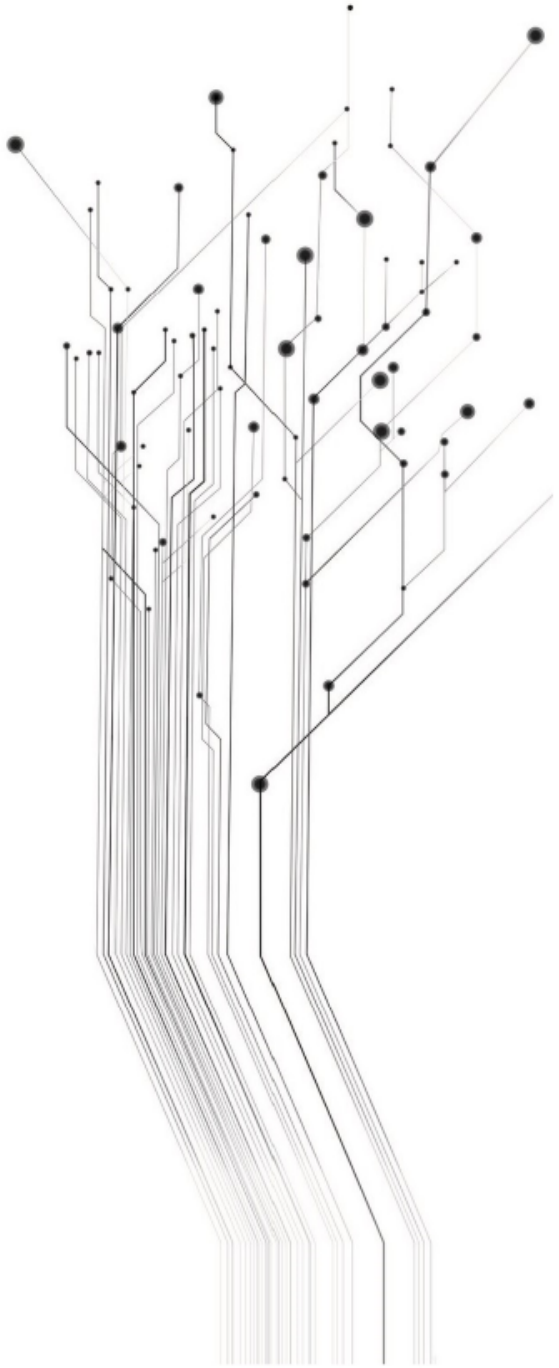


KYBERNETICKÉ OPERAČNÍ CENTRUM

# Představení oddělení KOC

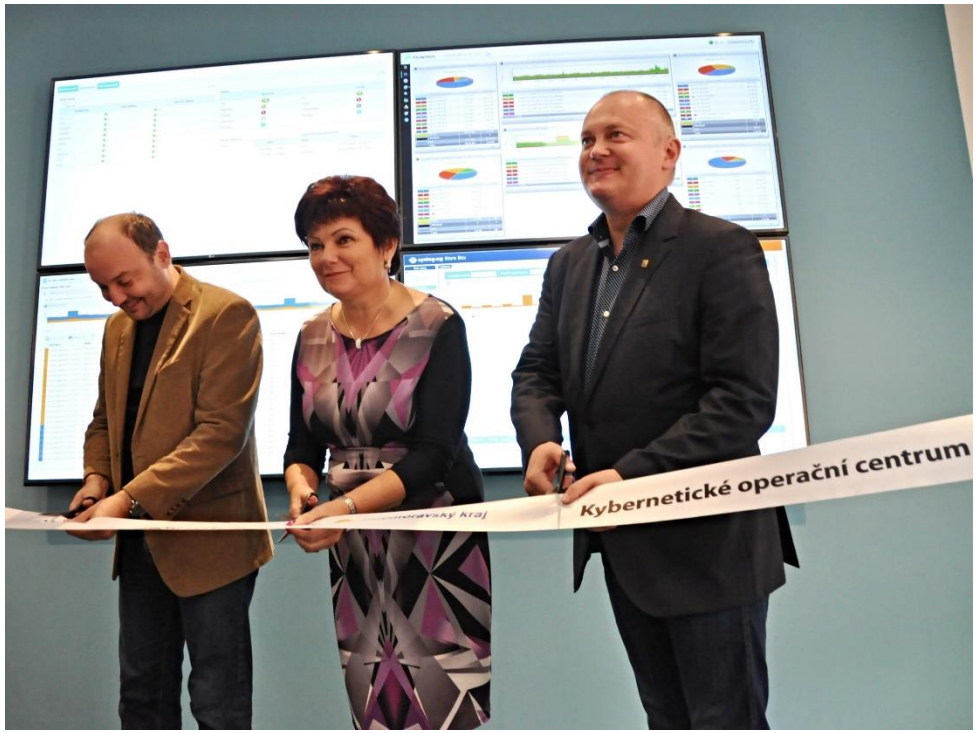
Aleš Staněk

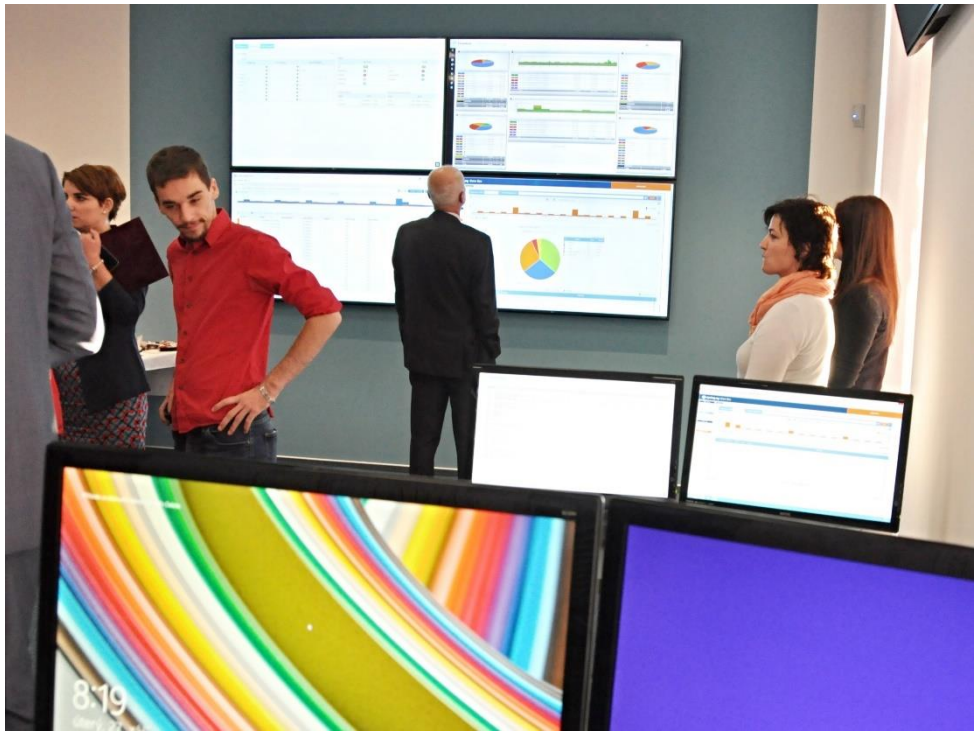
Jihomoravský kraj

