



# Flowmon 12

Novinky

**Milan Štěpánek**

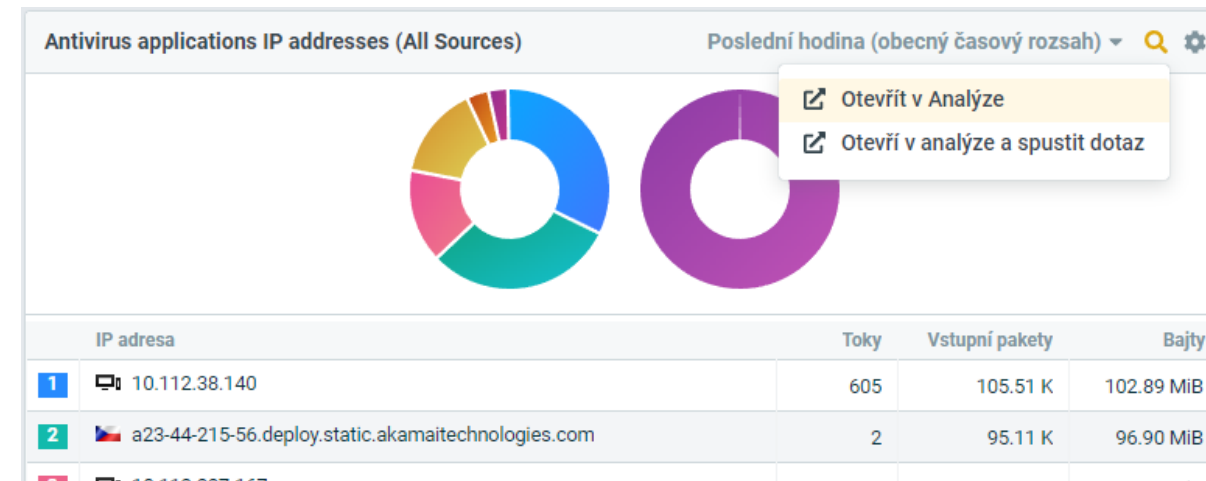
Sales Engineer

9. prosince 2022, Customer Days



# Flowmon 12.0 highlights

- Vylepšení uživatelského rozhraní
- Monitorování cloudového prostředí
- Flow Quality Analyzer
- Nové metody ADS
- Nové možnosti ladění ADS
- Attached flows
- Integrace s WUG



