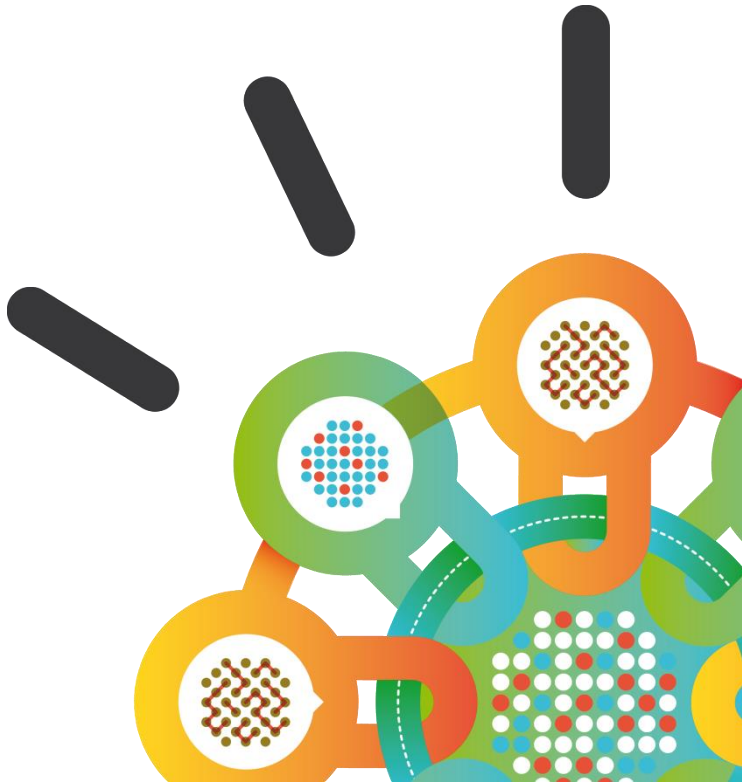
IBM Analyst Custom Searches for QRadar

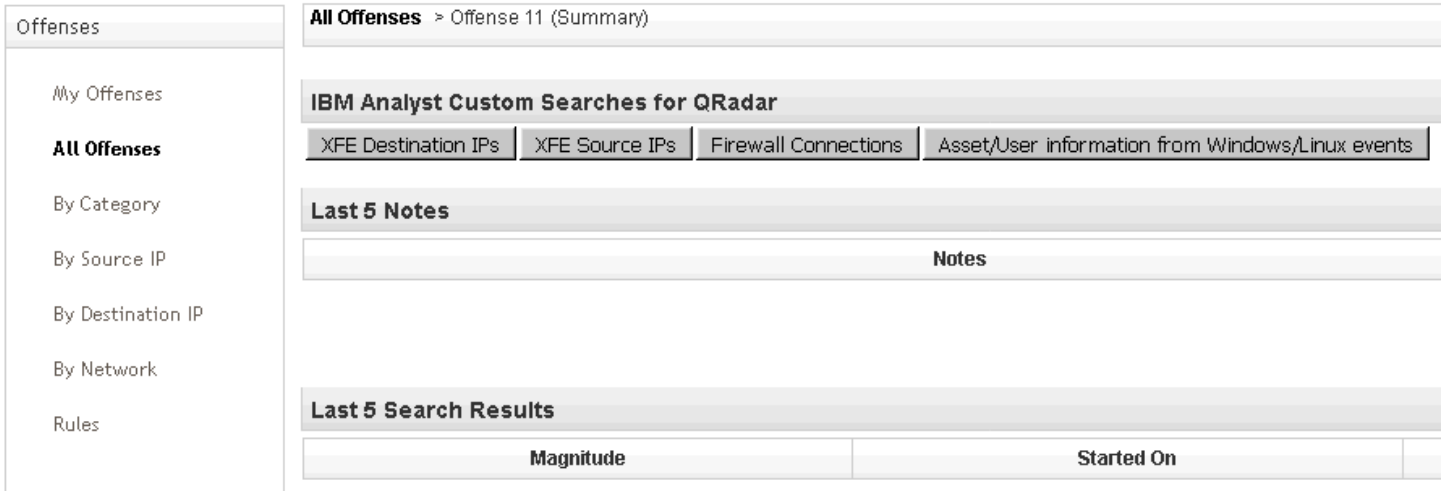
October, 2017



What this app does

- IBM Analyst Custom Searches for QRadar allows Admin users to create globally shared custom searches
- These searches can be used in all existing offenses
- This saves time by not configuring the same searches again each time an analyst wants to analyze an offense by predefining often used search patterns like
  - Specifying columns
  - Filtering on specific criteria like Log Source Types, Events or categories
  - Using aggregate functions like grouping
  - Using AQL functions

- With the press of a button the application enables users to quickly apply search templates to an existing offense