KYBERNETICKÉ OPERAČNÍ CENTRUM

# Organizačně je oddělení KOC začleněno do odboru kancelář ředitele Krajského úřad Jihomoravského kraje

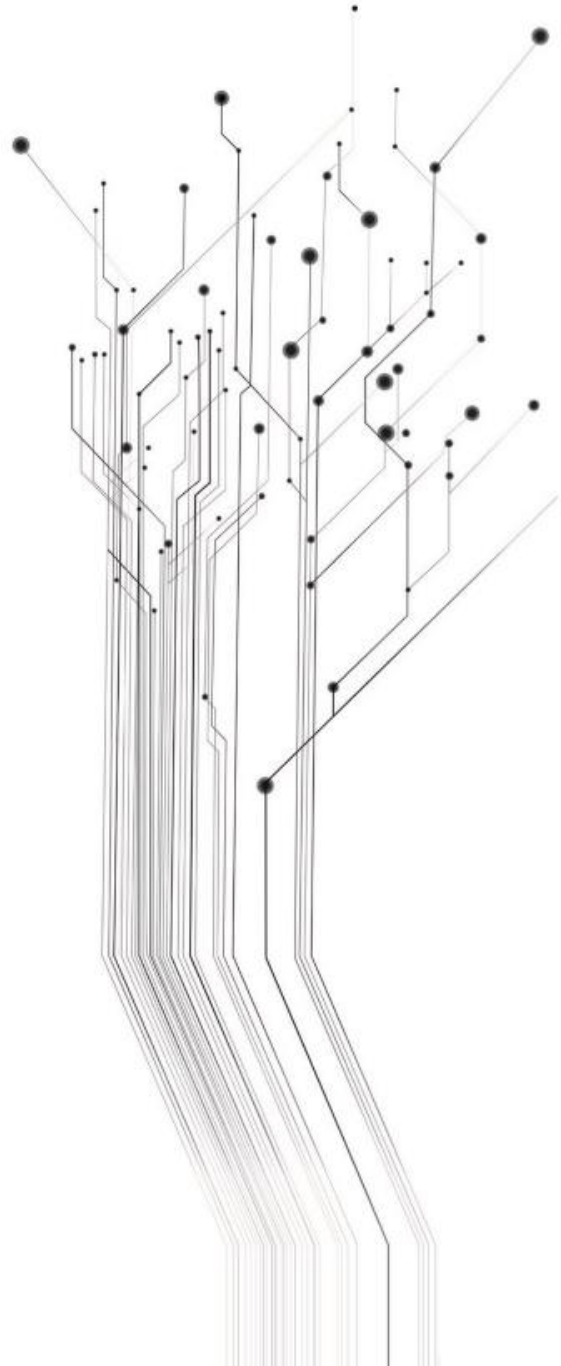
# Předání dohledového centra do provozu 09/2016



