

NIL





mag. Damijan Markovič



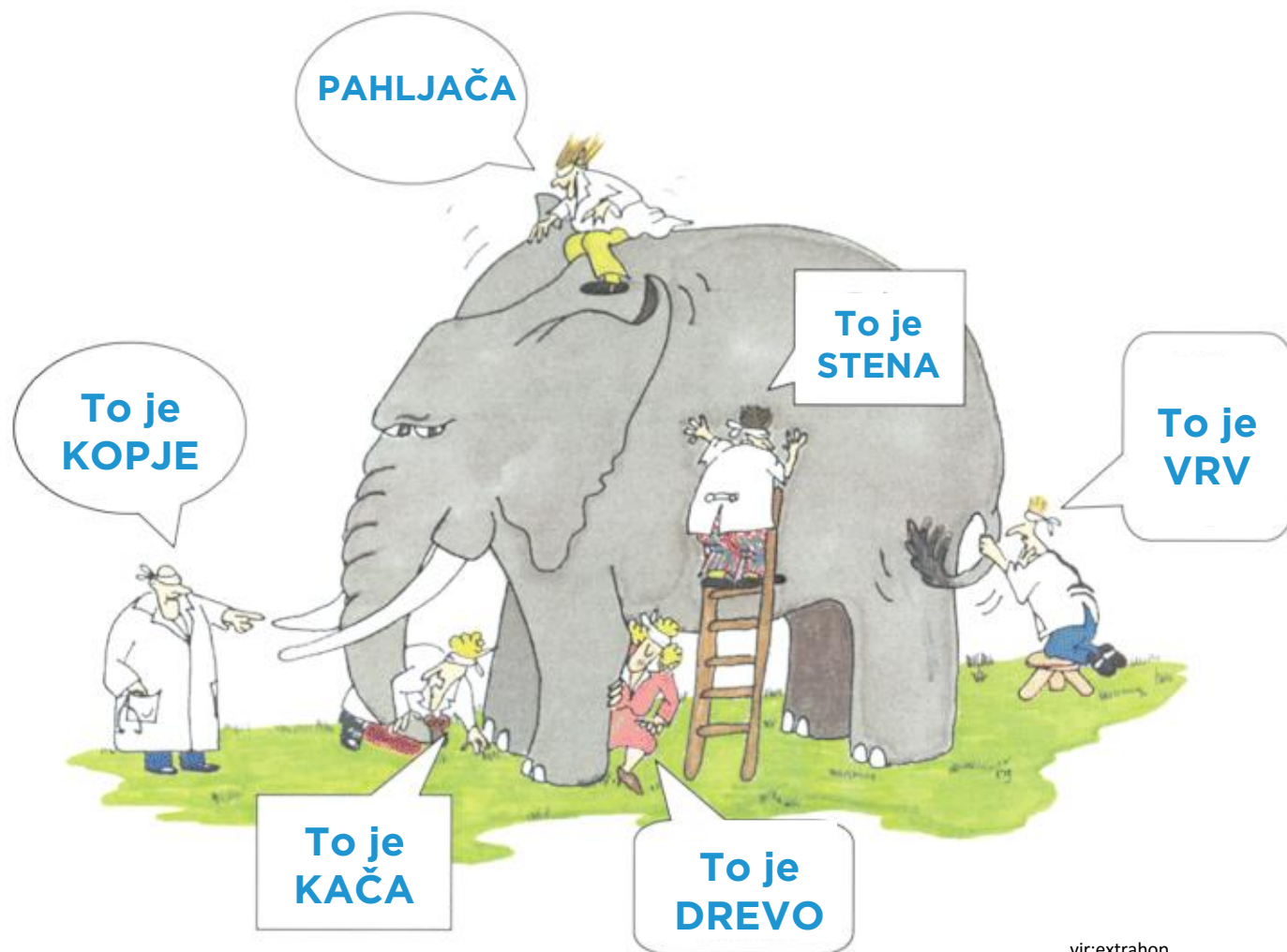
APLIKACIJA DELA POČASI, SPET TA MREŽA. ALI RES?

- Nadzorni sistemi
 - Agenti, ki simulirajo delovanje
 - Vedno ne odražajo dejanskega stanja
- Obveščanje preko uporabnikov



