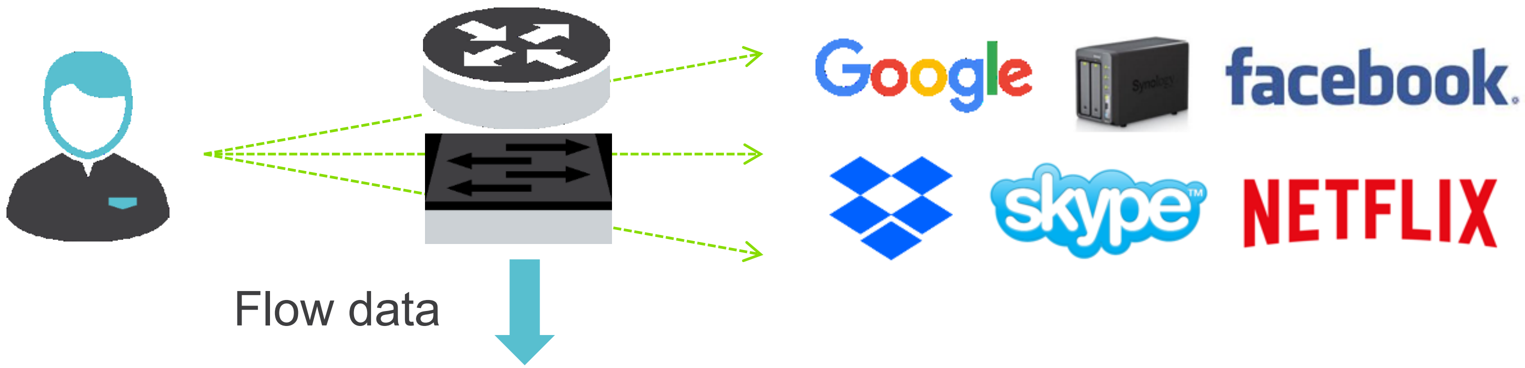
Role of Flow Monitoring in Cyber Security

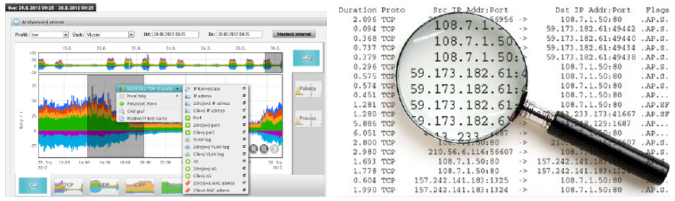
Zoltán Csecsodi, Sales Director CZ

Flowmon
Driving Network Visibility

What is Flow Data?

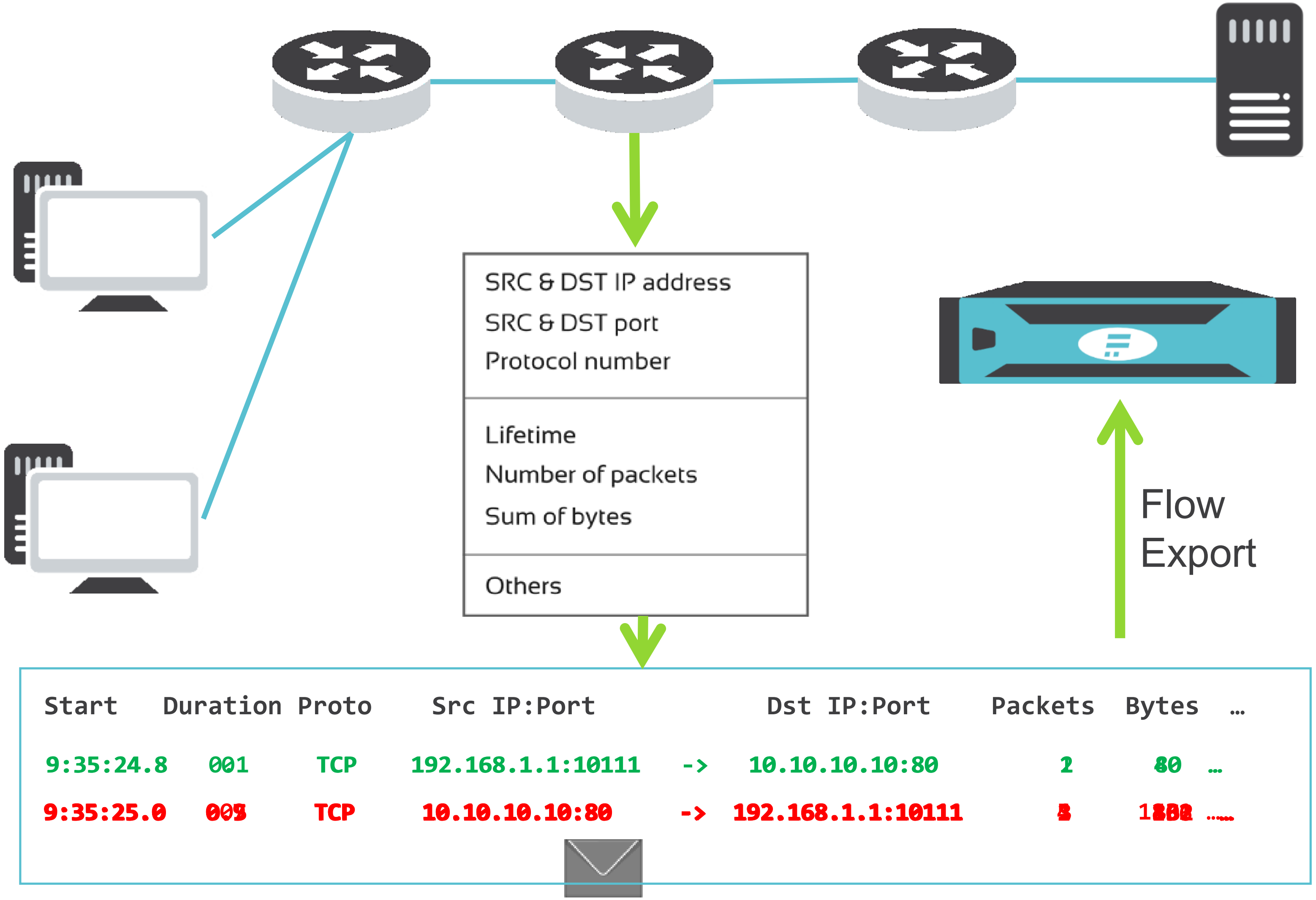
- Modern method for network monitoring – flow measurement
- Cisco standard NetFlow v5/v9, IETF standard IPFIX
- Focused on L3/L4 information and volumetric parameters
- Real network traffic to flow statistics reduction ratio 500:1





```
Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Flags
   2.096 TCP     2[illegible]:56956   ->       108.7.1.50:80     .AP.S.
   0.094 TCP     [illegible]          ->  59.173.182.61:49442    .AP.S.
   0.368 TCP     [illegible]          ->  59.173.182.61:49440    .AP.S.
   0.737 TCP     [illegible]          ->  59.173.182.61:49434    .AP.S.
   0.379 TCP     [illegible]          ->  59.173.182.61:49438    .AP.S.
   0.296 TCP     [illegible]                   108.7.1.50:80     .AP.S.
   0.575 TCP     [illegible]                   108.7.1.50:80     .AP.S.
   0.574 TCP     [illegible]                   108.7.1.50:80     .AP.S.
   0.451 TCP     [illegible]                   108.7.1.50:80     .AP...
   1.281 TCP     [illegible]                   108.7.1.50:80     .AP.SF
   1.280 TCP     [illegible]            [illegible].233.173:41667 .AP.SF
   5.886 TCP     [illegible]          ->  [illegible].248.129:1687 .AP...
   6.051 TCP     [illegible]13.233[illegible]687 ->  [illegible]:80  .AP...
   2.800 TCP         108.7.1.50:80    ->  210.5[illegible]:56607 .AP.S.
   2.980 TCP    210.56.6.116:56607    ->       108.7.[illegible]  .AP.S.
   1.693 TCP         108.7.1.50:80    ->  157.242.141.18[illegible]
   1.778 TCP         108.7.1.50:80    ->  157.242.141.183:132[illegible]
   0.604 TCP  157.242.141.183:1325    ->       108.7.1.50:80
   1.990 TCP  157.242.141.183:1324    ->       108.7.1.50:80     .AP.S.
```

Flow Monitoring Principle



SRC & DST IP address
SRC & DST port
Protocol number

Lifetime
Number of packets
Sum of bytes

Others

Flow Export

```
Start     Duration Proto    Src IP:Port               Dst IP:Port      Packets  Bytes  …
9:35:24.8   001     TCP   192.168.1.1:10111  ->  10.10.10.10:80          2       80   …
9:35:25.0   005     TCP    10.10.10.10:80    ->  192.168.1.1:10111       4     1800  ……
```

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.”

