Vzpostavitev več nivojske varnostne infrastrukture

S pomočjo Elektro Maribor, McAfee SIEM, CISCO ISE, NGFW …

Zorna Varga, Sfera IT d.o.o in Klemen Bačak, Sfera IT d.o.o.

Priprava na: Vzpostavitev več nivojske varnostne infrastrukture

Elektro Maribor

- **START:**
  - Zajemanje LOG-ov aktivne opreme in strežnikov je potekalo ločeno
  - Vsako orodje s svojim vmesnikom, pravili in logiko
  - Mnogo prijav na različne platforme
- **CILJ**
  - Standardizirana učinkovita platforma, temelječa na odprtosti, enostavnosti, skladnosti, prilagodljivosti, integraciji in kar se le da – enostavna

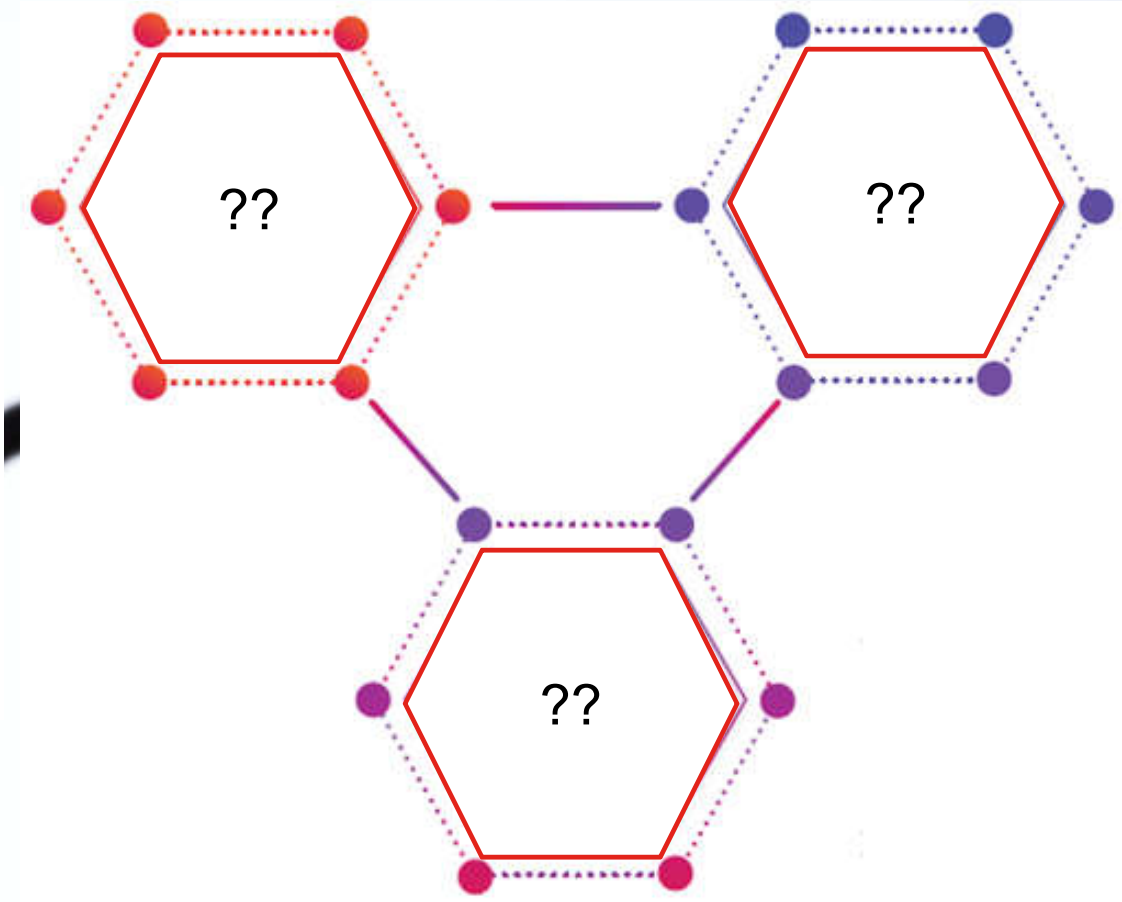
Sfera IT

- **START:**
  - Kje smo (Izkušnje in znanje do *zdaj*)
  - Zakaj, Kako in s čim (pregled trga)
  - Rokavi (zavihani)
- **CILJ**
  - Izkušnje in znanje (nove, skupne)
  - Podpora partnerju kot do sedaj
  - Enostavnost in harmonija za vse
  - Pripravljenost na nove izzive ;-)

Začetek projekta

Koraki

- Presek stanja
- Popis procesov
- Popis naprav in s njimi povezanih storitev
- Implementacija….