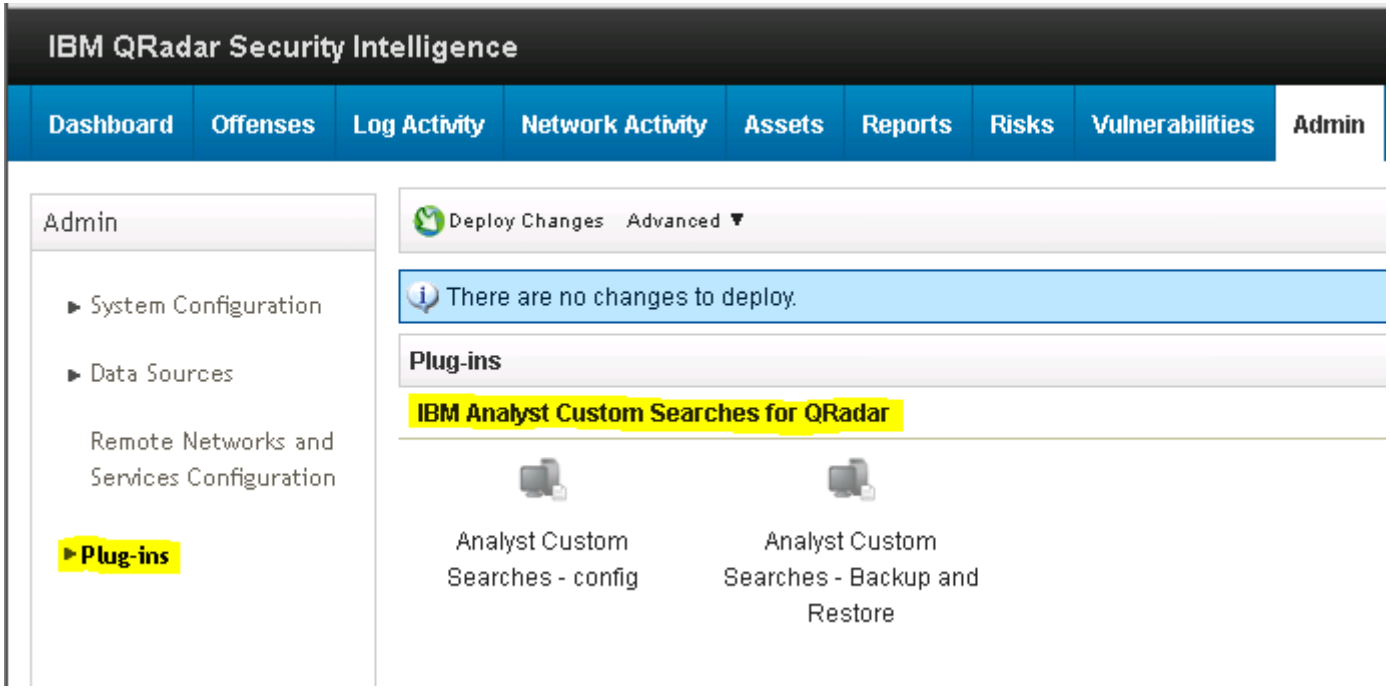


Installing the app

1. On the Admin tab, click Extension Management.
2. In the Extension Management window, click Add and select the IBMAnalystCustomSearches_<Version>.zip that you want to upload to the console.
3. Select the Install immediately check box, if you want QRadar to install the app immediately. Before the app is installed, a preview list of the content items is displayed.
4. To preview the contents of an App after it is added and before it is installed, select it from the list of extensions, and click More Details. Expand the folders to view the individual content items in each group. After installation is complete you will see two IBM Analyst Custom Searches Setting icons added to QRadar admin tab

