



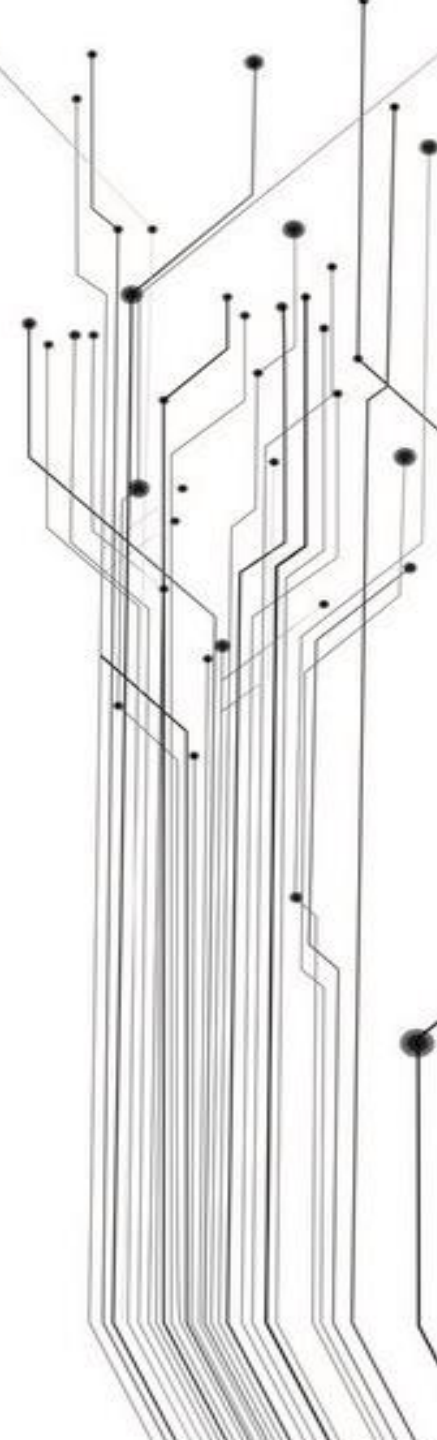
Jihomoravský kraj



KYBERNETICKÉ OPERAČNÍ CENTRUM

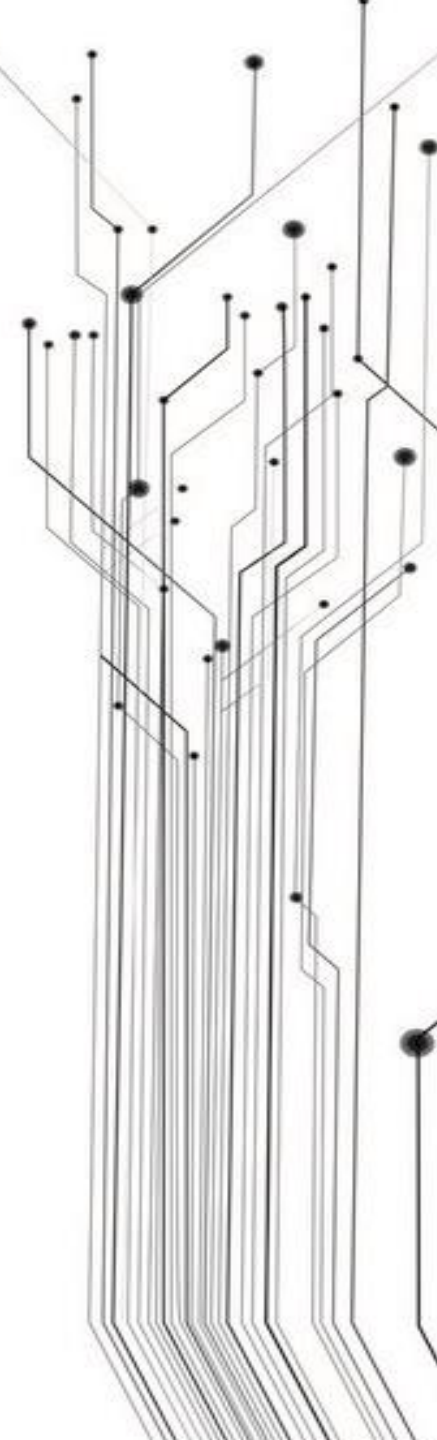
Den klastrů v Jihomoravském kraji
Aleš Staněk

12. 4. 2017

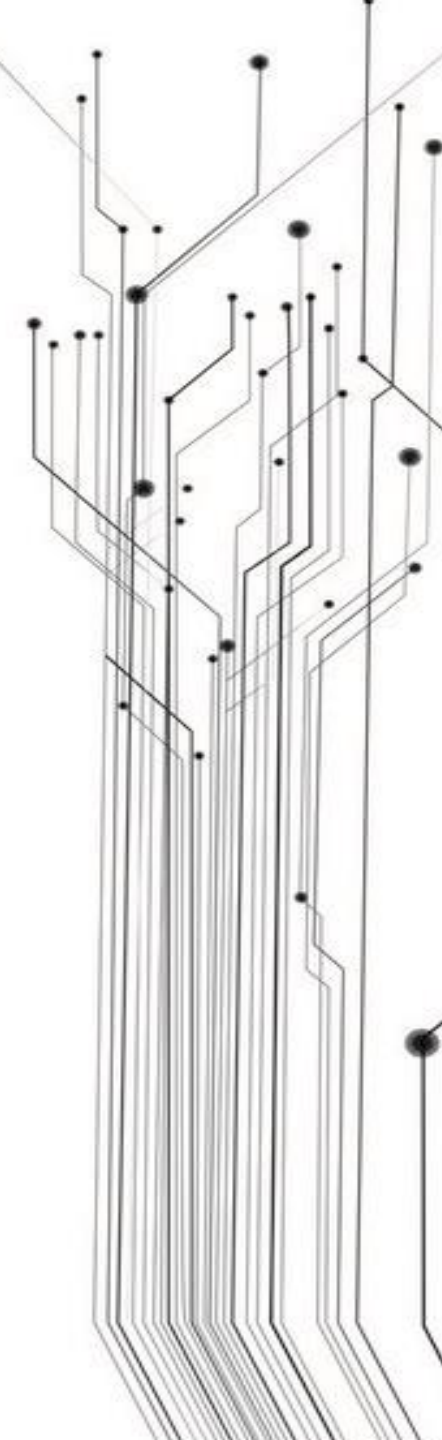


Zákon o kybernetické bezpečnosti 181/2014 Sb.

