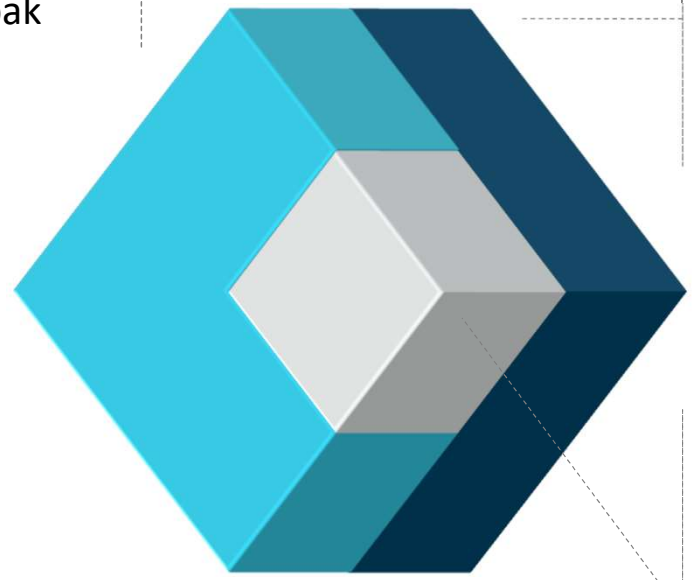
Simon Simčič, simon.simcic@src.si

Zakaj potrebujemo SIEM?

Operacije IT

- nadzor delovanja in uporabe
- pregled obremenitev
- ugotavljanje napak



Grožnje

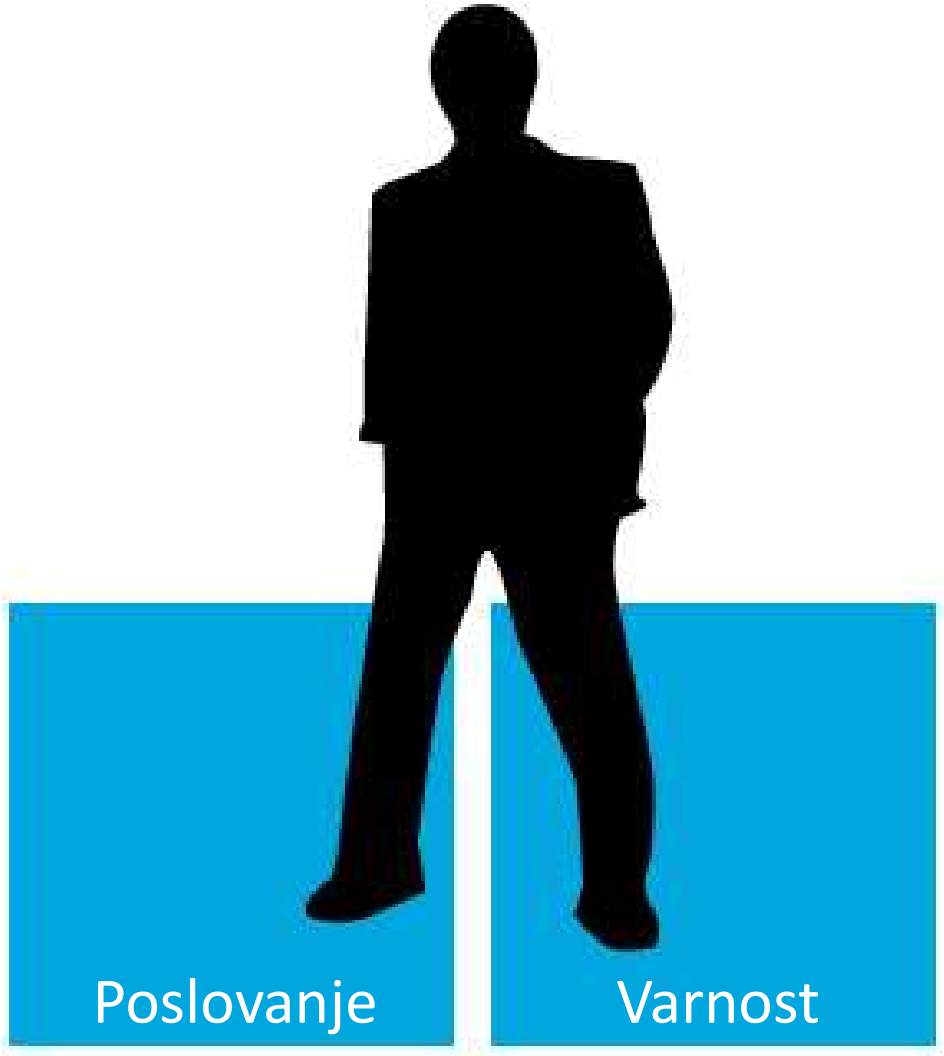
- notranje, zunanje
- splošne, ciljane

Skladnost

- ZVOP
- ISO 27001
- PCI DSS …

Kaj SIEM omogoča?