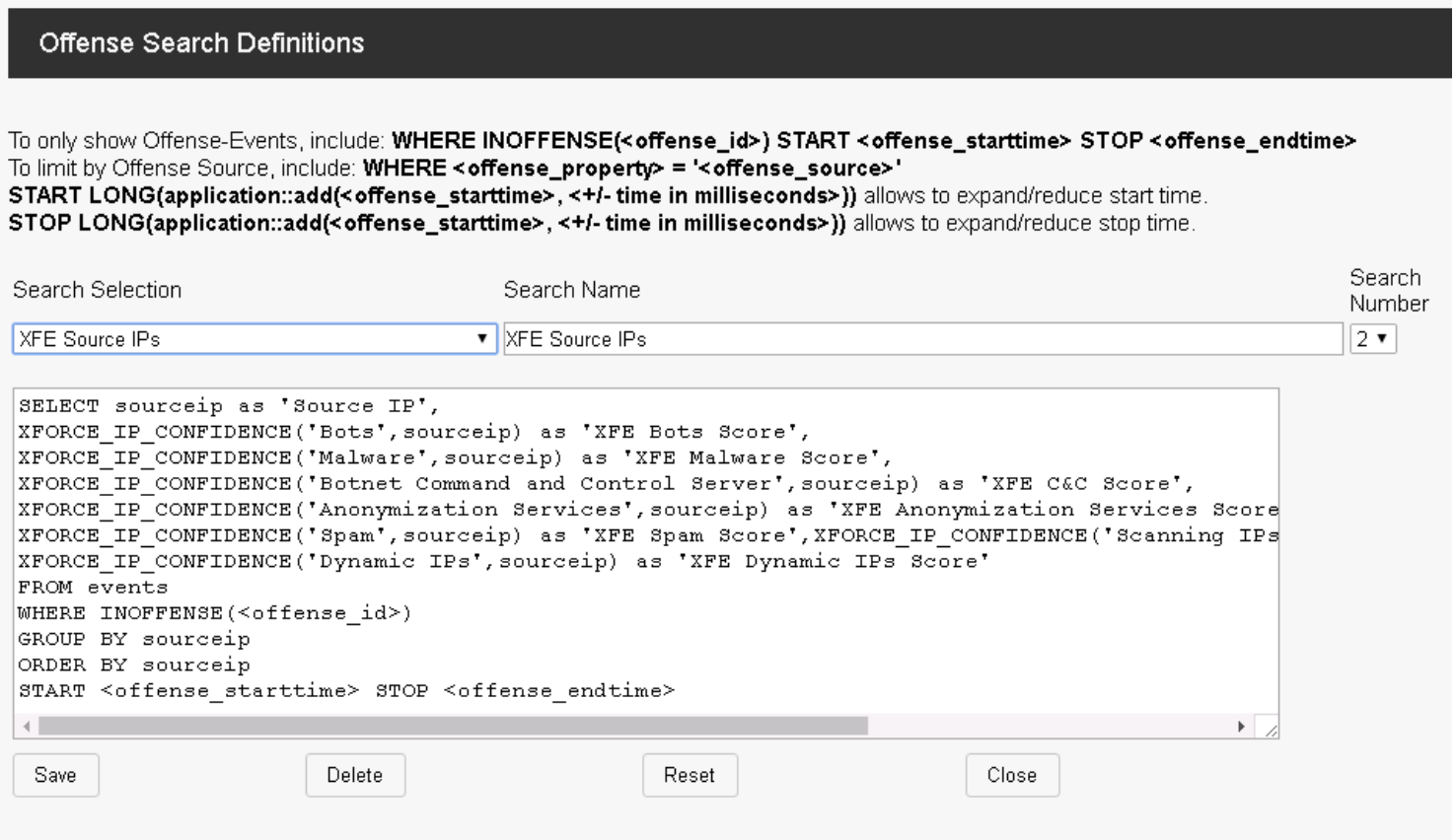
How to use this app

- This app can be configured in the QRadar Admin Menu
- The configured searches are stored here



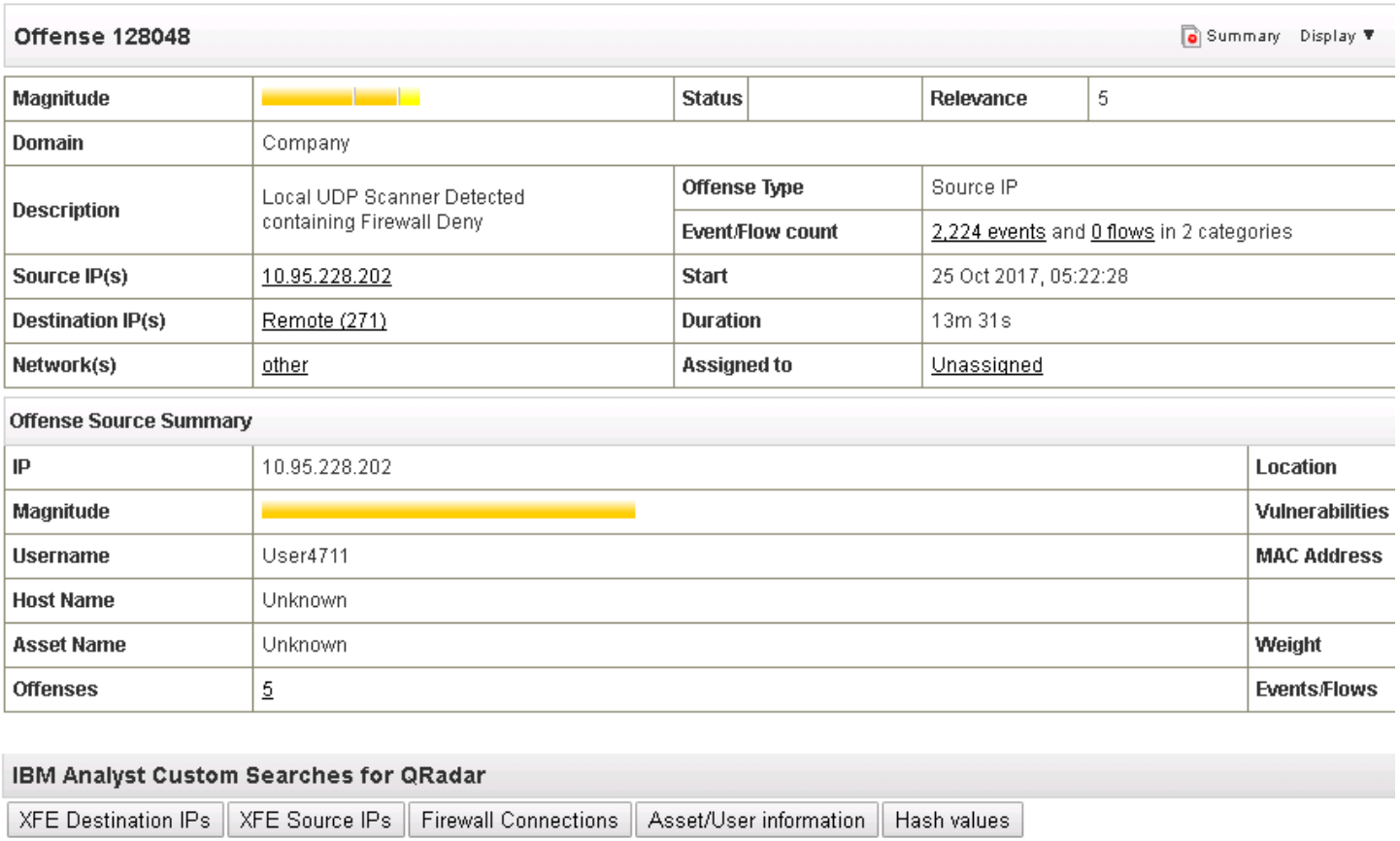
How to use this app

- This app comes with 4 predefined searches for analysts to use in offenses
- These can be used, modified or removed
- All searches will be shown in all Offense Summaries and can be executed by pressing the button with the Search Name



How to use this app – Example

- This offense was created by UDP scanning activity
- Now it would be interesting to know what X-Force says about the Destination IPs
- We can use a predefined Search for this: **XFE Destination IPs**
- You can see the result on the next page