Flow vs. Packet Analysis on 10G

	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

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, PCAPs when needed

L2

- MAC
- VLAN
- MPLS
- GRE
- ESP
- OTV

L3/L4

- Standard items
- NPM metrics
  - RTT, SRT, …
- TTL, SYN size, …
- ASN (BGP)
- Geolocation
- VxLAN

L7

- NBAR2
- HTTP
- SNI
- DNS
- DHCP
- IEC104
- SMB/CIFS
- VoIP (SIP)
- Email
- SQL
- SSL/TLS
- CoAP

Why Flow Monitoring?

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

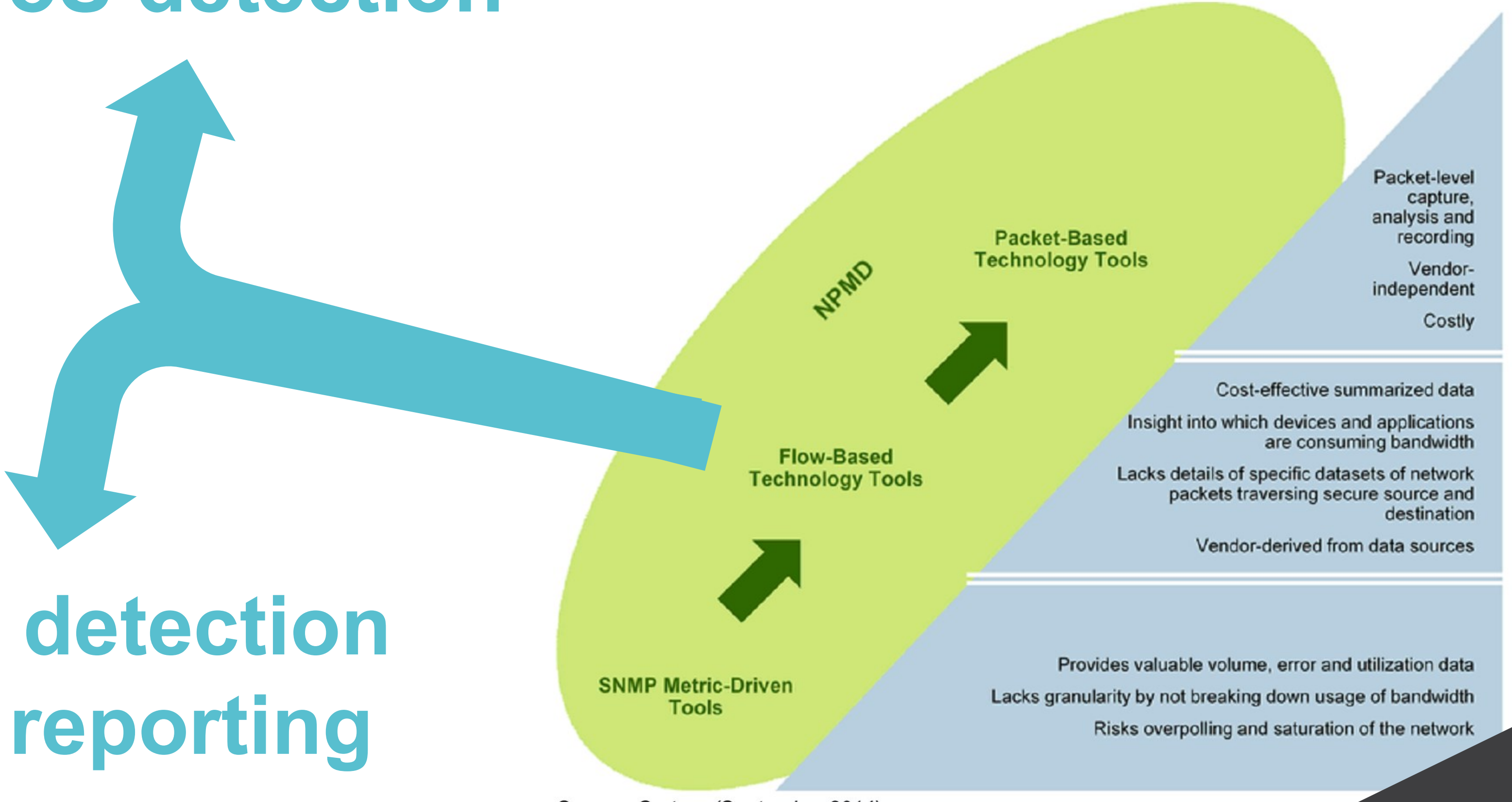
Gartner notes that 80% of network troubleshooting can be solved with NetFlow.

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.

Using Flow Data For Security

Volumetric
DDoS detection

Gartner


NPMD
Packet-Based Technology Tools
Flow-Based Technology Tools
SNMP Metric-Driven Tools
Packet-level capture, analysis and recording
Vendor-independent
Costly
Cost-effective summarized data
Insight into which devices and applications are consuming bandwidth
Lacks details of specific datasets of network packets traversing secure source and destination
Vendor-derived from data sources
Provides valuable volume, error and utilization data
Lacks granularity by not breaking down usage of bandwidth
Risks overpolling and saturation of the network

Anomaly detection
Incident reporting

Source: Gartner (September 2014)

Findings

- Most "advanced" attacks target basic vulnerabilities.
- The notion that "signatures are dead" is a misguided hyperbole.
- Your detection and response capabilities are more important than blocking and prevention.
- "Incident response" is the wrong mindset.
- Protection should be delivered as an integrated system, not delivered as siloed offerings.
- Monitoring and analytics should be at the core of all next-generation security platforms.
- Not all vendors will survive these shifts.

Gartner

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

Next Generation Network Security - Behavior Analysis & Anomaly Detection

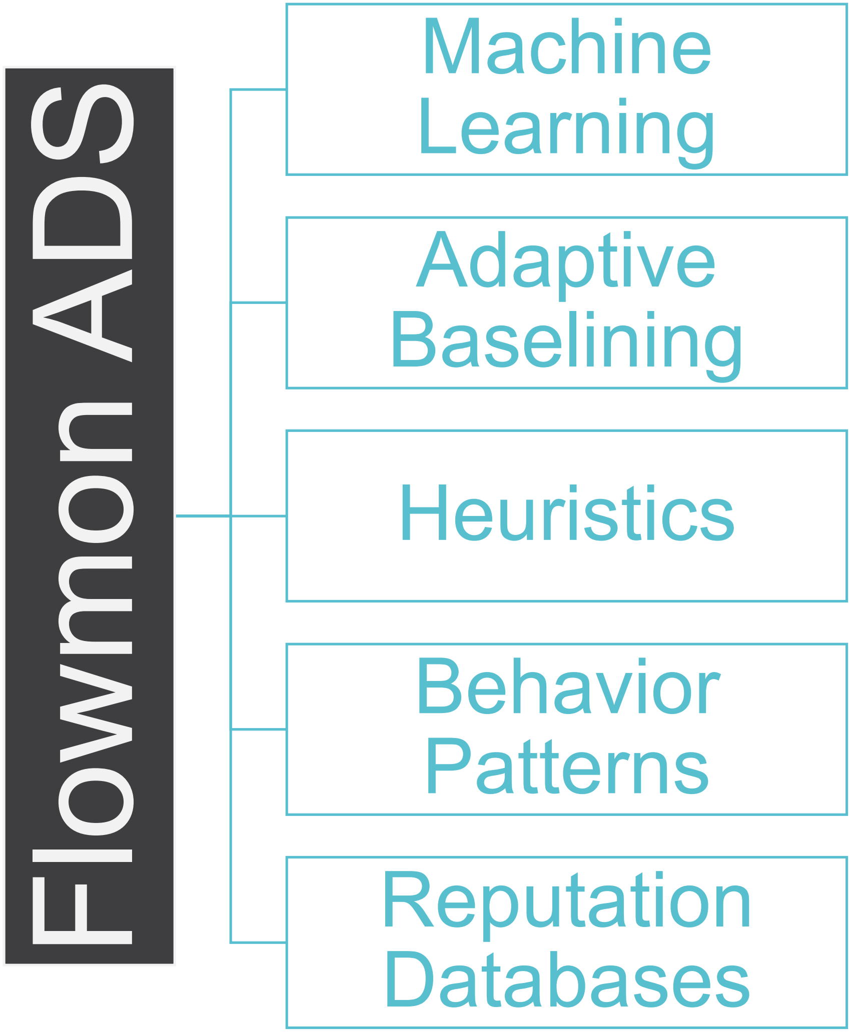
Detects and alerts on abnormal behaviors