- ▶ Jihomoravský kraj je správcem 5 významných informačních systémů
- ▶ Zákon mimo jiné ukládá za povinnost detekovat bezpečnostní události
- ▶ Vybudováním bezpečnostního dohledového centra náš kraj plní vše, co je vyžadováno Zákonem o KB.
- ▶ KOC a je značka neboli brand našeho kraje

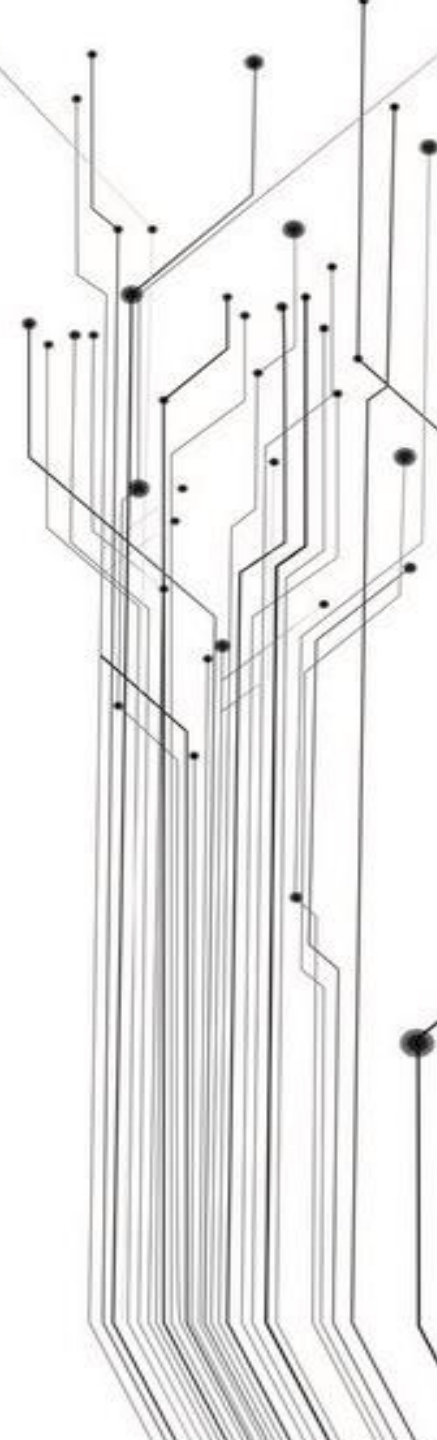
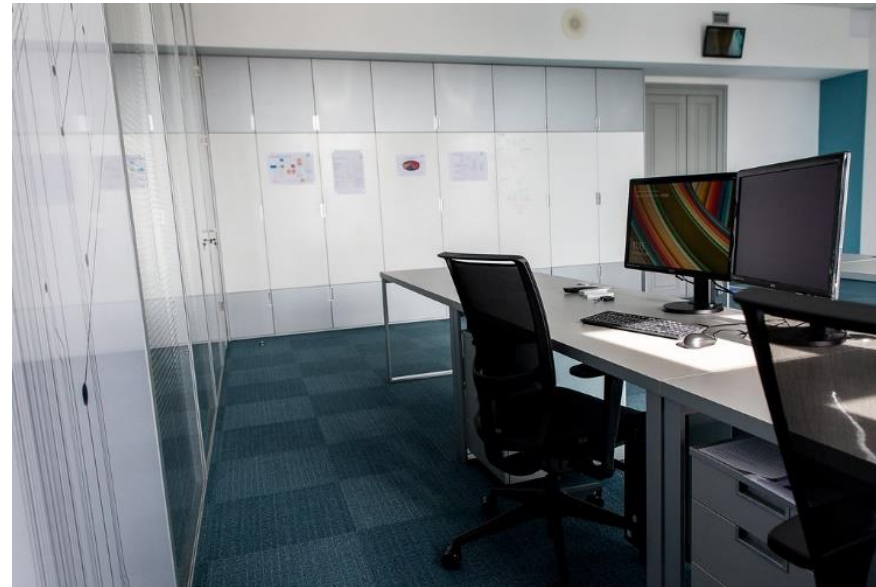


Předání do provozu 09/2016

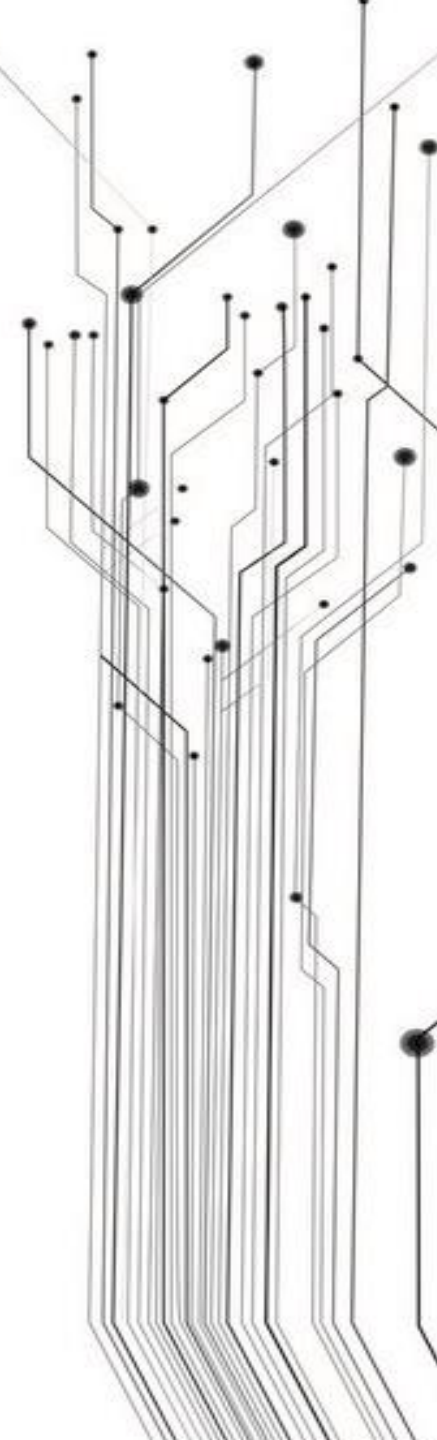
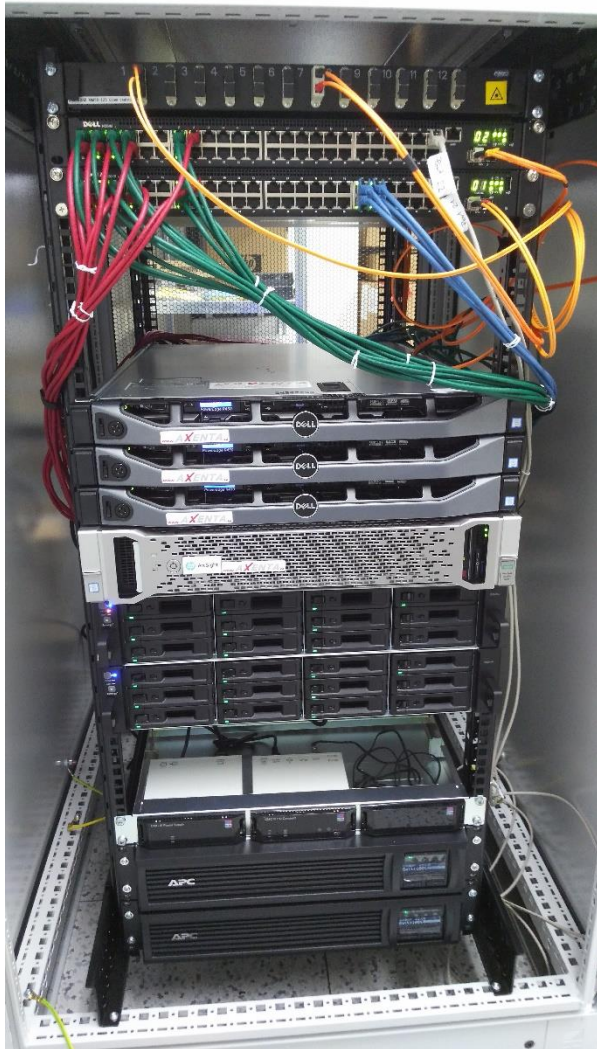


