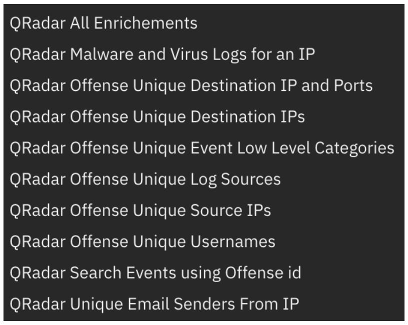
If needed; the list of keywords can be change for more matching or a better matching based on customer experience and offense list.

Query from Resilient to QRadar

A set of Queries can be done by the analyst, at will, from actions button when he needs more information.

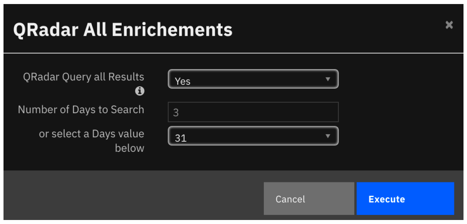
Queries at the Incident Level

List of Queries available:



QRadar All Enrichements
QRadar Malware and Virus Logs for an IP
QRadar Offense Unique Destination IP and Ports
QRadar Offense Unique Destination IPs
QRadar Offense Unique Event Low Level Categories
QRadar Offense Unique Log Sources
QRadar Offense Unique Source IPs
QRadar Offense Unique Usernames
QRadar Search Events using Offense id
QRadar Unique Email Senders From IP

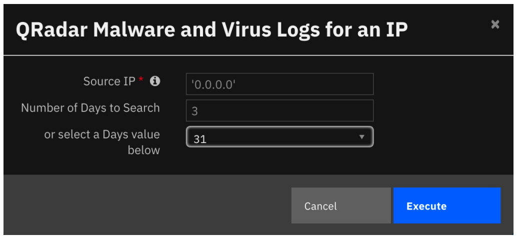
- **QRadar All Enrichments**
  will launch all above queries at once (expect Malware #2 and Email #10) using the following options:
  Get all Results (Top 100) or partial response (Default All)
  Specify a number of days to search back from current day 1, 7, 15, 31, 92, or your number. Default is 31:



QRadar All Enrichements

QRadar Query all Results: Yes
Number of Days to Search: 3
or select a Days value below: 31

- **QRadar Malware and Virus Logs for an IP**
  Description: For a given source IP address, return all the malware logs.
  The package ***IBM QRadar Cryptomining Content Extension*** must be installed to populate the values in QRadar. Please follow the instructions at https://exchange.xforce.ibmcloud.com/hub/extension/62fdde6955e3ee6937c819174d5758bb
  Query: SELECT QIDNAME(qid) AS "EventName", LOGSOURCENAME(logsourceid) AS "LogSource", "Threat Name", eventCount, DATEFORMAT(starttime, 'YYYY-MM-dd HH:mm') as "StartTime", CATEGORYNAME(category) AS "LowLevelCategory", username, sourceip, destinationip FROM events WHERE sourceip = ({source_ip}) AND CATEGORYNAME(highlevelcategory) = 'Malware' GROUP BY "Threat Name", username, eventCount ORDER BY eventCount DESC LIMIT 100 LAST ({days to search}) DAYS
  Note: This query is not launched by the QRadar All Enrichment and required specific Source IP address input addition:



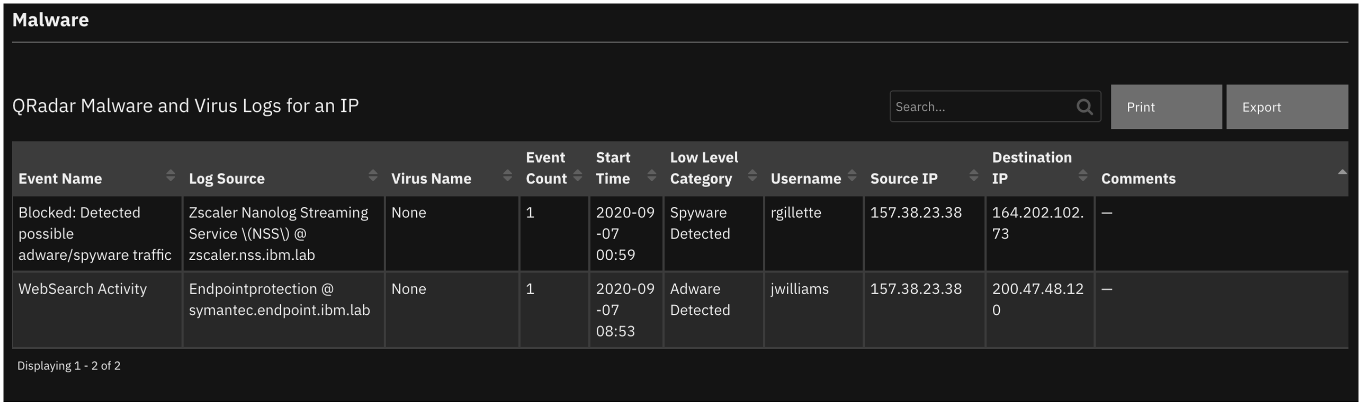
QRadar Malware and Virus Logs for an IP

Source IP * '0.0.0.0'

Number of Days to Search 3

or select a Days value below 31

Result is visible in QRadar Table:



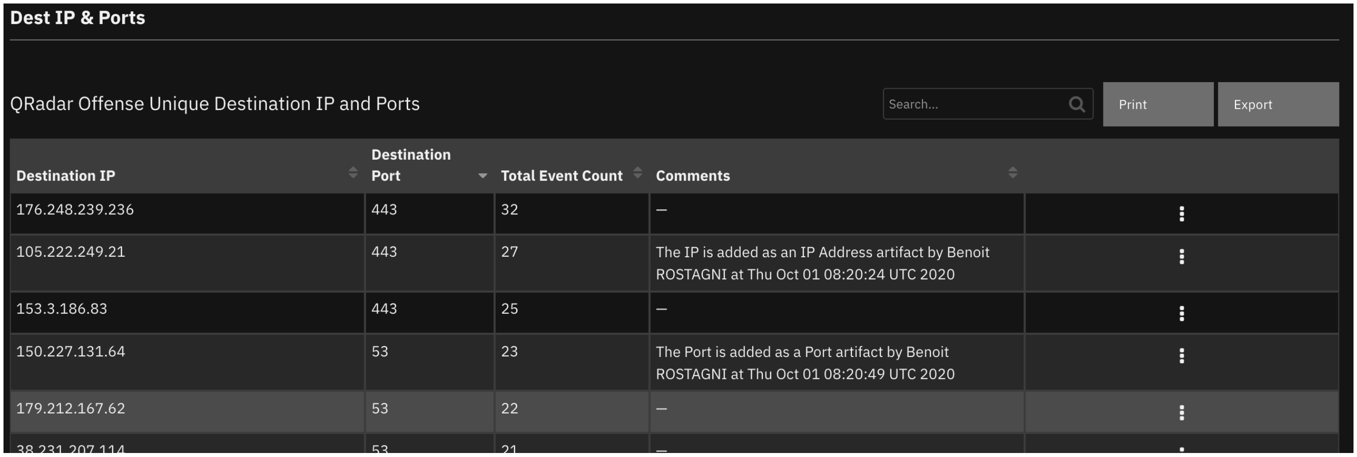
Malware

QRadar Malware and Virus Logs for an IP

Event Name	Log Source	Virus Name	Event Count	Start Time	Low Level Category	Username	Source IP	Destination IP	Comments
Blocked: Detected possible adware/spyware traffic	Zscaler Nanolog Streaming Service \(NSS\) @ zscaler.nss.ibm.lab	None	1	2020-09-07 00:59	Spyware Detected	rgillette	157.38.23.38	164.202.102.73	—
WebSearch Activity	Endpointprotection @ symantec.endpoint.ibm.lab	None	1	2020-09-07 08:53	Adware Detected	jwilliams	157.38.23.38	200.47.48.120	—

Displaying 1 - 2 of 2

- **QRadar Offense Unique Destination IP and Ports**
  Description: For a given offense ID, return all the unique combinations of destination IP and destination port and their counts from all the events associated with this offense ID
  Query: SELECT destinationip, destinationport, SUM(eventCount) AS "totaleventcount" FROM events WHERE InOffense({id}) GROUP BY destinationip, destinationport ORDER BY totaleventcount DESC LIMIT 100 LAST ({days to search}) DAYS
  Result is visible in QRadar Table:

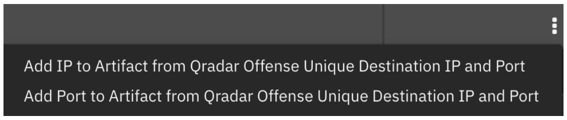


Dest IP & Ports

QRadar Offense Unique Destination IP and Ports

Destination IP	Destination Port	Total Event Count	Comments	
176.248.239.236	443	32	—	⋮
105.222.249.21	443	27	The IP is added as an IP Address artifact by Benoit ROSTAGNI at Thu Oct 01 08:20:24 UTC 2020	⋮
153.3.186.83	443	25	—	⋮
150.227.131.64	53	23	The Port is added as a Port artifact by Benoit ROSTAGNI at Thu Oct 01 08:20:49 UTC 2020	⋮
179.212.167.62	53	22	—	⋮
38.231.207.114	53	21	—	⋮

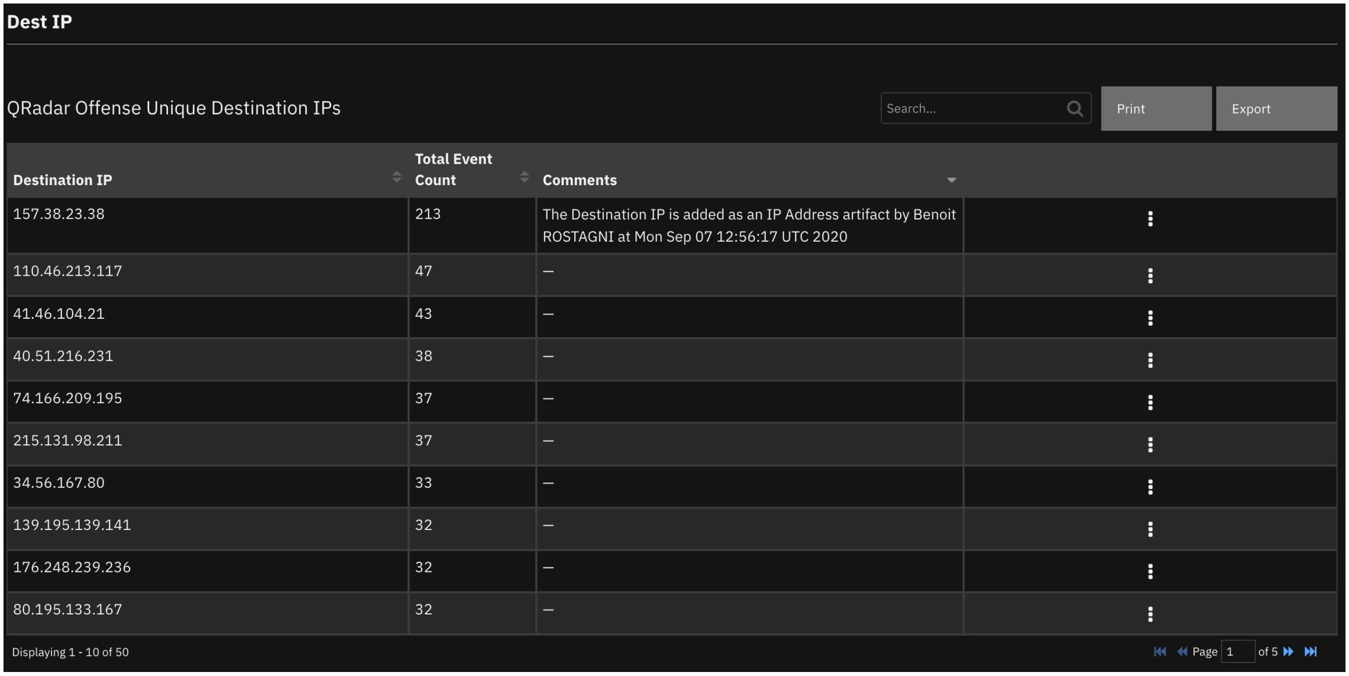
Action can be done from the action menu to populate artifacts from this table:



⋮
Add IP to Artifact from Qradar Offense Unique Destination IP and Port
Add Port to Artifact from Qradar Offense Unique Destination IP and Port

- **QRadar Offense Unique Destination Ips**
  Description: For a given offense ID, return all the unique destination IPs and their counts from all the events associated with this offense ID
  Query: SELECT destinationip, SUM(eventCount) AS "totaleventcount" FROM events WHERE InOffense({id}) GROUP BY destinationip ORDER BY totaleventcount DESC LIMIT 100 LAST

({days to search}) DAYS
Result is visible in QRadar Table:



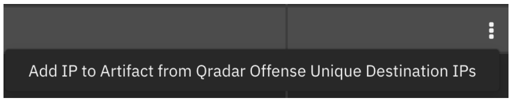
Dest IP

QRadar Offense Unique Destination IPs

Destination IP	Total Event Count	Comments	
157.38.23.38	213	The Destination IP is added as an IP Address artifact by Benoit ROSTAGNI at Mon Sep 07 12:56:17 UTC 2020	⋮
110.46.213.117	47	—	⋮
41.46.104.21	43	—	⋮
40.51.216.231	38	—	⋮
74.166.209.195	37	—	⋮
215.131.98.211	37	—	⋮
34.56.167.80	33	—	⋮
139.195.139.141	32	—	⋮
176.248.239.236	32	—	⋮
80.195.133.167	32	—	⋮

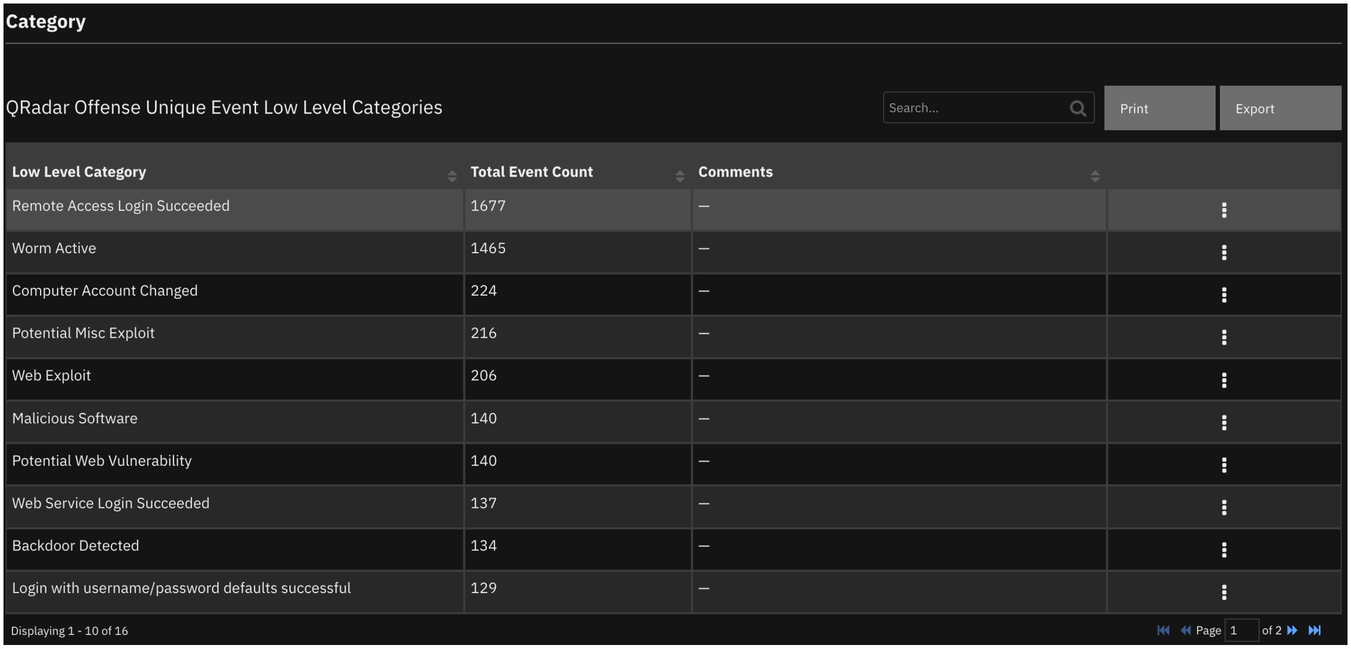
Displaying 1 - 10 of 50

Action can be done from the action menu to populate artifacts from this table:



Add IP to Artifact from Qradar Offense Unique Destination IPs

- **QRadar Offense Unique Event Low Level Categories**
  Description: For a given offense ID, return all the unique low level categories and their counts from all the events associated with this offense ID
  Query: SELECT CATEGORYNAME(category) AS "lowlevelcategory", SUM(eventCount) AS "totaleventcount" FROM events WHERE InOffense({id}) GROUP BY category ORDER BY totaleventcount DESC LIMIT 100 LAST ({days to search}) DAYS
  Result is visible in QRadar Table:



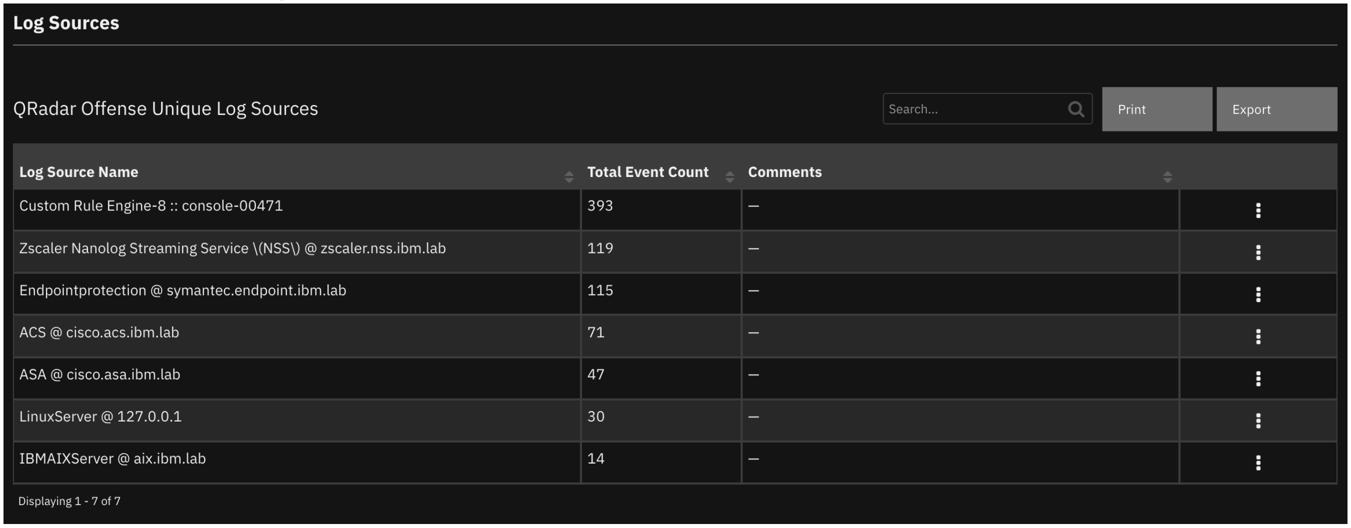
Category

QRadar Offense Unique Event Low Level Categories

Low Level Category	Total Event Count	Comments	
Remote Access Login Succeeded	1677	—	⋮
Worm Active	1465	—	⋮
Computer Account Changed	224	—	⋮
Potential Misc Exploit	216	—	⋮
Web Exploit	206	—	⋮
Malicious Software	140	—	⋮
Potential Web Vulnerability	140	—	⋮
Web Service Login Succeeded	137	—	⋮
Backdoor Detected	134	—	⋮
Login with username/password defaults successful	129	—	⋮

Displaying 1 - 10 of 16

- **QRadar Offense Unique Log Sources**
  Description: For a given offense ID, return all the unique log sources and their counts from all the events associated with this offense ID
  Query: SELECT LOGSOURCENAME(logsourceid) AS "LogSourceName", SUM(eventCount) AS "totaleventcount" FROM events WHERE InOffense({id}) GROUP BY logsourceid ORDER BY totaleventcount DESC LIMIT 100 LAST ({days to search}) DAYS
  Result is visible in QRadar Table:



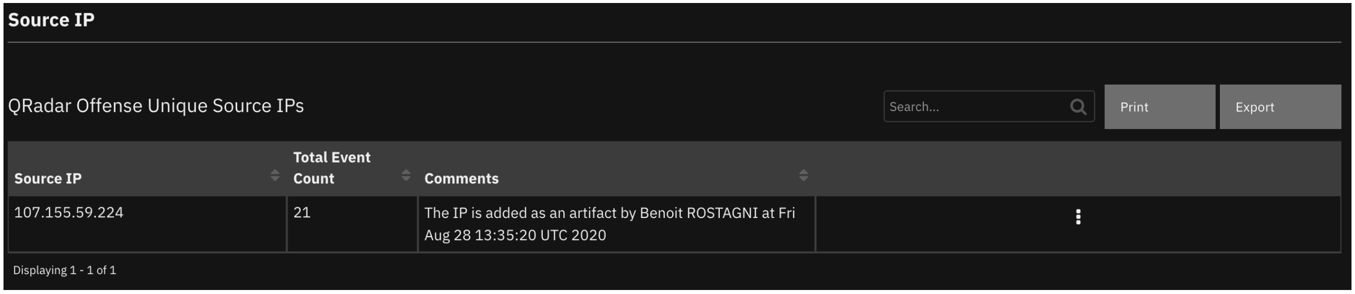
Log Sources

QRadar Offense Unique Log Sources

Log Source Name	Total Event Count	Comments	
Custom Rule Engine-8 :: console-00471	393	–	⋮
Zscaler Nanolog Streaming Service \(NSS\) @ zscaler.nss.ibm.lab	119	–	⋮
Endpointprotection @ symantec.endpoint.ibm.lab	115	–	⋮
ACS @ cisco.acs.ibm.lab	71	–	⋮
ASA @ cisco.asa.ibm.lab	47	–	⋮
LinuxServer @ 127.0.0.1	30	–	⋮
IBMAIXServer @ aix.ibm.lab	14	–	⋮

Displaying 1 - 7 of 7

- **QRadar Offense Unique Source Ips**
  Description: For a given offense ID, return all the unique source IPs and their counts from all the events associated with this offense ID
  Query: SELECT sourceip, SUM(eventCount) AS "totaleventcount" FROM events WHERE InOffense({id}) GROUP BY sourceip ORDER BY totaleventcount DESC LIMIT 100 LAST ({days to search}) DAYS
  Result is visible in QRadar Table:



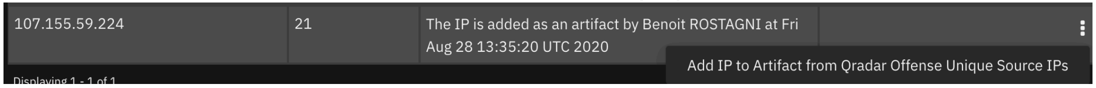
Source IP

QRadar Offense Unique Source IPs

Source IP	Total Event Count	Comments	
107.155.59.224	21	The IP is added as an artifact by Benoit ROSTAGNI at Fri Aug 28 13:35:20 UTC 2020	⋮

Displaying 1 - 1 of 1

Action can be done from the action menu to populate artifacts from this table:



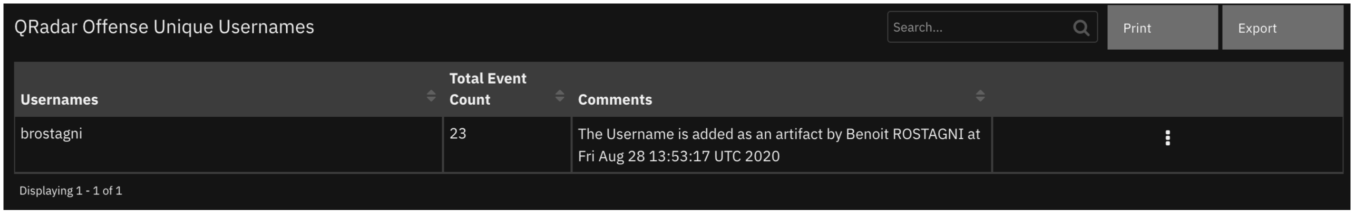
107.155.59.224	21	The IP is added as an artifact by Benoit ROSTAGNI at Fri Aug 28 13:35:20 UTC 2020	⋮

Displaying 1 - 1 of 1

- **QRadar Offense Unique Usernames**
  Description: For a given offense ID, return all the unique usernames and their counts from all the events associated with this offense ID
  Query: SELECT username, SUM(eventCount) AS "totaleventcount" FROM events WHERE InOffense({id}) GROUP BY username ORDER BY totaleventcount DESC LIMIT 100 LAST ({days

to search}) DAYS

Result is visible in QRadar Table:

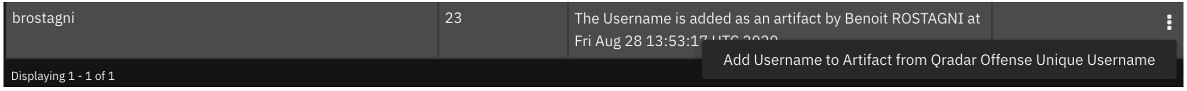


QRadar Offense Unique Usernames

Usernames	Total Event Count	Comments
brostagni	23	The Username is added as an artifact by Benoit ROSTAGNI at Fri Aug 28 13:53:17 UTC 2020

Displaying 1 - 1 of 1

Action can be done from the action menu to populate artifacts from this table:

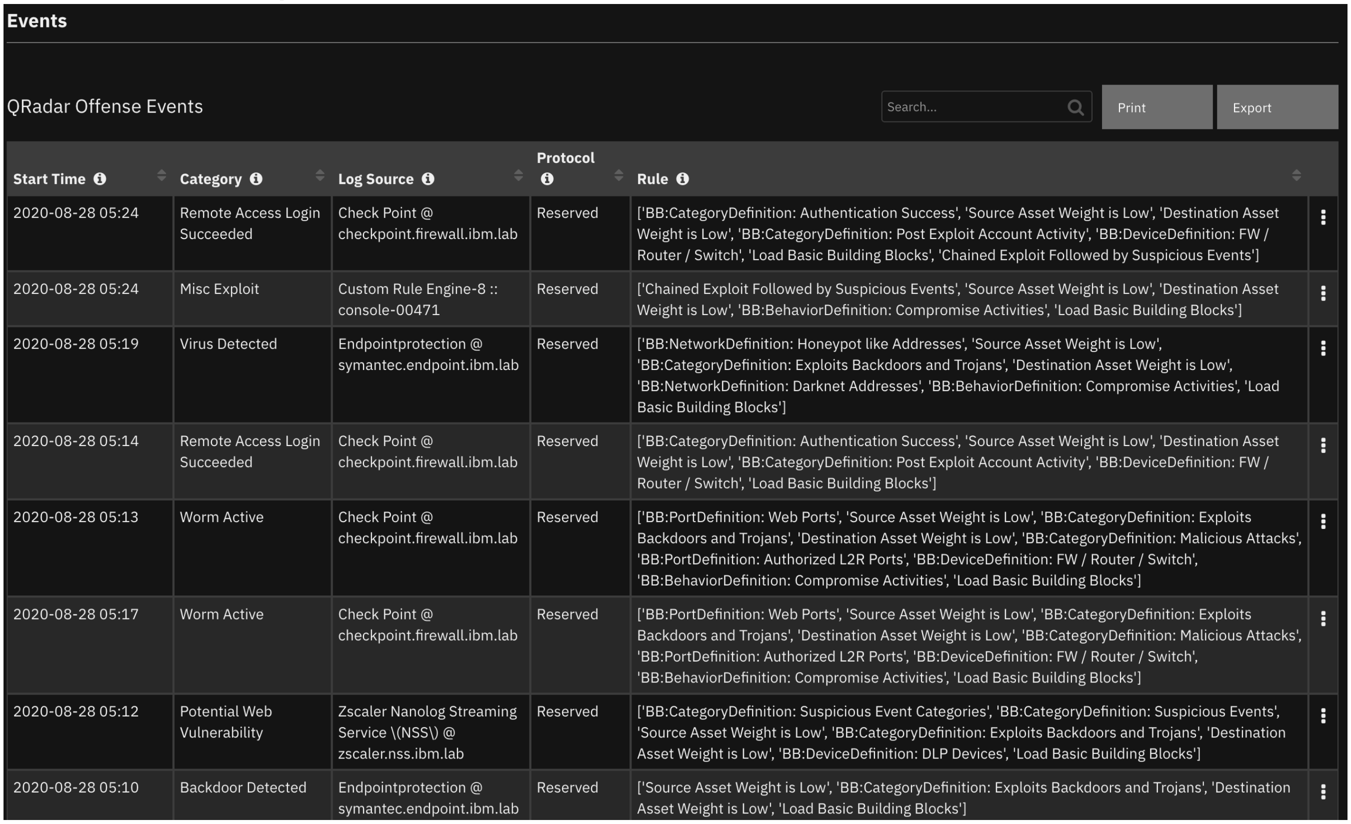


brostagni	23	The Username is added as an artifact by Benoit ROSTAGNI at Fri Aug 28 13:53:1

Add Username to Artifact from Qradar Offense Unique Username

Displaying 1 - 1 of 1

- **QRadar Offense Events using Offense id**
  Description: Use the qradar_id field of the incident to search qradar events, and update the data table, qradar_offense_event, with all results.
  Query: SELECT DATEFORMAT(starttime, 'YYYY-MM-dd HH:mm') as StartTime, CATEGORYNAME(category), LOGSOURCENAME(logsourceid), PROTOCOLNAME(protocolid), RULENAME(creeventlist)FROM events WHERE INOFFENSE({id}) LIMIT 100 LAST ({days to search}) DAYS
  Result is visible in QRadar Table:



Events

QRadar Offense Events

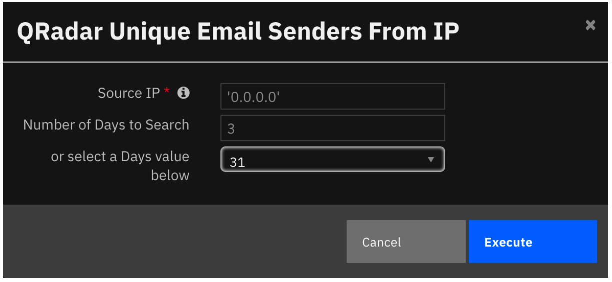
Start Time	Category	Log Source	Protocol	Rule
2020-08-28 05:24	Remote Access Login Succeeded	Check Point @ checkpoint.firewall.ibm.lab	Reserved	['BB:CategoryDefinition: Authentication Success', 'Source Asset Weight is Low', 'Destination Asset Weight is Low', 'BB:CategoryDefinition: Post Exploit Account Activity', 'BB:DeviceDefinition: FW / Router / Switch', 'Load Basic Building Blocks', 'Chained Exploit Followed by Suspicious Events']
2020-08-28 05:24	Misc Exploit	Custom Rule Engine-8 :: console-00471	Reserved	['Chained Exploit Followed by Suspicious Events', 'Source Asset Weight is Low', 'Destination Asset Weight is Low', 'BB:BehaviorDefinition: Compromise Activities', 'Load Basic Building Blocks']
2020-08-28 05:19	Virus Detected	Endpointprotection @ symantec.endpoint.ibm.lab	Reserved	['BB:NetworkDefinition: Honeypot like Addresses', 'Source Asset Weight is Low', 'BB:CategoryDefinition: Exploits Backdoors and Trojans', 'Destination Asset Weight is Low', 'BB:NetworkDefinition: Darknet Addresses', 'BB:BehaviorDefinition: Compromise Activities', 'Load Basic Building Blocks']
2020-08-28 05:14	Remote Access Login Succeeded	Check Point @ checkpoint.firewall.ibm.lab	Reserved	['BB:CategoryDefinition: Authentication Success', 'Source Asset Weight is Low', 'Destination Asset Weight is Low', 'BB:CategoryDefinition: Post Exploit Account Activity', 'BB:DeviceDefinition: FW / Router / Switch', 'Load Basic Building Blocks']
2020-08-28 05:13	Worm Active	Check Point @ checkpoint.firewall.ibm.lab	Reserved	['BB:PortDefinition: Web Ports', 'Source Asset Weight is Low', 'BB:CategoryDefinition: Exploits Backdoors and Trojans', 'Destination Asset Weight is Low', 'BB:CategoryDefinition: Malicious Attacks', 'BB:PortDefinition: Authorized L2R Ports', 'BB:DeviceDefinition: FW / Router / Switch', 'BB:BehaviorDefinition: Compromise Activities', 'Load Basic Building Blocks']
2020-08-28 05:17	Worm Active	Check Point @ checkpoint.firewall.ibm.lab	Reserved	['BB:PortDefinition: Web Ports', 'Source Asset Weight is Low', 'BB:CategoryDefinition: Exploits Backdoors and Trojans', 'Destination Asset Weight is Low', 'BB:CategoryDefinition: Malicious Attacks', 'BB:PortDefinition: Authorized L2R Ports', 'BB:DeviceDefinition: FW / Router / Switch', 'BB:BehaviorDefinition: Compromise Activities', 'Load Basic Building Blocks']
2020-08-28 05:12	Potential Web Vulnerability	Zscaler Nanolog Streaming Service \(NSS\) @ zscaler.nss.ibm.lab	Reserved	['BB:CategoryDefinition: Suspicious Event Categories', 'BB:CategoryDefinition: Suspicious Events', 'Source Asset Weight is Low', 'BB:CategoryDefinition: Exploits Backdoors and Trojans', 'Destination Asset Weight is Low', 'BB:DeviceDefinition: DLP Devices', 'Load Basic Building Blocks']
2020-08-28 05:10	Backdoor Detected	Endpointprotection @ symantec.endpoint.ibm.lab	Reserved	['Source Asset Weight is Low', 'BB:CategoryDefinition: Exploits Backdoors and Trojans', 'Destination Asset Weight is Low', 'Load Basic Building Blocks']