Reports anomalies and advanced persistent threats

Detect intrusions and attacks not visible by standard signature based tools

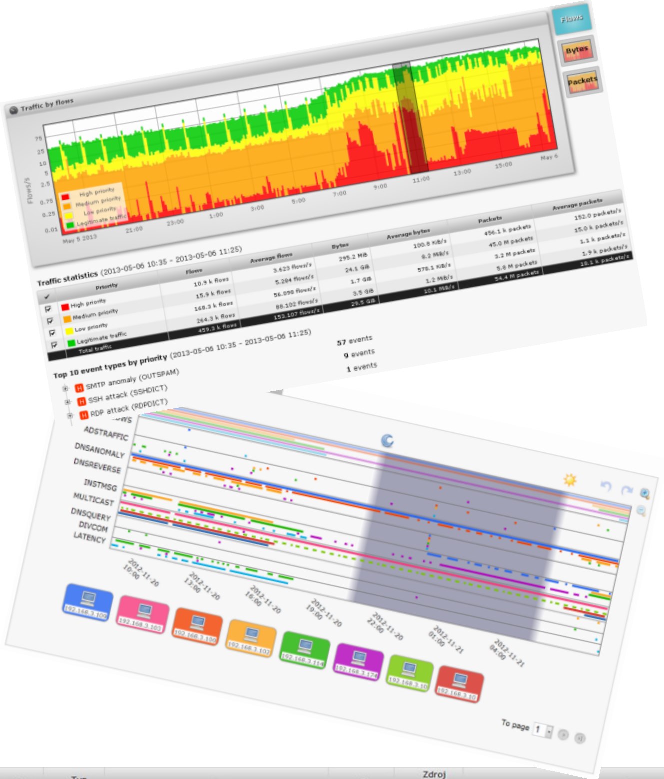
Gartner: *“Blocking and prevention is not sufficient. After you deployed firewall and IPS, you should implement network behavior analysis to identify problems that are undetectable using other techniques.”*

Flowmon ADS Principles



Flowmon ADS

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

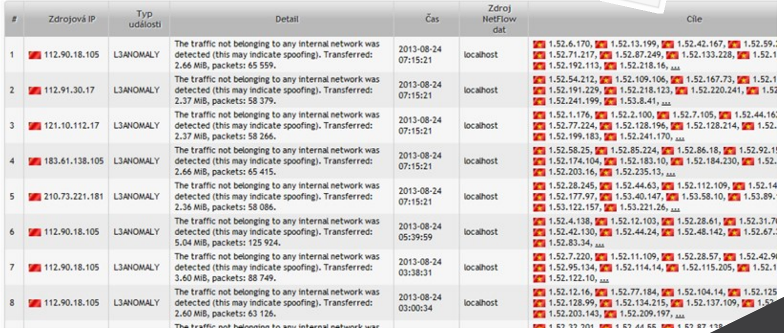


Traffic statistics (2013-05-06 10:35 - 2013-05-06 11:25)

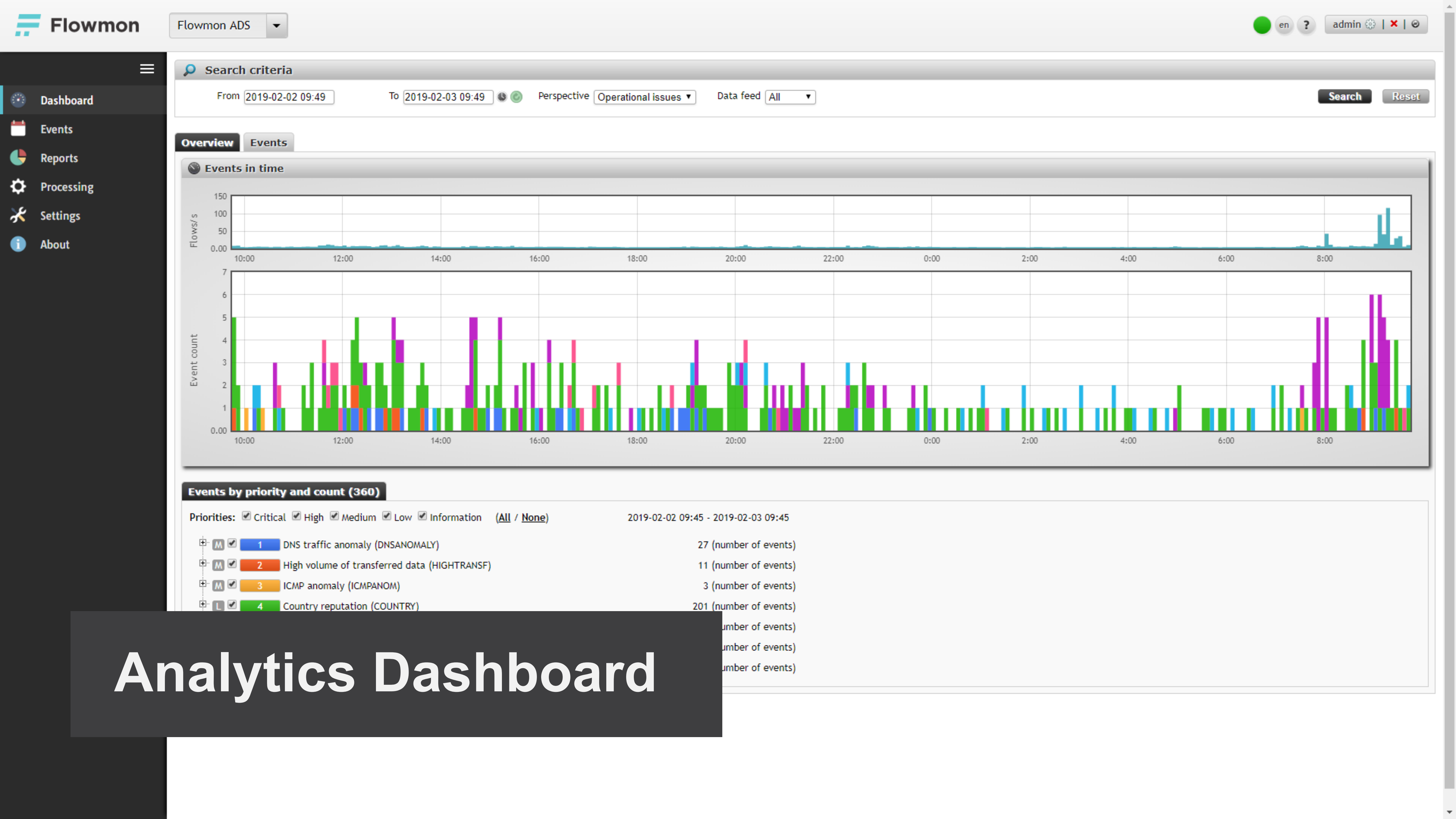
✓	Priority	Flows	Average flows	Bytes	Average bytes	Packets	Average packets
☑	🟥 High priority	10.9 k flows	3.623 flows/s	295.2 MiB	100.8 KiB/s	456.1 k packets	152.0 packets/s
☑	🟧 Medium priority	15.9 k flows	5.284 flows/s	24.1 GiB	8.2 MiB/s	45.0 M packets	15.0 k packets/s
☑	🟨 Low priority	168.3 k flows	56.098 flows/s	1.7 GiB	578.1 KiB/s	3.2 M packets	1.1 k packets/s
☑	🟩 Legitimate traffic	264.3 k flows	88.102 flows/s	3.5 GiB	1.2 MiB/s	5.8 M packets	1.9 k packets/s
	Total traffic	459.3 k flows	153.107 flows/s	29.5 GiB	10.1 MiB/s	54.4 M packets	18.1 k packets/s