Offense 128048 Summary Display

Magnitude		**Status**		**Relevance**	5
Domain	Company				
Description	Local UDP Scanner Detected containing Firewall Deny	**Offense Type**	Source IP		
		Event/Flow count	2,224 events and 0 flows in 2 categories		
Source IP(s)	10.95.228.202	**Start**	25 Oct 2017, 05:22:28		
Destination IP(s)	Remote (271)	**Duration**	13m 31s		
Network(s)	other	**Assigned to**	Unassigned		

Offense Source Summary

IP	10.95.228.202	**Location**
Magnitude		**Vulnerabilities**
Username	User4711	**MAC Address**
Host Name	Unknown	
Asset Name	Unknown	**Weight**
Offenses	5	**Events/Flows**

IBM Analyst Custom Searches for QRadar

XFE Destination IPs | XFE Source IPs | Firewall Connections | Asset/User information | Hash values

How to use this app – Example result

Search... ▼ Quick Searches ▼ Add Filter Save Criteria Save Results Cancel False Positive Rules ▼ Actions ▼

Advanced Search

```
SELECT destinationip as 'Destination IP',
XFORCE_IP_CONFIDENCE('Bots',destinationip) as 'XFE Bots Score',
XFORCE_IP_CONFIDENCE('Malware',destinationip) as 'XFE Malware Score',
XFORCE_IP_CONFIDENCE('Botnet Command and Control Server',destinationip) as 'XFE C&C Score',
XFORCE_IP_CONFIDENCE('Anonymization Services',destinationip) as 'XFE Anonymization Services Score',
XFORCE_IP_CONFIDENCE('Spam',destinationip) as 'XFE Spam Score',
XFORCE_IP_CONFIDENCE('Scanning IPs',destinationip) as 'XFE Scanning IPs Score',
XFORCE_IP_CONFIDENCE('Dynamic IPs',destinationip) as 'XFE Dynamic IPs Score'
FROM events
WHERE INOFFENSE(128048)
GROUP BY destinationip
ORDER BY destinationip
START 1508908948037 STOP 1508909759915
```

▼ Current Statistics

Total Results 2,224
Data Files Searched 104 (

(Show

Destination IP ▲	XFE Bots Score	XFE Malware Score	XFE C&C Score	XFE Anonymization Services Score	XFE Spam Score	XFE Scanning IPs Score	XFE Dynamic IPs Score
.22.7	0	0	0	0	0	0	0
.22.9	0	0	0	0	0	0	0
.22.10	0	0	0	0	0	0	0
.22.11	0	0	0	0	0	0	0
.22.12	0	0	0	0	0	0	0
.22.13	0	0	0	0	0	0	0
.22.14	0	0	0	0	0	0	0
.22.15	0	0	0	0	0	0	0
.22.16	0	0	0	0	0	0	0
.22.17	0	0	0	0	0	0	0
.22.19	0	0	0	0	0	0	0
.22.20	0	0	0	0	0	0	0
.22.21	0	0	0	0	0	0	0
.22.22	0	0	0	0	0	0	0
.22.23	0	0	0	0	0	0	0
.22.24	0	0	0	0	0	0	0
.22.25	0	0	0	0	0	0	0
.22.26	0	0	0	0	0	0	0
.22.27	0	0	0	0	0	0	0
.22.29	0	0	0	0	0	0	0

How to configure searches

- Custom searches are defined through AQL statements in the config menu
- The name of the button is set in the Search Name field
- The name of the search is used as the button name in the offense summaries and does not have to be unique, but this is recommended
- The AQL can be anything, but to benefit from the offense integration most, it is recommended to use one or more of the following placeholder strings. The app will automatically replace these placeholder strings with the corresponding content

`<offense_id>` should be used in the `WHERE` clause=> `WHERE INOFFENSE(<offense_id>)`
`<offense_property>` is the property the offense is based on like SourceIP, Eventname, username ...
`'<offense_source>'` is the specific value of the `<offense_property>` like 192.168.1.1, Login Failed, root
`<offense_starttime>` is the time, when the offense started. Should be used with `START` or `STOP`
`<offense_stoptime>` is the time, when the offense ended. Should be used with `START` or `STOP`

- This app also includes a Custom AQL function to modify the `START` and `STOP` of the search interval
  `LONG(application::add(<offense_starttime>, -900000))`
  This subtracts 900000 milliseconds (15 minutes) from the offense start time
  `LONG(application::add(<offense_stoptime>, +1800000))`
  This adds 1800000 milliseconds (30 minutes) to the offense stop time.

- Sample how to modify the search interval:
  `START LONG(application::add(<offense_starttime>, -900000)) STOP LONG(application::add(<offense_stoptime>, +1800000))`

How to configure searches – with Samples

- Sample:

```
MySearch:SELECT sourceip FROM events WHERE INOFFENSE(<offense_id>)
GROUP BY sourceip START '<offense_starttime>' STOP '<offense_endtime>'
```

This search shows all source IPs of the offense (`WHERE INOFFENSE(<offense_id>)`)
only once (**`GROUP BY`** `sourceip`) . The time interval is between start and end of the offense

- Sample:

```
MySearch:SELECT QIDNAME(qid) as 'Event Name',sourceip,destinationip
FROM events
WHERE <offense_property> = '<offense_source>'
START LONG(application::add(<offense_starttime>, -900000))
STOP  '<offense_starttime >'
```

Shows all events with Event Name, source IP and destination IPs, which share the offense source
(`<offense_property> = '<offense_source>'`)
like `sourceip = '10.10.10.10'`
The search interval is from 15 minutes before the offense started
(`START LONG(application::add(<offense_starttime>, -900000))`)
to offense start time
(`STOP <offense_starttime>`)

