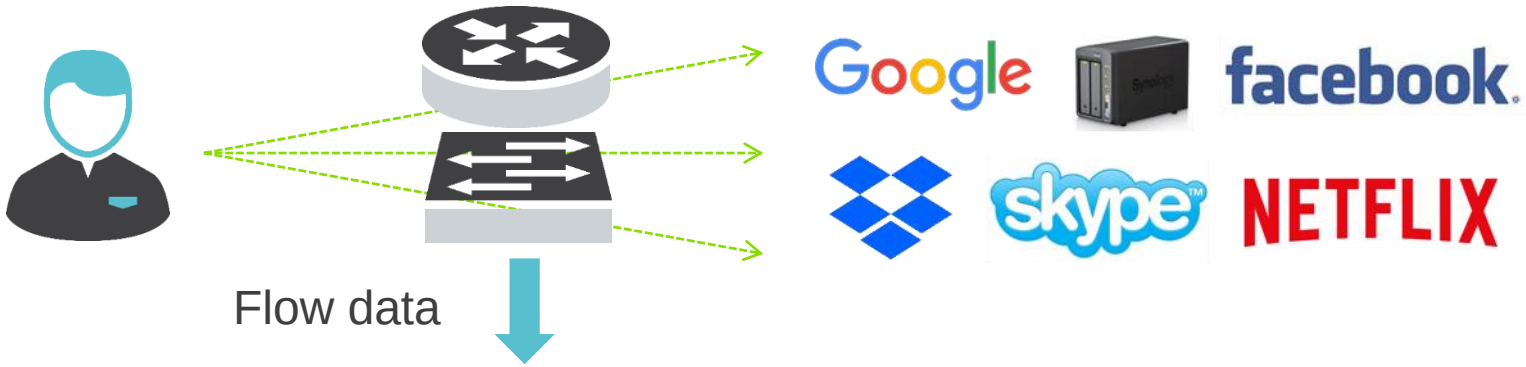
Role of Flow Monitoring in Cyber Security

Pavel Minařík, Chief Technology Officer

Flowmon
Driving Network Visibility

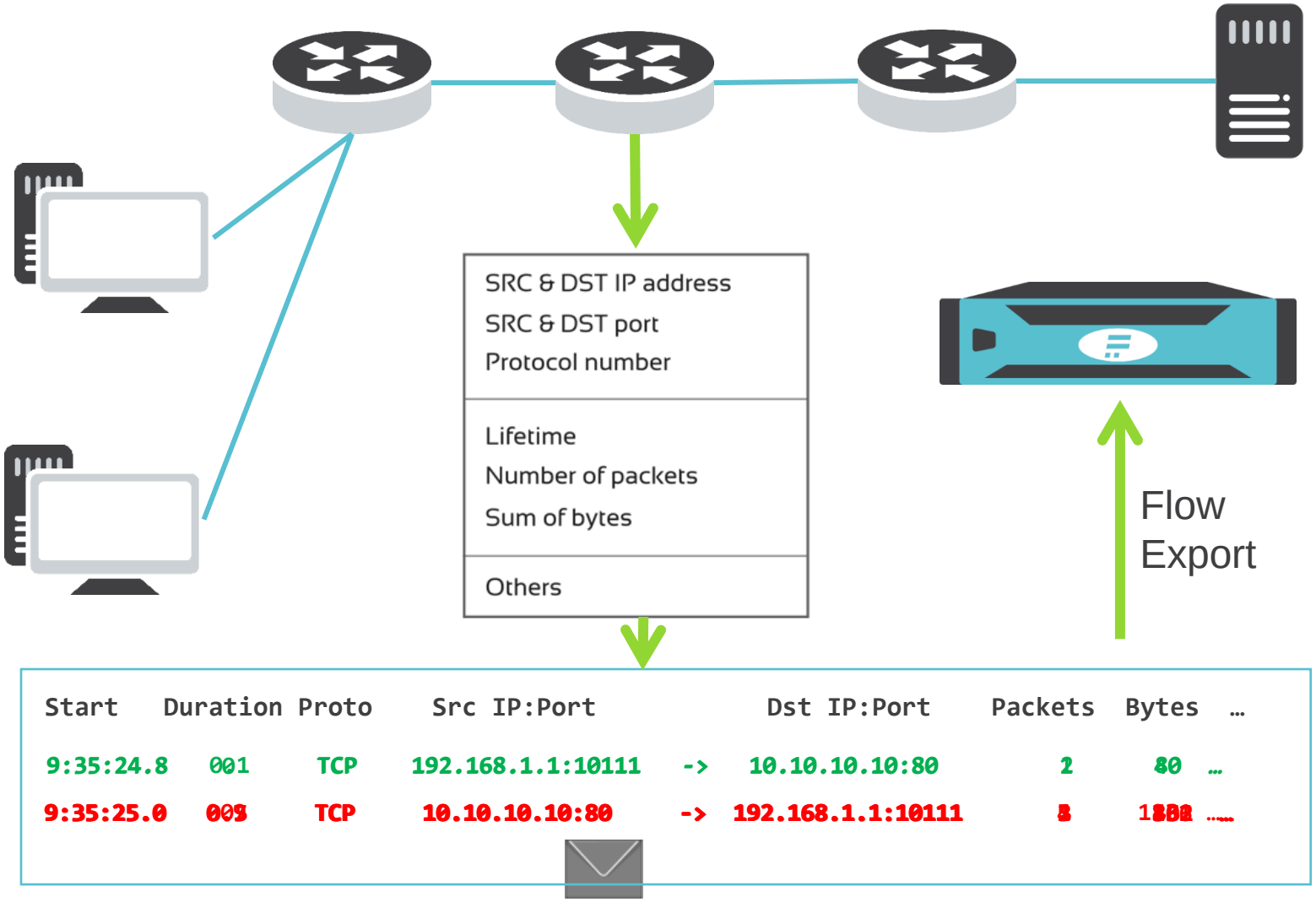
What is Flow Data?

- Modern method for network monitoring – flow measurement
- Cisco standard NetFlow v5/v9, IETF standard IPFIX
- Focused on L3/L4 information and volumetric parameters
- Real network traffic to flow statistics reduction ratio 500:1



Flowmon
Driving Network Visibility

Flow Monitoring Principle



Flowmon
Driving Network Visibility

Myth: “Flow data do not provide sufficient level of detail when it comes to network troubleshooting or forensics. Full packet traces are absolute must to investigate on network issues and fight cyber crime.”

Flowmon
Driving Network Visibility

	Strong aspects		Weak aspects
Packet Analysis	+ Full network traffic + Enough details for troubleshooting + Supports forensic analysis + Signature based detection		- Useless for encrypted traffic - Usually too much details - Very resource consuming
1 min 75 GB	1 hour 4.5 TB		1 day 108 TB
Flow Data	+ Works in high-speed networks + Resistant to encrypted traffic + Visibility and reporting + Network behavior analysis		- No application layer data - Sometimes not enough details - Sampling (routers, switches)
1 min 150 MB	1 hour 9 GB		1 day 216 GB

Flow vs. Packet Analysis on 10G

Flowmon
Driving Network Visibility

Modern Flow Monitoring with Flowmon Probes

- Versatile and flexible network appliances
  - Monitoring ports convert packets to flows
  - Un-sampled export in NetFlow v5/v9 or IPFIX
  - Wire-speed, L2-L7 visibility, tunnel decapsulation, PCAPs when needed

L2	L3/L4	L7	
• MAC • VLAN • MPLS • GRE • ESP • OTV	• Standard items • NPM metrics • RTT, SRT, … • TTL, SYN size, … • ASN (BGP) • Geolocation • VxLAN	• NBAR2 • HTTP • SNI • DNS • DHCP • IEC104	• SMB/CIFS • VoIP (SIP) • Email • SQL • SSL/TLS • CoAP

Flowmon
Driving Network Visibility

Use Case: Retrospective Investigation

Traditional flow data compared to Flowmon L7 visibility

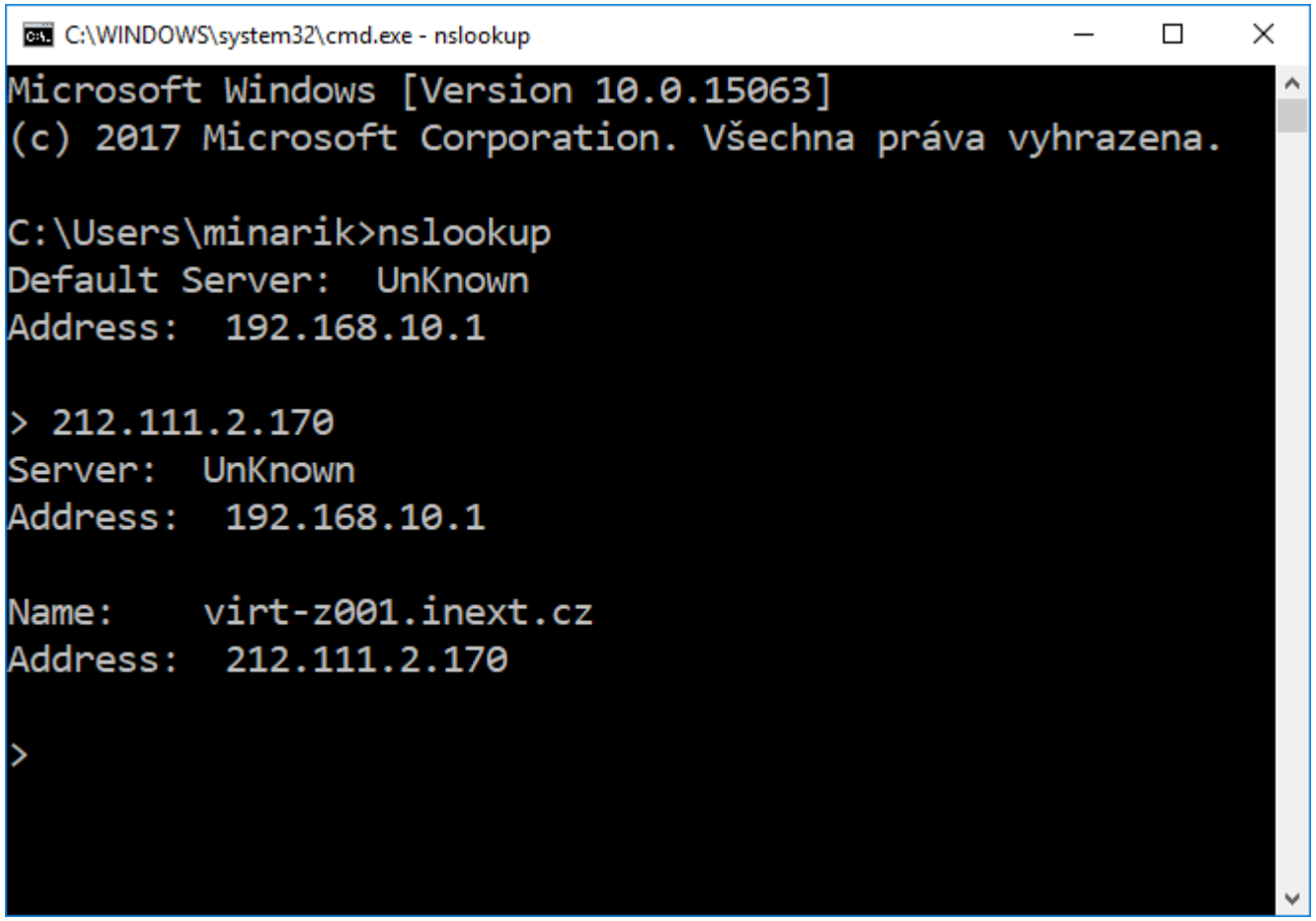
Flowmon
Driving Network Visibility

Investigate on **historical** network activity of a particular user. What was the **real website** visited by the user? How can we identify operating system and other details?

Probe HTTP visibility, user agent analysis.