4

V historické budově Krajského úřadu vzniklo moderní dohledové bezpečnostní centrum

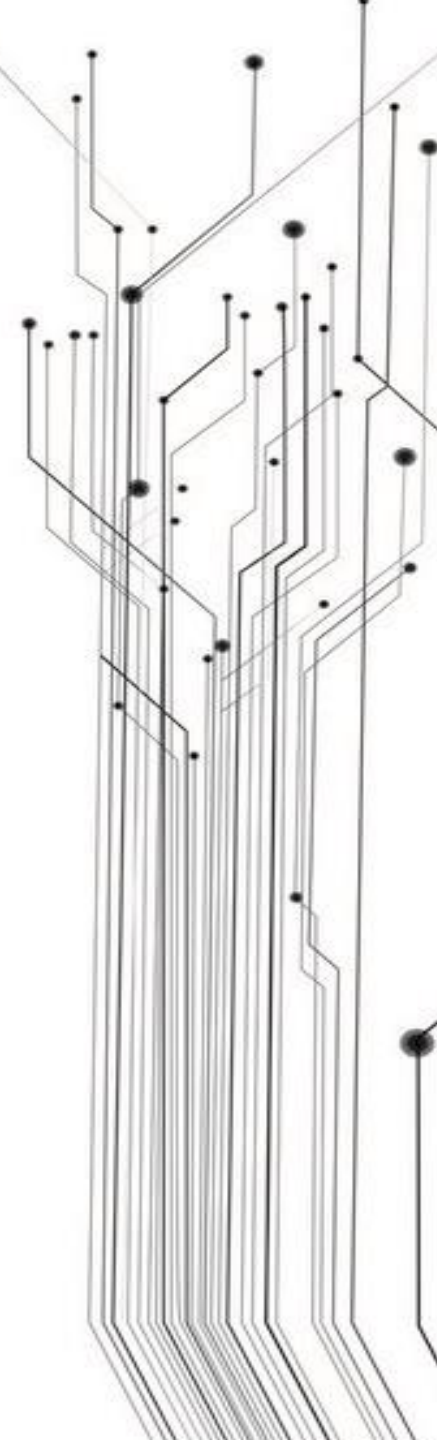


Technologie, HW srdce



Co je to vlastně KOC?

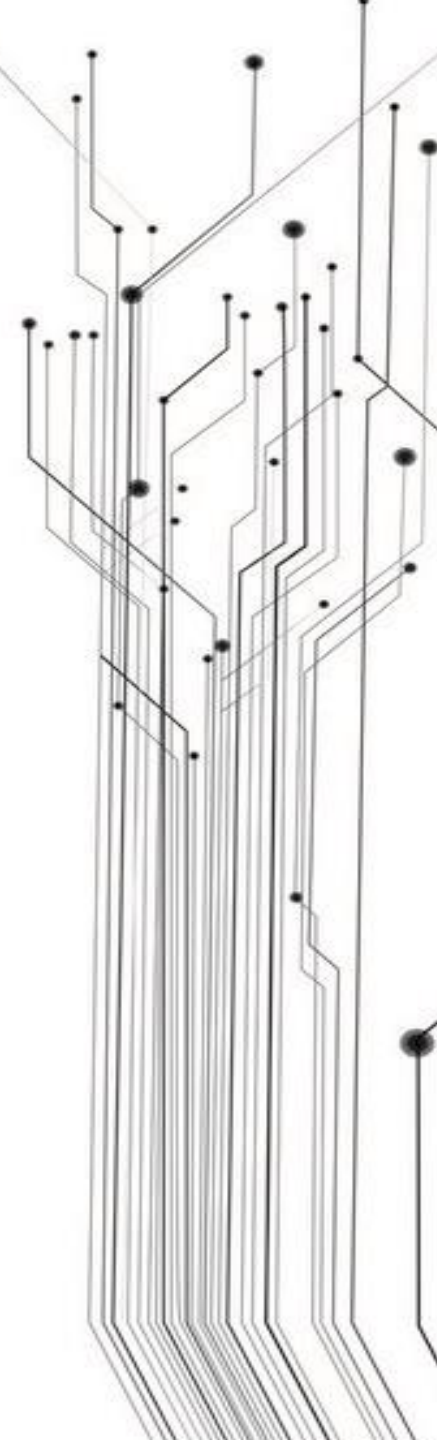
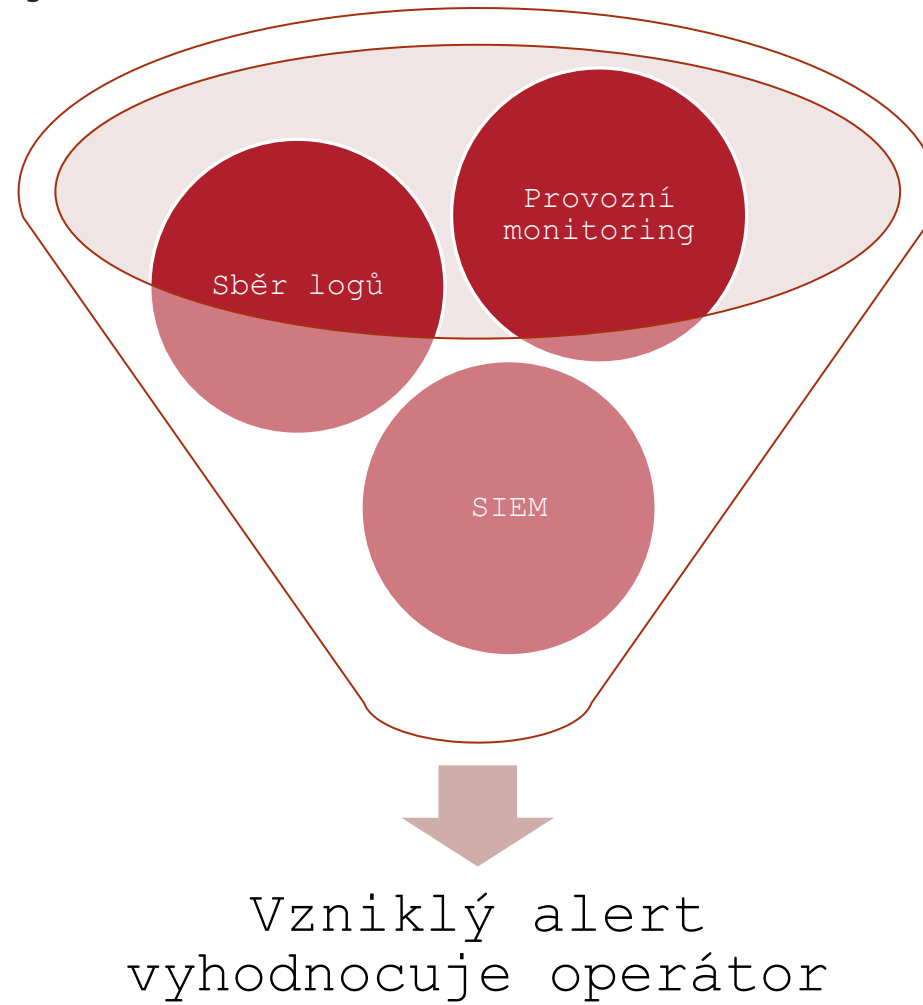
- Systémy, které sbírají **logy** z IT infrastruktury a pracují s nimi.
- Tyto systémy jsou tvořeny provozním, síťovým a aplikačním monitoringem.
- Log Management nástroj pro sběr, vyhledávání a ukládání těchto logů
- Detekce flow (síťový provoz)
- SIEM (bezpečnostní dohled) –vyhodnocuje (koreluje a alertuje) a reportuje zjištěné neshody na člověka
- Operátor bezpečnostního centra