# Cloud Monitoring

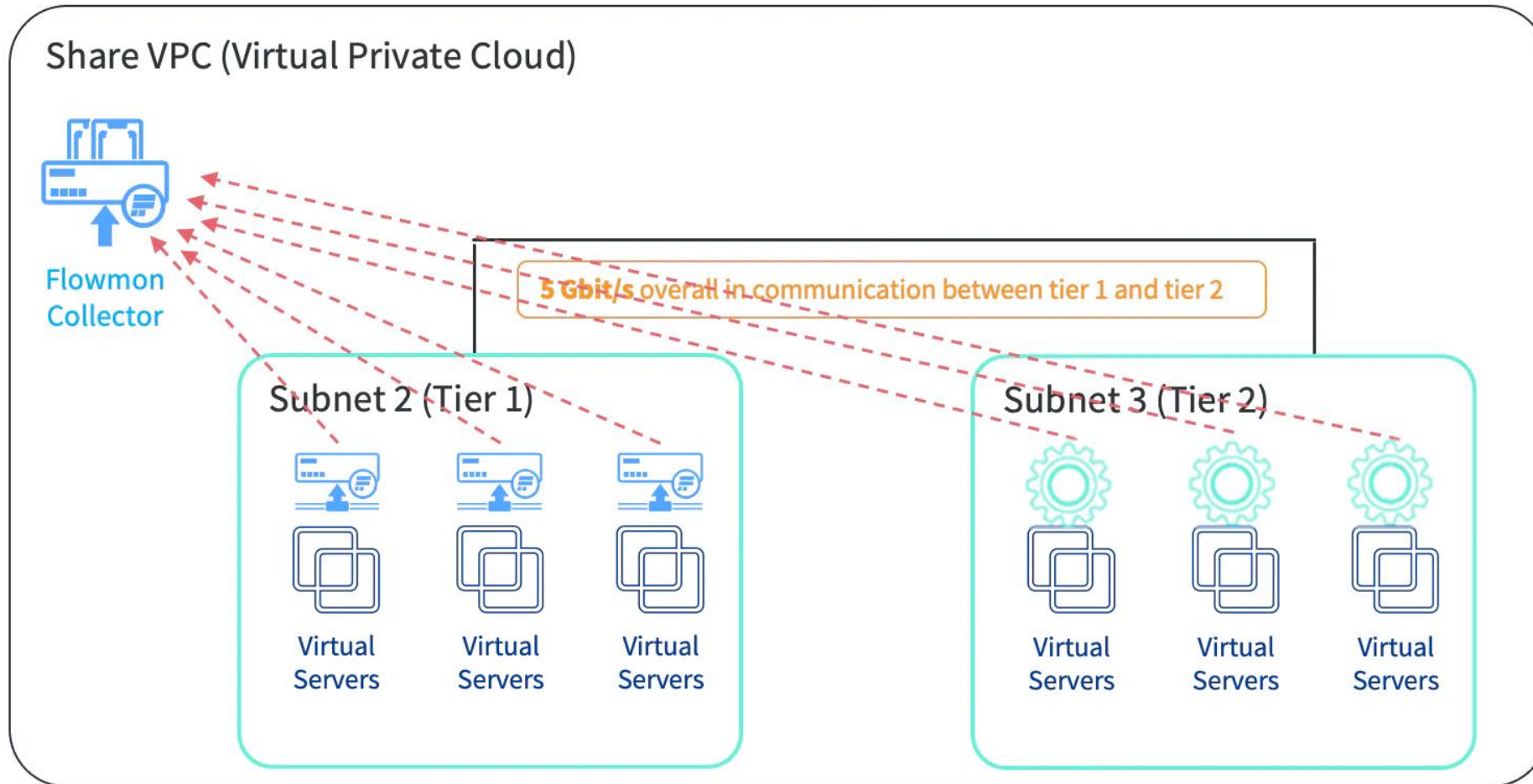
GCP - Google Cloud Platform

AWS - Amazon Web Services

Azure - Microsoft Azure



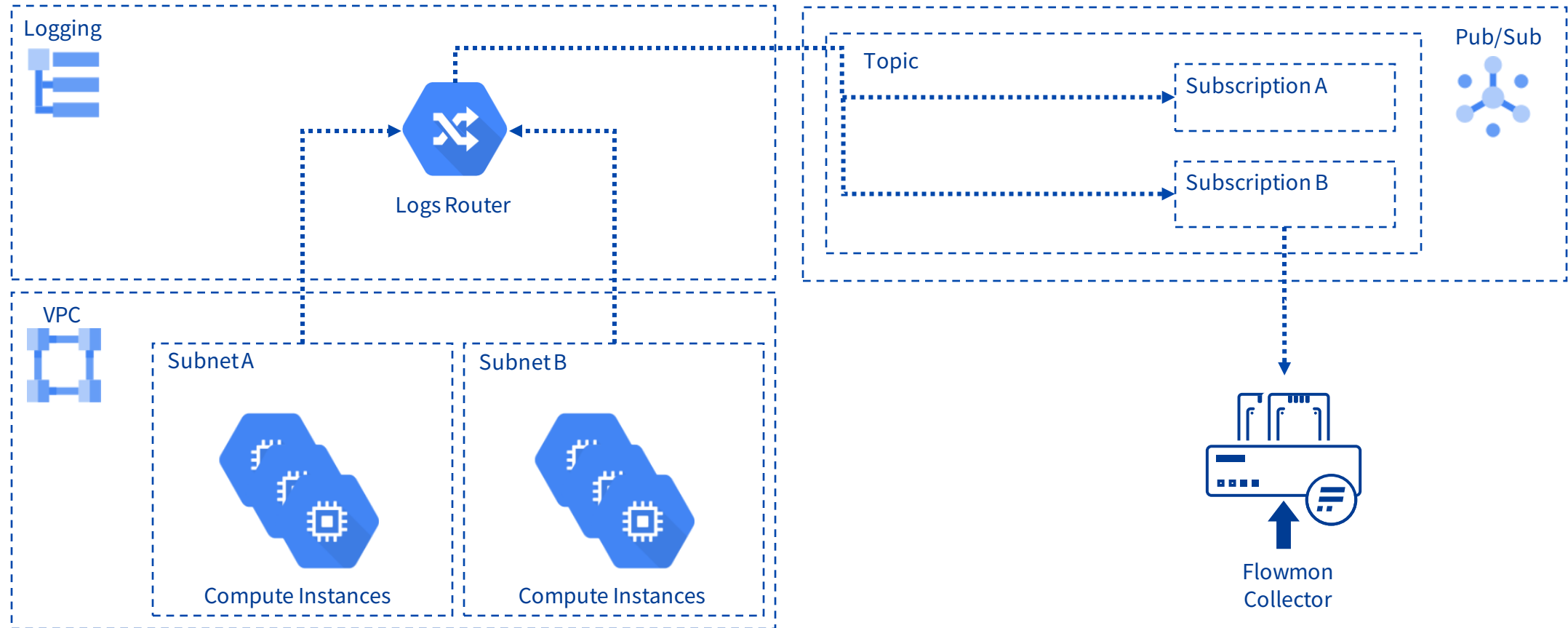
# Cloud Monitoring - Flowmon Probe/Flow logs





# GCP - Flow Logs monitoring concept

Transport mechanism for Flow Logs





# GCP Flow Logs flow source

Each VPC within a ProjectID is assigned to a flow source in Monitoring Center automatically

