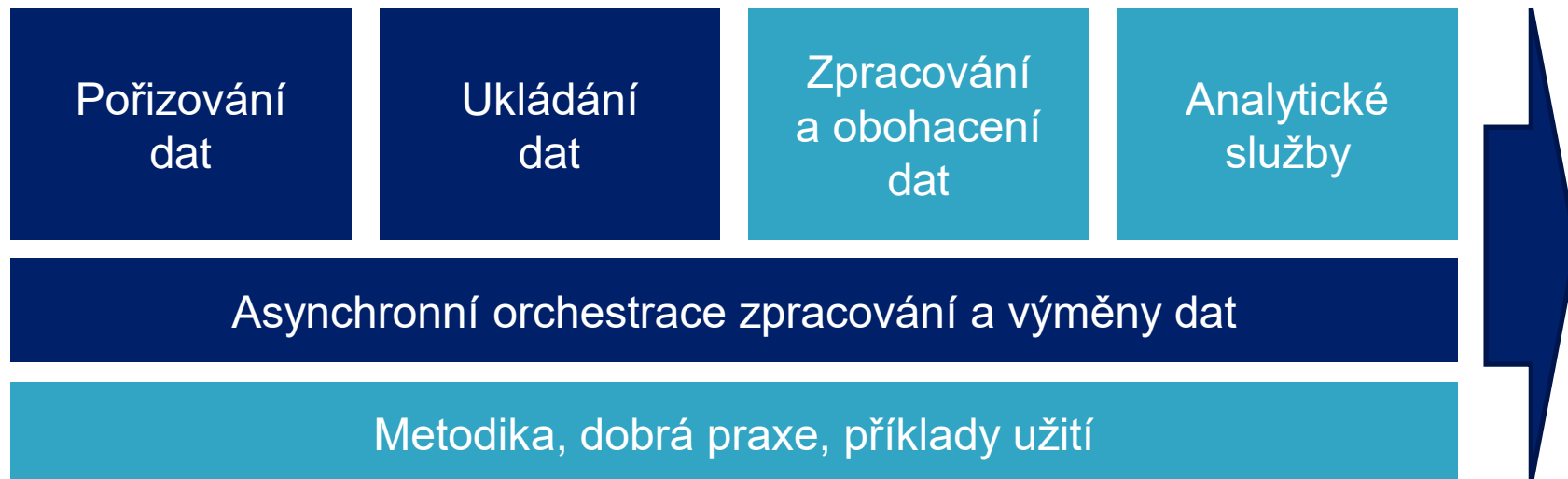


Pokročilé techniky analýzy informací z ICT infrastruktury

Seminář Od dat ke znalostem II.
28. 11. 2019 Policejní akademie, Praha

find ►
understand ►
use ►