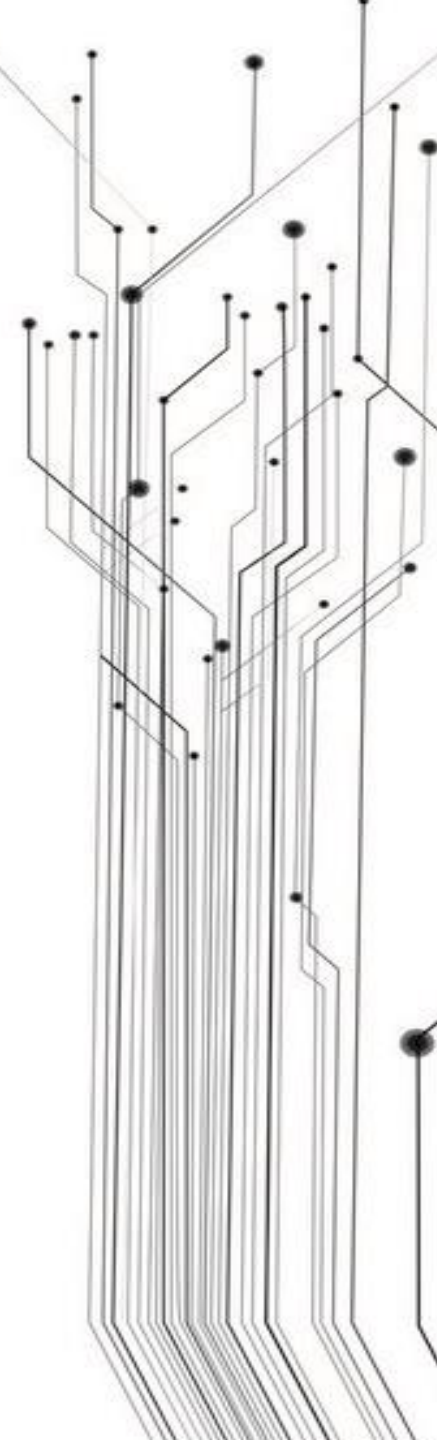
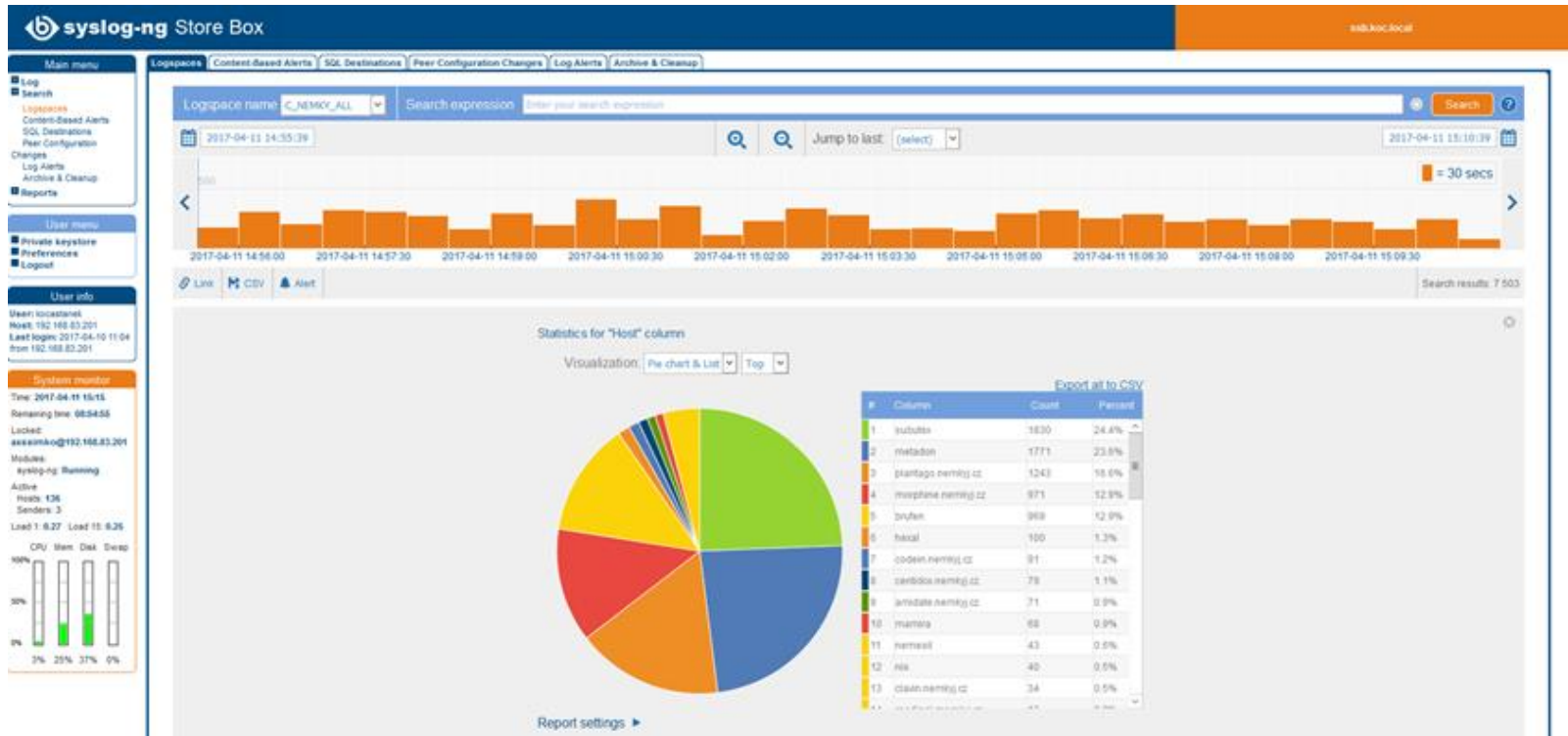
Ukázka logu