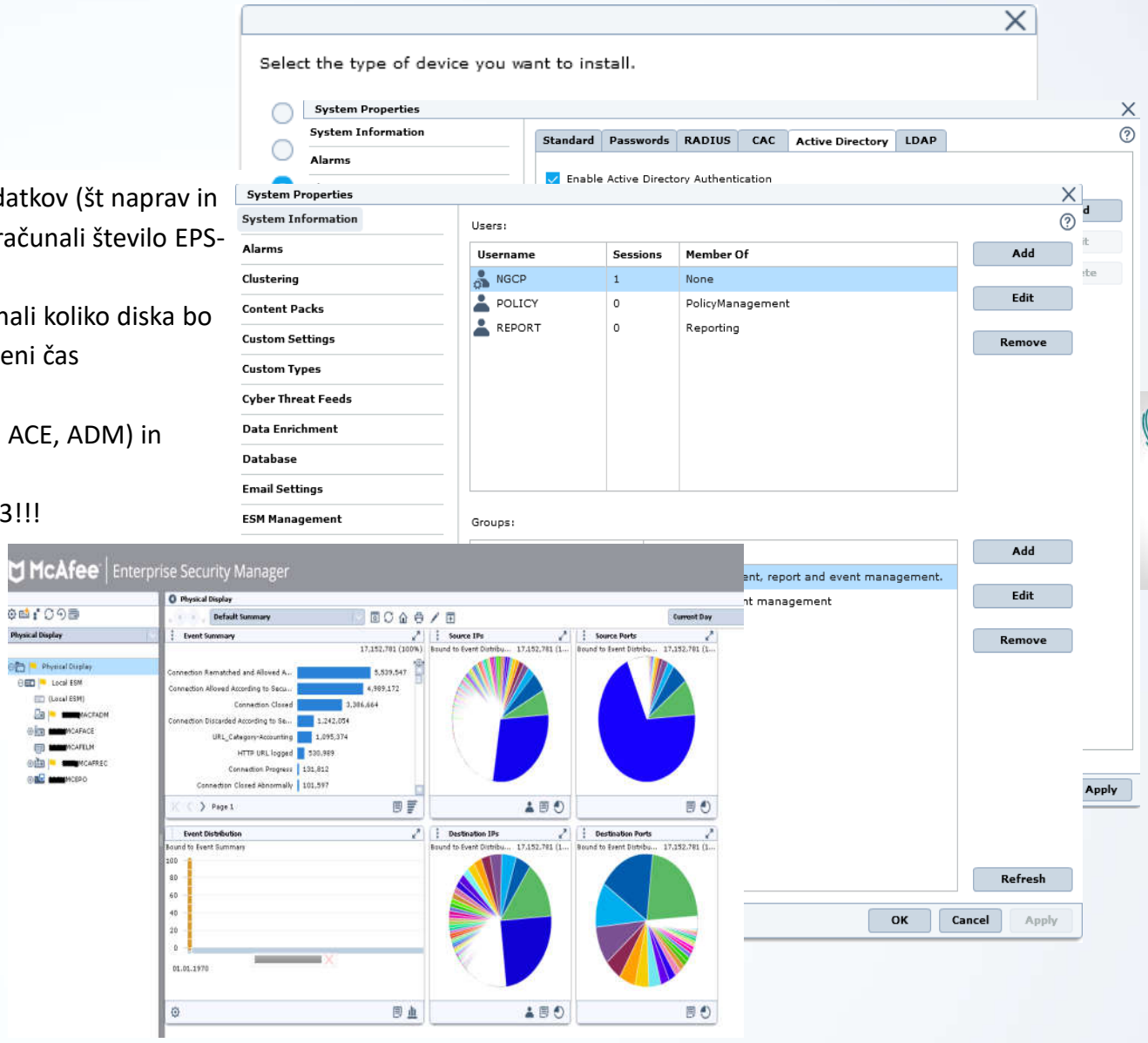
McAfee - SIEM

- Posvetovali smo se z Mcafee-jem in na podlagi naših podatkov (št naprav in katere ter število strežnikov) smo z EPS estimator-jem izračunali število EPS-jev, ki bodo te naprave proizvajale.
- Prav tako smo na podoben način z sizing orodjem izračunali koliko diska bo okvirno potrebno, da bomo lahko shranjevali loge za željeni čas

1. Nakup licence
2. Download .ova datotek za vsak produkt (ESM, ELM, REC, ACE, ADM) in import v vmware

   <u>Priporočene specifikacije za VM:</u> -- verzija 11.0.3!!!

   a. ESM - 250 GB HDD, 8vCPU, 16 GB RAM
   b. REC - 250 GB HDD, 8vCPU, 8 GB RAM
   c. ELM - 250 GB HDD, 8vCPU, 8 GB RAM
   d. ACE - 250 GB HDD, 8vCPU, 32 GB RAM
   e. ADM - 250 GB HDD, 8vCPU, 16 GB RAM