- Zbiranje, analizo in hrambo dnevnikov
- Širok nabor informacij za raziskovanje izrednih dogodkov
- Obveščanje v realnem času na podlagi korelacije varnostnih dogodkov
- Strukturirano ali nestrukturirano iskanje in vizualizacije dogodkov
- Spremljanje aktivnosti uporabnikov, tudi v namensko razvitih lastnih aplikacijah
- Nadzor zaupnosti in celovitosti datotek in map
- Nadzorne plošče, pred-pripravljena in namenska poročila

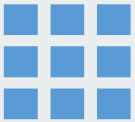


Kako vpeljemo SIEM?

Analiza okolja

- Arhitektura okolja
- Varnostna politika
- Zakonodaja
- Zahteve deležnikov

Priprava načrta



- Primeri uporabe
- Izvedbeni načrt

Postavitev sistema

- Namestitev in zagon
- Priprava modela
- Parametrizacija vsebine

Kako vpeljemo SIEM?

Vključevanje virov

- Interno omrežje
- DMZ cone
- Druge domene

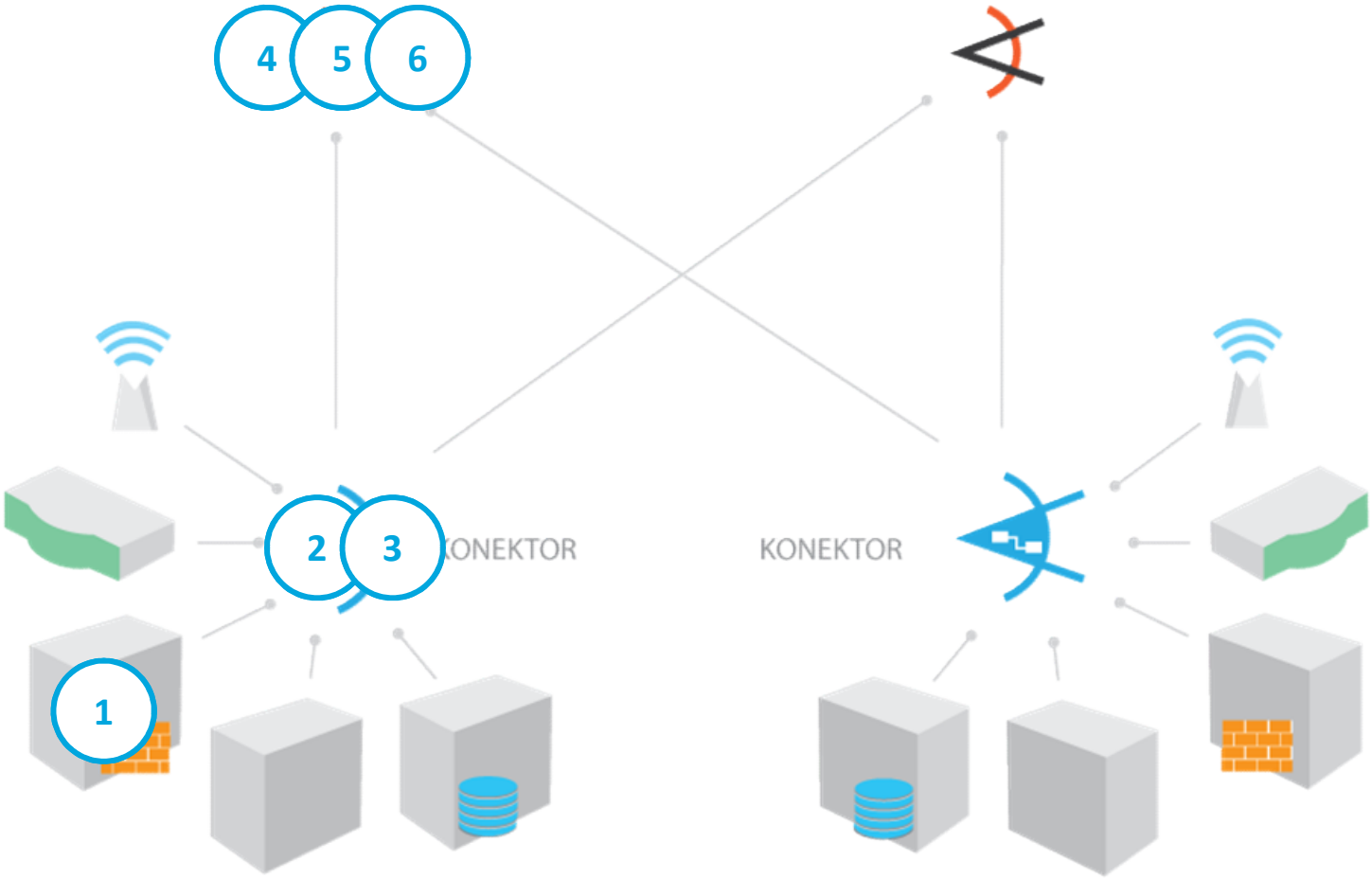
Prilagojeni konektorji

- Namensko razvite lastne aplikacije
- Drugi specifični sistemi

Uporabniški pregledi

- Skladnost z ZVOP , ISO 27001, PCI DSS …
- Nadzorne plošče
- Specifični pregledi

Faze obdelave dogodkov
na primeru postavitve sistema



Vključevanje virov

Primeri rabe

- Priprava primera rabe
  - Primere rabe razvijamo sproti
  - Stranka poda zahteve
  - Pregledamo dogodke, ki so vezani na nek primer rabe
    - Katera naprava
    - Kateri dogodek
  - Pripravimo konektor
  - Dogodke posredujemo v SIEM
  - Primer rabe realiziramo skozi Poročilo, Dashboard ali Alarm

- Na podoben način stranki svetujemo med Log Management ali SIEM rešitvijo – glede na primer rabe.

Primeri rabe

- Primeri iz prakse
  - Spremljanje sprememb konfiguracij na mrežni opremi