vir:youtube.com



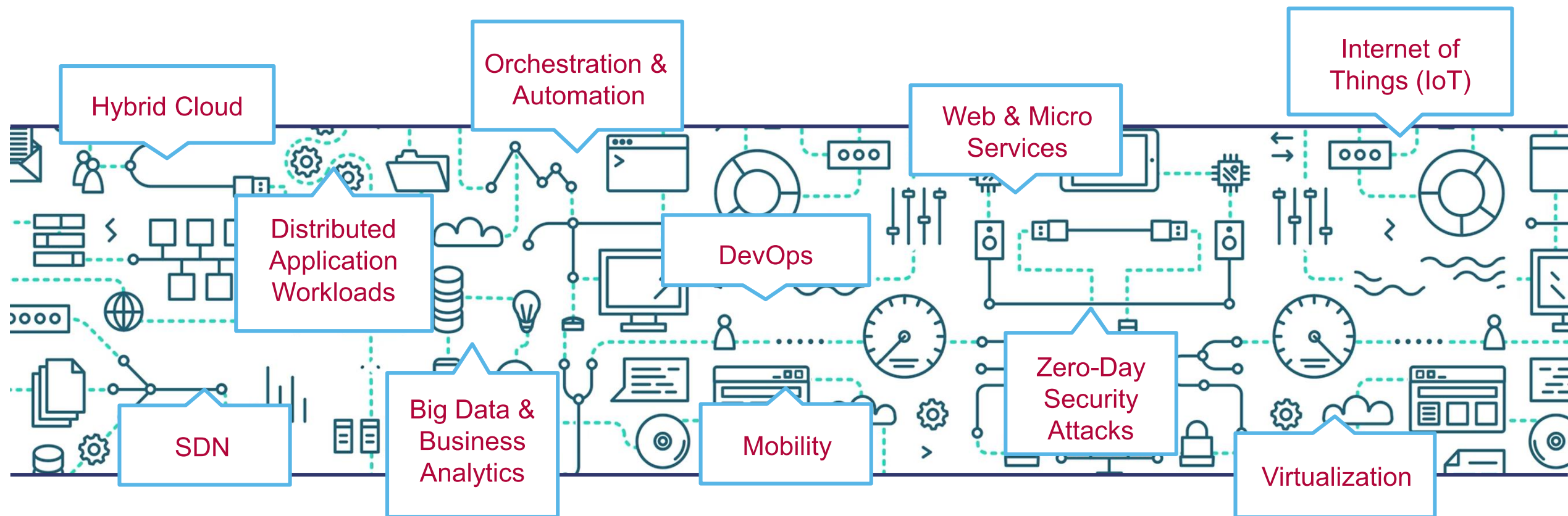


vir:extrahop

- Vsak tim pregleduje svoje okolje
- Vsak tim je omejen s svojim področjem
- „Pri nas ni videti težav!„
- **„Zagotovo je nekaj na omrežju!“**



- Poslovno okolje zahteva nove storitve in nove aplikacije
- Vse več medsebojnega sodelovanja med aplikacijami (Web - App - DB)



Ročno pregledovanje:

- Ping
- TraceRT

Zajemanje podatkov:

- Wireshark
- TCPdump

Poznavanje delovanja aplikacij

No.	Time	Source	Destination	Protocol	Length
708	13.650579	192.168.1.77	173.194.33.6	TCP	54
709	13.662945	173.194.33.6	192.168.1.77	TCP	60
710	13.995895	Actionte_d8:a3:88	Msi_74:82:e6	ARP	60
711	13.995922	Msi_74:82:e6	Actionte_d8:a3:88	ARP	42
712	15.030559	fe80::bdca:e67b:5eb7:1ff02::c		SSDP	200
713	15.058140	192.168.1.76	239.255.255.250	UDP	50
714	15.123002	192.168.1.74	239.255.255.250	UDP	56
715	17.628874	192.168.1.77	208.43.115.82	TCP	60
716	17.711021	208.43.115.82	192.168.1.77	TCP	60

Frame 1: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits)
Ethernet II, Src: Msi_74:82:e6 (00:16:17:74:82:e6), Dst: Actionte_d8:a3:88 (08:00:27:08:00:27)
Internet Protocol Version 4, Src: 192.168.1.77 (192.168.1.77), Dst: 72.165.67.144 (72.165.67.144)
User Datagram Protocol, Src Port: 53691 (53691), Dst Port: 27017 (27017)
Data (84 bytes)



Omrežje
dela BP



Odkrivanje (Discover)

Neprestano
pregledovanje in
kategoriziranje
omrežnega prometa



Opazovanje (Observe)

Spremljanje
aktivnih sej
v realnem času



Analiziranje (Analyze)