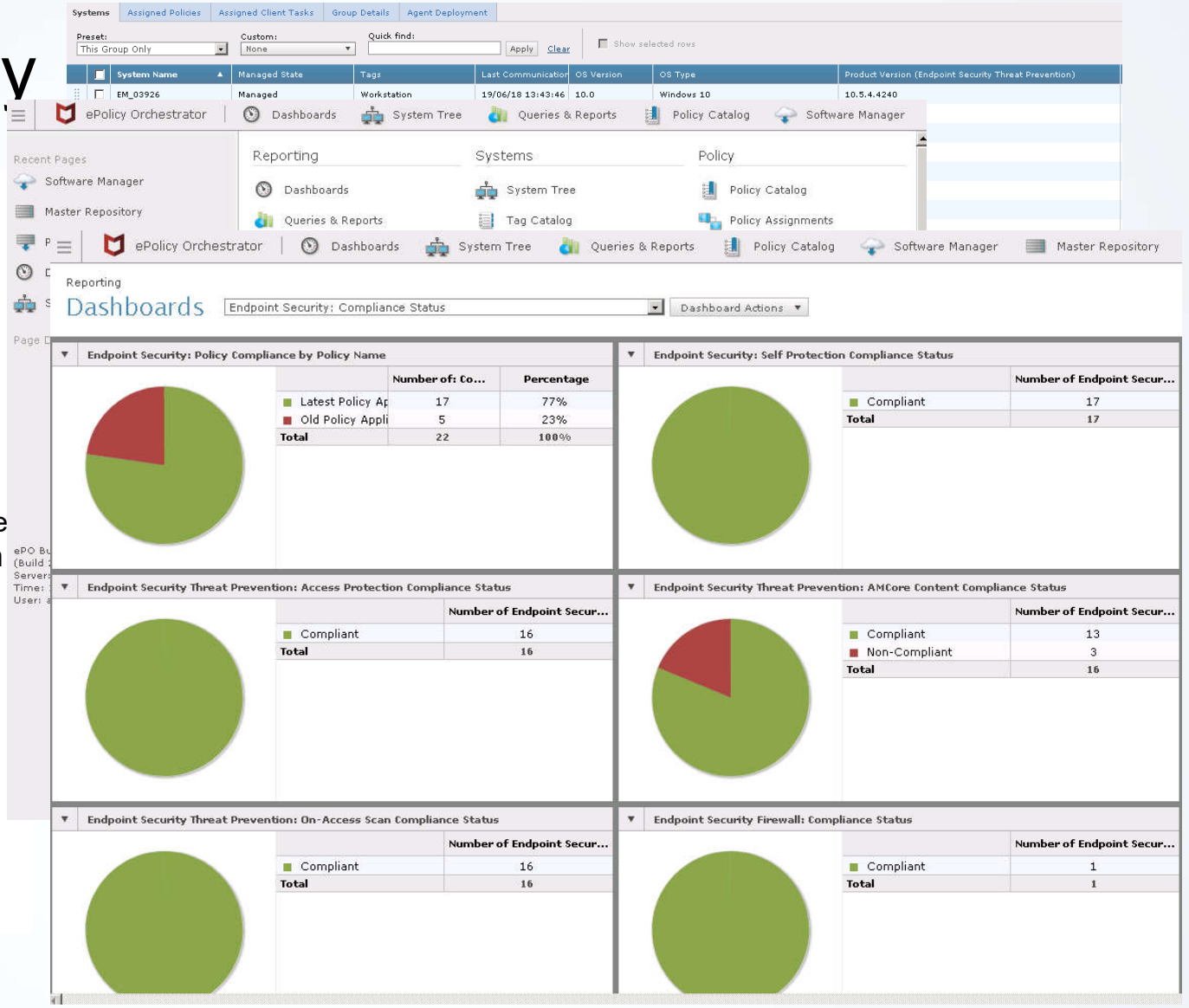
EndPoint security

Endpoint

Te rešitve **omogočajo kreiranje varnostne platforme IS**, katero je mogoče enostavno **nadgraditi** oz. **razširiti** na način, da se bo **sposobna odzvati na varnostne izzive** IT.

Nove varnostne rešitve za končne naprave **zagotavljajo večjo zaščito na delovnih postajah in strežnikih**. Hkrati je omogočeno tudi **izvajanje centraliziranega upravljanja**, **nadzora** in **avtomatiziranih namestitev**.

Tako se **zagotavlja večplastna napredna obramba** s številnimi funkcijami, ki pokrivajo **vse vektorje potencialnih nevarnosti** in bistveno izboljšajo varnost kot celoto.