- **QRadar Unique Email Senders From IP**
  Description: For a given source IP address, return all the unique email senders and their counts
  The package *IBM QRadar Phishing and Email Content Extension* must be installed to populate the values in QRadar. Please follow the instructions at

https://exchange.xforce.ibmcloud.com/hub/extension/d47bae0e01d42970c272dcc773eed3bf

Query: SELECT Sender, SUM(eventCount) AS "totaleventcount" FROM events WHERE sourceip = '{source_ip}' GROUP BY Sender ORDER BY totaleventcount DESC LIMIT 100 LAST ({days to search}) DAYS

Note: This query is not launched by the QRadar All Enrichment and required specific Source IP address input addition :



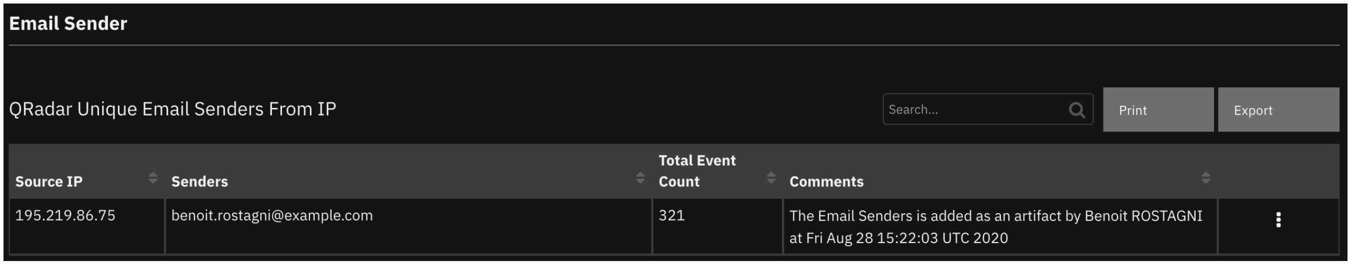
QRadar Unique Email Senders From IP

Source IP * : '0.0.0.0'

Number of Days to Search: 3

or select a Days value below: 31

Result is visible in QRadar Table:

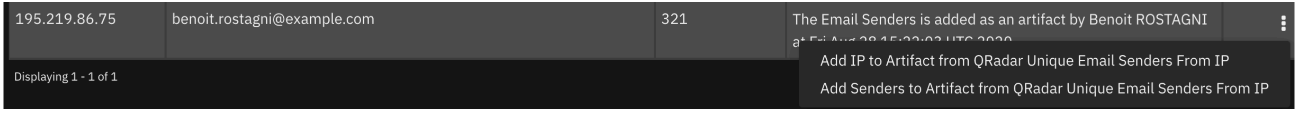


Email Sender

QRadar Unique Email Senders From IP

Source IP	Senders	Total Event Count	Comments	
195.219.86.75	benoit.rostagni@example.com	321	The Email Senders is added as an artifact by Benoit ROSTAGNI at Fri Aug 28 15:22:03 UTC 2020	⋮

Actions can be done from the action menu to populate artifacts from this table:



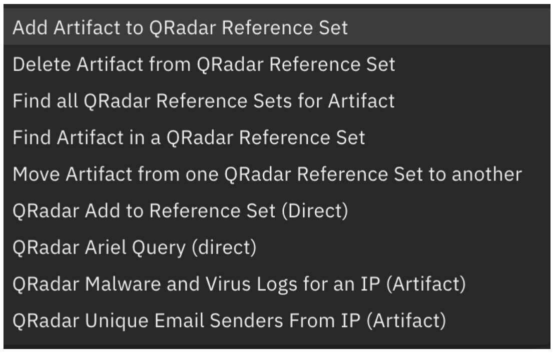
195.219.86.75	benoit.rostagni@example.com	321	The Email Senders is added as an artifact by Benoit ROSTAGNI	⋮

Displaying 1 - 1 of 1

Add IP to Artifact from QRadar Unique Email Senders From IP
Add Senders to Artifact from QRadar Unique Email Senders From IP

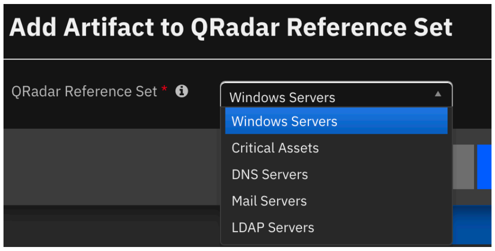
Queries at the Artifact Level

List of Queries available:



Add Artifact to QRadar Reference Set
Delete Artifact from QRadar Reference Set
Find all QRadar Reference Sets for Artifact
Find Artifact in a QRadar Reference Set
Move Artifact from one QRadar Reference Set to another
QRadar Add to Reference Set (Direct)
QRadar Ariel Query (direct)
QRadar Malware and Virus Logs for an IP (Artifact)
QRadar Unique Email Senders From IP (Artifact)

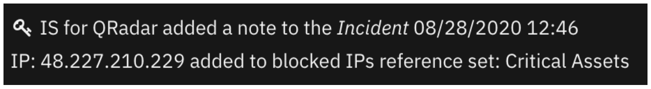
- **Add Artifact to QRadar Reference Set**
  Description: offer a list of Reference Set configured in QRadar from the Resilient App to be selected. Will add the artifact in the list.



Add Artifact to QRadar Reference Set

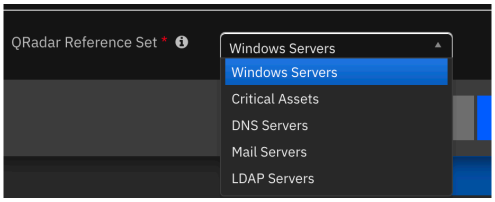
QRadar Reference Set * Windows Servers

Result is written in a Note:



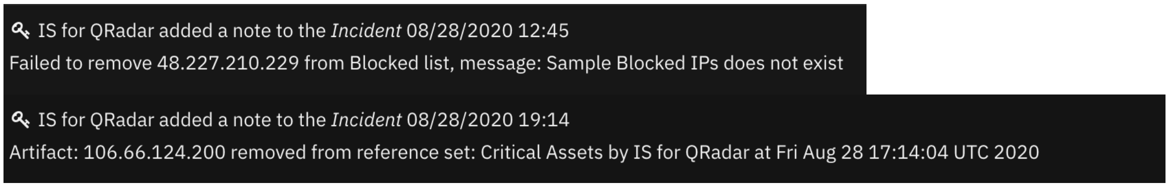
IS for QRadar added a note to the *Incident* 08/28/2020 12:46
IP: 48.227.210.229 added to blocked IPs reference set: Critical Assets

- **Delete Artifact from QRadar Reference Set**
  Description: offer a list of Reference Set configured in QRadar from the Resilient App to be selected. Will delete the artifact in the list.



QRadar Reference Set * Windows Servers

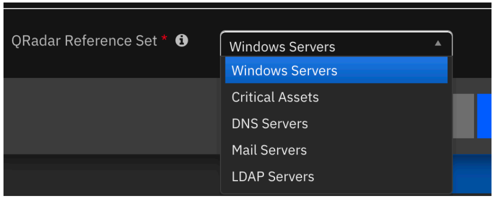
Result is written in a Note:



IS for QRadar added a note to the *Incident* 08/28/2020 12:45
Failed to remove 48.227.210.229 from Blocked list, message: Sample Blocked IPs does not exist

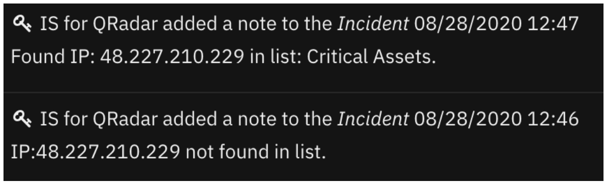
IS for QRadar added a note to the *Incident* 08/28/2020 19:14
Artifact: 106.66.124.200 removed from reference set: Critical Assets by IS for QRadar at Fri Aug 28 17:14:04 UTC 2020

- **Find Artifact in a QRadar Reference Set**
  Description: offer a list of Reference Set configured in QRadar from the Resilient App to be selected. Will say if the artifact is in the list.



