

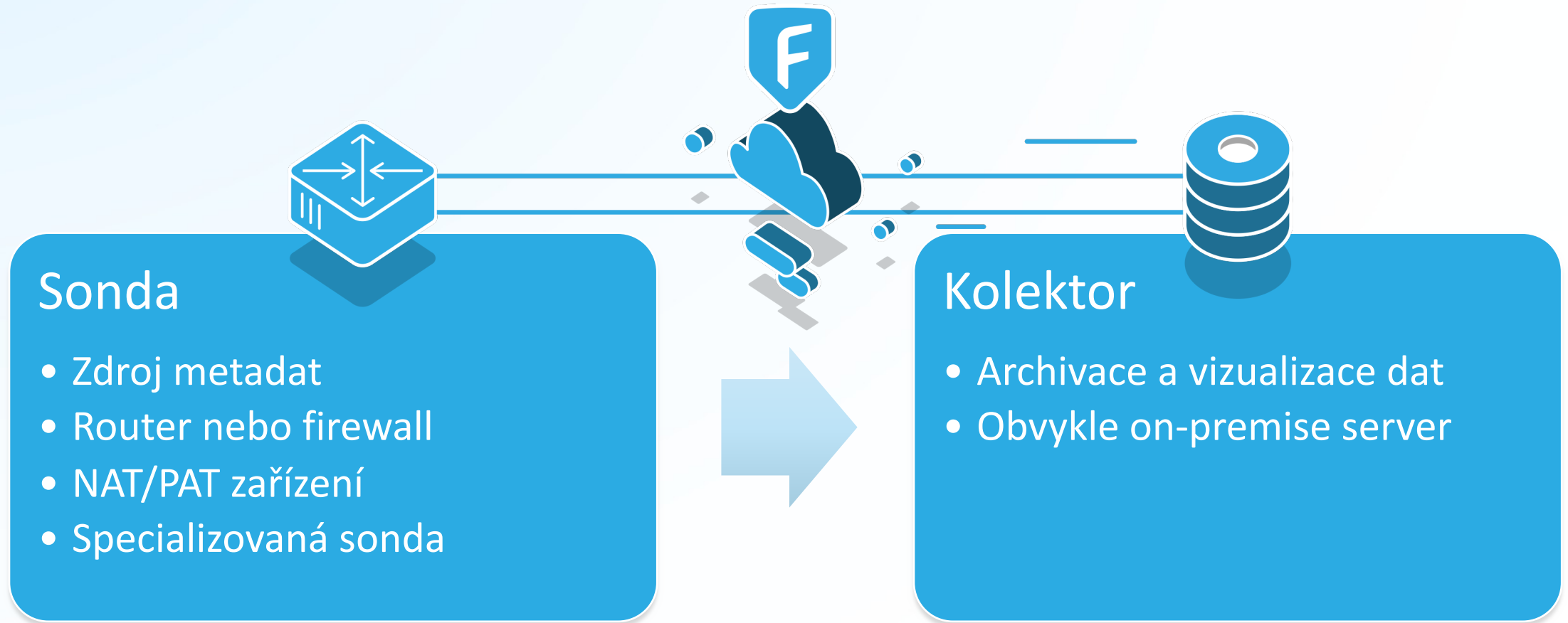


Nový pohled na využití Data Retention řešení pro ISP

Petr Kadlec, ComSource



DR - metadata o síťovém provozu



Date, Time, Protocol, SrcIP, DstIP, SrcPort, DstPort, TCP flags, TTL, Packets, Octets, ToS, Iniface, Outiface, SrcAS, DstAS, etc.