What the predefined searches do

- ***XFE Destination IPs***
-
```
SELECT destinationip as 'Destination IP',
XFORCE_IP_CONFIDENCE('Bots',destinationip) as 'XFE Bots Score',
XFORCE_IP_CONFIDENCE('Malware',destinationip) as 'XFE Malware Score',
XFORCE_IP_CONFIDENCE('Botnet Command and Control Server',destinationip) as 'XFE C&C Score',
XFORCE_IP_CONFIDENCE('Anonymization Services',destinationip) as 'XFE Anonymization Score',
XFORCE_IP_CONFIDENCE('Spam',destinationip) as 'XFE Spam Score',
XFORCE_IP_CONFIDENCE('Scanning IPs',destinationip) as 'XFE Scanning IPs Score',
XFORCE_IP_CONFIDENCE('Dynamic IPs',destinationip) as 'XFE Dynamic IPs Score'
FROM events
WHERE INOFFENSE(<offense_id>)
GROUP BY destinationip
ORDER BY destinationip
START <offense_starttime> STOP <offense_endtime>
```

- This search shows the scores of the X-Force Exchange categories of all Destination IPs (`XFORCE_IP_CONFIDENCE('…',destinationip) , GROUP BY destinationip`) in the offense (`WHERE INOFFENSE(<offense_id>)`)
- The search interval is the time from offense start to offense end

- ***XFE Source IPs***
- Does the same as Destination IPs, but for Source IPs instead

- Notice: Both searches require the X-Force Exchange Feed to be activated

What the predefined searches do

- ***Firewall Connections***
- ```
  SELECT sourceip as 'Source IP',
  sourcemac,
  destinationip as 'Destination IP',
  destinationmac,
  destinationport as 'Destination Port',
  CATEGORYNAME(category) as 'Category'
  FROM events
  WHERE INOFFENSE(<offense_id>) AND LOGSOURCEGROUPNAME(devicegrouplist) = 'Firewall'
  ORDER BY sourceip,destinationip,destinationport,category
  START LONG(application::add(<offense_starttime>, -900000))
  STOP LONG(application::add(<offense_endtime>, +900000))
  ```

- This search shows the Offense events (**`WHERE`** `INOFFENSE(<offense_id>)`), which are also in the Log Source Group ‚Firewall‘ (`AND LOGSOURCEGROUPNAME(devicegrouplist)= 'Firewall'`)
- It only shows columns, which are relevant to Firewall events. It is possible to add custom property fields, which are often used. These could not be added in the predefined search since they can differ between environments

