Jihomoravský kraj

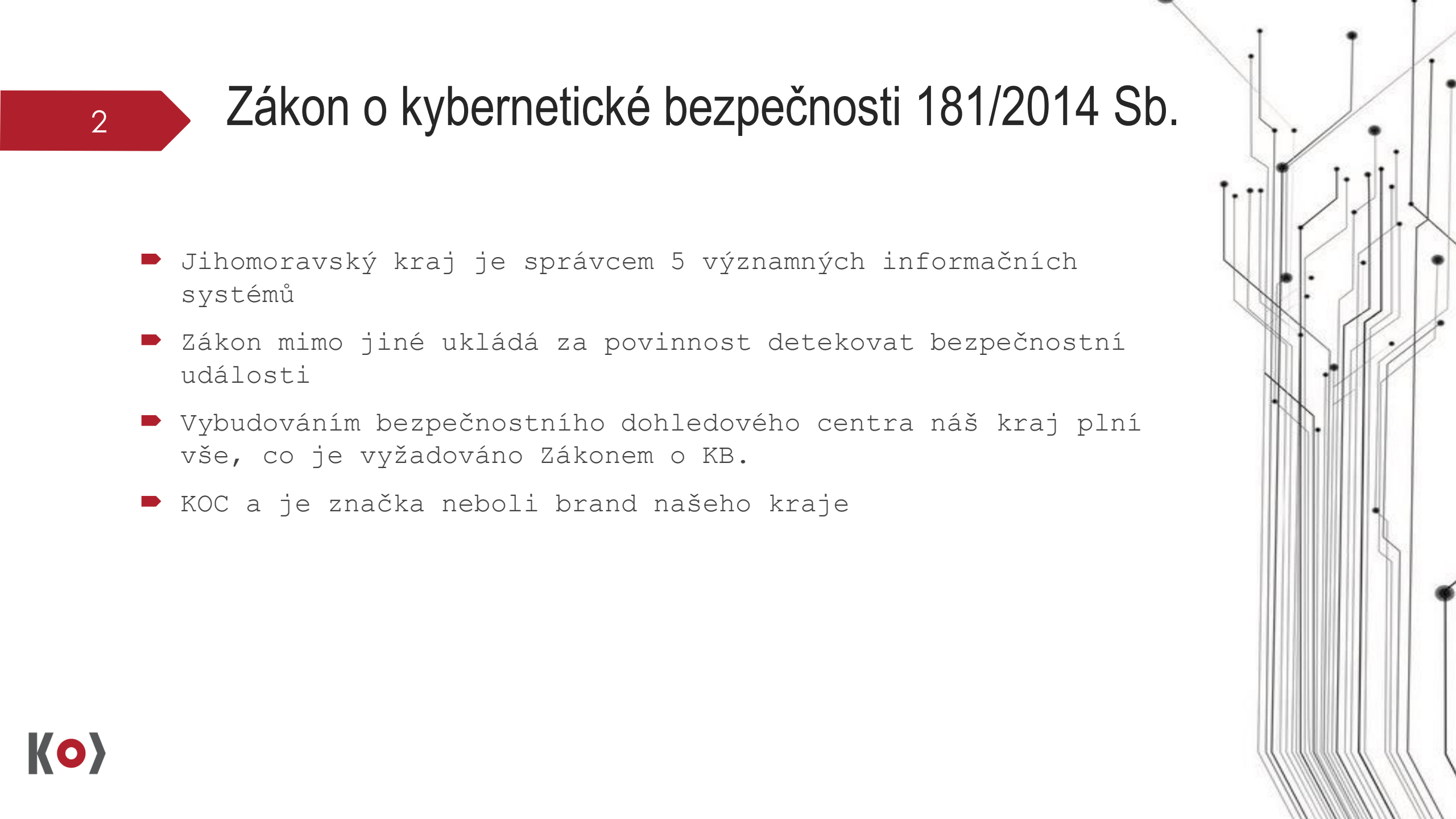
KYBERNETICKÉ OPERAČNÍ CENTRUM

Den klastrů v Jihomoravském kraji 12. 4. 2017

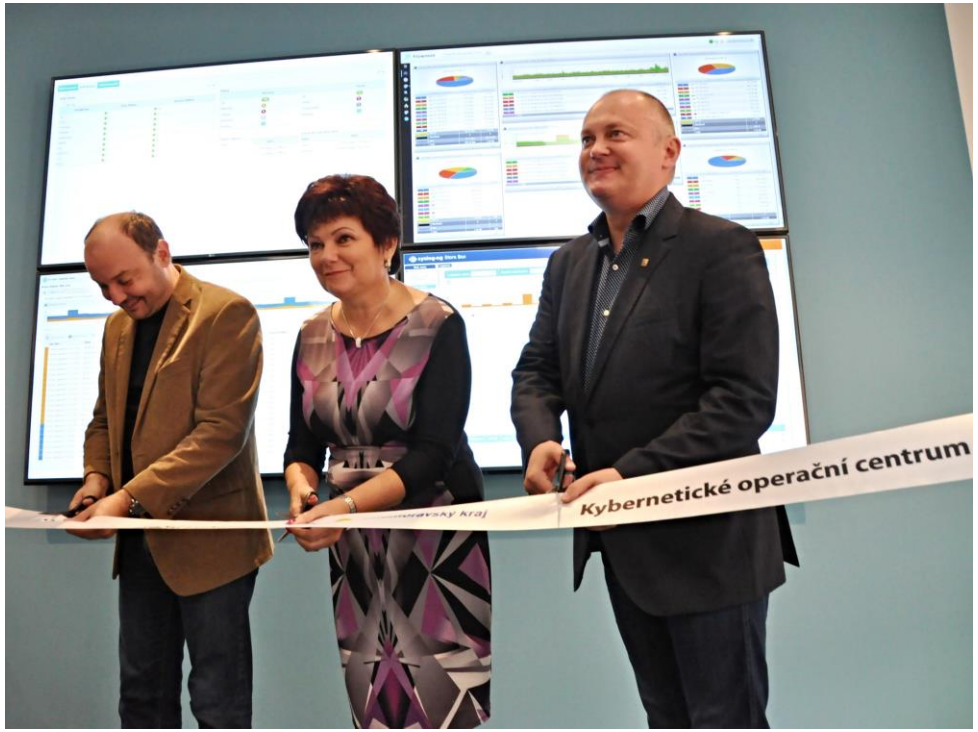
Aleš Staněk

Zákon o kybernetické bezpečnosti 181/2014 Sb.

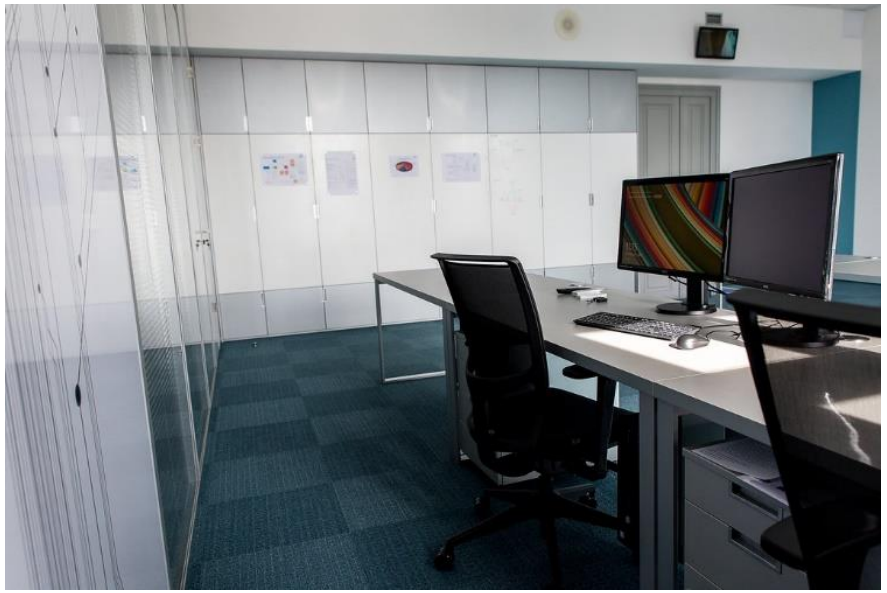
- Jihomoravský kraj je správcem 5 významných informačních systémů
- Zákon mimo jiné ukládá za povinnost detekovat bezpečnostní události
- Vybudováním bezpečnostního dohledového centra náš kraj plní vše, co je vyžadováno Zákonem o KB.
- KOC a je značka neboli brand našeho kraje