Analiza in **prikazovanje**
ključnih podatkov



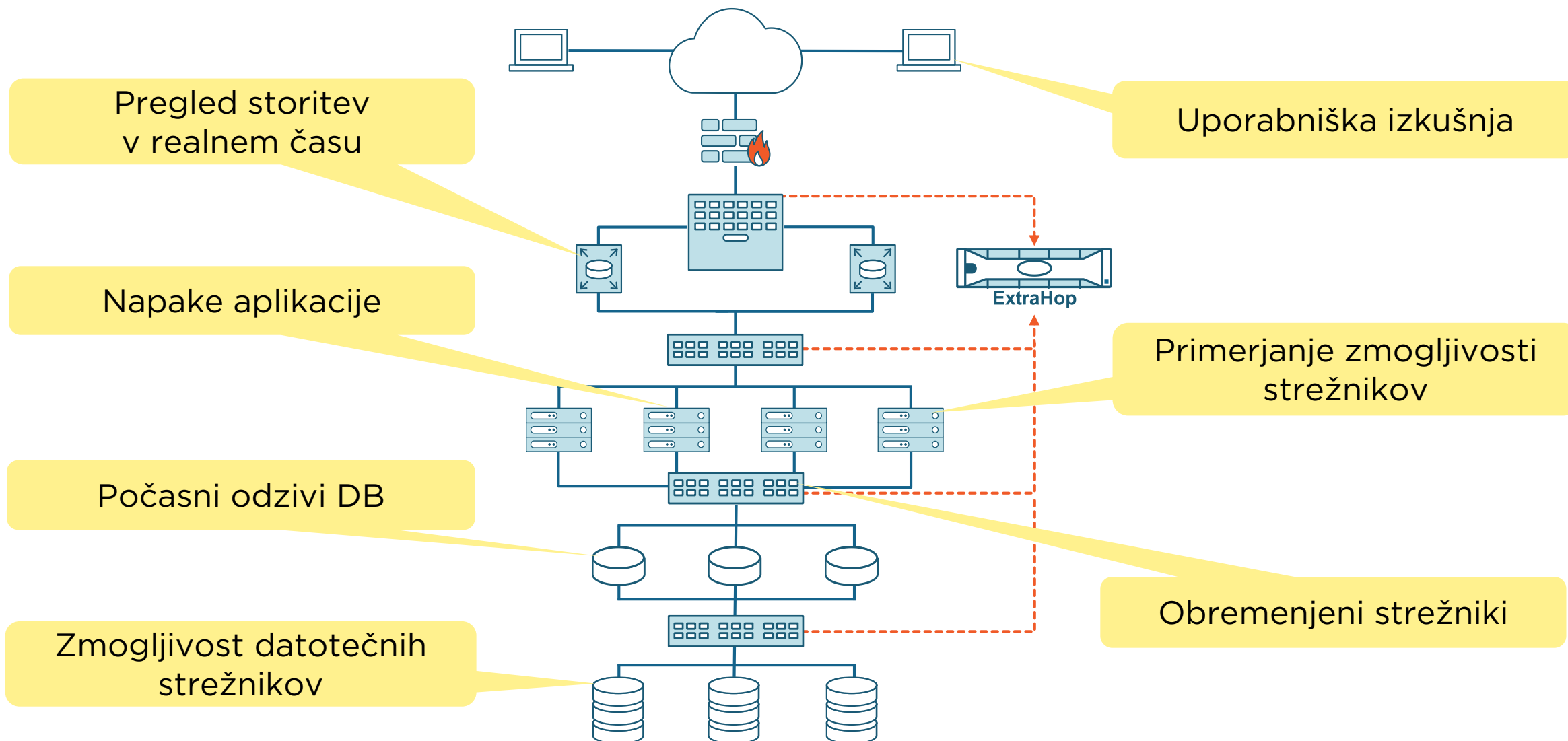
Z analitiko prometnih tokov se podatki na omrežju spremenijo v poslovne informacije

Neurejeni podatki v omrežju...



... v strukturirano obliko

```
9/11/12                                xml-request.txt
1  <?xml version="1.0" encoding="UTF-8"?>
2  <Request>
3    <NewOrder>
4      <OrbitalConnectionUsername>TESTUSER123</OrbitalConnectionUsername>
5      <OrbitalConnectionPassword>abcd1234</OrbitalConnectionPassword>
6      <IndustryType>EC</IndustryType>
7      <MessageType>AC</MessageType>
8      <BIN>000001</BIN>
9      <MerchantID>123456</MerchantID>
10     <TerminalID>001</TerminalID>
11     <CardBrand></CardBrand>
12     <AccountNum>5454545454545454</AccountNum>
13     <Exp>0112</Exp>
14     <CurrencyCode>840</CurrencyCode>
15     <CurrencyExponent>2</CurrencyExponent>
16     <AVSzip>25541</AVSzip>
17     <AVSAddress1>123 Test Street</AVSAddress1>
18     <AVSAddress2>Suite 350</AVSAddress2>
19     <AVScity>Test City</AVScity>
20     <AVSstate>FL</AVSstate>
21     <AVSphoneNum>8004564512</AVSphoneNum> <OrderID>8316384413</OrderID>
22     <Amount>2500</Amount>
23   </NewOrder>
24 </Request>
25
```