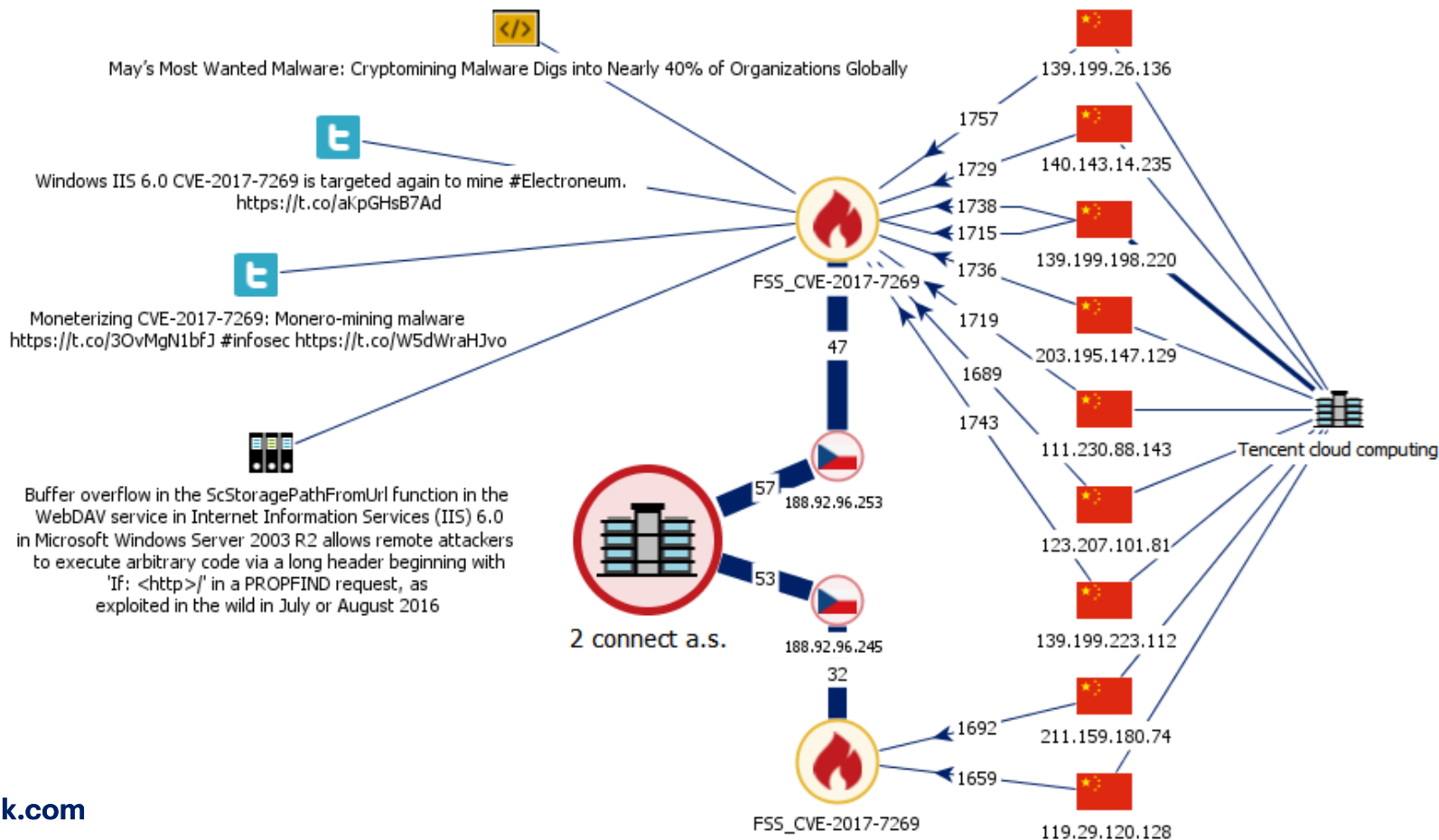
Data – informace – znalosti



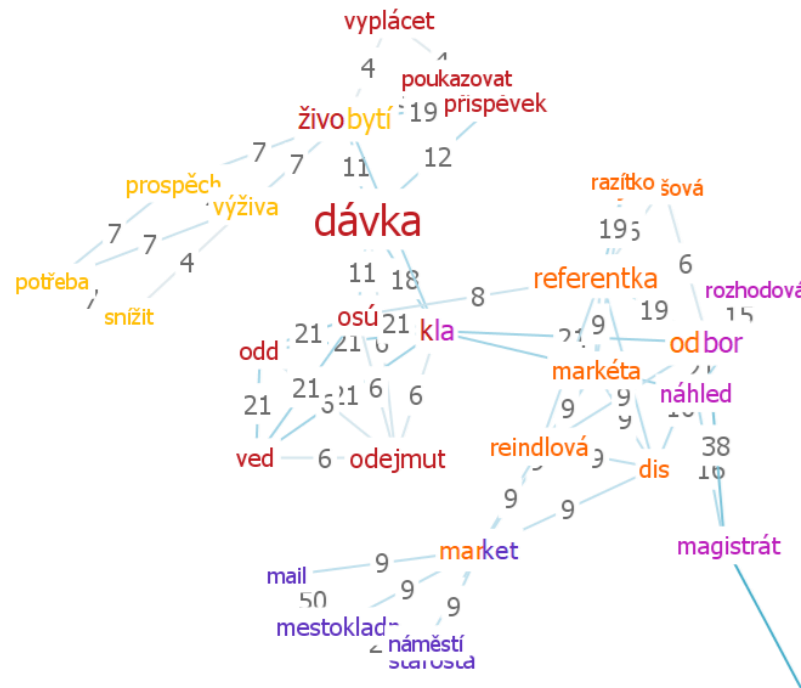
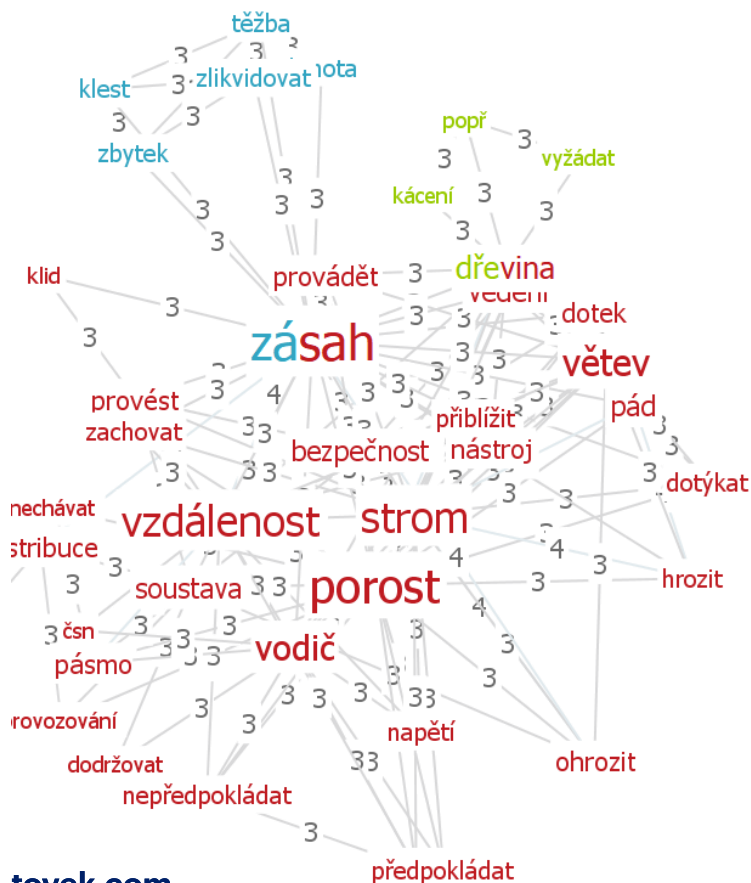
Motivace

- ▶ Dostat informace ze stroje k člověku
 - ▶ Potřeba porozumět a rozhodnout