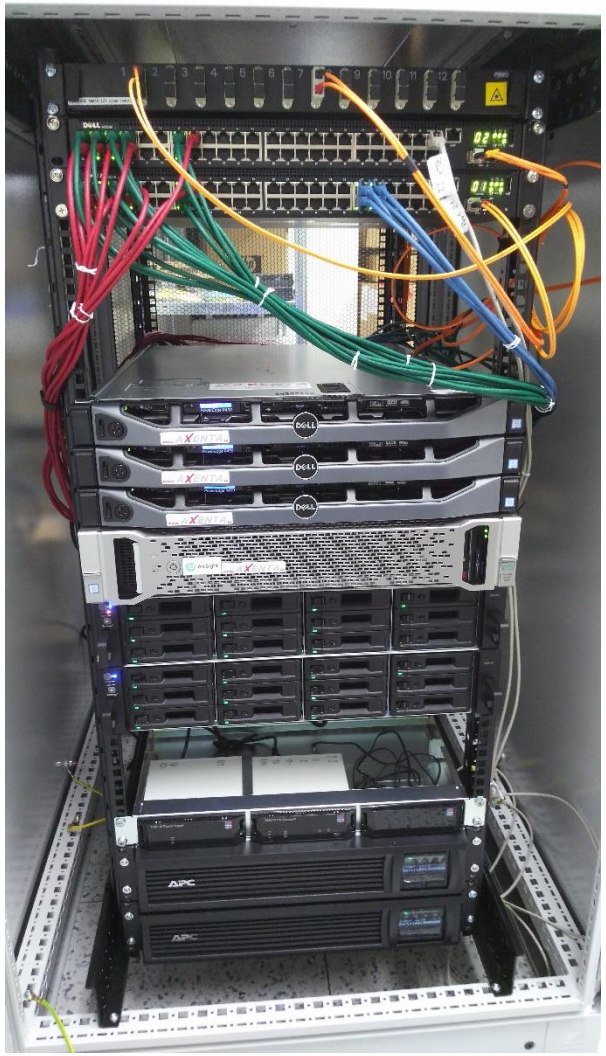
Předání do provozu 09/2016



V historické budově Krajského úřadu vzniklo moderní dohledové bezpečnostní centrum