- The time interval is from offense start time minus 15 minutes (900000 milliseconds) to offense stop time plus 15 minutes. Sometimes the start offense time does not match the time of the first event
  ```

What the predefined searches do

- ***Asset/User information from Windows/Linux events***

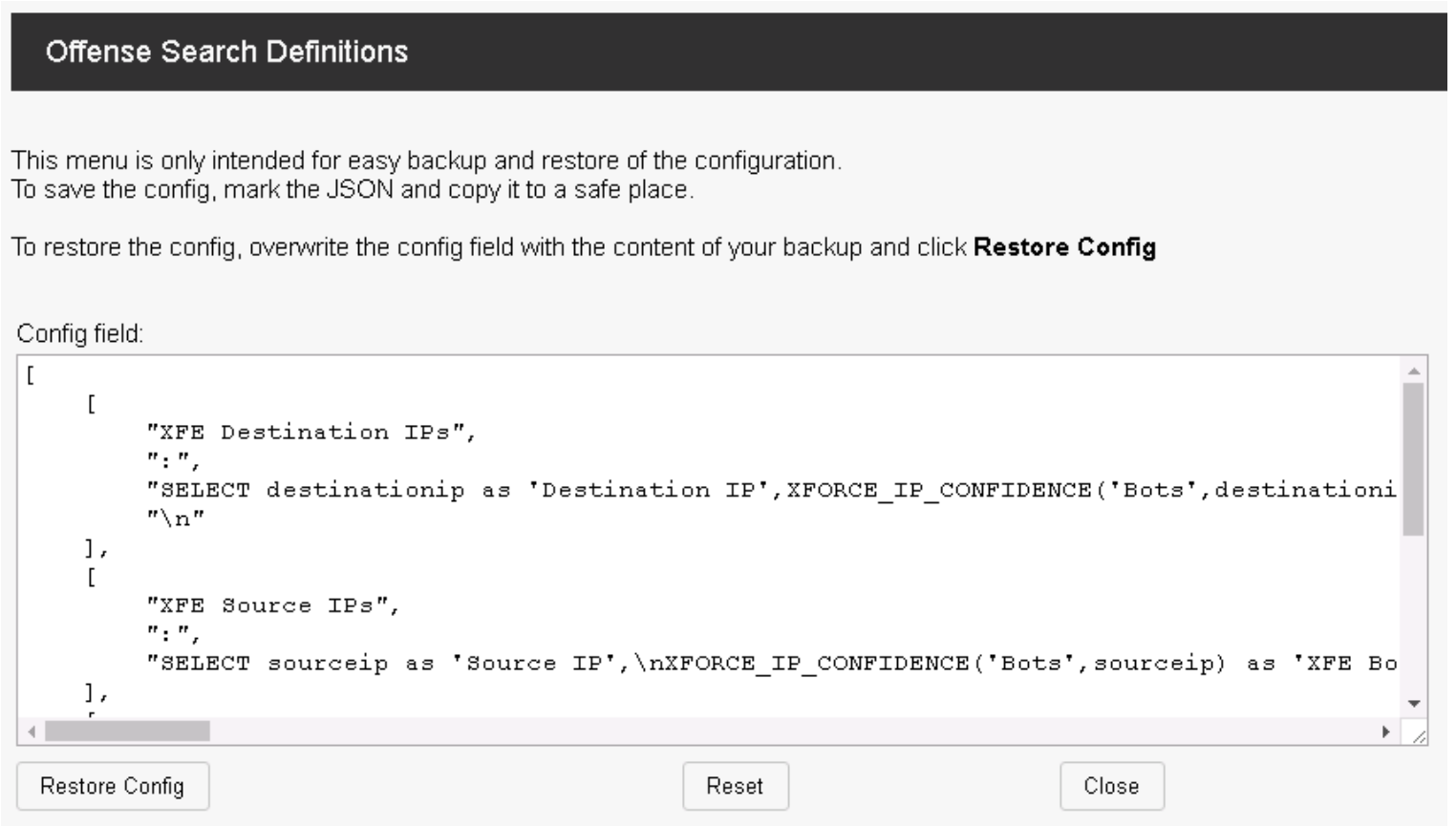
```
SELECT QIDNAME(qid) as 'Event Name',LOGSOURCENAME(logsourceid) as 'Log Source',sourceip as
'Source IP',destinationip as 'Destination IP',destinationmac,destinationport as
'Destination Port',"Hostname",username as 'Username',ASSETHOSTNAME(sourceip,devicetime) as
'Source Asset Hostname',ASSETUSER(sourceip,devicetime) as
'Source Asset User',ASSETUSER(destinationip,devicetime) as
'Destination Asset User',ASSETHOSTNAME(destinationip,devicetime) as
'Destination Asset Hostname'
FROM events
WHERE <offense_property> = '<offense_source>' AND (devicetype=11 OR devicetype=12)
START LONG(application::add(<offense_starttime>, -900000))
STOP LONG(application::add(<offense_endtime>, +900000))
```

- This search uses the AQL functions **`ASSETHOSTNAME`** and **`ASSETUSER`** to show the information the QRadar Asset DB has about sourceip and destinationip at the time of the Log Source Device Timestamp. It does not limit on the events in the offense, but on Linux events (**`devicetype=11`**) and windows events (**`devicetype=12`**) with have the property value as the offense
- Search interval is from offense start time minus 15 minutes to offense end time plus 15 minutes

- Nice to know: You can limit the events with
  `WHERE devicetype=[ID of devicetype]`
  or use the lookup function LOGSOURCETYPENAME(devicetype)
  `WHERE LOGSOURCETYPENAME(devicetype) = '[Exact devicetype]'`
  `WHERE LOGSOURCETYPENAME(devicetype) ILIKE '%[part of devicename ignore case]%'`

Backup and Restore

- The configuration of all searches can be seen in the **Analyst Custom Searches - Backup and Restore** menu. This can be used for Saving and Restoring the complete config
- Searches should not be modified here, but only in the dedicated menu



Supporting information

- Please check the following links to get the most out of AQL queries
  https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.0/com.ibm.qradar.doc/c_aql_introduction.html
  https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.0/com.ibm.qradar.doc/r_aql_supported_functions.html
  https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.0/com.ibm.qradar.doc/c_aql_intro.html
  https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.0/com.ibm.qradar.doc/c_qradar_ug_search_bar_examples.html

- On the next pages you will find the IDs and names needed for limiting to events of specific Log Source types
- The ID of a custom Log source type can usually be found in the Log Source extension (Admin menu) it creates and is usually an ID equal or greater than 4000

Supporting information

ID	LOGSOURCETYPENAME
2	Snort Open Source IDS
3	Check Point
4	Configurable Firewall Filter
5	Juniper Networks Firewall and VPN
6	Cisco PIX Firewall
7	Configurable Authentication message filter
8	SOAP Webservice-based messages, pre-normalized
9	Extreme Dragon Network IPS
10	Apache HTTP Server
11	Linux OS
12	Microsoft Windows Security Event Log
13	Microsoft IIS
14	Linux iptables Firewall
15	IBM Proventia Network Intrusion Prevention System (IPS)
16	Flow Classification Engine
17	Juniper Networks Intrusion Detection and Prevention (IDP)
18	Custom Rule Engine
19	TippingPoint Intrusion Prevention System (IPS)
20	Cisco IOS
21	Nortel Contivity VPN Switch (obsolete)
22	Nortel Multiprotocol Router
23	Cisco VPN 3000 Series Concentrator
24	Solaris Operating System Authentication Messages
25	McAfee IntruShield Network IPS Appliance
26	Cisco CSA
28	Extreme Matrix E1 Switch
29	Solaris Operating System Sendmail Logs
30	Cisco Intrusion Prevention System (IPS)
31	Cisco Firewall Services Module (FWSM)
33	IBM Proventia Management SiteProtector
35	CyberGuard TSP Firewall/VPN
36	Juniper Networks Secure Access (SA) SSL VPN
37	Nortel Contivity VPN Switch
38	Top Layer IPS
39	Universal DSM
40	Tripwire Enterprise

ID	LOGSOURCETYPENAME
41	Cisco Adaptive Security Appliance (ASA)
42	Niksun 2005 v3.5
45	Juniper Networks Network and Security Manager
46	Squid Web Proxy
47	Ambiron TrustWave ipAngel Intrusion Prevention System (IPS)
48	Oracle RDBMS Audit Record
49	F5 Networks BIG-IP LTM
50	Solaris Operating System DHCP Logs
