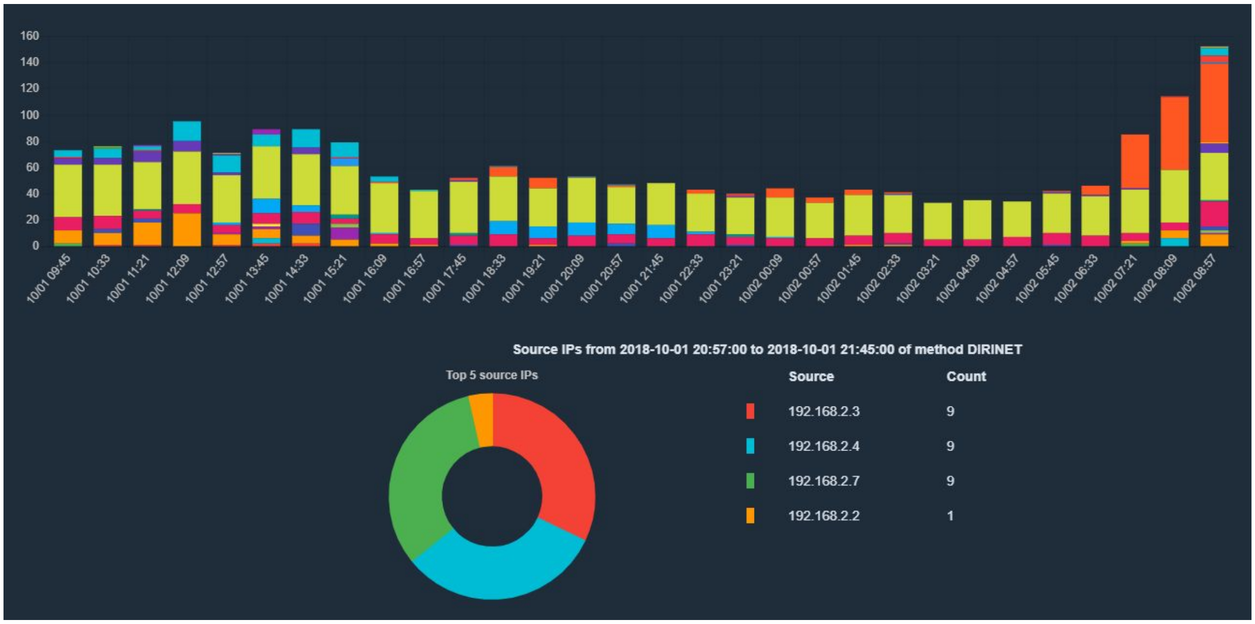
Flowmon
Networks

Flowmon Application for QRadar User Guide

Version 1.0



Source IPs from 2018-10-01 20:57:00 to 2018-10-01 21:45:00 of method DIRINET

	Source	Count
🟥	192.168.2.3	9
🟦	192.168.2.4	9
🟩	192.168.2.7	9
🟧	192.168.2.2	1

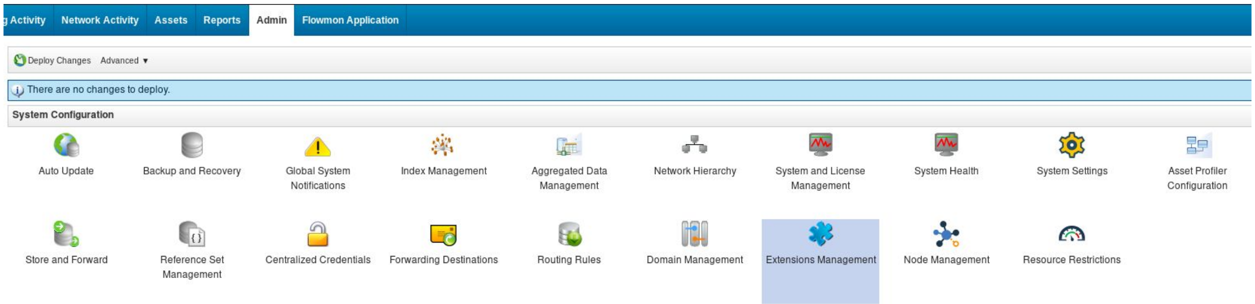
Flowmon Application for QRadar is an extension connecting IBM QRadar with events from Flowmon ADS Solution. Flowmon Application was built with our best practices in mind: it's easy to use, offers intuitive drill-down from dashboard down to the individual flows to quickly resolve issues and to uncover malicious and suspicious behavior. It enables to view flows and events right in the QRadar without having to switch between two different interfaces while simultaneously taking advantage of the power of Flowmon Solution. This seamless integration is achieved by leveraging Flowmon REST API and syslog message standard. QRadar connector and correlation rules are pre-configured in an installation package.

This guide explains all the steps necessary to install, configure and start using the Flowmon Application for QRadar.

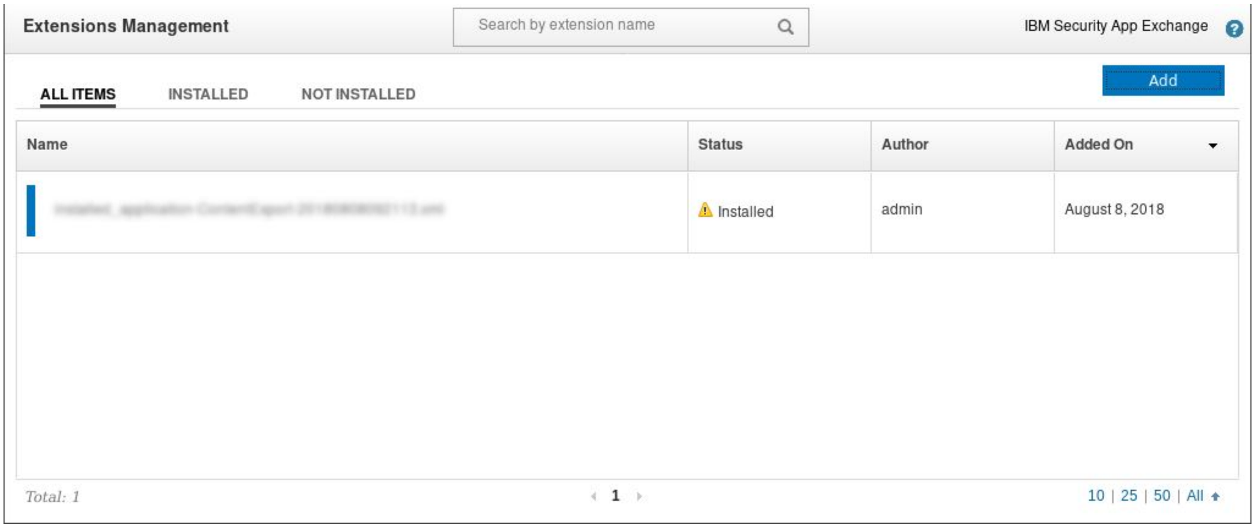
Content

Installation

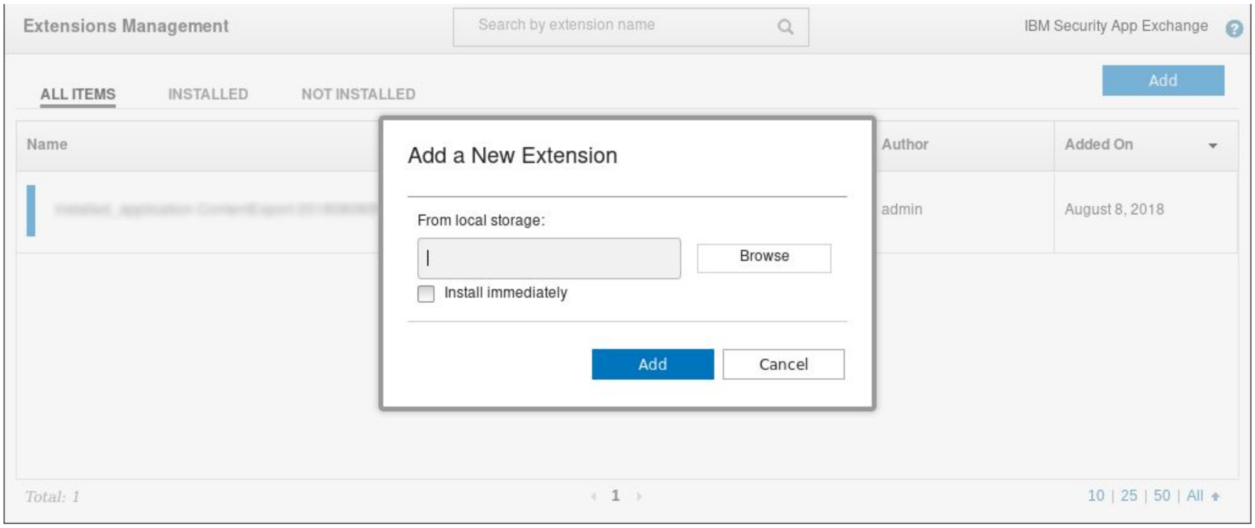
After downloading zip package from IBM X-Force Exchange to your computer open QRadar Console GUI, sign in to account with admin rights, open tab *Admin* (in some versions navigation menu, *Admin tab*), then click on ***Extension Management*** in the section *System Configuration*.



In newly opened window click on button "*Add*" and choose package that was previously downloaded.

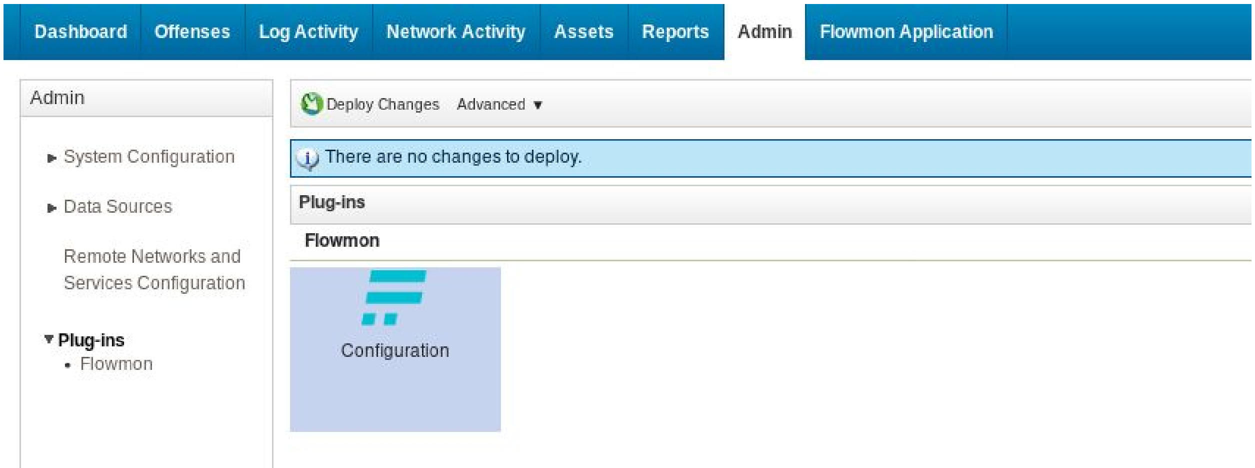


Name	Status	Author	Added On
[redacted]	Installed	admin	August 8, 2018



Configuration

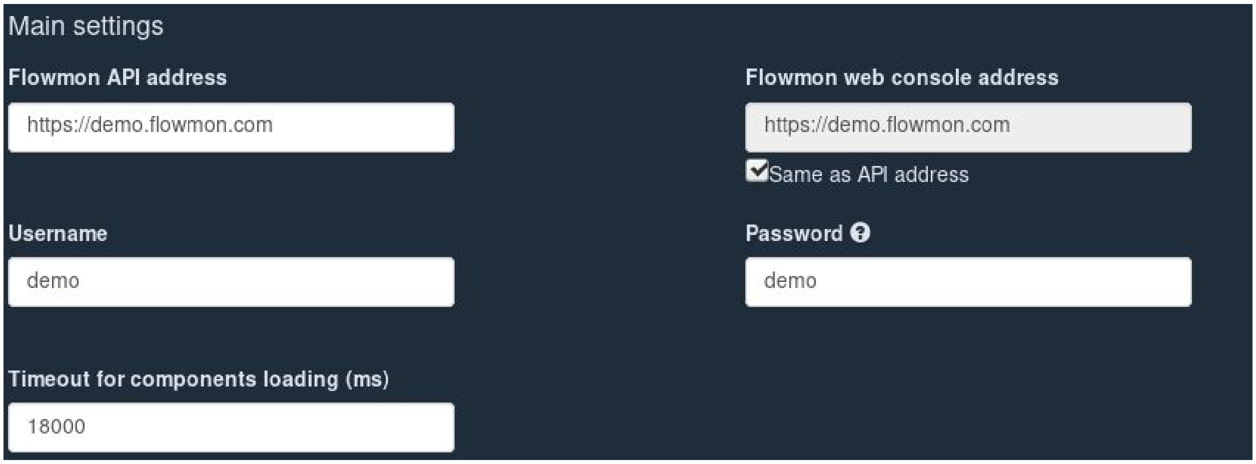
Before starting using application it must be configured. Configuration page is located in the tab *Admin* under the section *Plug-ins* (in some versions section *Apps*).



There are no changes to deploy.

Main settings

Following screenshot illustrates connecting Flowmon Application to Flowmon public demo:



Main settings

Flowmon API address: https://demo.flowmon.com

Flowmon web console address: https://demo.flowmon.com

☑ Same as API address

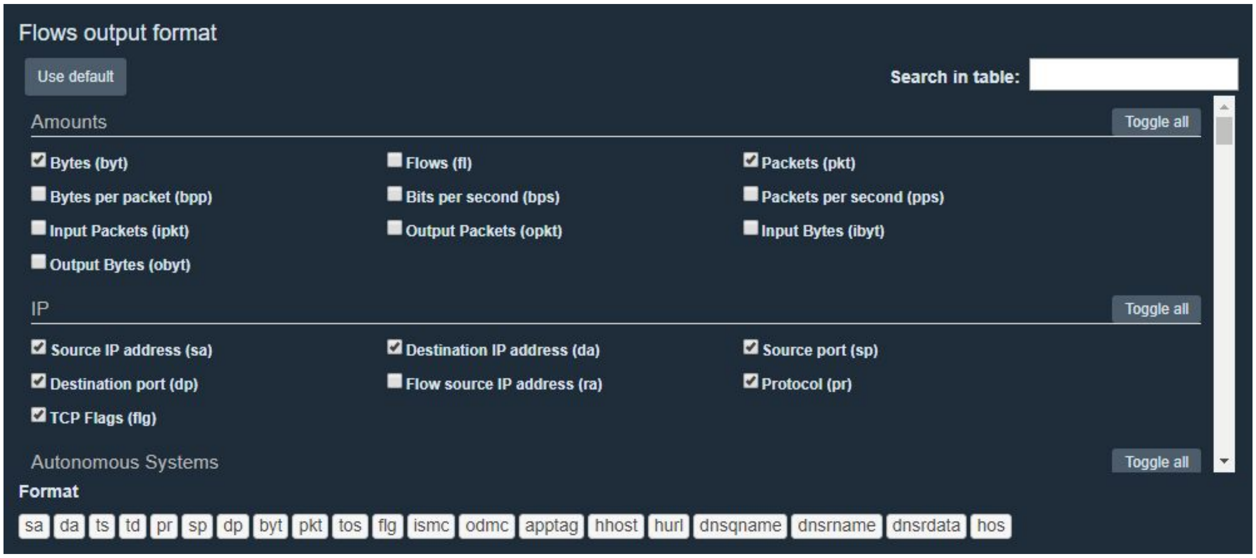
Username: demo

Password: demo

Timeout for components loading (ms): 18000

- Input address to Flowmon API. In case Flowmon Console GUI has the same IP address you can just check “Same as API address” - second address is used for generating links to open concrete event in the Flowmon Console GUI.
- Username and Password values are used for obtaining token, which is necessary for API calls. During the first configuration input that values into the fields. If you open configuration page once again after saving, field Password will remain empty - that is done for security reasons. If you want to leave the same password, just leave this field empty. In case you want to change password, input new value to this field.
- Due to possible long time of collecting data from Flowmon user can change Timeout value by himself. If you get notification that timeout was reached during usage of application too often, try to increase this value.

Flows output format



Flows output format

Use default

Search in table:

Amounts — Toggle all

☑ Bytes (byt)
□ Flows (fl)
☑ Packets (pkt)
□ Bytes per packet (bpp)
□ Bits per second (bps)
□ Packets per second (pps)
□ Input Packets (ipkt)
□ Output Packets (opkt)
□ Input Bytes (ibyt)
□ Output Bytes (obyt)

IP — Toggle all

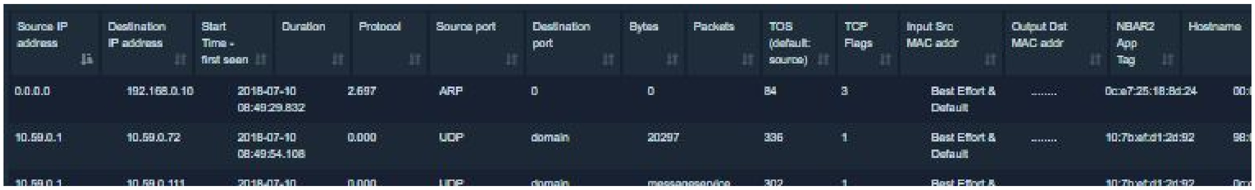
☑ Source IP address (sa)
☑ Destination IP address (da)
☑ Source port (sp)
☑ Destination port (dp)
□ Flow source IP address (ra)
☑ Protocol (pr)
☑ TCP Flags (flg)

Autonomous Systems — Toggle all

Format

sa da ts td pr sp dp byt pkt tos flg ismc odmc apptag hhost hurl dnsqname dnsrname dnsrdata hos

Corresponding columns in Flow view:



Source IP address	Destination IP address	Start Time - first seen	Duration	Protocol	Source port	Destination port	Bytes	Packets	TOS (default: source)	TCP Flags	Input Src MAC addr	Output Dst MAC addr	NBAR2 App Tag	Hostname
0.0.0.0	192.168.0.10	2018-07-10 08:49:29.832	2.697	ARP	0	0	84	3	Best Effort & Default	....	0c:a7:25:18:8d:24	00:		
10.59.0.1	10.59.0.72	2018-07-10 08:49:54.108	0.000	UDP	domain	20297	336	1	Best Effort & Default	....	10:7b:af:d1:2d:92	98:		
10.59.0.1	10.59.0.111	2018-07-10	0.000	UDP	domain	messageservice	302	1	Best Effort &		10:7b:af:d1:2d:92	0c:		

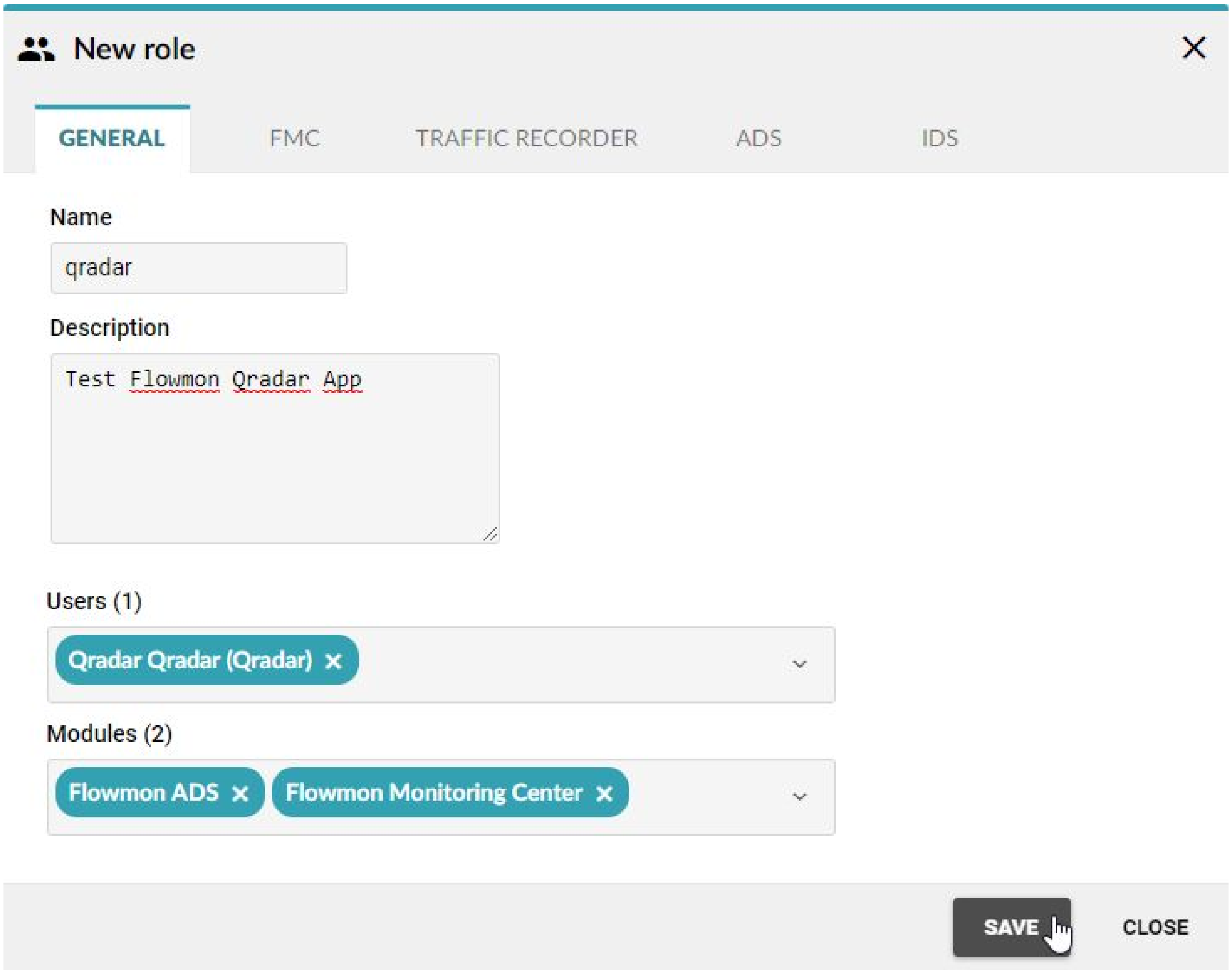
To save new configuration click button “Save” at the bottom part of the page.