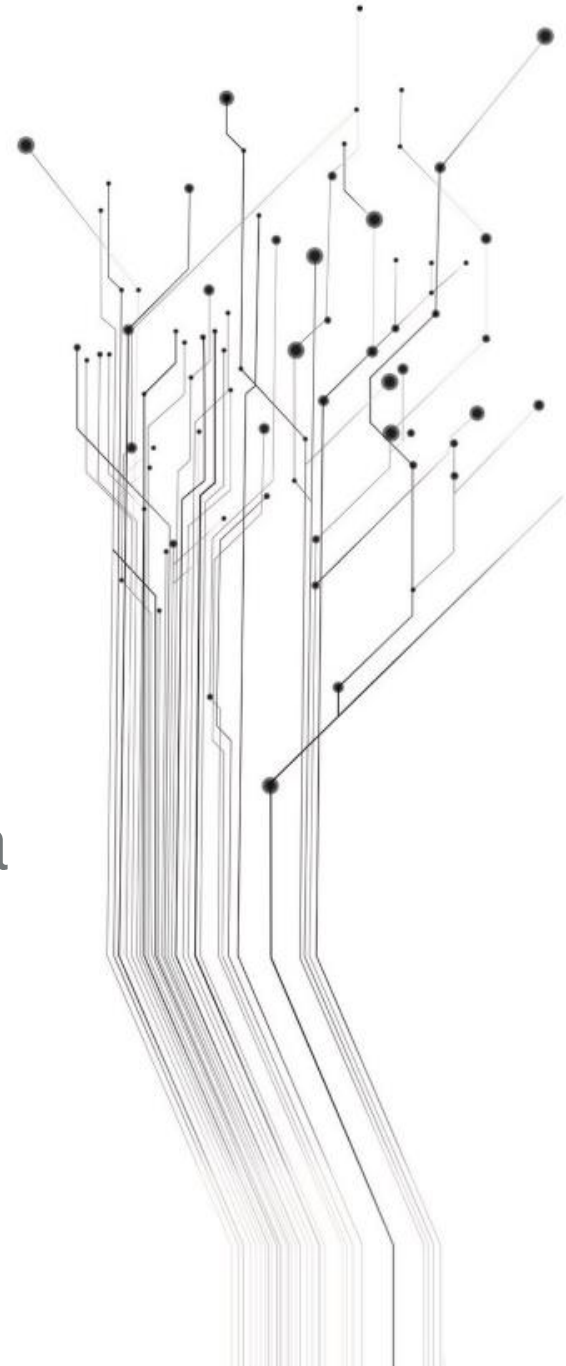
# Proč budovat bezpečnostní dohledové centrum

- Ochrana aktiv
  - Aktivum je cokoli, co má pro organizaci nějakou hodnotu
- Pro komerční sféru je to otázka přežití
  - První on-line bankomat spustila Komerční banka v roce 1992
- Státní správa čekala na právní normu
  - Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
- Jihomoravský kraj je prvním krajem, který ke splnění požadavků ZoKB vybudoval bezpečnostní dohledové centrum



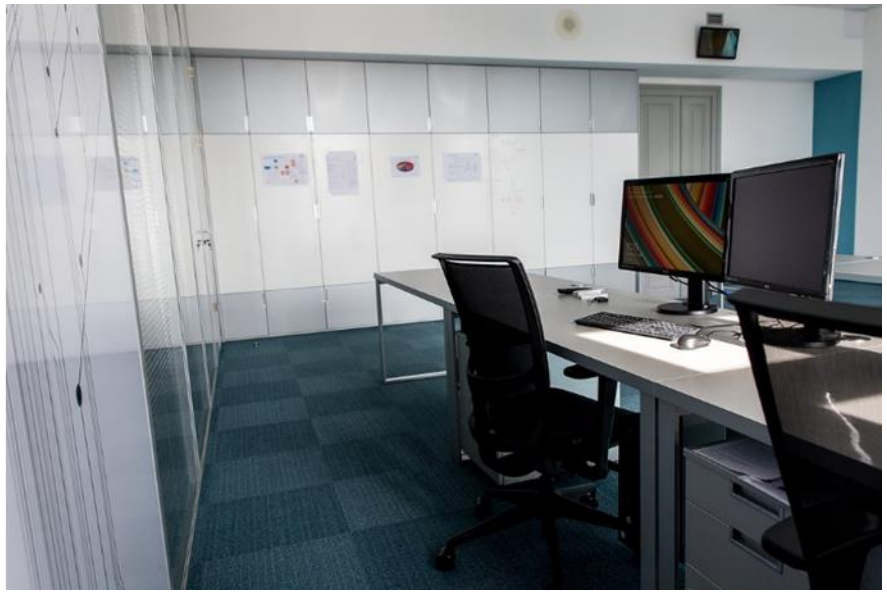
# Zákon o kybernetické bezpečnosti 181/2014 Sb.

