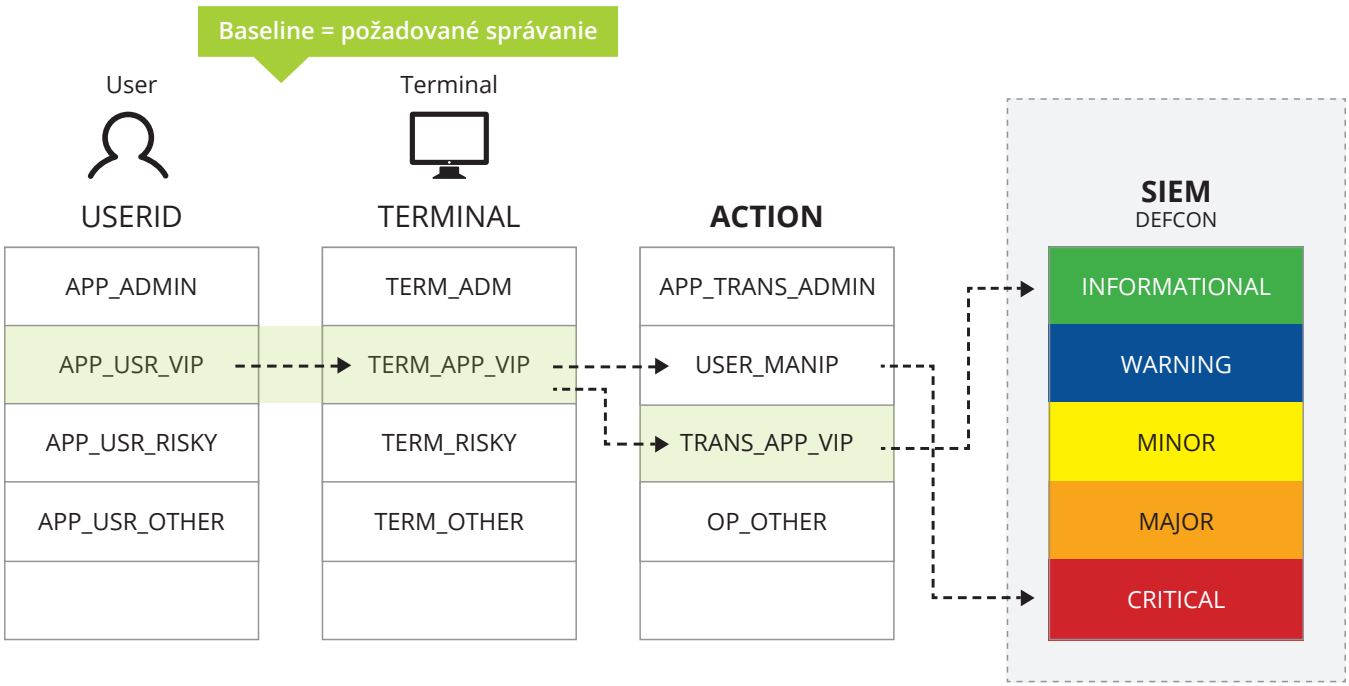
COMPLIANCE CHECK POMOCOU PCE

Produktový list

Policy Compliance Engine (PCE) - je zariadenie vyvinuté našou spoločnosťou, ktoré umožňuje definovať priority bezpečnostného monitorovania (významných používateľov, významných operácií, časových a ďalších aspektov) a zohľadňovať charakteristiky obvyklých aktivít.

Baseline – ide o skupinu informácií, ktorá umožňuje definovať priority monitorovania (významných používateľov, operácií) a do určitej miery charakteristiky normálnej činnosti (vzťahy medzi objektmi baseline navzájom a k focusovaným objektom). Po získaní hlásenia z monitorovaného zdroja PCE porovnáva každé hlásenie aplikácie s informáciami v baseline a následne vyhodnocuje. Výsledkom je obohatené pôvodné hlásenie.

Princíp baseline



Real-time porovnávanie každého hlásenia s baseline a označovanie odchýliek

- Neovplyvňuje prevádzku aplikácie

Baseline - model popisujúci požadovaný stav

- Jednoduché naplnenie - napríklad import xls
- Ochrana baseline dát pred ovplyvnením
- Možné definovanie nezávislou zložkou napríklad audit

KOŠICE
Gavlovičova 9
040 17 Košice
T: +421 55 727 17 17
E: lynx@lynx.sk

BRATISLAVA
Jelačičova 8A
821 08 Bratislava
T: +421 2 501 065 11
E: lynxba@lynx.sk

CERTIFIKÁTY
STN EN ISO 9001
STN OHSAS 18001
STN EN ISO 14001
STN ISO/IEC 27001

www.lynx.sk

Ohodnocovanie udalostí

Focus level - na jednoduchú identifikáciu:

- Aktivity dôležitých užívateľov, operácií, nad dôležitými objektmi

Violácie - na detekciu odchýlok od predpísaného správania:

- Detekcia použitia nesprávneho prostredia užívateľom
- Detekcia použitia nesprávneho terminálu
- Detekcia použitia nesprávnej operácie
- Detekcia použitia operácie v nesprávnom prostredí

Možnosť obohatenia hlásenia o referenčné údaje (napríklad Identity Management)

Takto obohatené hlásenie je posielané do SIEM riešenia, kde je možné napríklad:

- jednoducho filtrovať udalosti privilegovaných používateľov
- automatickú detekciu porušenia „segregation of duties“ (takzvané oddelenie rolí)
- automatickú detekciu porušenia pravidiel organizácie
- analyzovať udalosti na základe referenčných údajov