AlienVault OSSIM – Open source SIEM

Jernej Suhadolc, Virtua IT

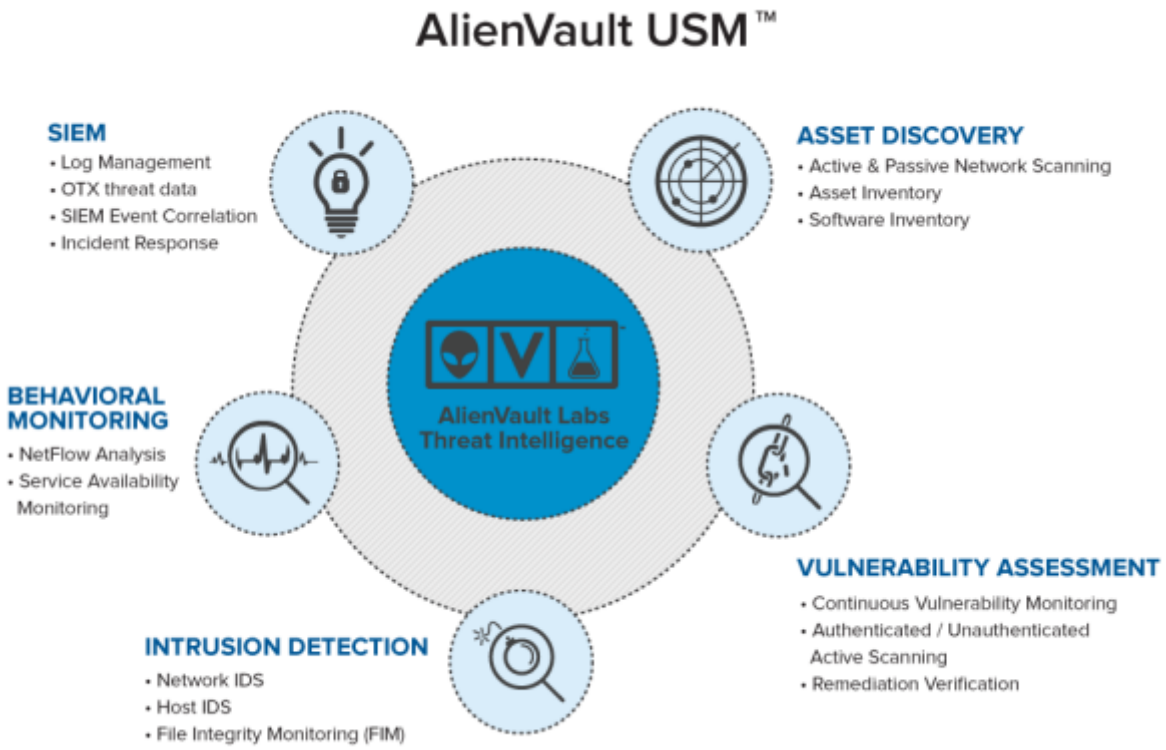
Ljubljana, 28. 10. 2016

Uvod

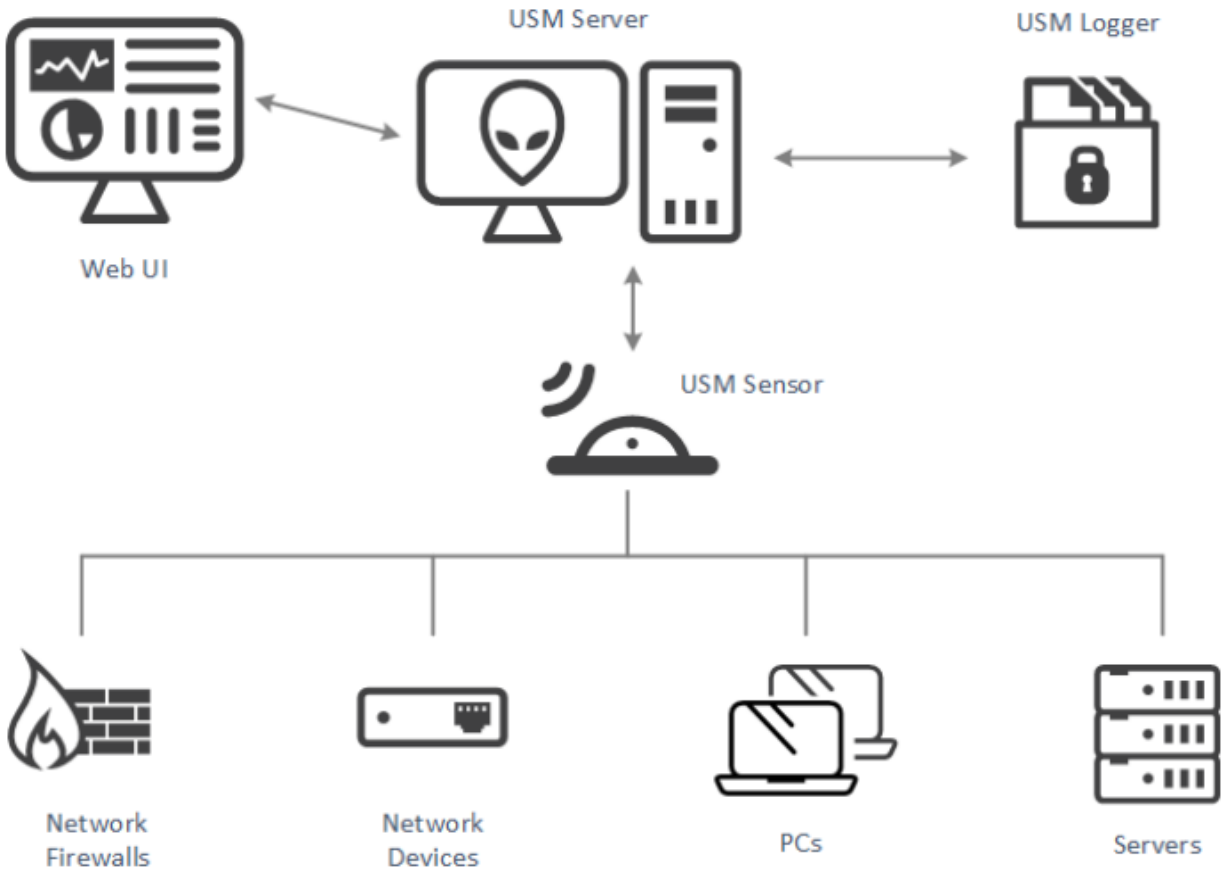
- Zakaj sploh SIEM?,
  - Principi dela hackerjev ostajajo že leta enaki,
  - Spreminja se hitros, količina podatkov, kompleksnost sistemov
  - Potrebujemo rešitev, ki naredi pregled nad omrežjem in strežniki približno vzdržno.
- Možno je postopati sistematično
  - Primer tega je Sans Institute Critical Security Controls: https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf ,
  - Če temu pristopu verjamemo, je treba le najti rešitev, ki najbolje pokrije teh 20 kontrol, ostale pokrijemo z drugimi sistemi,
  - SANS ni edini, pomembno vodilo pri vpeljavi varnosti ima tudi NIST. Obstaja celo mapping med enim in drugim: https://www.cisecurity.org/critical-controls/tools/