Využití metadat o síťovém provozu



Tradiční

- Legislativní povinnost pro ztotožnění IP adres
- Reporting síťového provozu

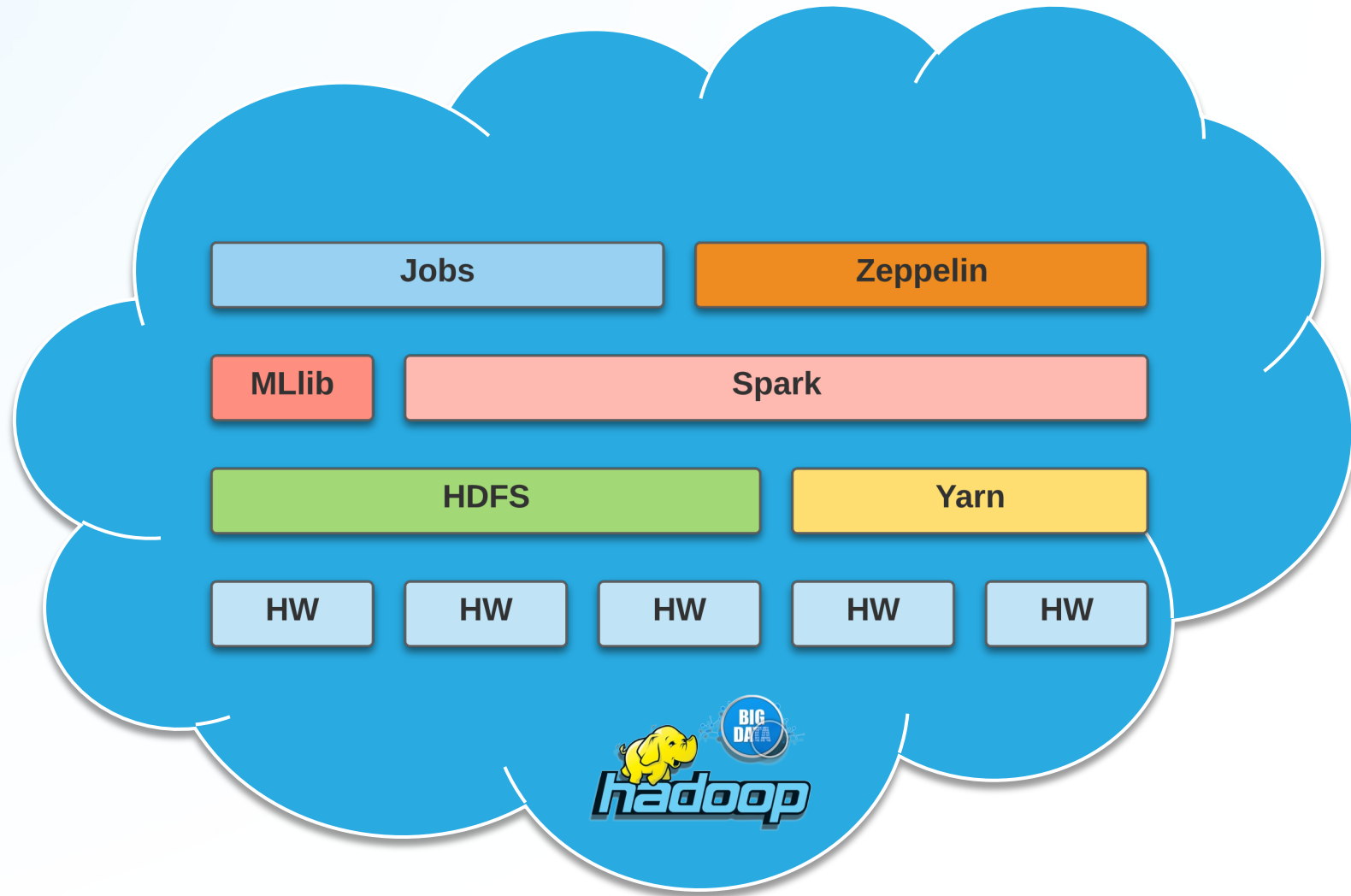
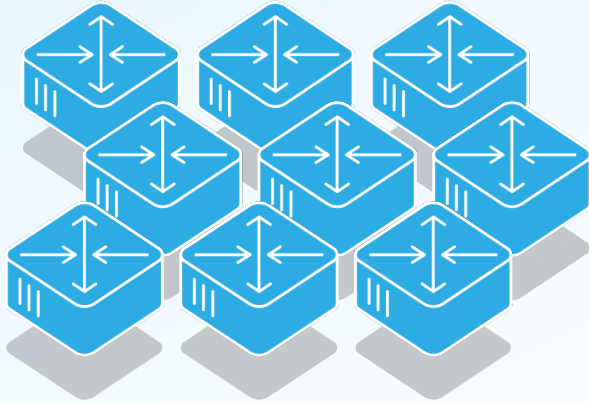