QRadar Reference Set * Windows Servers

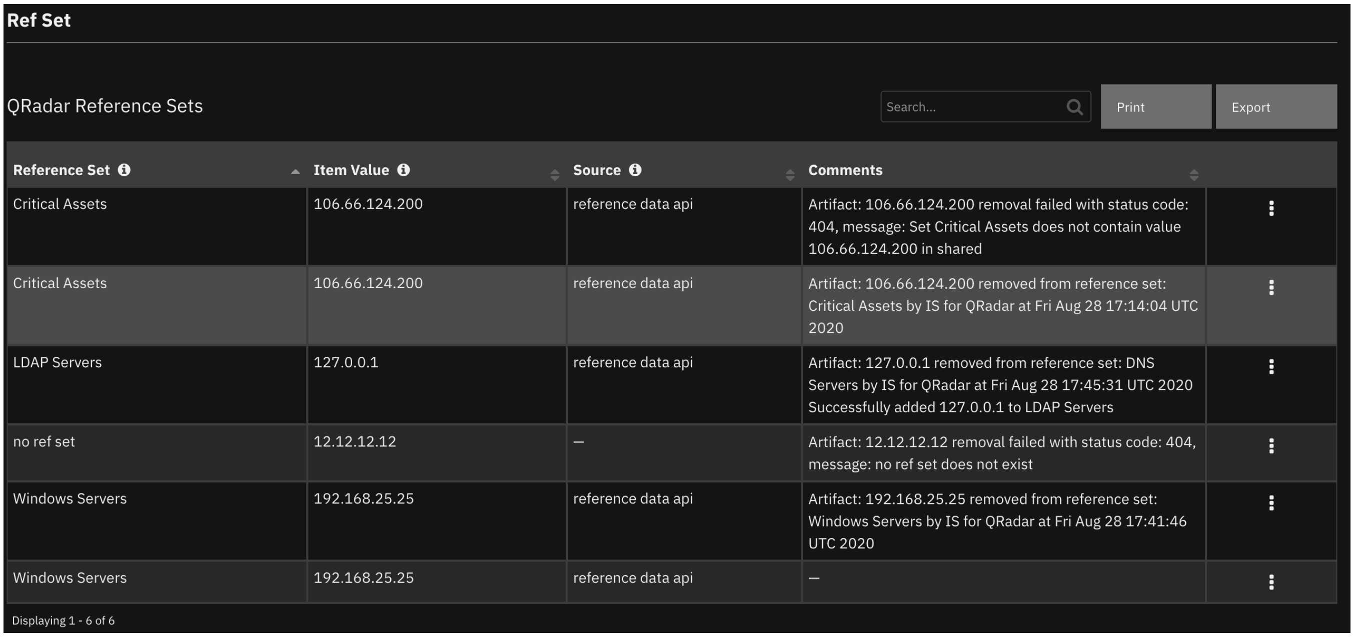
Result is written in a Note:



IS for QRadar added a note to the *Incident* 08/28/2020 12:47
Found IP: 48.227.210.229 in list: Critical Assets.

IS for QRadar added a note to the *Incident* 08/28/2020 12:46
IP:48.227.210.229 not found in list.

- **Find all QRadar Reference Sets for Artifact**
  Description: Will list in QRadar Reference Set table all Reference Sets where this artifact exist.



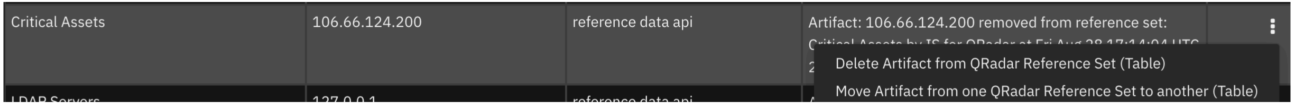
Ref Set

QRadar Reference Sets

Reference Set	Item Value	Source	Comments
Critical Assets	106.66.124.200	reference data api	Artifact: 106.66.124.200 removal failed with status code: 404, message: Set Critical Assets does not contain value 106.66.124.200 in shared
Critical Assets	106.66.124.200	reference data api	Artifact: 106.66.124.200 removed from reference set: Critical Assets by IS for QRadar at Fri Aug 28 17:14:04 UTC 2020
LDAP Servers	127.0.0.1	reference data api	Artifact: 127.0.0.1 removed from reference set: DNS Servers by IS for QRadar at Fri Aug 28 17:45:31 UTC 2020 Successfully added 127.0.0.1 to LDAP Servers
no ref set	12.12.12.12	–	Artifact: 12.12.12.12 removal failed with status code: 404, message: no ref set does not exist
Windows Servers	192.168.25.25	reference data api	Artifact: 192.168.25.25 removed from reference set: Windows Servers by IS for QRadar at Fri Aug 28 17:41:46 UTC 2020
Windows Servers	192.168.25.25	reference data api	–

Displaying 1 - 6 of 6

Actions can be done from the action menu to populate artifacts from this table:



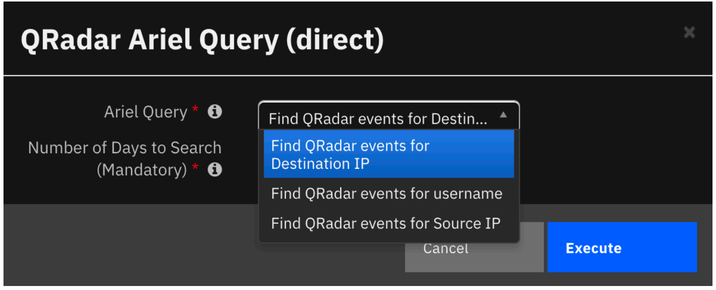
Critical Assets	106.66.124.200	reference data api	Artifact: 106.66.124.200 removed from reference set:

Delete Artifact from QRadar Reference Set (Table)
Move Artifact from one QRadar Reference Set to another (Table)

- **Move Artifact from one QRadar Reference Set to another**
  Note : Currently not enable but should be in the future.
  (Just the default non configured sample)

- **QRadar Add to Reference Set (Direct)**
  Description: Similar to Add Artifact to QRadar Reference Set, but using another order path.

- **QRadar Ariel Query (direct)**
  Description: will launch the preconfigured Queries in Resilient App on QRadar. By default, you will have access to the 3 following Queries:



QRadar Ariel Query (direct)

Ariel Query *: Find QRadar events for Destin...

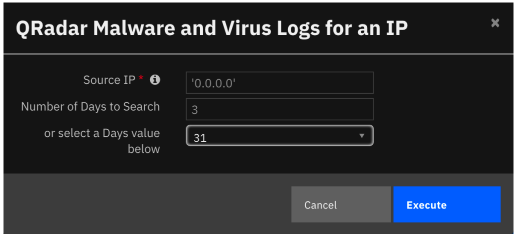
Number of Days to Search (Mandatory) *

Find QRadar events for Destination IP
Find QRadar events for username
Find QRadar events for Source IP
Cancel
Execute

The result is store in a log text file in attachment to the incident.
We recommend using these queries when a lot of results (hundreds, thousands…) are expected.