Configuration in Flowmon Solution

Permissions

Create or edit role in Flowmon Configuration Center/System/User Settings with following permissions. It is recommended to create also a new user for Qradar concern.

Application requires access to Flowmon Monitoring Center (FMC) and Flowmon ADS:



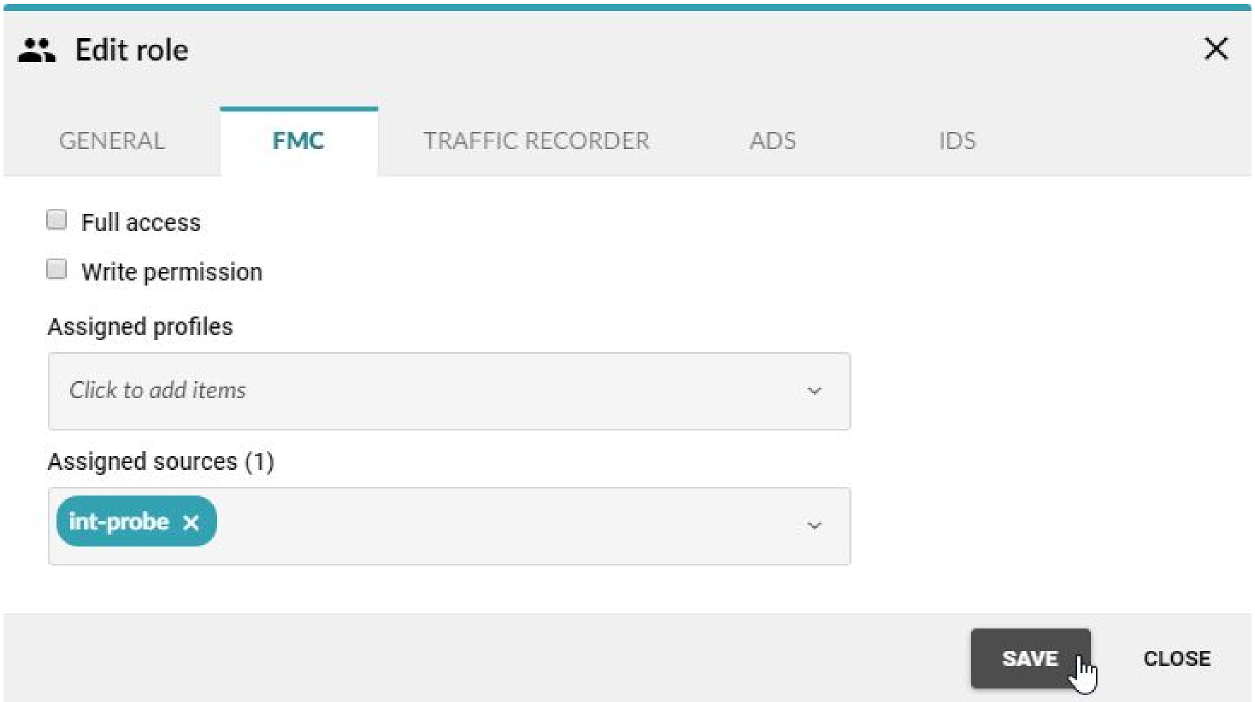
Name
qradar

Description
Test Flowmon Qradar App

Users (1)
Qradar Qradar (Qradar) ×

Modules (2)
Flowmon ADS × Flowmon Monitoring Center ×

Select at least one source. *All Sources* profile is always available as well as profiles for selected sources. Optionally, select additional profiles to make them available in application.



Edit role

□ Full access

□ Write permission

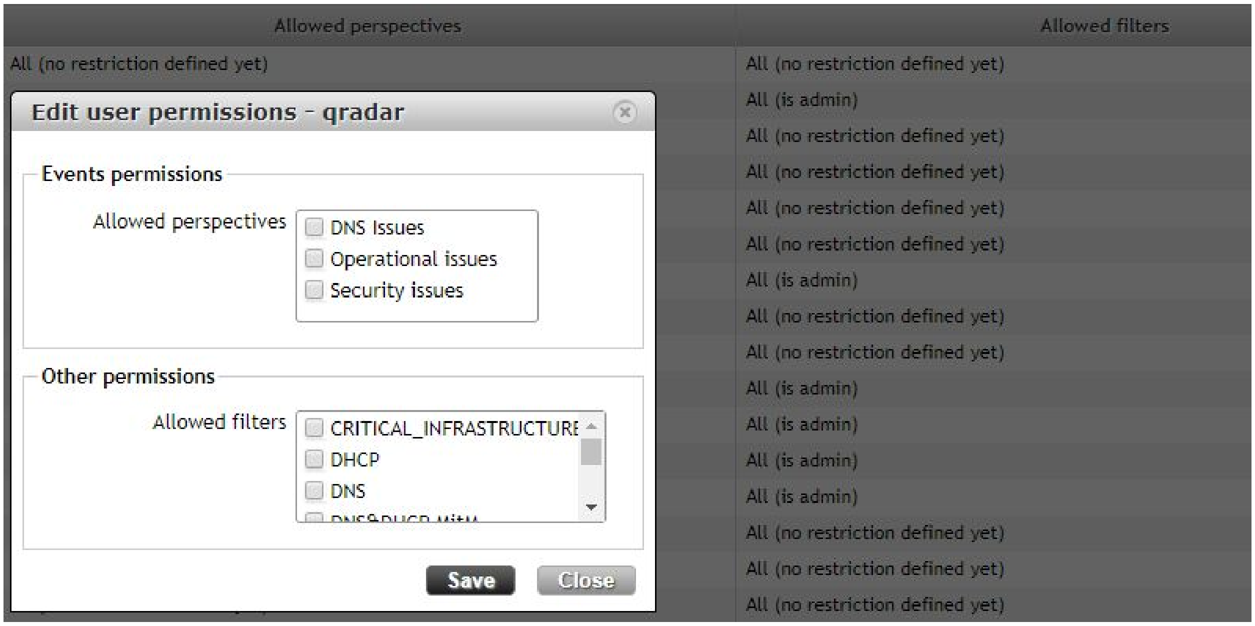
Assigned profiles

Click to add items

Assigned sources (1)

int-probe ×

User permissions in Flowmon ADS Settings control which perspectives and filters are available in application. All perspectives and filters are allowed by default. Optionally, select individual perspectives and filters in *Flowmon ADS/Settings/User permissions*



Allowed perspectives	Allowed filters
All (no restriction defined yet)	All (no restriction defined yet)
	All (is admin)
	All (no restriction defined yet)
	All (no restriction defined yet)
	All (no restriction defined yet)
	All (no restriction defined yet)
	All (is admin)
	All (no restriction defined yet)
	All (no restriction defined yet)
	All (is admin)
	All (is admin)
	All (is admin)
	All (is admin)
	All (no restriction defined yet)
	All (no restriction defined yet)
	All (no restriction defined yet)

Edit user permissions - qradar

Events permissions

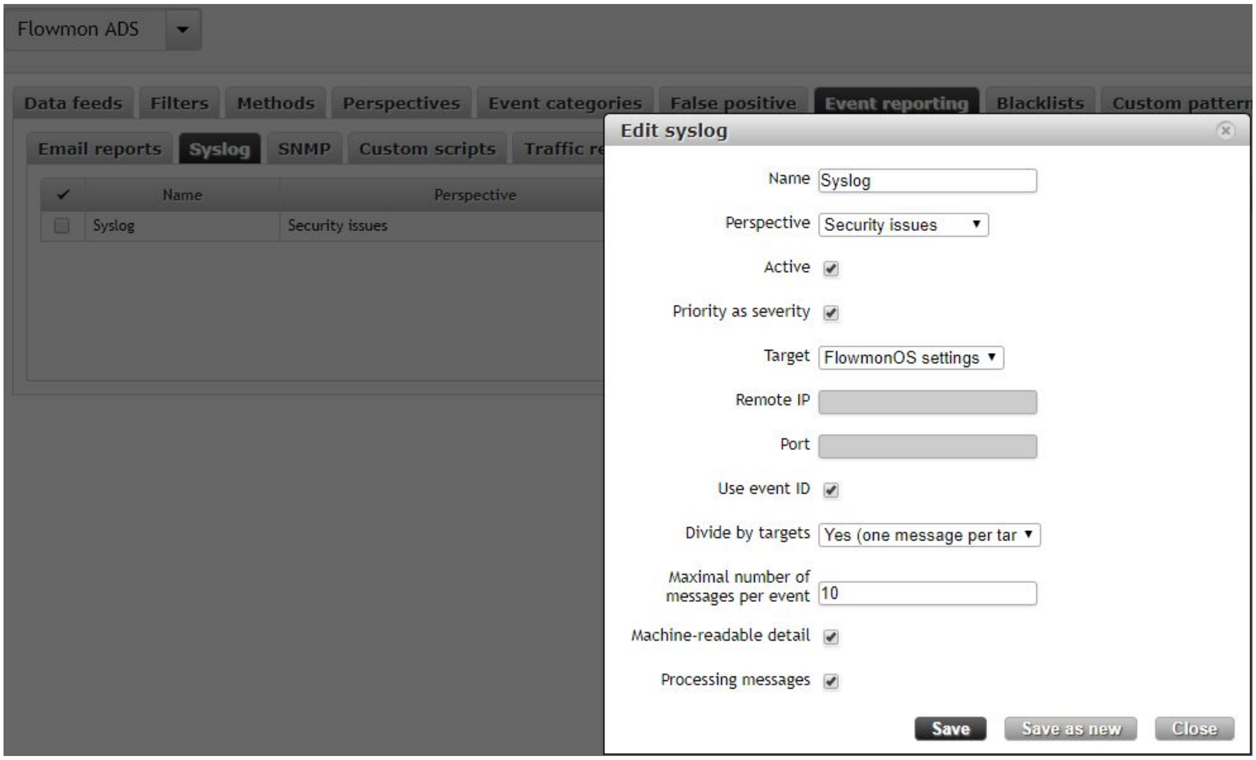
Allowed perspectives
□ DNS Issues
□ Operational issues
□ Security issues

Other permissions

Allowed filters
□ CRITICAL_INFRASTRUCTURE
□ DHCP
□ DNS

Syslog

In Flowmon ADS, Processing page, Event reporting tab - Syslog configure syslog as illustrated in the screenshot below.



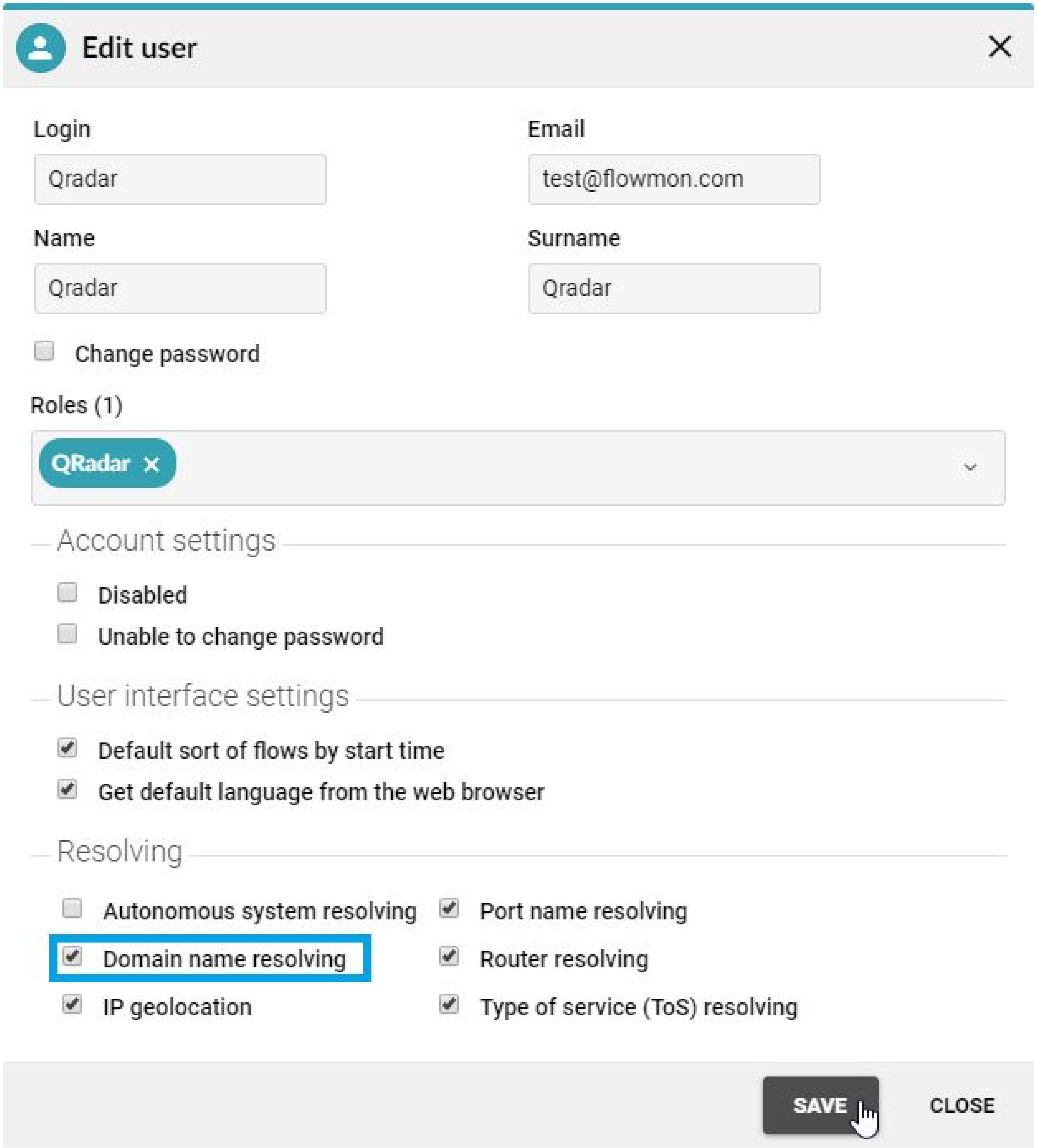
✓	Name	Perspective
□	Syslog	Security issues

Edit syslog

- Name: Syslog
- Perspective: Security issues
- Active: ☑
- Priority as severity: ☑
- Target: FlowmonOS settings
- Remote IP:
- Port:
- Use event ID: ☑
- Divide by targets: Yes (one message per tar
- Maximal number of messages per event: 10
- Machine-readable detail: ☑
- Processing messages: ☑

DNS Resolving

Please note that the domain name resolving user settings in Flowmon Solution has an immediate effect on values appearing in Flowmon ADS for QRadar (Event evidence and Flows).