Progresivní

- Troubleshooting
- Forenzní analýza
- Bezpečnost sítě
- Automatizace správy sítě
- Data Driven Company



Architektura FlowGuard DR



Data Pipeline FlowGuard DR



portal.flowguard.io

COMS-0001 Dashboard Monitoring Firewall IP Prefixes Statistics Data Retention Reports

Data Retention

Search Results

Search From: 13.7.2021, 11:00 Search To: 13.7.2021, 12:00

Source IP: Destination IP: 8.8.8.8

Source Port: Destination Port:

Protocol: UDP

Search



portal.flowguard.io

COMS-0001 Dashboard Monitoring Firewall IP Prefixes Statistics Data Retention Reports

Data Retention

Search Results

Search Request

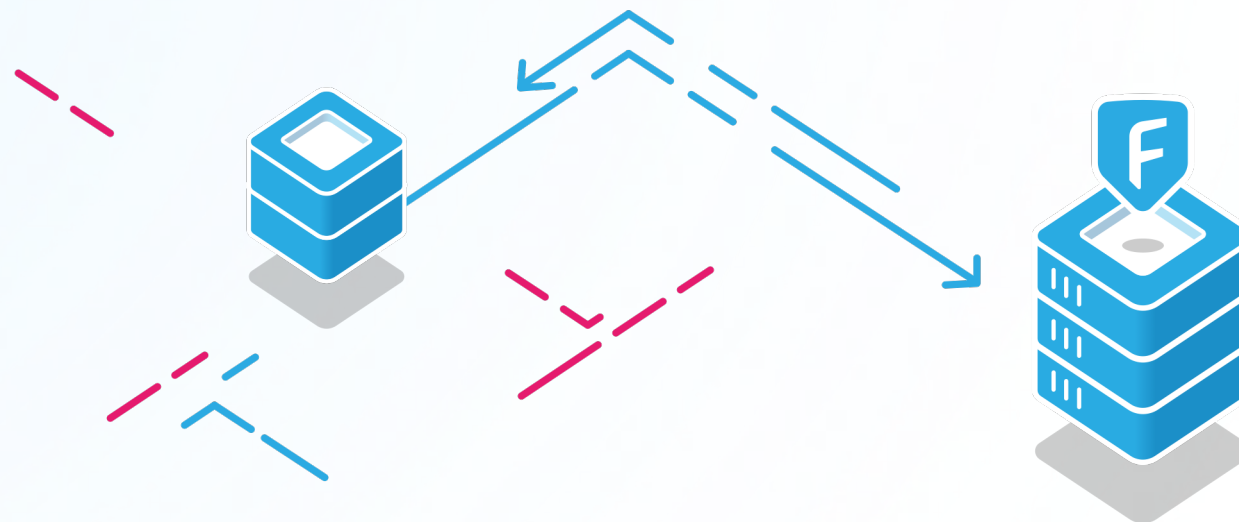
Status	completed
From	2021-07-13 11:00
To	2021-07-13 12:00
Source IP	
Source Port	
Destination IP	8.8.8.8
Destination Port	
Protocol	

Back Download

Start time	End time	Client		Public source		Destination		Protocol
		Address	Port	Address	Port	Address	Port	
13.7.2021, 11:15:06	13.7.2021, 11:15:10	192.168.168.30	47295	185.45.202.2	38559	8.8.8.8	53	UDP
13.7.2021, 11:15:11	13.7.2021, 11:15:15	192.168.168.30	54007	185.45.202.2	35604	8.8.8.8	53	UDP
13.7.2021, 11:15:11	13.7.2021, 11:15:15	192.168.168.30	40736	185.45.202.2	35189	8.8.8.8	53	UDP
13.7.2021, 11:15:11	13.7.2021, 11:15:15	192.168.168.30	55911	185.45.202.2	61805	8.8.8.8	53	UDP
13.7.2021, 11:15:11	13.7.2021, 11:15:15	192.168.168.30	34554	185.45.202.2	57011	8.8.8.8	53	UDP