Investigation on User Activity

- Traffic of Interest
  - Internal IP address 192.168.70.35
  - External IP address 212.111.2.170
  - Timeframe 2017-09-22 09:00 - 2017-09-22 10:00
- Need to analyze historical data, no PCAP available
- What we do?
  - Check for the reverse DNS record
  - Check for whois record
  - See what domains are hosted on IP
  - See what content is there
  - Look into flows from the router



- IP address translates to domain name that is not helpful at all

Flowmon
Driving Network Visibility

```
inetnum: 212.111.0.0 - 212.111.4.127
netname: INEXT-NET
descr: INTERNEXT 2000
descr: Vsetin
country: CZ
admin-c: RH163-RIPE
tech-c: RH163-RIPE
status: ASSIGNED PA
mnt-by: INEXT-CZ-MNT
created: 1970-01-01T00:00:00Z
last-modified: 2012-04-01T08:19:53Z
source: RIPE # Filtered

person: Radim Hajek
address: INTERNEXT 2000, s.r.o.
address: Palackeho 166
address: Vsetin
address: 755 01
address: The Czech Republic
phone: +420 576 510000
nic-hdl: RH163-RIPE
abuse-mailbox: abuse@inext.cz
mnt-by: INEXT-CZ-MNT
created: 1970-01-01T00:00:00Z
last-modified: 2016-01-07T18:01:11Z
source: RIPE # Filtered
```

- General whois information related to IP address
- IP belongs to local ISP in Czech

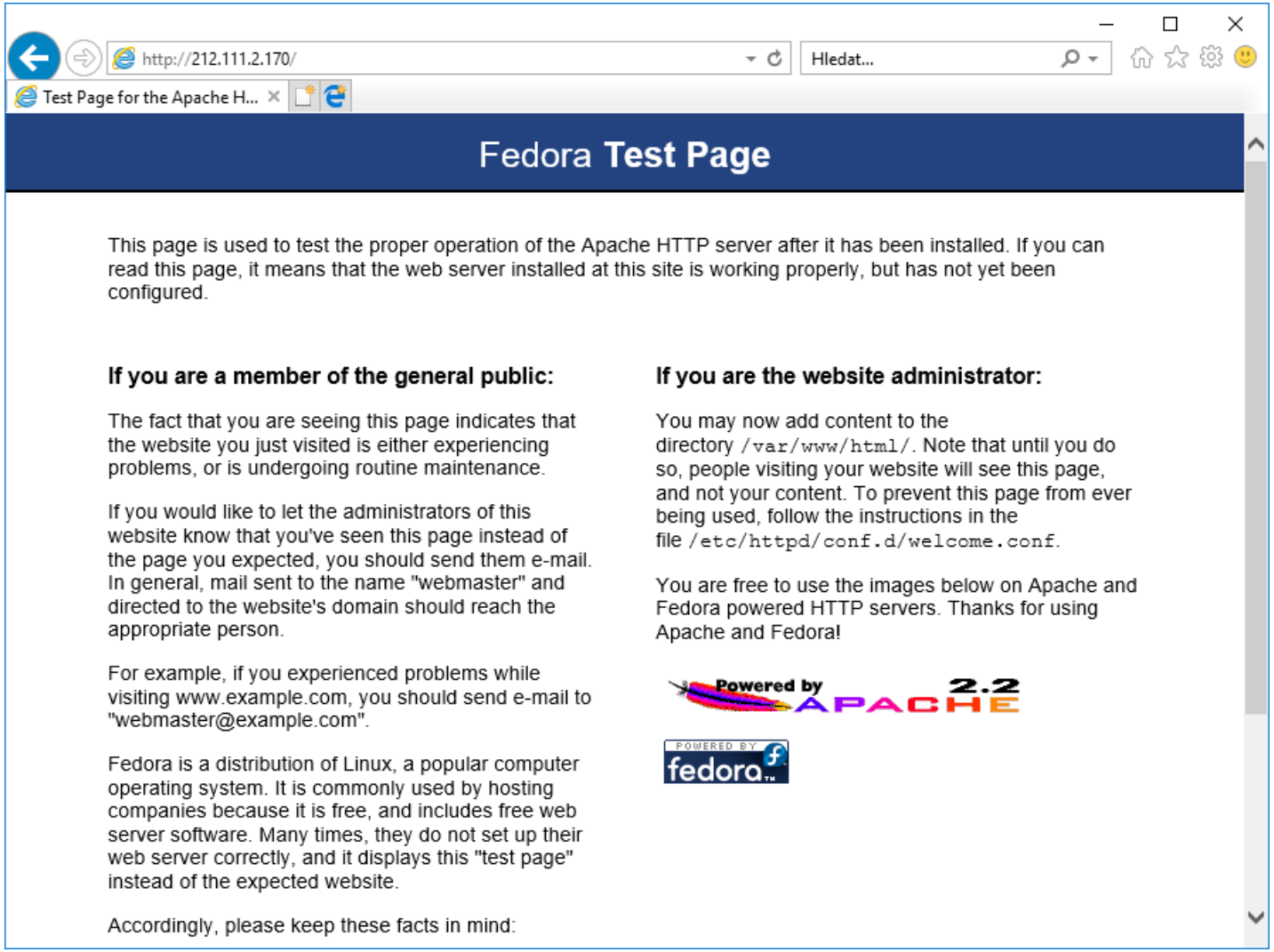
Reverse IP lookup for: 212.111.2.170

Found **3** domains hosted on IP address 212.111.2.170.

#	Domain	Tools
1	**mmsystems.cz**	Whois+ Domain Search Domain Typos
	Name servers: **inext.inext.cz** (used by 479 domains) **ns2.inext.cz** (used by 340 domains) Mail servers: **mail.radiozlin.cz** (used by 4 domains) **relay1.inext.cz** (used by 331 domains) IPv4: **212.111.2.170** (used by 3 domains)	
2	**radiozlin.cz**	Whois+ Domain Search Domain Typos
	Name servers: **inext.inext.cz** (used by 479 domains) **ns2.inext.cz** (used by 340 domains) Mail servers: **mail.radiozlin.cz** (used by 4 domains) **relay1.inext.cz** (used by 331 domains) IPv4: **212.111.2.170** (used by 3 domains) Google Analytics ID: **ua-4884579** (used by 1 domain)	
3	**rockmax.cz**	Whois+ Domain Search Domain Typos
	Name servers: **ns2.inext.cz** (used by 340 domains) **inext.inext.cz** (used by 479 domains) Mail servers: **mx.inext.cz** (used by 141 domains) **relay1.inext.cz** (used by 331 domains) IPv4: **212.111.2.170** (used by 3 domains) Google Analytics ID: **ua-4881996** (used by 1 domain)	

- 3 different domains for IP address of interest
- We are getting closer with our analysis

Flowmon
Driving Network Visibility



- Content on the IP address is not really helpful
- IP is running Fedora OS and Apache web server

Flowmon
Driving Network Visibility

Start Time - first seen	Duration	Protocol	Source IP address	Source port	Destination IP address	Destination port	TCP Flags	TOS	Packets	Bytes	Flows
2017-09-22 08:59:30.515	0.024 s	TCP	192.168.70.35	53739	212.111.2.170	http	...AP.SF	Best Effort & Default	5	862	1
2017-09-22 08:59:30.524	0.024 s	TCP	212.111.2.170	http	192.168.70.35	53739	...AP.SF	Best Effort & Default	5	520	1
2017-09-22 08:59:33.464	0.02 s	TCP	192.168.70.35	53740	212.111.2.170	http	...AP.SF	Best Effort & Default	5	897	1
2017-09-22 08:59:33.465	0.02 s	TCP	192.168.70.35	53741	212.111.2.170	http	...AP.SF	Best Effort & Default	5	897	1
2017-09-22 08:59:33.473	0.02 s	TCP	212.111.2.170	http	192.168.70.35	53740	...AP.SF	Best Effort & Default	5	362	1
2017-09-22 08:59:33.474	0.02 s	TCP	212.111.2.170	http	192.168.70.35	53741	...AP.SF	Best Effort & Default	5	362	1
2017-09-22 08:59:41.363	0.028 s	TCP	192.168.70.35	53742	212.111.2.170	http	...AP.SF	Best Effort & Default	5	862	1
2017-09-22 08:59:41.372	0.028 s	TCP	212.111.2.170	http	192.168.70.35	53742	...AP.SF	Best Effort & Default	5	520	1
2017-09-22 08:59:52.221	0.023 s	TCP	192.168.70.35	53743	212.111.2.170	http	...AP.SF	Best Effort & Default	5	862	1
2017-09-22 08:59:52.230	0.023 s	TCP	212.111.2.170	http	192.168.70.35	53743	...AP.SF	Best Effort & Default	5	520	1
2017-09-22 09:00:03.056	0.059 s	TCP	192.168.70.35	53744	212.111.2.170	http	...AP.SF	Best Effort & Default	5	862	1
2017-09-22 09:00:03.065	0.059 s	TCP	212.111.2.170	http	192.168.70.35	53744	...AP.SF	Best Effort & Default	5	520	1
2017-09-22 09:00:03.467	0.029 s	TCP	192.168.70.35	53745	212.111.2.170	http	...AP.SF	Best Effort & Default	5	897	1
2017-09-22 09:00:03.468	0.027 s	TCP	192.168.70.35	53746	212.111.2.170	http	...AP.SF	Best Effort & Default	5	897	1
2017-09-22 09:00:03.476	0.029 s	TCP	212.111.2.170	http	192.168.70.35	53745	...AP.SF	Best Effort & Default	5	362	1
2017-09-22 09:00:03.477	0.027 s	TCP	212.111.2.170	http	192.168.70.35	53746	...AP.SF	Best Effort & Default	5	362	1
2017-09-22 09:00:13.873	0.024 s	TCP	192.168.70.35	53747	212.111.2.170	http	...AP.SF	Best Effort & Default	5	862	1
2017-09-22 09:00:13.882	0.025 s	TCP	212.111.2.170	http	192.168.70.35	53747	...AP.SF	Best Effort & Default	5	520	1
2017-09-22 09:00:24.730	0.024 s	TCP	192.168.70.35	53749	212.111.2.170	http	...AP.SF	Best Effort & Default	5	862	1
2017-09-22 09:00:24.740	0.023 s	TCP	212.111.2.170	http	192.168.70.35	53749	...AP.SF	Best Effort & Default	5	520	1
							Flows 1.15 K		Bytes 755.8 K		Packets 5.7 K

Client IP: **192.168.70.35**
Server IP: **212.11.2.170**
HTTP hostname: **unknown**
URL: **unknown**
Client OS: **unknown**
Browser: **unknown**

Flows From the Router (L3/L4)

Flowmon
Driving Network Visibility

And Now For Something Completely Different

- Flow data with HTTP visibility
  - HOST NAME
  - URL
  - METHOD TYPE
  - STATUS CODE
  - REQUEST – RESPONSE STITCHING
  - USER AGENT ANALYSIS
    - OPERATING SYSTEM + VERSION
    - HTTP APPLICATION + VERSION

Start Time - first seen	Duration	Source IP address	Destination IP address	Hostname	Source port	Destination port	Packets	Bytes	HTTP method	HTTP result code	URL	Operating System	OS Major Version	OS Minor Version	Application Info	Application Major Version	Application Minor Version
2017-09-22 08:59:30.515	0.024 s	192.168.70.35	212.111.2.170	www.rockmax.cz	53739	http	5	862	GET	200	/stream_live/get_songs_cover.php?r=1463	Windows	10	0	Chrome	60	0
2017-09-22 08:59:30.524	0.024 s	212.111.2.170	192.168.70.35	www.rockmax.cz	http	53739	5	520	GET	200	/stream_live/get_songs_cover.php?r=1463	N/A	N/A	N/A	N/A	N/A	N/A
2017-09-22 08:59:33.464	0.02 s	192.168.70.35	212.111.2.170	www.rockmax.cz	53740	http	5	897	GET	304	/stream_live/hraje.txt	Windows	10	0	Chrome	60	0
2017-09-22 08:59:33.465	0.02 s	192.168.70.35	212.111.2.170	www.rockmax.cz	53741	http	5	897	GET	304	/stream_live/hralo.txt	Windows	10	0	Chrome	60	0
2017-09-22 08:59:33.473	0.02 s	212.111.2.170	192.168.70.35	www.rockmax.cz	http	53740	5	362	GET	304	/stream_live/hraje.txt	N/A	N/A	N/A	N/A	N/A	N/A
2017-09-22 08:59:33.474	0.02 s	212.111.2.170	192.168.70.35	www.rockmax.cz	http	53741	5	362	GET	304	/stream_live/hralo.txt	N/A	N/A	N/A	N/A	N/A	N/A
2017-09-22 08:59:41.363	0.028 s	192.168.70.35	212.111.2.170	www.rockmax.cz	53742	http	5	862	GET	200	/stream_live/get_songs_cover.php?r=5933	Windows	10	0	Chrome	60	0
2017-09-22 08:59:41.372	0.028 s	212.111.2.170	192.168.70.35	www.rockmax.cz	http	53742	5	520	GET	200	/stream_live/get_songs_cover.php?r=5933	N/A	N/A	N/A	N/A	N/A	N/A
2017-09-22 08:59:52.221	0.023 s	192.168.70.35	212.111.2.170	www.rockmax.cz	53743	http	5	862	GET	200	/stream_live/get_songs_cover.php?r=2054	Windows	10	0	Chrome	60	0
2017-09-22 08:59:52.230	0.023 s	212.111.2.170	192.168.70.35	www.rockmax.cz	http	53743	5	520	GET	200	/stream_live/get_songs_cover.php?r=2054	N/A	N/A	N/A	N/A	N/A	N/A
2017-09-22 09:00:03.056	0.059 s	192.168.70.35	212.111.2.170	www.rockmax.cz	53744	http	5	862	GET	200	/stream_live/get_songs_cover.php?r=2054	Windows	10	0	Chrome	60	0
2017-09-22 09:00:03.065	0.059 s	212.111.2.170	192.168.70.35	www.rockmax.cz	http	53744	5	520	GET	200	/stream_live/get_songs_cover.php?r=2054	N/A	N/A	N/A	N/A	N/A	N/A
2017-09-22 09:00:03.467	0.029 s	192.168.70.35	212.111.2.170	www.rockmax.cz	53745	http	5	897	GET	304	/stream_live/hraje.txt	Windows	10	0	Chrome	60	0
2017-09-22 09:00:03.468	0.027 s	192.168.70.35	212.111.2.170	www.rockmax.cz	53746	http	5	897	GET	304	/stream_live/hralo.txt	Windows	10	0	Chrome	60	0
2017-09-22 09:00:03.476	0.029 s	212.111.2.170	192.168.70.35	www.rockmax.cz	http	53745	5	362	GET	304	/stream_live/hraje.txt	N/A	N/A	N/A	N/A	N/A	N/A
2017-09-22 09:00:03.477	0.027 s	212.111.2.170	192.168.70.35	www.rockmax.cz	http	53746	5	362	GET	304	/stream_live/hralo.txt	N/A	N/A	N/A	N/A	N/A	N/A
2017-09-22 09:00:13.873	0.024 s	192.168.70.35	212.111.2.170	www.rockmax.cz	53747	http	5	862	GET	200	/stream_live/get_songs_cover.php?r=1709	Windows	10	0	Chrome	60	0
2017-09-22 09:00:13.882	0.025 s	212.111.2.170	192.168.70.35	www.rockmax.cz	http	53747	5	520	GET	200	/stream_live/get_songs_cover.php?r=1709	N/A	N/A	N/A	N/A	N/A	N/A
2017-09-22 09:00:24.730	0.024 s	192.168.70.35	212.111.2.170	www.rockmax.cz	53749	http	5	862	GET	200	/stream_live/get_songs_cover.php?r=7897	Windows	10	0	Chrome	60	0
2017-09-22 09:00:24.740	0.023 s	212.111.2.170	192.168.70.35	www.rockmax.cz	http	53749	5	520	GET	200	/stream_live/get_songs_cover.php?r=7897	N/A	N/A	N/A	N/A	N/A	N/A
														Flows 1.15 K		Bytes 755.8 K	Packets 5.7 K

Client IP: **192.168.70.35**
Server IP: **212.11.2.170**
HTTP hostname: **www.rockmax.cz**
URL: **/stream_live/get_songs_...**
Client OS: **Windows 10**
Browser: **Chrome 60.0**

Flow From the Probe (L2-L7)

Flowmon
Driving Network Visibility

Use Case: Encrypted Traffic Analysis

Understand Encrypted Traffic While Preserving User Privacy

Flowmon
Driving Network Visibility

What About Encrypted Traffic?