Uporaba

- N/APM (Network/Application Performance Monitor)
- Varnost

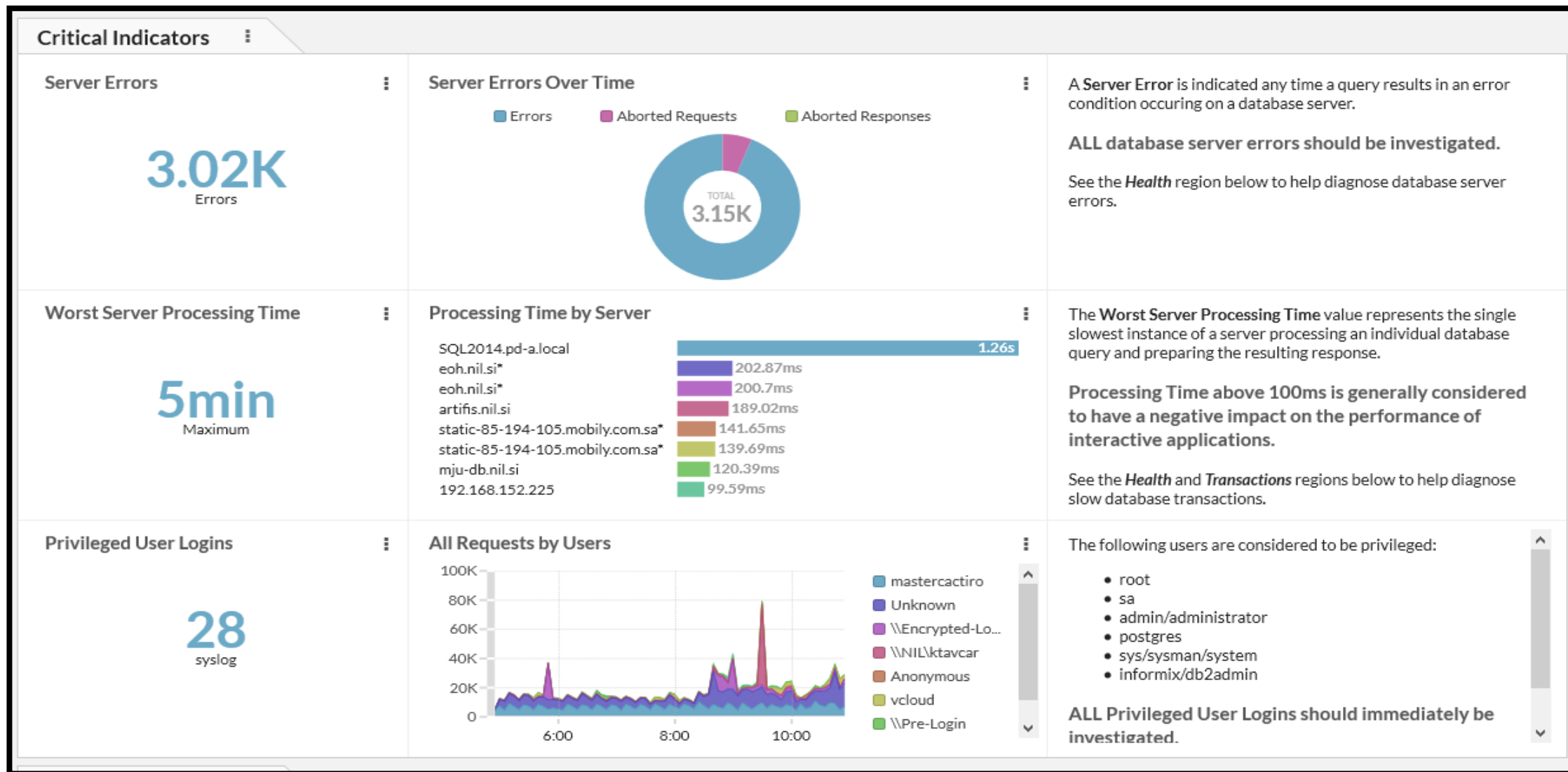
Orodje za:

- Administratorje omrežja
- Administratorje aplikacij/storitev
- Vodje

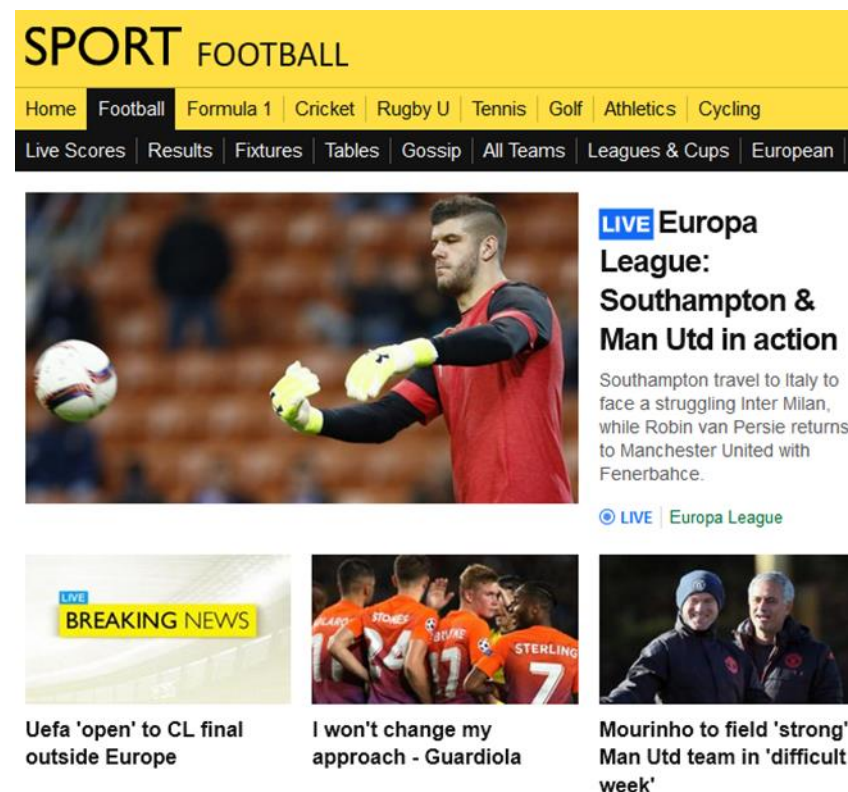
Področja

- Vladne institucije
- Finančne ustanove
- Bolnice
- Proizvodnja





- Prikaz spletne strani deluje počasi
- Povprečna spletna stran
 - Vsebina iz različnih strežnikov
 - 5-20 poizvedb v DNS
- Razlog se lahko skriva v storitvi strežnika DNS



Key DNS performance indicators (Region 1 of 4)