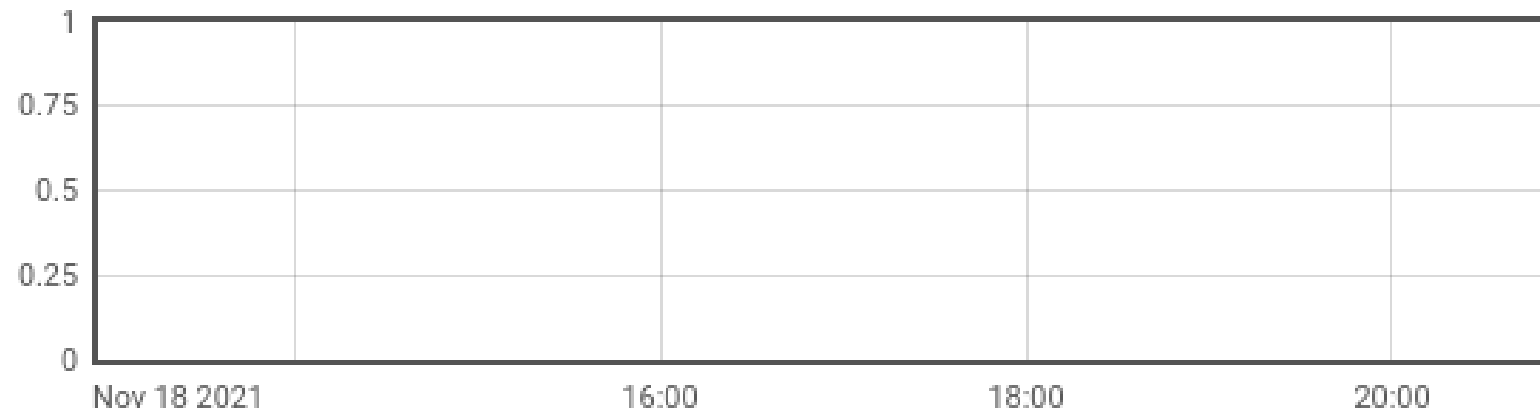
Flow source IP address is automatically generated and thus artificial

Interfaces are created from subnets

Corresponding names of VPCs, projects and subnets are obtained from Google Cloud API automatically including potential updates

Rest of the work with flow data from Google Cloud is exactly the same as with traditional NetFlow/IPFIX

● 127.129.0.1 (jansky-flowmon-vnet-mon1, dev-platform-team)



Type here to search

Profiled, Not profiled

All Ports

jansky-f...net-monitored

**Subnet Name**

1

# Flowmon 12 - Monitoring hybridních sítí

## Fyzická infrastruktura



## Virtuální prostředí



## Cloud



# Flow Quality Analyzer

- CLI tool to automatically analyze and review quality of flow data from third party flow sources
- Looks for specific issues in flow data such as missing attributes, inaccuracy of timestamps, timeout settings, etc.
- Provide human readable output showing results of all the tests performed with the data
- Documented in [Solution Maintenance](#) guide

```
[flowmon@flowmon-collector ~]$ fqa start 2055
Flow Quality Analyser
  Started 2022-05-30T21.40
  Status
    Flows collected :      156
    Time remaining  :      67 / 330 s
    Space used      :      260K / 300M
```



# Flow Quality Analyzer

---

Missing basic fields

---

Duplicated flows

---

Only one direction of traffic

---

Missing TCP flags

---

Wrong active/inactive timeouts

---

Missing templates

---

Wrong timestamps

---

```
flowmon@localhost:~  
[CHECK] Checking timestamp sanity...  
[SUCCESS] All timestamp values have passed the sanity check.  
  
[CHECK] Checking overlapping flows...  
[FAIL] There are overlapping flows with the same Observation Domain ID and Template ID (based on the standard 5-tuple).  
  
[CHECK] Looking for TCP flags in non-TCP flows...  
[SUCCESS] TCP flags are not exported for non-TCP traffic.  
  
[INFO] Looking for encoding of TCP flags...  
Following Information Elements are present in Templates for TCP flags: iana:tcpControlBits.  
  
[INFO] TCP flags statistics
```

Value	Binary	Meaning	Flows	Percentage
27	11011	....AP.SF	2980	99.666
17	10001	....A...F	4	0.134
16	10000	....A....	4	0.134
25	11001	....AP..F	2	0.067

```
[CHECK] Looking up for transport protocols...  
[SUCCESS]  
Exported protocols: [1, 6, 17, 249, 58]  
  
[CHECK] Looking up for ICMP representation...  
ICMPv4:  
[FAIL] no ICMPv4 traffic  
ICMPv6:  
[FAIL] no ICMPv6 traffic  
  
[CHECK] Looking up for end reasons...  
Present endreasons: [None]  
  
[INFO] Type of Service Statistics
```

ToS	Binary	Flows	Percentage
0	Na	3118	98.702
None	Na	40	1.266
96	1100000	1	0.032

```
Current specification is according to the RFC 2474 (Section 3):
```