- Analysis of **characteristics and patterns, not decryption**
  - L3/L4: src/dsct IP:port, protocol, timestamp, data volume
- Leveraging unencrypted part of the TLS traffic
  - SSL/TLS handshake

Monitoring and security

- SNI to report on „hostname“
- Malicious patterns in encrypted traffic
- JA3 fingerprinting to pinpoint suspicious actors

Cryptographic assessment

- SSL/TLS policy compliance
- Cyphersuites (encryption algorithms, key lengths)
- Certificates

Flowmon
Driving Network Visibility

IP Header

TCP Header

TLS Header

TLS Record

TLS server version
TLS cipher suite
TLS server name indication
TLS client version
TLS certificate issuer common name
TLS subject common name
TLS public key algorithm
TLS certificate validity until
TLS JA3 fingerprint
and many others

Enriched Flow

- Patterns and characteristics of malicious behavior in L3/L4 of encrypted traffic
- SSL/TLS policy compliance

Flowmon
Driving Network Visibility

TLS Traffic

Last week (generic time span)

	SSL/TLS version	Maximal bits/s	Bits per second	Bytes
1	TLS 1.2	10.8 M	219.5 K	15.46 GiB
2	TLS 1.0	508.5 K	861.6	62.12 MiB
3	TLS 1.1	1.9 K	23.8	1.71 MiB
	Total	**10.8 M**	**220.4 K**	**15.52 GiB**

2019-04-14 17:15 - 2019-04-21 17:15

TLS Traffic

Last week (generic time span)

	SSL/TLS version	Bits per second	Bytes
1	TLS 1.2	219.5 K	15.46 GiB
2	TLS 1.0	861.6	62.12 MiB
3	TLS 1.1	23.8	1.71 MiB
	Total	**220.4 K**	**15.52 GiB**

2019-04-14 17:15 - 2019-04-21 17:15

New widget

TLS/SSL Version Distribution Dashboard

Why Flow Monitoring?

Continuous full packet capture tools cannot scale with bandwidth explosion in corporate networks and companies are switching to flow technologies.

Gartner notes that 80% of network troubleshooting can be solved with NetFlow.

Flowmon combines best of breed: flow data enriched with L7 and performance metrics. This helps to solve 95% of all troubleshooting cases. In addition, Flowmon provides on-demand packet capture when flow visibility is not enough.

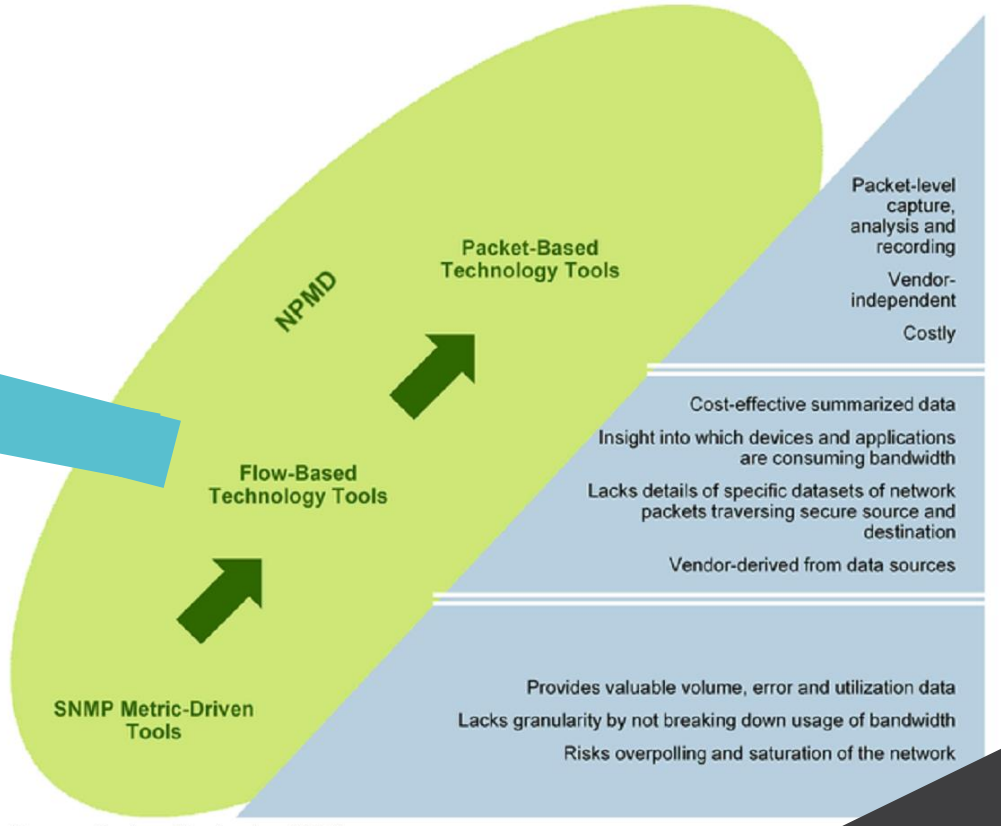
Flowmon
Driving Network Visibility

Using Flow Data For Security

Volumetric
DDoS detection

Anomaly detection
Incident reporting

Gartner



Source: Gartner (September 2014)

Flowmon
Driving Network Visibility

Neil MacDonald, VP Distinguished Analyst

Gartner Security & Risk Management Summit, London 2015

Align NetOps & SecOps Tool Objectives With Shared Use Cases

Gartner report ID G00333211, 2018

Flowmon
Driving Network Visibility

Next Generation Network Security - Behavior Analysis & Anomaly Detection

Detects and alerts on abnormal behaviors

Reports anomalies and advanced persistent threats

Detect intrusions and attacks not visible by standard signature based tools

Gartner: *“Blocking and prevention is not sufficient. After you deployed firewall and IPS, you should implement network behavior analysis to identify problems that are undetectable using other techniques.”*

Flowmon
Driving Network Visibility

Flowmon ADS Principles

Flowmon ADS

- Machine Learning
- Adaptive Baselining
- Heuristics
- Behavior Patterns
- Reputation Databases

#	Zdrojová IP	Typ události	Detail	Čas	Zdroj NetFlow dat	Cíle
1	112.90.18.105	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.66 MiB, packets: 65 559.	2013-08-24 07:15:21	localhost	1.52.6.170, 1.52.13.199, 1.52.42.167, 1.52.59.1 1.52.71.217, 1.52.87.249, 1.52.133.228, 1.52.1 1.52.192.113, 1.52.218.16, ...
2	112.91.30.17	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.37 MiB, packets: 58 379.	2013-08-24 07:15:21	localhost	1.52.54.212, 1.52.109.106, 1.52.167.73, 1.52.1 1.52.191.229, 1.52.218.123, 1.52.220.241, 1.52 1.52.241.199, 1.53.8.41, ...
3	121.10.112.17	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.37 MiB, packets: 58 266.	2013-08-24 07:15:21	localhost	1.52.1.176, 1.52.2.100, 1.52.7.105, 1.52.44.16 1.52.77.224, 1.52.128.196, 1.52.128.214, 1.52. 1.52.199.183, 1.52.241.170, ...
4	183.61.138.105	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.66 MiB, packets: 65 415.	2013-08-24 07:15:21	localhost	1.52.58.25, 1.52.85.224, 1.52.86.18, 1.52.92.1 1.52.174.104, 1.52.183.10, 1.52.184.230, 1.52. 1.52.203.16, 1.52.235.13, ...
5	210.73.221.181	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.36 MiB, packets: 58 086.	2013-08-24 07:15:21	localhost	1.52.28.245, 1.52.44.63, 1.52.112.109, 1.52.14 1.52.177.97, 1.53.40.147, 1.53.58.10, 1.53.89. 1.53.122.157, 1.53.221.26, ...
6	112.90.18.105	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 5.04 MiB, packets: 125 924.	2013-08-24 05:39:59	localhost	1.52.4.138, 1.52.12.103, 1.52.28.61, 1.52.31.7 1.52.42.130, 1.52.44.24, 1.52.48.142, 1.52.67. 1.52.83.34, ...
7	112.90.18.105	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 3.60 MiB, packets: 88 749.	2013-08-24 03:38:31	localhost	1.52.7.220, 1.52.11.109, 1.52.28.57, 1.52.42.9 1.52.95.134, 1.52.114.14, 1.52.115.205, 1.52.1 1.52.122.10, ...
8	112.90.18.105	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.60 MiB, packets: 63 126.	2013-08-24 03:00:34	localhost	1.52.12.16, 1.52.77.184, 1.52.104.14, 1.52.125 1.52.128.99, 1.52.134.215, 1.52.137.109, 1.5 1.52.203.143, 1.52.209.197, ...

Flowmon
Driving Network Visibility

Flowmon | Flowmon ADS | en | admin

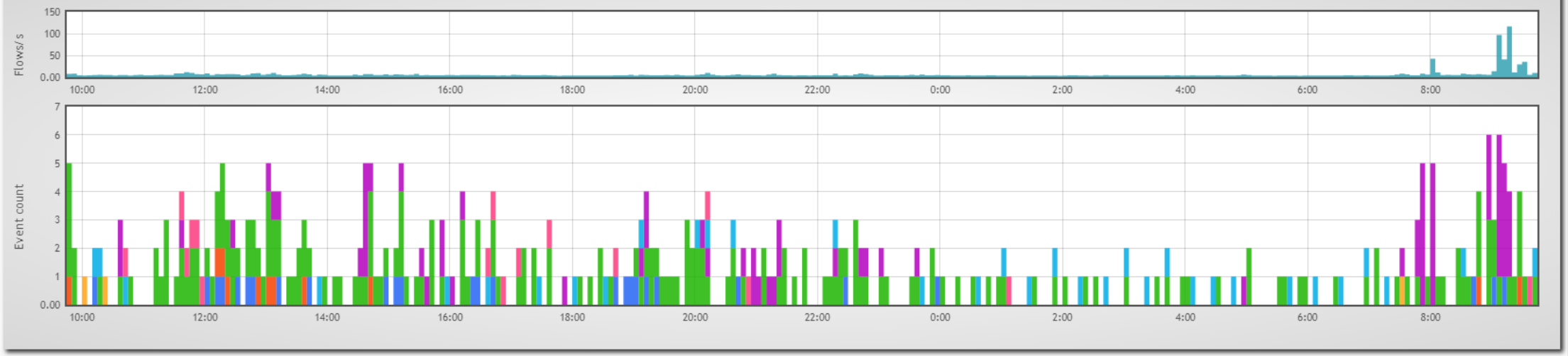
- Dashboard
- Events
- Reports
- Processing
- Settings
- About

Search criteria

From 2019-02-02 09:49 To 2019-02-03 09:49 Perspective Operational issues Data feed All Search Reset

Overview | Events

Events in time



Events by priority and count (360)

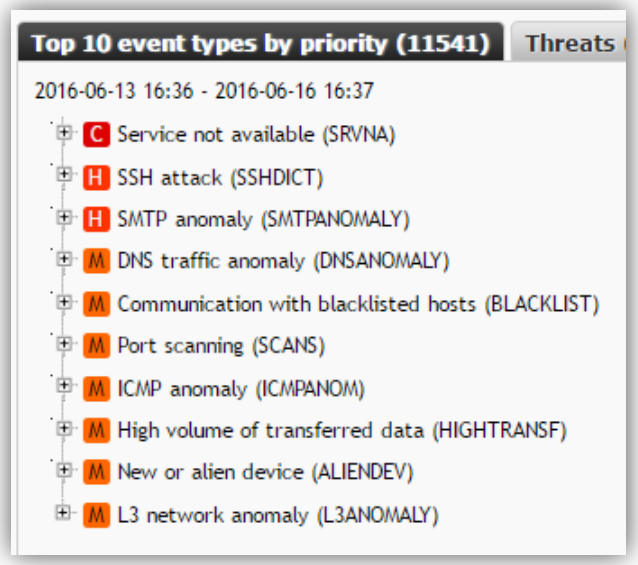
Priorities: Critical High Medium Low Information (All / None) 2019-02-02 09:45 - 2019-02-03 09:45