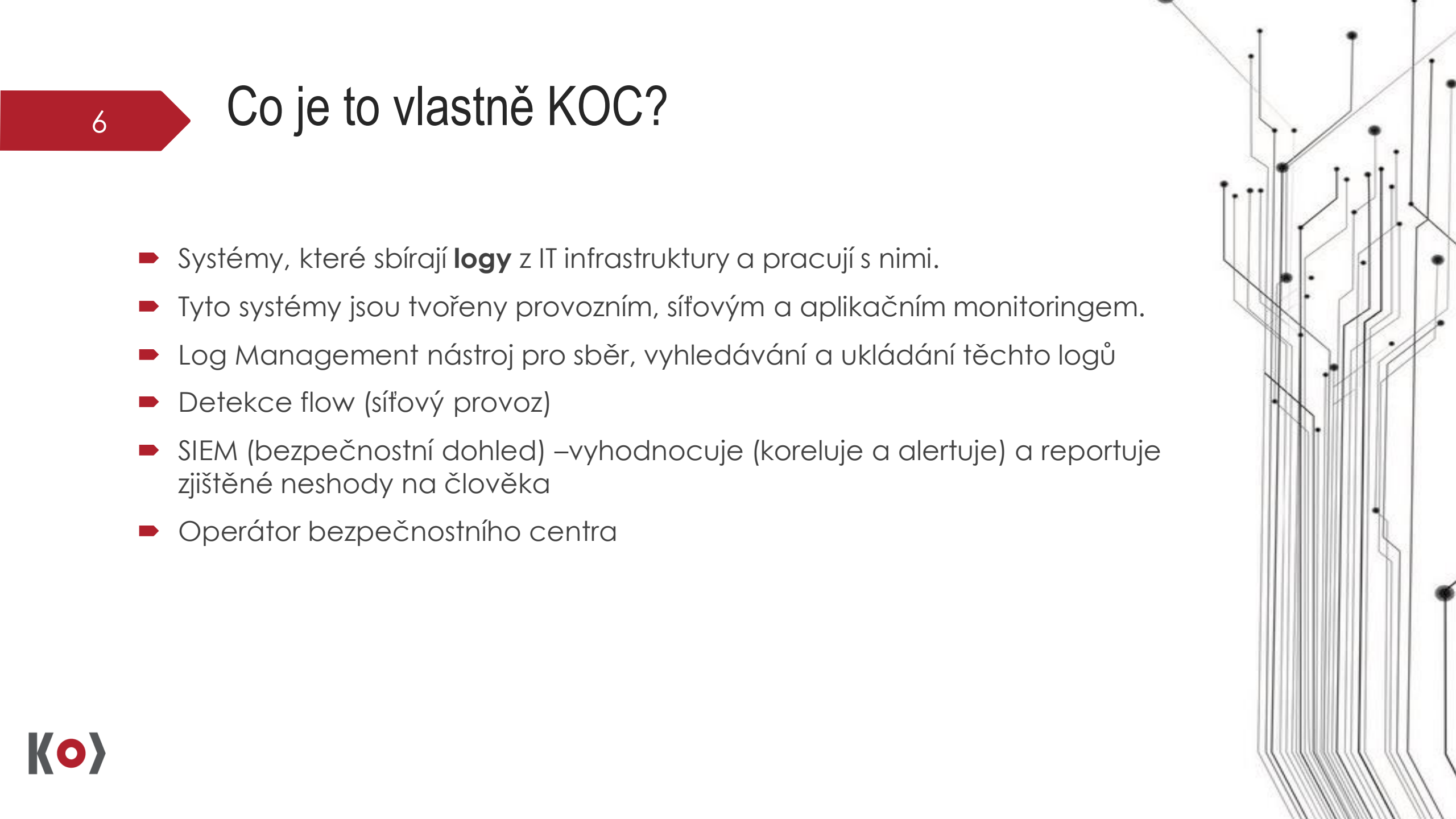


Technologie, HW srdce



Co je to vlastně KOC?

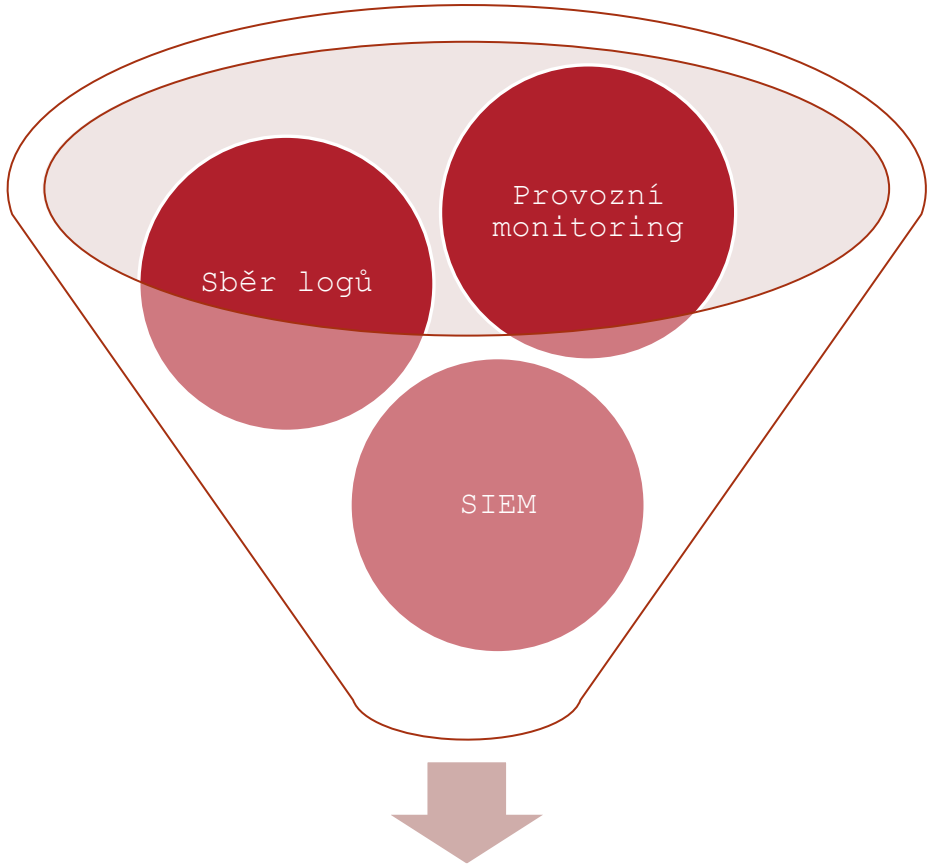
- Systémy, které sbírají **logy** z IT infrastruktury a pracují s nimi.
- Tyto systémy jsou tvořeny provozním, síťovým a aplikačním monitoringem.
- Log Management nástroj pro sběr, vyhledávání a ukládání těchto logů
- Detekce flow (síťový provoz)
- SIEM (bezpečnostní dohled) –vyhodnocuje (koreluje a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