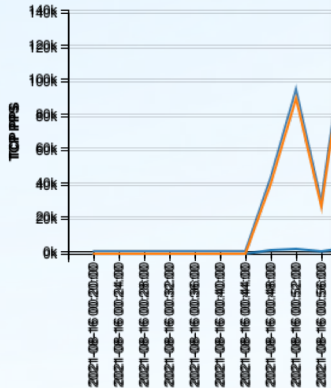
FlowGuard
Data retention



Příklady dalšího možného využití



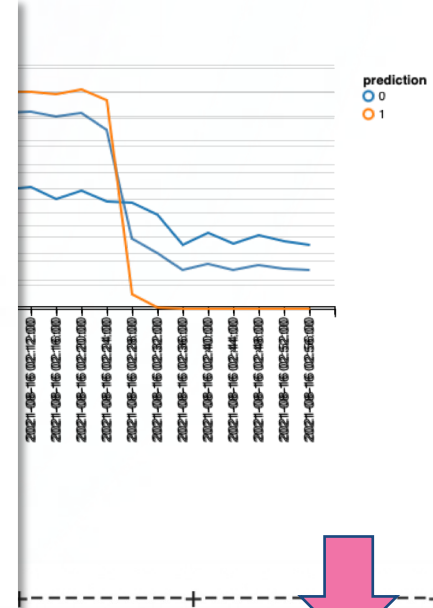
Příklad 1: Forenzní analýza a troubleshooting



```
%spark
import org.apache.spark.ml.clustering.BisectingKMeans
import org.apache.spark.ml.feature.StandardScaler

val k = 2
val cols = Array("pktSizeAvg", "pkts2flow", "pkts", "pctNoEndFlows")
val assembler = new VectorAssembler().setInputCols(cols).setOutputCol("featuresNS")
val inputML = assembler.transform(demo2)

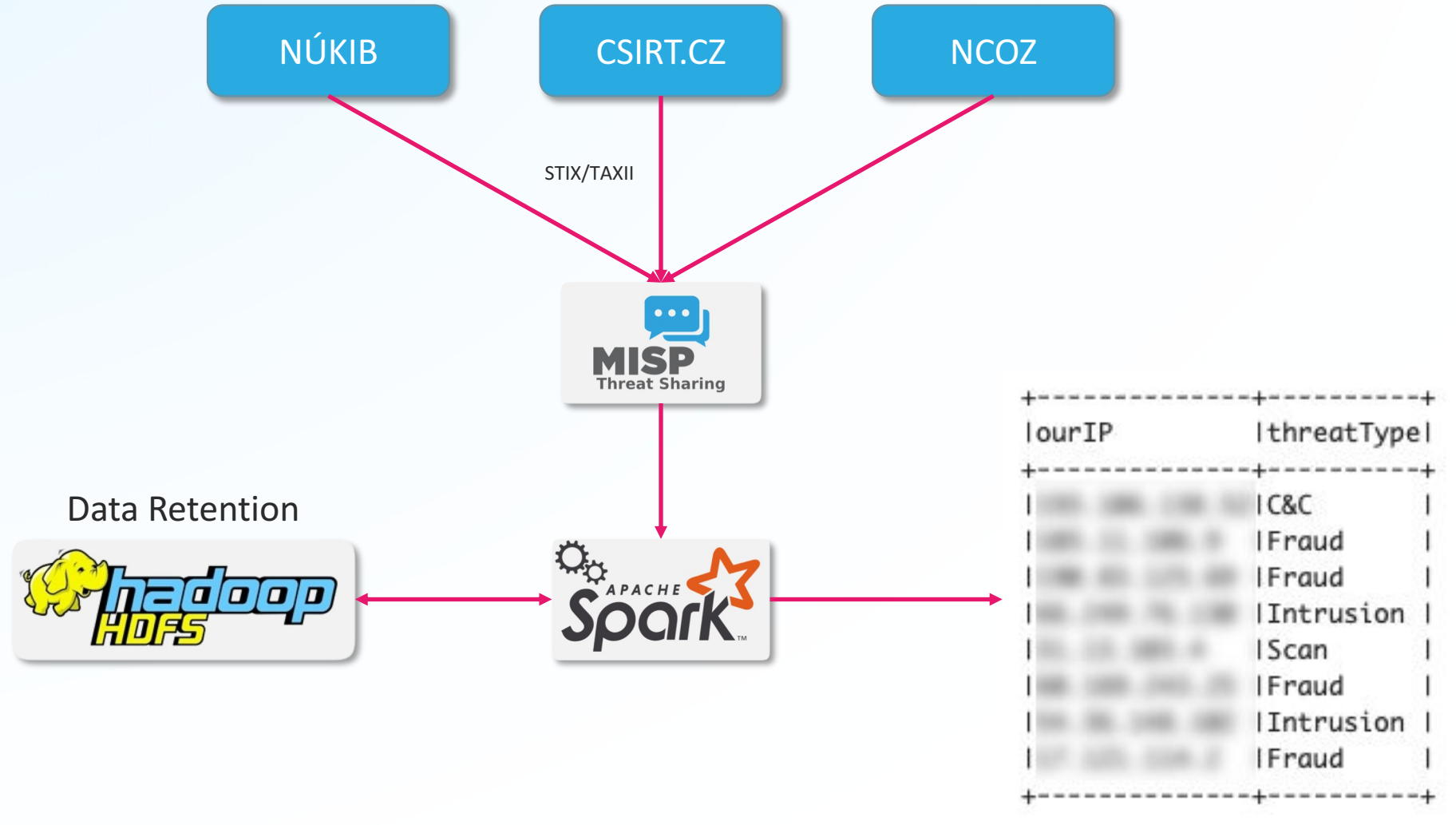
val scaler = new StandardScaler()
  .setInputCol("featuresNS")
  .setOutputCol("features")
  .setWithStd(true)
  .setWithMean(false)
```



