



# Role of Flow Monitoring in Cyber Security

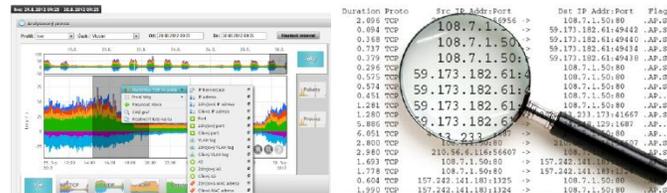
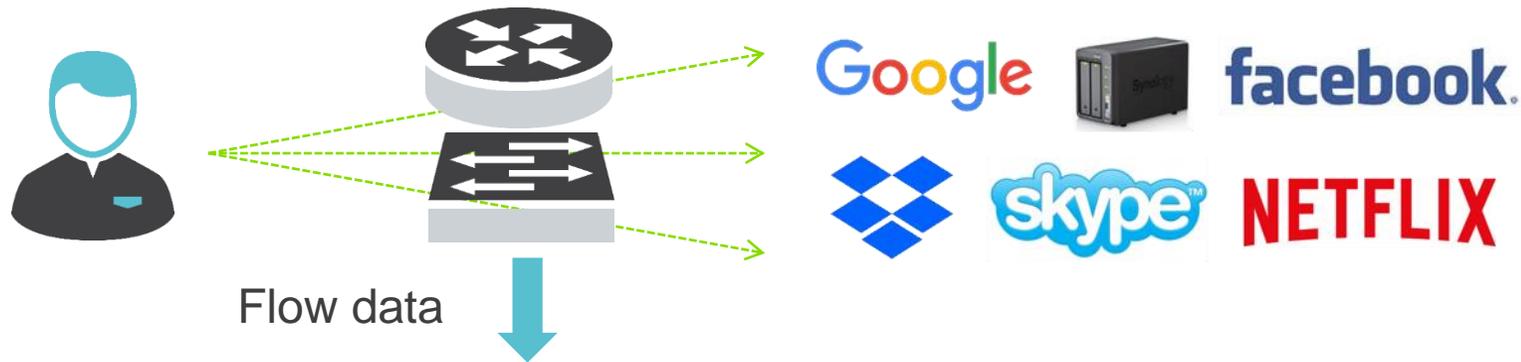
Pavel Minařík, Chief Technology Officer



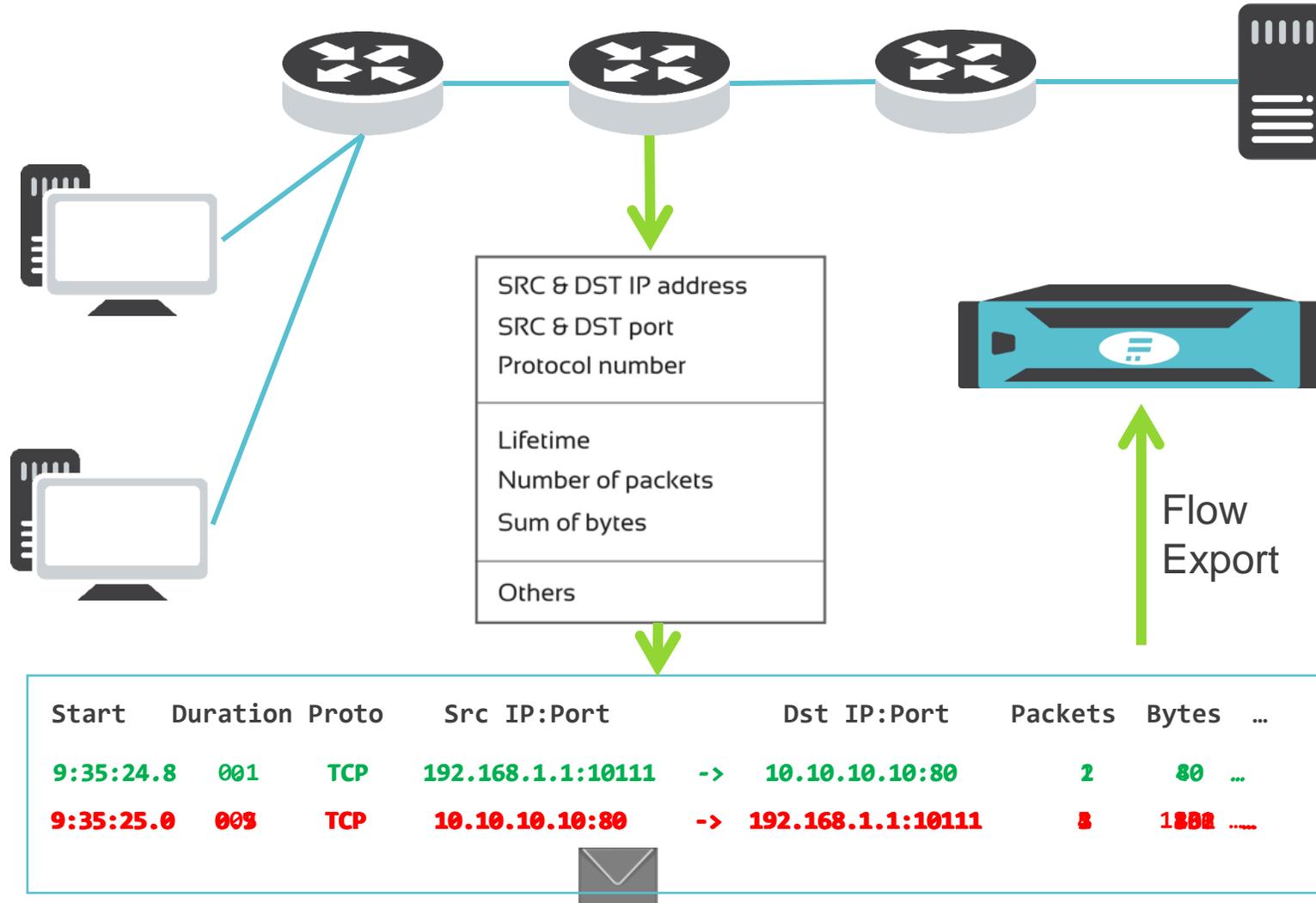
**Flowmon**  
Driving Network Visibility

# 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



# Flow Monitoring Principle



A person in a dark suit and tie is pointing their right index finger at a glowing, stylized cloud icon. The cloud is connected to a network of nodes, represented by glowing circles with lines connecting them. The background is a blurred image of the person's suit and tie. The overall color scheme is blue and white, with a dark grey diagonal bar at the bottom right.

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.”

Strong aspects		Weak aspects		
Packet Analysis	<ul style="list-style-type: none"> <li>+ Full network traffic</li> <li>+ Enough details for troubleshooting</li> <li>+ Supports forensic analysis</li> <li>+ Signature based detection</li> </ul>	<ul style="list-style-type: none"> <li>- Useless for encrypted traffic</li> <li>- Usually too much details</li> <li>- Very resource consuming</li> </ul>		
	<table border="1"> <tr> <td>1 min 75 GB</td> <td>1 hour 4.5 TB</td> <td>1 day 108 TB</td> </tr> </table>	1 min 75 GB	1 hour 4.5 TB	1 day 108 TB
1 min 75 GB	1 hour 4.5 TB	1 day 108 TB		
Flow Data	<ul style="list-style-type: none"> <li>+ Works in high-speed networks</li> <li>+ Resistant to encrypted traffic</li> <li>+ Visibility and reporting</li> <li>+ Network behavior analysis</li> </ul>	<ul style="list-style-type: none"> <li>- No application layer data</li> <li>- Sometimes not enough details</li> <li>- Sampling (routers, switches)</li> </ul>		
	<table border="1"> <tr> <td>1 min 150 MB</td> <td>1 hour 9 GB</td> <td>1 day 216 GB</td> </tr> </table>	1 min 150 MB	1 hour 9 GB	1 day 216 GB
1 min 150 MB	1 hour 9 GB	1 day 216 GB		

## Flow vs. Packet Analysis on 10G

# 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	
<ul style="list-style-type: none"><li>• MAC</li><li>• VLAN</li><li>• MPLS</li><li>• GRE</li><li>• ESP</li><li>• OTV</li></ul>	<ul style="list-style-type: none"><li>• Standard items</li><li>• NPM metrics<ul style="list-style-type: none"><li>• RTT, SRT, ...</li></ul></li><li>• TTL, SYN size, ...</li><li>• ASN (BGP)</li><li>• Geolocation</li><li>• VxLAN</li></ul>	<ul style="list-style-type: none"><li>• NBAR2</li><li>• HTTP</li><li>• SNI</li><li>• DNS</li><li>• DHCP</li><li>• IEC104</li></ul>	<ul style="list-style-type: none"><li>• SMB/CIFS</li><li>• VoIP (SIP)</li><li>• Email</li><li>• SQL</li><li>• SSL/TLS</li><li>• CoAP</li></ul>



