

SIEM včera a dnes

Pavol Dovičovič, EMM

*e*FOCUS

EMM

CHRÁNIME VAŠE HODNOTY

SIEM

- Security Information and Event Management
- Prvýkrát pomenovaný v roku 2005
- V novembri 2014 bolo na trhu 73 SIEM produktov

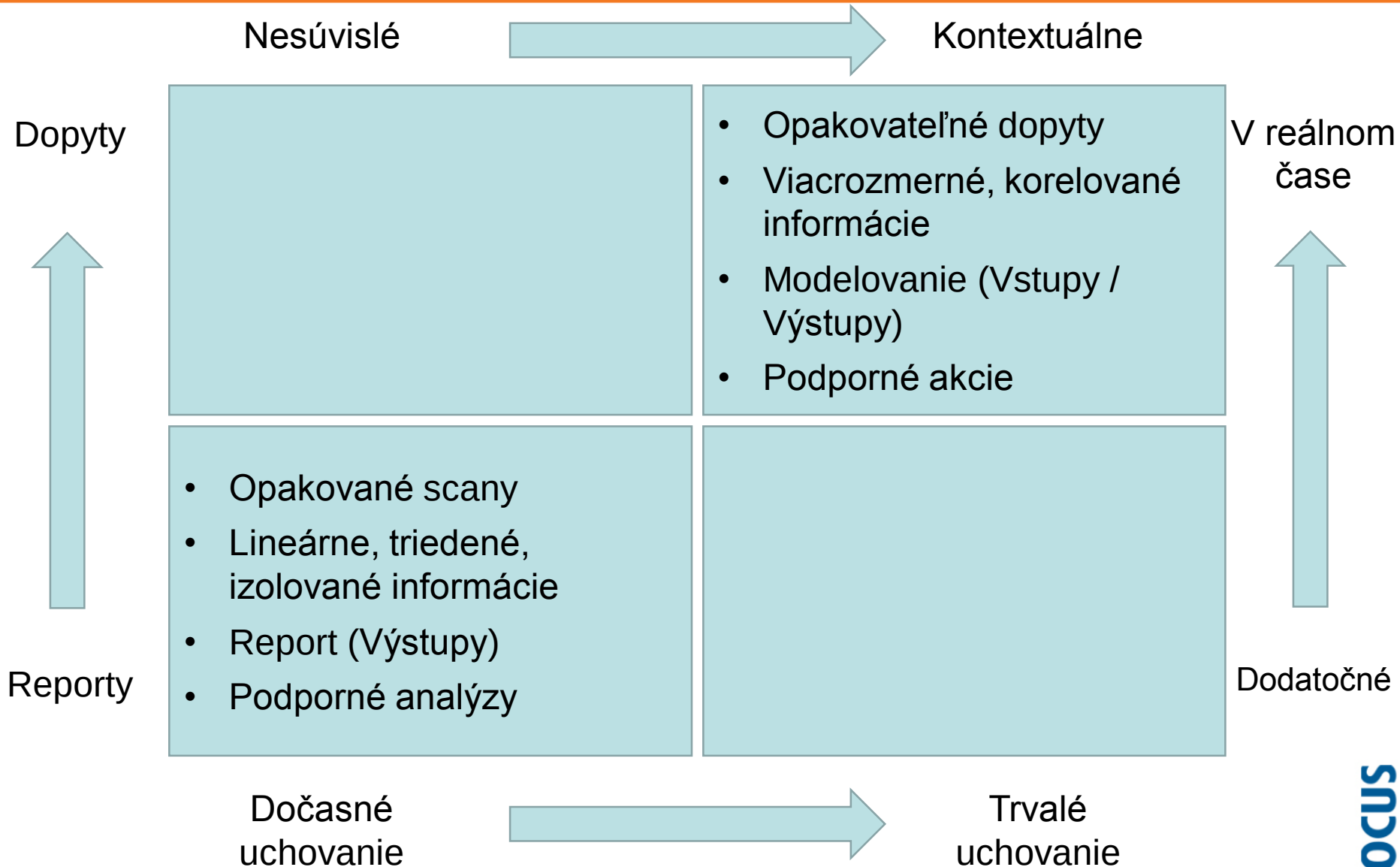
SIEM včera



- Éra pred SIEM-om
- Logovanie ???
- Centralizovaný zber logov ???
- Kontinuálne vyhodnocovanie ???

