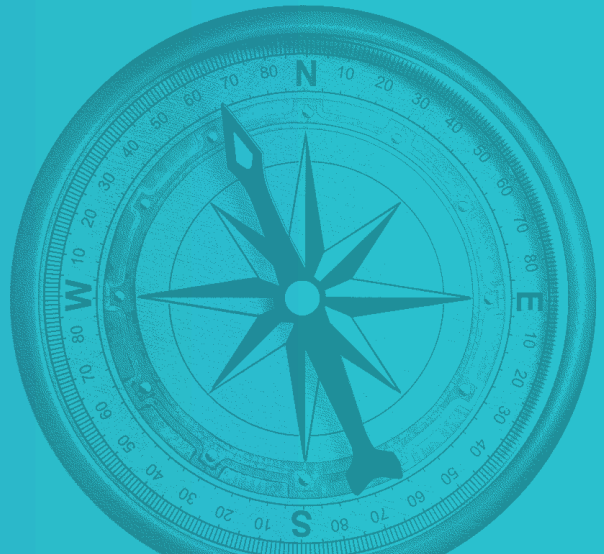
Bezpečnostní monitoring a ochrana citlivých informací

Radek Vašíček
Security BDM

radek.vasicek@alef.com



ALEF

Proč sbírat a analyzovat informace?

Pokud nesbírám …

Nevidím a nevím,

- že se **NĚCO** děje
- **CO** se děje?
- **ČEHO/KOHO** se to týká?
- **KDY** se to děje?
- Jak **DLOUHO** se to děje?
- **PROČ** se to děje?
- Jaké jsou **DŮSLEDKY**
- **…**

Nemohu

- Včas reagovat
- Rychle a řešit

ALEF

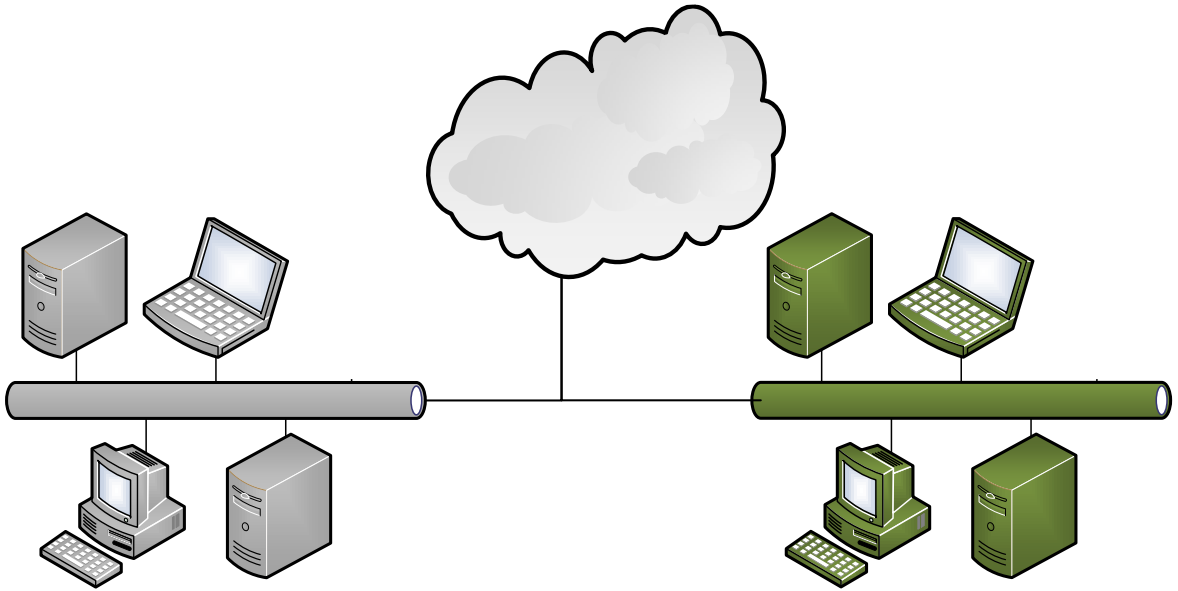
Monitoring jako opatření

- Bez bezpečnostního monitoringu problematická detekce porušení zabezpečení citlivých informací