Top 10 event types by priority (2013-05-06 10:35 - 2013-05-06 11:25)

H SMTP anomaly (OUTSPAM)	57 events
H SSH attack (SSHDICT)	9 events
H RDP attack (RDPDICT)	1 events



#	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. 1.52.71.217, 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, 1.52 1.52.203.143, 1.52.209.197, ...
			The traffic not belonging to any internal network was			1.52.32.201, 1.52.44.55, 1.52.87.138



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

Events by priority and count (360)

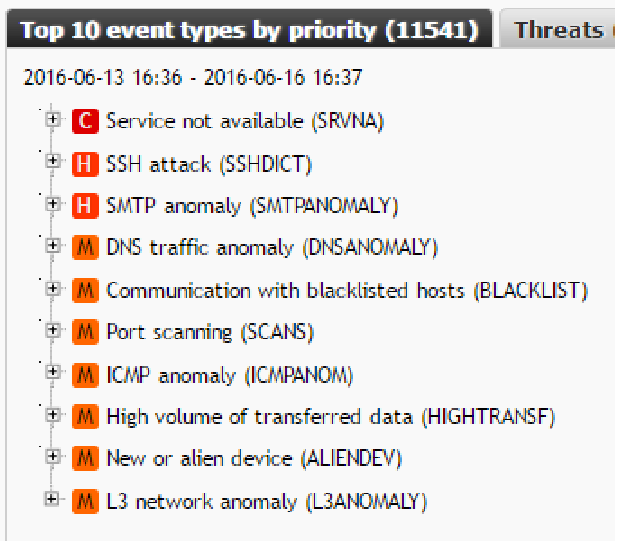
Priorities: ☑ Critical ☑ High ☑ Medium ☑ Low ☑ Information (All / None) 2019-02-02 09:45 - 2019-02-03 09:45

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)
				umber of events)
				umber of events)
				umber 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



2016-06-13 16:36 - 2016-06-16 16:37

- C Service not available (SRVNA)
- H SSH attack (SSHDICT)
- H SMTP anomaly (SMTPANOMALY)
- M DNS traffic anomaly (DNSANOMALY)
- M Communication with blacklisted hosts (BLACKLIST)
- M Port scanning (SCANS)
- M ICMP anomaly (ICMPANOM)
- M High volume of transferred data (HIGHTRANSF)
- M New or alien device (ALIENDEV)
- M L3 network anomaly (L3ANOMALY)

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

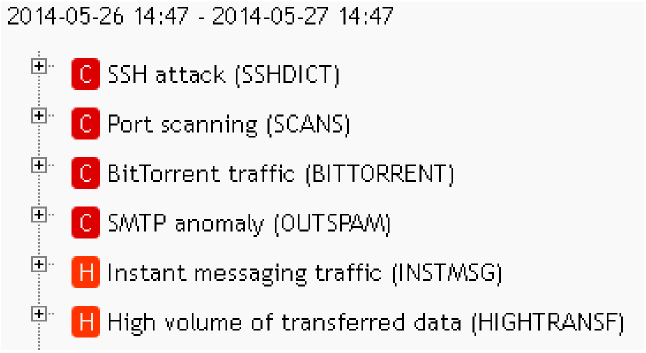
User Defined Anomaly Detection Methods

- 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

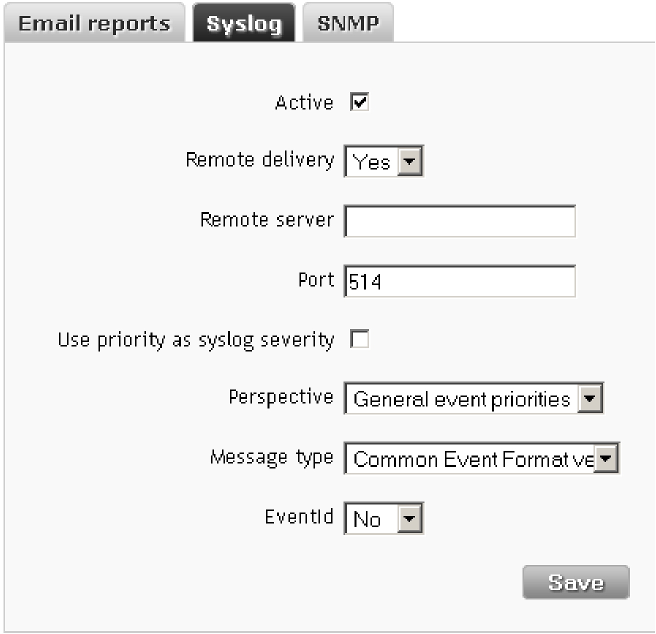
ADS Alerting and Integration

- 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

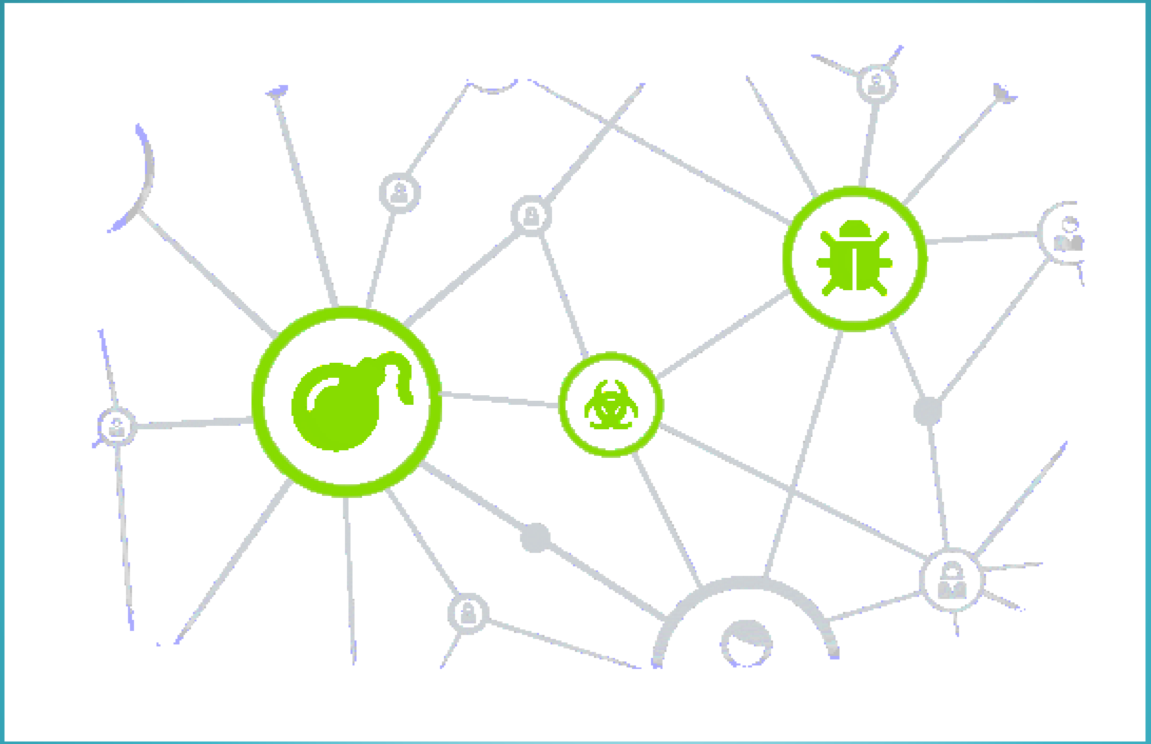


2014-05-26 14:47 - 2014-05-27 14:47

- ⊞ C SSH attack (SSHDICT)
- ⊞ C Port scanning (SCANS)
- ⊞ C BitTorrent traffic (BITTORRENT)
- ⊞ C SMTP anomaly (OUTSPAM)
- ⊞ H Instant messaging traffic (INSTMSG)
- ⊞ H High volume of transferred data (HIGHTRANSF)