# Use Case: Retrospective Investigation

## Traditional flow data compared to Flowmon L7 visibility

Application TAG	Flows	Input Packets	Input Bytes							
http	11.96 K (6.2%)	638.27 K (23.8%)	539.96 MB (40.7%)		http	...AP.SF	Best Effort & Default	1 s, 116.461 ms	65.766 ms	1.282
mysql	6.04 K (3.1%)	864.16 K (32.2%)	405.91 MB (30.6%)							
secure-http	2.52 K (1.3%)	131.58 K (4.9%)	102.96 MB (7.8%)							
cifs	6.16 K (3.2%)	470.11 K (17.5%)	85.06 MB (6.4%)		39742	...AP.SF	Best Effort & Default	1 s, 116.461 ms	223.604 ms	3.691
dns	60.53 K (31.5%)	159.44 K (5.9%)	83.38 MB (6.3%)							
pop3	534 (0.3%)	54.43 K (2.0%)	46.41 MB (3.5%)							
snmp	79.48 K (41.3%)	198.01 K (7.4%)	33.19 MB (2.5%)							
secure-imap	300 (0.2%)	12.16 K (0.5%)	7.15 MB (0.5%)							
syslog	1 (0.0%)	1 (0.0%)	1 (0.0%)							
icmp	1 (0.0%)	1 (0.0%)	1 (0.0%)							
other	18.38 K (9.6%)	68.05 K (2.5%)	11.39 MB (0.9%)		39752	...AP.SF	Best Effort & Default	714.436 ms	204.453 ms	7.285
Hostname	URL	Destination port	HTTP method	HTTP result code						
pxl.jivox.com					http	...AP.SF	Best Effort & Default	12 s, 45.473 ms	1 s, 47.544 ms	1.289
cz.search.etaargetnet.com	/a/?ref=1&cpp=1339817%2C1339829	http	GET	200						
static-tag.rgd1.mookie1.com	/s1/sas/le1/tagr_lib.min.js?np.subdomain=cz-gmtdmp&tagid=V2_126	http	GET	200						
ib.adnxs.com	/mapuid?member=364&user=11435343141365603708&redir=https%3A%2F%	http	GET	302	39754	...AP.SF	Best Effort & Default	45.473 ms	2 s, 677.057 ms	6.727
cpex.demdex.net	/event?d_nsid=0&d_ld=_ts%3D1498718439247&d_rtbd=json&d_jsonv=1&	http	GET	200						
adx.adform.net	/adx/?rp=4&bWIKPTI3MDE2Mw%3D%3D&mkw=idos%2Cbrno%2Cvyhled%C3%A1n%C3%	http	GET	200	http	...AP.SF	Best Effort & Default	11 s, 204.179 ms	589.800 ms	
ads.rubiconproject.com	/ad/10900.js	http	GET	200						
1gr.cz	/js/uni/uni.js?rr=23	http	GET	200						
green.erne.co	/stroer/cm?uid=418941481546250377&tpid=84&cburl=http%3A%2F%2Fih	http	GET	302						
1gr.cz	/data/aam/jizdni-rady.js	http	GET	304	39756	...AP.SF	Best Effort			

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

```
C:\WINDOWS\system32\cmd.exe - nslookup
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. Všechna práva vyhrazena.

C:\Users\minarik>nslookup
Default Server:  UnKnown
Address:  192.168.10.1

> 212.111.2.170
Server:  UnKnown
Address:  192.168.10.1

Name:    virt-z001.inext.cz
Address:  212.111.2.170

>
```

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

```
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
```

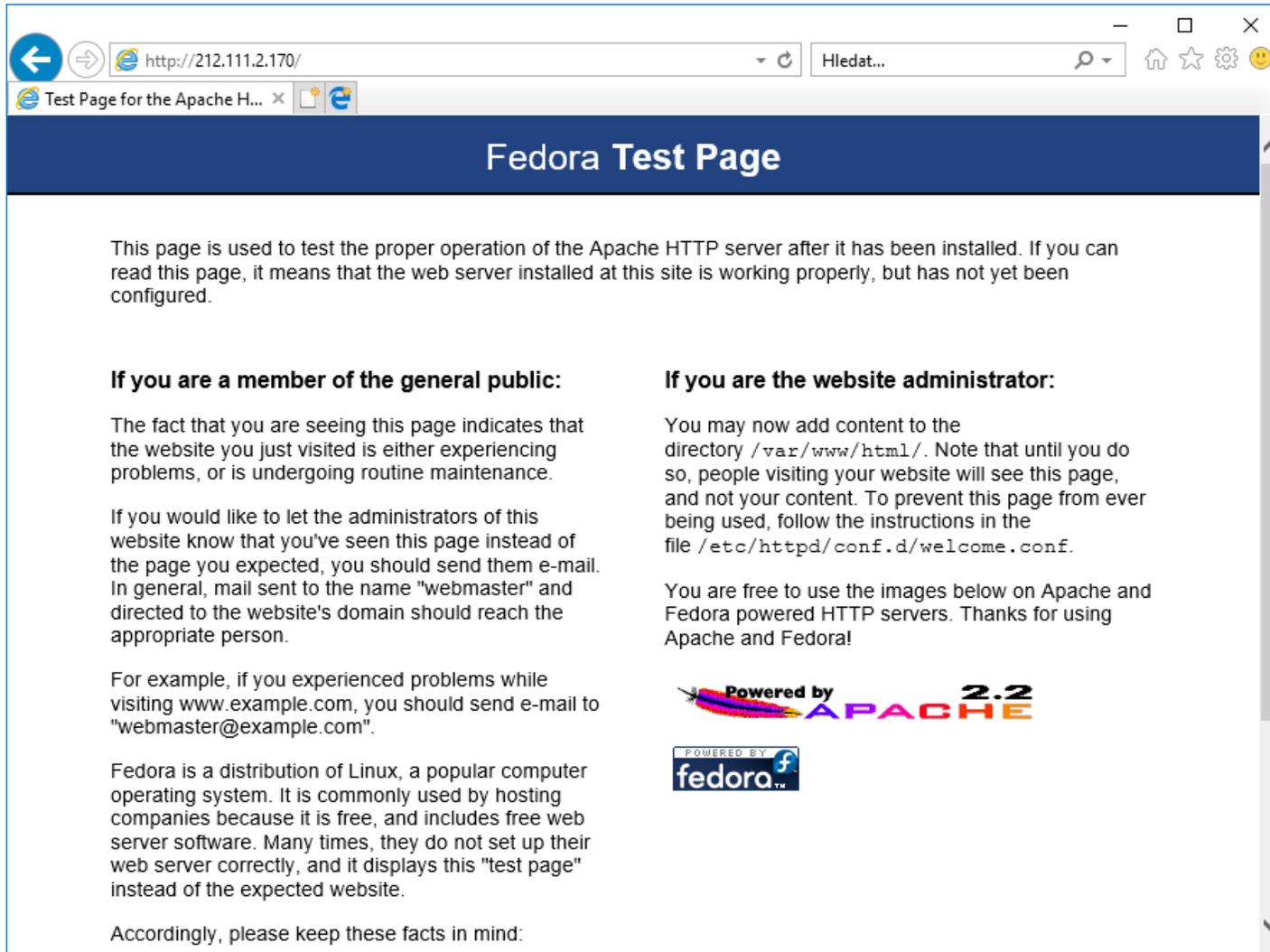
- General whois information related to IP address
- IP belongs to local ISP in Czech

## Reverse IP lookup for: 212.111.2.170

Found 3 domains hosted on IP address 212.111.2.170.

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

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



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

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)

# 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=1463	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=1463	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=1463	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=1463	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=1463	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=1463	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

Client IP: 192.168.70.35  
 Server IP: 212.11.2.170  
 HTTP hostname: [www.rockmax.cz](http://www.rockmax.cz)  
 URL: /stream\_live/get\_songs\_...  
 Client OS: Windows 10  
 Browser: Chrome 60.0