- Potenciálně citelné reputační riziko při jeho absenci

ALEF

Monitoring jako opatření



ALEF

LOG management – příklady

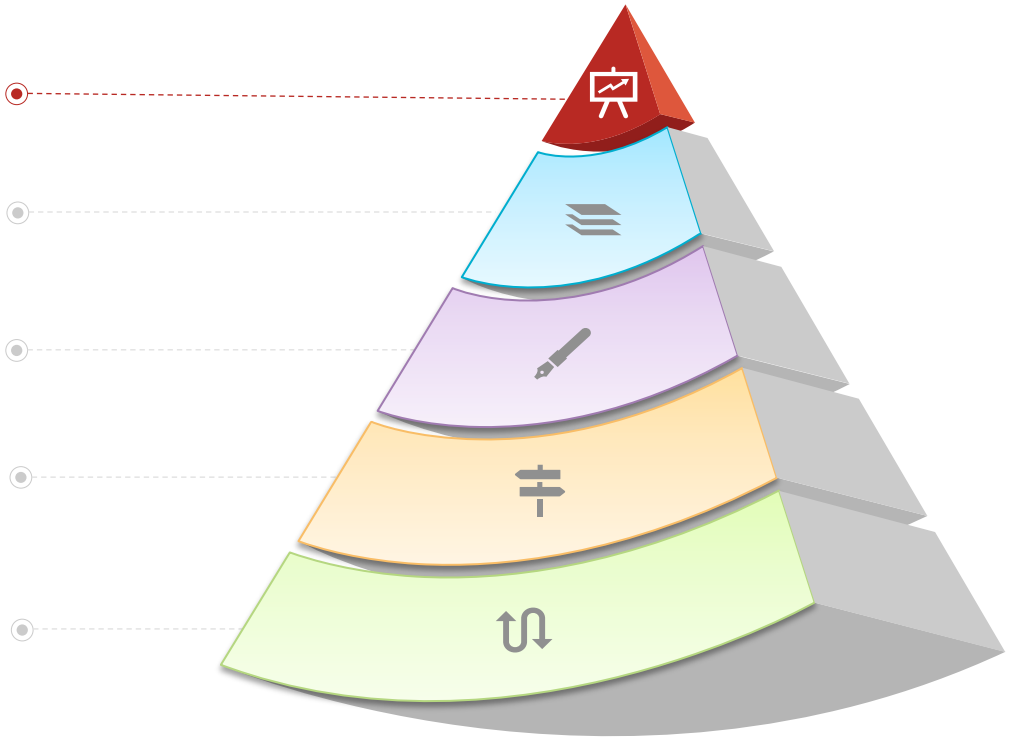
Drill-down v událostech

Sledování přístupu ke službám (adresářovým / db / souborovým)