 - ▶ Omezení časem, znalostmi a schopnostmi
- ▶ Definovat vlastní pravidla
 - ▶ Unikátní know-how
 - ▶ Pohled nezávislý na třetí straně

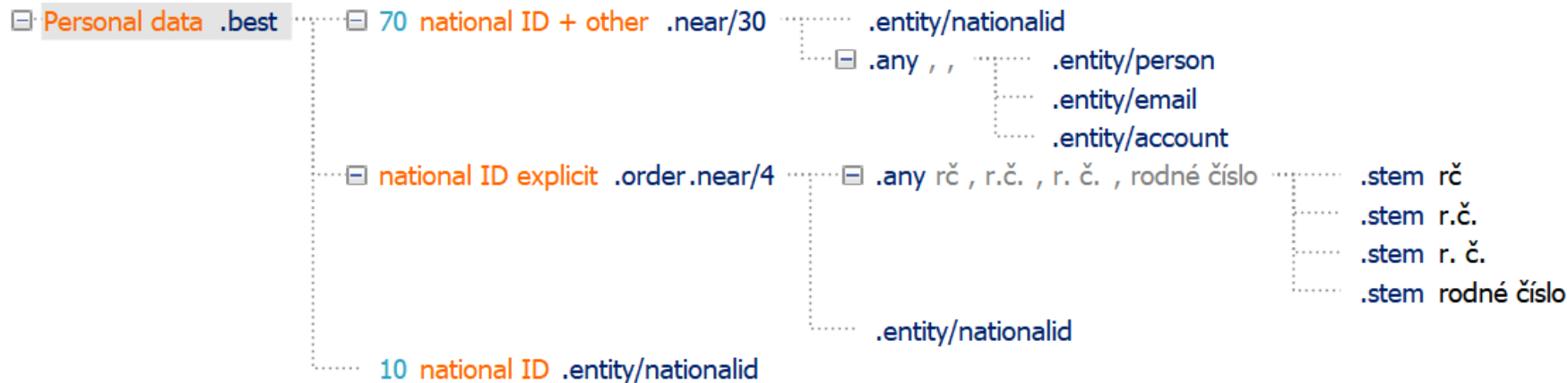
Linková analýza bezpečnostních incidentů