  - Spremljanje Windows dogodkov, spremembe avtorizacij
  - Spremljanje statusov vmesnikov, posebej pri redundančnih povezavah
  - Spremljanje vpogledov v osebne podatke ZVOP
  - Blokade na IPS Sistemu in prehod preko FW

Primeri rabe

- Spremljanje sprememb konfiguracij na mrežni opremi
  - Konkretno CISCO požarna pregrada
  - Spremembe konfiguracije se izvaja preko CLI
  - Vsak ukaz z izjemo „show“, je tip dogodka 111008 –
    primer: `PIX|ASA-5-111008: User user executed the command string`
  - Iščemo torej te dogodke
  - Če v Filter dodamo še prijave uporabnika, vidimo tudi izvorni IP odkod se je prijavil
  - Rezultat je poročilo o vseh ne-show ukazih, ki so se izvedli na neki požarni pregradi

Primeri rabe

- Spremljanje Windows dogodkov, spremembe avtorizacij
  - Praviloma gre za spremembe na ravni domene
  - Izvor dogodka so domenski krmilniki
  - „Lovimo“ dogodke tipa oz. Event Id 4728 in 4729
  - Dogodek vsebuje informacijo kdo je dodal uporabnika v neko skupino
  - Rezultat je poročilo o izvedenih spremembah v nekem okolju
  - Dodatno lahko navedemo seznam kritičnih skupin, ob spremembi članstva v takšni skupini je rezultat Alarm. (Domain Admin, Exchange Admins ipd)

Primeri rabe

- Spremljanje statusov vmesnikov, posebej pri redundančnih povezavah
  - Stranka ima redundančno povezavo, če ena povezava odpove tega ni zaznati, ker vse deluje – nima pa redundance
  - Lovimo dogodek Interface down na CISCO usmerjevalniku na točno določenem vmesniku
  - Niti ne potrebujemo SIEM rešitve – Log Management zadostuje
  - Izdelamo iskalni parameter, ki deluje v realnem času
  - Nastavimo prag 1 dogodek
  - Rezultat je alarm