Analýzy, reporty, dohled, monitoring, audit

Sledování konfiguračních změn

GDPR – Kdo, kdy a jakým způsobem přistupoval k systémům s osobními daty



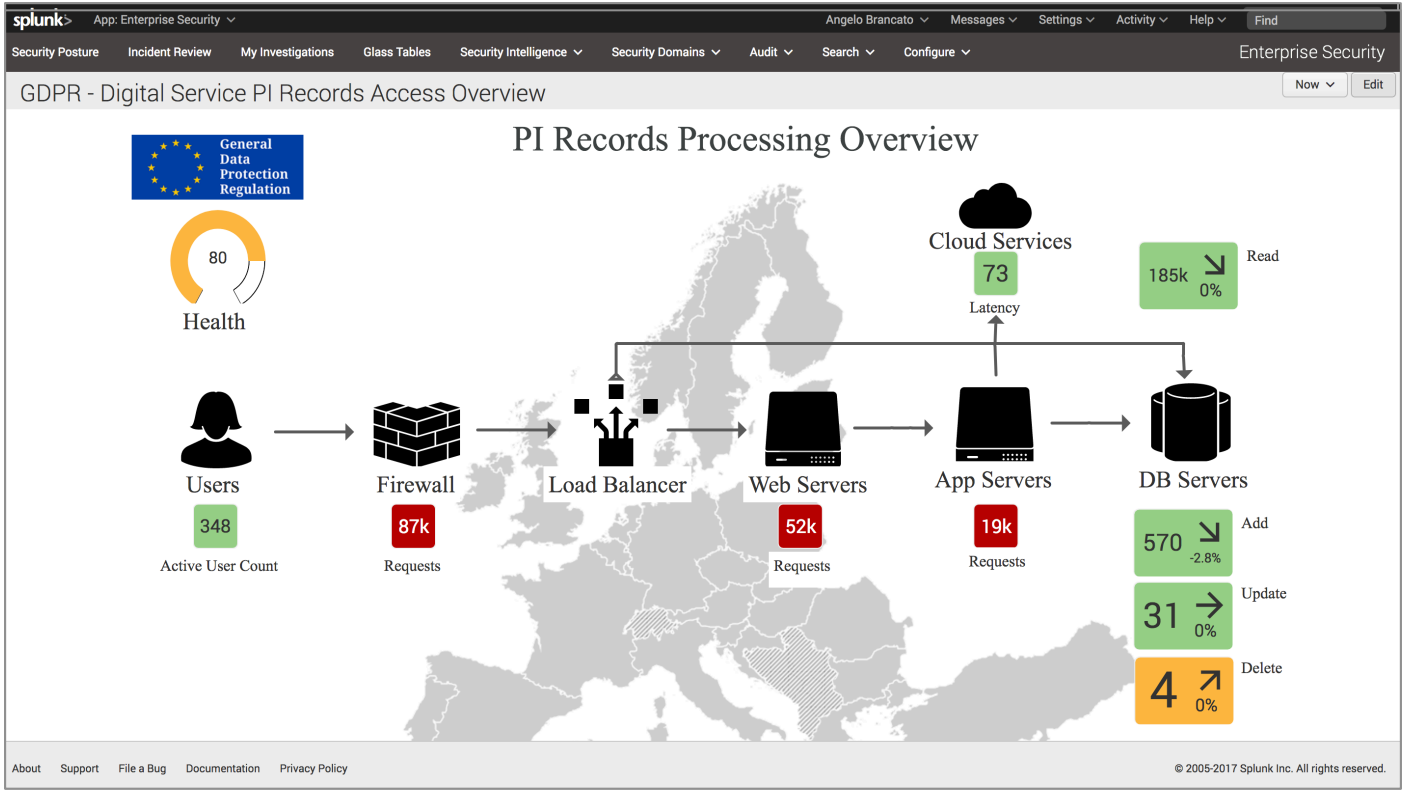
ALEF

Monitoring jako opatření

- Komplexnější variantou dobře navržený log management a SIEM
- Log management navíc nemusí agregovat pouze bezpečnostní data…
- …a SIEM nemusí být jen SIEM

ALEF

Monitoring jako opatření



ALEF

splunk>

Monitoring jako proces zpracování

Námět k zamyšlení:

Zpracováváme-li v rámci monitoringu IP adresy a další data útočníků…

….a o zpracování je třeba subjekt údajů informovat...

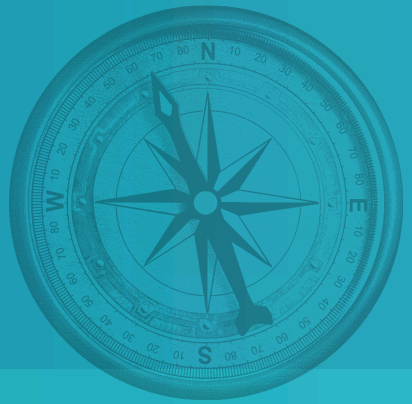
…není třeba útočníkům zpracování hlásit?

ALEF

Shrnutí

- Bezpečnostní monitoring je nutné zvažovat nejen jako opatření, ale i proces
- Nehlaste útočníkům, že zpracováváte jejich údaje

ALEF



Děkuji Vám za pozornost

ALEF