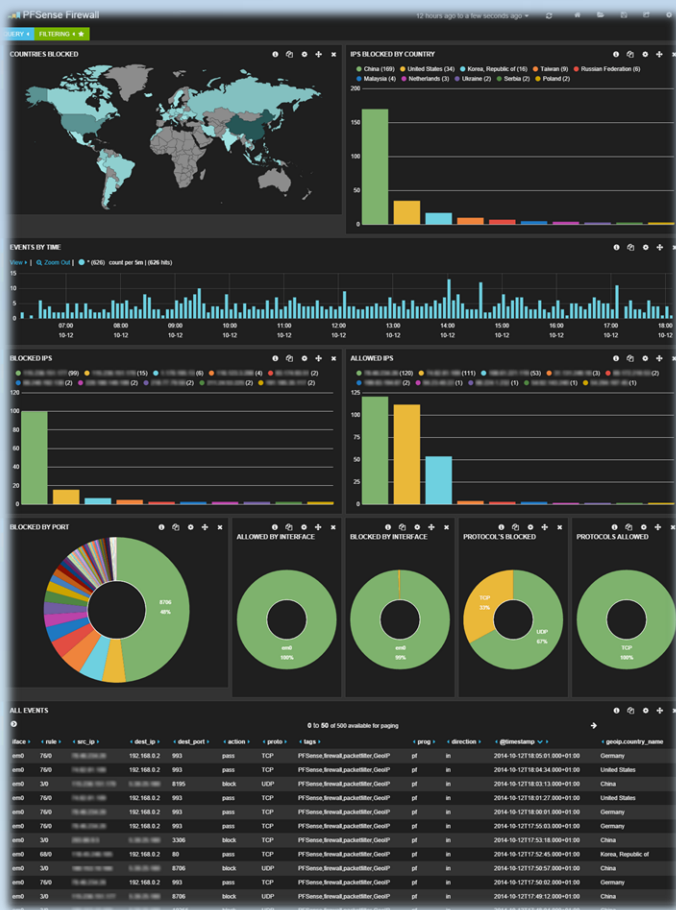


Outsourcing správy nástrojov SIEM – áno, alebo nie?

Ján Andraško, Binary Confidence

Prečo SIEM?



- úroveň a množstvo útokov, prienikov a hrozieb stúpili exponenciálne
- posun od prevencie k **detekcii**
- monitorovanie udalostí je nevyhnutný komponent v „defense-in-depth“ stratégii IT bezpečnosti
- všetky bezpečnostné normy (PCI-DSS, ISO 27k, ...) vyžadujú implementáciu a **aktívne používanie SIEM**
- SIEM nie je strieborná guľka, ktorá sama vyrieši všetky problémy

SIEM potrebuje ľudí

- SIEM nie je „nastav a zabudni“

Potrebné profily:

- SIEM administrátor
 - udržiava, aktualizuje
- SIEM expert
 - upravuje/prispôsobuje/vytvára nové pravidlá
- Bezpečnostný analytik
 - skúma reporty aktivity, prešetruje alerty



Výhody outsourcingu SIEM nástrojov



- zamestnanci
- zručnosti a povedomie o bezpečnosti
- technické prostriedky a infraštruktúra
- objektivita a nezávislosť
- kvalita poskytovanej služby
- náklady

Zamestnanci

- nedostatok kvalifikovaných bezpečnostných profesionálov na trhu
- náklady na prijatie, školenia, platy a udržanie vysoko kvalifikovaných zamestnancov prechádzajú na MSSP
- MSSP si skôr udrží bezpečnostných expertov ponukou množstva kariérnych možností v oblasti IT bezpečnosti
- klient môže sústrediť interné zdroje na činnosti spojené so svojim biznisom