Edit user

Login: Qradar

Email: test@flowmon.com

Name: Qradar

Surname: Qradar

□ Change password

Roles (1): QRadar

Account settings

- □ Disabled
- □ Unable to change password

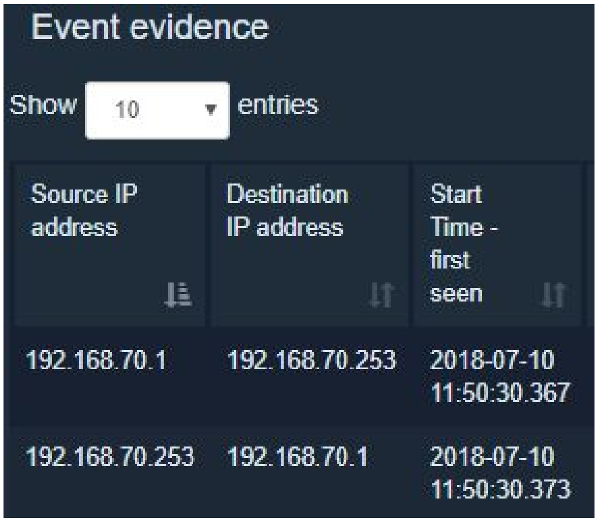
User interface settings

- ☑ Default sort of flows by start time
- ☑ Get default language from the web browser

Resolving

- □ Autonomous system resolving
- ☑ Domain name resolving
- ☑ IP geolocation
- ☑ Port name resolving
- ☑ Router resolving
- ☑ Type of service (ToS) resolving

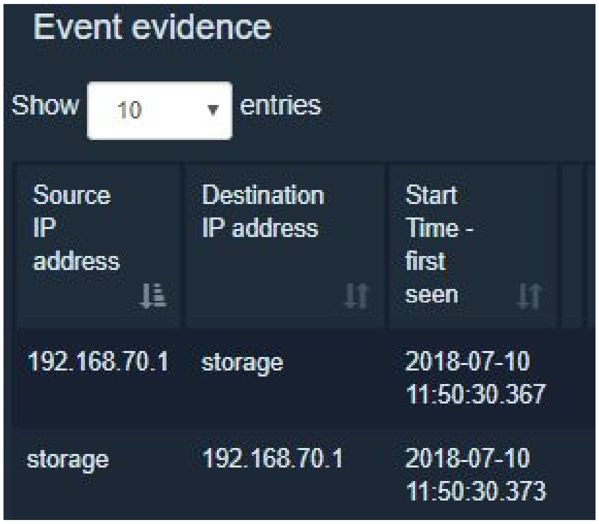
Comparison of domain name resolving turned off / on (left / right):



Event evidence

Show 10 entries

Source IP address	Destination IP address	Start Time - first seen
192.168.70.1	192.168.70.253	2018-07-10 11:50:30.367
192.168.70.253	192.168.70.1	2018-07-10 11:50:30.373



Event evidence

Show 10 entries

Source IP address	Destination IP address	Start Time - first seen
192.168.70.1	storage	2018-07-10 11:50:30.367
storage	192.168.70.1	2018-07-10 11:50:30.373

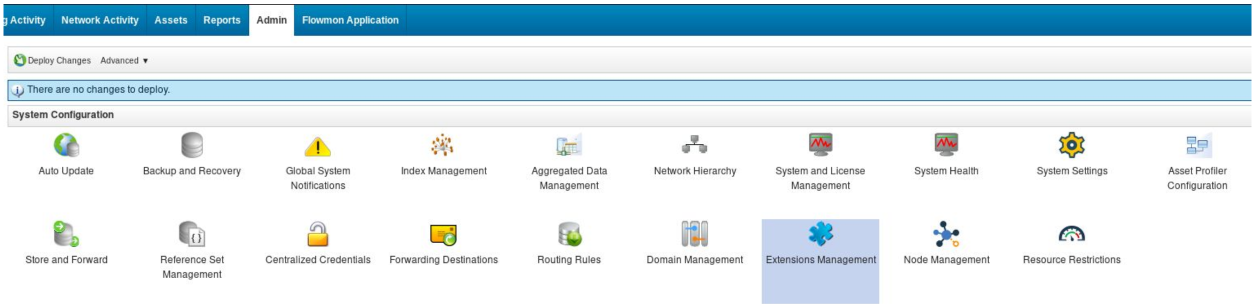
Usage

Connector

Connector is delivered as separate extension and can be installed and used without installation of main application. It has no GUI or configuration page, because it consists only of custom rules, custom DSMs, QID records and other internal things in order to help QRadar in recognizing events from Flowmon ADS. Its installation process is the same as installation of main app . Furthermore, Flowmon must be configured to send events info to QRadar.

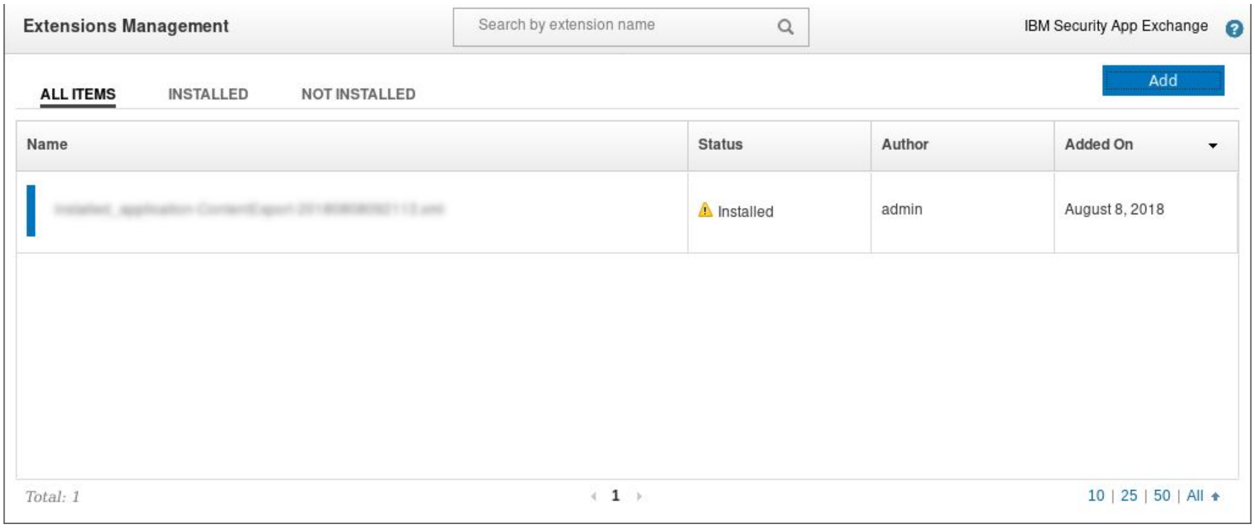
Connector installation

After downloading zip package with connector to your computer open QRadar Console GUI, sign in to account with admin rights, open tab Admin, then click on **Extension Management** in the section System Configuration.

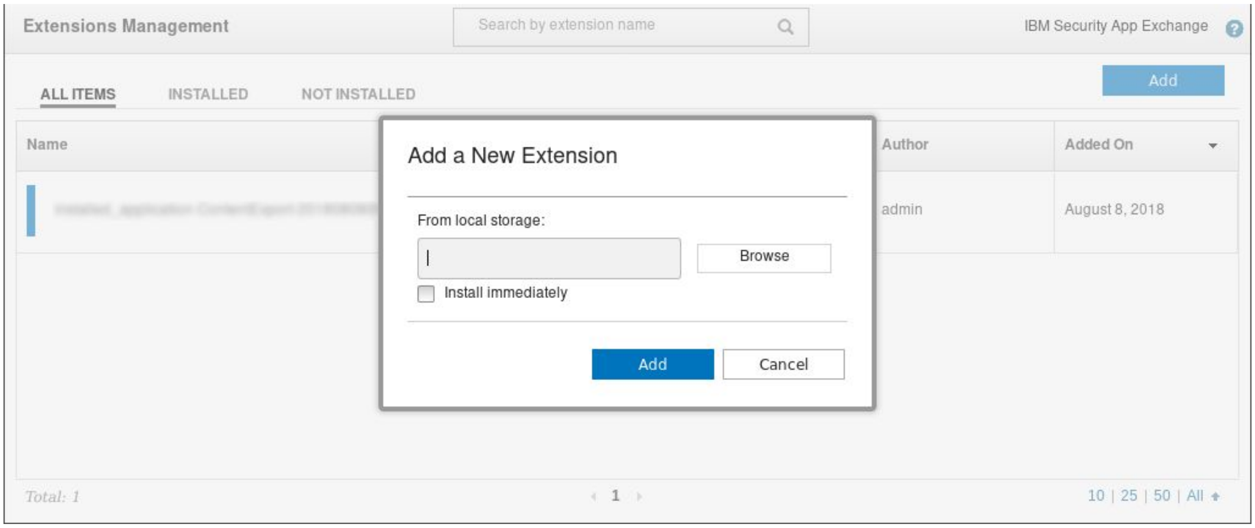


There are no changes to deploy.

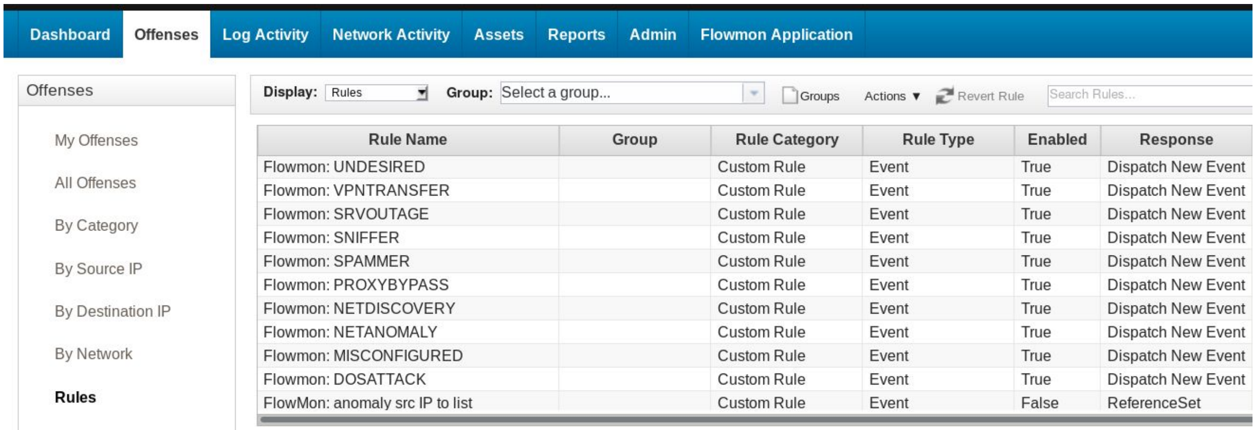
In newly opened window click on button “Add” and choose package that was previously downloaded



Name	Status	Author	Added On
[redacted]	⚠ Installed	admin	August 8, 2018



After successful installation you will see new custom rules on the Offenses page.



Rule Name	Group	Rule Category	Rule Type	Enabled	Response
Flowmon: UNDESIRED		Custom Rule	Event	True	Dispatch New Event
Flowmon: VPNTRANSFER		Custom Rule	Event	True	Dispatch New Event
Flowmon: SRVOUTAGE		Custom Rule	Event	True	Dispatch New Event
Flowmon: SNIFFER		Custom Rule	Event	True	Dispatch New Event
Flowmon: SPAMMER		Custom Rule	Event	True	Dispatch New Event
Flowmon: PROXYBYPASS		Custom Rule	Event	True	Dispatch New Event
Flowmon: NETDISCOVERY		Custom Rule	Event	True	Dispatch New Event
Flowmon: NETANOMALY		Custom Rule	Event	True	Dispatch New Event
Flowmon: MISCONFIGURED		Custom Rule	Event	True	Dispatch New Event
Flowmon: DOSATTACK		Custom Rule	Event	True	Dispatch New Event
FlowMon: anomaly src IP to list		Custom Rule	Event	False	ReferenceSet

Correlation rules

The main part of the Connector is custom rules with definitions of Flowmon ADS detection methods.

Flowmon: ACCESSATTACK
The method is aggregating the simple events informing about the attacks against authentication

Flowmon: Anomaly destination IP to list – Reference Set
Flowmon: Anomaly source IP to list – Reference Set
These methods are adding suspicious IP addresses to designated reference sets.

Flowmon: DATALEAKS
The method is aggregating the simple events informing about possible data leaks

Flowmon: DNSTRAFFIC
The method is aggregating simple events informing about the nonstandard DNS traffic

Flowmon: DOSATTACK
The method is aggregating simple events informing about different kinds of denial of service attacks

Flowmon: LARGETRANSFER
The method is aggregating simple events informing about the large data transfers

Flowmon: Load Basic Building Blocks
Rule ensures all Flowmon building blocks are being applied.

Flowmon: MALWARE
The method is aggregating simple events that could be the sign of malware infection

Flowmon: MISCONFIGURED
The method is aggregating simple events that could mean wrong configuration of the device

Flowmon: NETANOMALY
The method is aggregating simple events related to the standard behavior of the network

Flowmon: NETDISCOVERY
The method is aggregating simple events informing about the devices trying to discover the monitored network

Flowmon: PROXYBYPASS
The method is aggregating simple events informing about the devices that are bypassing (or trying to bypass) the specified proxy server

Flowmon: SNIFFER
The method is aggregating simple events unveiling the devices that are possibly eavesdropping the traffic on the network

Flowmon: SPAMMER
The method is aggregating simple events informing about potential spammers

Flowmon: SRVOUTAGE
The method is aggregating simple events informing about unavailable services

Flowmon: UNDESIRED
The method is aggregating simple events informing about the use of applications, that could be undesired in the given environment

Flowmon: VPNTRANSFER
The method is detecting VPN tunneled traffic.

Building blocks

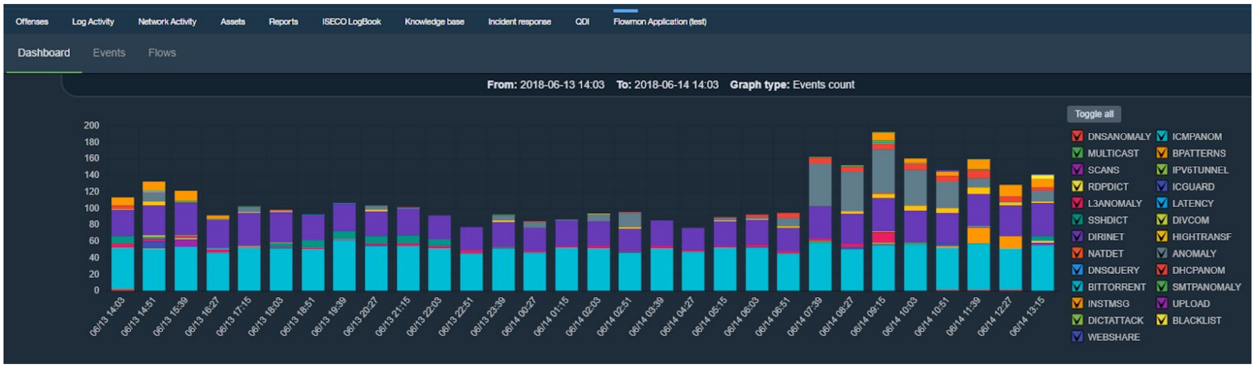
Flowmon content pack also includes several building blocks – these building blocks are used to label Flowmon single events or their combination, building blocks are used in the correlation rules but can be used also in user custom searches and reports.

- Flowmon: BB: ANOMALY
- Flowmon: BB: Anomaly DHCP
- Flowmon: BB: Anomaly L3
- Flowmon: BB: Anomaly or Attack
- Flowmon: BB: Anomaly SMTP
- Flowmon: BB: Attack dst IP followed Anomaly src IP
- Flowmon: BB: Attack or anomaly chain (malware)
- Flowmon: BB: BITTORRENT
- Flowmon: BB: BLACKLIST
- Flowmon: BB: BPATTERNS
- Flowmon: BB: COUNTRY
- Flowmon: BB: DIVCOM
- Flowmon: BB: DNSANOMALY
- Flowmon: BB: DNSQUERY
- Flowmon: BB: HONEYPOT
- Flowmon: BB: ICGUARD
- Flowmon: BB: INSTMSG
- Flowmon: BB: IPV6TUNNEL
- Flowmon: BB: Misconfigured device
- Flowmon: BB: MULTICAST
- Flowmon: BB: Network access attack
- Flowmon: BB: Network anomally
- Flowmon: BB: Network discovery
- Flowmon: BB: REFLECTDOS
- Flowmon: BB: SMTPANOMALY
- Flowmon: BB: SRVNA
- Flowmon: BB: TEAMVIEWER
- Flowmon: BB: TELNET
- Flowmon: BB: TOR
- Flowmon: BB: Undesired apps
- Flowmon: BB: Upload or Country
- Flowmon: BB: Upload or Webshare

- Flowmon: BB: Utilization
- Flowmon: BB: WEBSHARE

Flowmon App - Dashboard

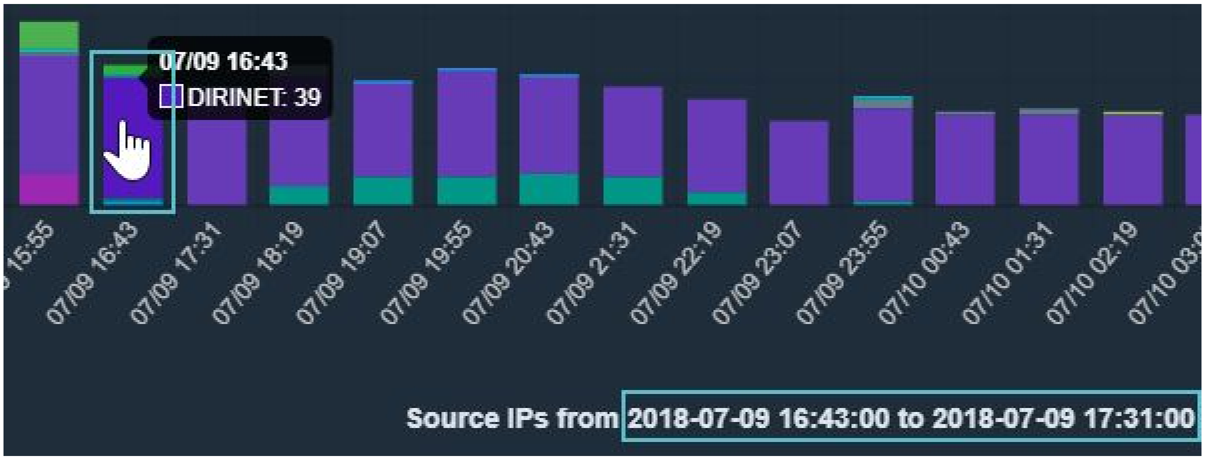
Flowmon App Dashboard provides overview of events and detection methods. Dashboard consists of a main stacked column graph, expandable filter above the main graph and interactive legend on the right side.



From: 2018-06-13 14:03 **To:** 2018-06-14 14:03 **Graph type:** Events count

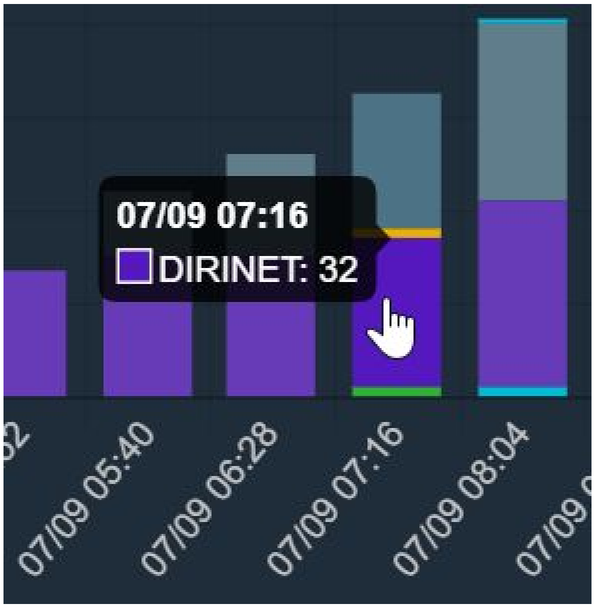
Main graph

Each column in the main graph represents timeframe which begins at time specified under the column and ends when the new column begins. There are always 30 columns and timeframe of each column scales with the time interval specified in the filter (For example, each column represents 1 minute when filter is set between 10:00 and 10:30).



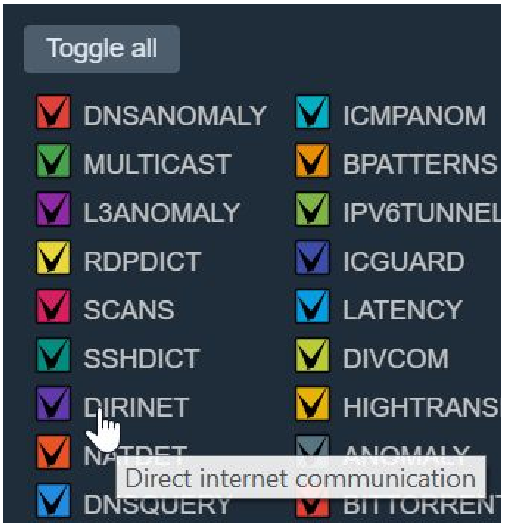
Source IPs from 2018-07-09 16:43:00 to 2018-07-09 17:31:00

Hovering over column segment in the main graph shows the name of detection method to which does the event relate to.