Active	☑
Remote delivery	Yes ▾
Remote server	
Port	514
Use priority as syslog severity	□
Perspective	General event priorities ▾
Message type	Common Event Format ve ▾
EventId	No ▾



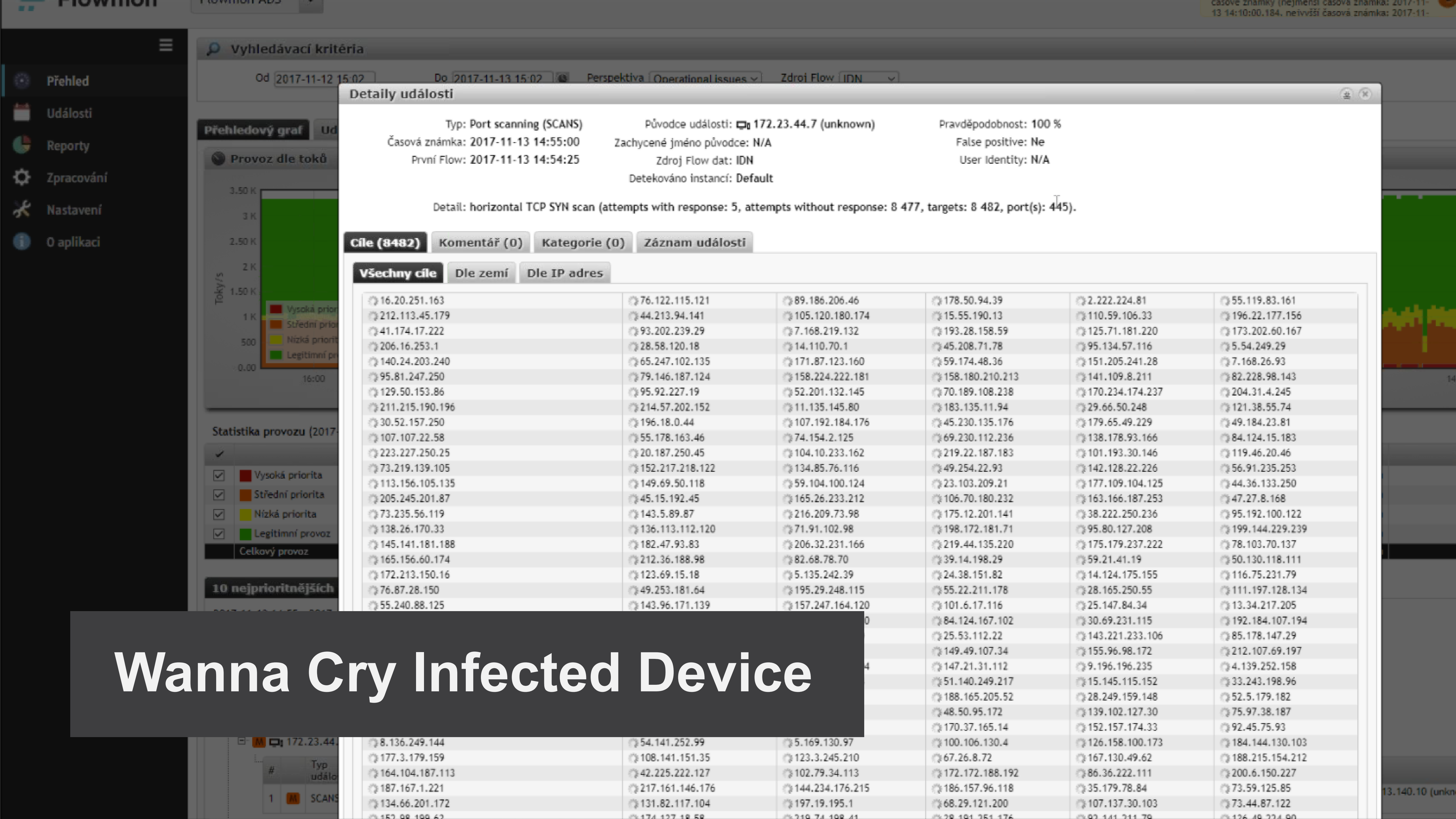
Use Case: Anomaly Detection in Enterprise

Selected Detections from our Customers

Recent Interesting Detections?

- 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



Vyhledávací kritéria

Od 2017-11-12 15:02 Do 2017-11-13 15:02 Perspektiva Operational issues Zdroj Flow IDN

Statistika provozu (2017-

☑ Vysoká priorita
☑ Střední priorita
☑ Nízká priorita
☑ Legitimní provoz

Detaily události

Typ: Port scanning (SCANS)
Časová známka: 2017-11-13 14:55:00
První Flow: 2017-11-13 14:54:25

Původce události: 172.23.44.7 (unknown)
Zachycené jméno původce: N/A
Zdroj Flow dat: IDN
Detekováno instancí: Default

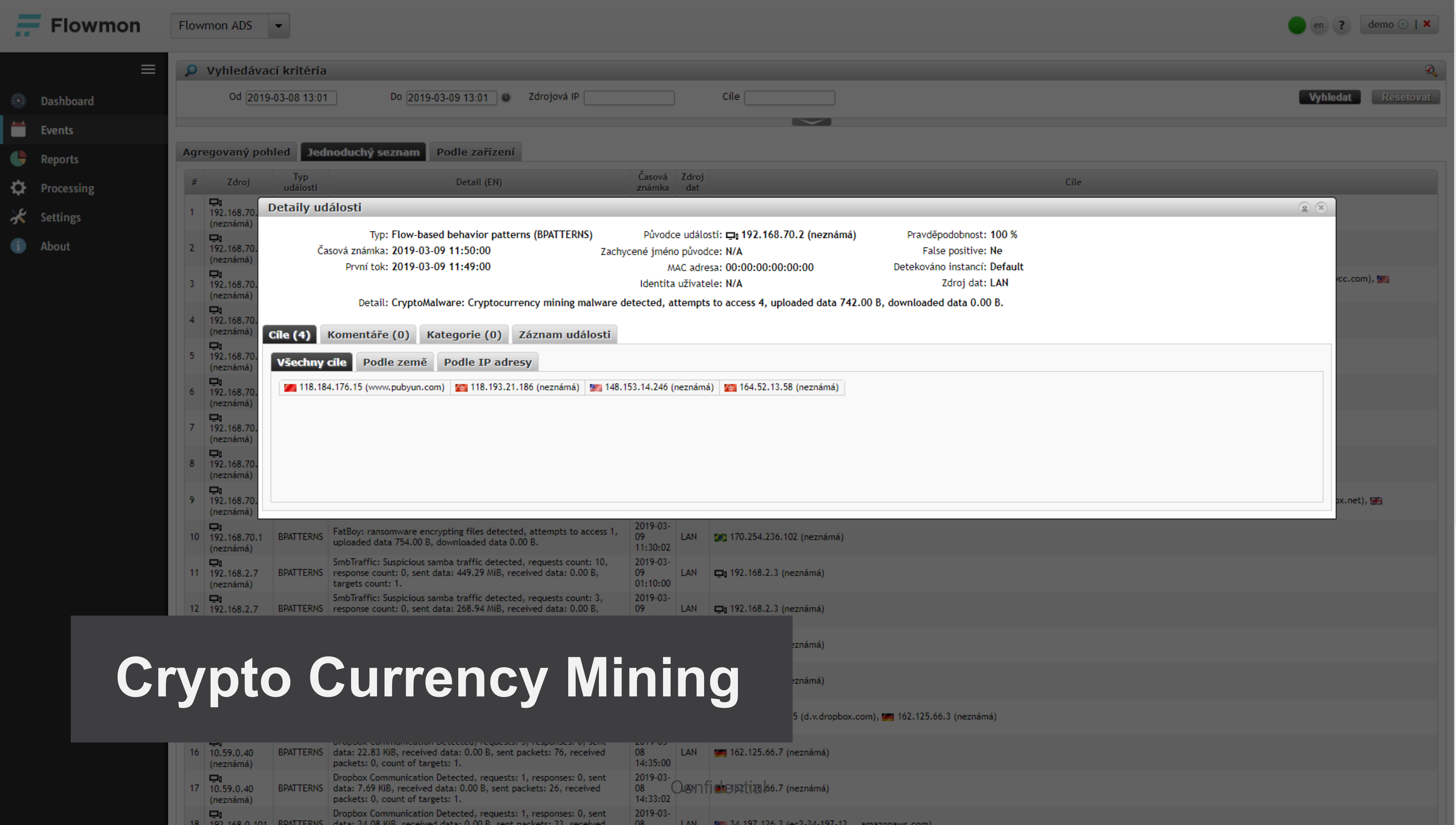
Pravděpodobnost: 100 %
False positive: Ne
User Identity: N/A