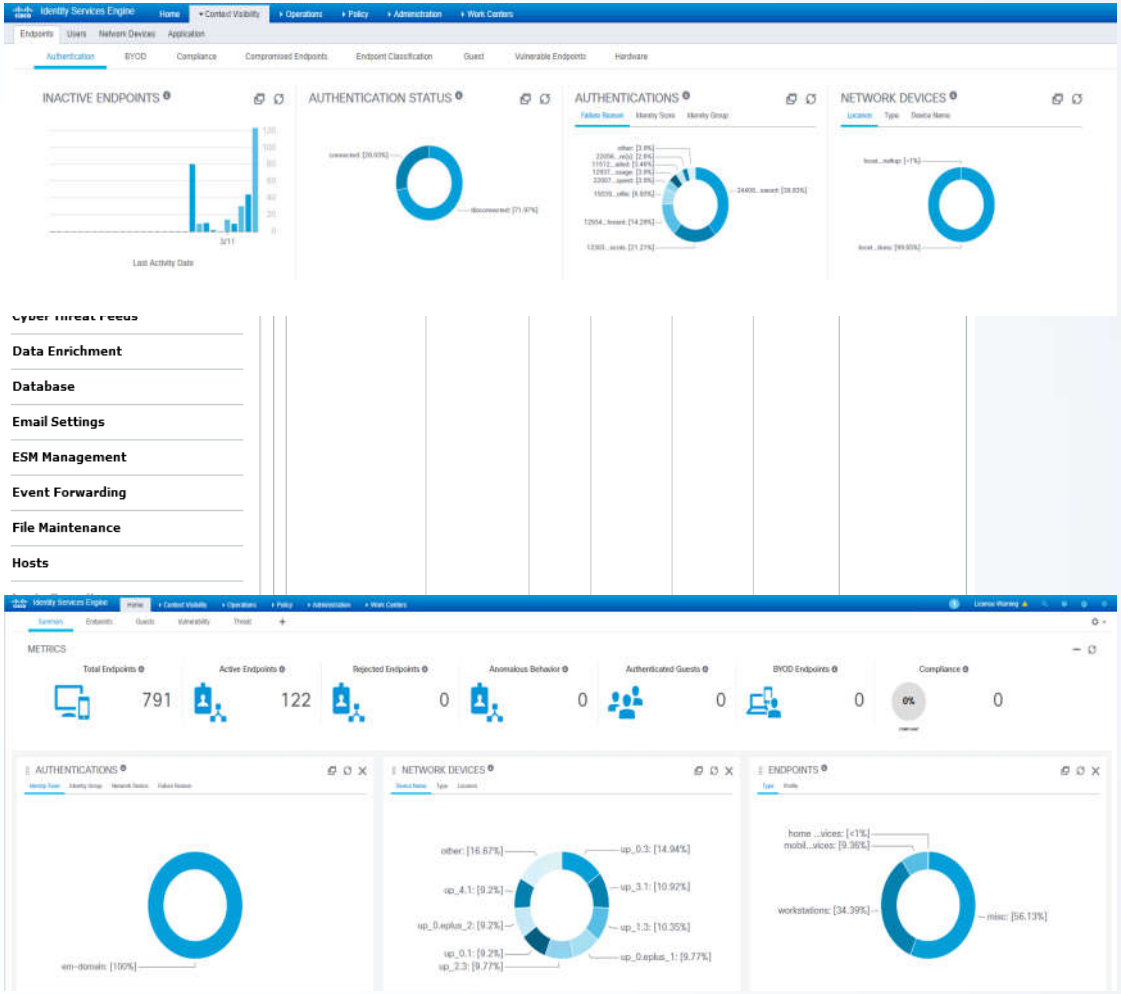


Identity – CISCO ISE

Identity

- Te rešitve omogočajo kreiranje varnostne platforme IS, ki jo je mogoče enostavno nadgraditi oziroma razširiti na način, da se bo sposobna odzvati na varnostne izzive IT. Nove varnostne rešitve za končne naprave zagotavljajo večjo zaščito na delovnih postajah in strežnikih, kakor tudi centralizirano upravljanje, nadzor in avtomatizirano namestitev. Tako se zagotavlja večplastna napredna obramba s številnimi funkcijami, ki pokrivajo vse vektorje potencialnih nevarnosti in bistveno izboljšajo varnost kot celoto.

- Povezava ISE in Mcafee ePO – interakcija Mcafee DXL (Data - Exchange Layer) in Cisco pxGrid