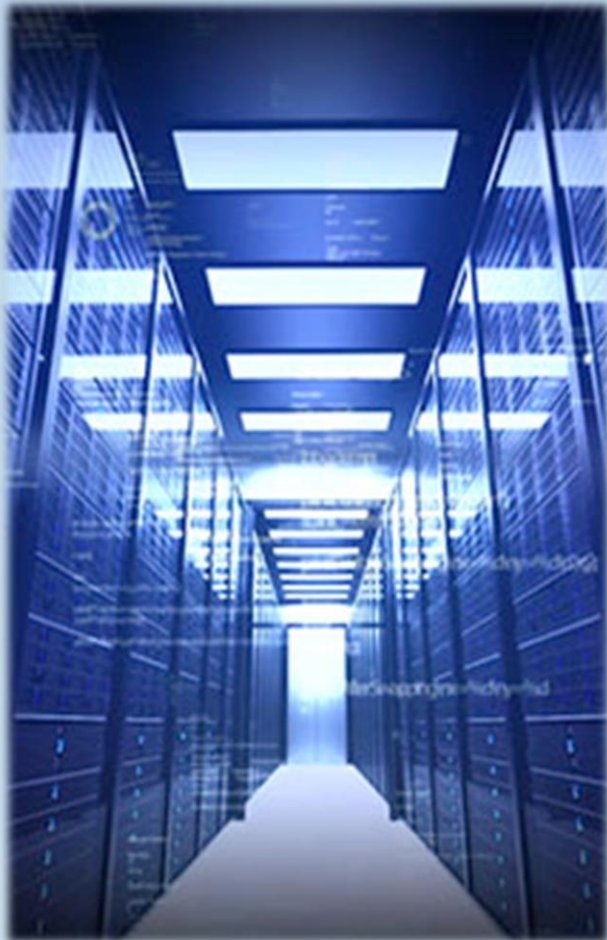
„Ak si myslíte že je drahé najať si profesionálov, počkajte keď si najmete amatérov“ (Red Adair)

Zručnosti a povedomie o bezpečnosti



- interní zamestnanci, ktorí nemajú bezpečnostné pozadie pravdepodobne nie sú takí kompetentní ako bezpečnostní profesionáli MSSP
- MSSP riešia stovky potenciálne nebezpečných situácií denne
- technické zručnosti zamestnancov sú síce žiadúce, no nie sú najdôležitejšie - dôležitejšia je ochota a schopnosť dodržiavať postupy a pravidlá pri riešení bezpečnostných incidentov

Technické prostriedky a infraštruktúra



Security operations center (SOC)

- fyzicky zabezpečené pracovisko s obmedzeným vstupom osôb
- bezpečnostné previerky všetkých zamestnancov
- oddelené miestnosti pre správu bezpečnostných zariadení
- najmodernejšia redundantná infraštruktúra
- fyzické a logické bezpečnostné kontroly
- certifikované a auditované systémy, nástroje, procesy

Objektivita a nezávislosť

- MSSP poskytuje objektívnu analýzu, neovplyvnenú internými vplyvmi
- nemá záujem skrývať, prípadne zľahčovať identifikované hrozby
- interní zamestnanci môžu byť ovplyvnení firemnou politikou či tlakom iných oddelení



Kvalita poskytovanej služby

MSSP:

- poskytuje bezpečnostnú službu 24x7x365 dní v roku
- garantuje úroveň služby a jej dostupnosť
- nedodržanie SLA môže mať finančné následky
- ak poskytuje aj hardvér, je zodpovedný za jeho funkčnosť, aktualizácie a bezpečnú konfiguráciu
- bezpečnostné procedúry sú zvyčajne veľmi dobre zdokumentované a vynucované



Náklady



- náklady na manažované bezpečnostné služby sú vo väčšine prípadov nižšie než náklady na vlastný hw/sw a interných expertov
- MSSP vie rozložiť náklady na viac klientov
- outsourcing je OPEX s **predpovedateľnými mesačnými nákladmi**
- celková úspora cca 20% pri 8x5 a až 75% pri 24x7, v prípade spoločností s mnohými prevádzkami ešte viac

Ďakujem za pozornosť