- **QRadar Malware and Virus Logs for an IP (Artifact)**
  Description: For a given source IP address, return all the malware logs.
  The package *IBM QRadar Cryptomining Content Extension* must be installed to populate the values in QRadar. Please follow the instructions at

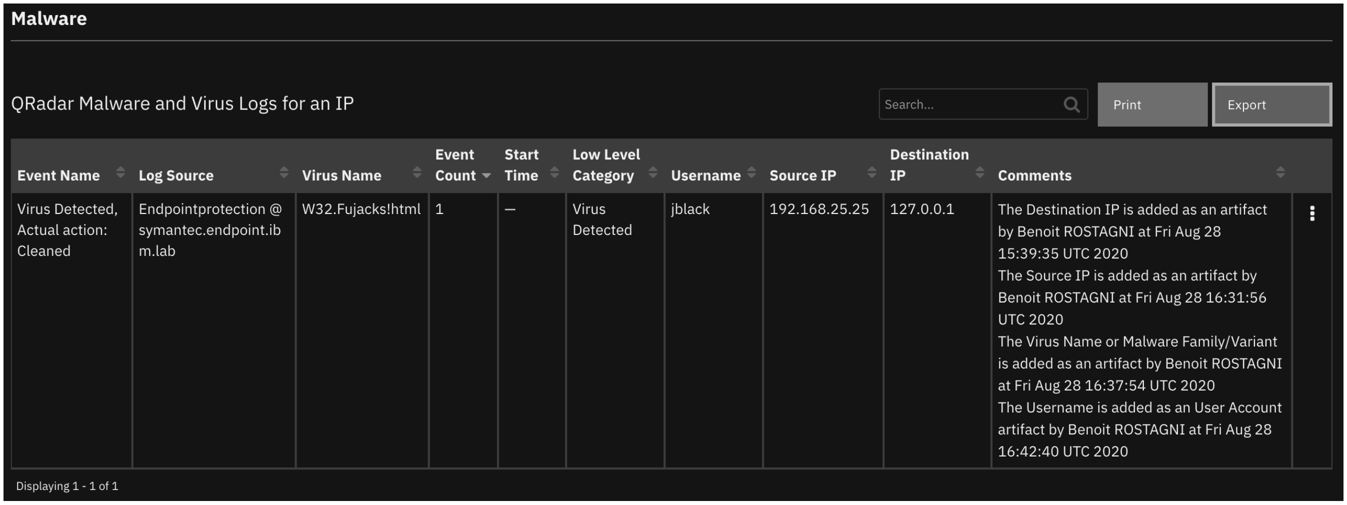
https://exchange.xforce.ibmcloud.com/hub/extension/62fdde6955e3ee6937c819174d5758bb
Query: SELECT QIDNAME(qid) AS "EventName", LOGSOURCENAME(logsourceid) AS "LogSource", "Threat Name", eventCount, DATEFORMAT(starttime, 'YYYY-MM-dd HH:mm') as "StartTime", CATEGORYNAME(category) AS "LowLevelCategory", username, sourceip, destinationip FROM events WHERE sourceip = ({source_ip}) AND CATEGORYNAME(highlevelcategory) = 'Malware' GROUP BY "Threat Name", username, eventCount ORDER BY eventCount DESC LIMIT 100 LAST ({days to search}) DAYS
Note: This query is not launched by the QRadar All Enrichment and required specific Source IP address input addition :



QRadar Malware and Virus Logs for an IP

Source IP *	'0.0.0.0'
Number of Days to Search	3
or select a Days value below	31

Result is visible in QRadar Table:



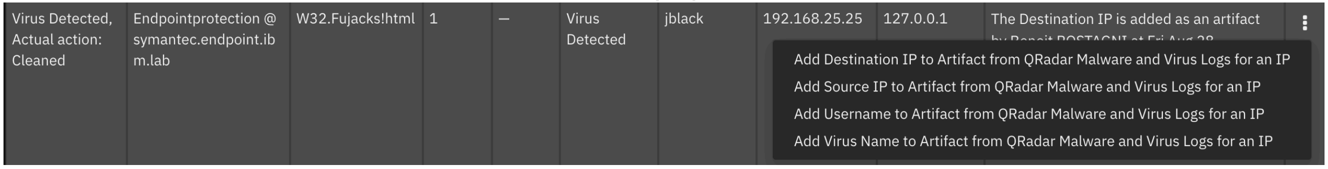
Malware

QRadar Malware and Virus Logs for an IP

Event Name	Log Source	Virus Name	Event Count	Start Time	Low Level Category	Username	Source IP	Destination IP	Comments
Virus Detected, Actual action: Cleaned	Endpointprotection @ symantec.endpoint.ibm.lab	W32.Fujacks!html	1	—	Virus Detected	jblack	192.168.25.25	127.0.0.1	The Destination IP is added as an artifact by Benoit ROSTAGNI at Fri Aug 28 15:39:35 UTC 2020 The Source IP is added as an artifact by Benoit ROSTAGNI at Fri Aug 28 16:31:56 UTC 2020 The Virus Name or Malware Family/Variant is added as an artifact by Benoit ROSTAGNI at Fri Aug 28 16:37:54 UTC 2020 The Username is added as an User Account artifact by Benoit ROSTAGNI at Fri Aug 28 16:42:40 UTC 2020

Displaying 1 - 1 of 1

Actions can be done from the action menu to populate artifacts from this table:

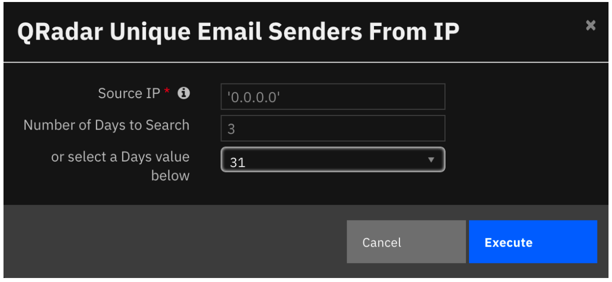


Virus Detected, Actual action: Cleaned	Endpointprotection @ symantec.endpoint.ibm.lab	W32.Fujacks!html	1	—	Virus Detected	jblack	192.168.25.25	127.0.0.1	The Destination IP is added as an artifact

Add Destination IP to Artifact from QRadar Malware and Virus Logs for an IP
Add Source IP to Artifact from QRadar Malware and Virus Logs for an IP
Add Username to Artifact from QRadar Malware and Virus Logs for an IP
Add Virus Name to Artifact from QRadar Malware and Virus Logs for an IP

- **QRadar Unique Email Senders From IP (Artifact)**
  Description: For a given source IP address, return all the unique email senders and their counts
  The package *IBM QRadar Phishing and Email Content Extension* must be installed to populate the values in QRadar. Please follow the instructions at https://exchange.xforce.ibmcloud.com/hub/extension/d47bae0e01d42970c272dcc773eed3bf
  Query: SELECT Sender, SUM(eventCount) AS "totaleventcount" FROM events WHERE sourceip = '{source_ip}' GROUP BY Sender ORDER BY totaleventcount DESC LIMIT 100 LAST ({days to search}) DAYS

Note: This query is not launched by the QRadar All Enrichment and required specific Source IP address input addition :



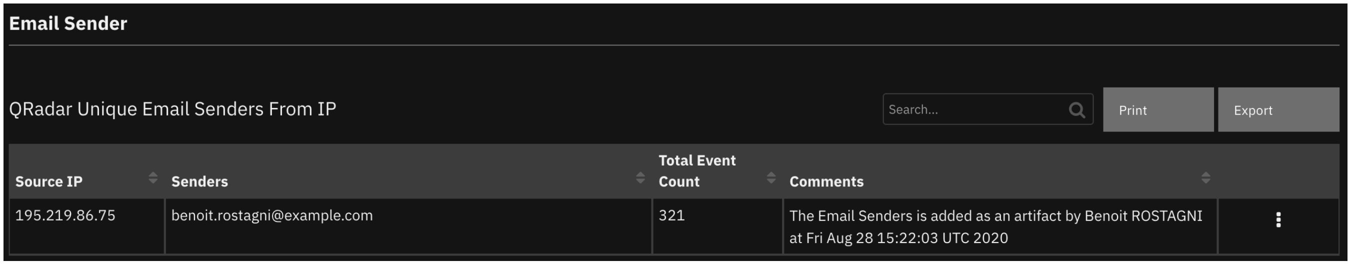
QRadar Unique Email Senders From IP

Source IP * : '0.0.0.0'

Number of Days to Search: 3

or select a Days value below: 31

Result is visible in QRadar Table:

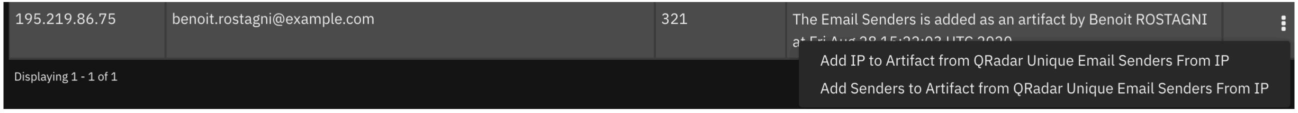


Email Sender

QRadar Unique Email Senders From IP

Source IP	Senders	Total Event Count	Comments
195.219.86.75	benoit.rostagni@example.com	321	The Email Senders is added as an artifact by Benoit ROSTAGNI at Fri Aug 28 15:22:03 UTC 2020

Action can be done from the action menu to populate artifacts from this table:



195.219.86.75	benoit.rostagni@example.com	321	The Email Senders is added as an artifact by Benoit ROSTAGNI at Fri Aug 28 15:22:03 UTC 2020

Displaying 1 - 1 of 1

Add IP to Artifact from QRadar Unique Email Senders From IP
Add Senders to Artifact from QRadar Unique Email Senders From IP