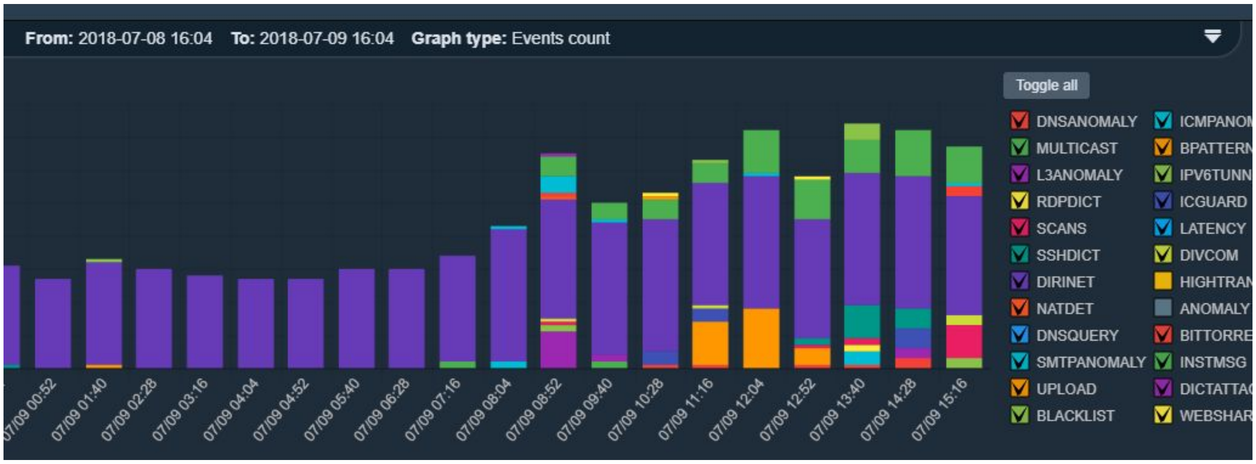


Legend

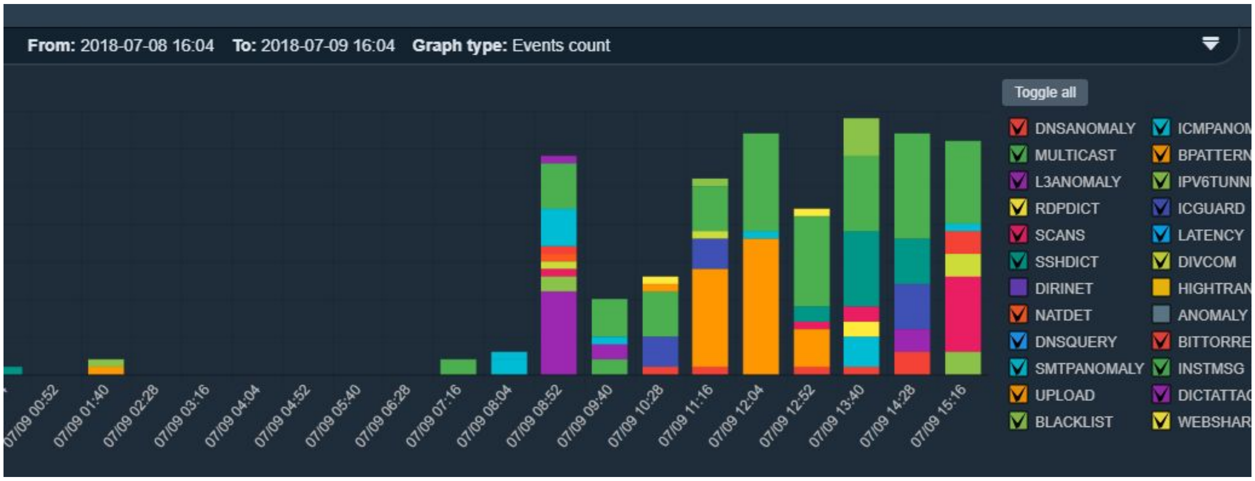
Hovering over the detection method abbreviation in legend reveals tooltip with explanation.



Use the legend to show/hide specific detection methods from the main graph (before and after hiding DIRINET):



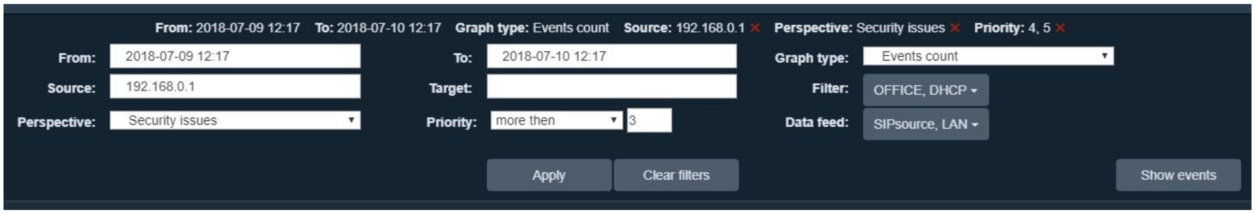
From: 2018-07-08 16:04 **To:** 2018-07-09 16:04 **Graph type:** Events count



From: 2018-07-08 16:04 **To:** 2018-07-09 16:04 **Graph type:** Events count

This is one of the ways to tidy up the main graph. Alternatively, click "Toggle all" above the legend to hide all detection methods and only select the ones you need.

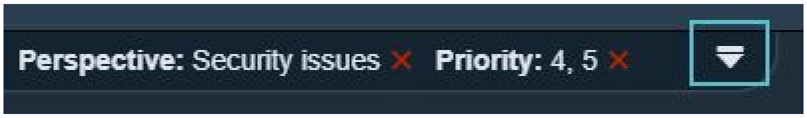
Filter



From: 2018-07-09 12:17 **To:** 2018-07-10 12:17 **Graph type:** Events count **Source:** 192.168.0.1 × **Perspective:** Security issues × **Priority:** 4, 5 ×

From:	2018-07-09 12:17	**To:**	2018-07-10 12:17	**Graph type:**	Events count
Source:	192.168.0.1	**Target:**		**Filter:**	OFFICE, DHCP
Perspective:	Security issues	**Priority:**	more then 3	**Data feed:**	SIPsource, LAN

Expand filter by clicking on the expand arrow on the right side:



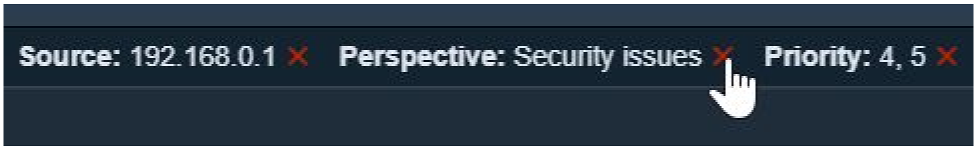
Perspective: Security issues × **Priority:** 4, 5 ×

Filter in Dashboard provides the following options:

- Filter by Time interval.

- Specify the graph type (Events, Sources or Targets count).
- Filter by Source and Target.
- Filter by Perspective.
- Filter by Priority (above, below and specific priority).
- Filter by both atomic and relations filters from Flowmon ADS Processing.
- Filter by Data feed (flow data source).
- Show Events button

Applied filter parameters can be quickly removed by clicking on the red x mark:



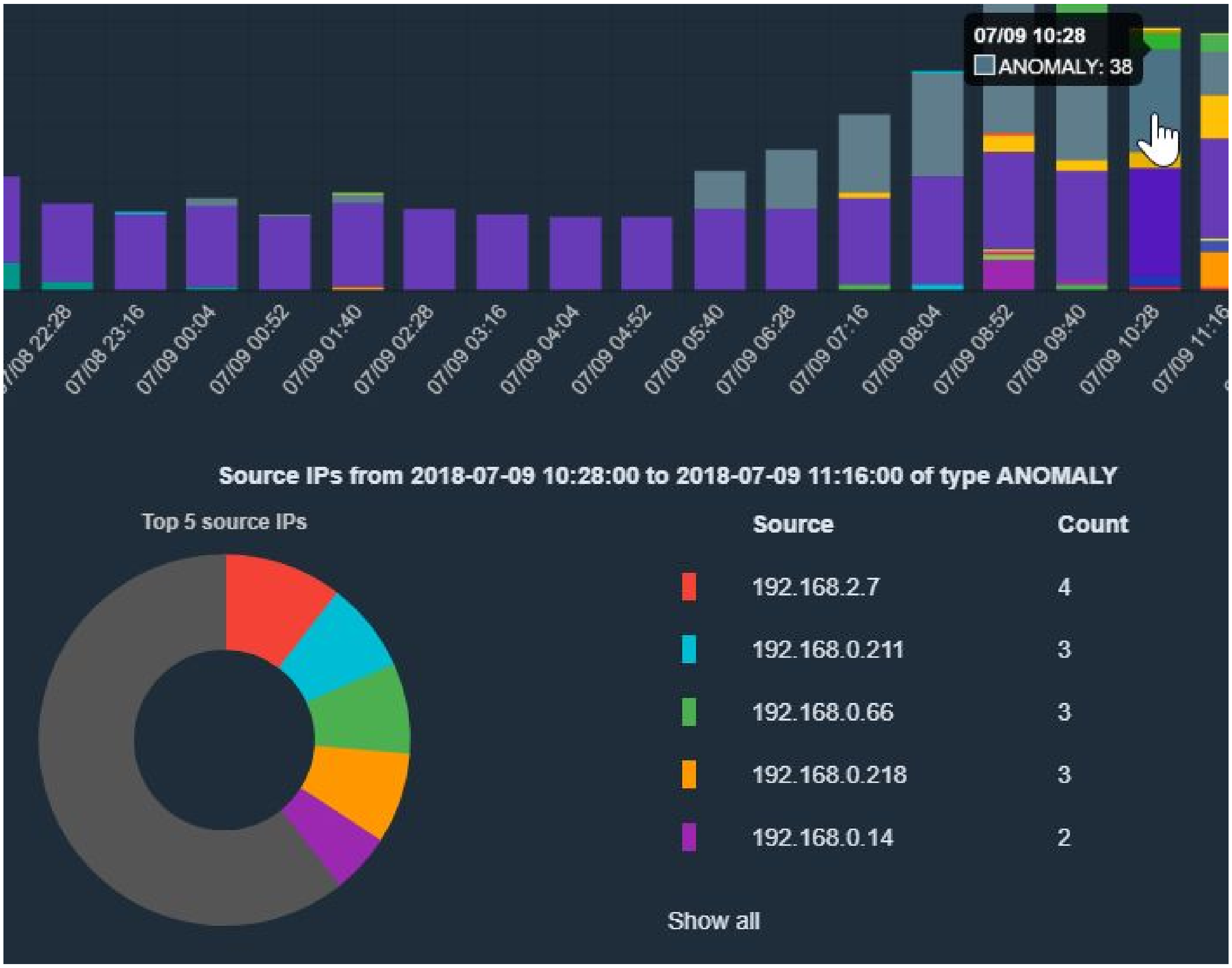
Source: 192.168.0.1 ✕ **Perspective:** Security issues ✕ **Priority:** 4, 5 ✕

Workflow of switching between Dashboard, Events and Flows

On Dashboard, clicking on the button "Show events" in the filter changes view to Events and automatically pre-filters the event list. Similarly, applying specific IP address as a filter to the Events table changes view to Events. In Events view there are similar buttons to switch back to Dashboard and drill-down to individual Flows. In Flows view you can switch back to Events. This makes investigation and switching between Dashboard, Events and Flows intuitive and easy.

Detail

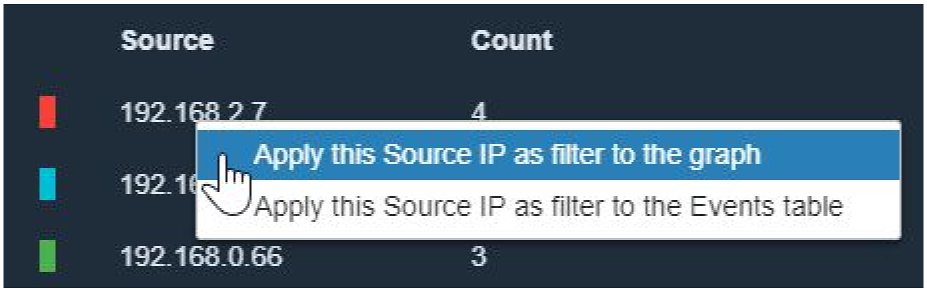
Clicking on a column in the main graph shows details for this timeframe and detection method. Donut chart shows event count for each of the top 5 source IP addresses for the specified detection method. Click "Show all" to expand the list of all IPs.



Source IPs from 2018-07-09 10:28:00 to 2018-07-09 11:16:00 of type ANOMALY

	Source	Count
🟥	192.168.2.7	4
🟦	192.168.0.211	3
🟩	192.168.0.66	3
🟧	192.168.0.218	3
🟪	192.168.0.14	2

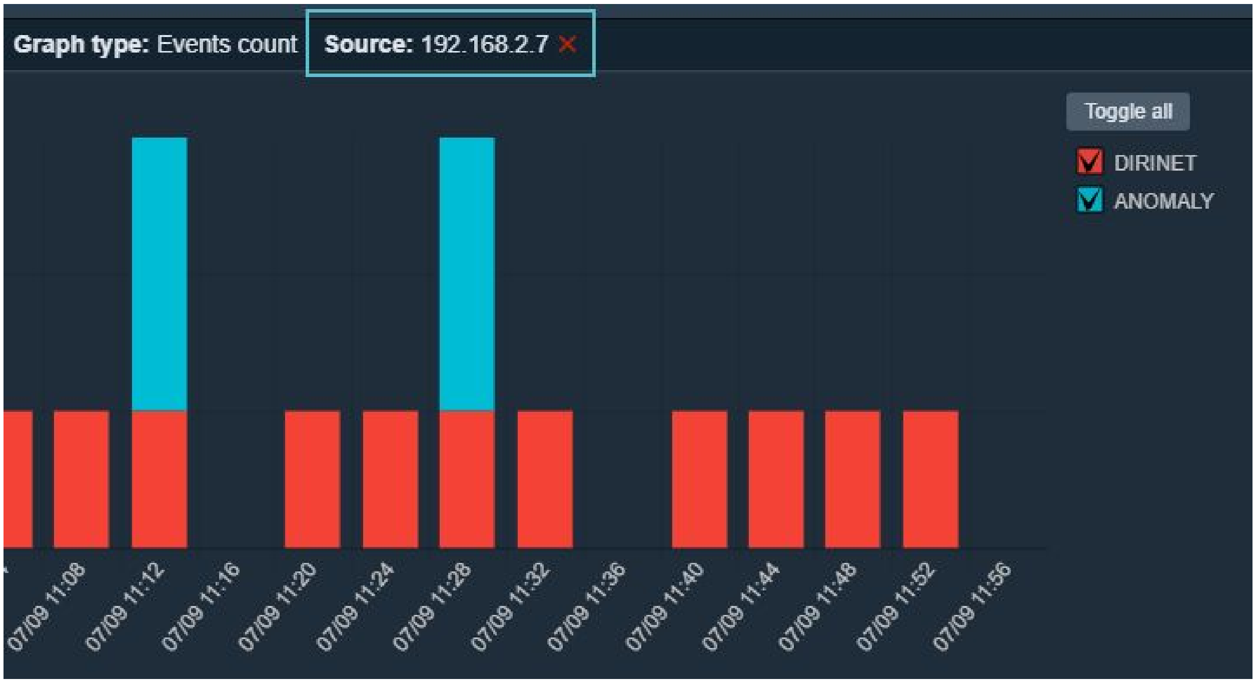
Click on the IP address to examine it further. There are two options:


Apply this Source IP as filter to the graph
Apply this Source IP as filter to the Events table

	Source	Count
🟥	192.168.2.7	4
🟦	192.1	
🟩	192.168.0.66	3

Detail - Apply Source IP to the graph

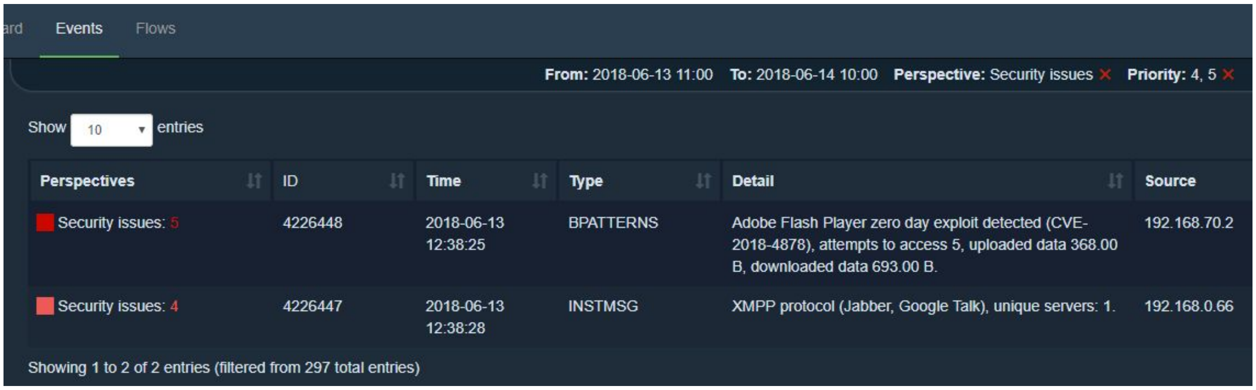
After applying IP to the main graph, filter above the graph shows selected IP as a Source. Main graph now shows what events and when does the IP caused.



Detail - Apply Source IP to the Events table

This action switches from Dashboard to Events view. Time interval in Events filter corresponds to column timeframe previously selected in the Dashboard.

Flowmon App - Events



ard Events Flows

From: 2018-06-13 11:00 **To:** 2018-06-14 10:00 **Perspective:** Security issues ✕ **Priority:** 4, 5 ✕

Show 10 entries

Perspectives	ID	Time	Type	Detail	Source
🟥 Security issues: 5	4226448	2018-06-13 12:38:25	BPATTERNS	Adobe Flash Player zero day exploit detected (CVE-2018-4878), attempts to access 5, uploaded data 368.00 B, downloaded data 693.00 B.	192.168.70.2
🟥 Security issues: 4	4226447	2018-06-13 12:38:28	INSTMSG	XMPP protocol (Jabber, Google Talk), unique servers: 1.	192.168.0.66

Showing 1 to 2 of 2 entries (filtered from 297 total entries)

In Events view you can inspect individual events. Events can be classified to perspectives (event can belong to zero or multiple perspectives). Similarly, event priority can be specified. Each event is identified with a unique ID and have a timestamp (Time). Type column specifies the detection method type. More detailed information can be found in the Detail column. Involved IP addresses are specified in columns Source and Targets. Data feeds specify flow data source.

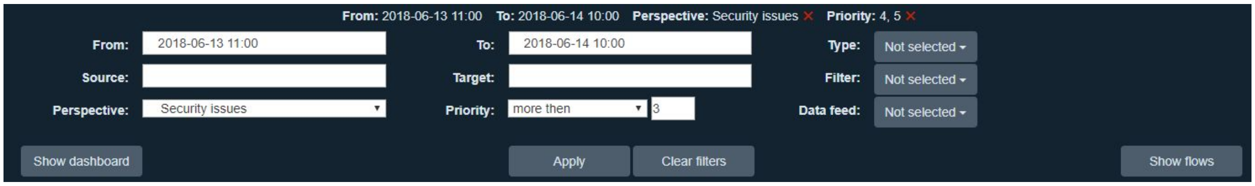
Perspectives and Data feeds are configured in Flowmon Solution. See Flowmon ADS User Guide for details.

Events unassigned to any perspective can be listed selecting the "-" in the Perspective drop-down menu in the filter. You can use this to verify that all events which should have been classified were assigned perspective. You can also check whether events are being classified to the right perspective when sending with syslog to QRadar.

