Představení služeb
Security Expert Center (SEC)

Den otevřených dveří

Petr Tejnský / 19.4.2016

O2 IT Services

Představení SEC

Varianta 1: **Customizace**

- Úprava bezpečnostního monitoringu u zákazníka
- Návrh optimálního řešení na základě detailní analýzy bezpečnostní infrastruktury: nákladový model, architektura, postup implementace atd.
- Maximalizace využití vlastního HW a SW a interních lidských zdrojů

Varianta 2: **Stavba**

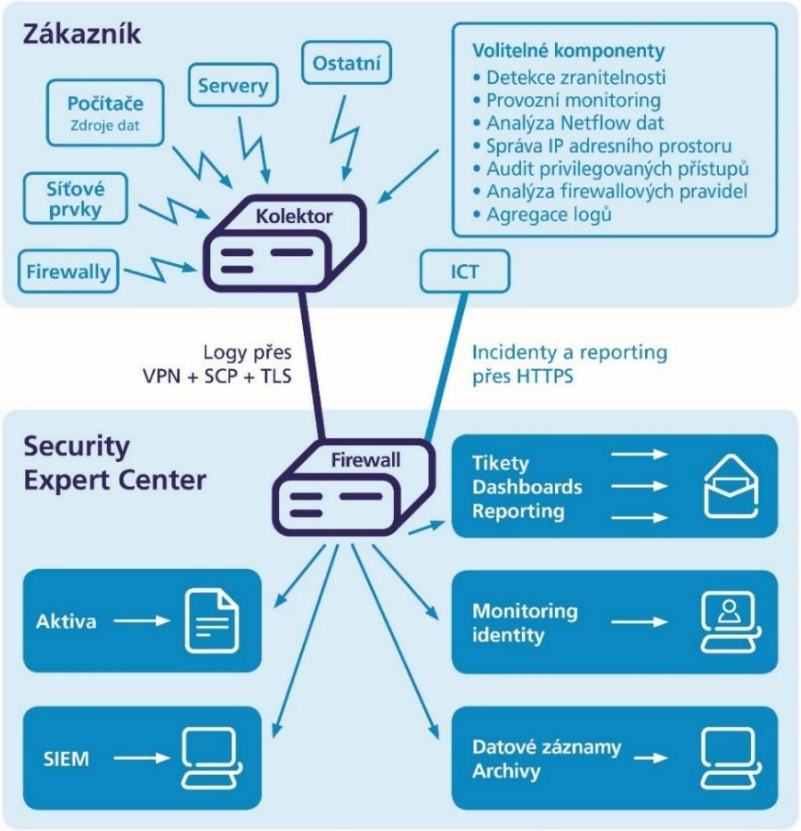
- Implementace nového řešení „na klíč“
- Bez nutnosti hledat volné lidské zdroje na trhu práce
- Náskok proti konkurenci díky prokázanému technickému, implementačnímu a provoznímu know-how

Varianta 3: **Služba SEC**

- Bezpečnostní dohled a monitoring jako komplexní služba, vč. potřebného zaškolení
- Minimalizace investičních nákladů na straně zákazníka
- Vhodné řešení i pro střední a malé společnosti a organizace

O2 IT Services

Ilustrace SEC



Prevence

Detekce

Odpovědnost

O_2 IT Services

Moduly služby SEC

Log Management

Security Management

Active Monitoring

Ticket System

O_2 IT Services

1. Modul Active Monitoring

Monitoring komponent SEC:

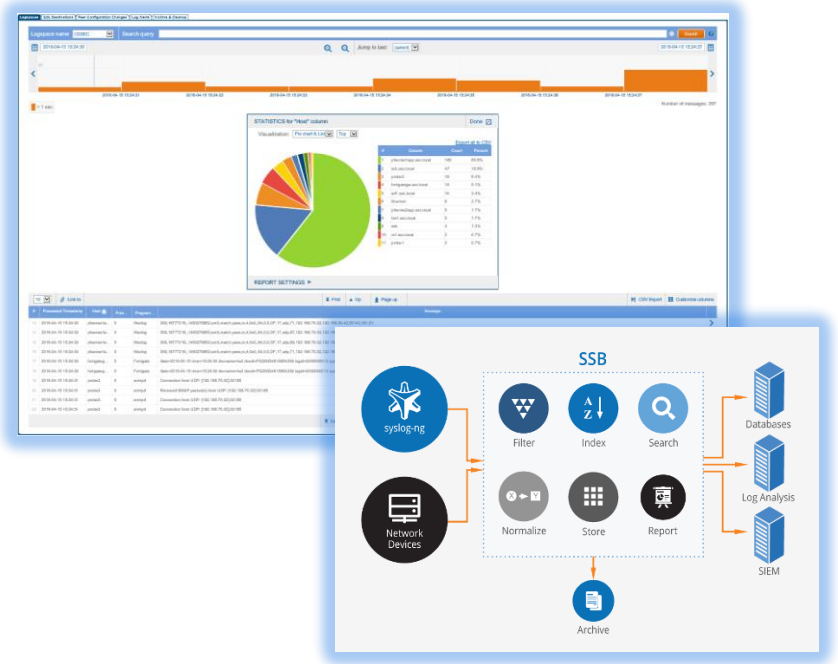
- Hosts
- Services
- VMware, vCenter
- Customer Collectors
- NAS
- NTP
- Switches/Routers/Firewalls/IPS
- FlowMon Anomaly Detection System (ADS)
- SCB Privileged Access Manager (PAM)