Flows 1.15 K Bytes 755.8 K Packets 5.7 K

# Flow From the Probe (L2-L7)



# Use Case: Encrypted Traffic Analysis

## Understand Encrypted Traffic While Preserving User Privacy

# 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

IP Header

TCP Header

TLS Header

TLS Record

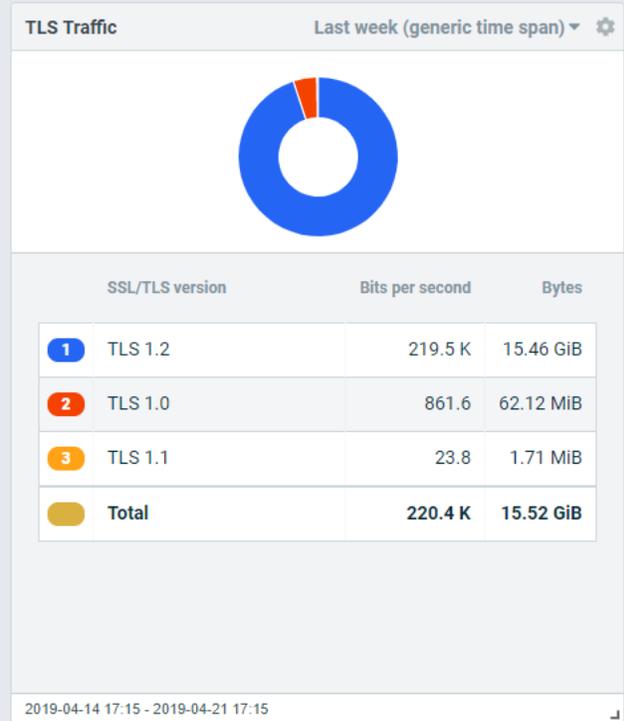
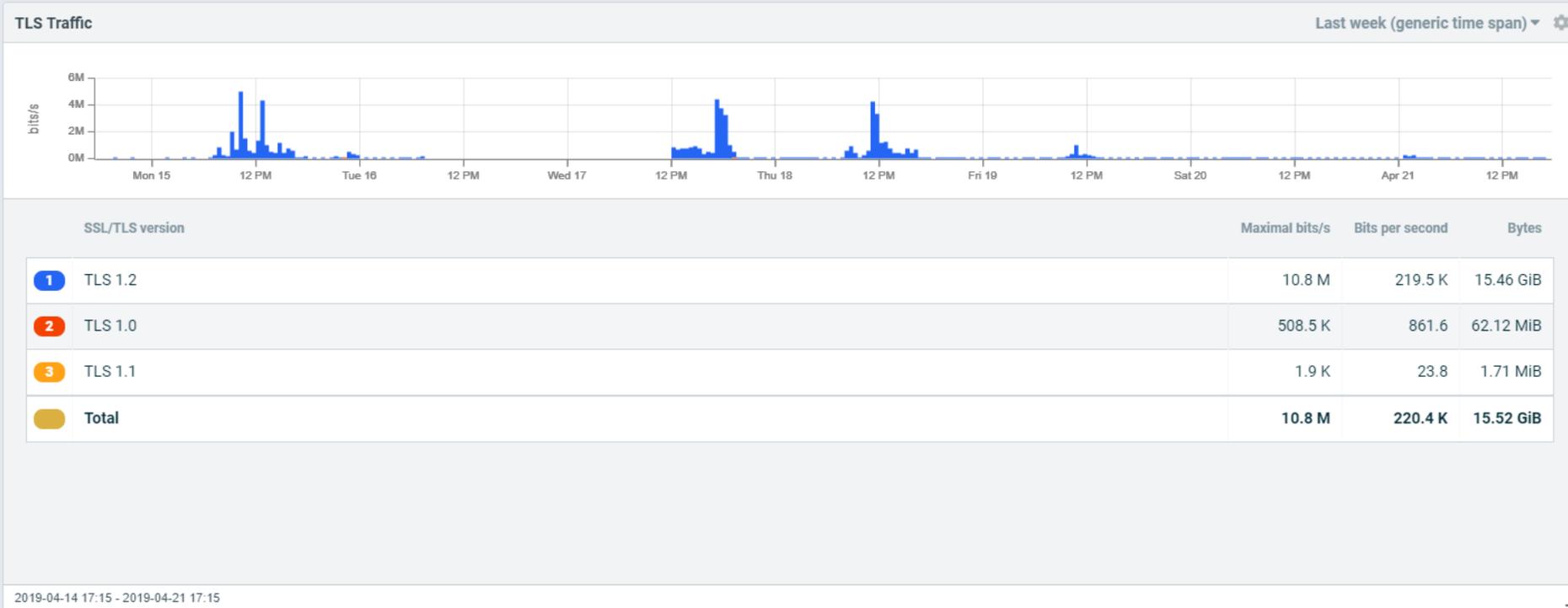
TLS server version  
TLS cipher suite  
TLS server name indication  
TLS client version  
TLS certificate issuer  
common name  
TLS subject common name  
TLS public key algorithm  
TLS certificate validity until  
TLS JA3 fingerprint  
and many others



**Enriched Flow**



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



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**.

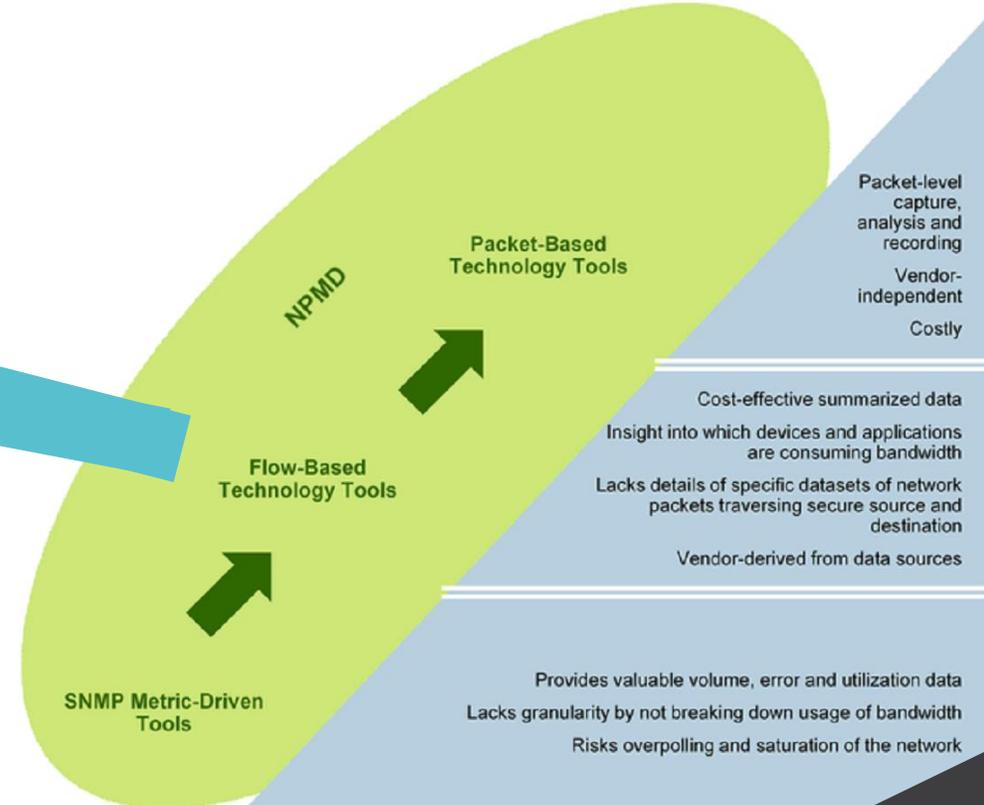
Flowmon combines best of breed: flow data enriched with L7 and performance metrics. This helps to **solve 95% of all troubleshooting cases**. In addition, Flowmon provides on-demand packet capture when flow visibility is not enough.

# Using Flow Data For Security

Gartner

Volumetric  
DDoS detection

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



#	Zdrojová IP	Typ události	Detail	Čas	Zdroj	Net/low 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, 1.52.11.199, 1.52.42.167, 1.52.59.101, 1.52.71.217, 1.52.87.249, 1.52.133.224, 1.52.1.52.192.113, 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: 58 279.	2013-08-24 07:15:21	localhost	1.52.54.212, 1.52.109.106, 1.52.167.73, 1.52.1.52.191.229, 1.52.218.125, 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, 1.52.92.1.52.174.104, 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: 5.04 MiB, packets: 125 924.	2013-08-24 07:15:21	localhost	1.52.28.245, 1.52.44.63, 1.52.112.109, 1.52.1.52.177.97, 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: 3.40 MiB, packets: 88 749.	2013-08-24 03:38:31	localhost	1.52.4.138, 1.52.12.103, 1.52.28.61, 1.52.31.71, 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: 2.40 MiB, packets: 63 126.	2013-08-24 03:00:24	localhost	1.52.7.220, 1.52.11.109, 1.52.28.57, 1.52.42.99, 1.52.95.134, 1.52.114.14, 1.52.115.205, 1.52.1.52.122.10, ...	
8	112.90.18.105	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.40 MiB, packets: 63 126.	2013-08-24 03:00:24	localhost	1.52.12.16, 1.52.77.184, 1.52.104.14, 1.52.128.99, 1.52.134.215, 1.52.137.109, 1.52.1.52.203.143, 1.52.209.197, ...	

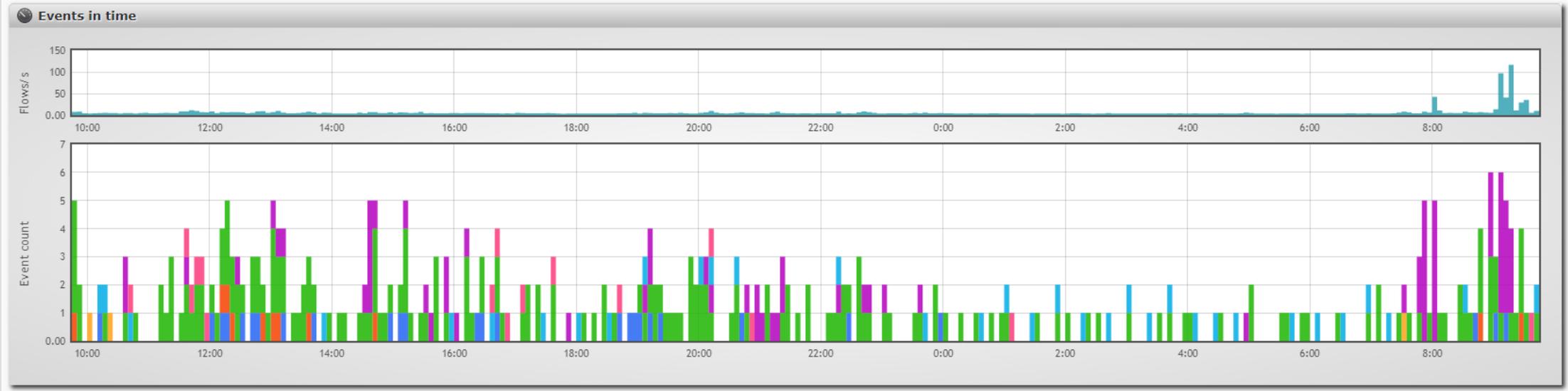
- Dashboard
- Events
- Reports
- Processing
- Settings
- About