Filter

Filter in Events view provides following options:

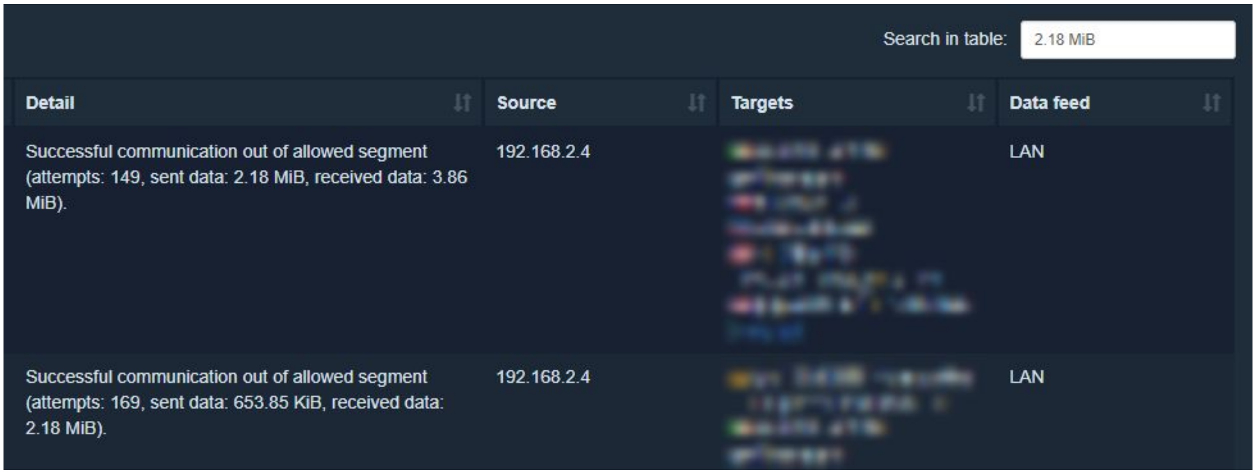
- Filter by Time interval.
- Filter by Type of detection method.
- Filter by Source and Target.
- Filter by Perspective.
- Filter by Priority (above, below and specific priority).
- Filter by both atomic and relations filters from Flowmon ADS Processing.
- Filter by Data feed (flow data source).
- Show Dashboard button and keep the filter
- Show flows - switch to Filters and keep the selected time interval



From: 2018-06-13 11:00 **To:** 2018-06-14 10:00 **Perspective:** Security issues ✕ **Priority:** 4, 5 ✕

From:	2018-06-13 11:00	To:	2018-06-14 10:00	Type:	Not selected
Source:		Target:		Filter:	Not selected
Perspective:	Security issues	Priority:	more then 3	Data feed:	Not selected

Instant search



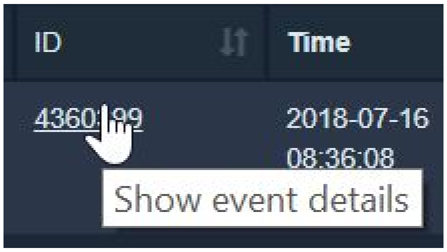
Search in table: 2.18 MiB

Detail	Source	Targets	Data feed
Successful communication out of allowed segment (attempts: 149, sent data: 2.18 MiB, received data: 3.86 MiB).	192.168.2.4	[redacted]	LAN
Successful communication out of allowed segment (attempts: 169, sent data: 653.85 KiB, received data: 2.18 MiB).	192.168.2.4	[redacted]	LAN

This feature allows to instantly find events by a particular piece of information. Just start typing and table of events will be filtered on-the-fly. Partial matches are supported.

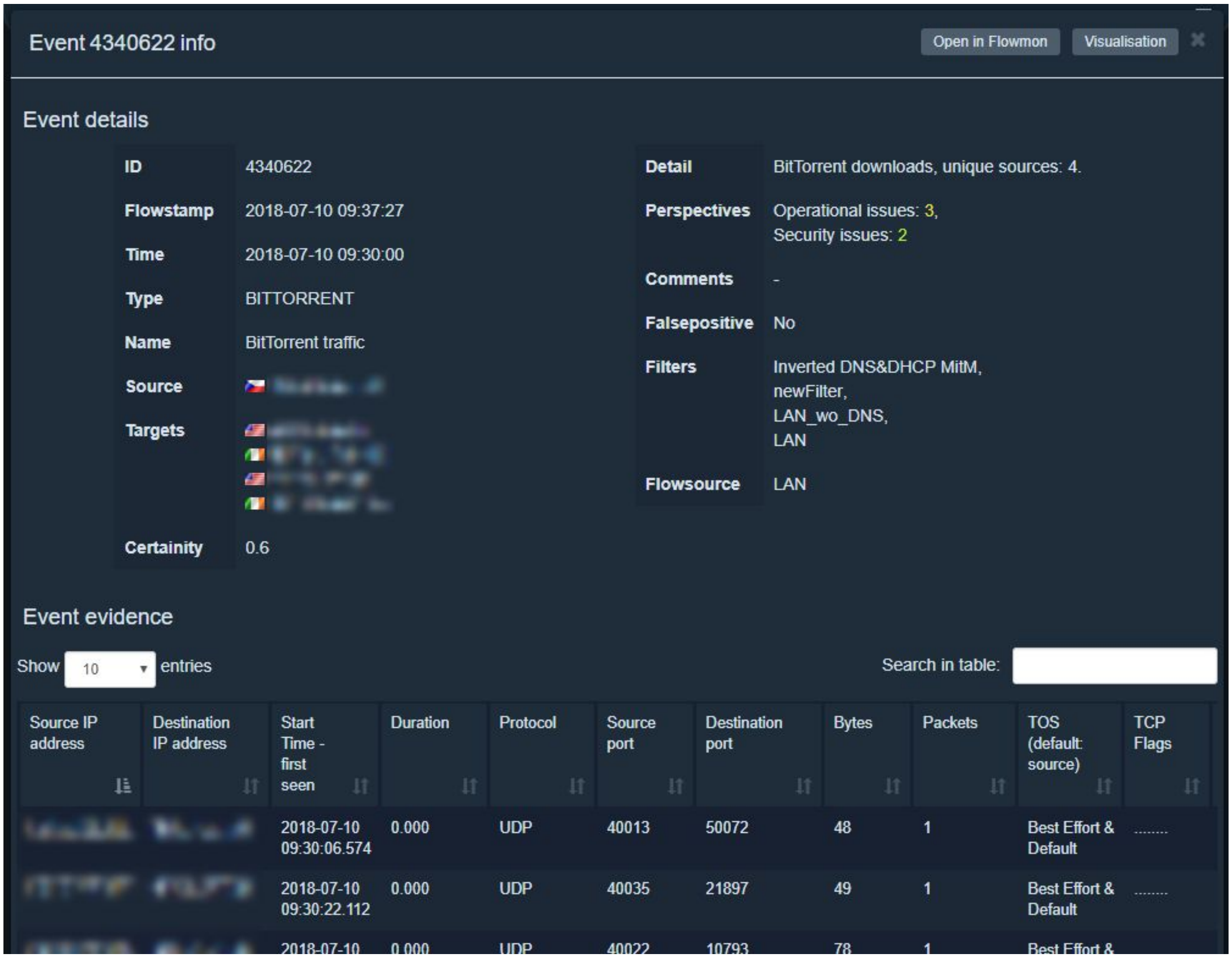
Event info (Event Details and Evidence)

Double-click on a event row in the table or click on an event ID to open window with event info window with event details and evidence.



ID	Time
4360[illegible]99	2018-07-16 08:36:08

Here you can see all the information about the event and associated flows.



Event 4340622 info

Event details

ID	4340622	**Detail**	BitTorrent downloads, unique sources: 4.
Flowstamp	2018-07-10 09:37:27	**Perspectives**	Operational issues: 3, Security issues: 2
Time	2018-07-10 09:30:00	**Comments**	-
Type	BITTORRENT	**Falsepositive**	No
Name	BitTorrent traffic	**Filters**	Inverted DNS&DHCP MitM, newFilter, LAN_wo_DNS, LAN
Source	[redacted]	**Flowsource**	LAN
Targets	[redacted]		
Certainity	0.6		

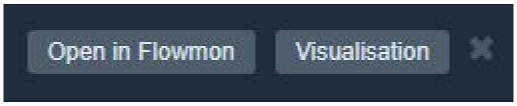
Event evidence

Show 10 entries

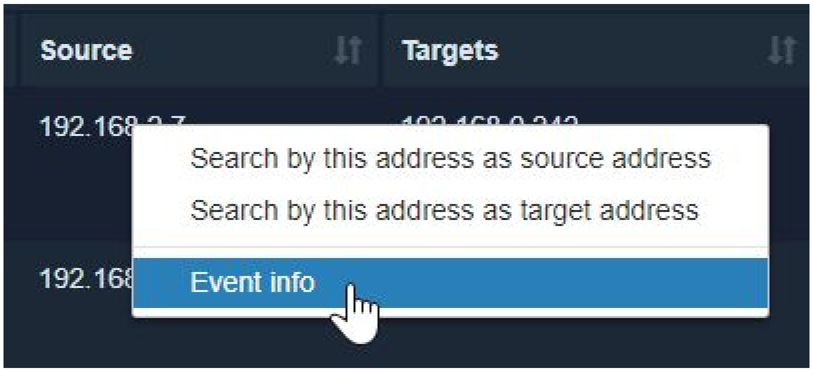
Search in table:

Source IP address	Destination IP address	Start Time - first seen	Duration	Protocol	Source port	Destination port	Bytes	Packets	TOS (default: source)	TCP Flags
[redacted]	[redacted]	2018-07-10 09:30:06.574	0.000	UDP	40013	50072	48	1	Best Effort & Default	....
[redacted]	[redacted]	2018-07-10 09:30:22.112	0.000	UDP	40035	21897	49	1	Best Effort & Default	....
[redacted]	[redacted]	2018-07-10	0.000	UDP	40022	10793	78	1	Best Effort &	

You can inspect event directly in Flowmon Solution. Use the buttons in the top right corner. *Open in Flowmon* button opens a new browser tab with a deep link right to the event details in Flowmon Solution. Similarly, *Visualisation* button opens an interactive event visualization in Flowmon Solution.

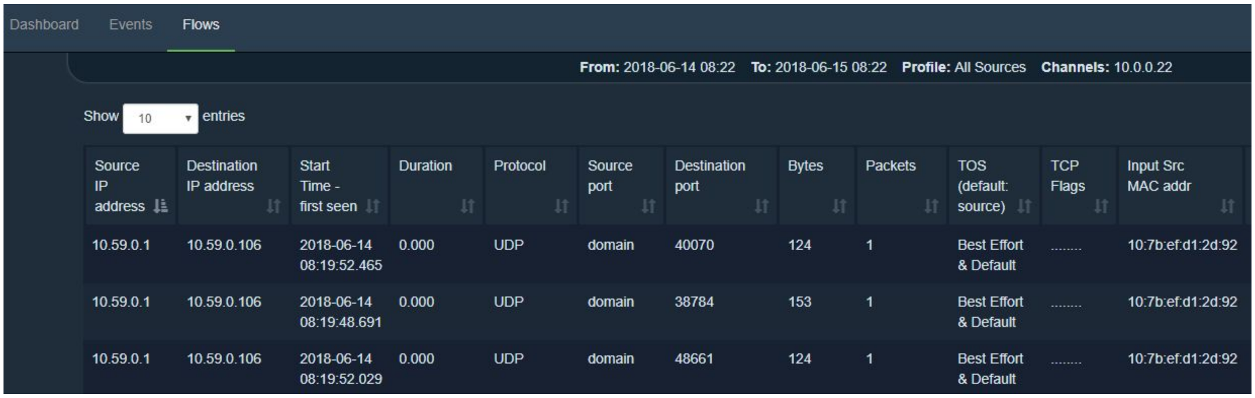


Right-click on Source and Target IP addresses provides an option to add address to a filter. Right-click anywhere on event row provides an option to open event info window.


Source
Targets
192.168.2.7
192.168.0.242
Search by this address as source address
Search by this address as target address
Event info
192.168

Flowmon App - Flows

In Flows view you can inspect individual flows, sort flows by columns, use instant search and apply filters.



From: 2018-06-14 08:22 **To:** 2018-06-15 08:22 **Profile:** All Sources **Channels:** 10.0.0.22

Show 10 entries

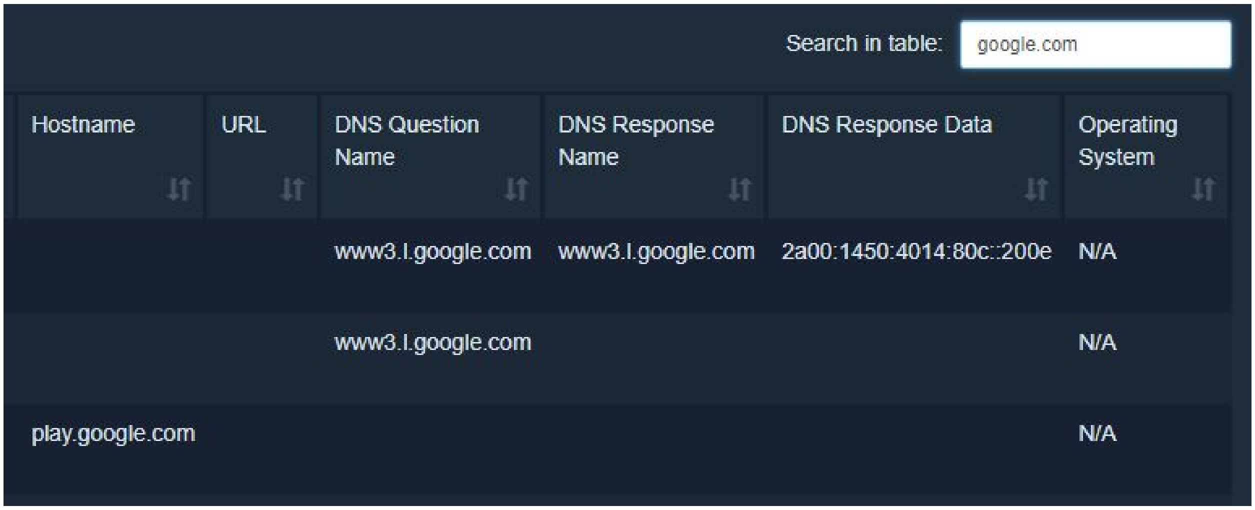
Source IP address	Destination IP address	Start Time - first seen	Duration	Protocol	Source port	Destination port	Bytes	Packets	TOS (default: source)	TCP Flags	Input Src MAC addr
10.59.0.1	10.59.0.106	2018-06-14 08:19:52.465	0.000	UDP	domain	40070	124	1	Best Effort & Default	....	10:7b:ef:d1:2d:92
10.59.0.1	10.59.0.106	2018-06-14 08:19:48.691	0.000	UDP	domain	38784	153	1	Best Effort & Default	....	10:7b:ef:d1:2d:92
10.59.0.1	10.59.0.106	2018-06-14 08:19:52.029	0.000	UDP	domain	48661	124	1	Best Effort & Default	....	10:7b:ef:d1:2d:92

Column configuration

See chapter Flows output format to configure which columns are shown and their order.

Instant search

This feature enables you to type in any column value and immediately get a list of flows where is this value used. Partial matches are supported.



Search in table: google.com

Hostname	URL	DNS Question Name	DNS Response Name	DNS Response Data	Operating System
		www3.l.google.com	www3.l.google.com	2a00:1450:4014:80c::200e	N/A
		www3.l.google.com			N/A
play.google.com					N/A

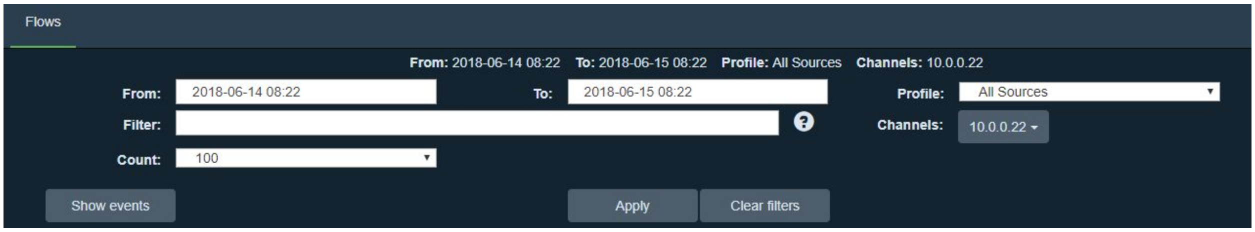
Filters

In Flows view you can use filters to narrow down list of flows before turning to instant search.

Filter in Flows provides option to:

- Filter by Time interval
- Filter by Profile
- Filter by Channels
- Use advanced filter (click on the question mark icon to show how-to)
- Specify number of flows in the result (Count)

- Switch to Events and keep the selected time interval (Show events)



From: 2018-06-14 08:22 **To:** 2018-06-15 08:22 **Profile:** All Sources **Channels:** 10.0.0.22

From: 2018-06-14 08:22

To: 2018-06-15 08:22

Profile: All Sources

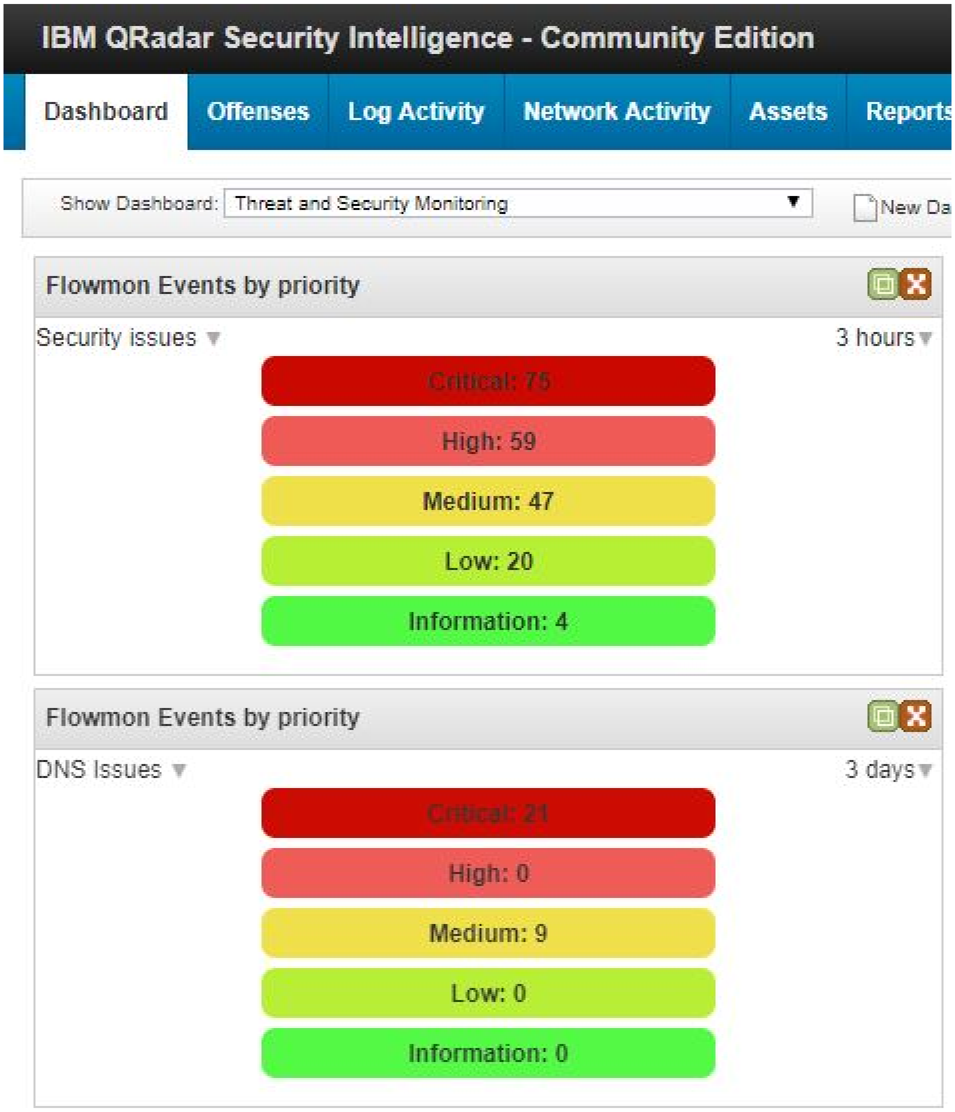
Filter:

Channels: 10.0.0.22

Count: 100

Flowmon QRadar Dashboard Widget

Widgets provide a quick overview of events by priority right in IBM QRadar Dashboard. Up to 5 Flowmon widgets can be added. Perspective and Time interval can be specified for each widget.