# ADS

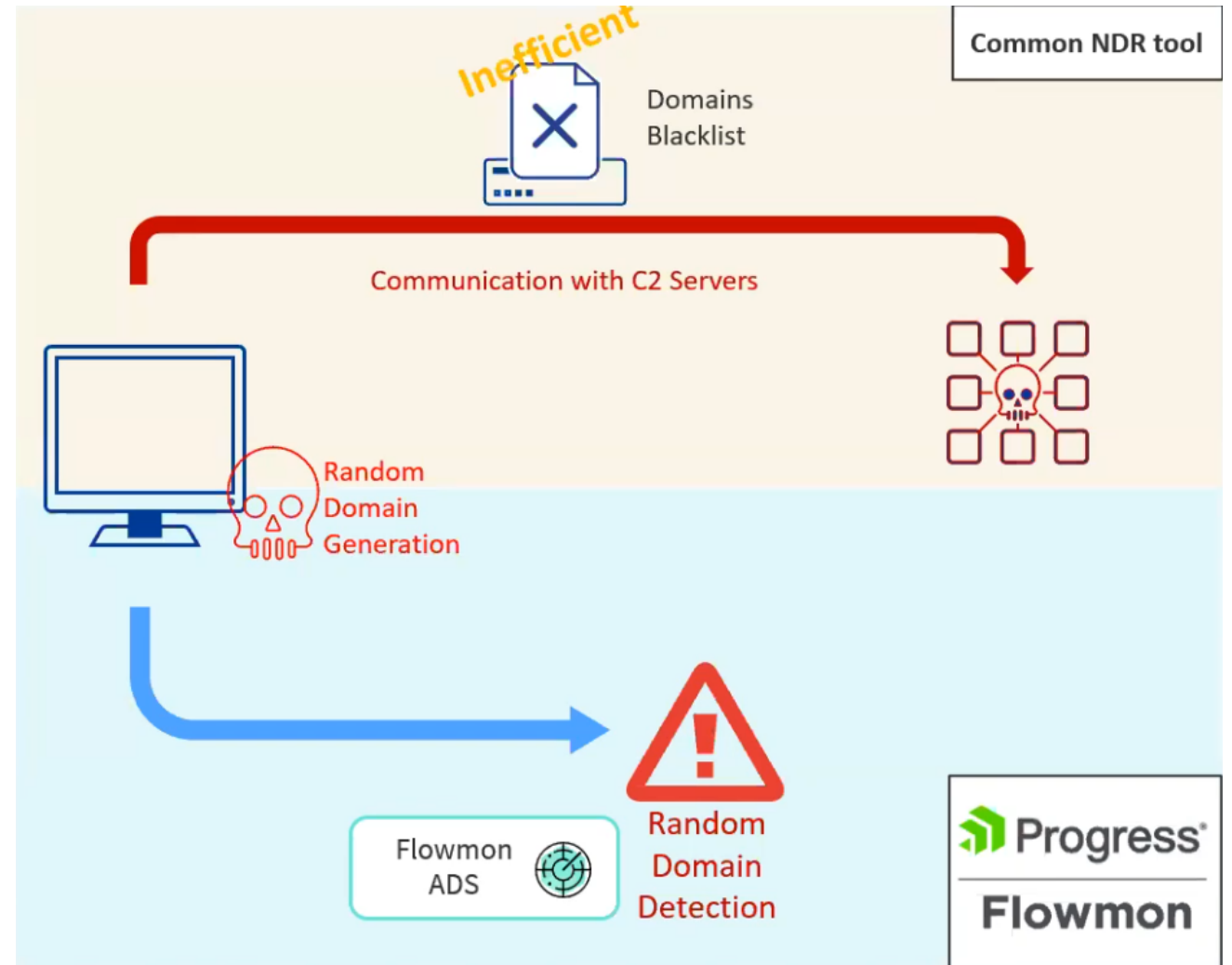
## Nové detekční metody

# RANDOMDOMAIN

Attackers are using domain generation algorithms to hide botnet command & control communication and prevent it from being detected and blocked

Detection method RANDOMDOMAIN is based on unsupervised machine learning techniques and is able to recognize a random domain without prior knowledge

This detection technique accompanies traditional detection based on known indicators of compromise as well as detection based on behavior analysis

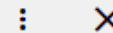


# RANDOMDOMAIN

Událost č. 5911471

KOPIROVAT ID UDÁLOSTI

UKOTVIT OKNO



**Typ** Random domain name (RANDOMDOMAIN)

**Podtyp** General  
Upozorňuje na využití náhodně generovaných názvů domén. Tento druh názvů domén může být využíván malware pro komunikaci se servery velení a řízení (Command and Control).

**Detail** Byl detekován přístup k náhodně generovaným doménám. Domény: **us.64e98469810bd13e2b45e52d19d6fddfe333b3528350d8cfa792d478.com.**

**MITRE ATT&CK** Taktika Command and Control >> Technika Dynamic Resolution

**Čas detekce** 2022-05-29 08:26:31

**Naposledy aktualizováno** 2022-05-29 08:26:31

**První tok** 2022-05-29 08:25:58

**Původce události** 10.112.224.19 (neznámá)

**Zachycené jméno původce** Neuvedeno

**MAC adresa** 74:4d:28:07:79:51

**Identita uživatele** Neuvedeno

**Pravděpodobnost** 100 %

**False positive** Ne

**Detekováno instancí** Default

**Zdroj dat** Default2

**CÍLE (1)** KOMENTÁŘE (0) KATEGORIE (0) ATRIBUTY ZÁZNAM UDÁLOSTI SOUVISEJÍCÍ UDÁLOSTI IDS (0)









**VEŠKERÉ IP ADRESY** PODLE ZEMĚ PODLE IP ADRESY

10.112.1.1 (neznámá)