Primeri rabe

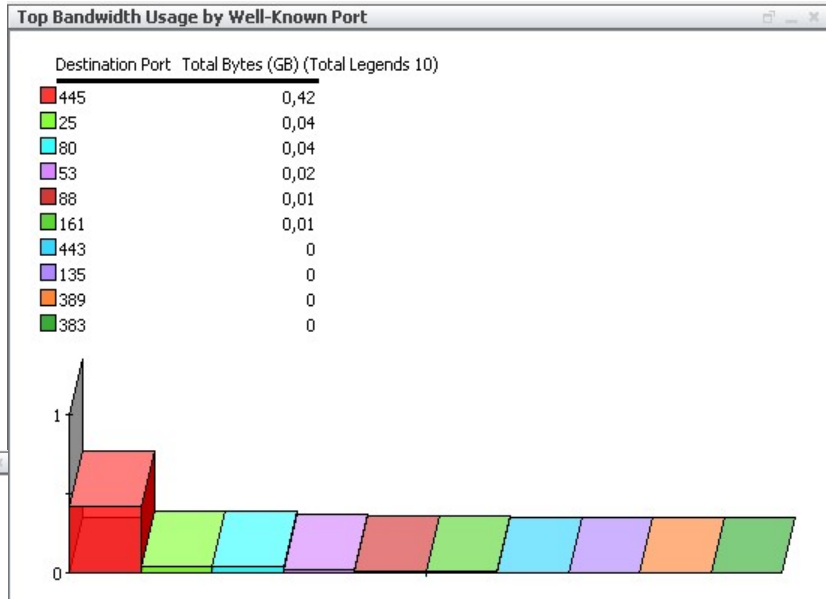
- Spremljanje vpogledov v osebne podatke ZVOP
  - Stranka je razvila revizijsko sled v aplikaciji
  - Revizijska sled se generira znotraj ene tabele v podatkovni bazi
  - Prilagojen konektor z SQL poizvedbami zbira dogodke in jih normalizira
  - Z eno poizvedbo iščemo vpoglede preko 10tih poslovnih aplikacij
  - Zadostuje Log Management
  - Rezultat : Dashboard s statističnimi pregledi

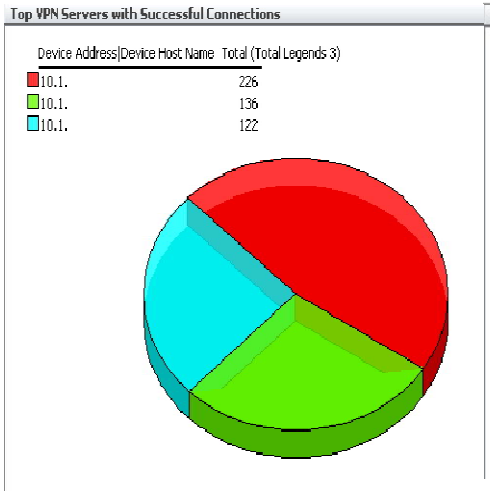
Primeri rabe

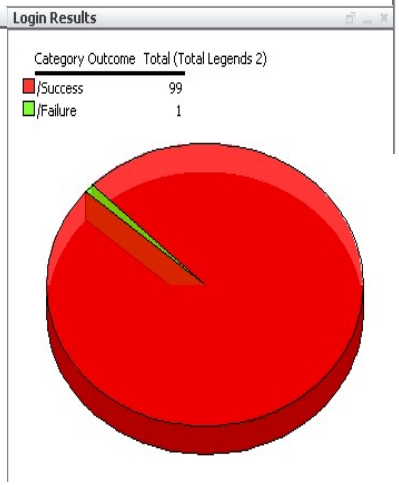
- Blokade na IPS Sistemu in prehod preko FW
  - Cilj spremljati – spremljati uspešne prehode na požarni potem, ko so bili blokirani na IPS Sistemu
  - Log Management ne zadostuje
  - Zbirati moramo dogodke iz požarne pregrade – v tem primeru je to bil Checkpoint ter IPS Sistema – IBM Proventia
  - Pravilo, ki gleda – Izvorni IP na IPS in Block dogodek ter enak Izvorni IP na požarni pregradi in uspešen prehod oz. Accept v zadnji minuti
  - Izkušnja – potrebno je prilagoditi IPS filter, da čimbolj izključimo False positives