Ukázka logu

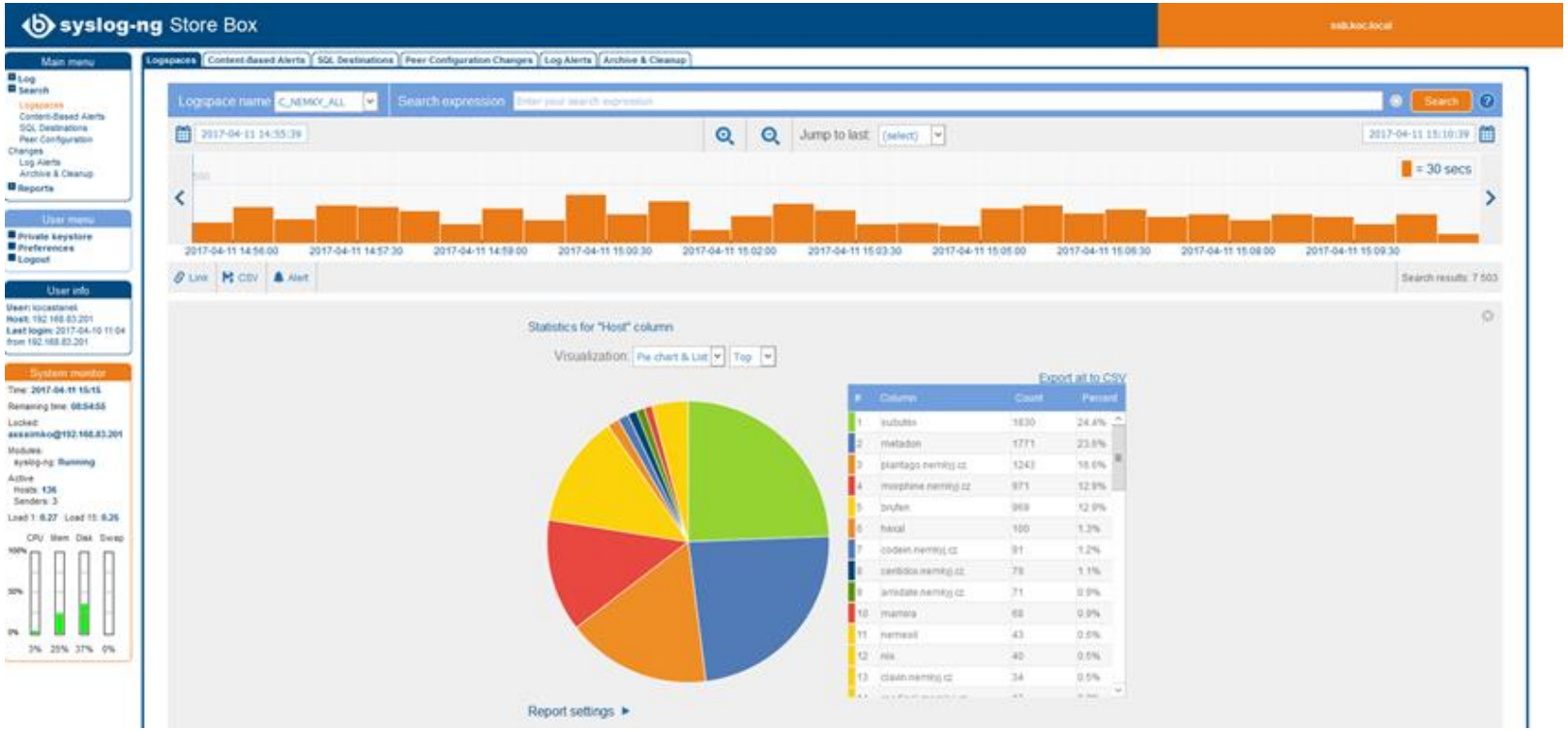
- Aug 26 08:13:28 FW-Z-01 EXT-HTTP-GPAPP[32058.24.16]: HTTP-888-I PROXY-EVENT PROTOCOL=TCP CLIENT=se7x.mullvad.net CLIENT-IP=185.65.132.121 CLIENT-PORT=53534 SERVER=195.113.158.123 SERVER-IP=195.113.158.123 SERVER-PORT=80 SERVER-PORT-NAME='http' USER=<NULL> BYTES-CIN=947 BYTES-COUT=343 BYTES-SIN=947 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?