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 by priority and count (360)

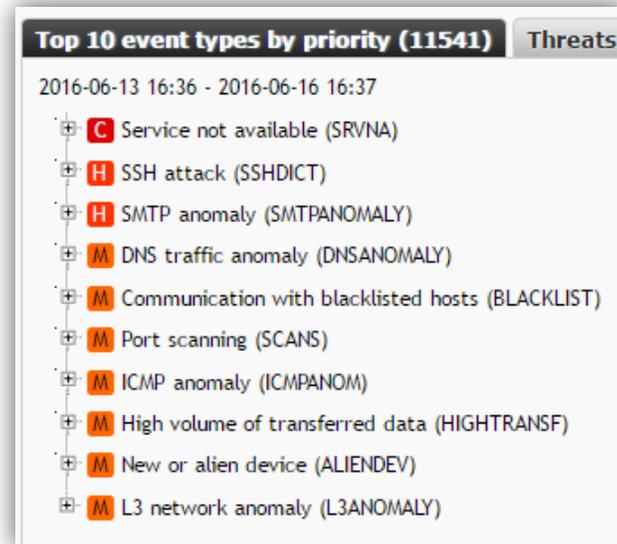
Priorities:  Critical  High  Medium  Low  Information (All / None) 2019-02-02 09:45 - 2019-02-03 09:45

<input checked="" type="checkbox"/> M	1	DNS traffic anomaly (DNSANOMALY)	27 (number of events)
<input checked="" type="checkbox"/> M	2	High volume of transferred data (HIGHTRANSF)	11 (number of events)
<input checked="" type="checkbox"/> M	3	ICMP anomaly (ICMPANOM)	3 (number of events)
<input checked="" type="checkbox"/> L	4	Country reputation (COUNTRY)	201 (number of events)
<input checked="" type="checkbox"/> L	5	Behavior anomaly (ANOMALY)	68 (number of events)
<input checked="" type="checkbox"/> L	6	DNS query volume anomaly (DNSQUERY)	34 (number of events)
<input checked="" type="checkbox"/>			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