Process Playbooks

Local L2L SSH Server Scanner

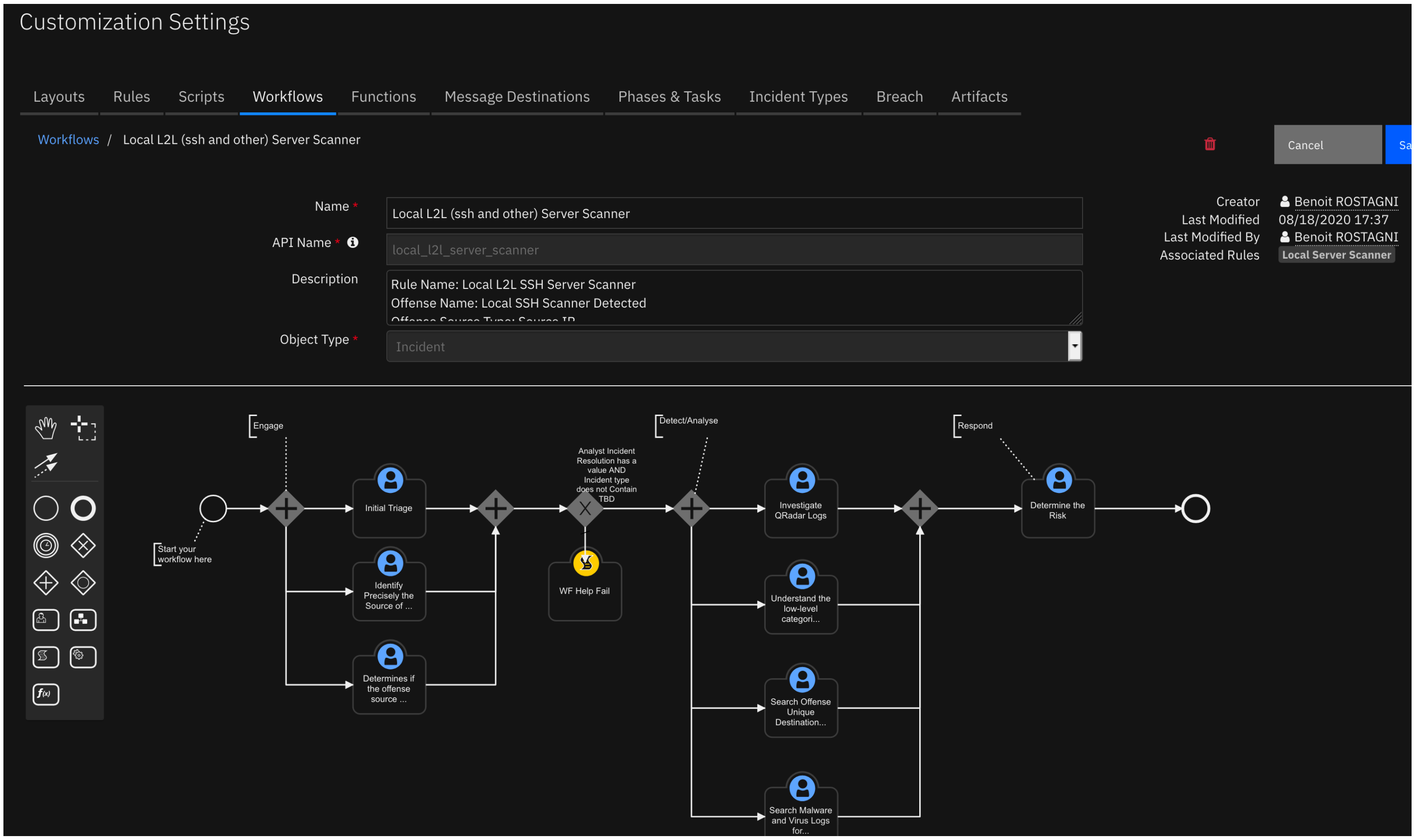
Rule Name: Local L2L SSH Server Scanner
Offense Name: Local SSH Scanner Detected
Offense Source Type: Source IP

Description: this rule triggers when a single local machine communicates to more than X different local machines in a short period of time on destination port 22, indicating a potential host scan. Typically, the source machine in question is a vulnerability scanner of some sort, or it could be a legitimate malicious scanner.

Workflow:

- Analyst performs a DNS lookup on the offense source (which is the source IP, i.e. the machine in question). The machine name usually provides information to the user on what it is (server, user, database, appliance, etc.).
- Analyst determines if the offense source is a server or a user machine. This is accomplished in several ways; either by the hostname from the DNS lookup where the customer has a naming convention that easily identifies this, or by looking up networking information on the subnet of the IP from an external source, or by common analyst knowledge that the subnet the IP belongs to is either a server subnet or a user subnet.
- Analyst clicks on "X events" in QRadar to bring up a window that shows all the QRadar logs associated with this offense to begin his investigation.
- Analyst runs another search, see query Offense Unique Event Low Level Categories, to understand the low-level categories of the events. Maybe all the events are categorized as Firewall Deny, meaning all the traffic was blocked - that's insight for the analyst.
- Analyst runs another search, see query Offense Unique Destination IPs, to understand the unique destination IPs and their counts. Was the offense source mostly talking to a specific set of destination IPs? Ones in a particular subnet? Analyst can also do a DNS lookup for the top 3 or so destination IPs to determine what/who they are, in additional to potentially looking up external network information on the description of the subnet of those IPs. The analyst can use this information to understand the traffic pattern and whether such source IP *should* or *should not* be doing an SSH scan on those destination IPs. Maybe the source was a user machine and the destinations are indeed servers. And based on the previous information gathered about the event categories, was the traffic blocked or not. If it was a user machine, why was his machine doing a scan?
- (Optional) Look up any endpoint protection / antivirus logs associated with this source IP to find out if maybe it has malware that has not been cleaned. This could either be a QRadar search (see query Malware and Virus Logs for an IP - that query needs further tuning because it will list all malware related events for the IP but not necessarily ones that are critical e.g. malware that wasn't cleaned), or this could be an external lookup on the actual EDR platform (Crowdstrike/Symantec/etc.).
- If in the end this offense is determined to be a false positive (i.e. the offense source is expected to exhibit such behavior), the QRadar rule is modified to exclude the IP. By default, this QRadar rule does not have a built-in reference-set mechanism to exclude the IP, so the analyst either modifies the logic of the rule to include an exclusion directly for this IP address, or the analyst creates a reference set and excludes this reference set in this rule, to plan for any additional future exclusions as well.

Workflow Implementation:


Customization Settings
Layouts
Rules
Scripts
Workflows
Functions
Message Destinations
Phases & Tasks
Incident Types
Breach
Artifacts
Workflows / Local L2L (ssh and other) Server Scanner
Cancel
Sa
Engage
Detect/Analyse
Respond
Start your workflow here
Initial Triage
Identify Precisely the Source of ...
Determines if the offense source ...
Analyst Incident Resolution has a value AND Incident type does not Contain TBD
WF Help Fail
Investigate QRadar Logs
Understand the low-level categori...
Search Offense Unique Destination...
Search Malware and Virus Logs for...
Determine the Risk

Name * Local L2L (ssh and other) Server Scanner

API Name * local_l2l_server_scanner

Description Rule Name: Local L2L SSH Server Scanner
Offense Name: Local SSH Scanner Detected
Offense Source Type: Source IP

Object Type * Incident

Creator Benoit ROSTAGNI
Last Modified 08/18/2020 17:37
Last Modified By Benoit ROSTAGNI
Associated Rules Local Server Scanner

Please follow ordered task instructions.

Local L2L {type} Server Scanner

This process Playbook as has been currently set as the same as Local L2L SSH Server Scanner above.

Malware

This process playbook is the Best Practice playbook from NIST, SANS and US-CERT. Please follow ordered task instructions.

Phishing

This process playbook is the Best Practice playbook from NIST, SANS and US-CERT. Please follow ordered task instructions.

Denial of Service

This process playbook is the Best Practice playbook from NIST, SANS and US-CERT. Please follow ordered task instructions.

Intrusion detection

This process playbook is the Best Practice playbook from NIST, SANS and US-CERT. Please follow ordered task instructions.

Error when importing the res file

If you have an error when importing the res file, please do:

- Delete the rules created by QRadar
    - Add to QRadar Reference Set
    - QRadar Ariel Query
    - Move Artifact from one QRadar Reference Set to another
- Install my QRadar res file package
- Verify and configure again the Resilient App on QRadar to update the 2 rules fields (list of Ariel query, list of ref sets) overwritten by the res file.