SIEM evolúcia

(od zásobníka bezpečnostných informácií ku bezpečnostnému spravodajstvu)

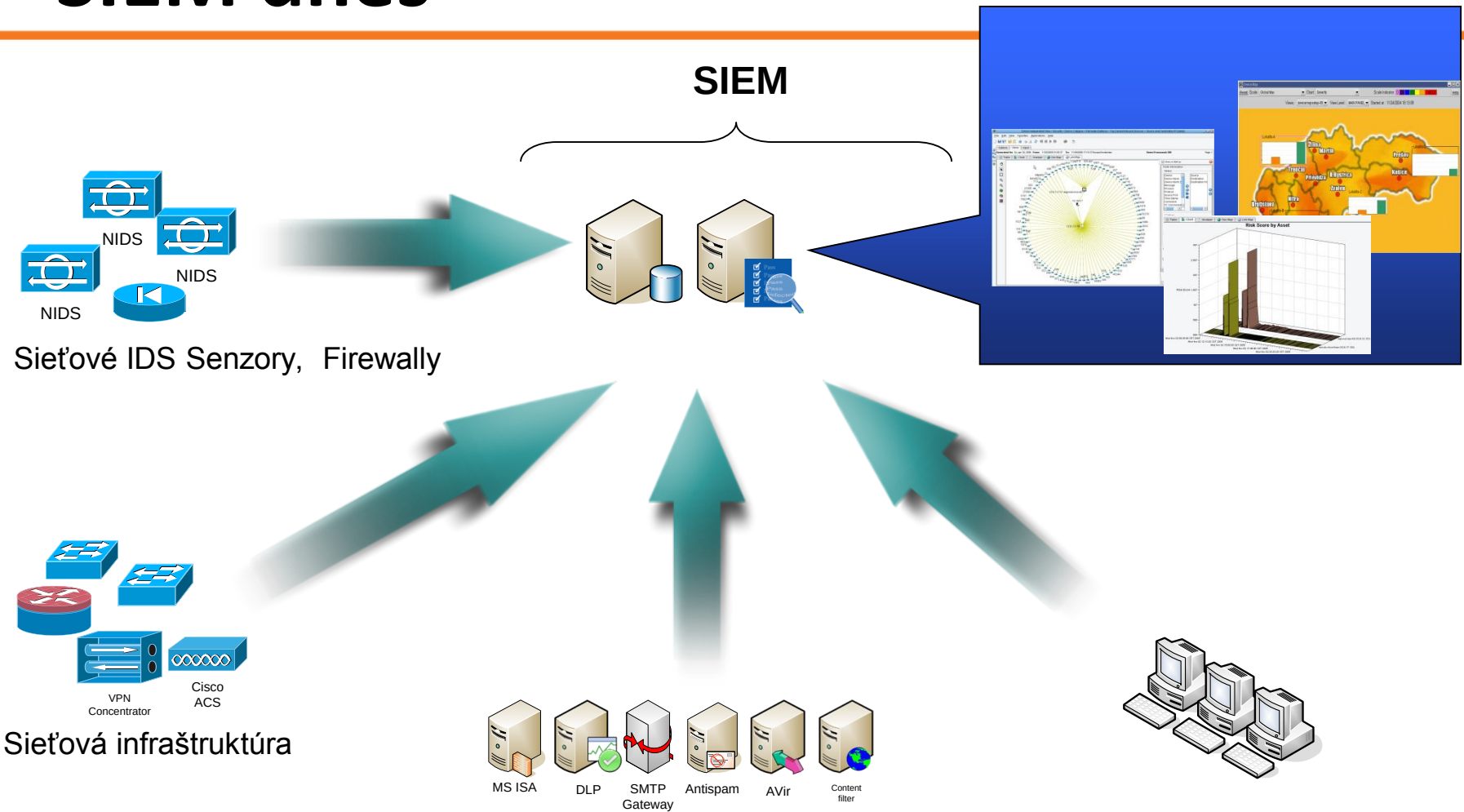


SIEM dnes



- **Včera – Zber**
 - Zber logov a udalostí
 - Signatúry
- **Dnes – Aktivita**
 - Real-time monitoring
 - „Context-aware“ detekcia anomálií
 - Automatické korelácie a analýza