Detail: horizontal TCP SYN scan (attempts with response: 5, attempts without response: 8 477, targets: 8 482, port(s): 445).

Cíle (8482) | Komentář (0) | Kategorie (0) | Záznam události

Všechny cíle | Dle zemí | Dle IP adres

16.20.251.163	76.122.115.121	89.186.206.46	178.50.94.39	2.222.224.81	55.119.83.161
212.113.45.179	44.213.94.141	105.120.180.174	15.55.190.13	110.59.106.33	196.22.177.156
41.174.17.222	93.202.239.29	7.168.219.132	193.28.158.59	125.71.181.220	173.202.60.167
206.16.253.1	28.58.120.18	14.110.70.1	45.208.71.78	95.134.57.116	5.54.249.29
140.24.203.240	65.247.102.135	171.87.123.160	59.174.48.36	151.205.241.28	7.168.26.93
95.81.247.250	79.146.187.124	158.224.222.181	158.180.210.213	141.109.8.211	82.228.98.143
129.50.153.86	95.92.227.19	52.201.132.145	70.189.108.238	170.234.174.237	204.31.4.245
211.215.190.196	214.57.202.152	11.135.145.80	183.135.11.94	29.66.50.248	121.38.55.74
30.52.157.250	196.18.0.44	107.192.184.176	45.230.135.176	179.65.49.229	49.184.23.81
107.107.22.58	55.178.163.46	74.154.2.125	69.230.112.236	138.178.93.166	84.124.15.183
223.227.250.25	20.187.250.45	104.10.233.162	219.22.187.183	101.193.30.146	119.46.20.46
73.219.139.105	152.217.218.122	134.85.76.116	49.254.22.93	142.128.22.226	56.91.235.253
113.156.105.135	149.69.50.118	59.104.100.124	23.103.209.21	177.109.104.125	44.36.133.250
205.245.201.87	45.15.192.45	165.26.233.212	106.70.180.232	163.166.187.253	47.27.8.168
73.235.56.119	143.5.89.87	216.209.73.98	175.12.201.141	38.222.250.236	95.192.100.122
138.26.170.33	136.113.112.120	71.91.102.98	198.172.181.71	95.80.127.208	199.144.229.239
145.141.181.188	182.47.93.83	206.32.231.166	219.44.135.220	175.179.237.222	78.103.70.137
165.156.60.174	212.36.188.98	82.68.78.70	39.14.198.29	59.21.41.19	50.130.118.111
172.213.150.16	123.69.15.18	5.135.242.39	24.38.151.82	14.124.175.155	116.75.231.79
76.87.28.150	49.253.181.64	195.29.248.115	55.22.211.178	28.165.250.55	111.197.128.134
55.240.88.125	143.96.171.139	157.247.164.120	101.6.17.116	25.147.84.34	13.34.217.205
[illegible]	[illegible]	[illegible]	84.124.167.102	30.69.231.115	192.184.107.194
[illegible]	[illegible]	[illegible]	25.53.112.22	143.221.233.106	85.178.147.29
[illegible]	[illegible]	[illegible]	149.49.107.34	155.96.98.172	212.107.69.197
[illegible]	[illegible]	[illegible]	147.21.31.112	9.196.196.235	4.139.252.158
[illegible]	[illegible]	[illegible]	51.140.249.217	15.145.115.152	33.243.198.96
[illegible]	[illegible]	[illegible]	188.165.205.52	28.249.159.148	52.5.179.182
[illegible]	[illegible]	[illegible]	48.50.95.172	139.102.127.30	75.97.38.187
[illegible]	[illegible]	[illegible]	170.37.165.14	152.157.174.33	92.45.75.93
8.136.249.144	54.141.252.99	5.169.130.97	100.106.130.4	126.158.100.173	184.144.130.103
177.3.179.159	108.141.151.35	123.3.245.210	67.26.8.72	167.130.49.62	188.215.154.212
164.104.187.113	42.225.222.127	102.79.34.113	172.172.188.192	86.36.222.111	200.6.150.227
187.167.1.221	217.161.146.176	144.234.176.215	186.157.96.118	35.179.78.84	73.59.125.85
134.66.201.172	131.82.117.104	197.19.195.1	68.29.121.200	107.137.30.103	73.44.87.122
152.98.199.62	174.127.18.58	219.74.198.41	28.191.251.176	92.141.211.79	126.49.224.90



Od 2019-03-08 13:01 Do 2019-03-09 13:01 Zdrojová IP Cíle

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

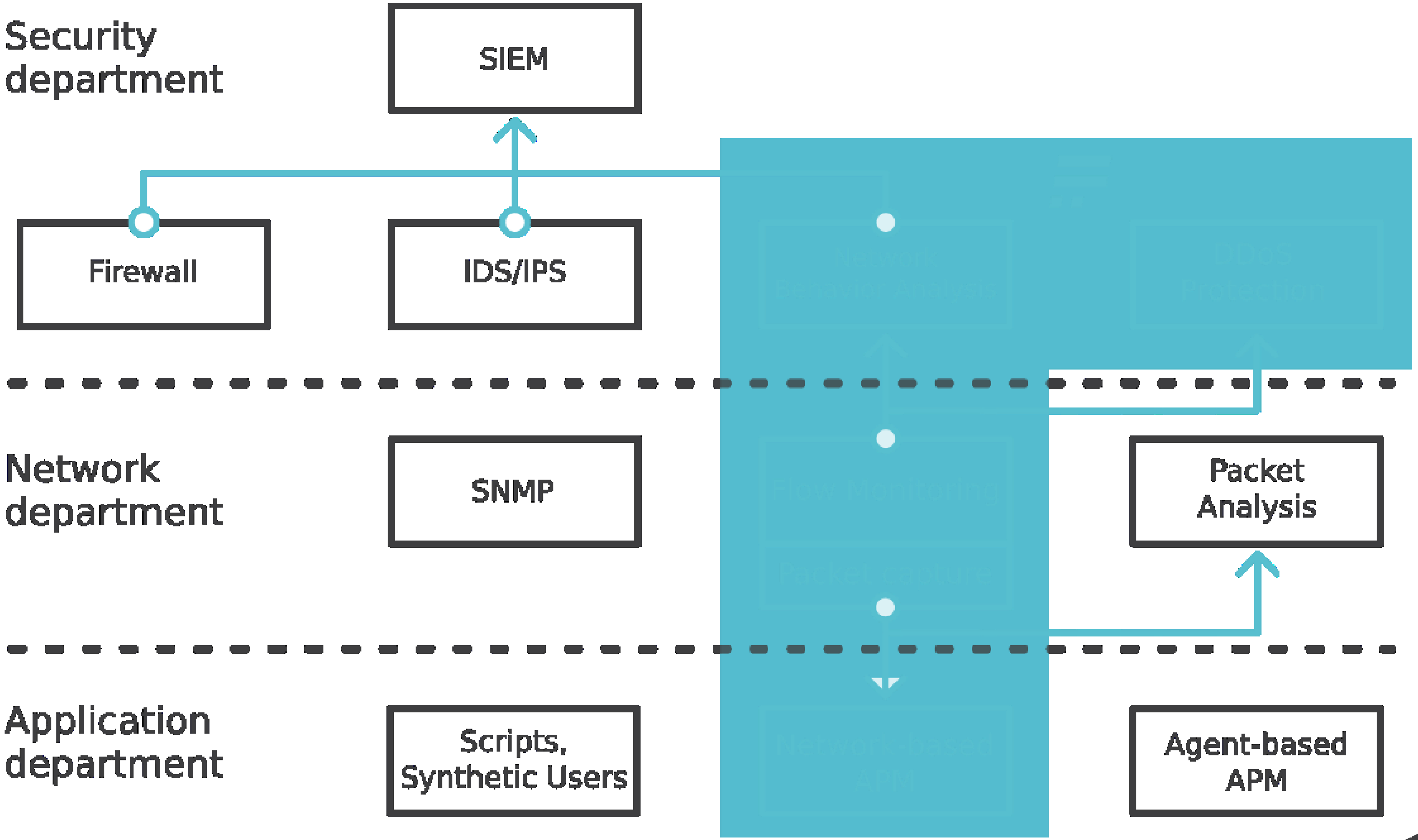
Detail: CryptoMalware: Cryptocurrency mining malware detected, attempts to access 4, uploaded data 742.00 B, downloaded data 0.00 B.