- Aug 26 08:13:28 FW-Z-01 EXT-HTTP-GPAPP[32058.24.16]: HTTP-888-I PROXY-EVENT PROTOCOL=TCP CLIENT=se7x.mullvad.net CLIENT-IP=185.65.132.121 CLIENT-PORT=53534 SERVER=195.113.158.123 SERVER-IP=195.113.158.123 SERVER-PORT=80 SERVER-PORT-NAME='http' USER=<NULL> BYTES-CIN=947 BYTES-COUT=343 BYTES-SIN=947 BYTES-SOUT=338 DURATION=0.003703 STATUS=ACCEPTED RESULT=OK RULE='REQ-OK' USER-GROUPS=<NULL> METHOD=GET
URI='http://195.113.158.123:80//?lang=../../../../../../../../../../../../windows/win.ini%00.png&p_id=60' CONTENT-TYPE='text/html' STATUS-CODE=200 VIRUS-STATUS=0 PAGE-VIEW=1 BYPASS=0 CATEGORIES=<NULL> REFERER=<NULL>

Jak to funguje?



Logmanagement



Monitoring síťového provozu

Flowmon Dashboard

Flowmon Dashboard

Úč Dneš 1 den

On Nyní

Uložit

Default

10 nejčastějších událostí podle typu

Typ události	Jméno	Počet událostí
1 ANOMALY	Behavior anomaly	13
2 COUNTRY	Country reputation	9
3 BLACKLIST	Communication with blacklisted hosts	3
4 DIVCOM	Target hosts/poD anomaly	2
5 DNSREVERSE	DNS reverse records missing	1
Ostatní		0

Data za interval 2017-04-10 22:11 - 2017-...

10 nejčastějších původců událostí

Zdroj události	Počet událostí
1 ssb.koc.bca	5
2 FW 2 (1.koc.bca)	5
3 net.ko.bca	3
4 D-W10-11	3

Poslední události

Typ události	Zdroj události	Cíle	Časová známka
COUNTRY	vd100.koc.bca	ec2-31-161-121-126.us-west-2.compute.amazonaws.com, ec2-31-166-191-186.us-west-2.compute.amazonaws.com, ec2-54-148-59-150.us-west-2.compute.amazonaws.com, ec2-34-201-148-11.us-west-2.compute.amazonaws.com, ec2-54-213-74-99.us-west-2.compute.amazonaws.com	2017-04-11 14:43:00
COUNTRY	ssb.koc.bca	google public dns a.google.com	2017-04-11 13:05:00
COUNTRY	vd1.koc.bca	server-54-210-210-210.waw50.cloudfront.net, pr0302-in-f97.1e100.net, pr0302-in-f110.1e100.net	2017-04-11 12:00:00
DIVCOM	FW-2-01.koc.bca	195.113.158.116, pr0302-in-f193.1e100.net, ns.cesnet.cz, 2.21.74.63, 2.21.74.59, 65.32.139.158, pr0302-in-f02.1e100.net	2017-04-11 11:55:00
DIVCOM	FW-2-01.koc.bca	uk.cesnet.cz, lak.cesnet.cz, 193.115.192.110, box-1e-hp-pool.centrim.cz, 152.115.75.199, pr0302-in-f110.1e100.net, ec2-52-59-35-156.eu-central-1.compute.amazonaws.com, line-pool.centrim.cz, prague-161.cdn77.com, 151.101.36.114, ad.seznam.cz	2017-04-11 11:50:00
BLACKLIST	D-W10-11	175.197.forpsinet	2017-04-11 11:10:00
BLACKLIST	D-W10-11	175.197.forpsinet	2017-04-11 11:08:06
BLACKLIST	D-W10-11	175.197.forpsinet	2017-04-11 10:56:15
COUNTRY	SwitchWsk.koc.bca	ec2-52-2-1-24.compute-1.amazonaws.com	2017-04-11 09:50:00
ANOMALY	vd1.koc.bca	ec2.koc.bca, vd1.koc.bca, centrim.koc.bca	2017-04-11 04:15:00

Data za interval 2017-04-10 22:11 - 2017-04-11 22:11

10 nejpriornějších typů událostí

Typ události	Počet událostí
1 BLACKLIST	3
2 COUNTRY	5
3 ANOMALY	13
4 DIVCOM	2
5 DNSREVERSE	1

Data za interval 2017-04-10 7:11 - 2017-...