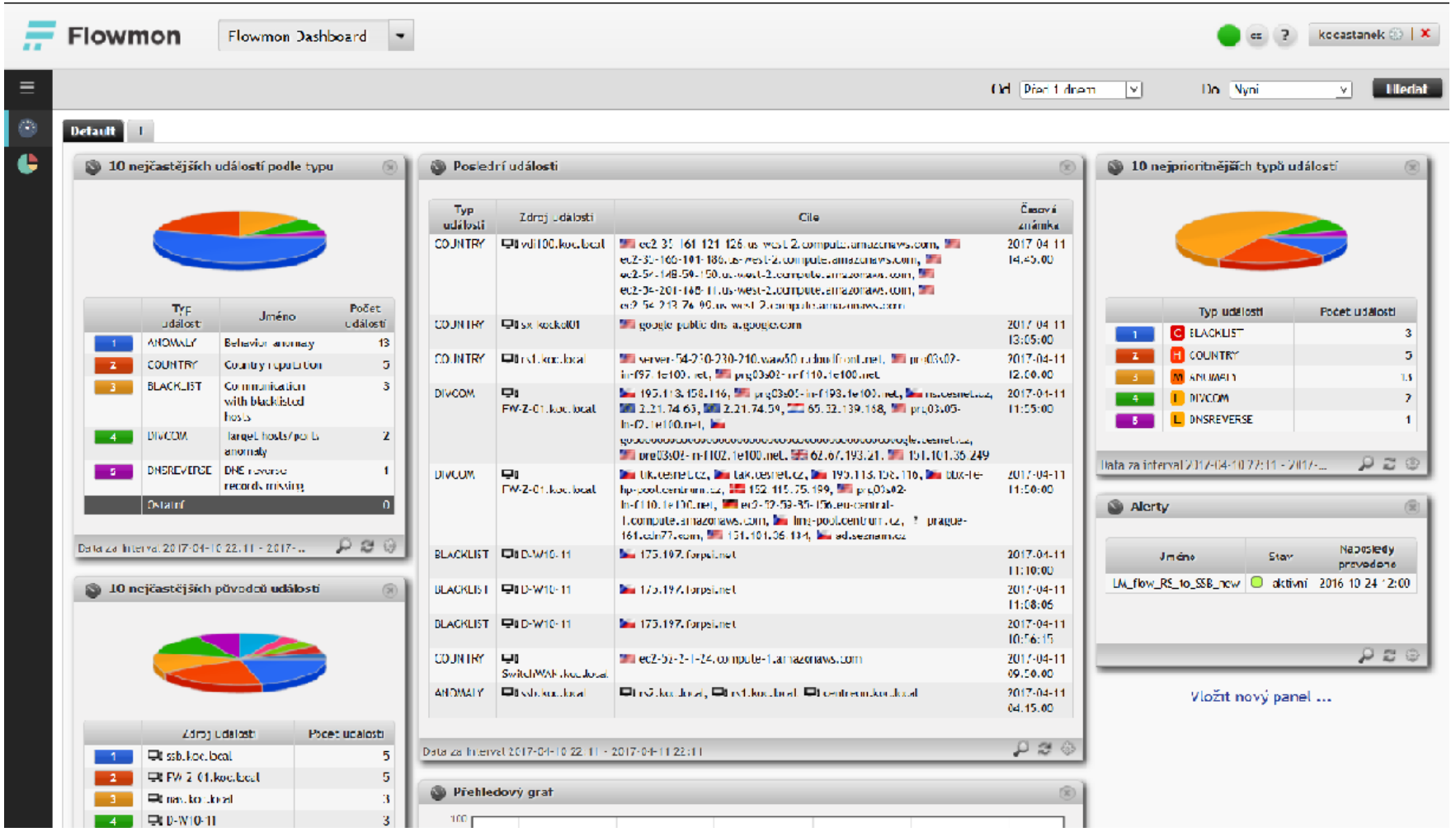


Vzniklý alert vyhodnocuje operátor

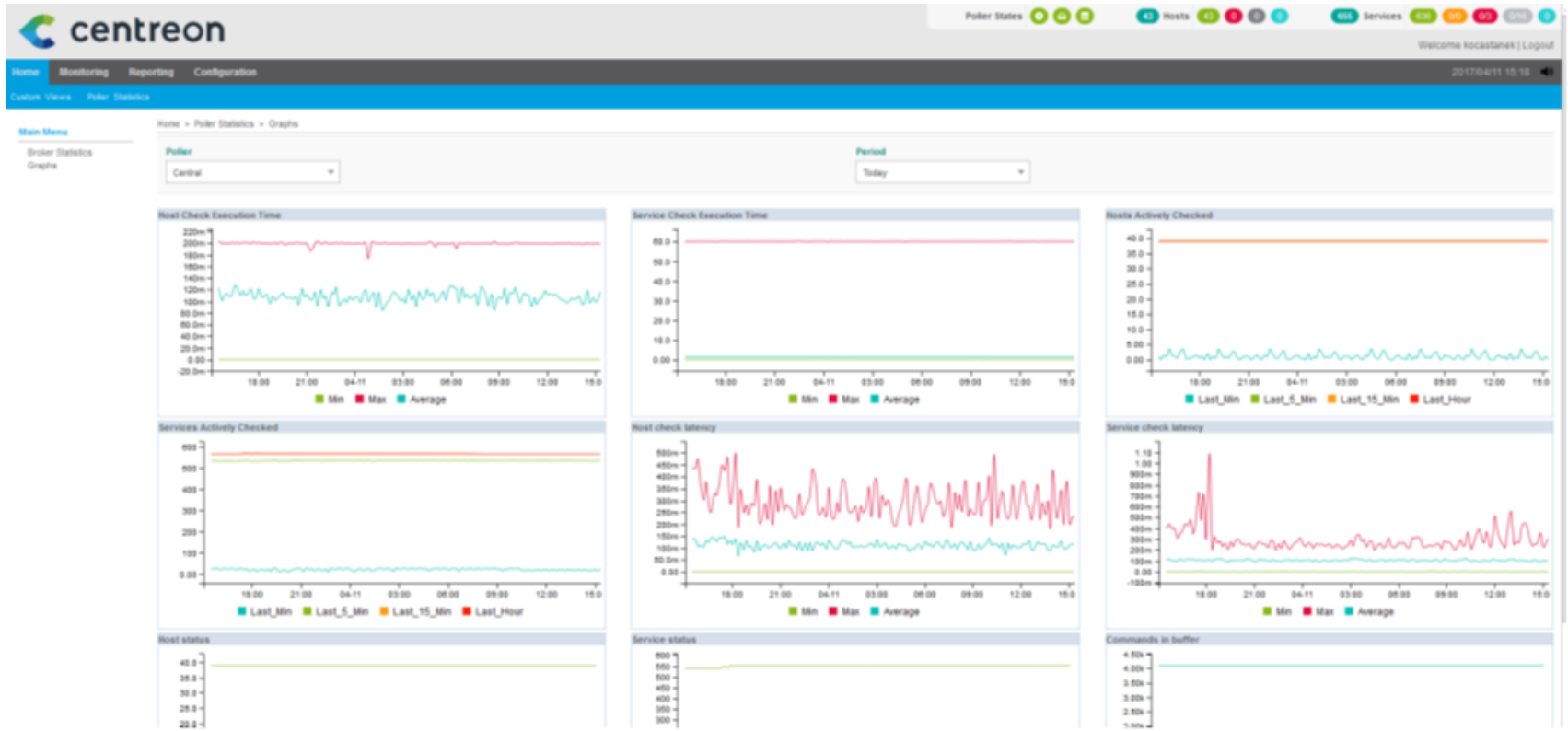
Logmanagement



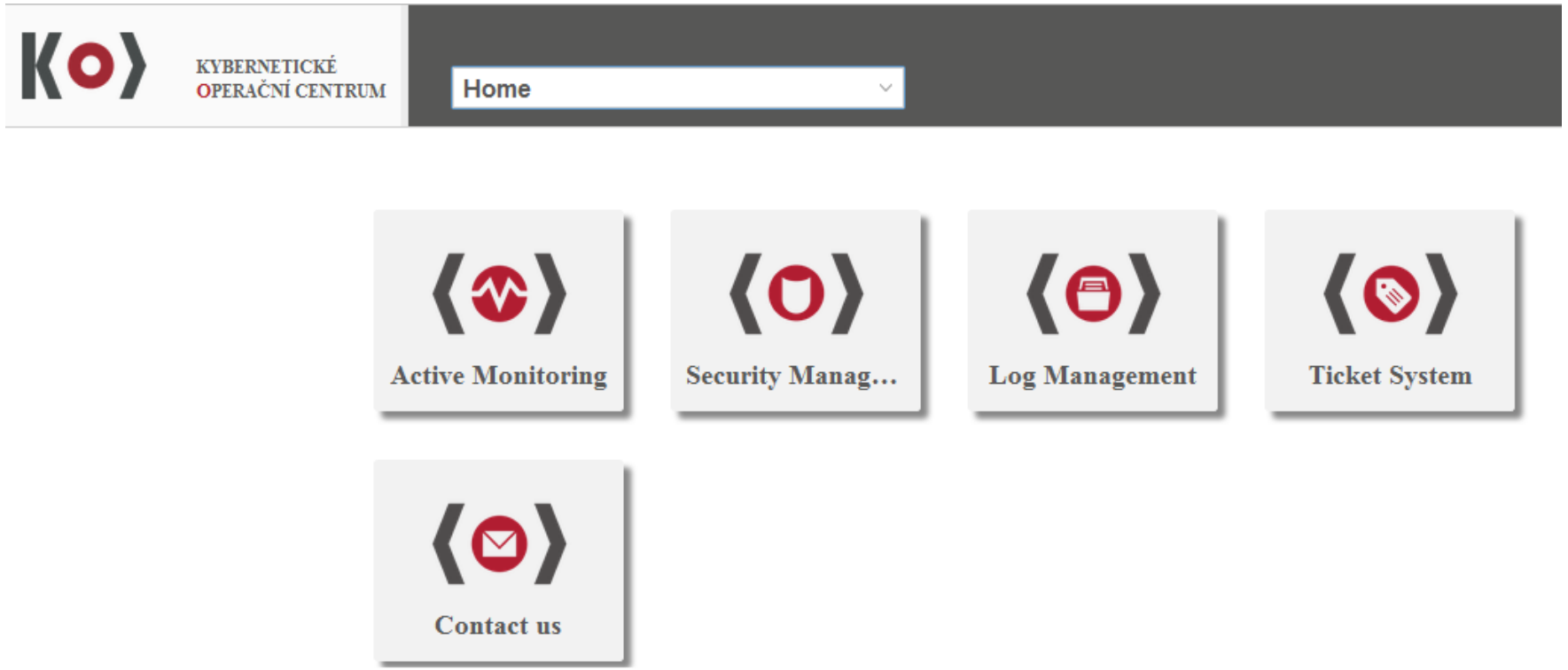
Monitoring síťového provozu