Show Dashboard: Threat and Security Monitoring

Flowmon Events by priority

Security issues ▼ 3 hours ▼

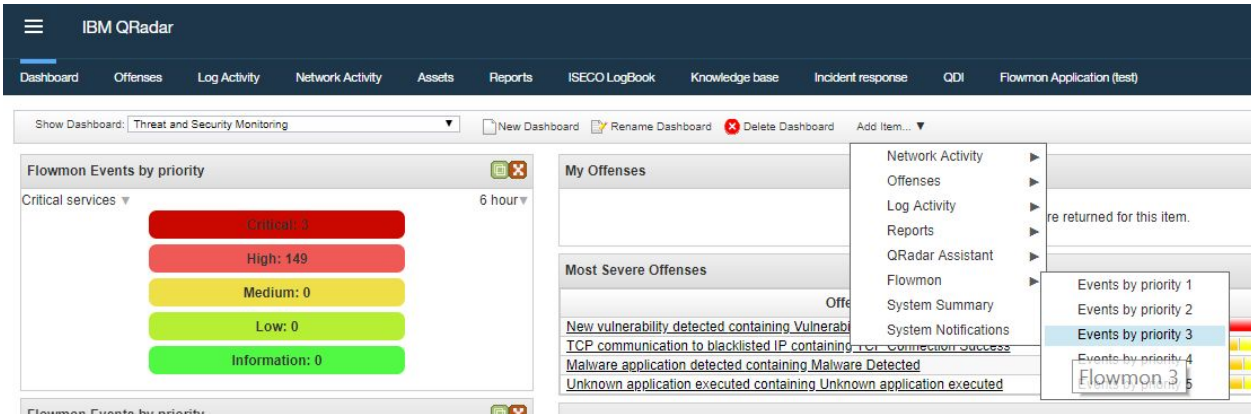
Critical: 75
High: 59
Medium: 47
Low: 20
Information: 4

Flowmon Events by priority

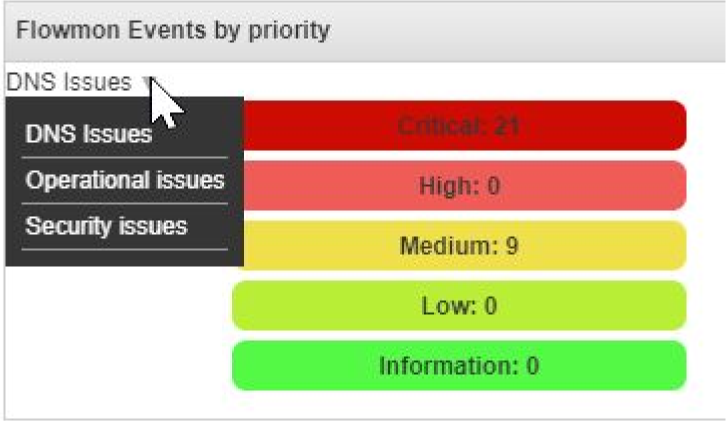
DNS Issues ▼ 3 days ▼

Critical: 21
High: 0
Medium: 9
Low: 0
Information: 0

To add a new Flowmon widget, press Add item, select Flowmon and add desired Widget. There can be up to 5 widgets (numbered 1 to 5), as QRadar allows to place the widget 5 times each time with a different configuration. Drag and drop widget to move it to a specific place on the dashboard.



To change widget perspective, click on currently selected perspective and choose a new one.

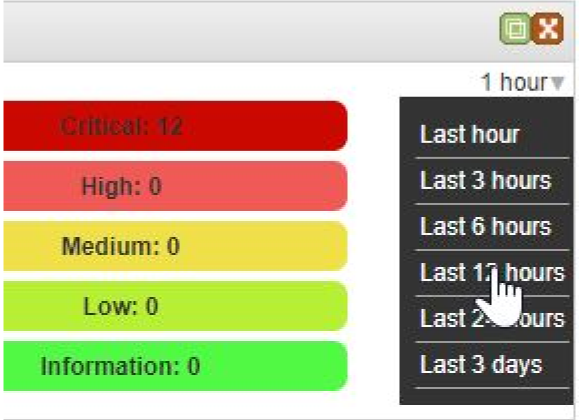


Note that perspectives are defined in Flowmon ADS. In this example we are using perspectives from our demo:

- Man-in-the-Middle Attack, DNS amplification, DHCP (APT)
- Critical services
- Alerts
- Operational issues
- Security issues

To define your own perspectives, follow Flowmon ADS User Guide (Chapter 2: Installation and configuration > Configuration of perspectives).

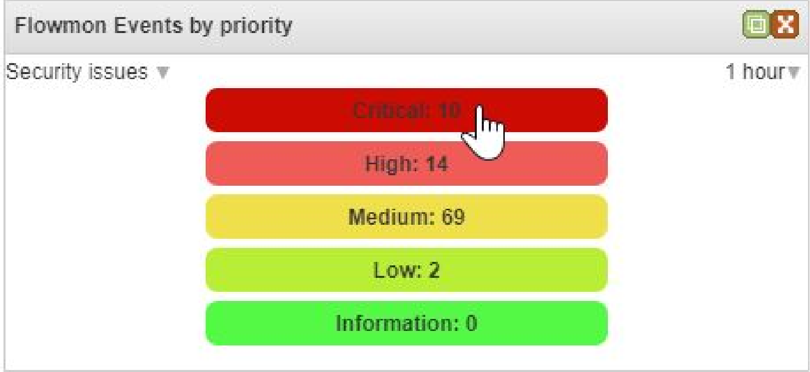
To change Time interval, click on the currently selected Time interval and choose a new one.



Critical: 12
High: 0
Medium: 0
Low: 0
Information: 0

Clicking on any row in a Widget (Critical, High, Medium, Low or Information) takes you directly to automatically pre-filtered list of events in Flowmon App.

For example, clicking on Critical row in this widget:

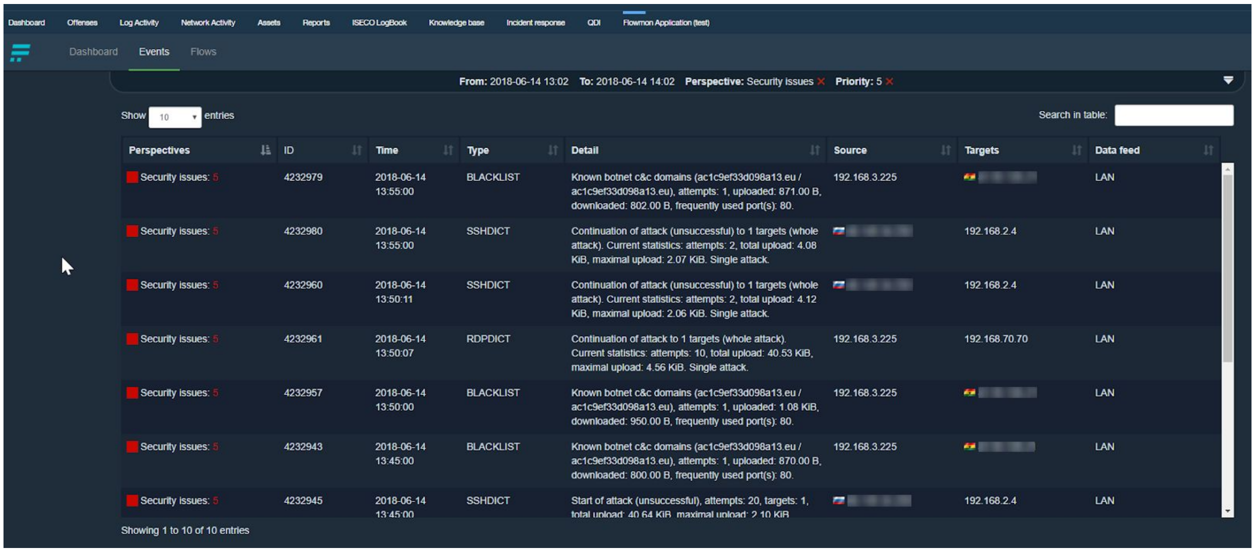


Flowmon Events by priority

Security issues ▾ 1 hour ▾

Critical: 10
High: 14
Medium: 69
Low: 2
Information: 0

Will open list of related events in Flowmon App:



From: 2018-06-14 13:02 **To:** 2018-06-14 14:02 **Perspective:** Security issues ✕ **Priority:** 5 ✕

Show 10 ▾ entries

Search in table:

Perspectives	ID	Time	Type	Detail	Source	Targets	Data feed
🟥 Security issues: 5	4232979	2018-06-14 13:55:00	BLACKLIST	Known botnet c&c domains (ac1c9ef33d098a13.eu / ac1c9ef33d098a13.eu), attempts: 1, uploaded: 871.00 B, downloaded: 802.00 B, frequently used port(s): 80.	192.168.3.225	[redacted]	LAN
🟥 Security issues: 5	4232980	2018-06-14 13:55:00	SSHDICT	Continuation of attack (unsuccessful) to 1 targets (whole attack). Current statistics: attempts: 2, total upload: 4.08 KiB, maximal upload: 2.07 KiB. Single attack.	[redacted]	192.168.2.4	LAN
🟥 Security issues: 5	4232960	2018-06-14 13:50:11	SSHDICT	Continuation of attack (unsuccessful) to 1 targets (whole attack). Current statistics: attempts: 2, total upload: 4.12 KiB, maximal upload: 2.06 KiB. Single attack.	[redacted]	192.168.2.4	LAN
🟥 Security issues: 5	4232961	2018-06-14 13:50:07	RDPDICT	Continuation of attack to 1 targets (whole attack). Current statistics: attempts: 10, total upload: 40.53 KiB, maximal upload: 4.56 KiB. Single attack.	192.168.3.225	192.168.70.70	LAN
🟥 Security issues: 5	4232957	2018-06-14 13:50:00	BLACKLIST	Known botnet c&c domains (ac1c9ef33d098a13.eu / ac1c9ef33d098a13.eu), attempts: 1, uploaded: 1.08 KiB, downloaded: 950.00 B, frequently used port(s): 80.	192.168.3.225	[redacted]	LAN
🟥 Security issues: 5	4232943	2018-06-14 13:45:00	BLACKLIST	Known botnet c&c domains (ac1c9ef33d098a13.eu / ac1c9ef33d098a13.eu), attempts: 1, uploaded: 870.00 B, downloaded: 800.00 B, frequently used port(s): 80.	192.168.3.225	[redacted]	LAN
🟥 Security issues: 5	4232945	2018-06-14 13:45:00	SSHDICT	Start of attack (unsuccessful), attempts: 20, targets: 1, total upload: 40.64 KiB, maximal upload: 2.10 KiB	[redacted]	192.168.2.4	LAN

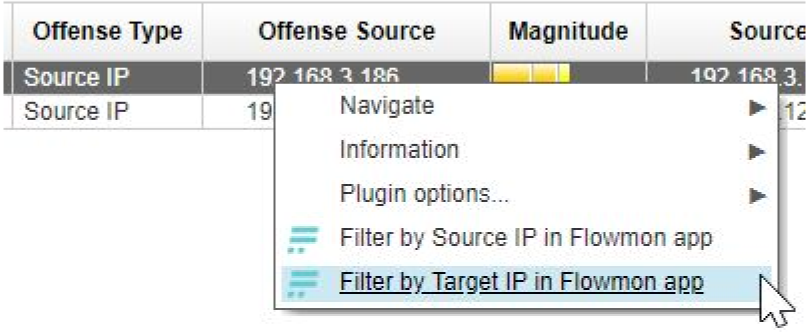
Showing 1 to 10 of 10 entries

Note automatically applied filter above the list:

Opening Flowmon Application directly from Offenses & Log Activity

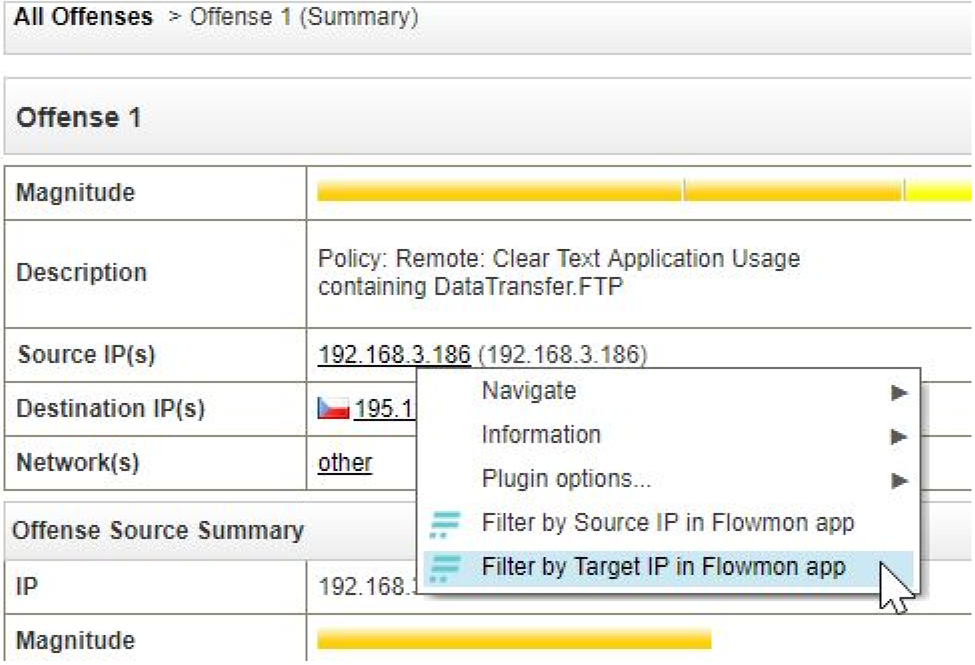
Quickly find related events for a particular IP addresses directly from Offenses and Log Activity pages. Options to pre-filter IP address has been added to the context menu (you can choose whether to filter the IP as Source or Target).

Context menu is available in both offenses list and in offense summary.



Offense Type	Offense Source	Magnitude	Source
Source IP	192.168.3.186		192.168.3.
Source IP	19		12

Navigate ▶
Information ▶
Plugin options... ▶
Filter by Source IP in Flowmon app
Filter by Target IP in Flowmon app



All Offenses > Offense 1 (Summary)

Offense 1

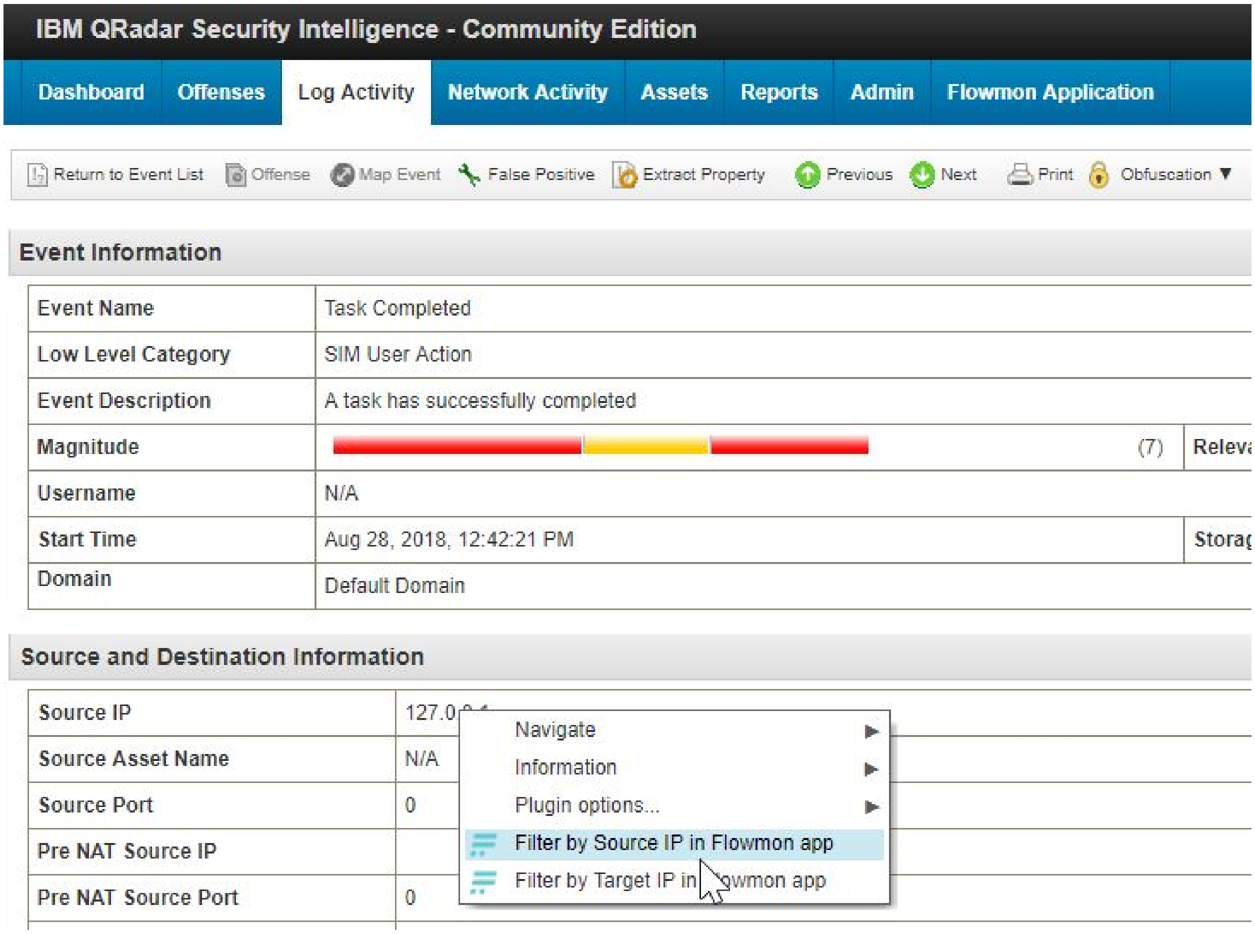
Magnitude	
Description	Policy: Remote: Clear Text Application Usage containing DataTransfer.FTP
Source IP(s)	192.168.3.186 (192.168.3.186)
Destination IP(s)	195.1
Network(s)	other

Offense Source Summary

IP	192.168.3
Magnitude	

Navigate ▶
Information ▶
Plugin options... ▶
Filter by Source IP in Flowmon app
Filter by Target IP in Flowmon app

Context menu in Log Activity.