# 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



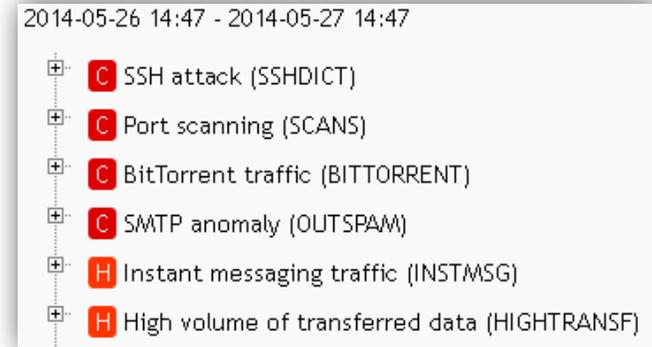
Specific OS detection

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



Email reports **Syslog** SNMP

Active

Remote delivery

Remote server

Port

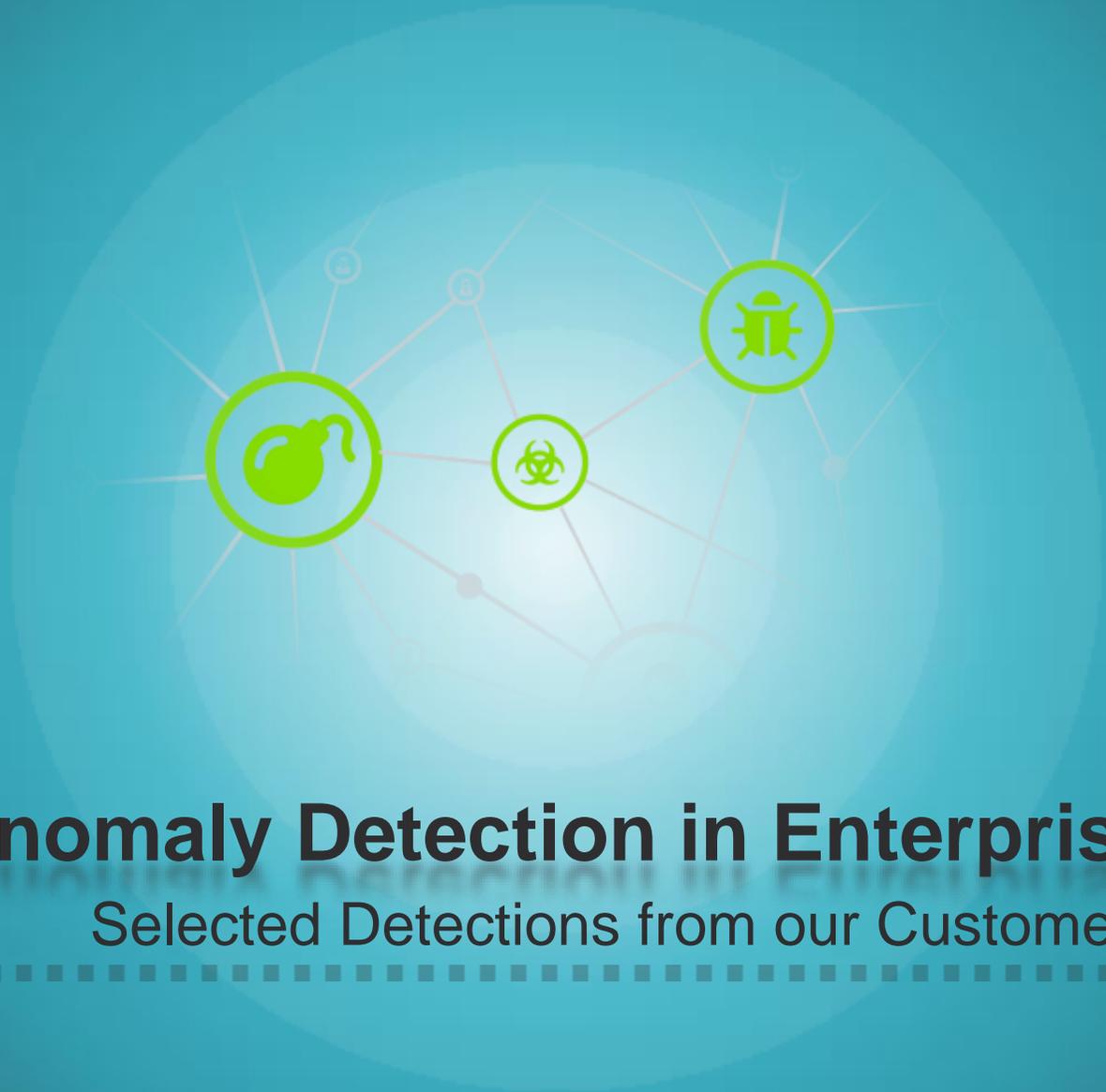
Use priority as syslog severity

Perspective

Message type

EventId

Save



# Use Case: Anomaly Detection in Enterprise

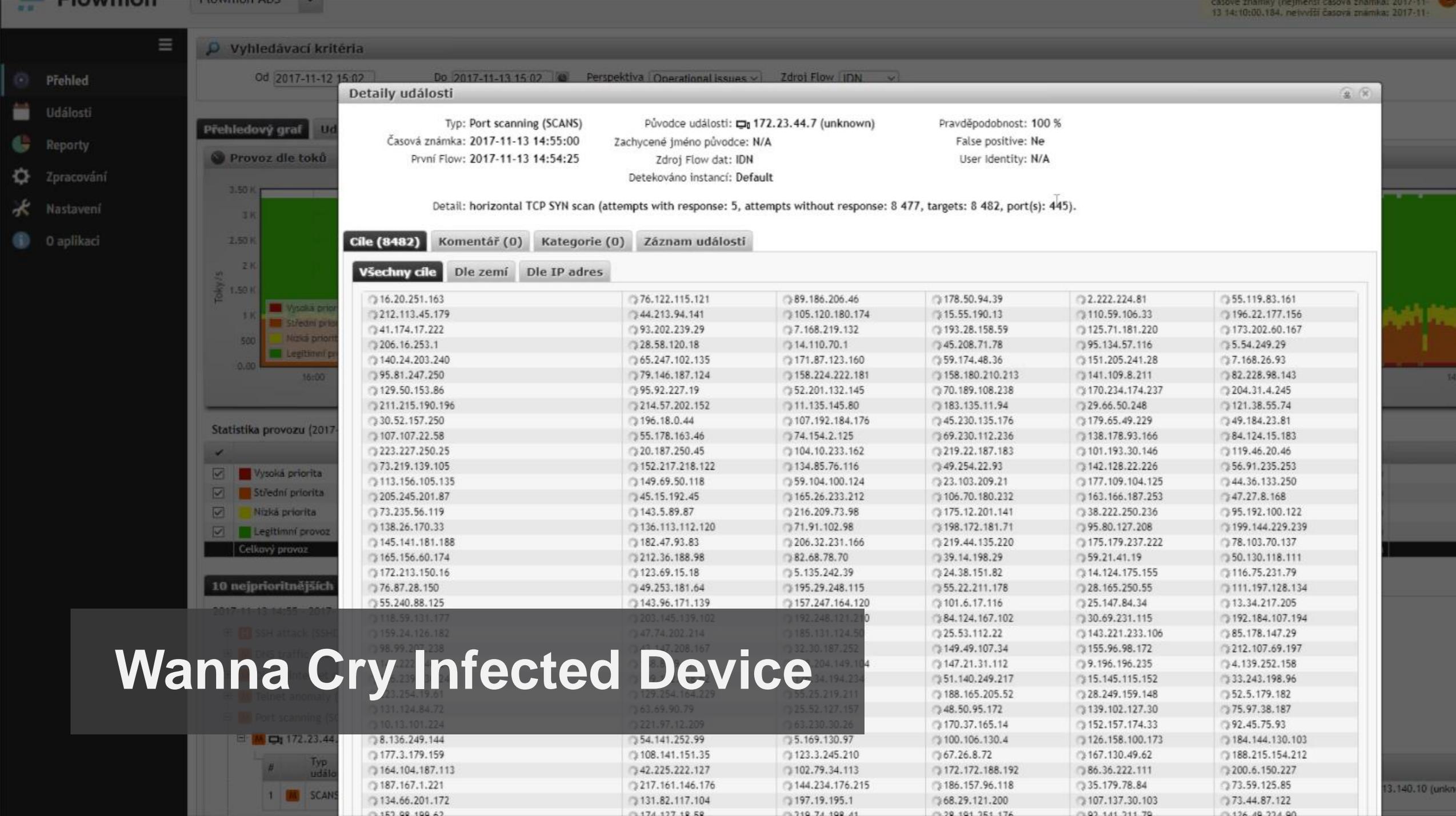
Selected Detections from our Customers

---



# 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...



Vyhledávací kritéria

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

Detaily události

Typ: Port scanning (SCANS) Původce události: 172.23.44.7 (unknown) Pravděpodobnost: 100 %  
Časová známka: 2017-11-13 14:55:00 Zachycené jméno původce: N/A False positive: Ne  
První Flow: 2017-11-13 14:54:25 Zdroj Flow dat: IDN User Identity: N/A  
Detekováno instancí: Default

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 země 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
118.59.131.177	203.145.139.102	192.248.121.210	84.124.167.102	30.69.231.115	192.184.107.194
159.24.126.182	47.74.202.214	185.131.124.50	25.53.112.22	143.221.233.106	85.178.147.29
98.99.207.238	147.208.167	32.30.187.252	149.49.107.34	155.96.98.172	212.107.69.197
222.222.222.222	8.8.8.8	204.149.104	147.21.31.112	9.196.196.235	4.139.252.158
6.239.8.8	8.8.8.8	34.194.234	51.140.249.217	15.145.115.152	33.243.198.96
23.254.19.81	129.254.164.229	95.25.219.211	188.165.205.52	28.249.159.148	52.5.179.182
131.124.84.72	63.69.90.79	25.52.127.157	48.50.95.172	139.102.127.30	75.97.38.187
10.13.101.224	221.97.12.209	63.230.30.26	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
153.98.199.62	174.127.18.58	219.74.198.41	28.191.261.176	92.141.211.79	126.49.224.80

Wanna Cry Infected Device

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

#	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)					
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)					
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 (neznámá)	BPATTERNS	SmbTraffic: Suspicious samba traffic detected, requests count: 3, response count: 0, sent data: 268.94 MiB, received data: 0.00 B, targets count: 1.	2019-03-09 01:05:00	LAN	192.168.2.3 (neznámá)
13	192.168.2.7 (neznámá)	BPATTERNS	SmbTraffic: Suspicious samba traffic detected, requests count: 4, response count: 0, sent data: 286.57 MiB, received data: 0.00 B, targets count: 1.	2019-03-09 00:35:00	LAN	192.168.2.3 (neznámá)
15	192.168.0.101 (neznámá)	BPATTERNS	Dropbox Communication Detected, requests: 0, sent data: 24.41 KiB, received data: 0.00 B, sent packets: 42, received packets: 0, count of targets: 2.	2019-03-08 14:40:02	LAN	108.160.172.215 (d.v.dropbox.com), 162.125.66.3 (neznámá)
16	10.59.0.40 (neznámá)	BPATTERNS	Dropbox Communication Detected, requests: 3, responses: 0, sent data: 22.83 KiB, received data: 0.00 B, sent packets: 76, received packets: 0, count of targets: 1.	2019-03-08 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 (neznámá)	BPATTERNS	Dropbox Communication Detected, requests: 1, responses: 0, sent data: 24.08 KiB, received data: 0.00 B, sent packets: 33, received packets: 0, count of targets: 2.	2019-03-08 14:33:02	LAN	34.197.126.3 (ec2-34-197-126-3.us-east-2.amazonaws.com)

**Detaily události**

Typ: Flow-based behavior patterns (BPATTERNS) Původce události: 192.168.70.2 (neznámá) Pravděpodobnost: 100 %  
 Časová známka: 2019-03-09 11:50:00 Zachycené jméno původce: N/A False positive: Ne  
 První tok: 2019-03-09 11:49:00 MAC adresa: 00:00:00:00:00:00 Detekováno instancí: Default  
 Identita uživatele: N/A Zdroj dat: LAN

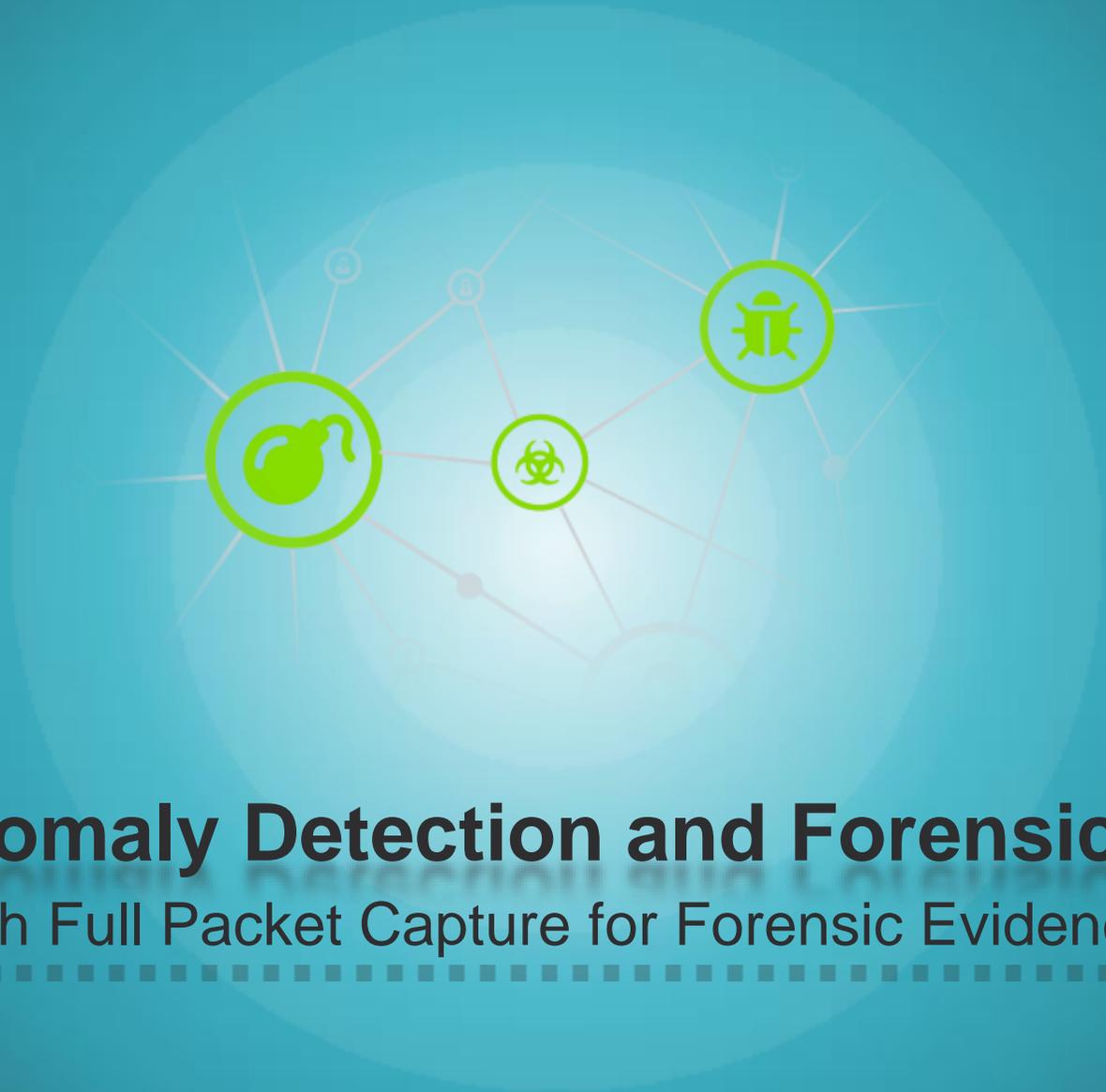
Detail: CryptoMalware: Cryptocurrency mining malware detected, attempts to access 4, uploaded data 742.00 B, downloaded data 0.00 B.