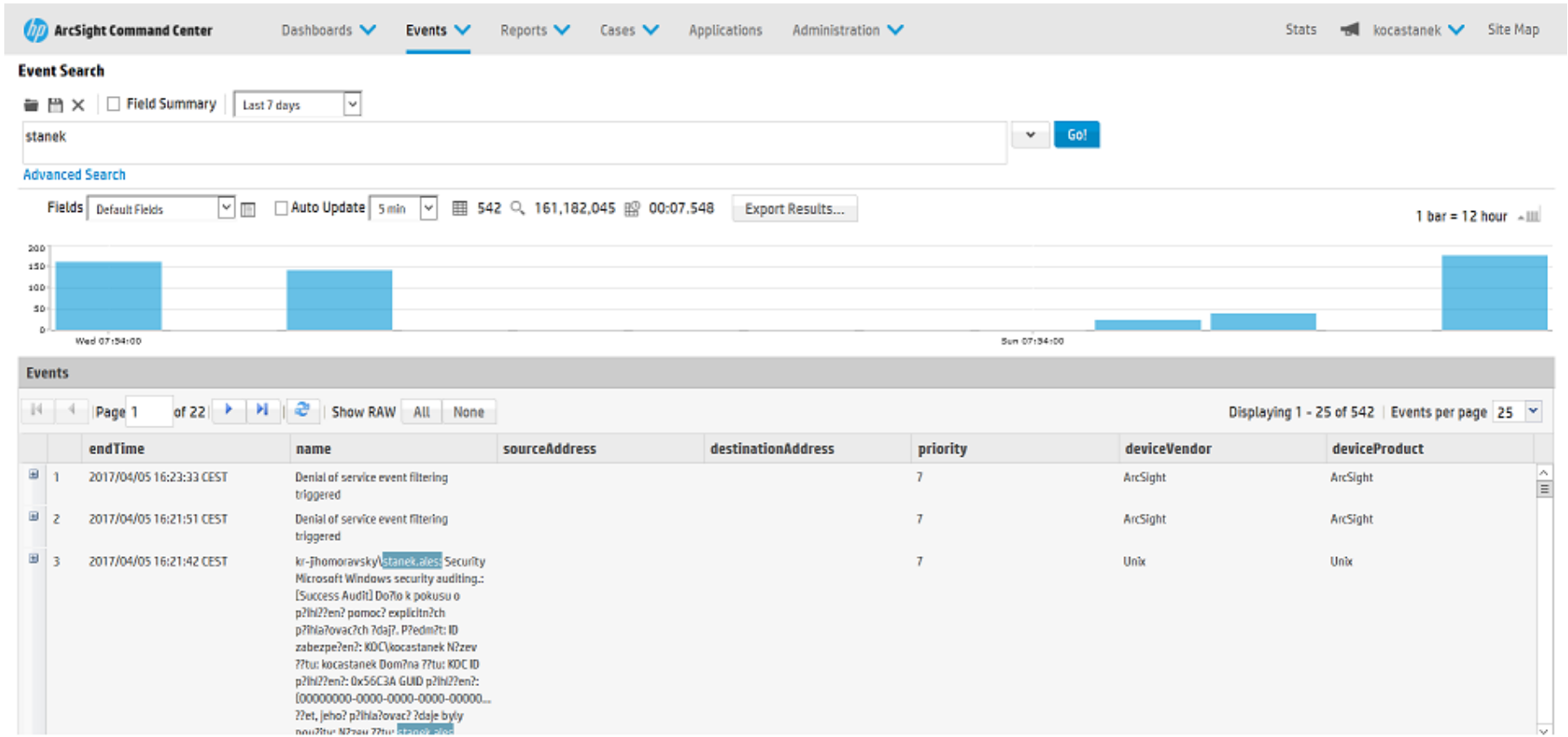
Provozní monitoring



Webové prostředí pro zákazníky



SIEM – Security information & event management mozek KOC



Přínosy KOC JMK

- Vytvoření jednoho společného KOC pro všechny krajem zřizované společnosti – maximální efektivita.
- Jeden silně specializovaný technický tým KOC – Tým vyškolených exportů 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!