SIEM
Bezpečnostní monitoring

13.4.2015

Experience the commitment®

O společnosti CGI

High-end business and IT consulting

69,000 professionals, 85% shareholders*

10,000 clients across the globe

System integration, IT and business process outsourcing

400 offices, 40 countries around the world

Client satisfaction: 9.1/10

100+ mission-critical IP-based solutions

$10B annualized revenue

Světově 5. největší nezávislý dodavatel IT služeb

CGI Czech, Slovak & Eastern Europe (CS&EE)

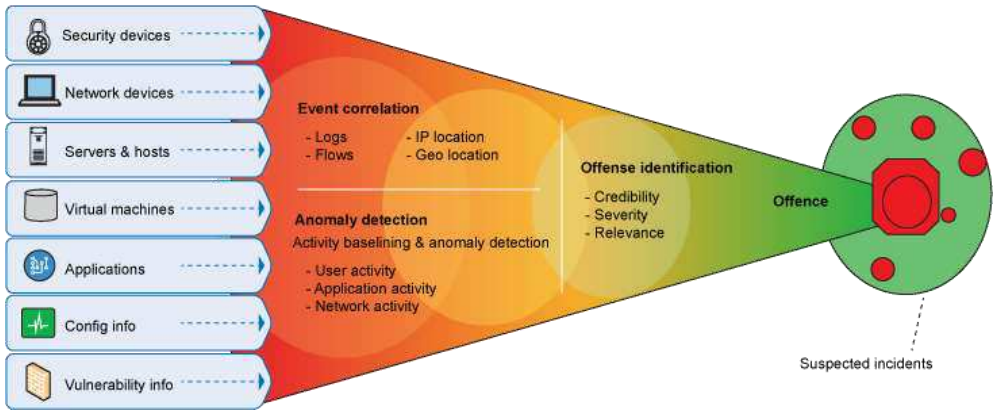
- Sídlo v Praze
- Téměř 600 zaměstnanců, z toho 300 v ČR
- Kanceláře: Praha, Brno, Plzeň, Bratislava, Budapešť; otevíráme v Ostravě
- Působíme v regionu CSEE (CZ, SK, HU, HR, MK etc.)
- Dodáváme pro veřejný sektor, průmysl, transport a distribuci, energetiku & utility, finanční sektor
- Datová centra umístěná v Praze a v Brně
- Certifikáty: ISO 9001:2000 & TickIT, ISO 9001:2008 & TickIT, EN ISO 14001:2004, ISO/IEC 20000-1:2011, ISO/IEC 27001:2006

Co je SIEM (Security Information and Event Management)

- Řešení pro správu bezpečnostních informací a událostí
- Zahrnuje:
  - **SIM** – dlouhodobé uložení událostí, jejich analýza a hlášení problémů
  - **SEM** – monitoring infrastruktury, korelace a generování výstrah v reálném čase

Klíčové funkce SIEM

- Agregace a filtrace dat – sběr logů
- Korelace událostí
- Generování výstrah
- Reporting
- Detekce hrozeb a anomálií
- Správa incidentů



Proč Implementovat SIEM ?

- Požadavky odvětvových regulátorů – NERC, HIPAA, PCI DSS …
- Legislativní požadavky – zákon o kybernetické bezpečnosti (sběr, detekce a vyhodnocení událostí)
- Požadavky auditorů a dobrých praktik
- Zvýšení úrovně bezpečnosti
  - Vlastní uvědomění potřeby správy, detekce a následné forenze událostí a incidentů
  - Přehled v událostech a orientace v prostředí - řešení problému s hledáním jehly v kupce sena)

SIEM jako univerzální řešení všech problémů

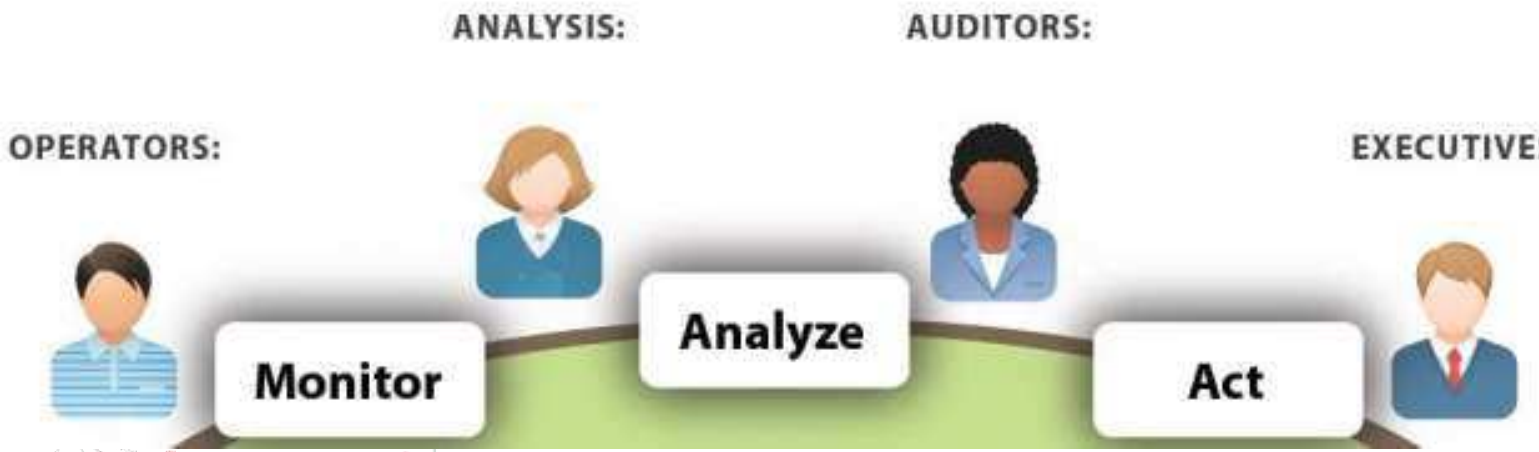
- **SIEM nasadíme a máme na pár let vystaráno**
  - Nutnost reagovat na interní podněty/změny – nové systémy, pracovníci, update/upgrade systémů a aplikací (s novými zranitelnostmi), nové interní hrozby
  - Nutnost reagovat na externí podněty – nové hrozby externí hrozby, nové systémy a způsoby práce
- **V logách to určitě bude** - podcenění prvotní analýzy, log management a retence dat
- **Hlavně něco rychle koupíme a pak to zaintegrujeme** - opomíjení organizačních a procesních dopadů (absence koncepčního přístupu)

- **Výrobce SIEM určitě ví co potřebujeme logovat a navíc použijeme generické korelace** – podcenění požadavků na lidské zdroje, integrátora/implementátora

CGI

Doporučení pro implementaci SIEM

- Před výběrem technologie proveďte detailní analýzu prostředí a obecně požadavků – technických i organizačních
- Buďte připraveni na změny – technické, procesní i organizační (např. nutnost úprav eskalační procesů) – SIEM prorůstá celou organizací
- Začněte od základních příkladů užití a postupujte ke komplexnějším a systém postupně rozšiřujte
- Člověka nelze plně nahradit – berte v potaz požadavky na lidské zdroje, organizační zajištění a součinnost s ostatními útvary



Děkuji!

CGI

Experience the commitment®