# RANDOMDOMAIN

- nová metoda je automaticky spuštěna
- metoda se nijak nenastavuje, běží zcela automaticky
- ale pozor, pokud máte Flowmon již delší dobu tak metoda RANDOMDOMAIN není zapnuta ve stávající perspektivě => Flowmon sice něco detekuje, ale já to nevidím
- je nutné přidat metodu RANDOMDOMAIN do stávající perspektivy => Security issues/Medium, Operational issues/Informational
- nebo smazat stávající perspektivu a nechat si vytvořit defaultní novou

## Perspectives

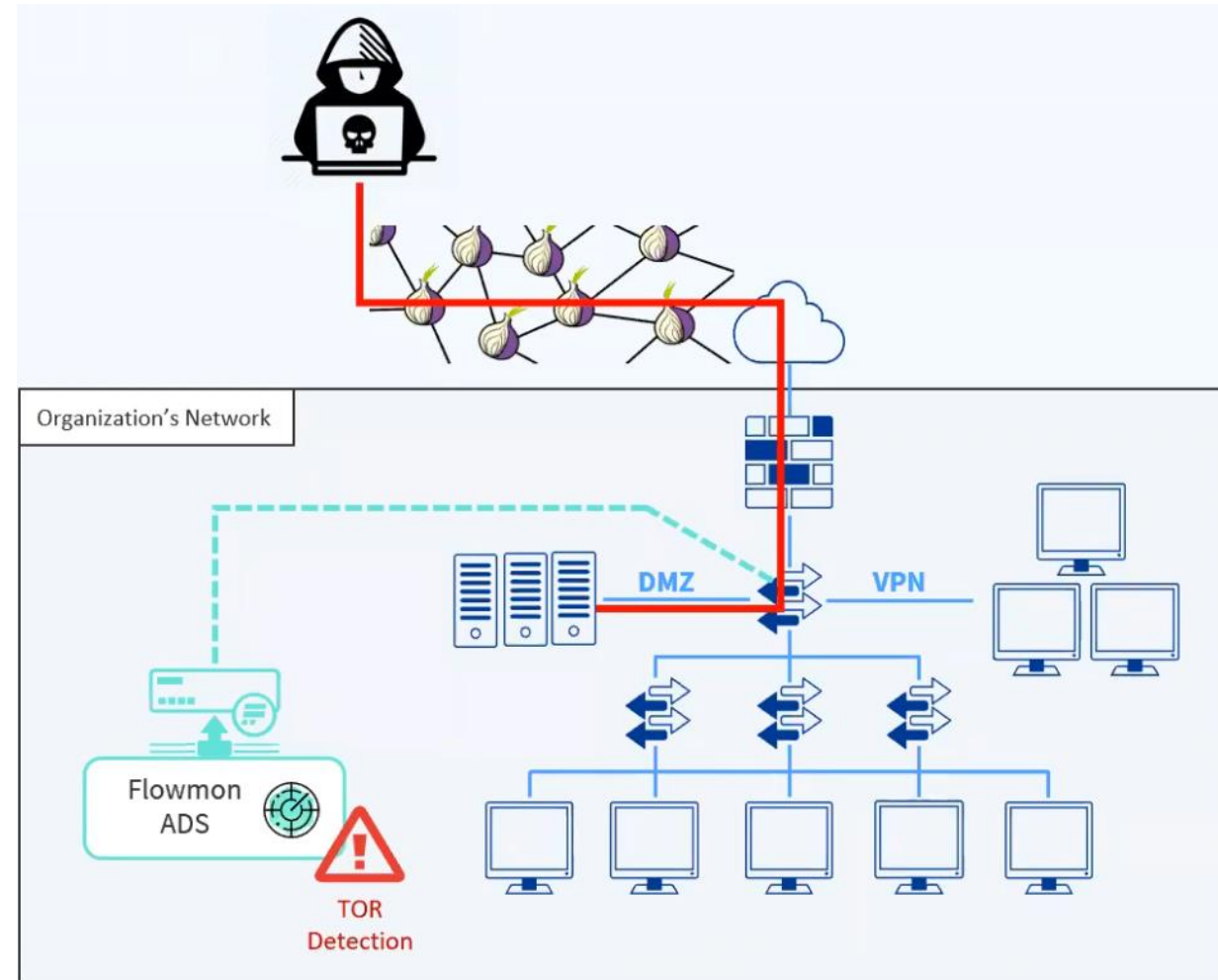
NAME	PRIORITIES		
Backbone issues	25 (number of defined priorities)		
FPI zachyt	2 (number of defined priorities)		
Operational issues	40 (number of defined priorities)		
Security issues	40 (number of defined priorities)		