O2 IT Services

2. Modul Log Management

Základní parametry Log Managementu:

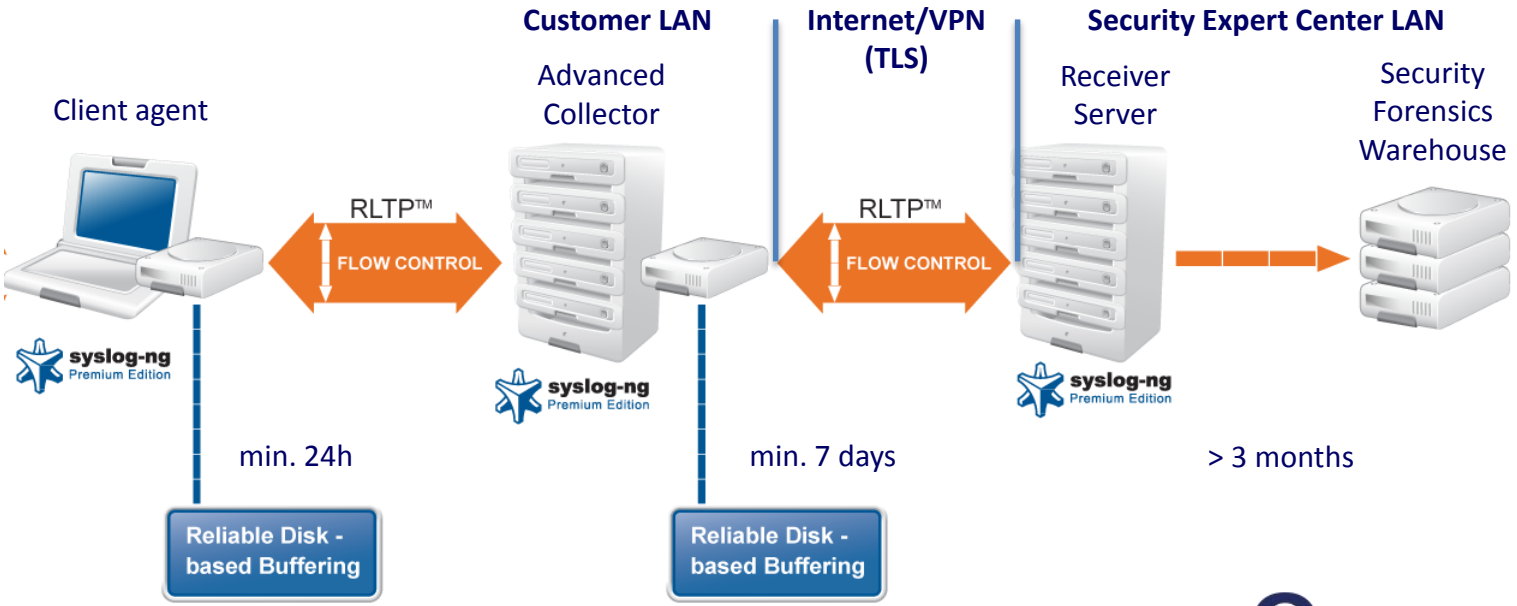
- Archivuje na důvěryhodné a certifikované úložiště (šifrování, časové razítko)
- Klientský agent je součástí služby (Windows, Linux, UNIX)
- webGUI rozhraní pro přístup zákazníků
- Doba uchování záznamů minimálně 3 měsíce
- Indexace až **1,7 TB/day** (100 kEPS) pro TLS komunikaci



O2 IT Services

2. Modul Log Management - pokračování

Tříúrovňové zabezpečení sběru bezpečnostních událostí:

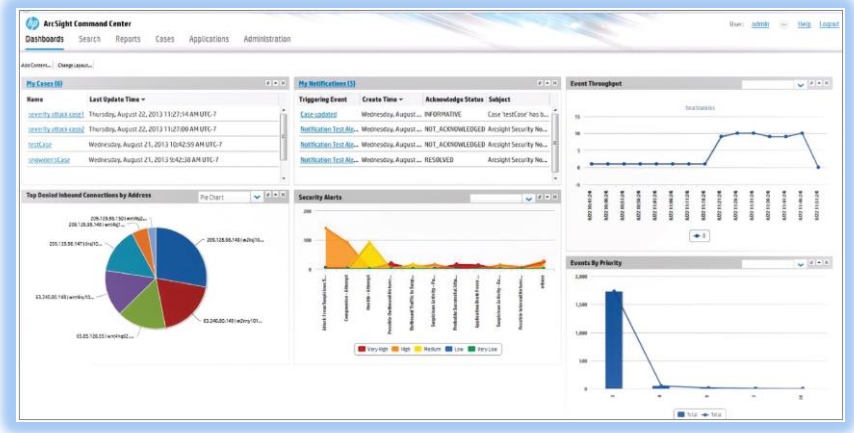


O2 IT Services

3. Modul Security Management

HPE Security ArcSight Enterprise Security Manager (ESM) unikátní SIEM řešení:

- Real-time korelace bezpečnostních událostí z různých typů zařízení (FWs, Switches, OS, App)
- Včasná a přesná detekce vnitřních a vnějších hrozeb (minimalizace „False Positive“)
- Rozsáhla kategorizace a normalizace dat
- Více jak 300 out-of-the-box Smart Connectors
- Snížená doba řešení incidentů z hodin na minuty
- Schopnost řešit 10x více hrozeb
- Automatický Compliance Monitoring a Reporting
  např. ISO/IEC 27002, PCI-DSS



O2 IT Services

4. Modul Ticket System

IT provozní portál iTOP:

- ITIL best practices
- Konfigurační databáze CMDB
- Flexibilní správa tiketů
- Analýza dopadů a závislostí
- Uživatelský portál
- Integrovaný audit

O2 IT Services

Služby SEC detailně

Položka služby	Bronze	Silver	Gold	Gold +
Plnění podmínek ZoKB	✗	✓	✓	✓
Log Management (LM)	✓	✓	✓	✓
Reporting	✓	✓	✓	✓
Analýzy	✓	✓	✓	✓
Rate Alerting	✓	✓	✓	✓
Ticketovací systém	✗	✓	✓	✓
Základní operační dohled	✗	✓	✓	✓
Pokročilý operační dohled	✗	✗	✓	✓
Základní monitoring dohled	✗	✓	✓	✓
Pokročilý monitoring dohled	✗	✗	✓	✓
Vulnerability scan (základní)	✗	✗	✓	✓
CMDB lite (1 rozměr)	✗	✓	✓	✓
CMDB full (2 rozměry)	✗	✗	✓	✓
Komunikace třetí strany (CERT, NBÚ)	✗	✗	✓	✓
Přístup k event analýze	✗	✗	✓	✓
Customizovaný reporting	✗	✗	✓	✓
Auditní záznam činností SEC	✓	✓	✓	✓
Bezpečnostní dohled	8 x 5	8 x 5	8 x 5	24 x 7

Přenesená data

Měsíční cena za přenesená data	
1 GB/den (50 EPS)	
2 GB/den (100 EPS)	
10 GB/den (500 EPS)	
20 GB/den (1000 EPS)	
50 GB/den (2500 EPS)	

Addons

Addons (inviduální cenová jednání)		
O2 Důvěryhodný archiv	volitelně	volitelně
O2 Next Generation FW	✗	
Cyber Security - Treats		
FlowMon/ADS		
PIM/PAM		
Firemon		

Cena služby = Rozsah služeb + Přenesená data + Addons

O2 IT Services

Role SEC

SEC Operator (L1)

- Sleduje active channels a dashboards
- Vytváří anotace a cases
- Předává events a cases na SEC Analysts k dalšímu prošetření

SEC Analyst (L2)

- Prošetřuje incidenty s použitím active channels, grafů, anotací, cases a reportů
- Doporučuje a implementuje protiopatření

SEC Expert (L3)

- Identifikuje a navrhuje nové use cases
- Rozvíjí existující use cases
- Navrhuje a testuje nové korelace, filtry, monitory, aktivní listy, active channels, dasboards, reporty a trendy
- Rozšiřuje a doplňuje znalostní bázi a „Pattern Discovery profiles“

SEC Administrator

- Je zodpovědný za instalaci bezpečnostních komponent a za jejich správné fungování

O2 IT Services

Otázky?