118.184.176.15 (www.pubyun.com) | 118.193.21.186 (neznámá) | 148.153.14.246 (neznámá) | 164.52.13.58 (neznámá)

#	Zdroj	Typ události	Detail (EN)	Časová známka	Zdroj dat	Cíle
1	192.168.70. (neznámá)					
2	192.168.70. (neznámá)					
3	192.168.70. (neznámá)					cc.com),
4	192.168.70. (neznámá)					
5	192.168.70. (neznámá)					
6	192.168.70. (neznámá)					
7	192.168.70. (neznámá)					
8	192.168.70. (neznámá)					
9	192.168.70. (neznámá)					x.net),
10	192.168.70.1 (neznámá)	BPATTERNS	FatBoy: ransomware encrypting files detected, attempts to access 1, uploaded data 754.00 B, downloaded data 0.00 B.	2019-03-09 11:30:02	LAN	170.254.236.102 (neznámá)
11	192.168.2.7 (neznámá)	BPATTERNS	SmbTraffic: Suspicious samba traffic detected, requests count: 10, response count: 0, sent data: 449.29 MiB, received data: 0.00 B, targets count: 1.	2019-03-09 01:10:00	LAN	192.168.2.3 (neznámá)
12	192.168.2.7	BPATTERNS	SmbTraffic: Suspicious samba traffic detected, requests count: 3, response count: 0, sent data: 268.94 MiB, received data: 0.00 B,	2019-03-09	LAN	192.168.2.3 (neznámá)
						eznámá)
						eznámá)
						5 (d.v.dropbox.com), 162.125.66.3 (neznámá)
16	10.59.0.40 (neznámá)	BPATTERNS	data: 22.83 KiB, received data: 0.00 B, sent packets: 76, received packets: 0, count of targets: 1.	08 14:35:00	LAN	162.125.66.7 (neznámá)
17	10.59.0.40 (neznámá)	BPATTERNS	Dropbox Communication Detected, requests: 1, responses: 0, sent data: 7.69 KiB, received data: 0.00 B, sent packets: 26, received packets: 0, count of targets: 1.	2019-03-08 14:33:02	LAN	162.125.66.7 (neznámá)
18	192.168.0.101	BPATTERNS	Dropbox Communication Detected, requests: 1, responses: 0, sent data: 24.08 KiB, received data: 0.00 B, sent packets: 33, received	2019-03-08	LAN	34.197.126.3 (ec2-34-197-12... amazonaws.com)

Crypto Currency Mining

Flowmon Fit with other Tools

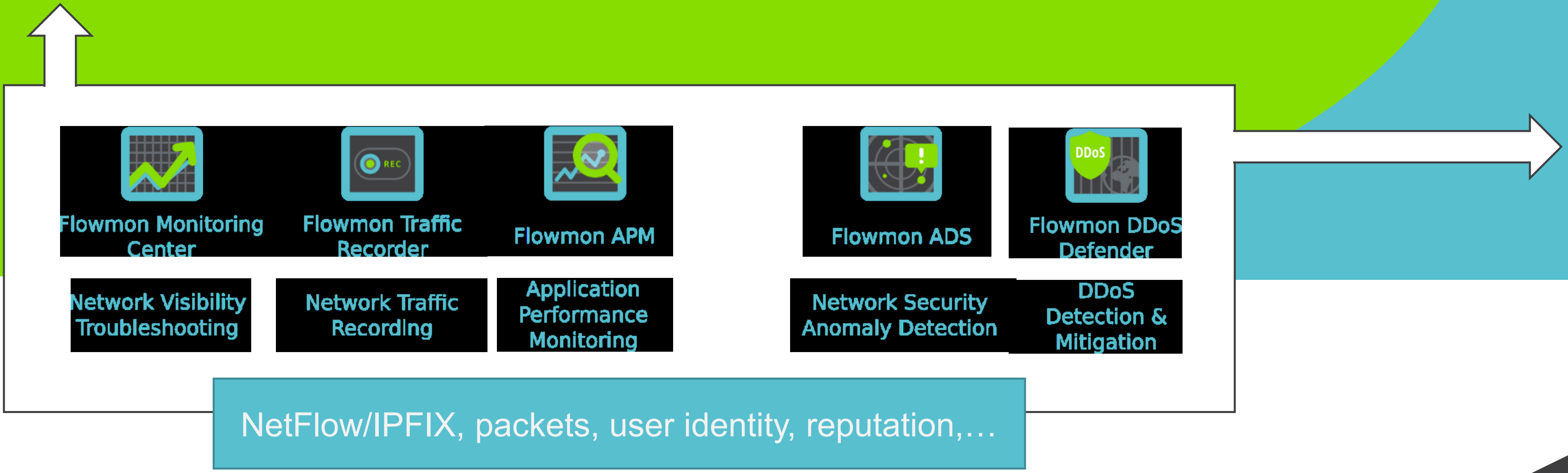


NetOps

NetSecOps shared use cases

- Infrastructure design & deployment
- Event/incident monitoring and investigation
- Incident response
- Change management/patch management
- Policy verification/enforcement