**=> 41**

# Access to server infrastructure via TOR

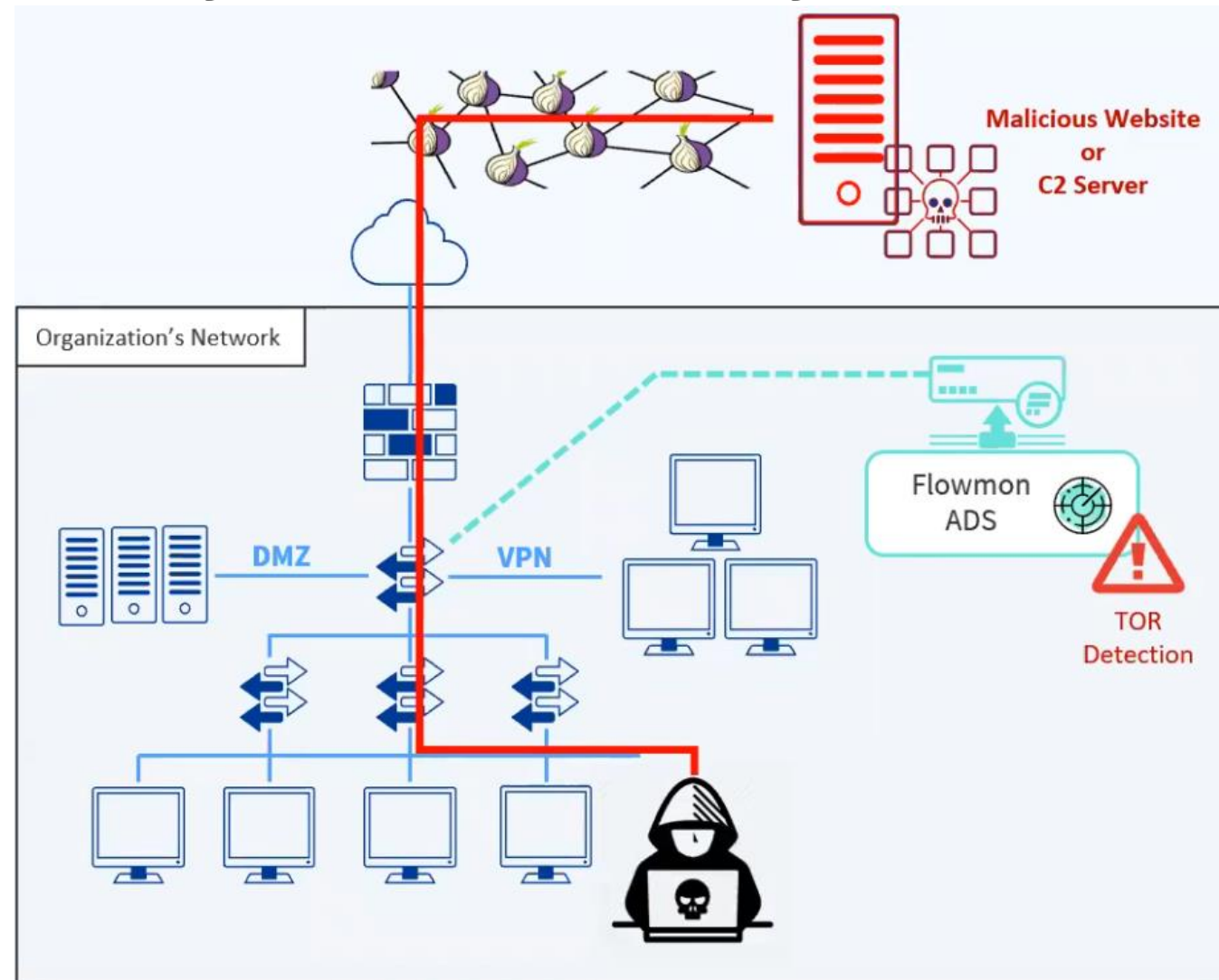
Detection of access to company servers (e.g. hosted in DMZ) via TOR networks

This may indicate initial access of an attacker mapping the target environment and masking his identity in TOR network



# Client leveraging TOR to bypass security measures

- Detection of clients in the corporate network that leverage TOR to access network resources
- This typically indicates that user is bypassing security measures and is trying to mask his activities in the network to prevent being monitored





# ADS

## Nové možnosti ladění



# Flowmon 11

Nové false positive

Metoda

Zdroj dat  Všechny  Vybrat zdroje dat

Komentář

Zdroj události

**Zdrojové IP adresy**  
IP adresy mohou být zadány jako seznam oddělený čárkami. Je-li vložena IPv4 adresa, lze jedno z jejích polí zapsat s pomocí rozšířené notace. [?](#)

Filtry

Cíl události

**Cílové IP adresy**  
IP adresy mohou být zadány jako seznam

# Flowmon 12

Nové false positive

Metoda

**Instance metody**  Všechny  Pouze vybrané instance metody

Zdroje dat  Všechny  Pouze zvolené zdroje dat

Popisek

Zdroj události

**IP adresy**  
IP adresy mohou být zadány jako seznam oddělený čárkami. Je-li vložena IPv4 adresa, lze jedno z jejích polí zapsat s pomocí rozšířené notace. [?](#)

Filtry

# Flowmon 11

**Nové false positive**

Cíl události

**Cílové IP adresy**  
IP adresy mohou být zadány jako seznam oddělený čárkami. Je-li vložena IPv4 adresa, lze jedno z jejích polí zapsat s pomocí rozšířené notace. ?