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

---

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

Search criteria

### 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

DNS Question name	Flow count
mmonteironavegacao.com.br	12
services.flowmon.com	4
21.30.24...ao.com.br	4
46.212.2...addr.arpa	2
35.30.24...addr.arpa	2

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

- 1 DNS traffic anomaly (DNSANOMALY) 32 (number of events)
- 2 New or alien device (ALIENDEV) 1 (number of events)
- 3 Behavior anomaly (ANOMALY) 59 (number of events)
- 4 DNS query volume anomaly (DNSQUERY) 56 (number of events)
- 5 Target hosts/ports anomaly (DIVCOM) 176 (number of events)
- 6 High volume of transferred data (HIGHTRANSF) 12 (number of events)

Search Reset

Data feed

- Default
- Default
- Default
- Default
- Default



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

Time	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 mmoniteironavegacao.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.ssdb02.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.ssdb02.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

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  
 Queries  
 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)  
 Authoritative nameservers  
 mmonteironavegacao.com.br: type SOA, class IN, mname ns1.ssdb02.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.ssdb02.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

- 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
  - VLAN
  - MPLS
  - IPv4
  - IPv6
  - ICMP
  - Port
  - SIP
  - 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

# 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.



# Sample Incident Handling and Security Automation

THREAT ID: 3196 (52D 0H 34M 7S)
Reaction time: 28D 3H 34M 25S  
Execution time: 23D 20H 59M 41S

  
10.8.8.250

30.08.2018 11:20:00  


  
192.168.30.11

Security incident       Security breach  
 False alarm             Taken actions

Compliance
Risk analysis
Incident consequences
Attack vector

Process
Details
Additional informations
Potential financial losses

← Action no. 1: 'Check the IP in the xForce database' from step no. 1: 'Checking the IP address in the reputation database'.

Available scripts

[Link](#)

Taken actions

**FrameId**  
*Text*

000100000001001A9AB9

**FrameStatus**  
*Number*

Parsed

**FrameAddDate**  
*Date*

8/30/2018 9:25:17 AM

**FrameDeviceId**  
*Number*

1003

**Parsed fields**

**Type**  
*Text*

SCANS

**EventName**  
*Text*

Port scanning

**Severity**  
*Number*

8

**SourceIp**  
*IpCollection*

10.8.8.250

**EventTime**  
*Date*

8/30/2018 11:20:00 AM

**DestinationIPs**  
*IpCollection*

192.168.30.11,192.168.30.12

**Niesformatowana ramka**

```
<178>Aug 30 11:25:17 localhost ADS: CEF:0|Flowmon Networks|Flowmon ADS Corporate|9.01.01|SCANS|Port scanning|8|src=10.8.8.250
start=Aug 30 2018 11:20:00 deviceCustomString1=192.168.30.100 deviceCustomString1Label=ADSHostName cn1=2980 cn1Label=EventID
msg=chaotic TCP SYN scan (attempts with response: 194, attempts without response: 0, targets: 2, port(s): 22, 443). targetList: 192.168.30.11,
192.168.30.12
```

### Security breaches consequences

**Consequences analysis** (\$)



SCADA\_OT

## SYSTEM\_11

192.168.30.11

Critical

✓ Incident consequences for safety zone:



## SCADA\_OT

✓ SCADA\_Operator

- Loss of reputation
- Disruption of important process of the organization:
  - Sales
  - SCADA\_OT



# Sample Flowmon to IBM QRadar Integration

IBM QRadar

Dashboard Offenses Log Activity Network Activity Assets Reports ISECO LogBook Knowledge base Incident response QDI Flowmon Application Web service response

IBM QRadar

Dashboard Offenses Log Activity Network Activity Assets Reports ISECO LogBook Knowledge base Incident response QDI Flowmon Application Web service response

System Time: 12:08

Dashboard Events Flows

## Event 4755031 info

### Event details

<b>ID</b>	4755031	<b>Detail</b>	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.
<b>Flowstamp</b>	2018-11-13 16:49:50	<b>Perspectives</b>	Security issues: 5, Operational issues: 2
<b>Time</b>	2018-11-13 16:50:00	<b>Comments</b>	-
<b>Type</b>	BPATTERNS	<b>Falsepositive</b>	No
<b>Name</b>	Flow-based behavior patterns	<b>Filters</b>	Inverted DNS&DHCP MITM
<b>Source</b>	103.77.119.227	<b>Flowsource</b>	LAN
<b>Targets</b>	10.0.0.22		
<b>Certainty</b>	1		

### 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

Close

## Graph type: Events count

Toggle all

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



## 15:01:00 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

## Detection and Mitigation Orchestration of Volumetric DoS/DDoS Attacks



Protect your business &  
customers satisfaction



Easy, flexible and  
cost efficient way of  
DDoS Protection

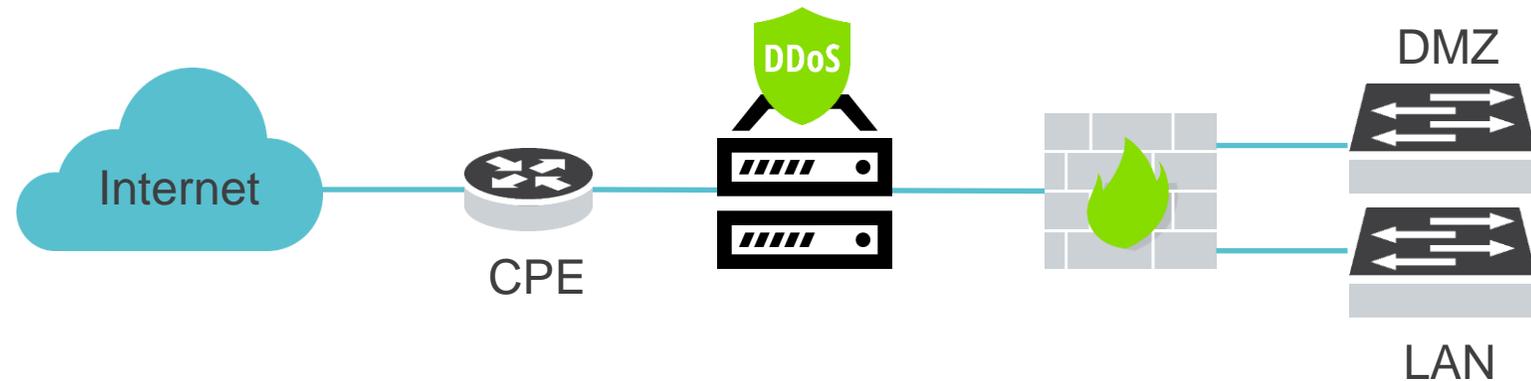


Saves costs on  
extra HW, mitigate  
with your network

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.”*

# 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

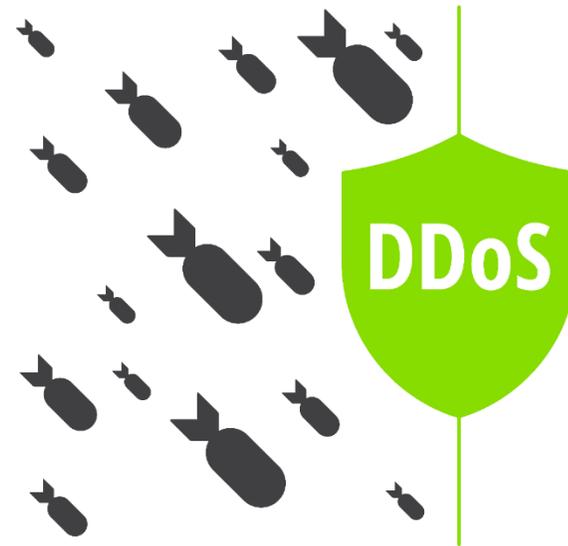
- Backbone perimeter specifics
  - Multiple peering points – routers & uplinks
  - Large transport capacity – tens of gigabits easily
  - In-line protection is close to impossible!



- 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

Configure Adaptive threshold

Use all baselines

ICMP	Attack and suspect
UDP	Attack and suspect
TCP	Attack and suspect
TCP Rst	Attack and suspect
TCP Syn	Attack and suspect
TCP Ack Fin	Attack and suspect
TCP Syn Ack	Attack and suspect