M 1	DNS traffic anomaly (DNSANOMALY)	27 (number of events)
M 2	High volume of transferred data (HIGHTRANSF)	11 (number of events)
M 3	ICMP anomaly (ICMPANOM)	3 (number of events)
L 4	Country reputation (COUNTRY)	201 (number of events)
L 5	Behavior anomaly (ANOMALY)	68 (number of events)
L 6	DNS query volume anomaly (DNSQUERY)	34 (number of events)
		16 (number of events)

Analytics Dashboard

ADS Detection Capabilities

- Attacks on network services
- Infected devices and communication botnet C&C, attackers, …
- Port scanning and similar symptoms of infected devices
- Applications like P2P networks or on-line messengers
- Outages of network services or improper configurations
- Potential data leakage and usage of data sharing on internet
- PROXY bypass, TOR
- Anomalies of DNS or DHCP traffic
- Attacks against VoIP, PBX, …
- Unexpected mail traffic and SPAM



Flowmon Threat Intelligence

- IP and host-based reputation feeds (community & commercial)
- Detection of C&C domains, P2P botnets, phishing, etc.
  - IP addresses
  - HTTP host names, URLs
  - Domain names

Flowmon
Driving Network Visibility

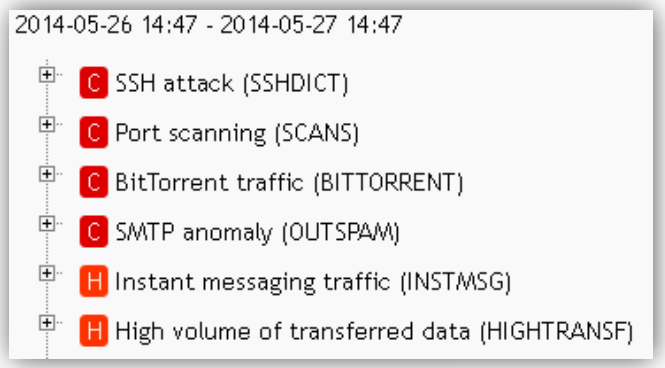
User Defined Anomaly Detection Methods

- Advanced users request maximal customization options
- Detection focused on specific use cases and scenarios followed by standard event pipeline (priority, notification, SIEM, …)
- Various benefits in different environments

Protocol anomalies	HTTP UDP traffic	req_transferred > 104857600 AND protocol = 17 AND destination_port = 80
Specific malware	Retefe2 banking trojan	http_url LIKE '/ICECVREU.js?%'
Regular expressions	SQL injection	Tools.re_match('.{1,4}[Oo][Rr].{1,4}\d.{1,3}\d', 'http_url') = 1
Specific OS detection	Windows XP	ua_os = 68 and ua_os_version = 5.1

ADS Alerting and Integration

- Perspectives to setup event priorities
- E-mail notifications
- PDF reports
- SIEM/log management
  - Syslog (native CEF format)
  - SNMPv2 traps
- Take action
  - Integrated (AddNet, ISE, …)
  - Triggered Capture
  - General Script



Flowmon
Driving Network Visibility

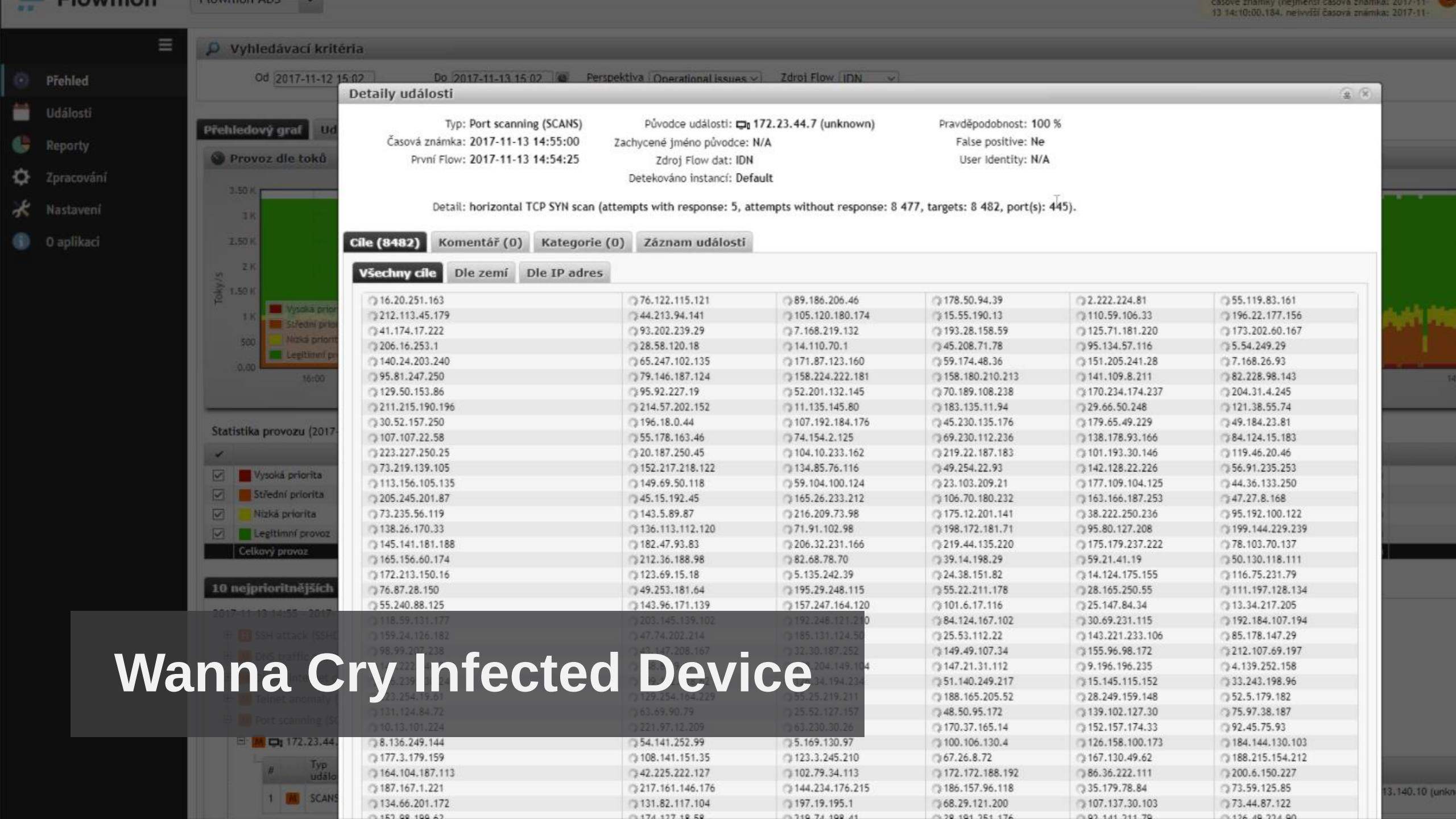
Use Case: Anomaly Detection in Enterprise

Selected Detections from our Customers

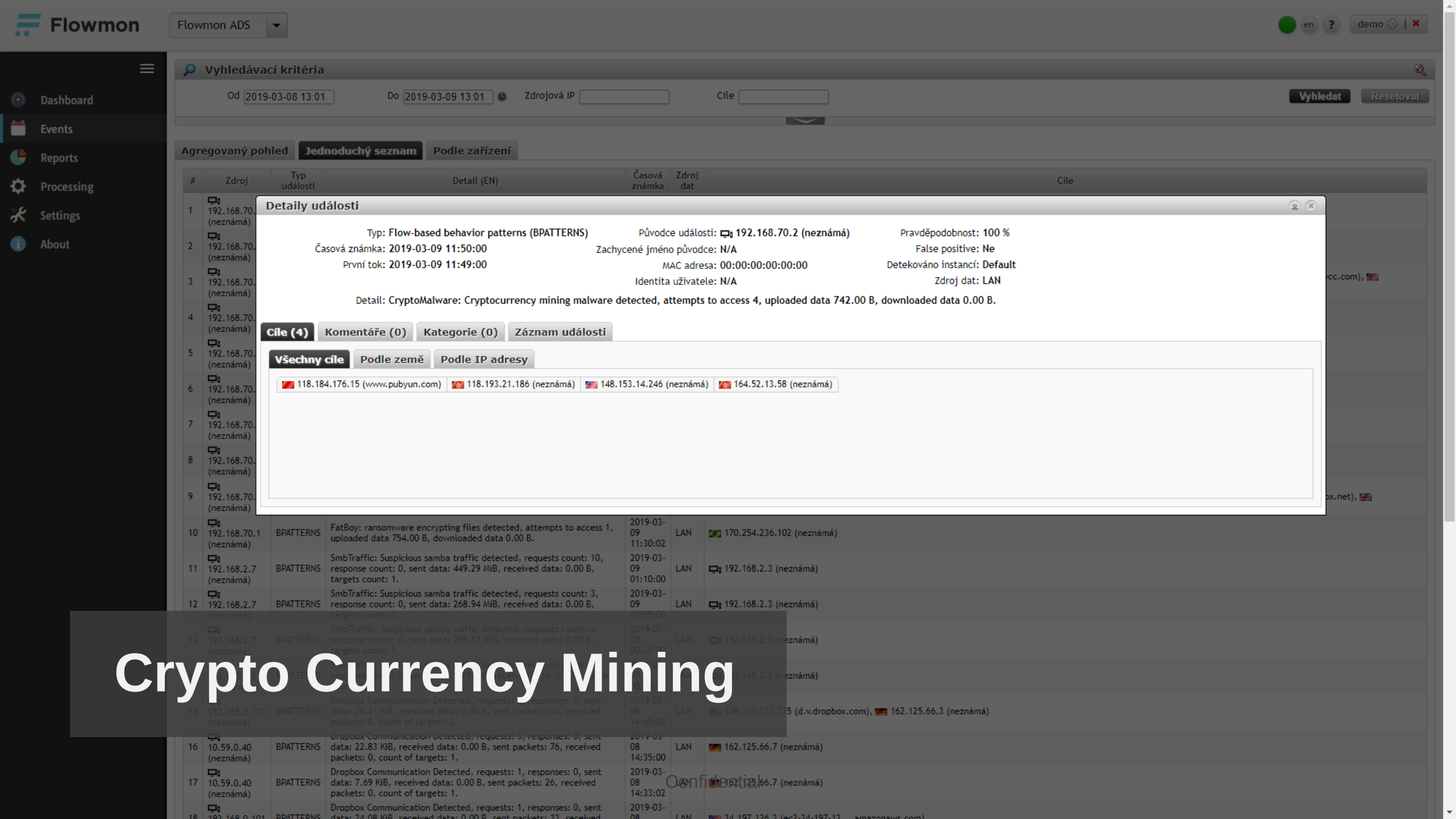
Flowmon
Driving Network Visibility

Recent Interesting Detections?

- OSX/MaMi in same way as DNSChanger in 2011
- WannaCry in large IT infrastructure organization
- Ransomware in action encrypting X-ray images in hospital
- Data leakage via DNS (TXT queries)
- Cryptocurrency Mining on various client devices
- Attacker controlling and sniffing traffic via DHCP spoofing
- And many botnet infected devices in various industry verticals…



Wanna Cry Infected Device


Flowmon
Flowmon ADS
Dashboard
Events
Reports
Processing
Settings
About
Vyhledávací kritéria
Od 2019-03-08 13:01
Do 2019-03-09 13:01
Zdrojová IP
Cíle
Vyhledat
Resetovat
Agregovaný pohled
Jednoduchý seznam
Podle zařízení
Detaily události
Typ: Flow-based behavior patterns (BPATTERNS)
Časová známka: 2019-03-09 11:50:00
První tok: 2019-03-09 11:49:00
Původce události: 192.168.70.2 (neznámá)
Zachycené jméno původce: N/A
MAC adresa: 00:00:00:00:00:00
Identita uživatele: N/A
Pravděpodobnost: 100 %
False positive: Ne
Detekováno instancí: Default
Zdroj dat: LAN
Detail: CryptoMalware: Cryptocurrency mining malware detected, attempts to access 4, uploaded data 742.00 B, downloaded data 0.00 B.
Cíle (4)
Komentáře (0)
Kategorie (0)
Záznam události
Všechny cíle
Podle země
Podle IP adresy
118.184.176.15 (www.pubyun.com)
118.193.21.186 (neznámá)
148.153.14.246 (neznámá)
164.52.13.58 (neznámá)
Crypto Currency Mining

Use Case: Anomaly Detection and Forensics

Integration with Full Packet Capture for Forensic Evidence

Flowmon
Driving Network Visibility

Flowmon | Flowmon ADS | en | admin

Dashboard | Events | Reports | Processing | Settings | About

Search criteria | Search | Reset

Event details

Type: Communication with blacklisted hosts (BLACKLIST)
Timestamp: 2019-04-12 16:22:18
First flow: 2019-04-12 16:22:18

Event source: 192.168.222.27 (localhost)
Captured source hostname: N/A
MAC address: 00:0c:29:64:28:2c
User identity: N/A

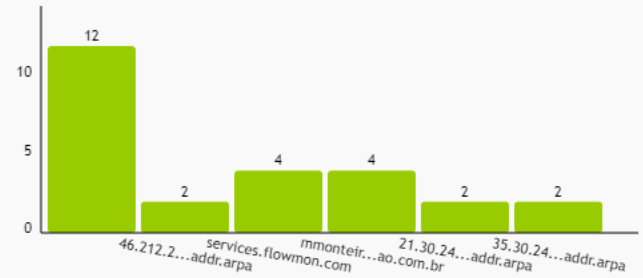
Probability: 100 %
False positive: No
Detected by instance: Default
Data feed: Default

Detail: Known malware domains (MD5:21d5abb9977d71918ee1de4e83dc8e84 / mmonteironavegacao.com.br), DNS queries: 2.