**Filtry**

# Flowmon 12

**Nové false positive**

Cíl události

**IP adresy**  
IP adresy mohou být zadány jako seznam oddělený čárkami. Je-li vložena IPv4 adresa, lze jedno z jejích polí zapsat s pomocí rozšířené notace. ?

**Filtry**

Více možností

**Pokročilé parametry filtrování**

**Autonomní systémy** ?

**Hostname**

HTTP hostname nebo dotazy DNS lze zadat jako seznam oddělený čárkami. ?

**8075:MICROSOFT-CORP-MSN-AS-BLOCK** x

\*office365.com

# Attached flows

- Součástí ADS události je "Event evidence", která zobrazuje detail události
- Monitoring center je výpis surových flow dat z FMC
- Attached flows je vzorek flow detekované události připojený k události v ADS

## Event #7615131

**Type** Communication with blacklisted hosts (BLACKLIST)

**Subtype** Host  
Upozorňuje na zařízení, která komunikují s IP adresami zařazenými na blacklist. Toto může ir  
IP adres zařazených na blacklist.

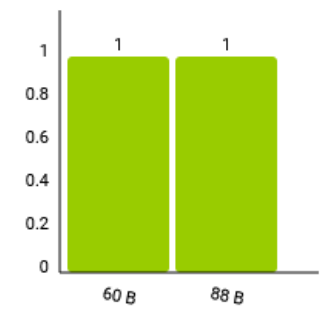
**Detail** Known attackers, pokusy: 1, nahráno: 60 B, staženo: 88 B, často používané porty: 6379

**MITRE ATT&CK** Tactic Initial Access >> Technique External Remote Services

<b>Detection time</b>	2022-11-28 10:03:39	<b>Event source</b>	39.108.152.96
<b>Last update</b>	2022-11-28 10:03:39	<b>Captured source hostname</b>	N/A
<b>First flow</b>	2022-11-28 10:03:10	<b>MAC address</b>	00:00:00:00:00:00
		<b>User identity</b>	N/A

TARGETS (1) COMMENTS (0) CATEGORIES (0) ATTRIBUTES **EVENT EVIDENCE**

### ATTACHED FLOWS MONITORING CENTER



SOURCE IP	DESTINATION IP	TIMESTAMP	DURATION	PROTOCOL	SOURCE PORT	DESTINATION PORT	TRA
39.108.152.96 (unknown)	10.112.129.20 (unknown)	2022-11-28 10:03:10.032	0	TCP	32794	6379	
10.112.129.20 (unknown)	39.108.152.96 (unknown)	2022-11-28 10:03:10.032	0	TCP	6379	32794	

# Attached flows / Připojené toky - nastavení

kemp > Anomaly Detection System ▾

ZPRACOVÁNÍ

NASTAVENÍ SYSTÉMU

ÚDRŽBA

## NASTAVENÍ APLIKACE

Obecná nastavení

IDS kolektor

**Nastavení úložiště**

Nastavení LDAP

Nastavení ePO

## UŽIVATELSKÁ NASTAVENÍ

Uživatelská oprávnění

Uživatelská nastavení

## PŘIZPŮSOBENÍ

Pojmenované služby

Externí dotazy

## Nastavení úložiště

### Odstranit události po

Nastaví parametr DeleteEventsAfter všem instancím metod (výchozí perioda - 183, nikdy - 0)

Implicitní perioda ▾

### Neaktivní časový limit

Není-li událost v tomto období opětovně detekována, dojde k jejímu uzavření.

15 minut ▾

### Interval aktualizace

Čas mezi aktualizacemi události.

5 minut ▾

### Odstranit graf flow po

Počet dnů pro uložení dat grafu

183

### Připojit toky



### Šablony toků (13)

Zdrojová IP x Zdrojový port x Cílová IP x Cílový port x Protokol x Časová známka x Trvání x Přeneseno x  
Pakety x Příznaky x TOS x MAC zdroje x Cílová MAC x

ULOŽIT



# Flowmon Roadmap

Flowmon 13.0 – est. Q4/2023

# Disclaimer

**All roadmaps are for informational purposes only, and the reader is hereby cautioned that actual product development may vary significantly from roadmaps**