- Jihomoravský kraj je správcem 5 významných informačních systémů
- Zákon mimo jiné ukládá v §5 povinnost zavést
  - Organizační opatření
  - Technická opatření
- Vybudováním bezpečnostního dohledového centra náš kraj plní vše, co je vyžadováno Zákonem o KB.

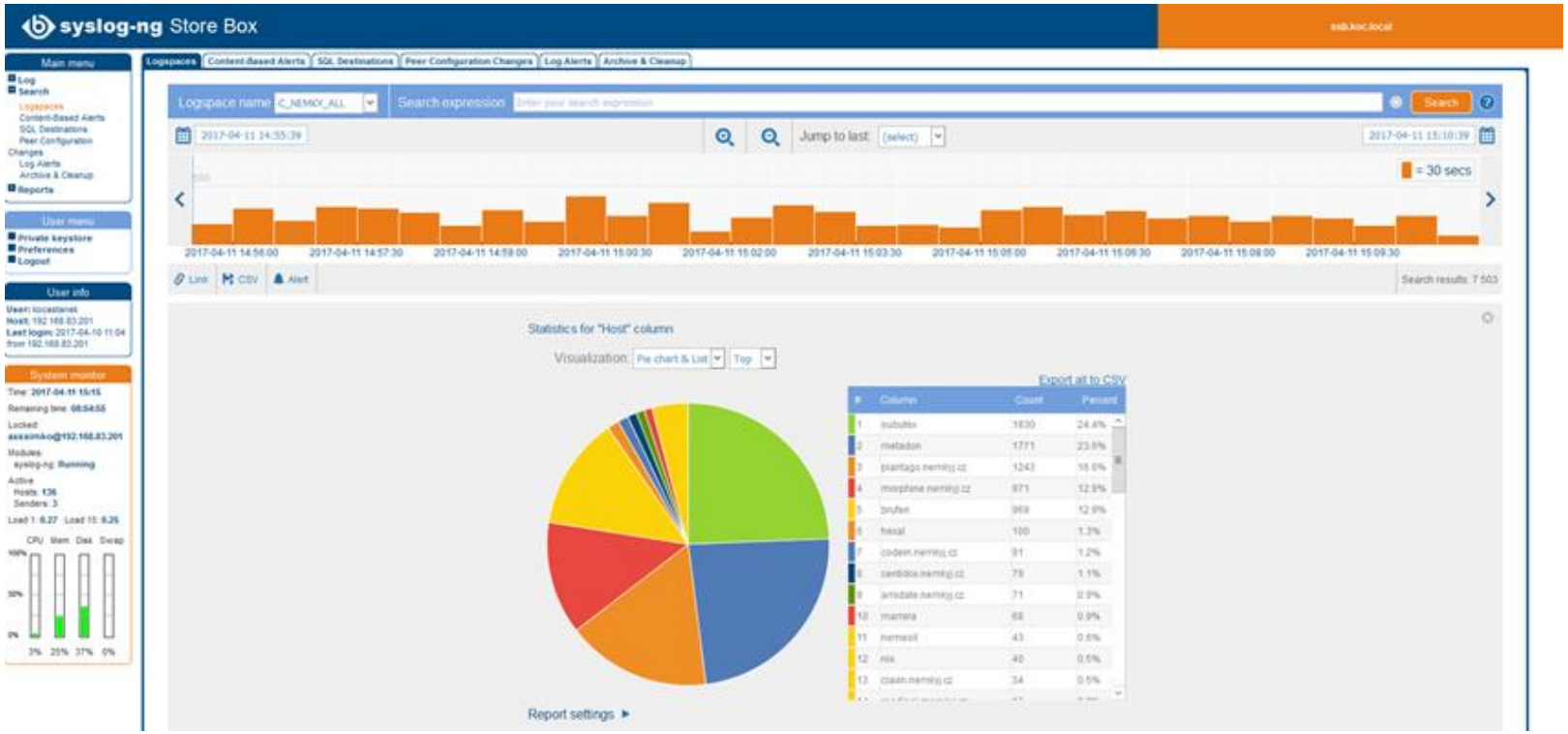


# Technologie, HW srdce KOC