SecOps



Flowmon Monitoring Center

Flowmon Traffic Recorder

Flowmon APM

Flowmon ADS

Flowmon DDoS Defender

Network Visibility Troubleshooting

Network Traffic Recording

Application Performance Monitoring

Network Security Anomaly Detection

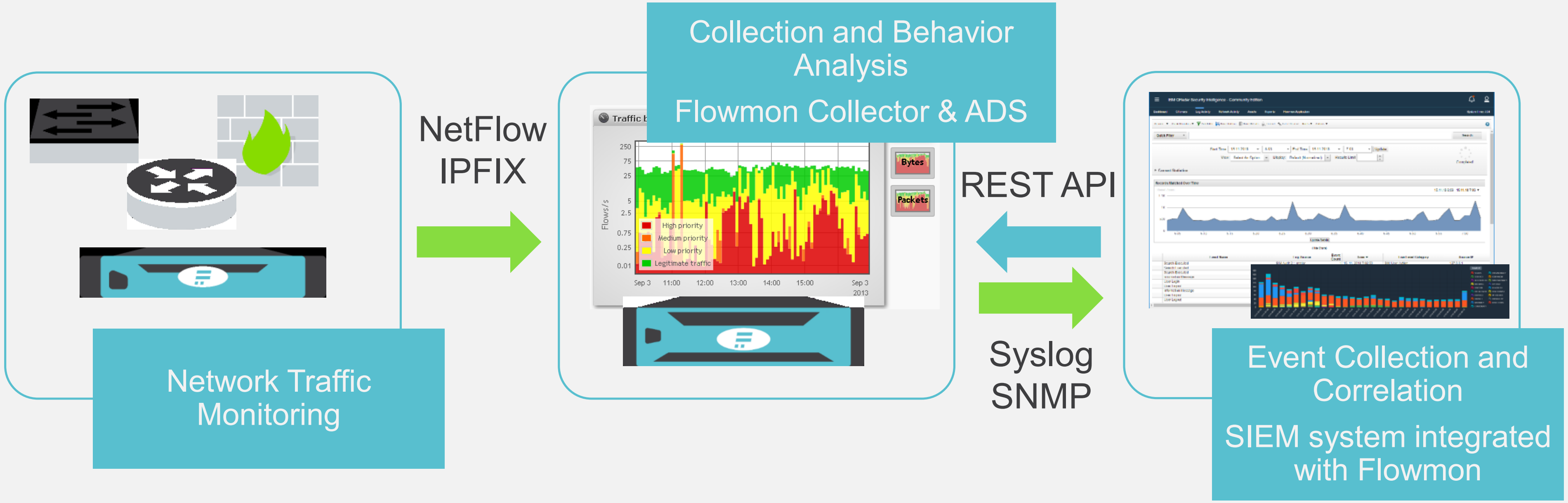
DDoS Detection & Mitigation

NetFlow/IPFIX, packets, user identity, reputation,…

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.



Network Traffic Monitoring

NetFlow
IPFIX

Collection and Behavior Analysis

Flowmon Collector & ADS

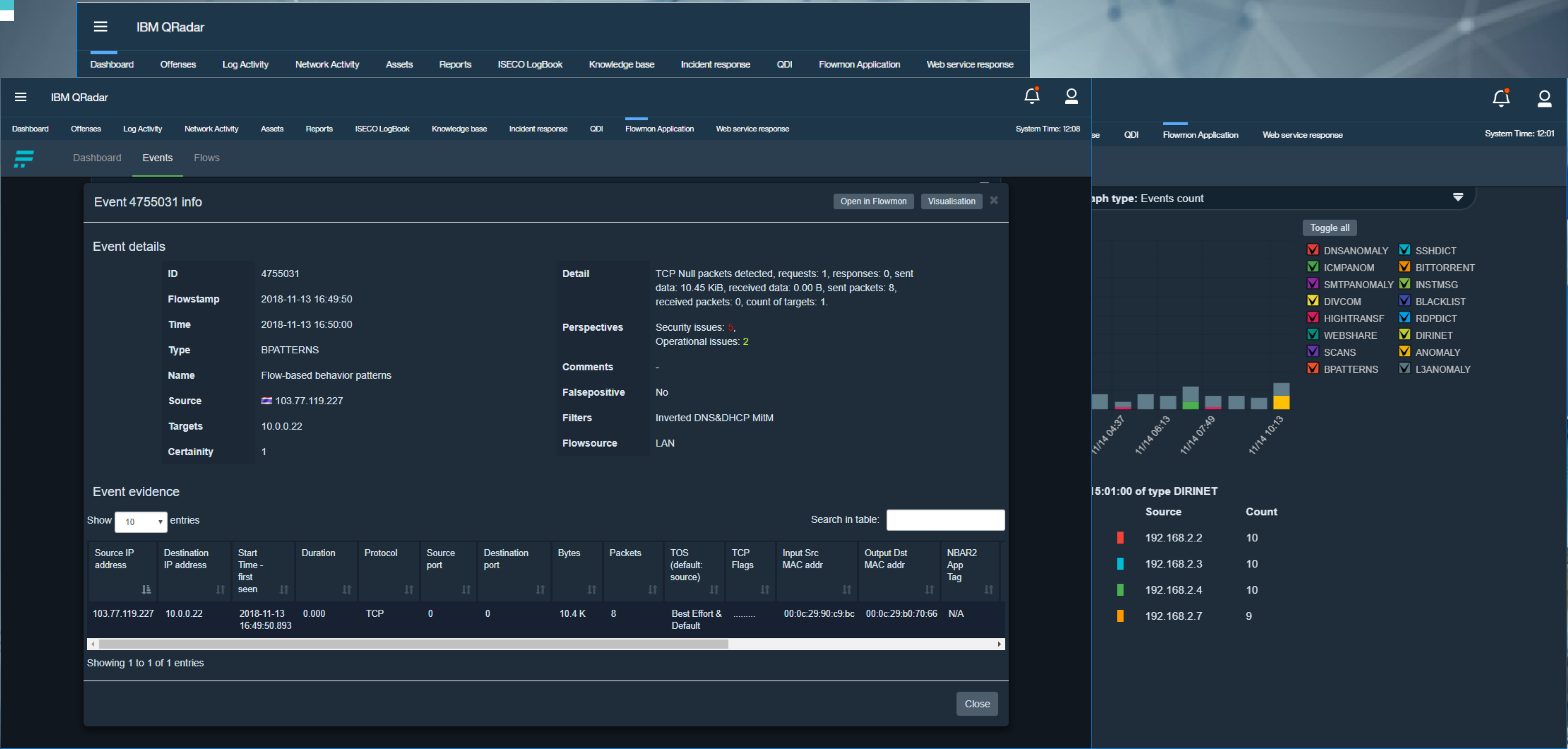
REST API

Syslog
SNMP

Event Collection and Correlation

SIEM system integrated with Flowmon

Sample Flowmon to IBM QRadar Integration



Event 4755031 info

Event details

ID	4755031
Flowstamp	2018-11-13 16:49:50
Time	2018-11-13 16:50:00
Type	BPATTERNS
Name	Flow-based behavior patterns
Source	103.77.119.227
Targets	10.0.0.22
Certainity	1

Detail	TCP Null packets detected, requests: 1, responses: 0, sent data: 10.45 KiB, received data: 0.00 B, sent packets: 8, received packets: 0, count of targets: 1.
Perspectives	Security issues: 5, Operational issues: 2
Comments	-
Falsepositive	No
Filters	Inverted DNS&DHCP MitM
Flowsource	LAN

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	Input Src MAC addr	Output Dst MAC addr	NBAR2 App Tag
103.77.119.227	10.0.0.22	2018-11-13 16:49:50.893	0.000	TCP	0	0	10.4 K	8	Best Effort & Default	....	00:0c:29:90:c9:bc	00:0c:29:b0:70:66	N/A

Showing 1 to 1 of 1 entries

aph type: Events count

☑ DNSANOMALY	☑ SSHDICT
☑ ICMPANOM	☑ BITTORRENT
☑ SMTPANOMALY	☑ INSTMSG
☑ DIVCOM	☑ BLACKLIST
☑ HIGHTRANSF	☑ RDPDICT
☑ WEBSHARE	☑ DIRINET
☑ SCANS	☑ ANOMALY
☑ BPATTERNS	☑ L3ANOMALY

5:01:00 of type DIRINET

	Source	Count
🟥	192.168.2.2	10
🟦	192.168.2.3	10
🟩	192.168.2.4	10
🟧	192.168.2.7	9

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

Packet Analysis

Premium price, resources required, racks space and complexity of operations are major blockers for adoption.

Packet analysis tools lack to scale with bandwidth grow in corporate networks and adoption of encryption.

To heavy for daily use and majority of use cases.

Flowmon

Easy to use network visibility, performance monitoring and troubleshooting beyond the scope and scale of traditional infrastructure monitoring tools.

Provides in-context and in-depth understanding of both normal traffic and network anomalies in terms of incident magnitude, impact and root cause.

SNMP Monitoring

Basic IT infrastructure monitoring to provide network, device and service status. Does not help to troubleshoot, track user experience or contribute to network security.

Infrastructure monitoring tools complement Flowmon.

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
[redacted]	SIEMENS	SLOVENSKÁ sporiteľňa
Volkswagen	orange	Telefónica
Allianz	hp	T · · Mobile ·
GÉANT Networks · Services · People	KIA	upc
Raiffeisen BANK	e·on	

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