55	Array Networks SSL VPN Access Gateways
56	Cisco CatOS for Catalyst Switches
57	ProFTPD Server
58	Linux DHCP Server
59	Juniper Networks Infranet Controller
64	Juniper Junos OS Platform
67	SIM Generic Log DSM
68	Extreme Matrix K/N/S Series Switch
70	Extreme Networks ExtremeWare Operating System (OS)
71	McAfee Firewall Enterprise
73	Fortinet FortiGate Security Gateway
78	SonicWALL SonicOS
79	Vericept Content 360
82	Symantec Gateway Security (SGS) Appliance
83	Juniper Steel-Belted Radius
85	IBM AIX Server
86	Metainfo MetaIP
87	Symantec System Center
90	Cisco ACS
92	ForeScout CounterACT
93	McAfee ePolicy Orchestrator
95	Cisco NAC Appliance
96	TippingPoint X Series Appliances
97	Microsoft DHCP Server
98	Microsoft IAS Server
99	Microsoft Exchange Server
100	Trend InterScan VirusWall
101	Microsoft SQL Server
102	Mac OS X
103	Blue Coat SG Appliance
104	Nortel Switched Firewall 6000
105	SIM Audit
106	3Com 8800 Series Switch
107	Nortel VPN Gateway
108	Nortel Threat Protection System (TPS) Intrusion Sensor

Supporting information

ID	LOGSOURCETYPENAME
110	Nortel Application Switch
111	Juniper DX Application Acceleration Platform
112	Snare Reflector Server
113	Cisco 12000 Series Routers
114	Cisco 6500 Series Switches
115	Cisco 7600 Series Routers
116	Cisco Carrier Routing System
117	Cisco Integrated Services Router
118	Juniper M Series Multiservice Edge Routing
120	Nortel Switched Firewall 5100
122	Juniper MX Series Ethernet Services Router
123	Juniper T Series Core Platform
134	Nortel Ethernet Routing Switch 8300/8600
135	Nortel Ethernet Routing Switch 2500/4500/5500
136	Nortel Secure Router
138	OpenBSD OS
139	Juniper EX-Series Ethernet Switch
140	Symark Power Broker
141	Oracle Database Listener
142	Samhain HIDS
143	Bridgewater Systems AAA Service Controller
144	Name Value Pair
145	Nortel Secure Network Access Switch (SNAS)
146	Starent Networks Home Agent (HA)
147	System Notification
148	IBM i
149	Foundry Fastiron
150	Juniper SRX Series Services Gateway
153	CRYPTOCard CRYPTOShield
154	Imperva SecureSphere
155	Aruba Mobility Controller
156	Extreme NetsightASM
157	Extreme HiGuard
158	Motorola SymbolAP
159	Extreme HiPath
160	Symantec Endpoint Protection
161	IBM Resource Access Control Facility (RACF)
163	RSA Authentication Manager
164	Redback ASE
165	Trend Micro Office Scan

ID	LOGSOURCETYPENAME
166	Extreme XSR Security Routers
167	Extreme Stackable and Standalone Switches
168	Juniper Networks AVT
169	OS Services Qidmap
170	Extreme A2-Series
171	Extreme B2-Series
172	Extreme B3-Series
173	Extreme C2-Series
174	Extreme C3-Series
175	Extreme D2-Series
176	Extreme G3-Series
177	Extreme I3-Series
178	Trend Micro Control Manager
179	Cisco IronPort
180	Hewlett Packard UniX
182	Cisco Aironet
183	Cisco Wireless Services Module (WiSM)
185	ISC BIND
186	IBM Lotus Domino
187	HP Tandem
188	Sentrigo Hedgehog
189	Sybase ASE
191	Microsoft ISA
193	Radware DefensePro
194	Cisco ACE Firewall
195	IBM DB2
196	Oracle Audit Vault
197	Cisco FireSIGHT Management Center
198	Forcepoint V Series
199	Oracle RDBMS OS Audit Record
200	Risk Manager Default Question
201	Risk Manager User Question
202	Risk Manager Default Simulation
203	Risk Manager User Simulation
204	Risk Manager Question and Simulations
205	Flow Device Type
206	Palo Alto PA Series
207	Anomaly Detection Engine
208	HP ProCurve
209	Microsoft Operations Manager

Supporting information

ID	LOGSOURCETYPENAME
210	EMC VMWare
211	IBM WebSphere Application Server
212	Universal LEEF
213	F5 Networks BIG-IP ASM
214	FireEye
215	Fair Warning
216	IBM Informix Audit
217	CA Top Secret
218	Extreme NAC
219	Microsoft SCOM
220	McAfee Web Gateway
221	CA ACF2
222	McAfee Application/Change Control
223	Lieberman Random Password Manager
224	Sophos Enterprise Console
225	NetApp Data ONTAP
226	Sophos PureMessage
227	Cyber-Ark Vault
228	Itron Smart Meter
230	Bit9 Security Platform
231	IBM IMS
232	F5 Networks FirePass
233	Citrix NetScaler
234	F5 Networks BIG-IP APM
235	Juniper vGW
236	Symantec DLP
238	Solaris BSM
239	Oracle BEA WebLogic
240	Sophos Web Security Appliance
241	Sophos Astaro Security Gateway
243	Infoblox NIOS
244	Tropos Control
245	Novell eDirectory
246	WinCollect
247	VMware vShield
249	IBM Guardium
250	Cisco Nexus
251	Stonesoft Management Center
252	SolarWinds Orion
253	Microsoft Endpoint Protection

ID	LOGSOURCETYPENAME
254	Great Bay Beacon
255	Damballa Failsafe
258	CA SiteMinder
259	IBM z/OS
260	Microsoft SharePoint
261	iT-CUBE agileSI