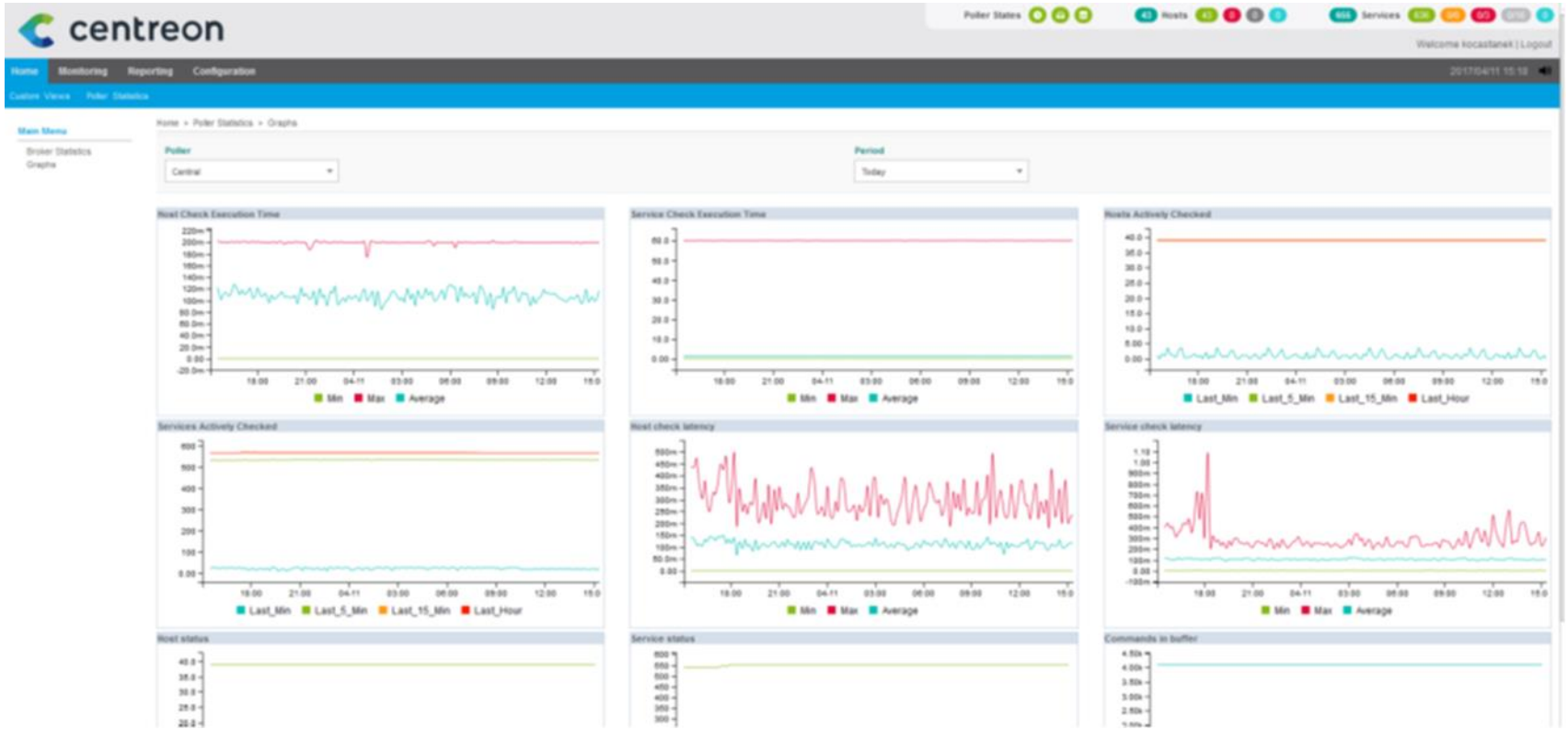

# V historické budově Krajského úřadu vzniklo moderní dohledové bezpečnostní centrum



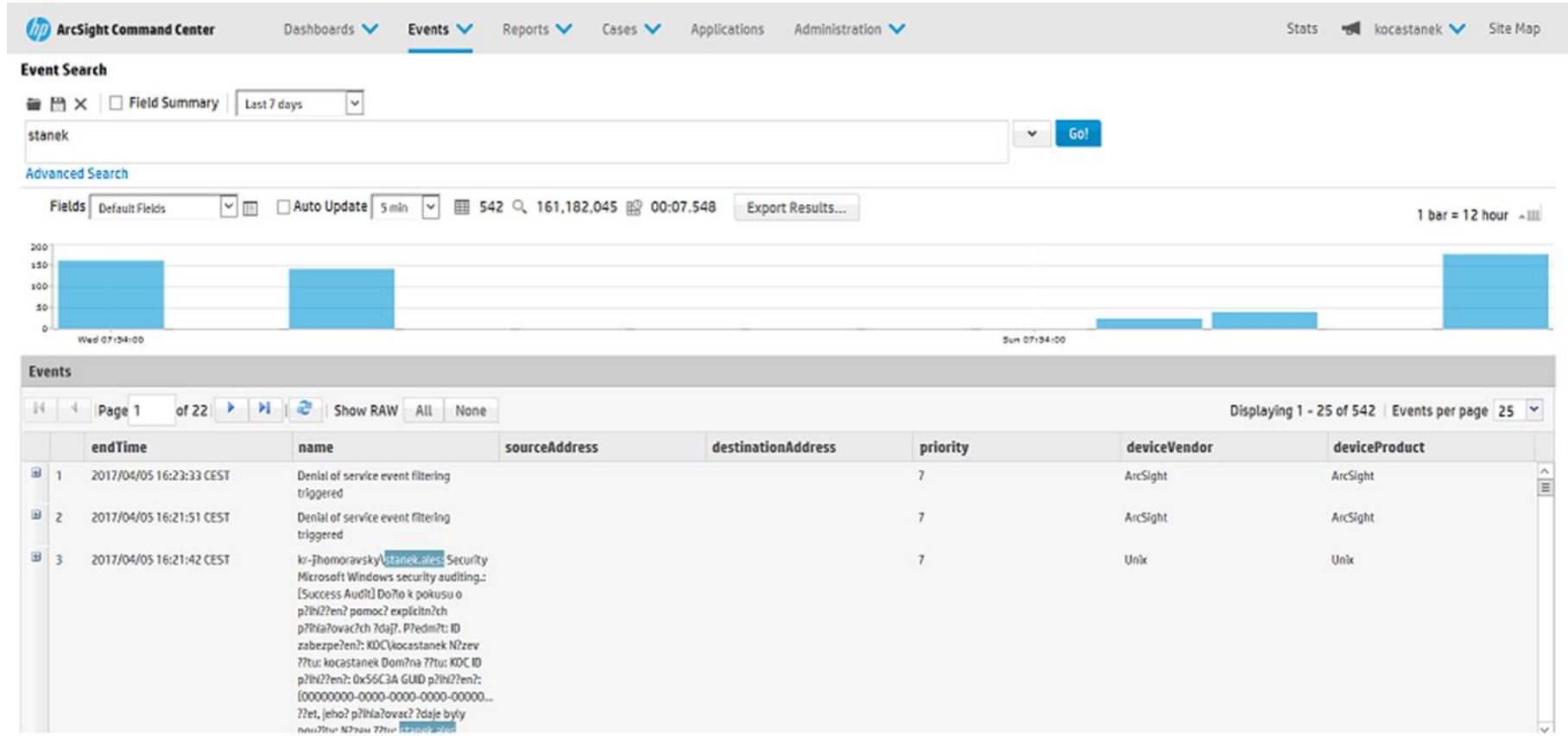