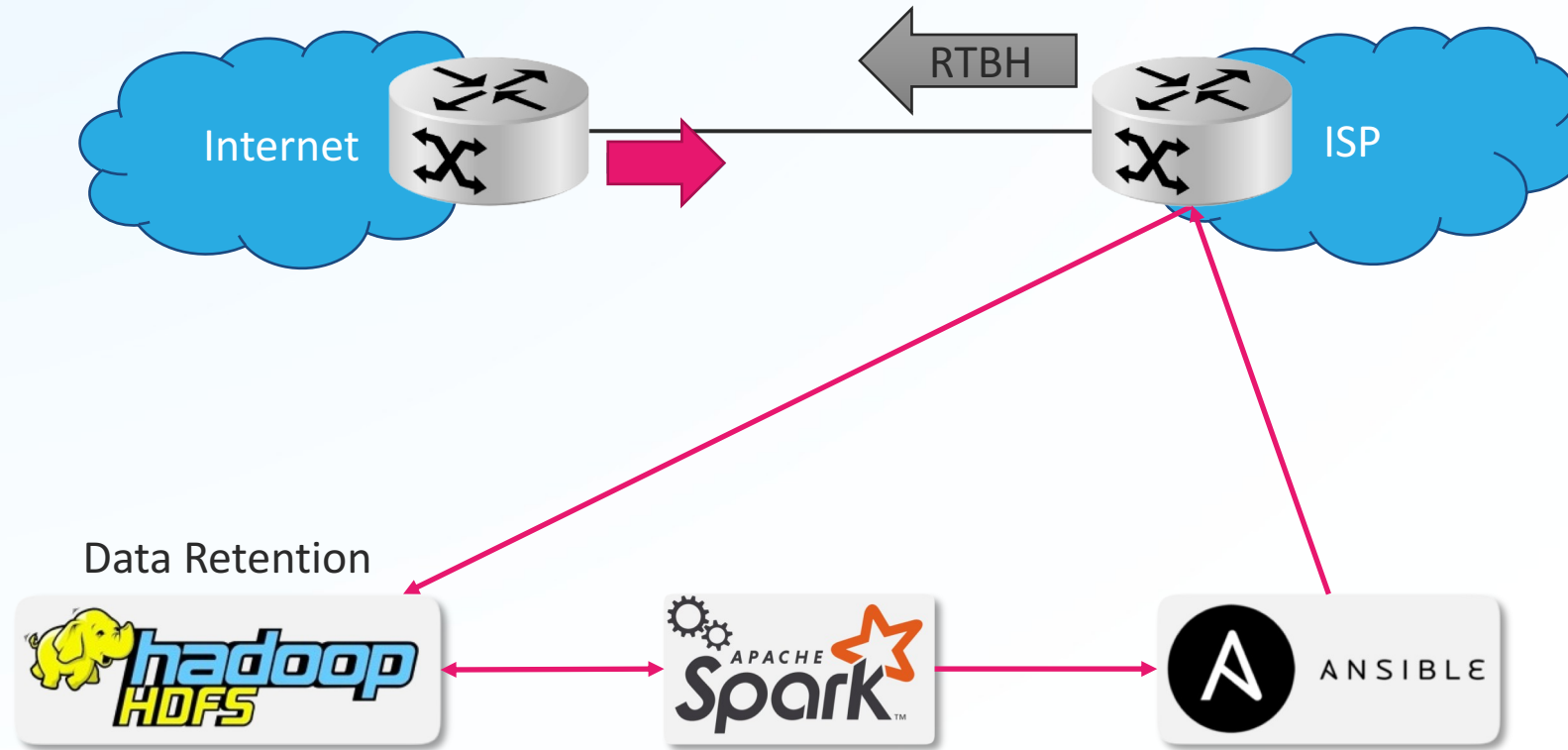
srcIP	pkts	bytes	flows	noEndFlows	flowTimeAvg	ttlVarAvg	ttlAvg	ttlDistanceAvg	lastTimeStamp	pktSizeAvg	pkts2flow	pctNoEndFlows	prediction
193.106.138.52	1975556	946096578	58363	451	7097.0	0.0	57.0	7.0	1629073547264	479.0	34.0	0.77	1
103.11.106.9	930021	387386609	60454	103	6856.0	0.0	51.0	13.0	1629073610496	417.0	15.0	0.17	1
190.83.125.69	1708	484065	117	3	6444.0	0.0	54.0	10.0	1629073457152	283.0	15.0	2.56	0
66.249.76.130	5	496	1	0	71424.0	0.0	111.0	17.0	1629071308544	99.0	5.0	0.0	0
31.13.103.4	20	2518	4	0	7360.0	0.0	82.5	46.0	1629070859008	126.0	5.0	0.0	0
60.169.243.25	4	1319	1	1	256.0	0.0	52.0	12.0	1629068415744	330.0	4.0	100.0	0
54.36.148.102	18	1647	7	4	366.0	0.0	56.0	8.0	1629073426176	92.0	3.0	57.14	0
17.121.114.2	3	502	1	1	0.0	0.0	49.0	15.0	1629072427264	167.0	3.0	100.0	0
114.119.153.112	3	548	1	1	0.0	0.0	46.0	18.0	1629072275968	183.0	3.0	100.0	0
190.83.125.91	3	610	1	1	256.0	0.0	54.0	10.0	1629070851328	203.0	3.0	100.0	0

only showing top 10 rows

Příklad 2: Threat Intelligence



Příklad 3: Automatizace



Závěrečné shrnutí

- Rodina služeb FlowGuard se rozrostla
 - Infrastructure Protection (Anti DDoS)
 - Website Protection (Anti DDoS)
 - **Data Retention** (DR v cloudu jako služba, monitoring a automatizace)
 - **Threat Intelligence** (MISP + Reputation Database)
- Využijte svá data
 - Nastala **doba datová**, kdo je neumí využívat, mává ujíždějícímu vlaku
 - Data Retention = **nejlevnější cesta** k informacím (refundace státem)
 - Bud'te **Data Driven Company** i ve smyslu provozních dat
 - Hledejte nové **Use Cases**, my vám je pomůžeme zrealizovat





Děkuji za pozornost

Email: petr.kadlec@comsource.cz

Tel: 774 744 725