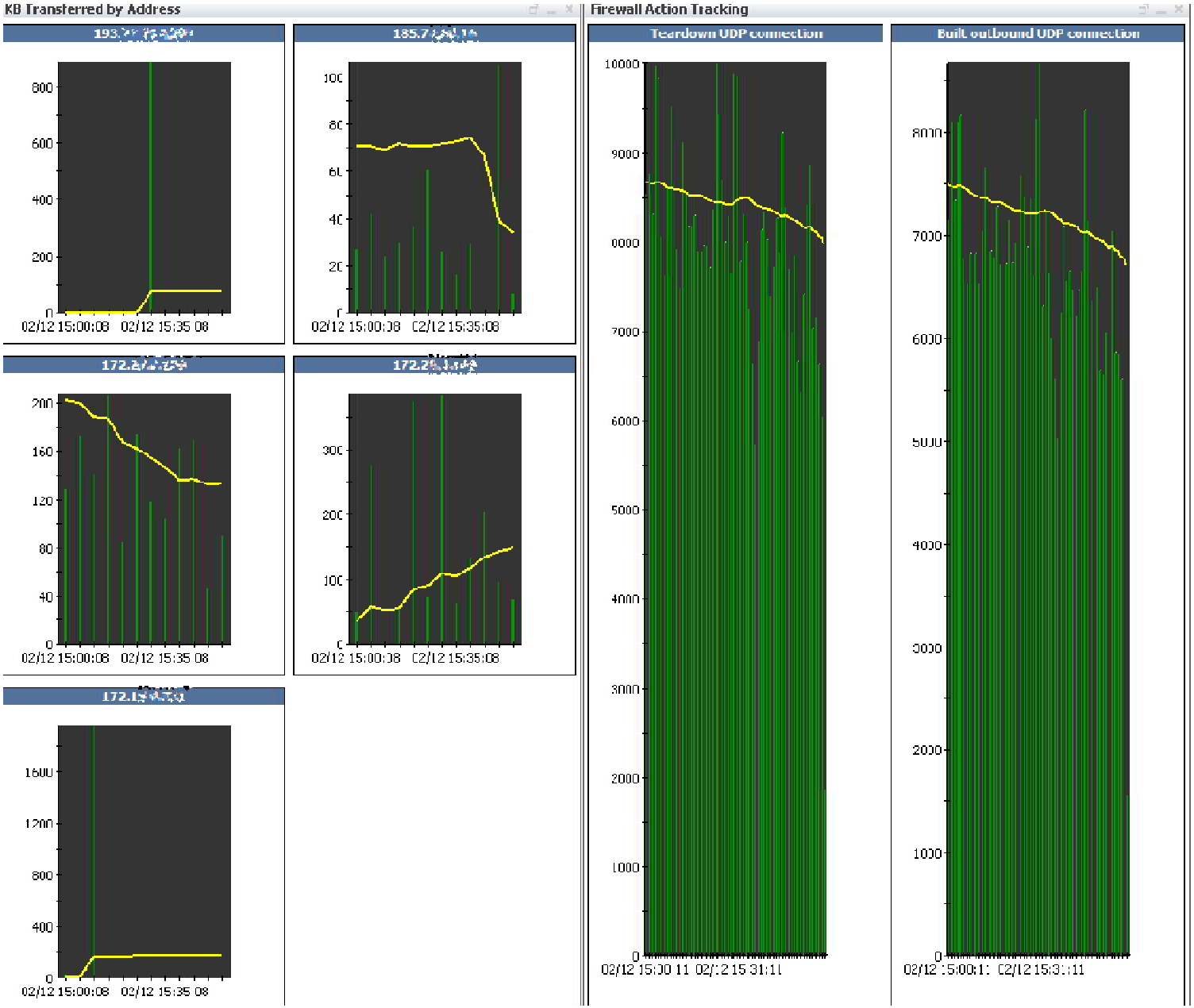
Za konec

- Kaj nam še omogoča SIEM
  - Enovit pogled čez „Machine generated data“
  - Statistično spremljanje – Poročila, trendi, dashboardi
  - Koreliranje med dogodki iz dveh različnih virov
  - Odziv na neko akcijo








KB Transferred by Address
Firewall Action Tracking
Teardown UDP connection
Built outbound UDP connection
02/12 15:00:08
02/12 15:35:08