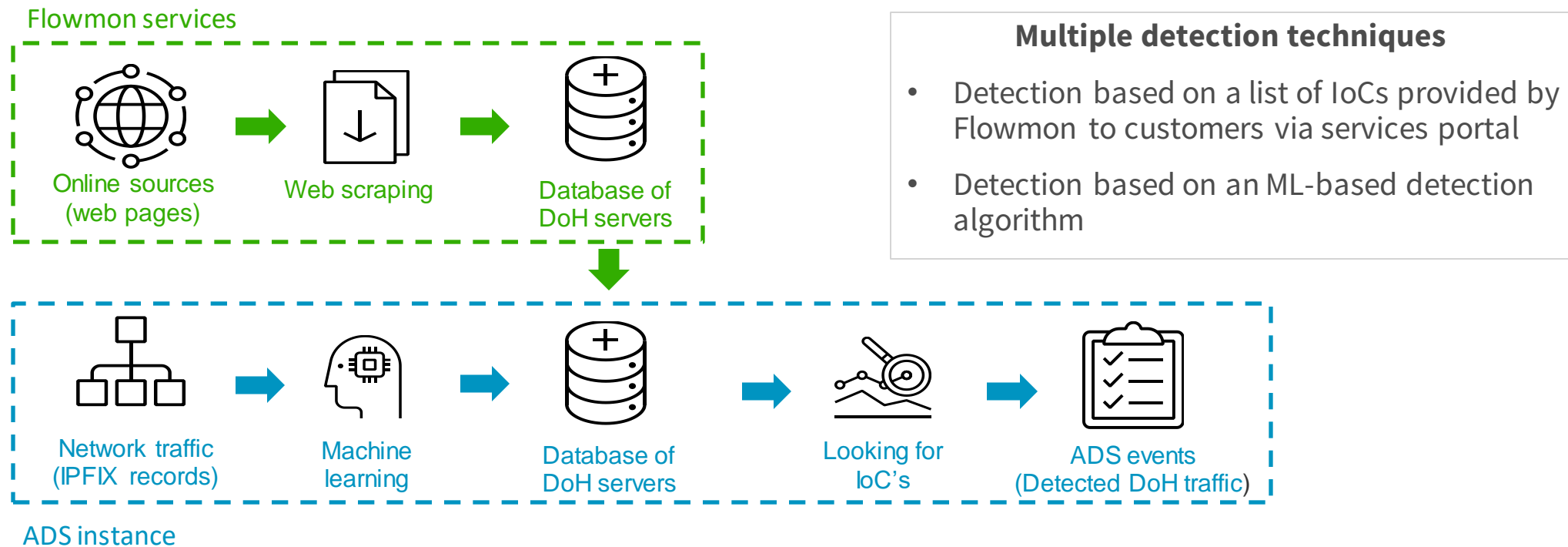
**These roadmaps may not be interpreted as any commitment on behalf of Progress, and future development, timing and release of any features or functionality described in the roadmaps remains at our sole discretion**

# Flowmon ADS 12.1 – est. Q1/2023

## Encrypted Traffic Analysis

Our new detection methods will uncover encrypted DNS servers attempting to hide from network monitoring tools

- **Detection of DNS over HTTPS (DoH)**



# Flowmon 13.0 – New Collector engine

## New collector backend engine

- Completely new collector backend engine respects the most modern trends and will bring **higher performance** (est. 2x – 7x) by usage of massive parallelization and lot of other improvements
- **Flexible design** allows us to easily support various IPFIX flow items useful for different monitoring use-cases

### Speciální pole (proprietary fields) pro Flowmon (IPFIX)

#### POLE PROTOKOLU DATABÁZE

- |   |  |  |
|---|--|--|
| <input type="checkbox"/> MSSQL pole           | <input checked="" type="checkbox"/> MySQL pole           | <input type="checkbox"/> PostgreSQL pole           |
| <input type="checkbox"/> MSSQL rozšířená pole | <input checked="" type="checkbox"/> MySQL rozšířená pole | <input type="checkbox"/> PostgreSQL rozšířená pole |

#### OSTATNÍ POLE

- |  |   |  |
|--|---|--|
| <input checked="" type="checkbox"/> DHCP pole            | <input checked="" type="checkbox"/> Pole e-mailu                            | <input checked="" type="checkbox"/> Pole ARP |
| <input checked="" type="checkbox"/> DNS pole             | <input checked="" type="checkbox"/> Samba pole                              | <input type="checkbox"/> VXLAN               |
| <input checked="" type="checkbox"/> L3/L4 rozšířená pole | <input checked="" type="checkbox"/> Časová známka toku přijatého kolektorem |  |

### Speciální pole (proprietary fields) pro CISCO (IPFIX)

- |                                      |  |                                   |
|--------------------------------------|--|-----------------------------------|
| <input type="checkbox"/> AVC metriky | <input type="checkbox"/> AVC histogram | <input type="checkbox"/> AVC HTTP |
|--------------------------------------|--|-----------------------------------|

### Speciální pole (proprietary fields) pro Gigamon (IPFIX)

- |  |                              |                                 |
|--|------------------------------|---------------------------------|
| <input type="checkbox"/> HTTP Host a URL | <input type="checkbox"/> SSL | <input type="checkbox"/> RADIUS |
| <input type="checkbox"/> DNS             |                              |                                 |

### Speciální pole (proprietary fields) pro VMware (IPFIX)

- NSX

### Speciální pole (proprietary fields) pro IXIA (IPFIX)

- HTTP Host a URL



# Flowmon 13.0 – Prediction & trending

## Prediction and trending

- Information about current and past situations in the network is not enough any more
- Predicting the future allows IT professionals to react proactively and to be prepared
- Predictions and trends will be available for both volumetric data and network performance metrics
- This will proactively help with situations like upcoming link saturation or gradual SLA degradations



# Flowmon ADS 13.0 – est. Q4/2023

## Flowmon ADS 13.0

Full multitenancy support

Anomaly detection for ICS/SCADA environments with a new set of detection methods

Improved detection accuracy and proxy correlation by adopting a new collector backend engine