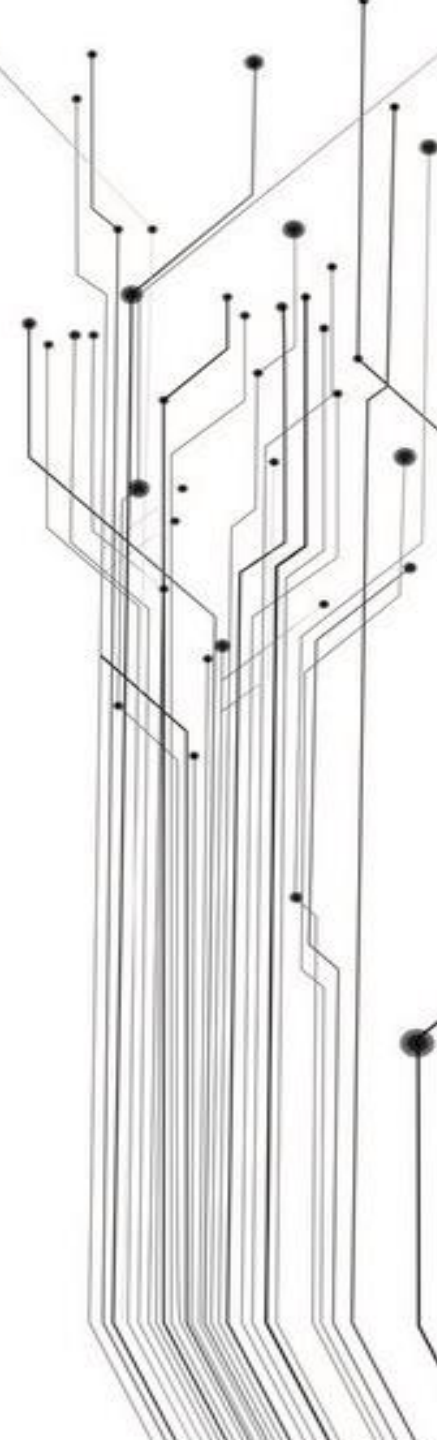
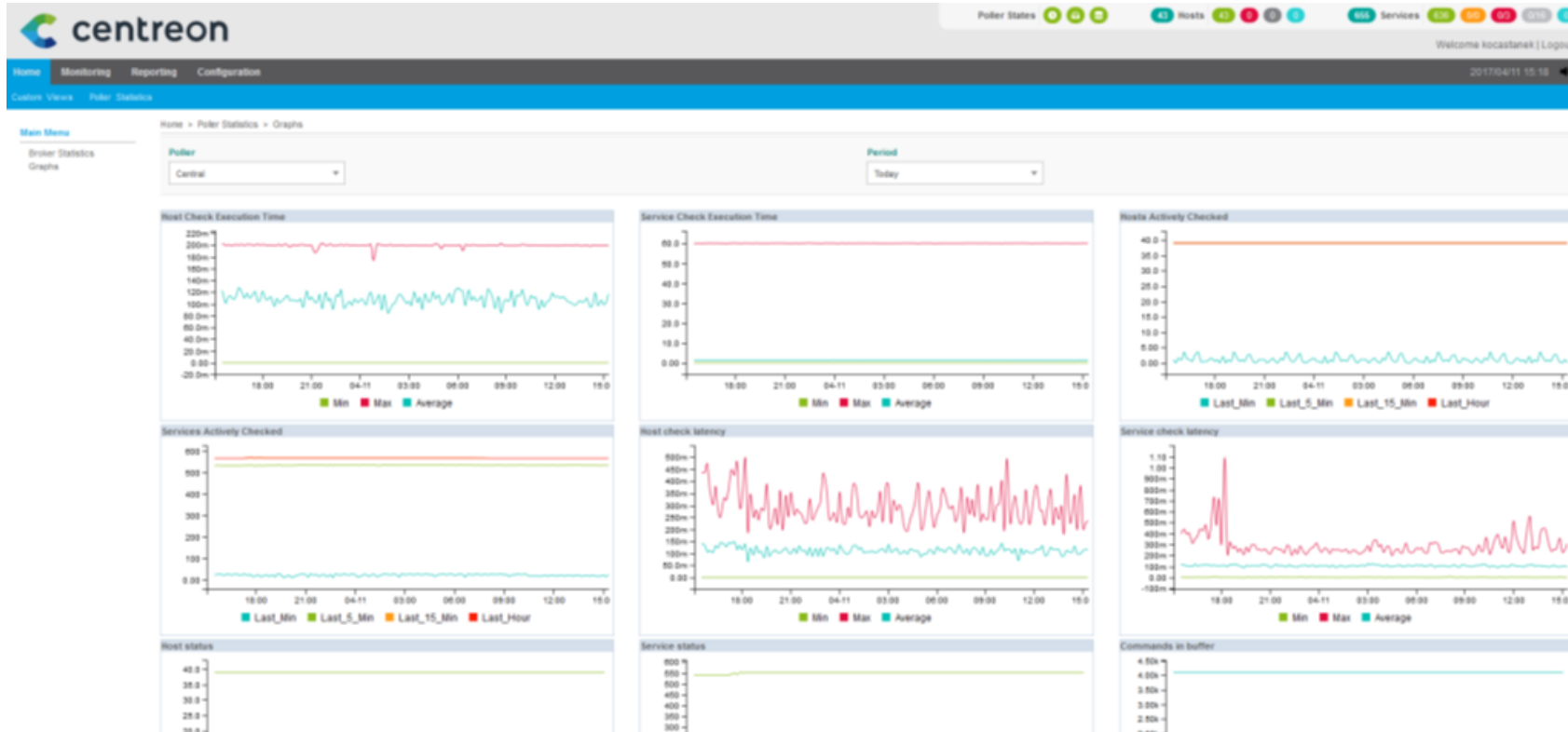
Alerty