DNS Response Errors

24.9K
Errors

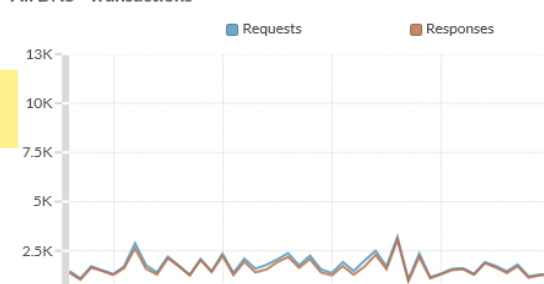
DNS errors over processing time



Zahtev DNS brez odgovora

10.9K
Request Timeouts

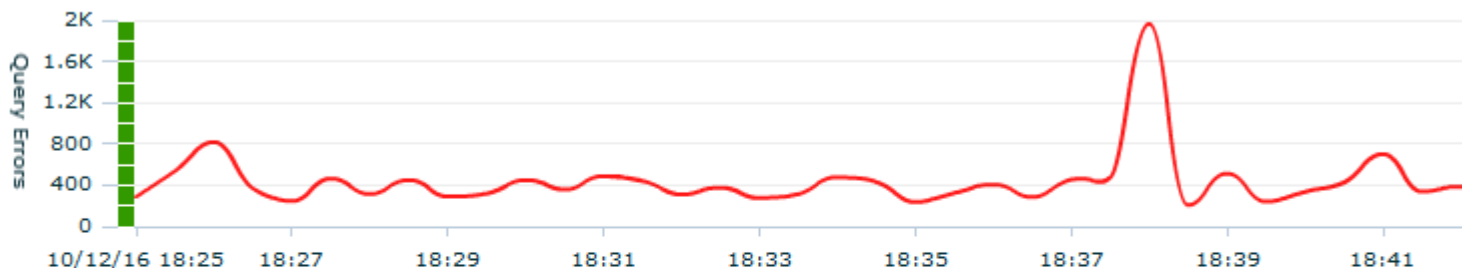
All DNS - Transactions



Zahtev DNS

127K
Requests

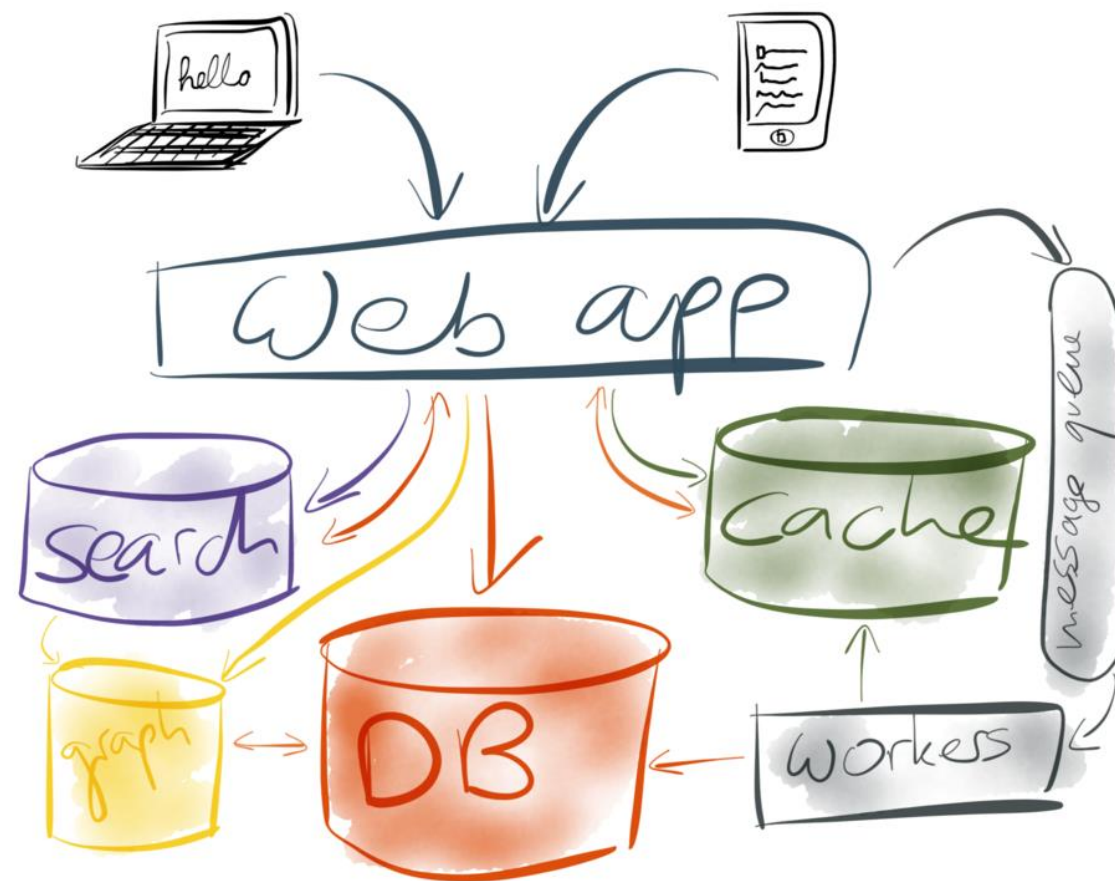
All Hosts



Host	Query Errors
nil-multi-sensor-test1.alienvault.cloud	1,500
gettingstarted.alienvault.cloud	1,457
salt	1,377

Record Type	Client	Client IPv4 Address	Server	Server IPv4 Address	Opcode	Query Name	Query Type
DNS Request	Cisco 20D316	193.110.145.101	google-public-dns-a.google.com	8.8.8.8	QUERY	gettingstarted.alienvault.cloud	A
DNS Request	av-ts.nil.com	192.168.252.165	google-public-dns-a.google.com	8.8.8.8	QUERY	gettingstarted.alienvault.cloud	A
DNS Request	Cisco 20D316	193.110.145.101	google-public-dns-a.google.com	8.8.8.8	QUERY	gettingstarted.alienvault.cloud	A
DNS Request	av-ts.nil.com	192.168.252.165	google-public-dns-a.google.com	8.8.8.8	QUERY	gettingstarted.alienvault.cloud	A

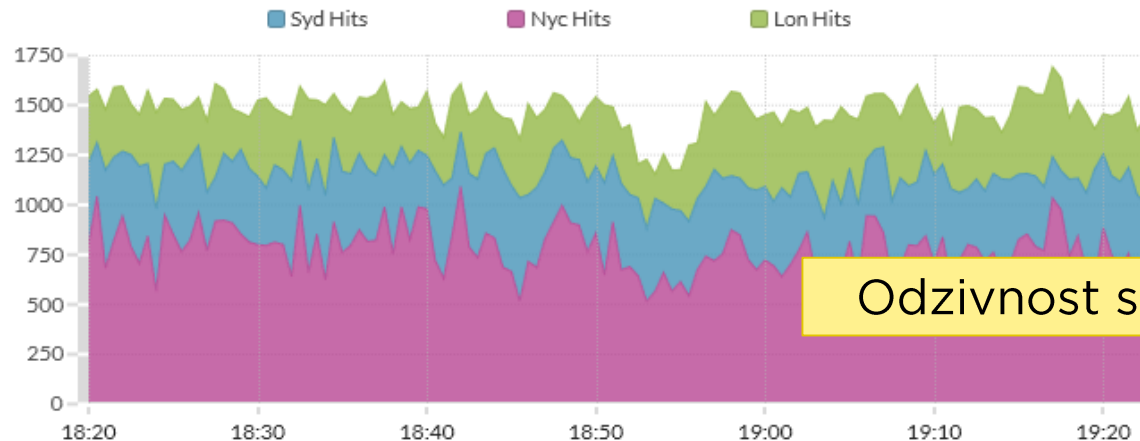
- Uporabniki se pritožujejo nad slabo odzivnostjo interne spletne aplikacije
- Za vsakim spletnim strežnikom je skrita kopica drugih aplikacij