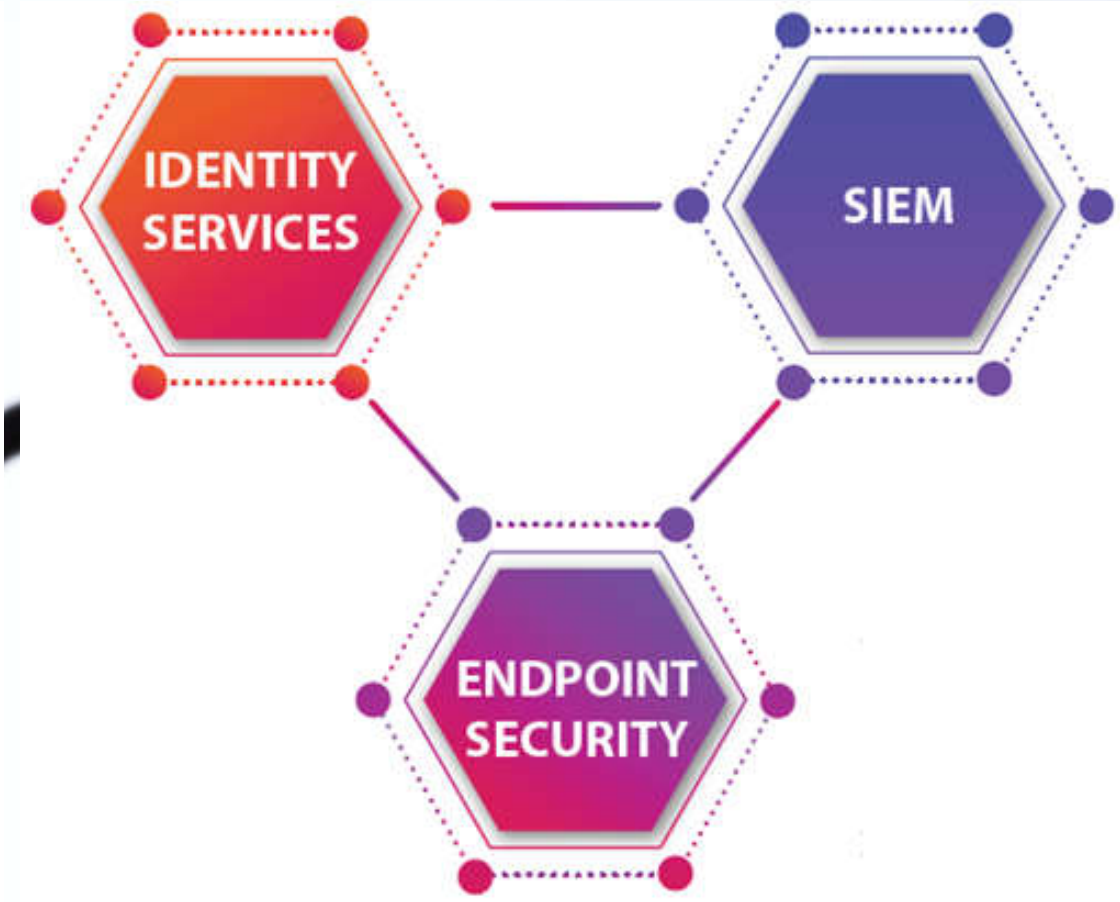
Korelacija – medsebojna povezava vsega

Korelacija

- Sodobne rešitve za spremljanje dogodkov in varnostno inteligenco (SIEM - Security Information and Event Management) beležijo in hkrati pomagajo aktivno zaznavati tovrstne zlorabe, ki bi sicer ostale neopažene. Z uporabo napredne analitike različnih tipov in virov podatkov je mogoče zaznati kritične dogodke v informacijskem sistemu podjetja.

- V želji zmanjšanja tveganj z vidika kibernetskih groženj za informacijske sisteme, se uporabljajo tudi tehnične rešitve za povečanje varnosti končnih naprav (angl. Endpoint Security).Te rešitve omogočajo kreiranje varnostne platforme IS, ki jo je mogoče enostavno nadgraditi oziroma razširiti na način, da se bo sposobna odzvati na varnostne izzive IT

- Sistemi za zaščito končnih točk se lahko dopolnjujejo s sistemi za kontrole dostopa in upravljanje z identitetami (angl. Identity and Access Management Systems), ki med drugim aktivno omejujejo dostope in širjenje varnostnih groženj na podlagi informacij, ki jih pridobijo s strani sistemov za varnost končnih naprav in ostalih varnostnih sistemov



Hvala.