# Log management



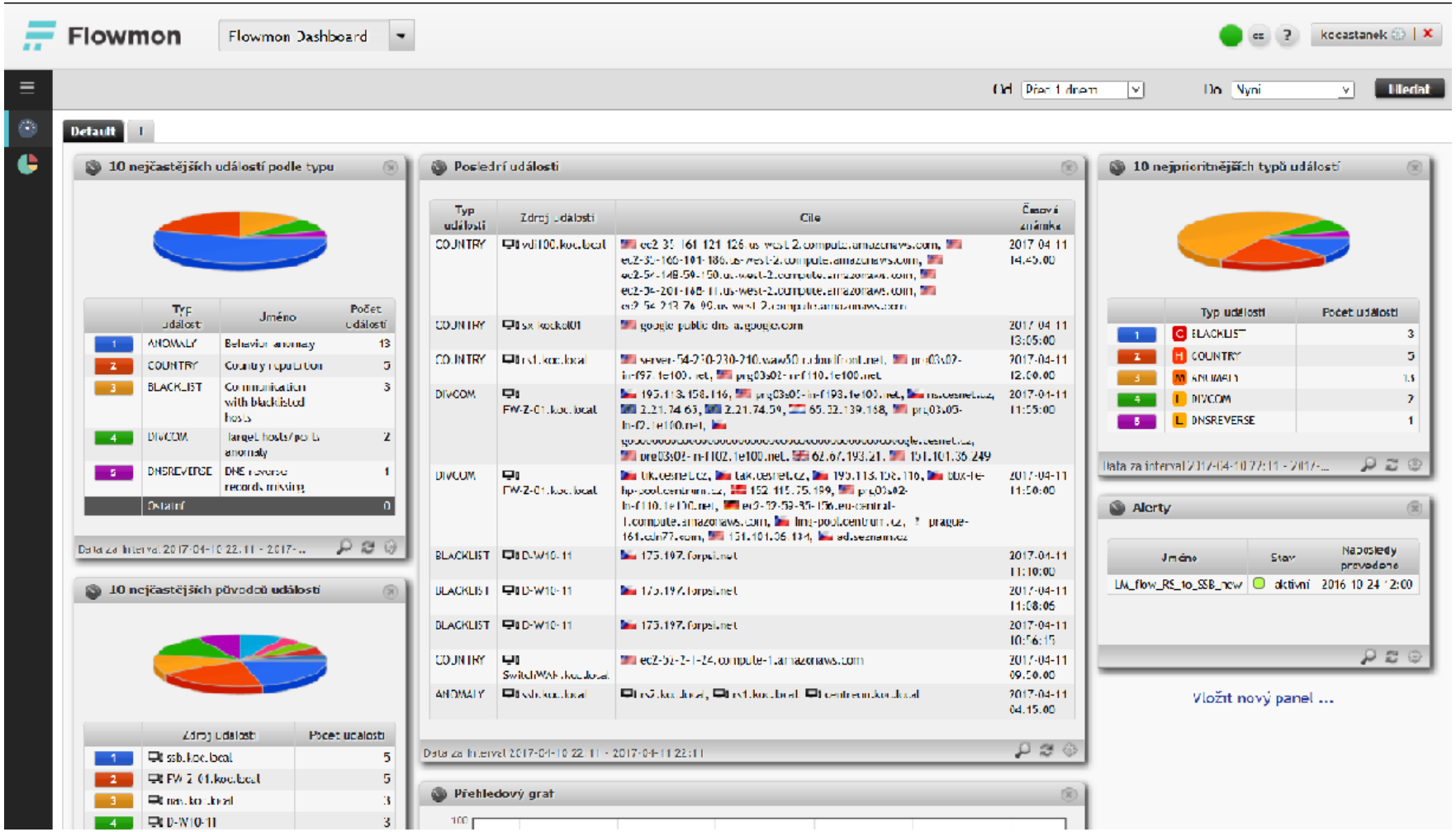
# Provozní monitoring



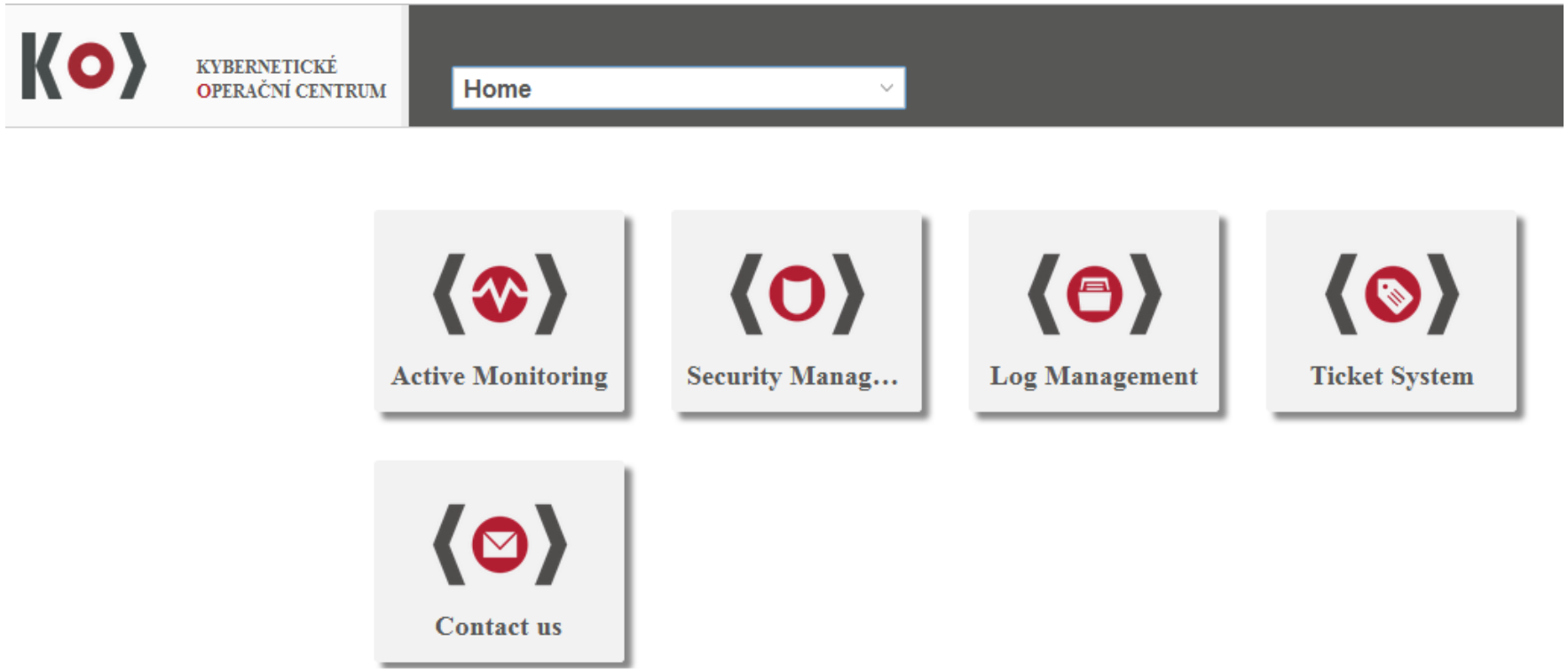
# SIEM – Security information & event management