Targets (1) | Comments (0) | Categories (0) | **Event evidence** | Related IDS events (0) | Traffic records

Flow count in relation to DNS Question name

Save as a text file
Query the Monitoring Center

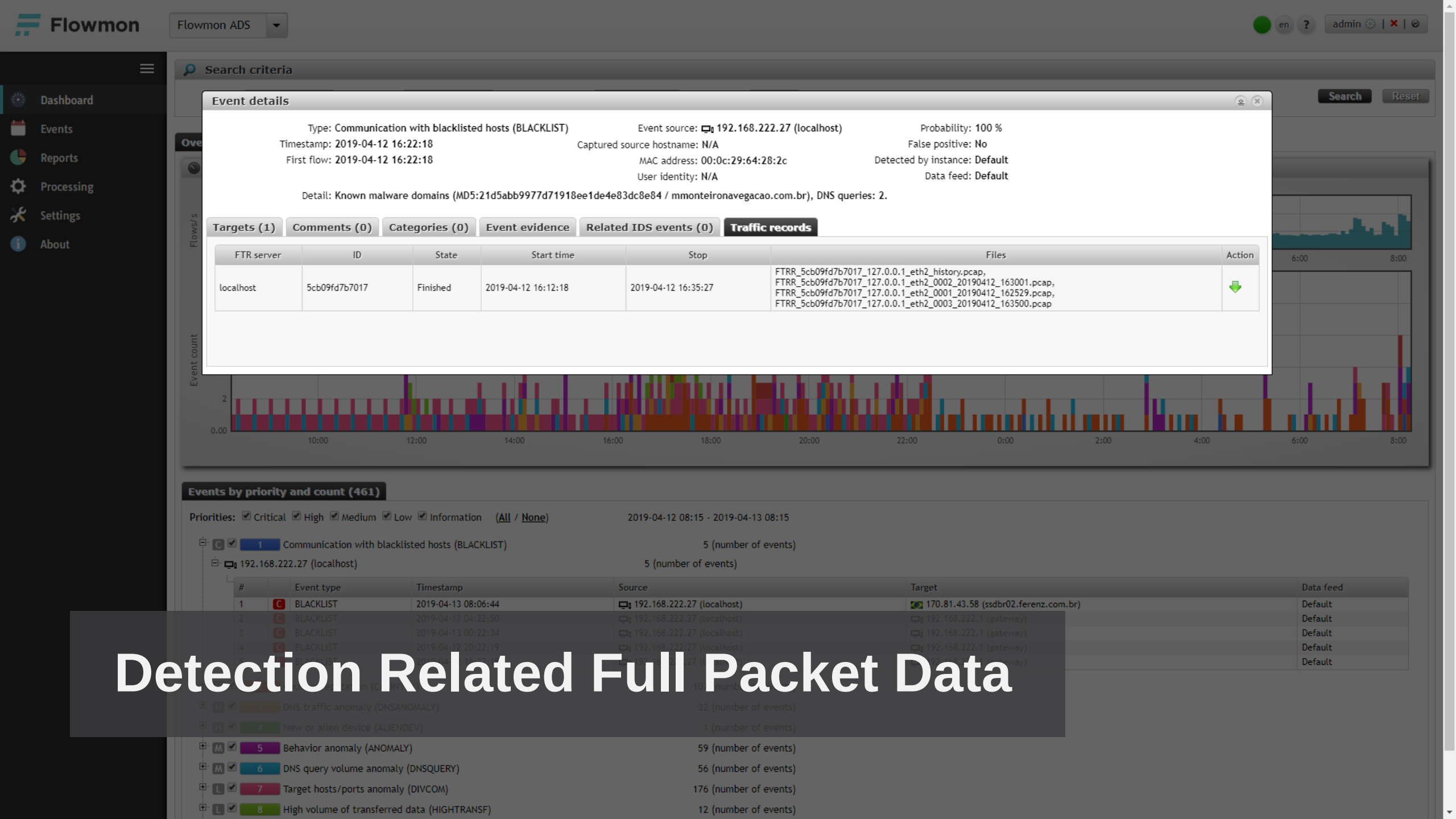


Filter flows: Show all flows

Source IP	Destination IP	Timestamp	Duration	Protocol	Source port	Destination port	Transferred	Packets	Flags	TOS	Source MAC	Destination MAC	App Tag	Data feed IP	DNS Question name
192.168.222.27 (localhost)	192.168.222.1 (gateway)	2019-04-12 16:22:18.135	0	UDP	46794	53	71	1	.....	Best Effort & Default	00:0c:29:64:28:2c	b0:b2:dc:bc:c0:90	dns	127.0.0.1	mmonteironavegacao.com.br
192.168.222.27 (localhost)	192.168.222.1 (gateway)	2019-04-12 16:22:18.135	0	UDP	46794	53	71	1	.....	Best Effort & Default	00:0c:29:64:28:2c	b0:b2:dc:bc:c0:90	dns	127.0.0.1	mmonteironavegacao.com.br
192.168.222.1 (gateway)	192.168.222.27 (localhost)	2019-04-12 16:22:18.394	0	UDP	53	46794	298	1	.....	Best Effort & Default	b0:b2:dc:bc:c0:90	00:0c:29:64:28:2c	dns	127.0.0.1	mmonteironavegacao.com.br
192.168.222.1 (gateway)	192.168.222.27 (localhost)	2019-04-12 16:22:18.451	0	UDP	53	46794	150	1	.....	Best Effort & Default	b0:b2:dc:bc:c0:90	00:0c:29:64:28:2c	dns	127.0.0.1	mmonteironavegacao.com.br

Malware Infected Device Detected via DNS

5 Behavior anomaly (ANOMALY) 59 (number of events)
6 DNS query volume anomaly (DNSQUERY) 56 (number of events)
7 Target hosts/ports anomaly (DIVCOM) 176 (number of events)
8 High volume of transferred data (HIGHTRANSF) 12 (number of events)



Detection Related Full Packet Data

FTRR_5cb09fd7b7017_127.0.0.1_eth2_history.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns.qry.name == "mmonteironavegacao.com.br"

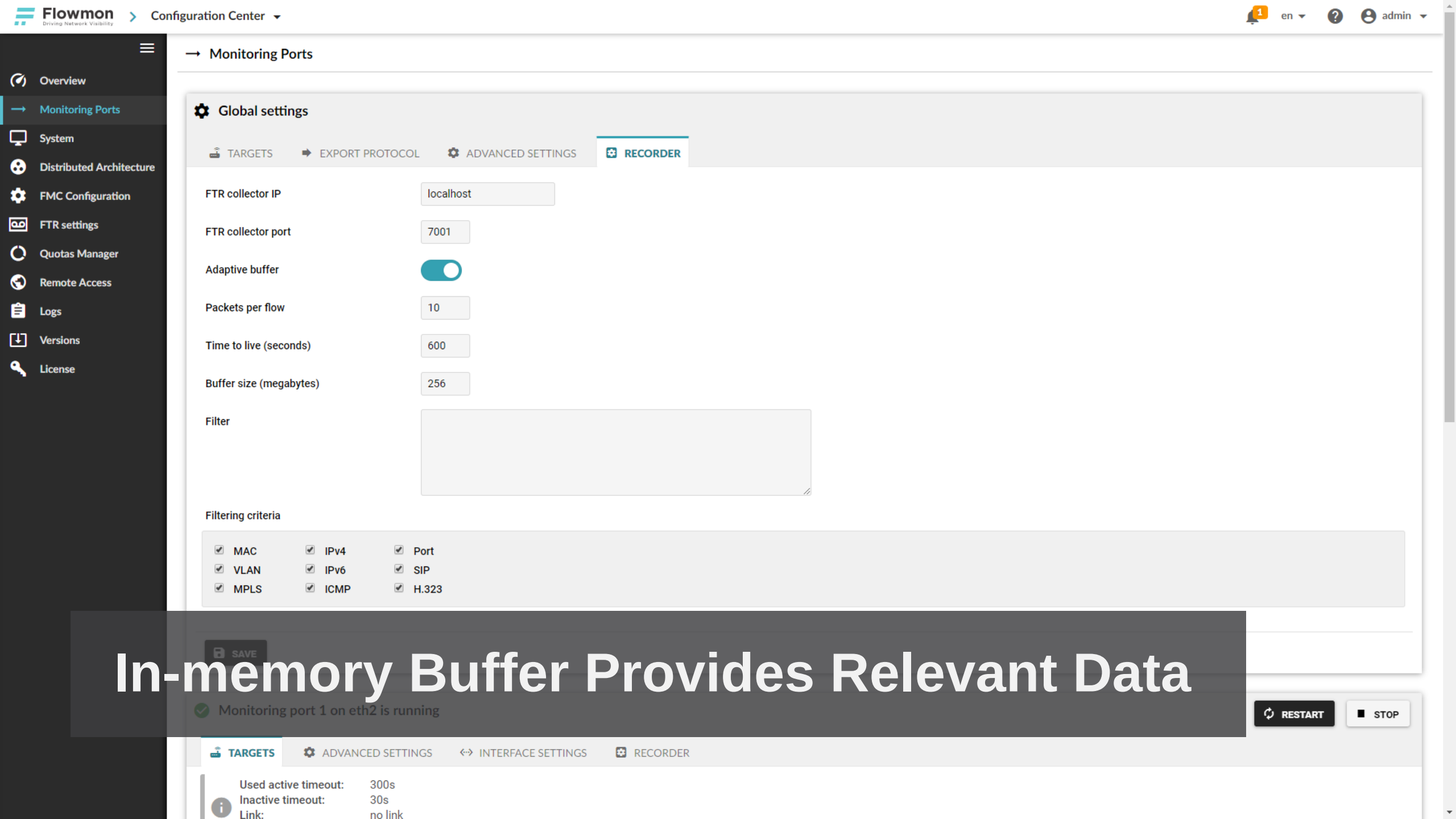
ime	Source	Destination	Protocol	Length	Info
019-04-12 16:22:18,135377	192.168.222.27	192.168.222.1	DNS	85	Standard query 0xde40 A mmonteironavegacao.com.br
019-04-12 16:22:18,135392	192.168.222.27	192.168.222.1	DNS	85	Standard query 0x3594 AAAA mmonteironavegacao.com.br
019-04-12 16:22:18,135392	192.168.222.27	192.168.222.1	DNS	85	Standard query 0x3594 AAAA mmonteironavegacao.com.br
019-04-12 16:22:18,394398	192.168.222.1	192.168.222.27	DNS	312	Standard query response 0xde40 A mmonteironavegacao.com.br A 170.81.43.58 NS f.root-servers.net NS g.root-servers.net NS h.root-servers.net NS i.root-servers.net NS j.root-servers.net NS k.r…
019-04-12 16:22:18,394398	192.168.222.1	192.168.222.27	DNS	312	Standard query response 0xde40 A mmonteironavegacao.com.br A 170.81.43.58 NS f.root-servers.net NS g.root-servers.net NS h.root-servers.net NS i.root-servers.net NS j.root-servers.net NS k.r…
019-04-12 16:22:18,451352	192.168.222.1	192.168.222.27	DNS	164	Standard query response 0x3594 AAAA mmonteironavegacao.com.br SOA ns1.ssdbr02.ferenz.com.br
019-04-12 16:22:18,451352	192.168.222.1	192.168.222.27	DNS	164	Standard query response 0x3594 AAAA mmonteironavegacao.com.br SOA ns1.ssdbr02.ferenz.com.br

```
> Frame 535: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits)
> Ethernet II, Src: ZyxelCom_bc:c0:90 (b0:b2:dc:bc:c0:90), Dst: Vmware_64:28:2c (00:0c:29:64:28:2c)
> Internet Protocol Version 4, Src: 192.168.222.1, Dst: 192.168.222.27
> User Datagram Protocol, Src Port: 53, Dst Port: 46794
v Domain Name System (response)
    Transaction ID: 0x3594
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
  v Queries
    v mmonteironavegacao.com.br: type AAAA, class IN
        Name: mmonteironavegacao.com.br
        [Name Length: 25]
        [Label Count: 3]
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
  v Authoritative nameservers
    v mmonteironavegacao.com.br: type SOA, class IN, mname ns1.ssdbr02.ferenz.com.br
        Name: mmonteironavegacao.com.br
        Type: SOA (Start Of a zone of Authority) (6)
        Class: IN (0x0001)
        Time to live: 600
        Data length: 67
        Primary name server: ns1.ssdbr02.ferenz.com.br
        Responsible authority's mailbox: niltonsouzza.hotmail.com
        Serial Number: 2018111902
        Refresh Interval: 3600 (1 hour)
        Retry Interval: 1800 (30 minutes)
        Expire limit: 1209600 (14 days)
        Minimum TTL: 86400 (1 day)
    [Request In: 515]
    [Time: 0.3159600 seconds]
```

Forensics in Wireshark with HISTORY PCAP

```
0030  00 00 00 01 00 00 12 6d  6d 6f 6e 74 65 69 72 6f   ·····m monteiro
```

Query Name (dns.qry.name), 27 bytes | Packets: 749 · Displayed: 7 (0.9%) | Profile: Default