Event Information

Event Name	Task Completed	
Low Level Category	SIM User Action	
Event Description	A task has successfully completed	
Magnitude	🟥🟨🟥 (7)	Releva
Username	N/A	
Start Time	Aug 28, 2018, 12:42:21 PM	Storag
Domain	Default Domain	

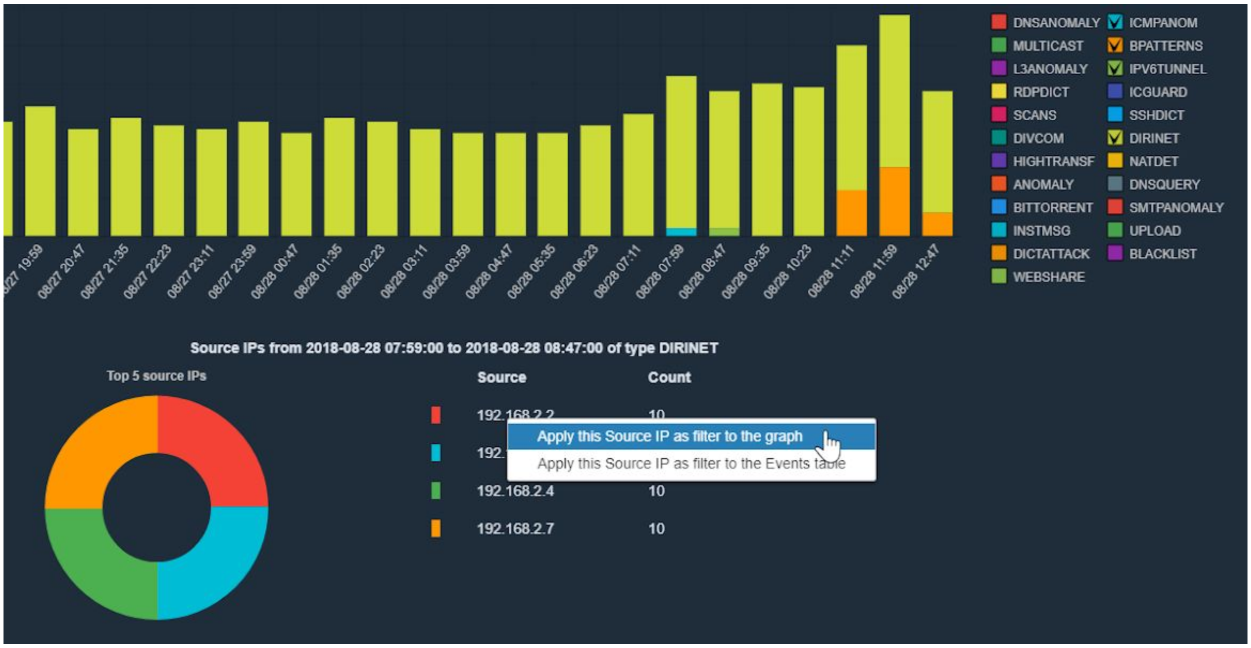
Source and Destination Information

Source IP	127.0
Source Asset Name	N/A
Source Port	0
Pre NAT Source IP	
Pre NAT Source Port	0

Investigation examples (use-cases)

Activities of a specific IP address

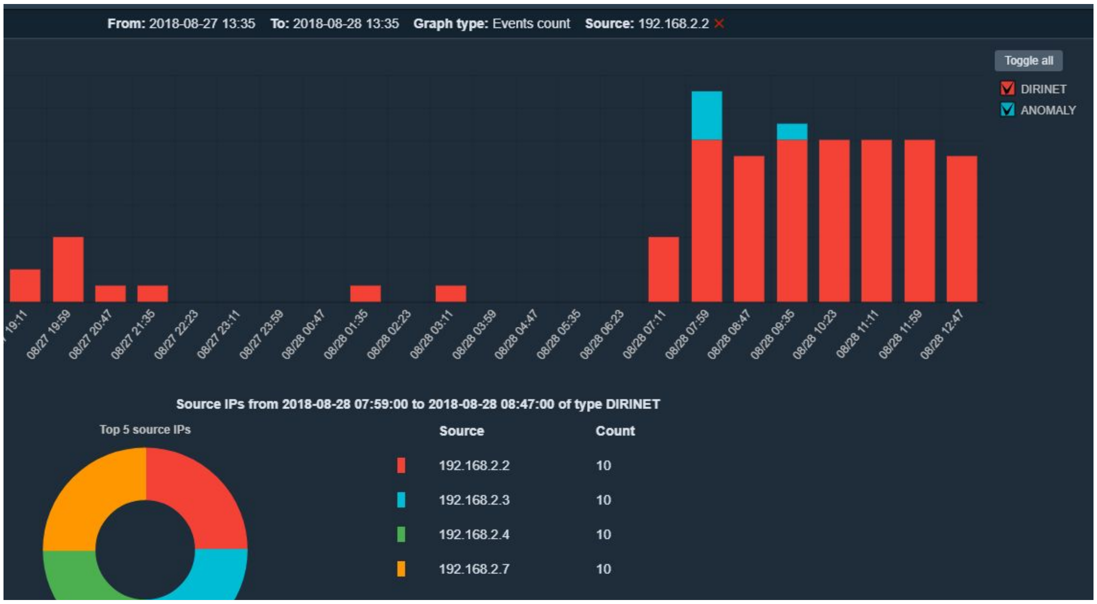
In Dashboard, we've selected several detection methods. Once of the peaks corresponds to DIRINET (Direct internet communication). By clicking on the bar in the chart we open details below with a donut chart and list of IPs.



Source IPs from 2018-08-28 07:59:00 to 2018-08-28 08:47:00 of type DIRINET

	Source	Count
🟥	192.168.2.2	10
🟦	192.	
🟩	192.168.2.4	10
🟧	192.168.2.7	10

We apply first IP with highest count as Source IP to the graph. This gives us an overview about detected activities throughout the day.



From: 2018-08-27 13:35 **To:** 2018-08-28 13:35 **Graph type:** Events count **Source:** 192.168.2.2 ✕

Source IPs from 2018-08-28 07:59:00 to 2018-08-28 08:47:00 of type DIRINET

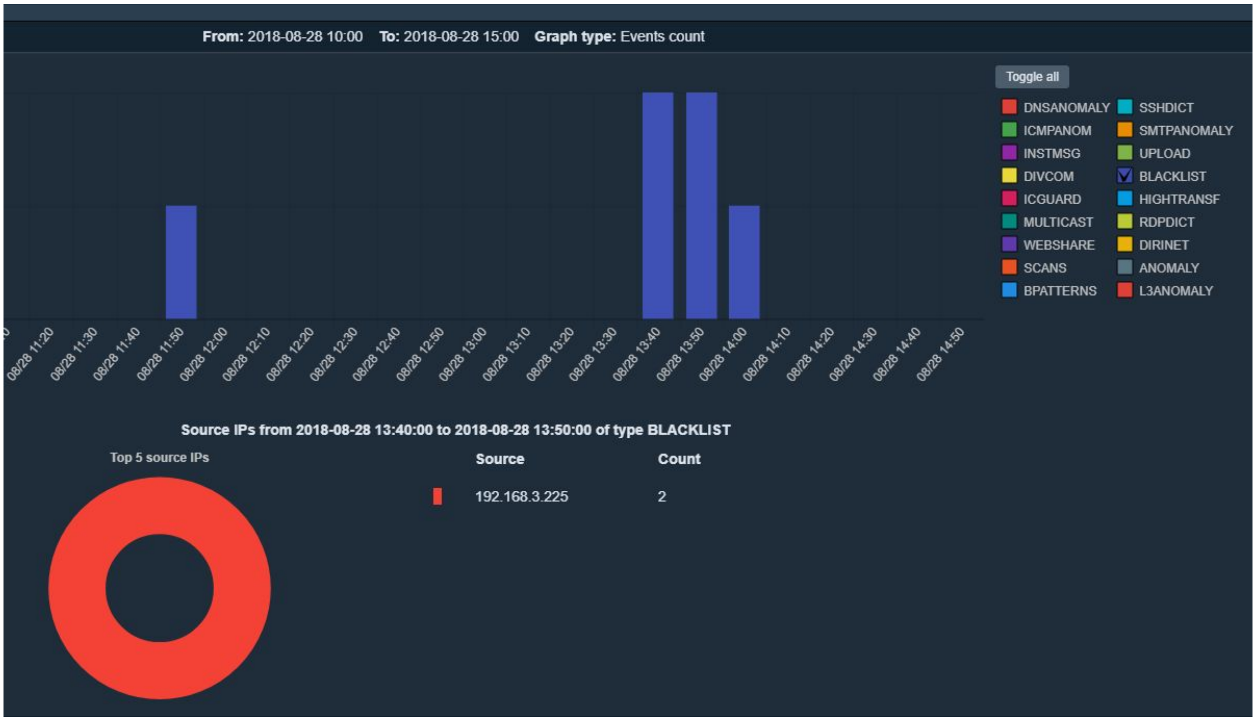
	Source	Count
🟥	192.168.2.2	10
🟦	192.168.2.3	10
🟩	192.168.2.4	10
🟧	192.168.2.7	10

We can see that there were a couple of ANOMALY events, the rest is DIRINET.

Suspicious activity of an IP

This is a basic example showing how to investigate suspicious host.

Let's investigate communication with blacklisted hosts in the Dashboard. Untoggle all and check BLACKLIST.

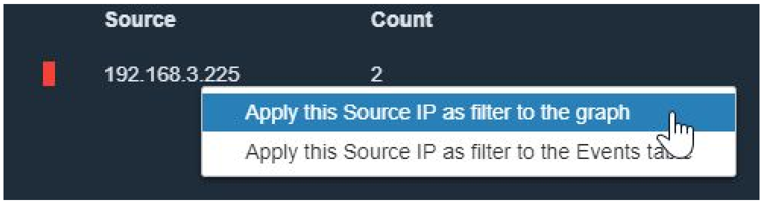


From: 2018-08-28 10:00 **To:** 2018-08-28 15:00 **Graph type:** Events count

Source IPs from 2018-08-28 13:40:00 to 2018-08-28 13:50:00 of type BLACKLIST

	Source	Count
🟥	192.168.3.225	2

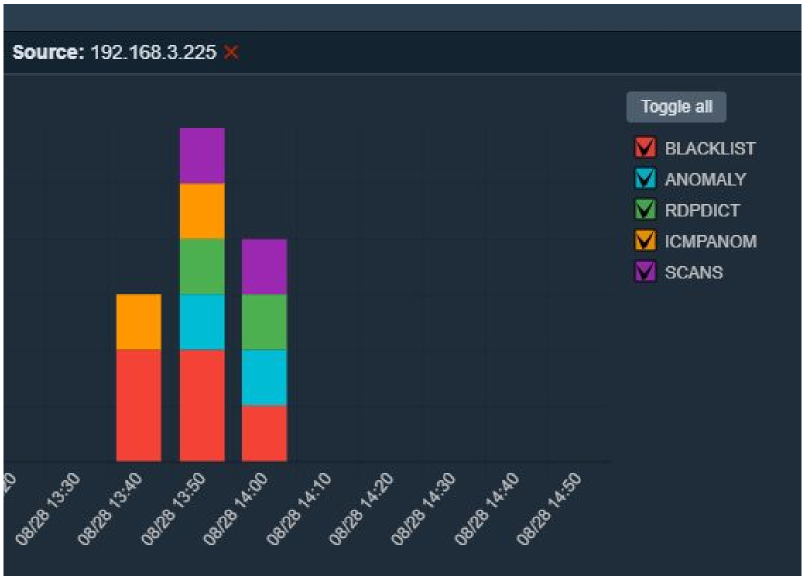
IP 192.168.3.225 is a source of this communication. This is an IoC (Indicator of Compromise). Let's what has been this IP up to by applying it as a filter to the graph.



	Source	Count
🟥	192.168.3.225	2

Apply this Source IP as filter to the graph
Apply this Source IP as filter to the Events ta

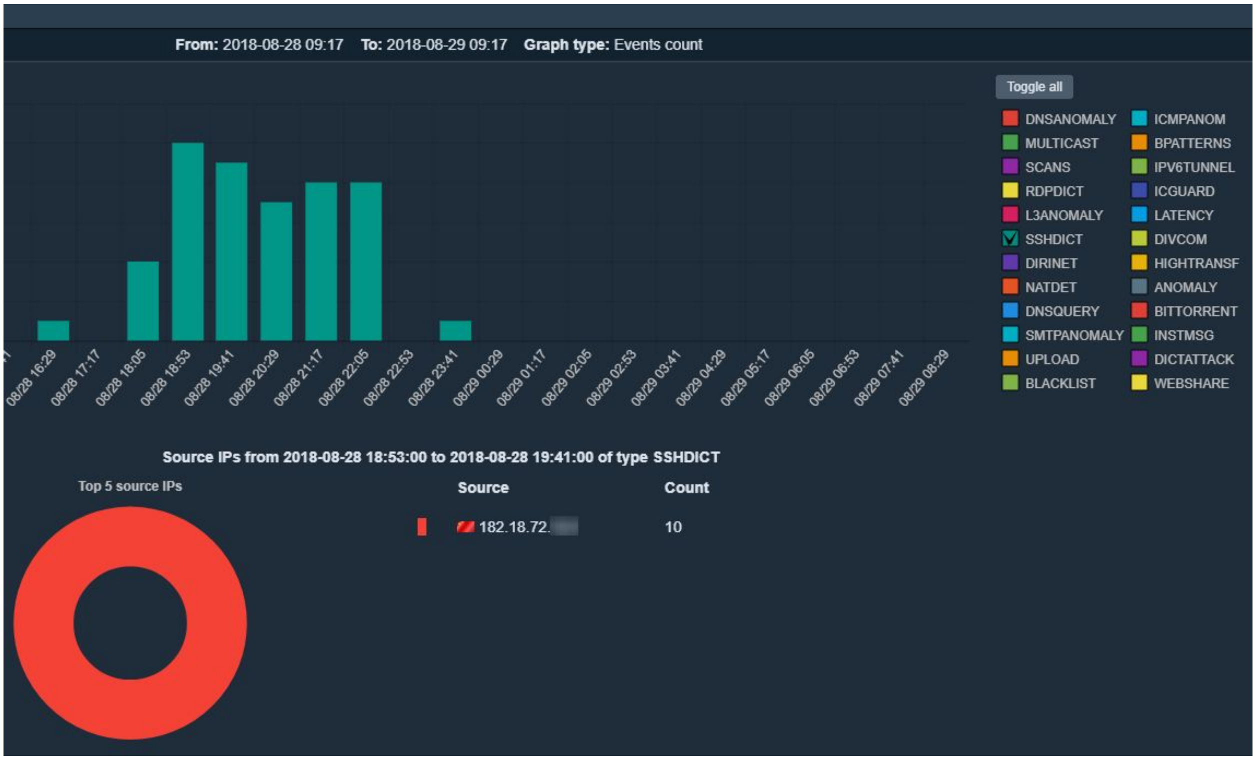
And we can see that the IP has been involved in scanning, dictionary attacks and anomalies as a source and it means that the host was probably compromised.


Source: 192.168.3.225 ×

From dictionary attacks to compromised host

In this example, we'll see how an attack can spread. We're going to observe host (victim) becoming the source of subsequent attacks and investigate the chain of events.

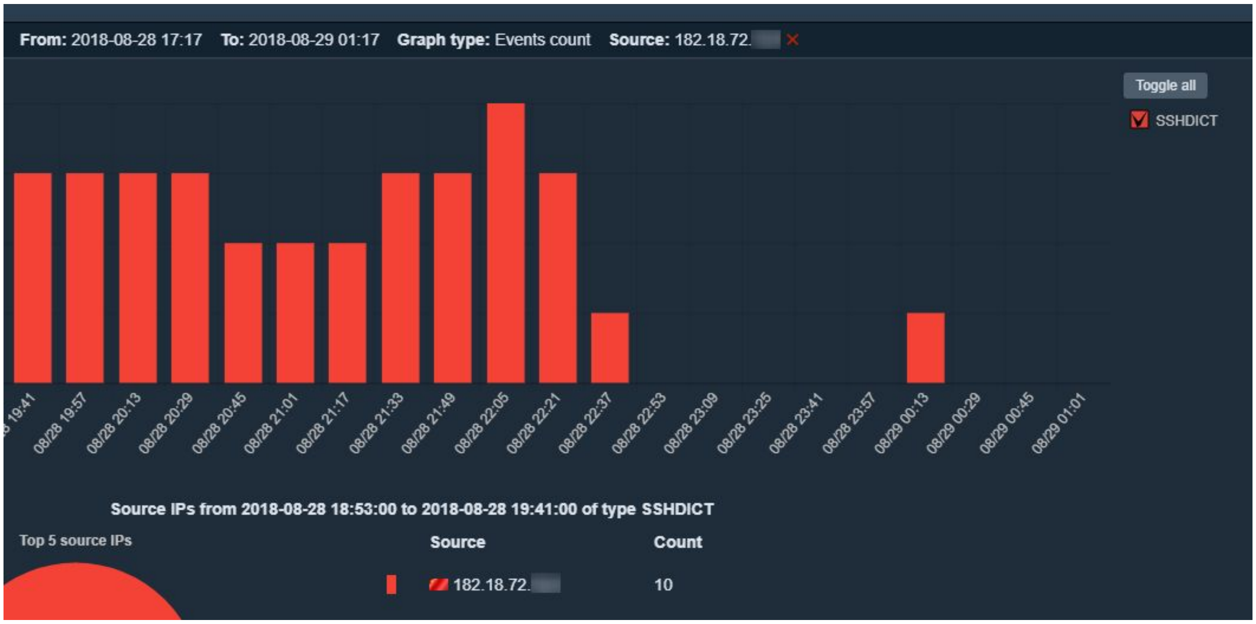
First, let's select the SSHDICT (SSH dictionary attacks) detection method.


From: 2018-08-28 09:17 **To:** 2018-08-29 09:17 **Graph type:** Events count

Source IPs from 2018-08-28 18:53:00 to 2018-08-28 19:41:00 of type SSHDICT

	Source	Count
🟥	182.18.72.[redacted]	10

Similarly, as in the first example we apply source IP as a filter to the graph. It's clear that the IP has done a substantial amount of scanning.

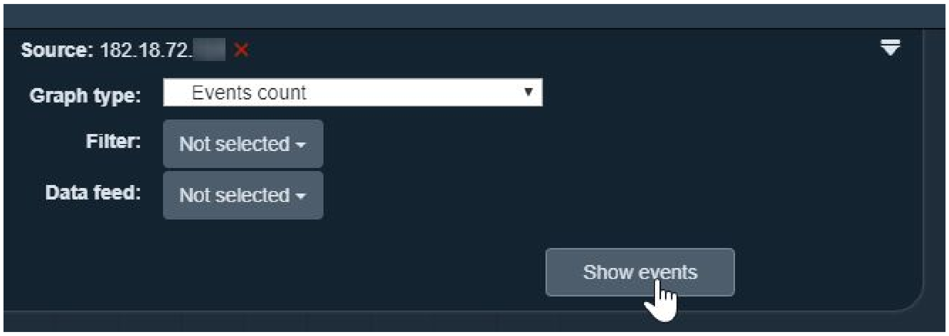


From: 2018-08-28 17:17 **To:** 2018-08-29 01:17 **Graph type:** Events count **Source:** 182.18.72.[redacted] ×

Source IPs from 2018-08-28 18:53:00 to 2018-08-28 19:41:00 of type SSHDICT

	Source	Count
🟥	182.18.72.[redacted]	10

Which hosts have been affected? Let's find out by expanding the filter (arrow in the corner) and clicking the Show events button.