262	Event CRE Injected
263	DCN DCS/DCRS Series
264	Juniper Security Binary Log Collector
265	Trend Micro Deep Discovery Inspector
266	IBM Tivoli Access Manager for e-business
267	Asset Profiler
268	Verdasys Digital Guardian
269	Huawei S Series Switch
270	Citrix Access Gateway
271	HBGary Active Defense
272	APC UPS
273	Cisco Wireless LAN Controllers
274	Cisco Call Manager
275	CRE System
276	IBM CICS
278	Barracuda Spam & Virus Firewall
279	Open LDAP Software
280	Application Security DbProtect
281	Barracuda Web Application Firewall
282	OSSEC
283	Huawei AR Series Router
284	Sun ONE LDAP
285	BlueCat Networks Adonis
286	IBM AIX Audit
287	PGP Universal Server
288	Kaspersky Security Center
289	IBM BigFix
290	Juniper Junos WebApp Secure
291	Nominum Vantio
292	Extreme 800-Series Switch
293	IBM zSecure Alert
294	IBM QRadar Network Security XGS
295	IBM Security Identity Manager
296	F5 Networks BIG-IP AFM

Supporting information

ID	LOGSOURCETYPENAME
297	IBM Security Network IPS (GX)
298	Fidelis XPS
299	Arpeggio SIFT-IT
300	Barracuda Web Filter
302	Brocade FabricOS
303	ThreatGRID Malware Threat Intelligence Platform
304	IBM Security Access Manager for Enterprise Single Sign-On
305	VMware vCloud Director
306	Venustech Venusense Unified Threat Management
307	Venustech Venusense Firewall
308	Venustech Venusense Network Intrusion Prevention System
309	ObserveIT
311	Pirean Access: One
312	Venustech Venusense Security Platform
313	PostFix MailTransferAgent
314	Oracle Fine Grained Auditing
315	VMware vCenter
316	Cisco Identity Services Engine
318	Honeycomb Lexicon File Integrity Monitor
319	Oracle Acme Packet SBC
320	Juniper WirelessLAN
321	Akamai KONA
330	Arbor Networks Peakflow SP
331	Zscaler Nss
332	Proofpoint Enterprise Protection/Enterprise Privacy
333	H3C Comware Platform
334	H3C Switches
335	H3C Routers
336	H3C Wireless LAN Devices
337	H3C IP Security Devices
338	Microsoft Hyper-V
339	Cilasoft QJRN/400
340	Vormetric Data Security
341	SafeNet DataSecure/KeySecure
342	OpenStack
343	STEALTHbits StealthINTERCEPT
344	Juniper DDoS Secure
345	Arbor Networks Pravail
346	IBM Security Trusteer Apex Advanced Malware Protection
347	Amazon AWS CloudTrail

ID	LOGSOURCETYPENAME
348	IBM Security Directory Server
349	Extreme A4-Series
350	Extreme B5-Series
351	Extreme C5-Series
352	Salesforce Security Monitoring
353	AhnLab Policy Center APC
354	Avaya VPN Gateway
355	Search Results
356	DG Technology MEAS
357	Salesforce Security Auditing
358	CloudPassage Halo
359	CorreLog Agent for IBM zOS
360	WatchGuard Fireware OS
361	IBM Fiberlink MaaS360
362	Trend Micro Deep Discovery Analyzer
363	Resolution1 CyberSecurity
364	IBM Privileged Session Recorder
365	Bluemix Platform
366	IBM SmartCloud Orchestrator
367	Universal CEF
368	Health Metrics
369	FreeRADIUS
370	Riverbed SteelCentral NetProfiler
371	Riverbed SteelCentral NetProfiler Audit
372	SSH CryptoAuditor
373	IBM DataPower
374	Symantec Critical System Protection
375	Kisco Information Systems SafeNet/i
376	IBM Federated Directory Server
377	HyTrust CloudControl
378	Lastline Enterprise
379	genua genugate
380	IBM Security Privileged Identity Manager
381	Netskope Active
382	Okta
383	Oracle Enterprise Manager
384	Microsoft DNS Debug
385	STEALTHbits StealthINTERCEPT Analytics
386	STEALTHbits StealthINTERCEPT Alerts
388	Cloudera Navigator

Supporting information

ID	LOGSOURCETYPENAME
389	IBM Security Access Manager for Mobile
390	Skyhigh Networks Cloud Security Platform
391	Aruba ClearPass Policy Manager
392	IBM Security Identity Governance
393	Seculert Seculert
394	Trend Micro Deep Security
395	Epic SIEM
396	Enterprise-IT-Security.com SF-Sherlock
397	Microsoft Office 365
398	Exabeam
399	Blue Coat Web Security Service
400	Carbon Black
401	Trend Micro Deep Discovery Email Inspector
402	Onapsis Inc Onapsis Security Platform
403	CyberArk Privileged Threat Analytics
404	Palo Alto Endpoint Security Manager
405	Box
406	Radware AppWall
407	CrowdStrike Falcon Host
408	IBM Sense
409	CloudLock Cloud Security Fabric
410	Vectra Networks Vectra
411	HP Network Automation
412	IBM QRadar Packet Capture
413	Microsoft Azure
414	Kaspersky Threat Feed Service
415	ESET Remote Administrator
416	Illumio Adaptive Security Platform
418	Niara
419	Cisco Cloud Web Security
421	IBM SAN Volume Controller
422	LightCyber Magna
423	Fasoo Enterprise DRM
425	Imperva Incapsula
426	IBM BigFix Detect
427	Centrify Server Suite
428	Carbon Black Protection
429	Cisco Stealthwatch