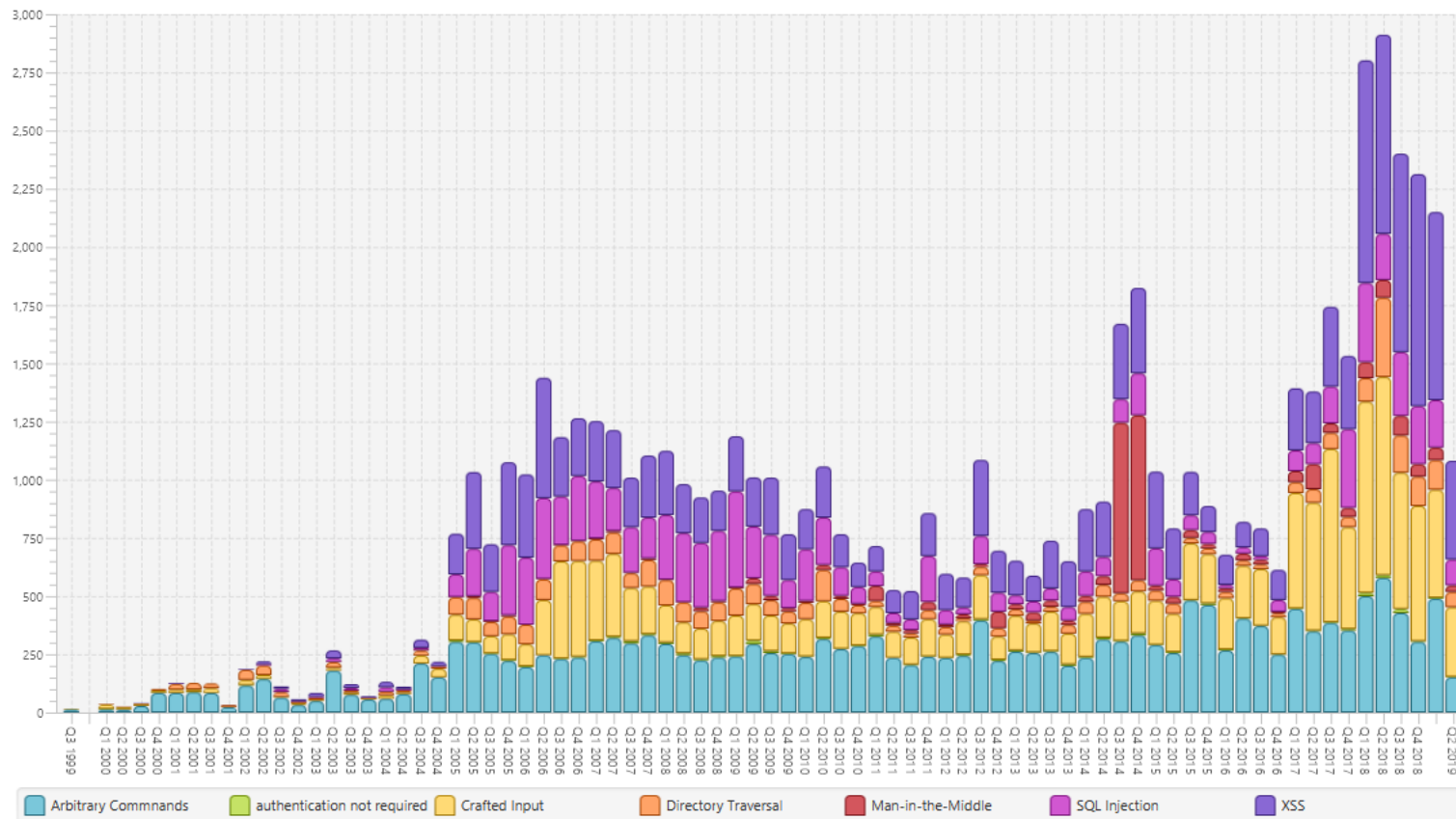
Obsahová analýza získaných dat



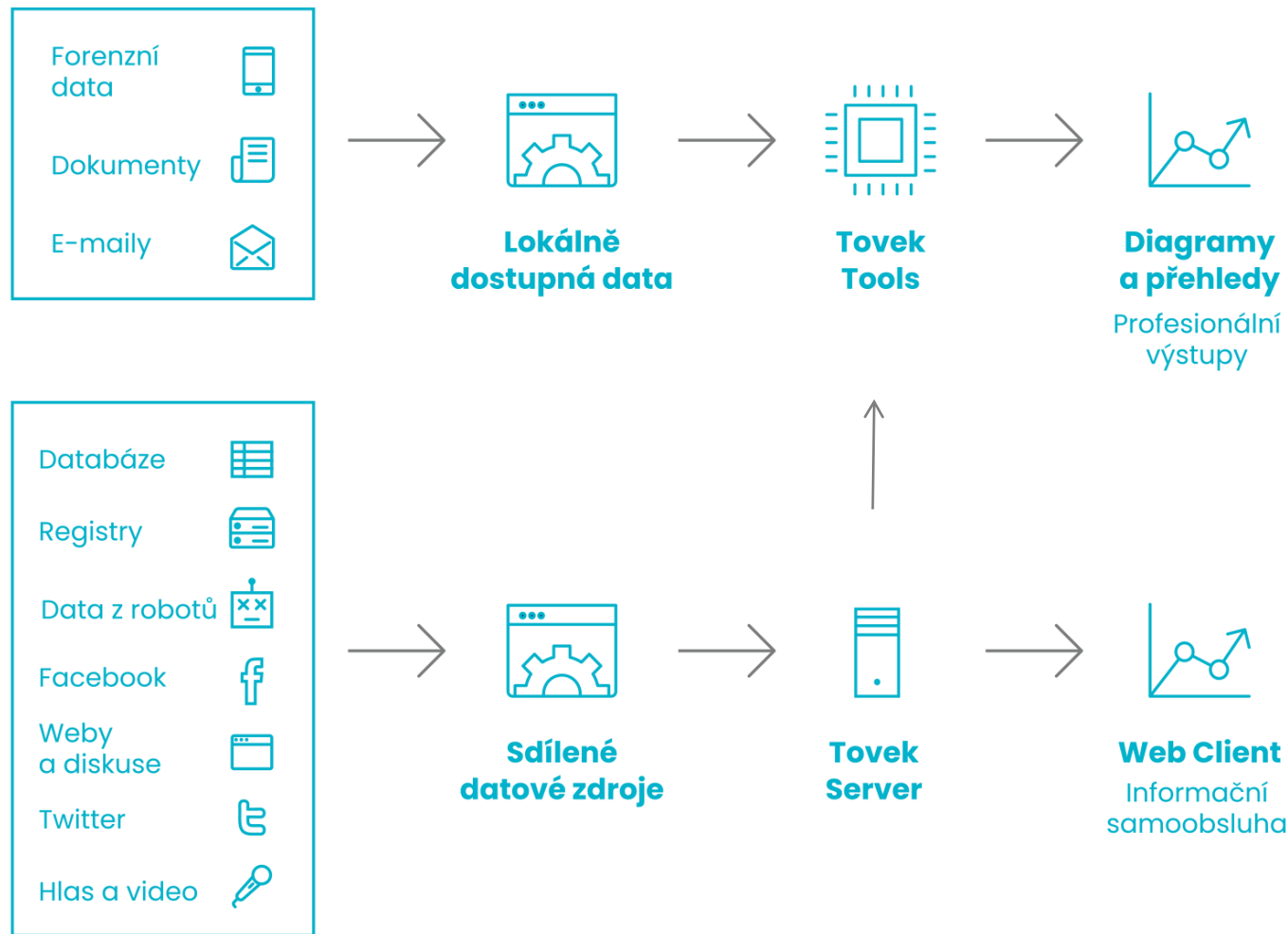
Extrakce entit ze získaných dat



Vyhledávání exploitů a zranitelností



Platforma TOVEK



Hlavní přínosy platformy TOVEK



Názorná prezentace **získaných znalostí** a jejich uchovávání, sdílení a využívání



Automatizace **zpracování dat**, více času na kvalitnější **analýzu informací**



Jednotný přístup k různorodým datovým zdrojům z **jednoho místa**

Information



Děkuji vám za pozornost

**Pokročilé techniky analýzy
informací z ICT infrastruktury**

Miroslav Nečas
necas@tovek.cz

www.tovek.cz