vir: <http://martin.kleppmann.com>

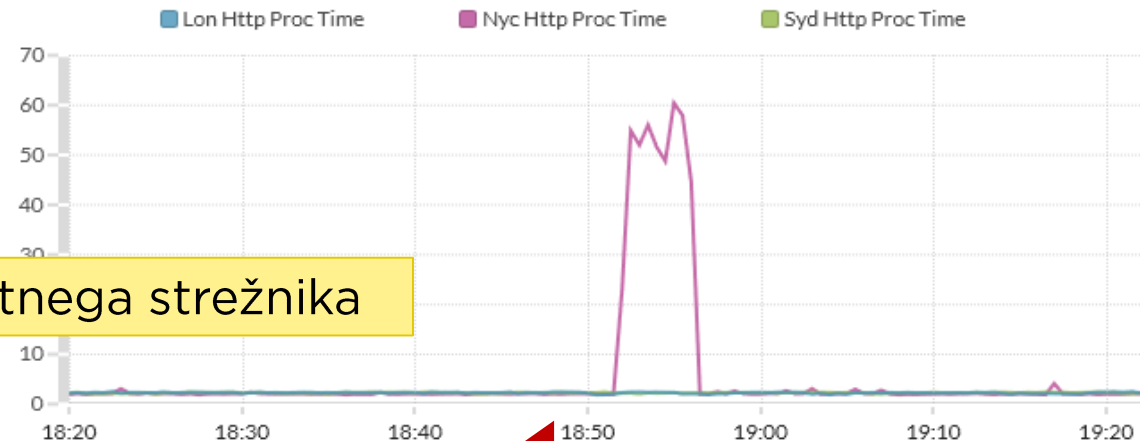
HTTP and Database Health

HTTP Requests by Region

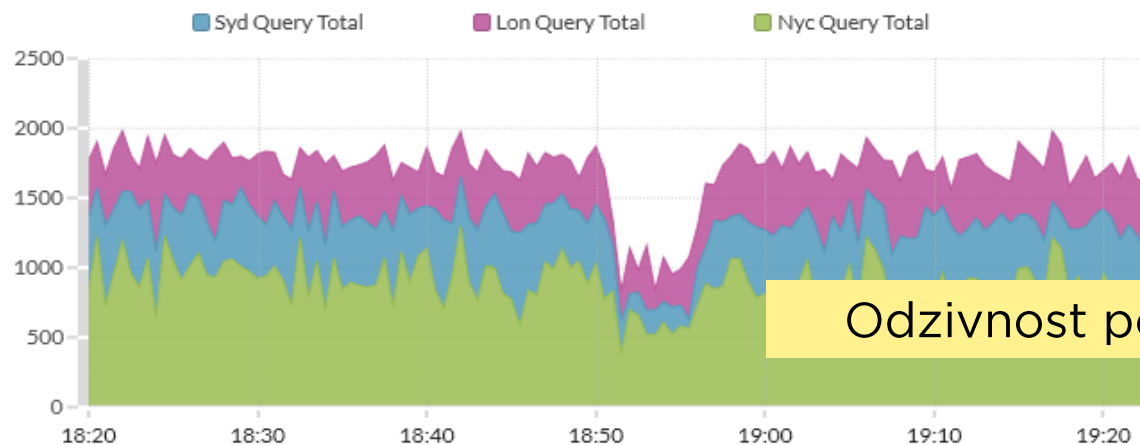


Odzivnost spletnega strežnika

HTTP Processing Time by Region

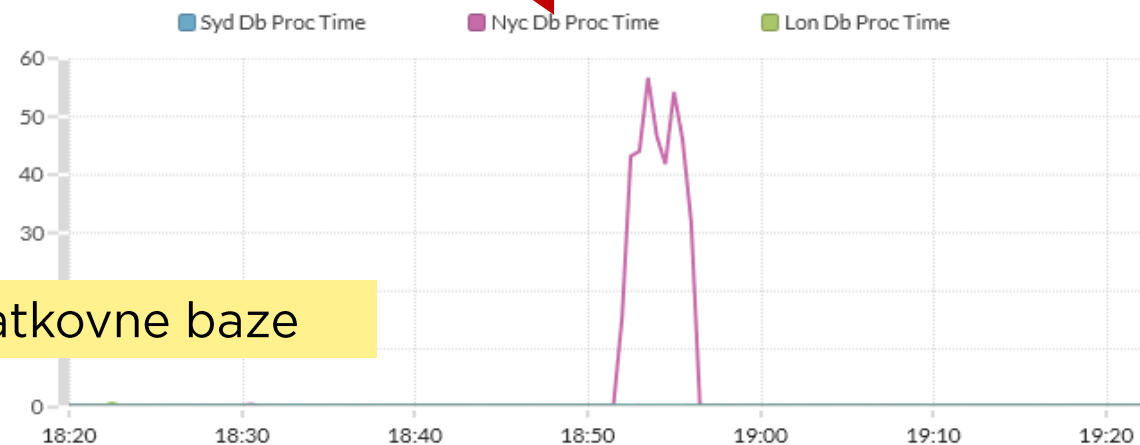


Database Queries by Region



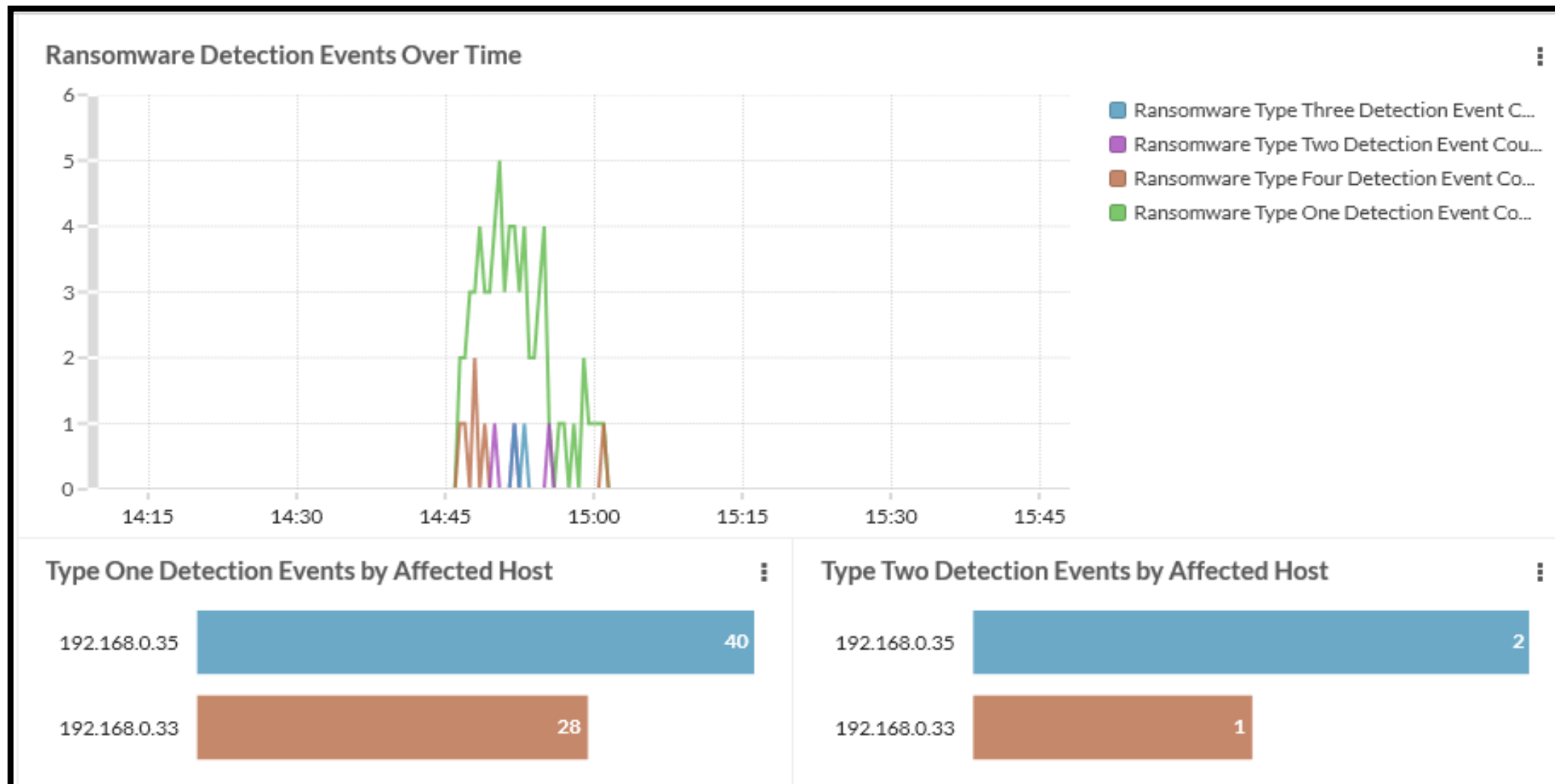
Odzivnost podatkovne baze

Database Processing Time by Region





Client IPv4 A...	Server	Server IPv4 Address	Met...	Er...	Data...	Statement	User	Processing Time
172.22.1.80	mysql1-nyc	172.22.2.33	SELECT	—	ecomapp	SELECT CATID AS categoryId, NAME, DESCN AS description FROM CATEGORY WHERE CATID = 'CATS'	eh	984,818
172.22.1.80	mysql1-nyc	172.22.2.33	SELECT	—	ecomapp	SELECT CATID AS categoryId, NAME, DESCN AS description FROM CATEGORY WHERE CATID = 'DOGS'	eh	733,425
172.22.1.80	mysql1-nyc	172.22.2.33	SELECT	—	ecomapp	SELECT PRODUCTID, NAME, DESCN as description, CATEGORY as categoryId FROM PRODUCT WHERE CATEGORY	eh	524,401
172.22.1.81	mysql1-nyc	172.22.2.33	SELECT	—	—	SELECT CATID AS categoryId, NAME, DESCN AS description FROM CATEGORY WHERE CATID = 'FISH'	—	501,689
172.22.1.81	mysql1-nyc	172.22.2.33	SELECT	—	—	SELECT CATID AS categoryId, NAME, DESCN AS description FROM CATEGORY WHERE CATID = 'FISH'	—	484,997
172.22.1.81	mysql1-nyc	172.22.2.33	SELECT	—	ecomapp	SELECT CATID AS categoryId, NAME, DESCN AS description FROM CATEGORY WHERE CATID = 'DOGS'	eh	478,402



- Enostaven uporabniški vmesnik
- Širši pogled na dogajanje v omrežju
- Hitrejši čas za odpravo napake (MTTR)
- Boljša uporabniška izkušnja
- Dodatni varnostni mehanizmi





dmarkovic@nil.com