Save Cancel

PDF report Mark as false positive Delete

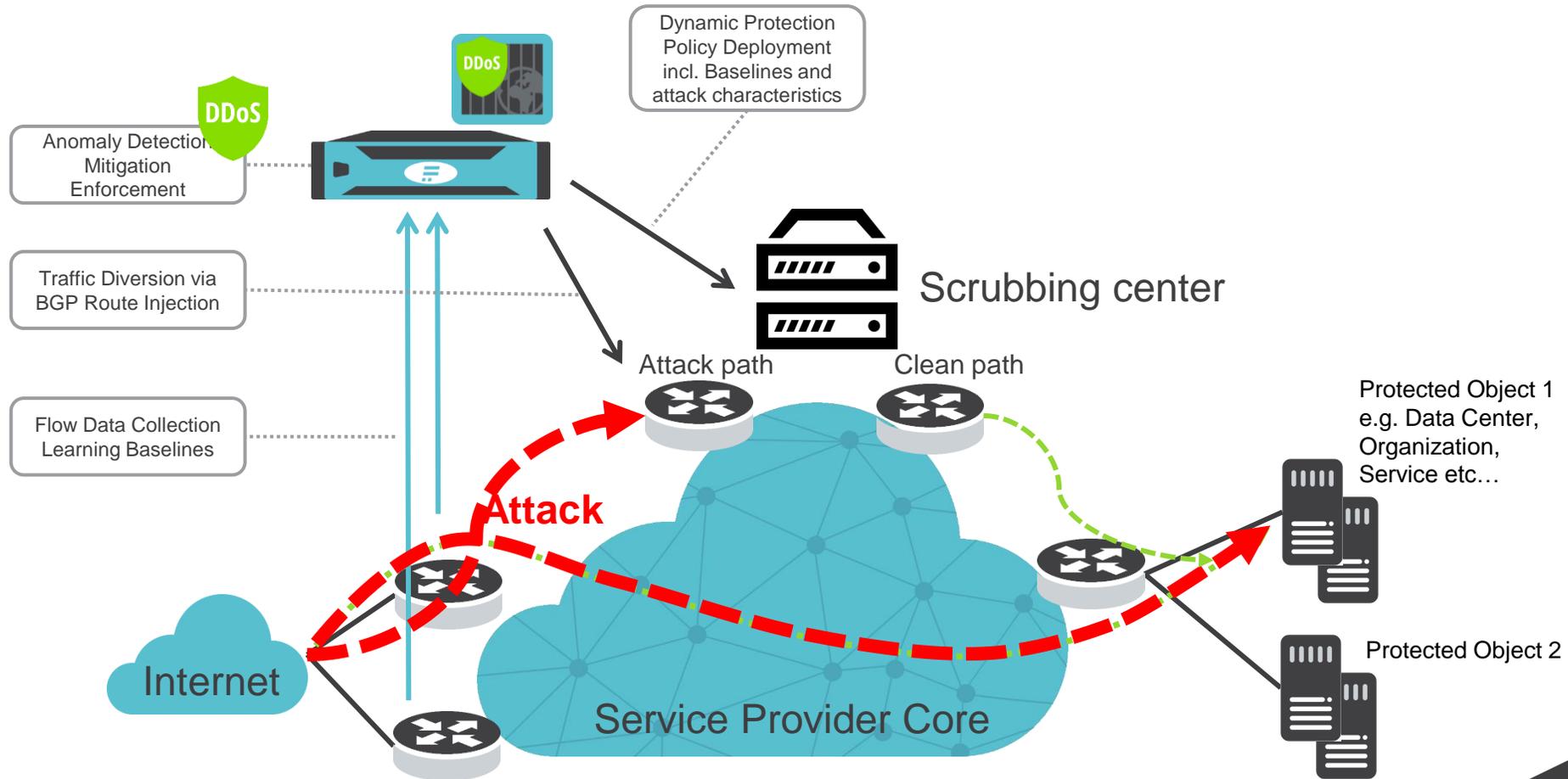


## Use Case: DDoS Protection

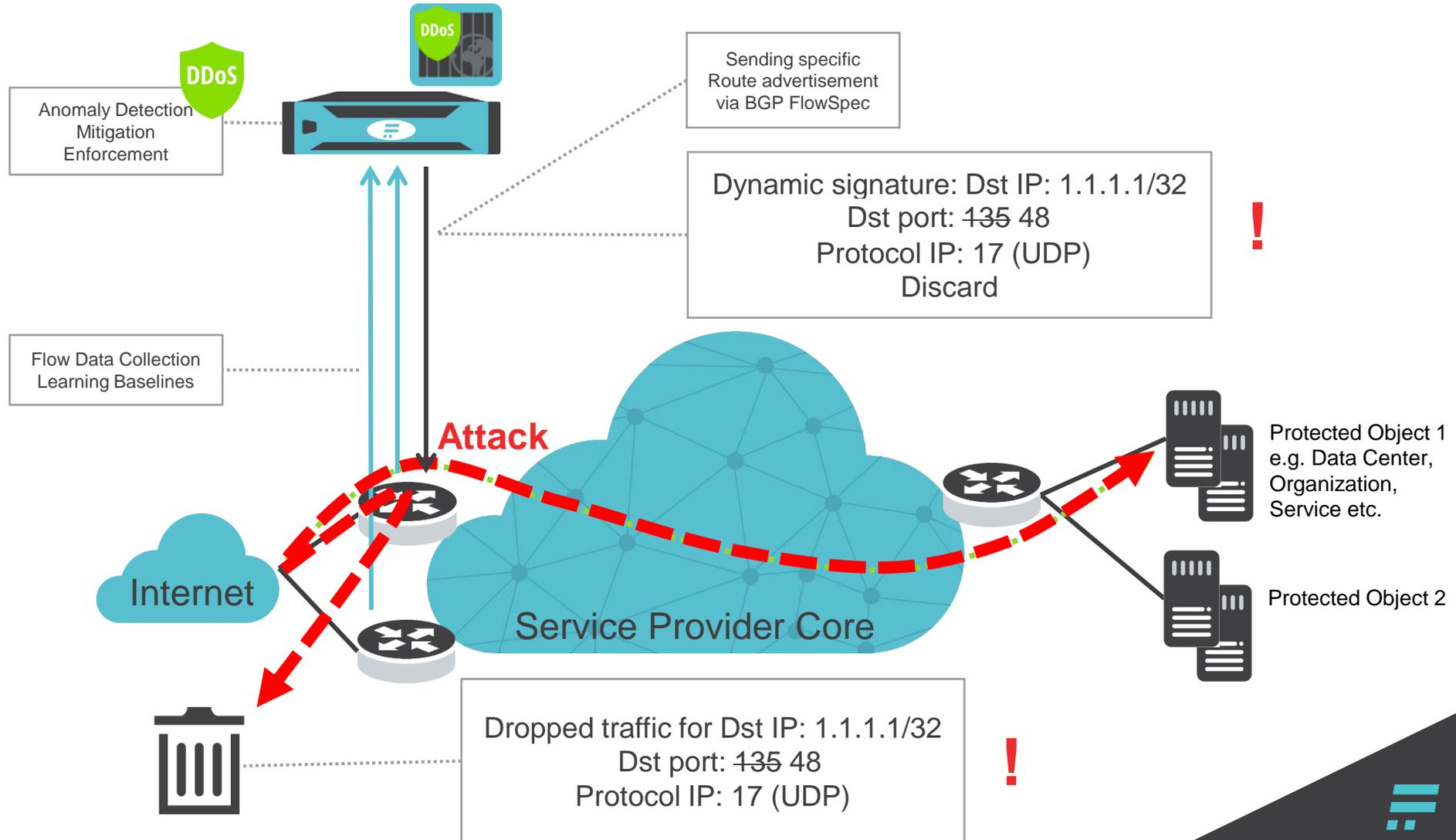
Various Protection Scenarios using Flow-based Detection

---

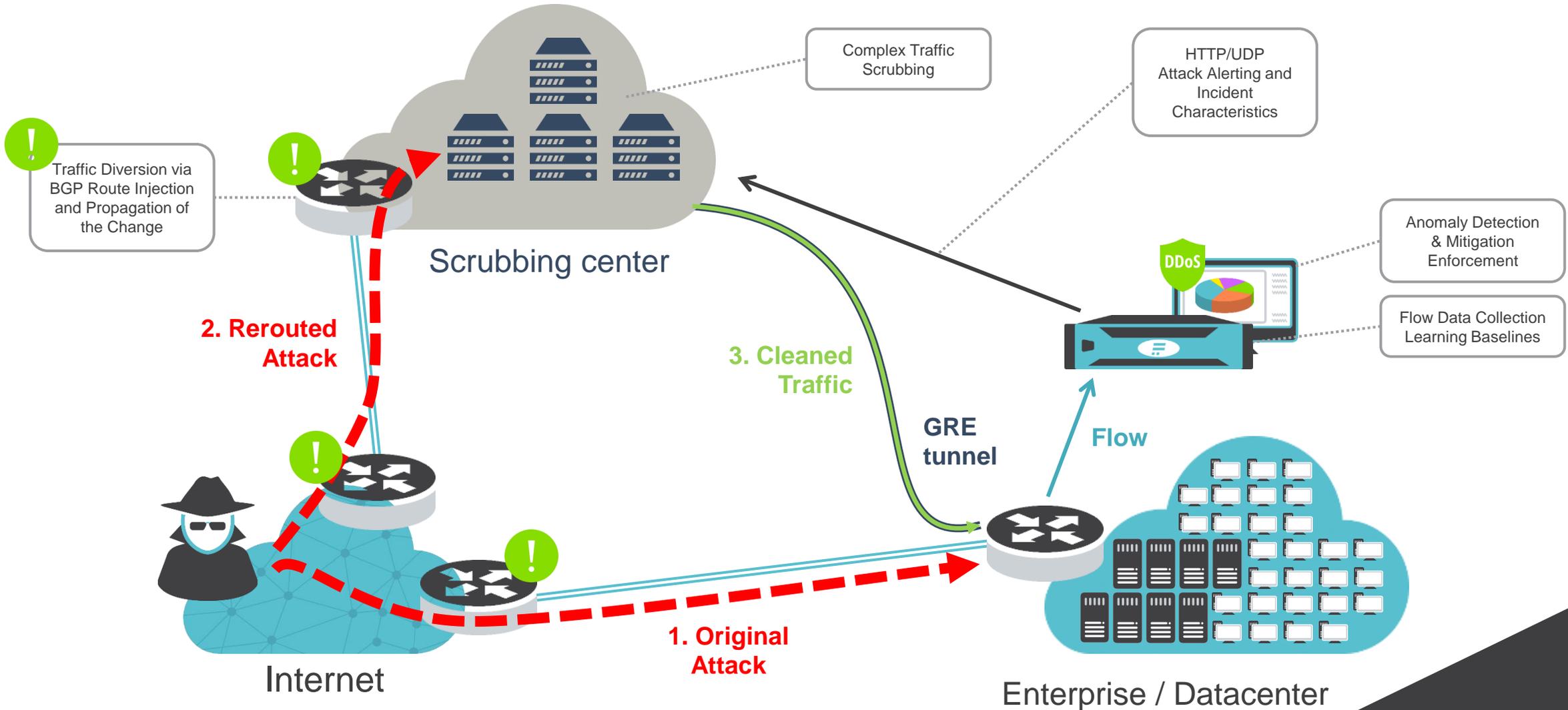
# Out-of-Band with Local Scrubbing Appliance



# Mitigation Through Infrastructure (BGP Flowspec)



# Cloud Scrubbing & Cloud Signaling





# Summary

## Benefit From Using Flow Data



## Packet Analysis

The complexity of such systems puts high demands on the knowledge/experience of administrators. These tools are simply too 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.