Flowmon
Configuration Center
en
admin
Overview
Monitoring Ports
System
Distributed Architecture
FMC Configuration
FTR settings
Quotas Manager
Remote Access
Logs
Versions
License
Monitoring Ports
Global settings
TARGETS
EXPORT PROTOCOL
ADVANCED SETTINGS
RECORDER
FTR collector IP
localhost
FTR collector port
7001
Adaptive buffer
Packets per flow
10
Time to live (seconds)
600
Buffer size (megabytes)
256
Filter
Filtering criteria
MAC
IPv4
Port
VLAN
IPv6
SIP
MPLS
ICMP
H.323
SAVE
In-memory Buffer Provides Relevant Data
Monitoring port 1 on eth2 is running
RESTART
STOP
TARGETS
ADVANCED SETTINGS
INTERFACE SETTINGS
RECORDER
Used active timeout:
300s
Inactive timeout:
30s
Link:
no link

Use of Flow Events for NetOps & SecOps

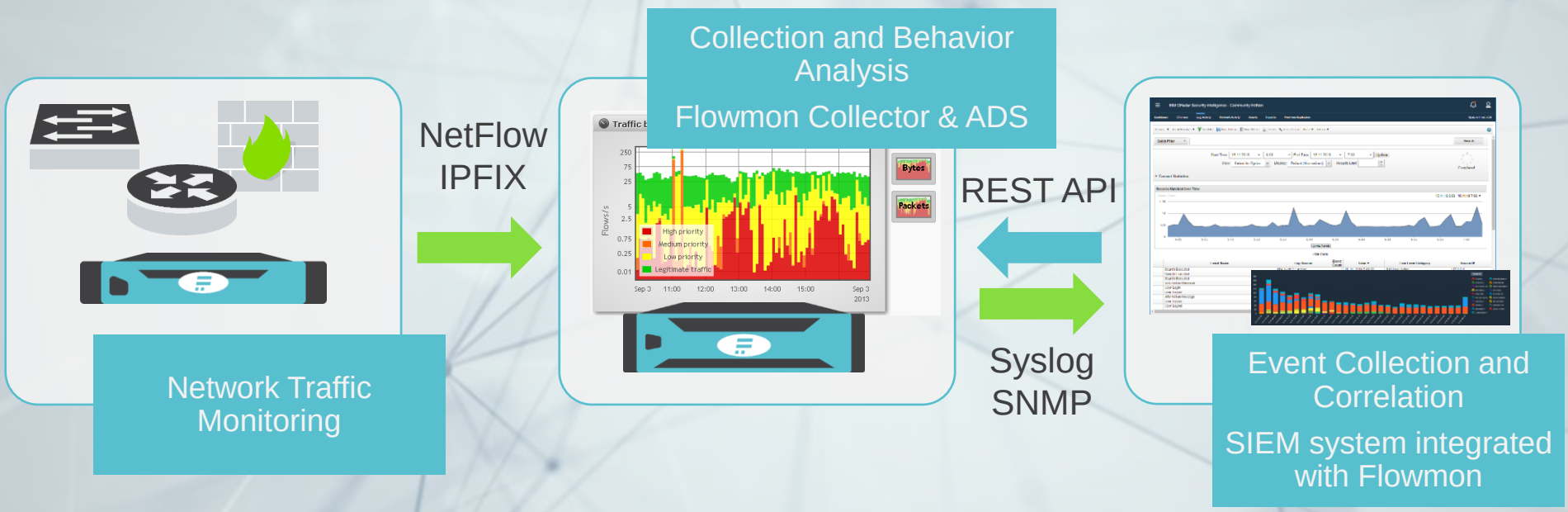
Integration to Streaming Data Analytics and Operations

Flowmon
Driving Network Visibility

Integration with SIEMs and Analytic Platforms

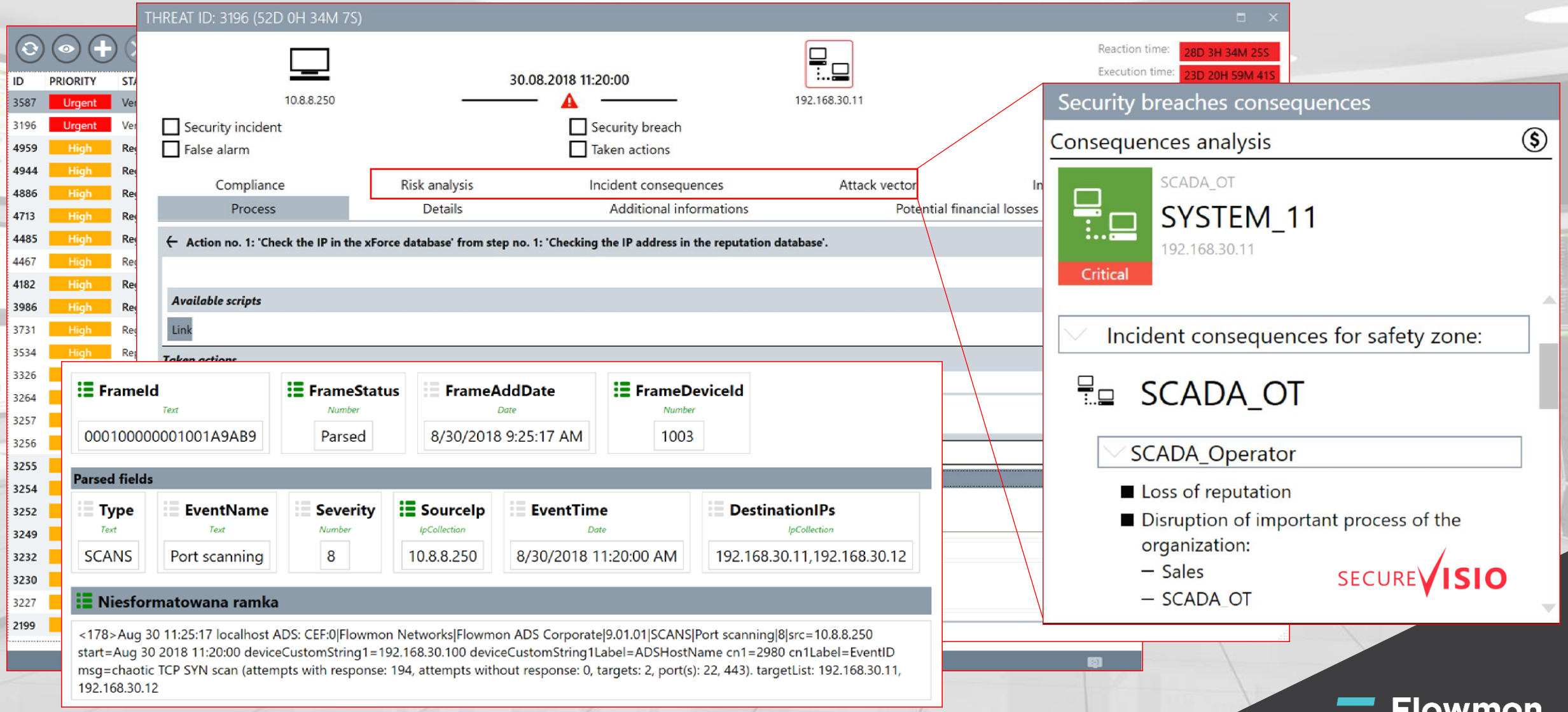
Flowmon ADS provides syslog feed of event to log management, SIEM, big data platform, incident handling or security automation tools.

These tools are only that powerful as their event sources.



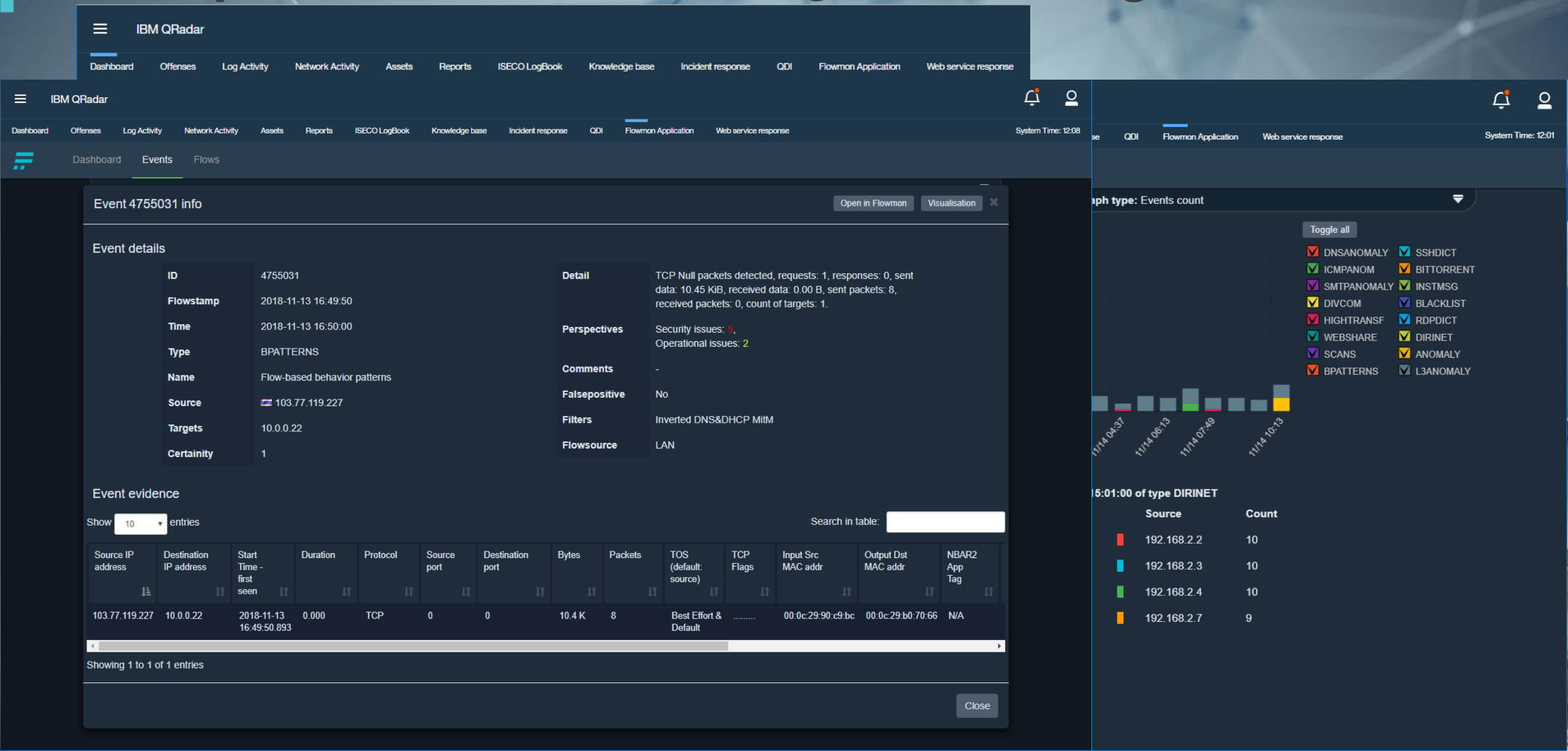
Flowmon
Driving Network Visibility

Sample Incident Handling and Security Automation



Flowmon
Driving Network Visibility

Sample Flowmon to IBM QRadar Integration



Detection and Mitigation Orchestration of Volumetric DoS/DDoS Attacks

Protect your business & customers satisfaction

Easy, flexible and cost efficient way of DDoS Protection

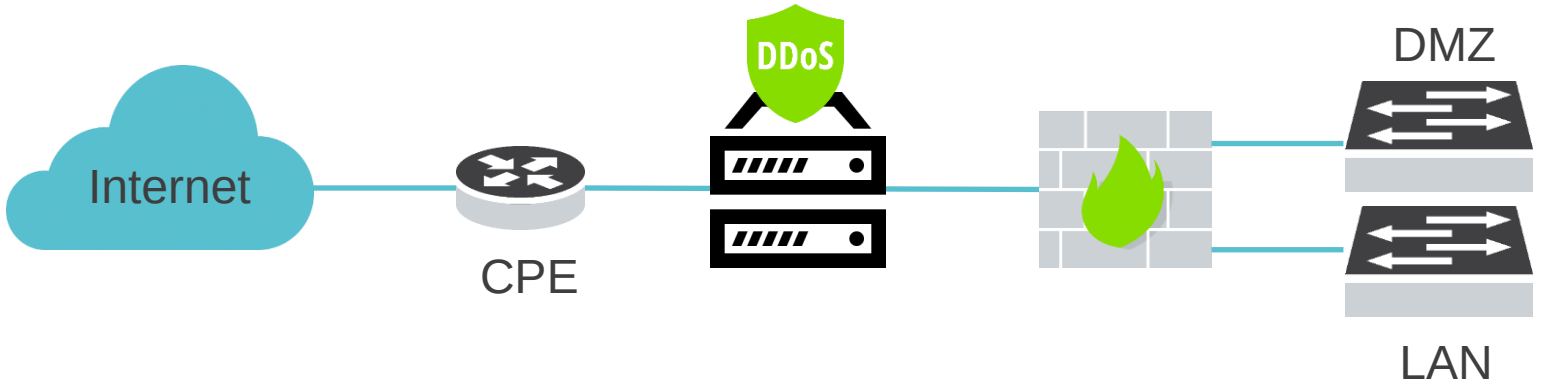
Saves costs on extra HW, mitigate with your network

Mikulas Labsky, Head of Telecommunications dept. at CD-Telematika: *“As a service provider, in-line DDoS protection didn’t fit our needs. Fast flow-based DDoS detection with out-of-path mitigation is the ideal solution for any ISP.“*

Flowmon
Driving Network Visibility

Enterprise Protection Strategy

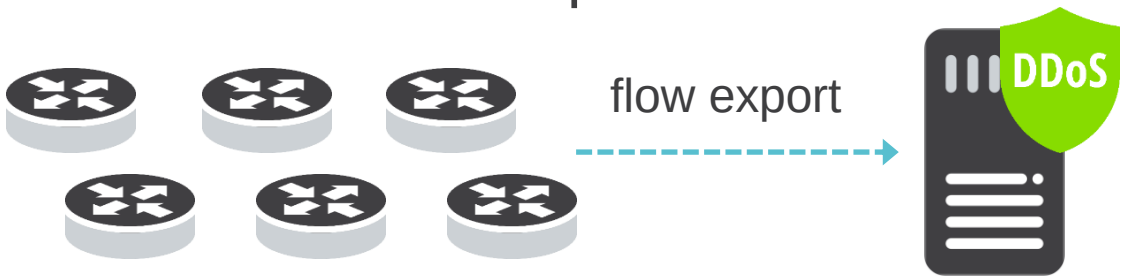
- Enterprise perimeter scheme
  - Limited number of uplinks and capacity



- In-line DDoS mitigation appliance
  - All-in-one detection & mitigation out of the box
  - Volumetric + application (L3/L4/L7) attacks coverage
  - Up to the uplink capacity!