Kaj zna AlienVault

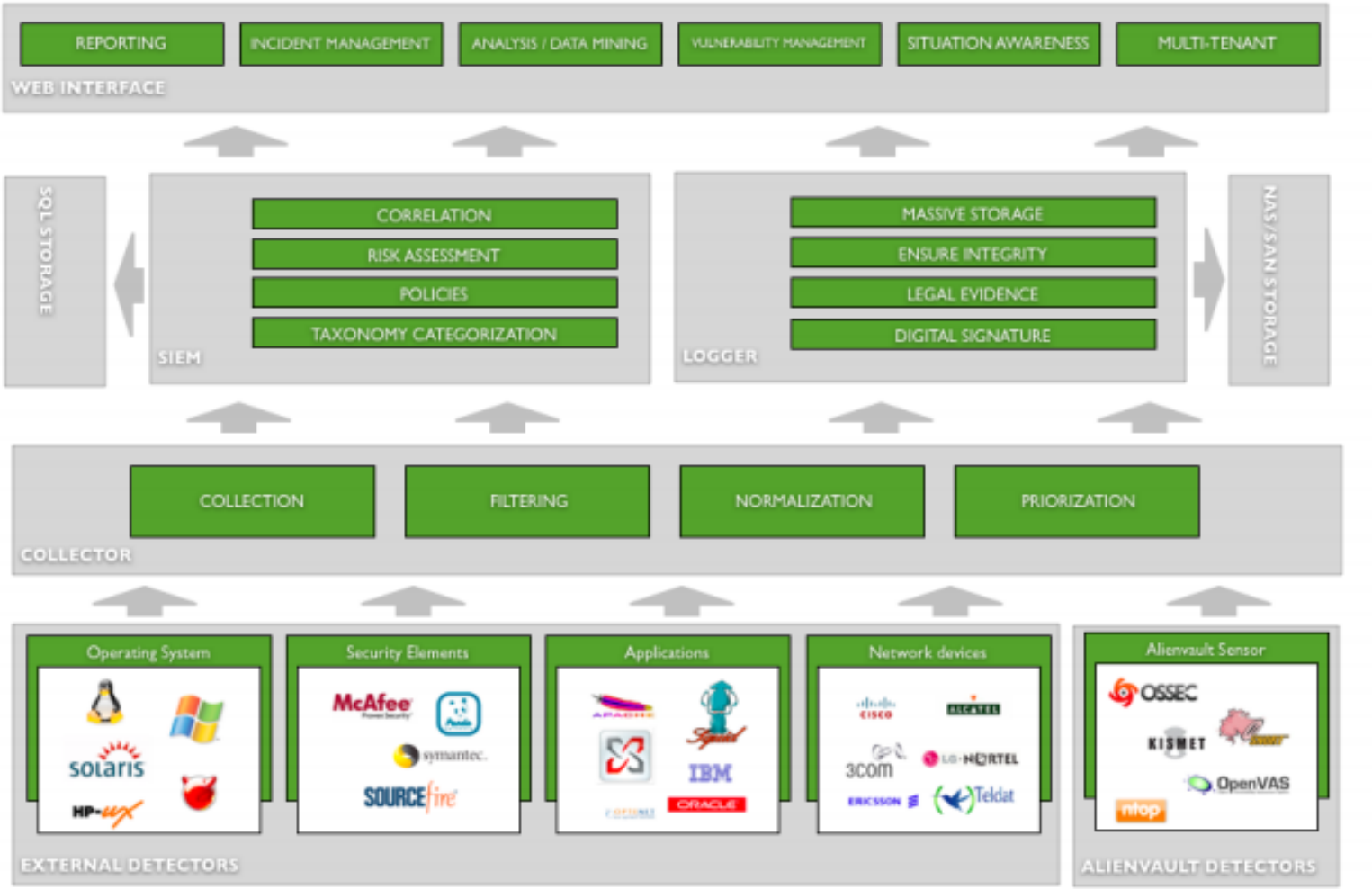
Kaj zna AlienVault



Arhitektura



Odprtokodna tehnologija



Prikaz v živo