Jméno	Stav	Naposledy provedeno
UA_flow_RS_to_SSB_new	aktivní	2016-10-24 12:00

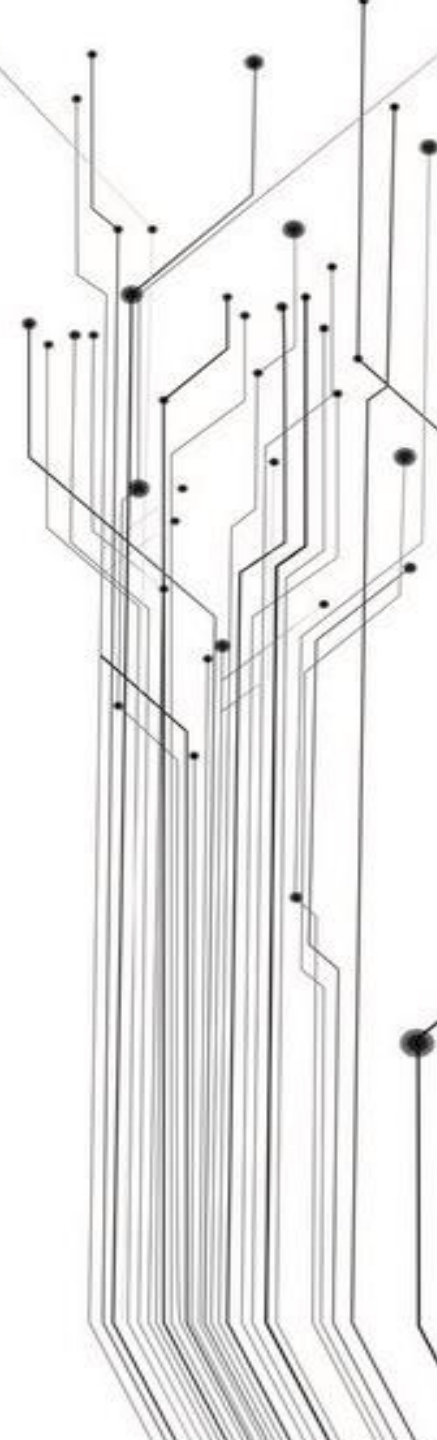
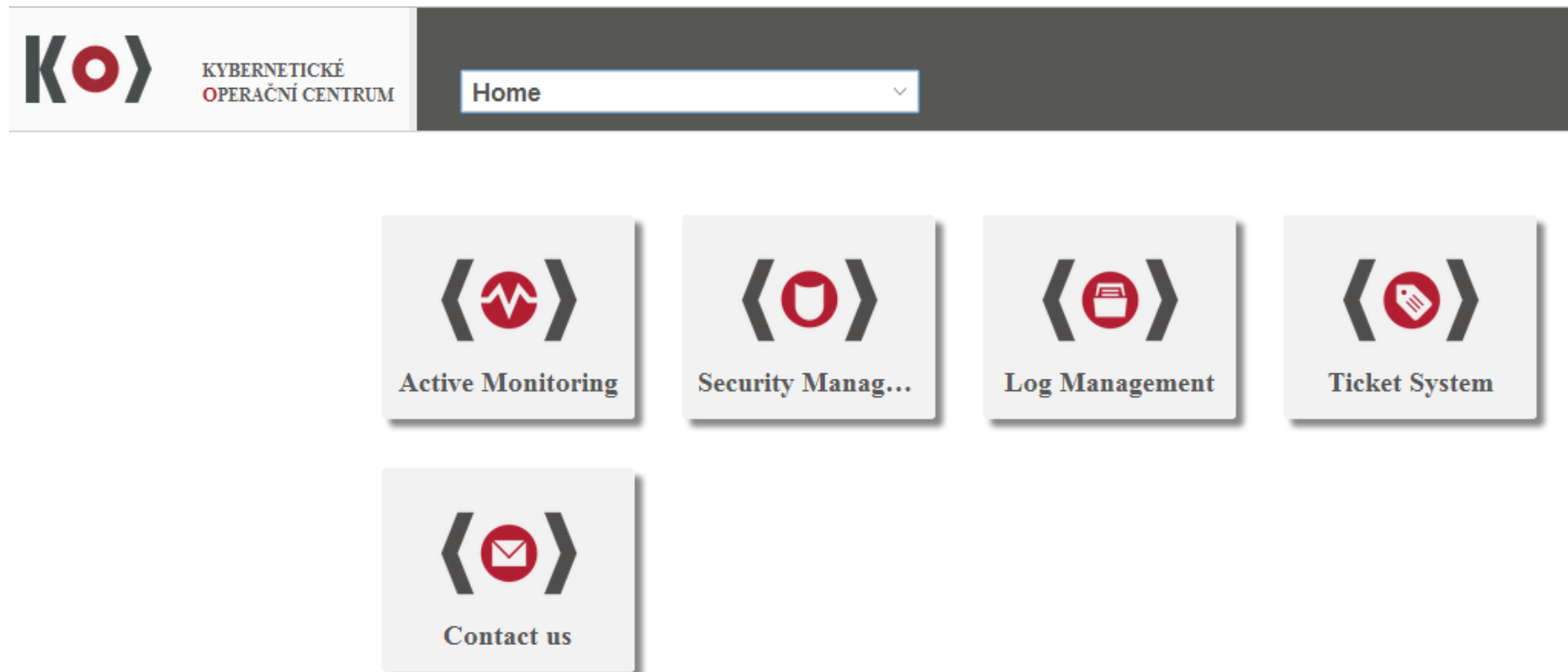
Vložit nový panel ...

Přehledový graf

Provozní monitoring



Webové prostředí pro zákazníky



SIEM – Security information & event management mozek KOC

ArcSight Command Center | Dashboards | **Events** | Reports | Cases | Applications | Administration | Stats | kocastanek | Site Map


Event Search

Field Summary | Last 7 days

staneK [Go!]

Advanced Search

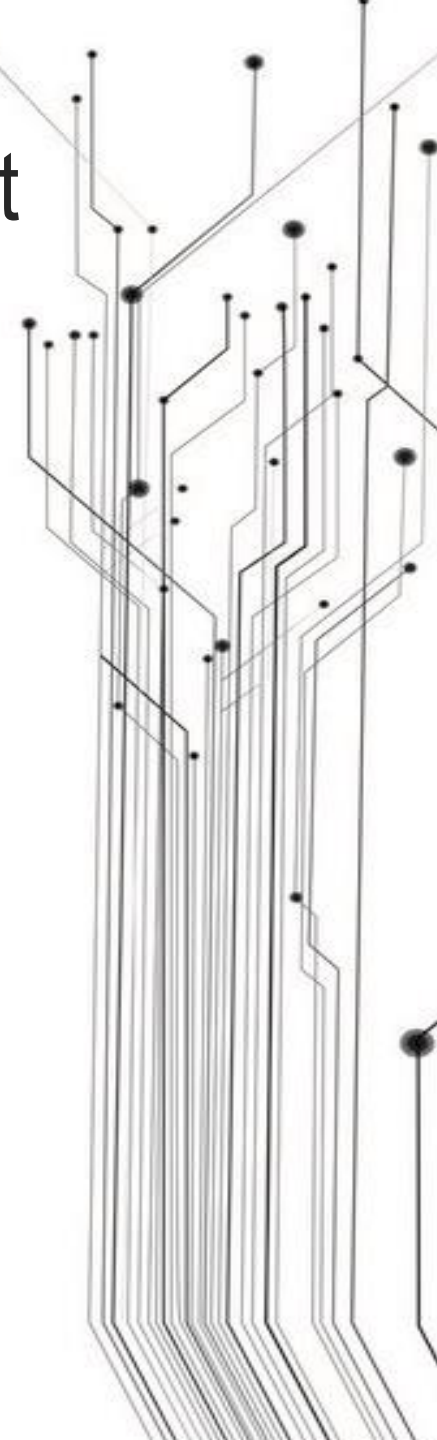
Fields: Default Fields | Auto Update: 5 min | 542 | 161,182,045 | 00:07.548 | Export Results... | 1 bar = 12 hour