# Monitoring síťového provozu

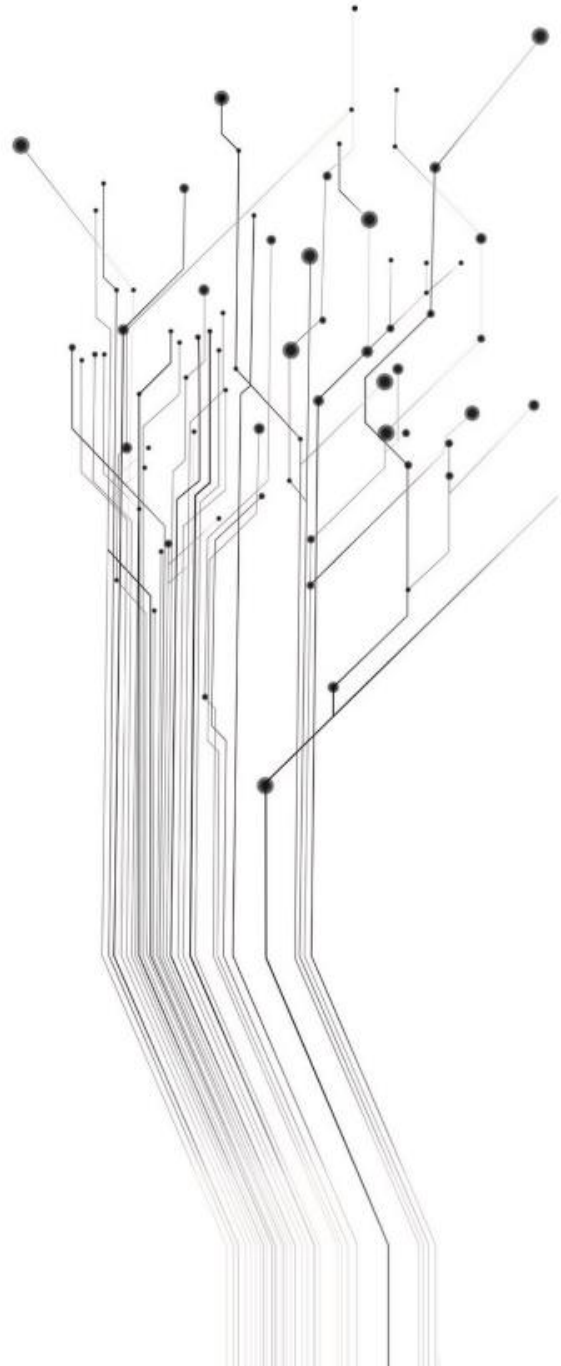


# Webové prostředí pro zákazníky



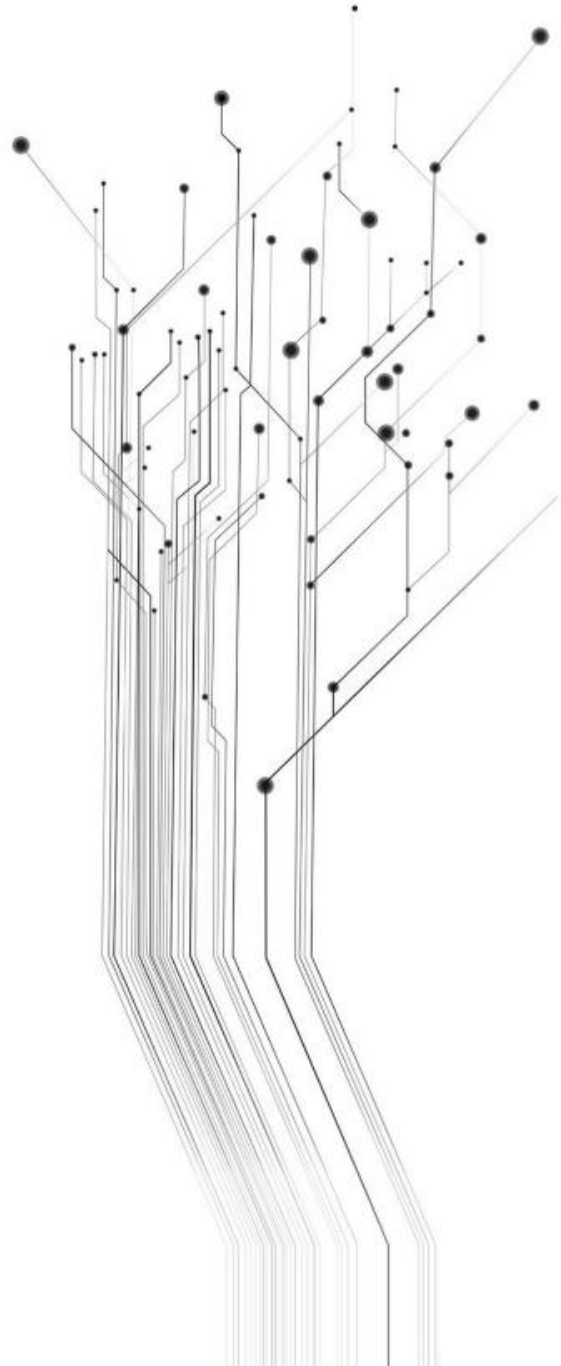
# Přínosy KOC JMK

- 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

- Je spuštěn monitoring sítí: KOC, JMK, SÚS, SŠIPF, Nemocnice Kyjov
- Do konce roku 2017 připojíme dalších šest organizací (budou to krajem zřízené nemocnice)



KYBERNETICKÉ OPERAČNÍ CENTRUM

# Dotazy?

Děkuji Vám za pozornost