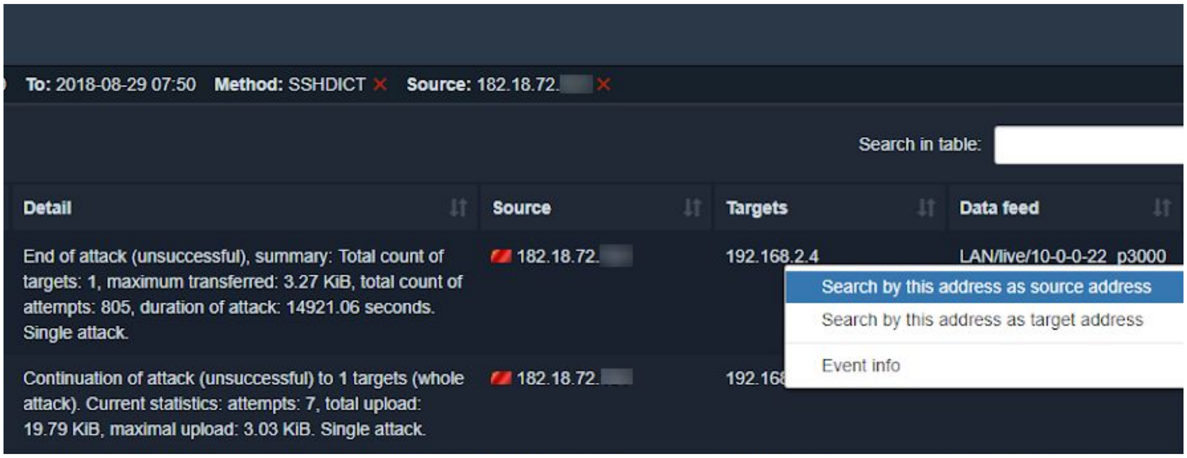
Source: 182.18.72.[redacted] ×

Graph type: Events count

Filter: Not selected

Data feed: Not selected

We can see a list of events with applied filter (SSHDICT, and our source IP). By clicking on an IP in the Targets column we can see whether the targets themselves tried anything suspicious. If so, this could mean that the dictionary attacks were successful and target host is compromised.



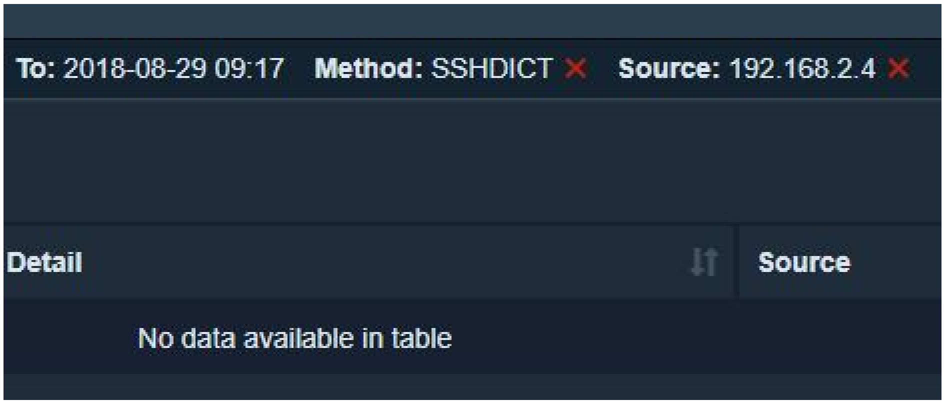
To: 2018-08-29 07:50 **Method:** SSHDICT ✕ **Source:** 182.18.72.[redacted] ✕

Search in table:

Detail	Source	Targets	Data feed
End of attack (unsuccessful), summary: Total count of targets: 1, maximum transferred: 3.27 KiB, total count of attempts: 805, duration of attack: 14921.06 seconds. Single attack.	182.18.72.[redacted]	192.168.2.4	LAN/live/10-0-0-22_p3000
Continuation of attack (unsuccessful) to 1 targets (whole attack). Current statistics: attempts: 7, total upload: 19.79 KiB, maximal upload: 3.03 KiB. Single attack.	182.18.72.[redacted]	192.168	

Search by this address as source address
Search by this address as target address
Event info

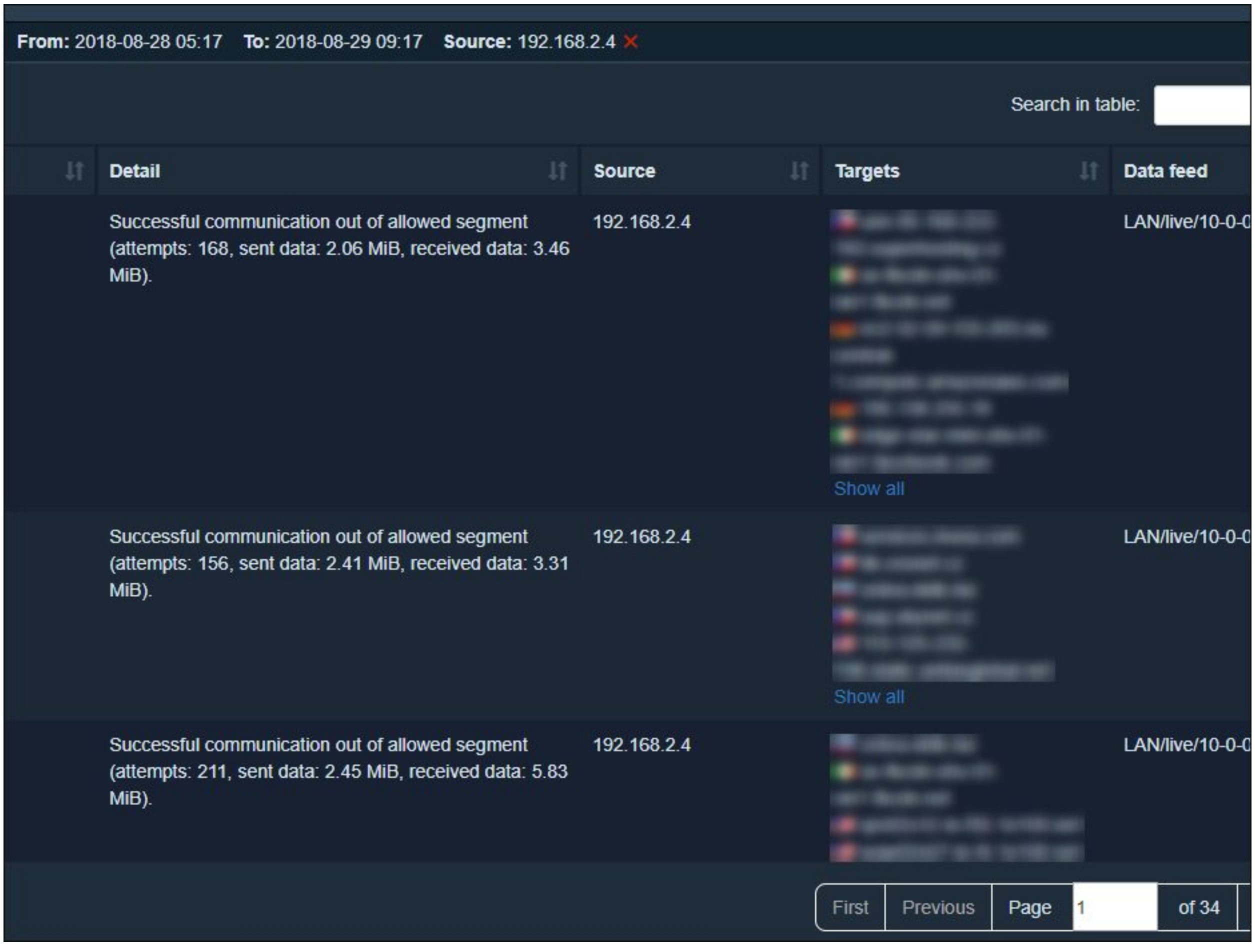
There are no events. This is because we're still applying the SSHDICT filter. Remove it by clicking on the red cross.



To: 2018-08-29 09:17 **Method:** SSHDICT ✕ **Source:** 192.168.2.4 ✕

Detail	Source
No data available in table	

There are 34 pages of events. This is too much to sift through and will be better to use high level graph view for fast analysis.

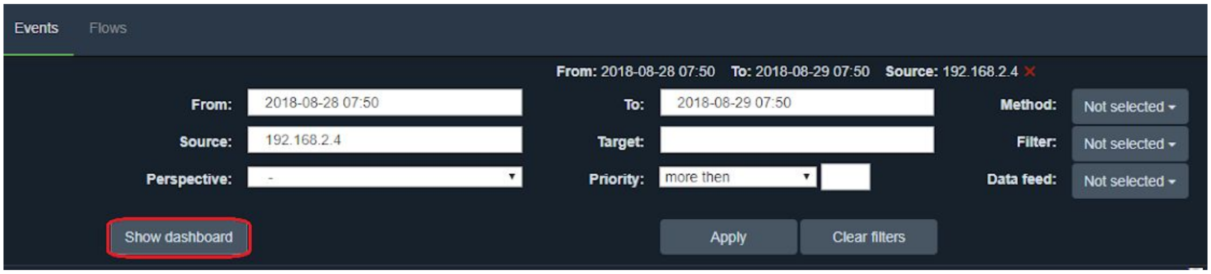


From: 2018-08-28 05:17 **To:** 2018-08-29 09:17 **Source:** 192.168.2.4 ✕

Search in table:

	Detail	Source	Targets	Data feed
	Successful communication out of allowed segment (attempts: 168, sent data: 2.06 MiB, received data: 3.46 MiB).	192.168.2.4	[redacted] Show all	LAN/live/10-0-0
	Successful communication out of allowed segment (attempts: 156, sent data: 2.41 MiB, received data: 3.31 MiB).	192.168.2.4	[redacted] Show all	LAN/live/10-0-0
	Successful communication out of allowed segment (attempts: 211, sent data: 2.45 MiB, received data: 5.83 MiB).	192.168.2.4	[redacted]	LAN/live/10-0-0

We can switch back to Dashboard by expanding the filter and clicking the Show dashboard button.



From: 2018-08-28 07:50 **To:** 2018-08-29 07:50 **Source:** 192.168.2.4 ✕

From: 2018-08-28 07:50

Source: 192.168.2.4

Perspective: -

To: 2018-08-29 07:50

Target:

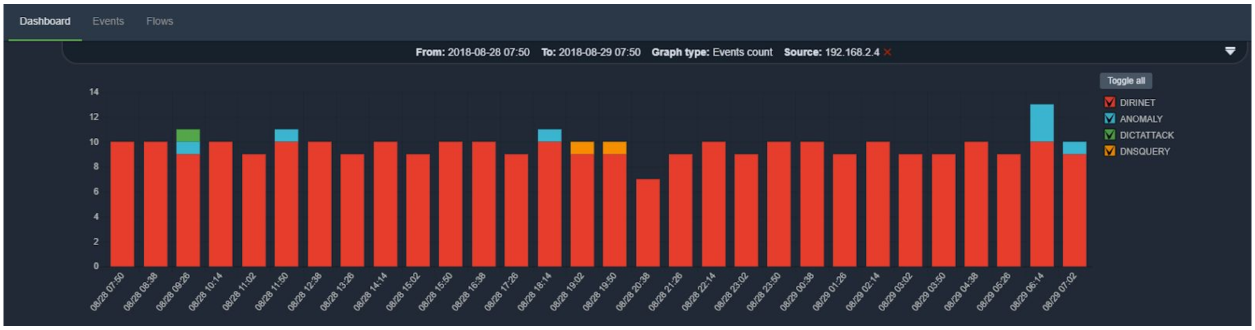
Priority: more then

Method: Not selected

Filter: Not selected

Data feed: Not selected

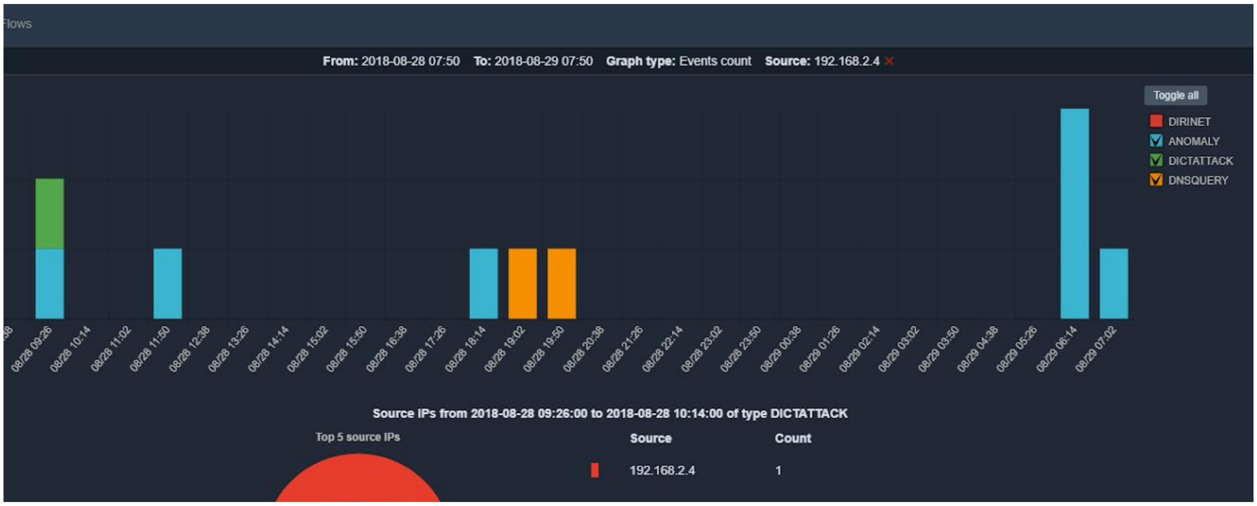
Now, we can see all events at once in an interactive visual form. There are few suspicious events and a lot of direct internet communication (DIRINET).



From: 2018-08-28 07:50 **To:** 2018-08-29 07:50 **Graph type:** Events count **Source:** 192.168.2.4 ✕

☑ DIRINET
☑ ANOMALY
☑ DICTATTACK
☑ DNSQUERY

Let's uncheck DIRINET. The first and most maliciously looking event is the green DICTATTACK in the morning. We can uncheck the rest of detection methods.

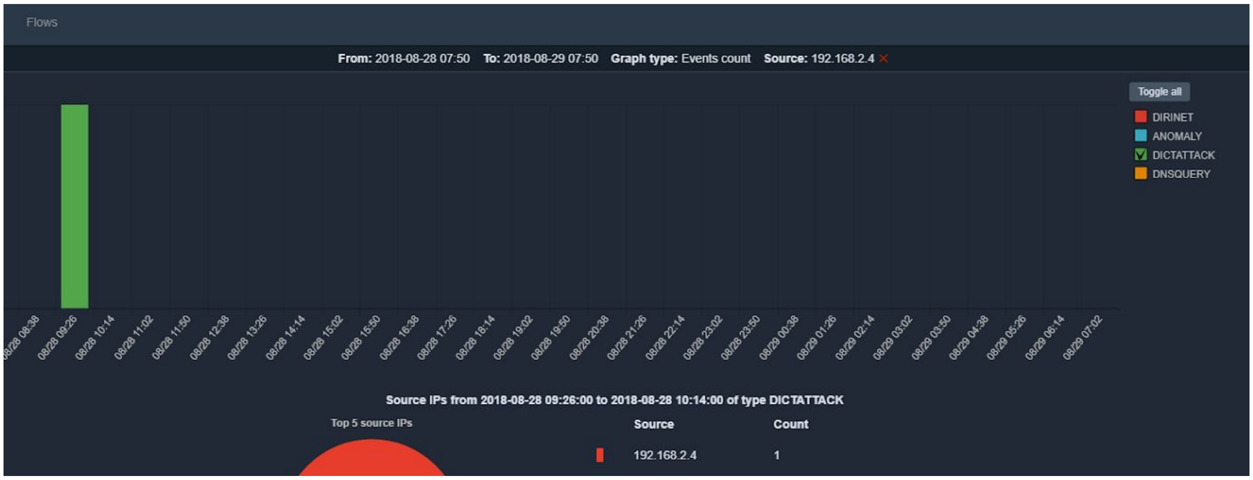


From: 2018-08-28 07:50 **To:** 2018-08-29 07:50 **Graph type:** Events count **Source:** 192.168.2.4 ✕

□ DIRINET
☑ ANOMALY
☑ DICTATTACK
☑ DNSQUERY

Source IPs from 2018-08-28 09:26:00 to 2018-08-28 10:14:00 of type DICTATTACK

	Source	Count
🟥	192.168.2.4	1



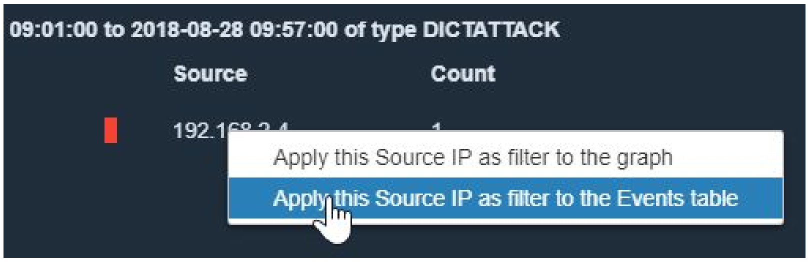
From: 2018-08-28 07:50 **To:** 2018-08-29 07:50 **Graph type:** Events count **Source:** 192.168.2.4 ✕

□ DIRINET
□ ANOMALY
☑ DICTATTACK
□ DNSQUERY

Source IPs from 2018-08-28 09:26:00 to 2018-08-28 10:14:00 of type DICTATTACK

	Source	Count
🟥	192.168.2.4	1

Apply the source IP as a filter to the Events table.

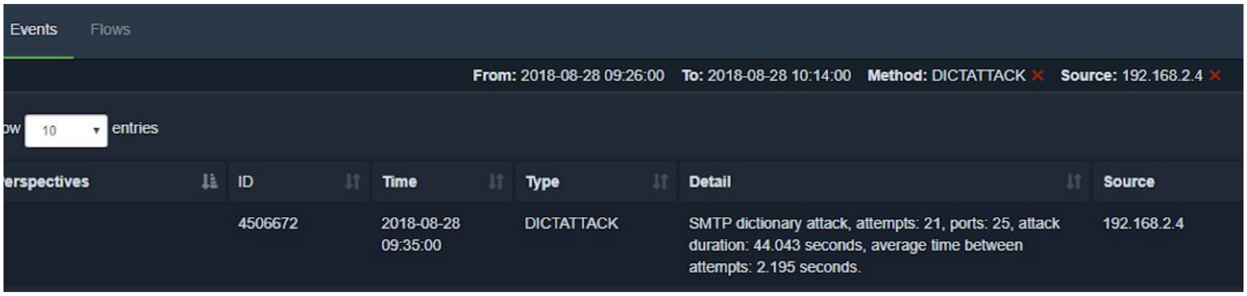


09:01:00 to 2018-08-28 09:57:00 of type DICTATTACK

Source	Count
192.168.2.4	1

Apply this Source IP as filter to the graph
Apply this Source IP as filter to the Events table

After applying DICTATTACK filter and the source IP we can see one event of an attack with all the details. it's clear that the previous target of an attack has itself became source of malicious activities.



From: 2018-08-28 09:26:00 **To:** 2018-08-28 10:14:00 **Method:** DICTATTACK ✕ **Source:** 192.168.2.4 ✕

ow 10 entries

erspectives	ID	Time	Type	Detail	Source
	4506672	2018-08-28 09:35:00	DICTATTACK	SMTP dictionary attack, attempts: 21, ports: 25, attack duration: 44.043 seconds, average time between attempts: 2.195 seconds.	192.168.2.4