Events

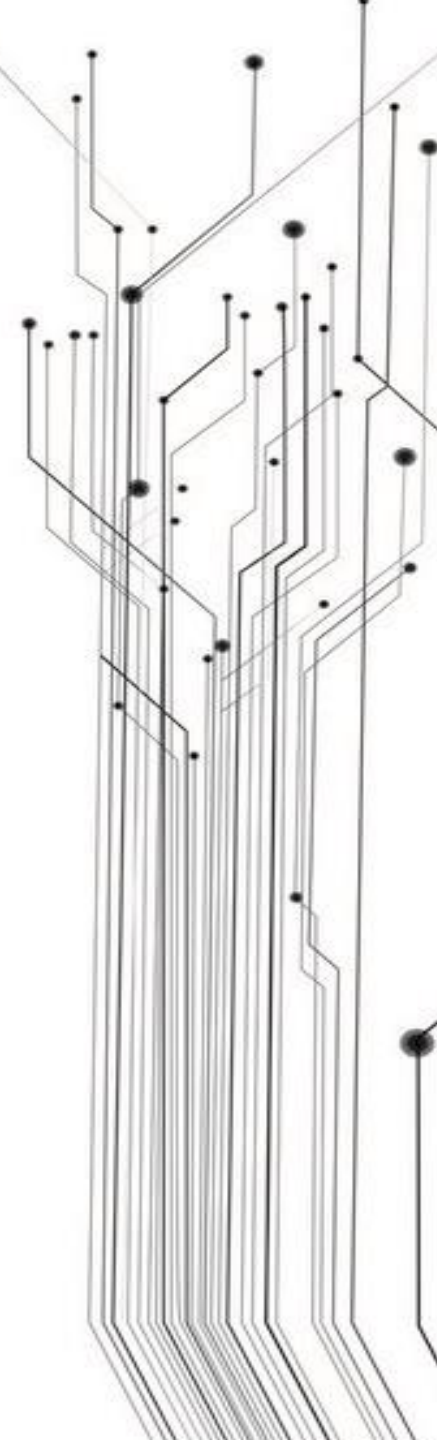
Page 1 of 22 | Show RAW | All | None | Displaying 1 - 25 of 542 | Events per page 25

	endTime	name	sourceAddress	destinationAddress	priority	deviceVendor	deviceProduct
1	2017/04/05 16:23:33 CEST	Denial of service event filtering triggered			7	ArcSight	ArcSight
2	2017/04/05 16:21:51 CEST	Denial of service event filtering triggered			7	ArcSight	ArcSight
3	2017/04/05 16:21:42 CEST	kr-jhomoravsky@staneK.ales: Security Microsoft Windows security auditing: [Success Audit] Dořto k pokusu o p?ln?en? pomoc? explicitn?ch p?lna?ovac?ch ?daj?, P?edm?t: ID zabezpe?en?: KDC\kocastanek N2zev ??tu: kocastanek Dom?na ??tu: KOC ID p?ln?en?: 0x56C3A GUID p?ln?en?: (00000000-0000-0000-0000-00000000... ??et, jeho? p?lna?ovac? ?daje byly nou?tu: N2zev ??tu: ArcSight			7	Unix	Unix



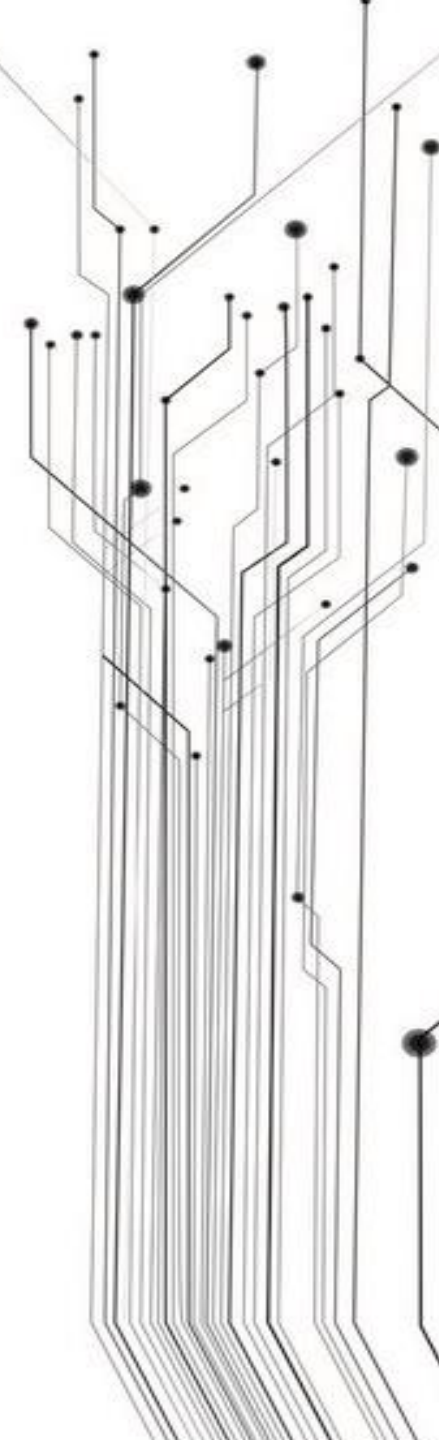
Přínosy KOC JMK

- ▶ Vytvoření jednoho společného KOC pro všechny kraje zřizované společnosti - maximální efektivita.
- ▶ Jeden silně specializovaný technický tým KOC - Tým vyškolených expertů na kybernetickou bezpečnost, který by si samostatně žádná společnost nemohla dovolit.
- ▶ Koordinovaný postup v Incident Response s možností sdílení zdrojů.
- ▶ Jednotný reporting umožňující benchmark společností JMK.
- ▶ Kooperace JMK s českými a evropskými institucemi kybernetické bezpečnosti.



Současný stav KOC JMK

- ▶ Systémy jsou v provozu
- ▶ Je spuštěn monitoring sítí: KOC, JMK, SÚS, SŠIPF, Nemocnice Kyjov
- ▶ Na základě provozních zkušeností jsou upravovány pravidla pro SIEM
- ▶ Plánujeme postupné připojování dalších organizací zřizovaných krajem





KYBERNETICKÉ OPERAČNÍ CENTRUM

► Děkuji Vám za pozornost!