SIEM dnes



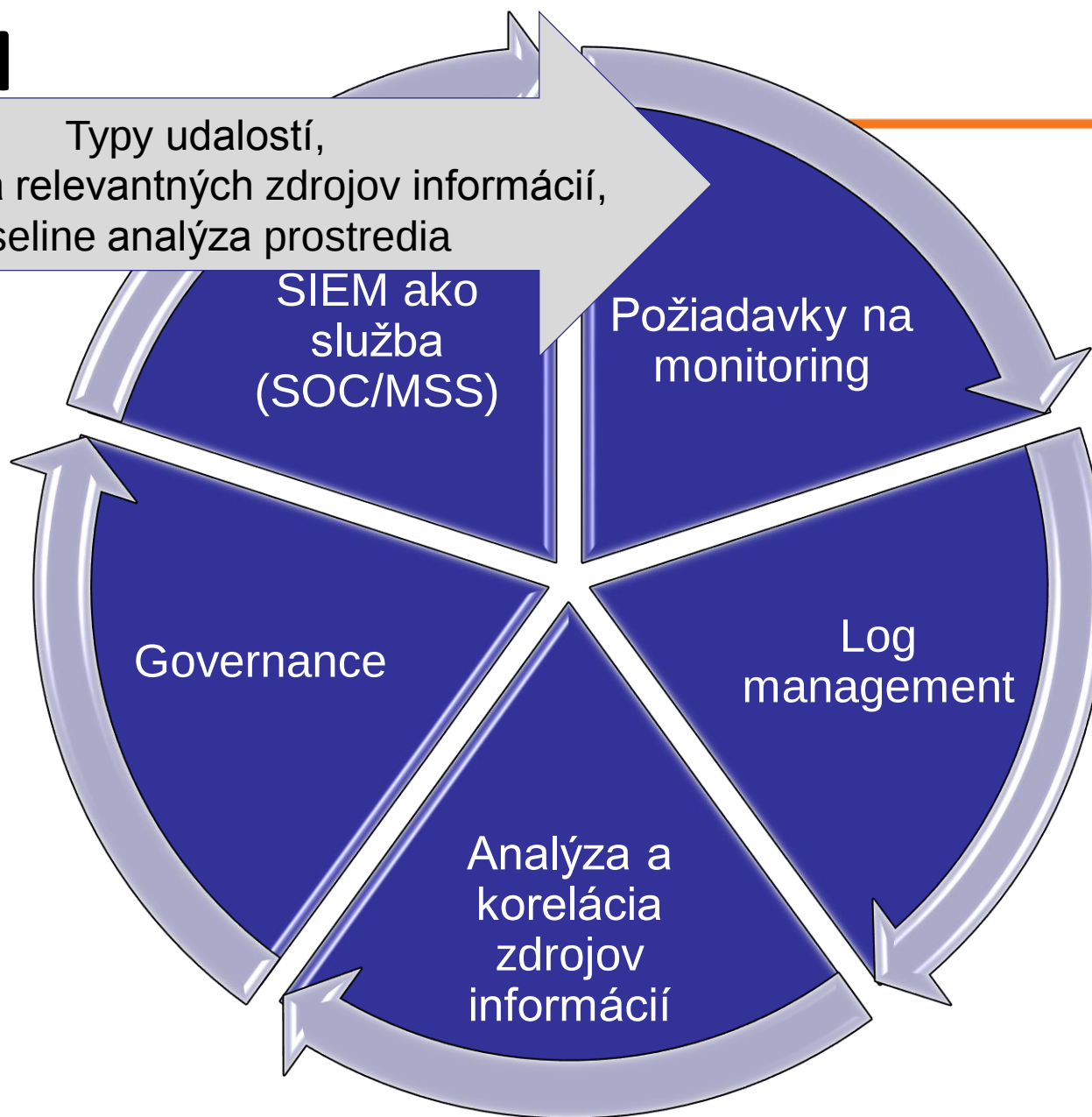
SIEM

- SIEM v „osobnom“ vlastníctve
- SIEM na „leasing“
- SIEM s podporou
- SIEM ako Cloud služba
- Prevádzkovanie SIEM v prospech zákazníka
- Monitoring bezpečnosti ako služba (SOC)

Managed Security Services