Backbone Protection Strategy

- Backbone perimeter specifics
  - Multiple peering points – routers & uplinks
  - Large transport capacity – tens of gigabits easily
  - In-line protection is close to impossible!

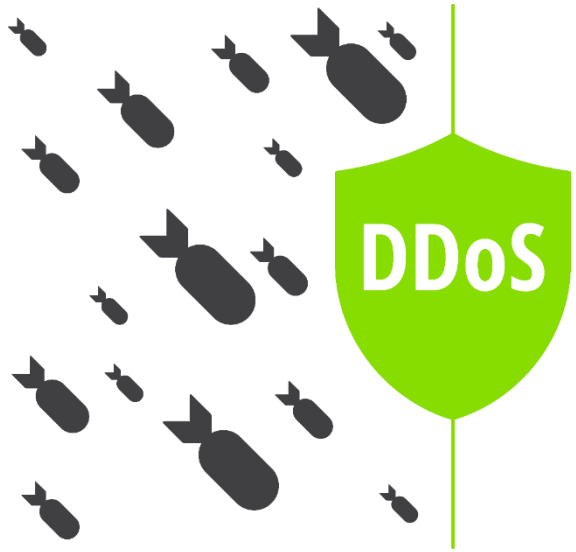


1. Flow collection
2. DDoS detection
3. Routing control
4. Mitigation control

- Flow-based detection and out-of-path mitigation
  - Easy and cost efficient to deploy in backbone/ISP
  - Prevents volumetric DDoS to reach enterprise perimeter

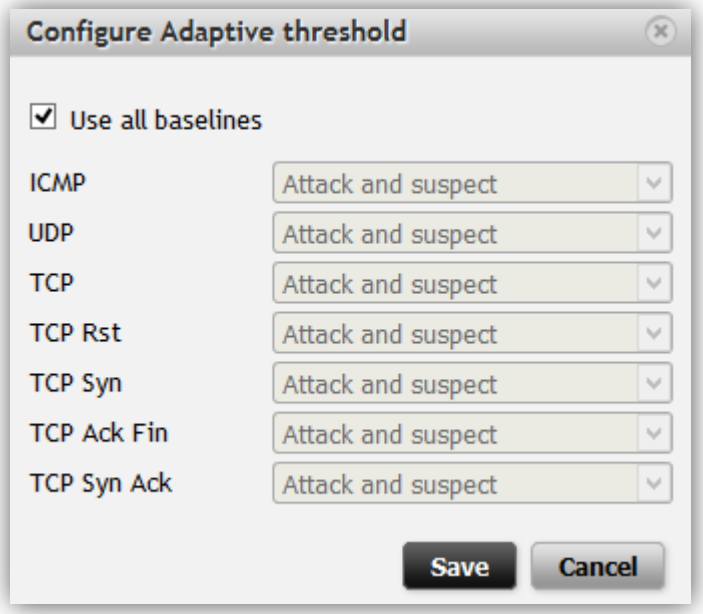
Attack Detection

- Detection performed over protected segments
  - Segments defined by network subnets
- For each segment, a set of baselines is learned from monitored traffic. The attack is detected if the current traffic exceeds defined threshold.
- Baseline is learned for:
  - TCP traffic with specific flags
  - UDP traffic
  - ICMP traffic



Adaptive Thresholds

- Fully automated approach how to set the baselines without the need of manual inputs
- Two levels of method sensitivity
  - Attack or suspect
- Simple configuration
- Configurable learning period
  - Continuous baseline update
- False positive tune-up
  - Per attack