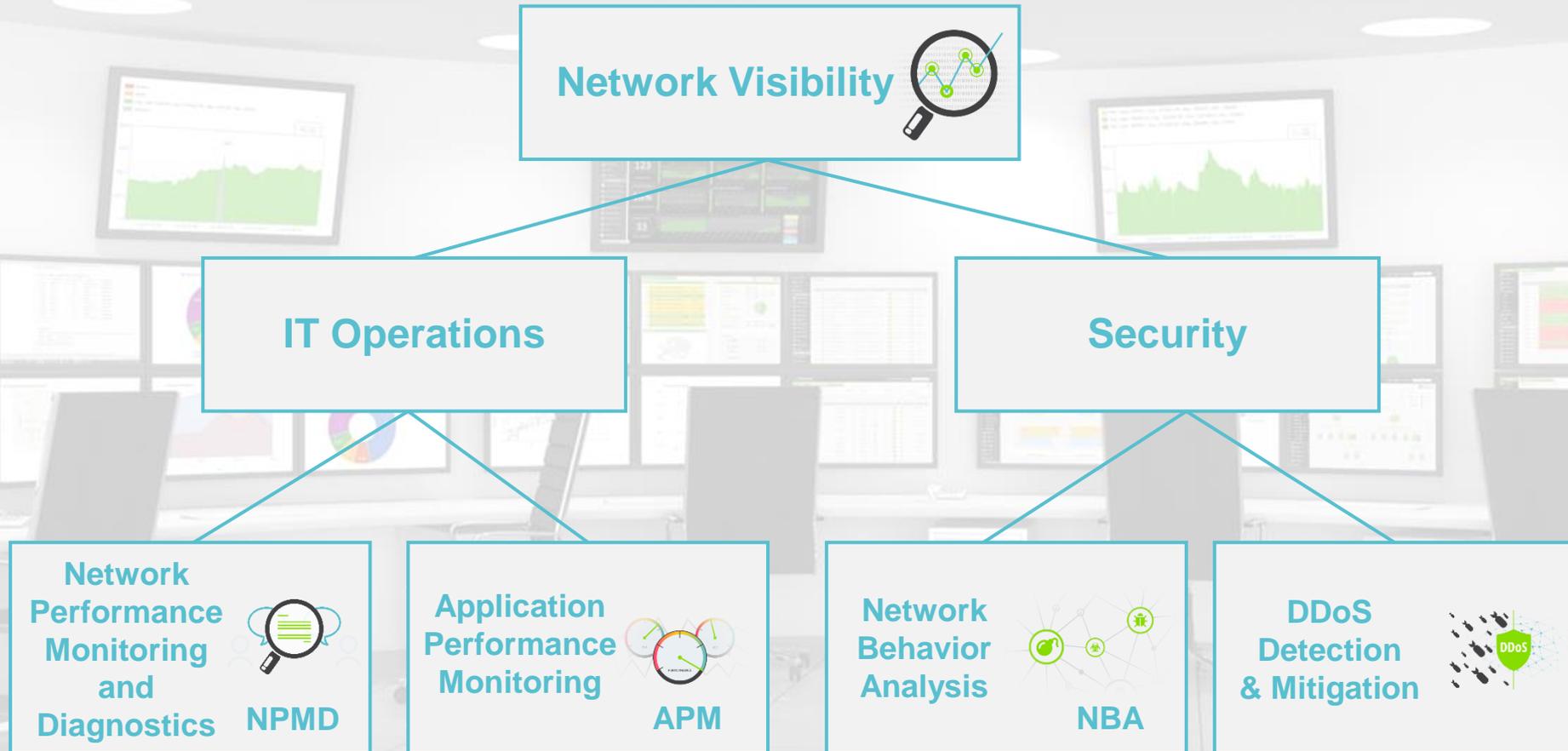
Flow enriched with L7 visibility and on-demand packet capture is the future of Network Performance Monitoring and Diagnostics.



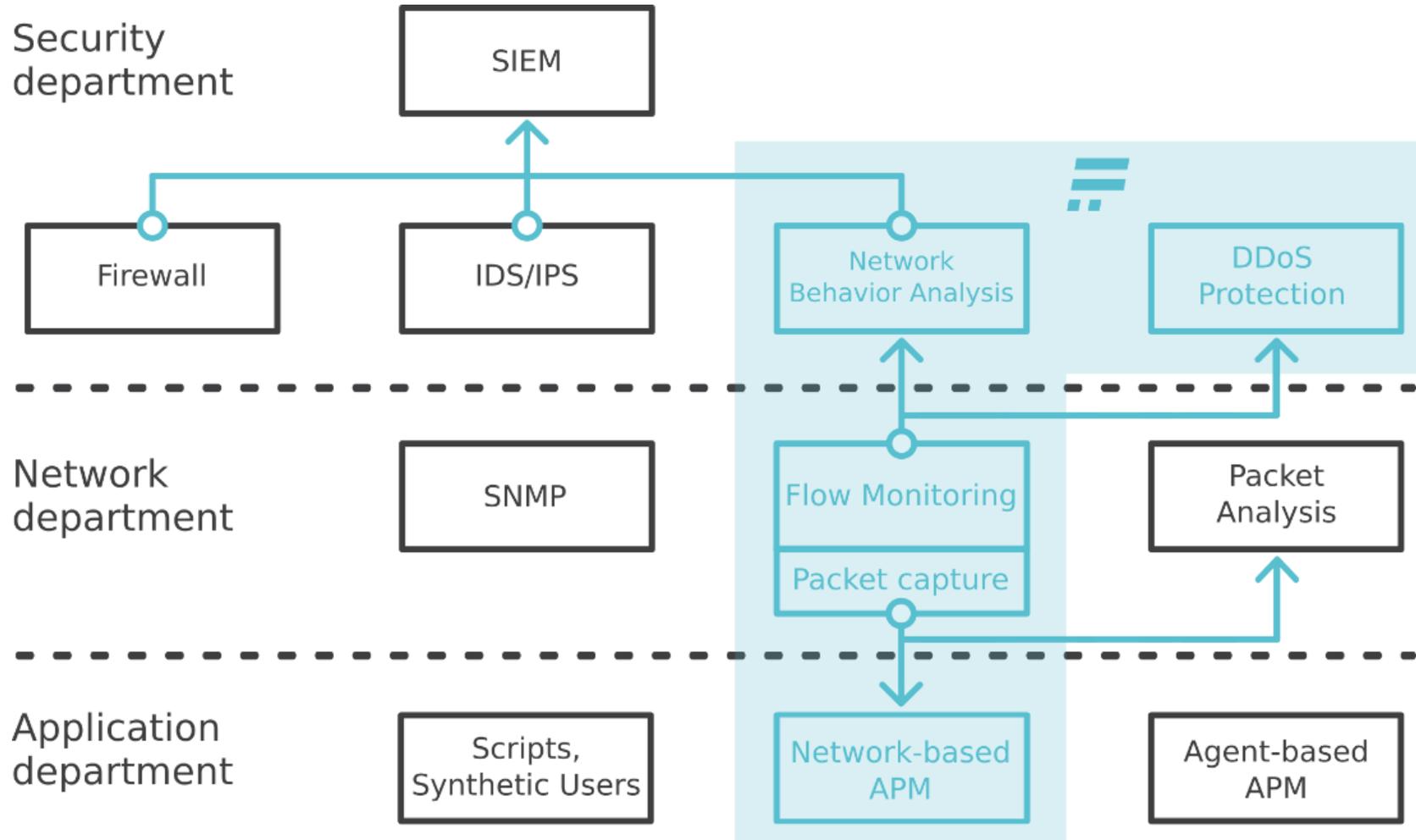
## SNMP Monitoring

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 Portfolio



# Flowmon Fit with other Tools



# 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 (3<sup>rd</sup> parties integration – SIEM etc.)



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



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



KONICA MINOLTA



vodafone



ORIFLAME SWEDEN



SIEMENS



SLOVENSKÁ sporiteľňa



Volkswagen



orange



Telefonica



Allianz



hp



T-Mobile



GÉANT Networks Services People



KIA



upc



Raiffeisen BANK



e-on



Czech Republic

# 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, ...