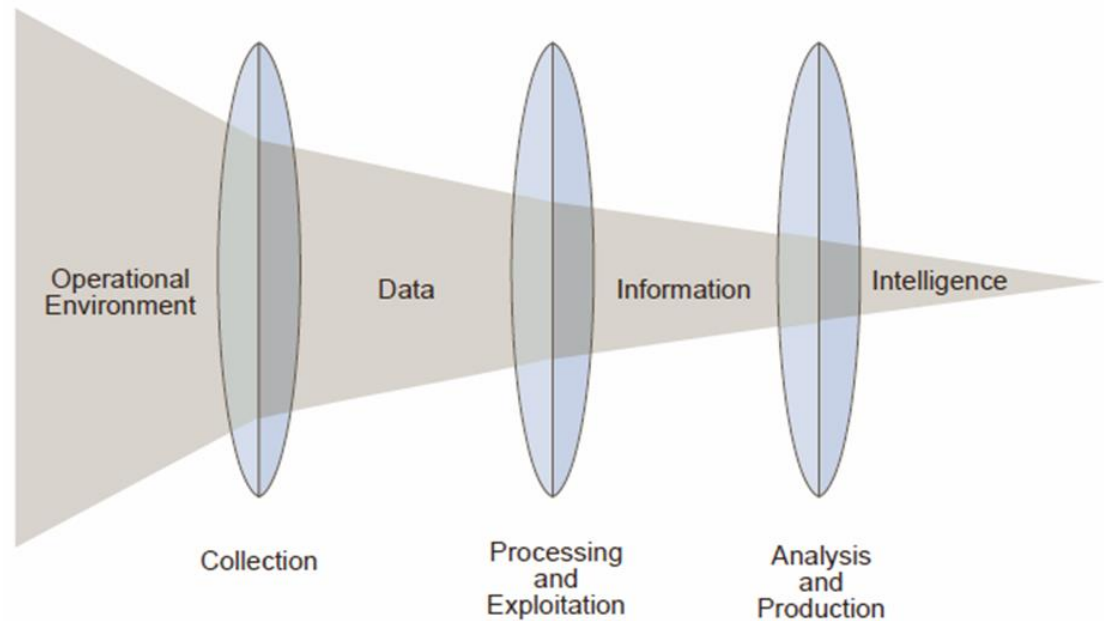
SIEM

Typy udalostí,
identifikácia relevantných zdrojov informácií,
baseline analýza prostredia



SIEM zajtra ?

- Nové zdroje informácií ?
- „Integrácia“ ľudí ?
- Internet of Things ?
- ...



Ďakujeme za pozornosť

eFOCUS

EMM

CHRÁNIME VAŠE HODNOTY