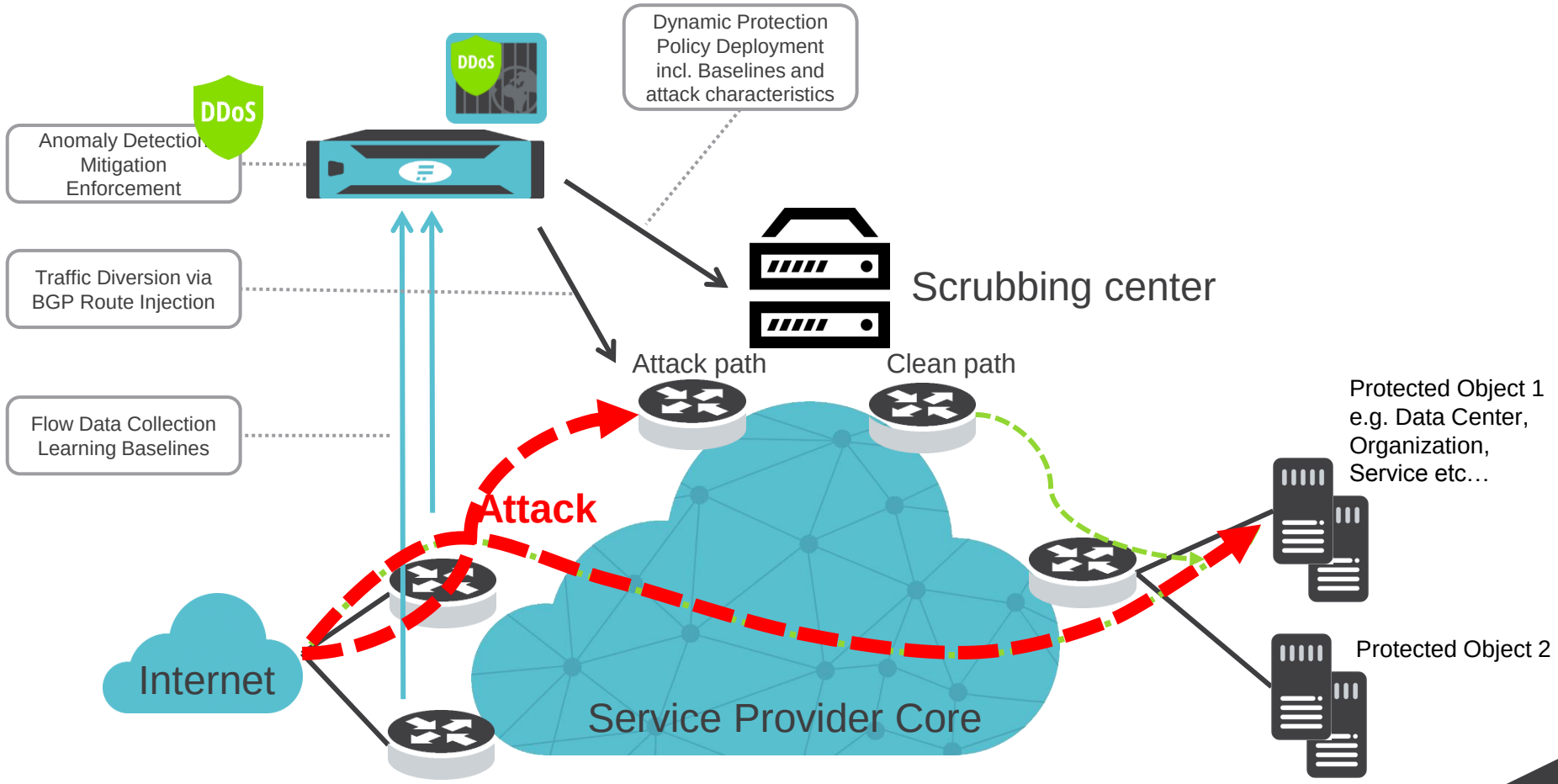
Flowmon
Driving Network Visibility

Use Case: DDoS Protection

Various Protection Scenarios using Flow-based Detection

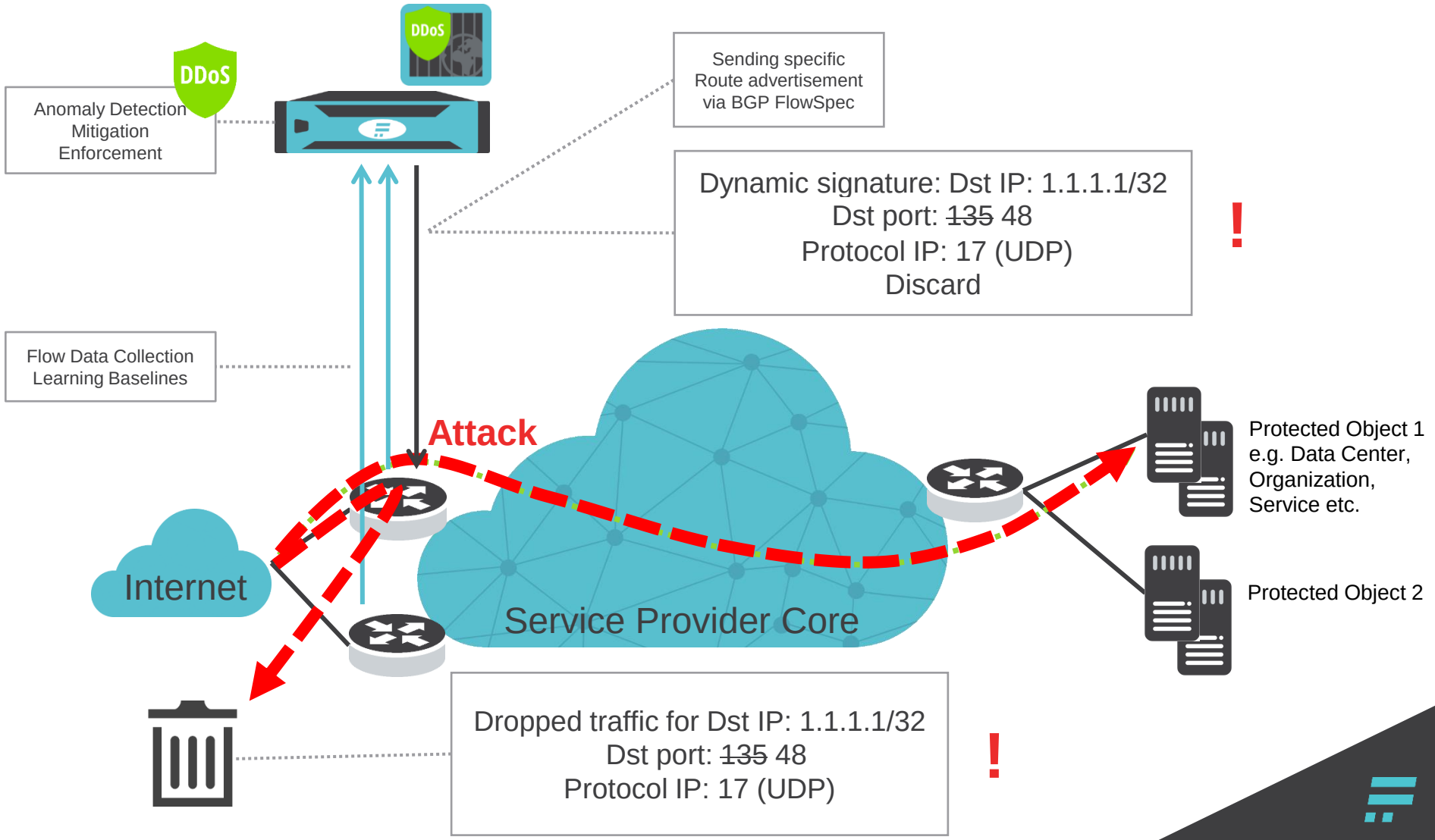
Flowmon
Driving Network Visibility

Out-of-Band with Local Scrubbing Appliance



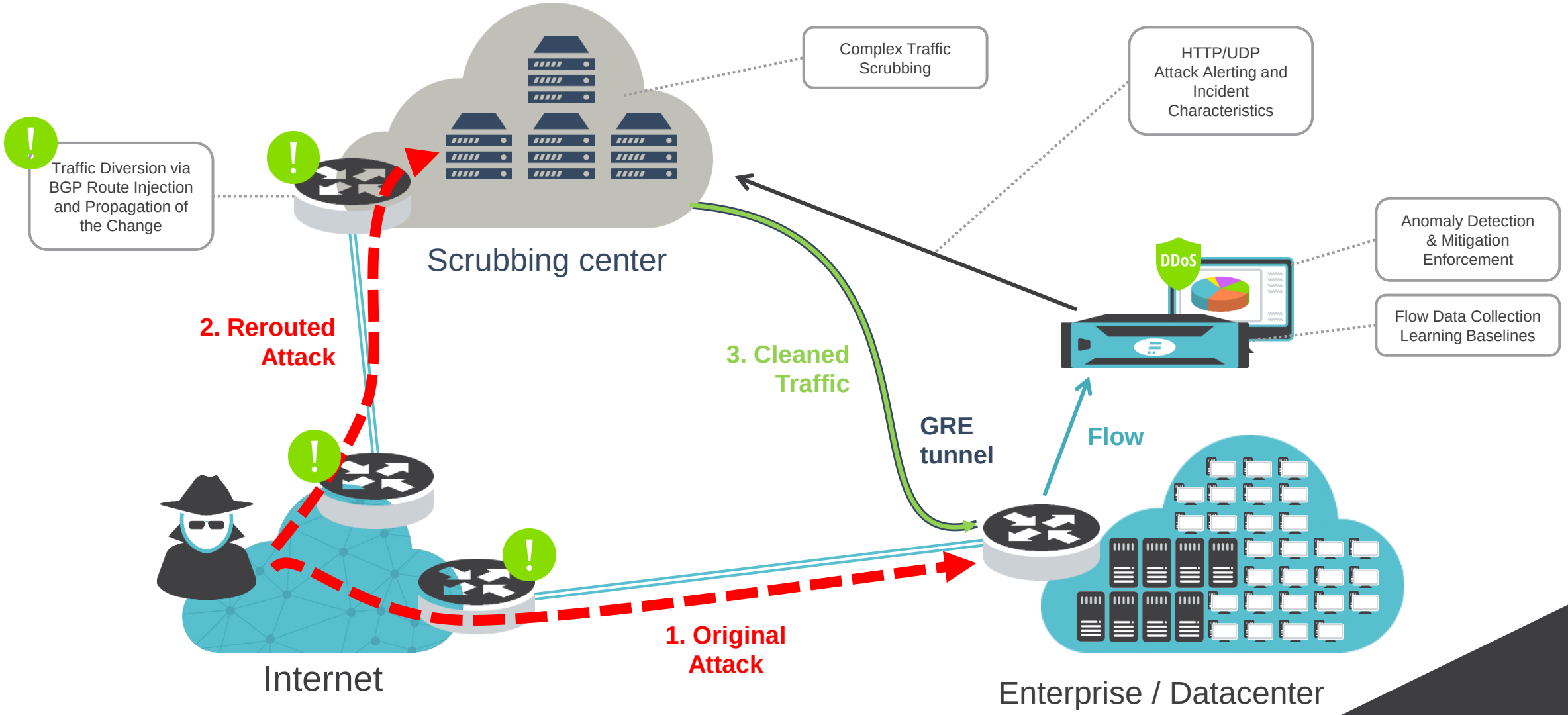
Flowmon
Driving Network Visibility

Mitigation Through Infrastructure (BGP Flowspec)



Flowmon
Driving Network Visibility

Cloud Scrubbing & Cloud Signaling



Flowmon
Driving Network Visibility

Summary

Benefit From Using Flow Data

Flowmon
Driving Network Visibility

Packet Analysis

The complexity of such systems puts high demands on the knowledge/experience of administrators. These tools are simply to heavy for daily use and majority of use case.

Packet analysis tools do not scale to current backbone bandwidth and available budget.

Flow Monitoring

Flow-based easy to use and affordable solution to enable network visibility and easy to use troubleshooting. Extendable to application monitoring and security means single platform and lower costs.

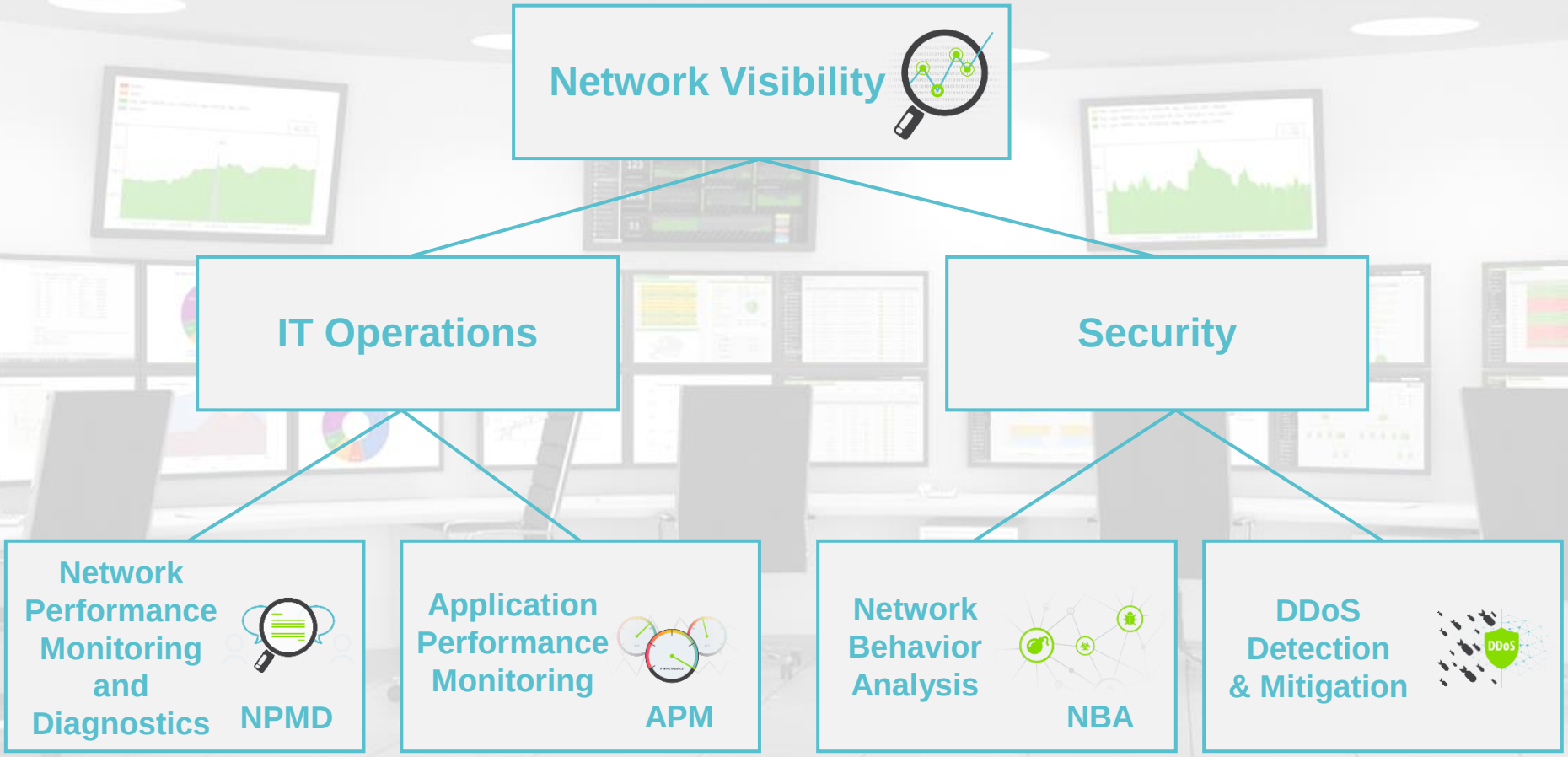
Flow enriched with L7 visibility and on-demand packet capture is the future of Network Performance Monitoring and Diagnostics.

SNMP Monitoring

Basic IT infrastructure monitoring to provide network, device and service status. Limited flow support – technically inadequate commodity solution. Does not help to troubleshoot, track user experience or contribute to network security.

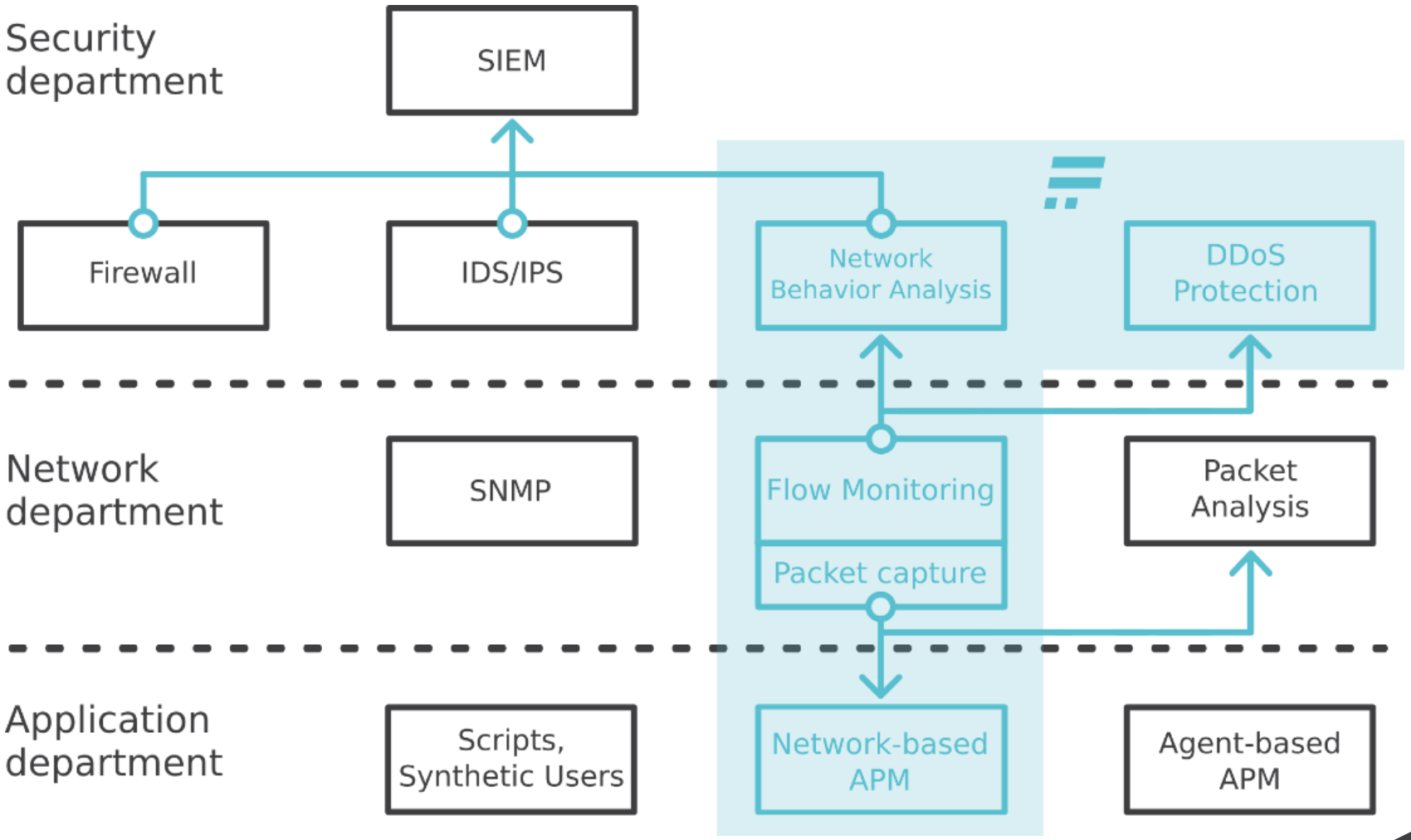
Flowmon
Driving Network Visibility

Flowmon Portfolio



Flowmon
Driving Network Visibility

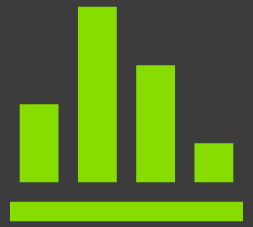
Flowmon Fit with other Tools



Flowmon
Driving Network Visibility

Real-time Detection & Response

45-250 days in average to detect an incident



Occurs when malfunction of critical service happened (NISD)

Occurs when sensitive or personal data breach (GDPR)

Detect attack, event or incident in real-time, analyze it in few minutes

Use automation processes for alerting & reporting (3rd parties integration – SIEM etc.)

Classify information automatically (based on manual data predefinition), immediate response

Flowmon
Driving Network Visibility

Flowmon Networks

is an Czech based vendor devoted to innovative network traffic & performance & security monitoring

1000+ customers
40+ countries

First 100G probes in the world

Strong R&D background

European origin

Customer references

SEGA, AVG, KBC, Konica Minolta, vodafone, TDK, Oriflame Sweden, Siemens, Slovenská sporiteľňa, Volkswagen, orange, Telefónica, Allianz, hp, T-Mobile, GÉANT Networks • Services • People, KIA, upc, Raiffeisen BANK, e·on

Flowmon
Driving Network Visibility

Information Sources

- Public available **technical documentation** and **specifications**
  - https://www.flowmon.com/en/resources
  - All the models, parameters included in specification documents online
- Many **case studies** and **whitepapers** on-line
  - https://www.flowmon.com/en/company/success-stories-case-studies
- **Technical materials** are available on support portal
  - https://support.flowmon.com
  - APIs, technical documentation, software packages, …
- Flowmon **BLOG**
  - https://www.flowmon.com/en/blog
  - New features, releases, use cases, …
- Flowmon Youtube **video channel**
  - https://www.youtube.com/c/FlowmonNetworkMonitoringSecurity
  - Webinar recordings, tutorials, demos, …

Thank you

Performance monitoring, visibility and security with a single solution

Zoltán Csecsodi, Sales Director CZ

zoltan.csecsodi@flowmon.com, +420 723 555 057

Pavel Minarik, Chief Technology Officer

Pavel.minarik@flowmon.com. +420 733 713 703

Flowmon Networks, a.s.
Sochorova 3232/34
619 00 Brno, Czech Republic
www.flowmon.com

Flowmon
Driving Network Visibility