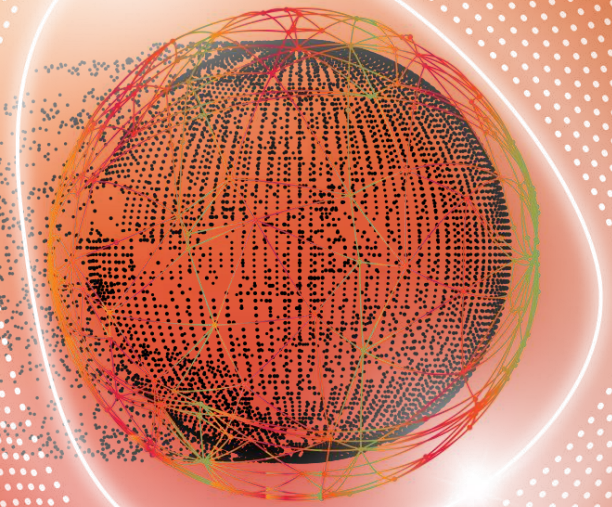


Roglit 25

Trend Micro Vision One

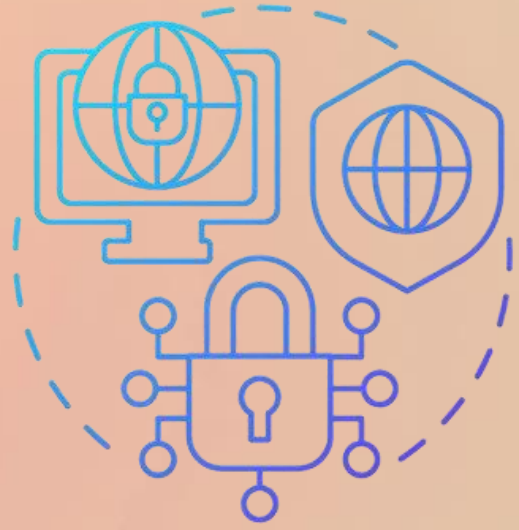
Ključ do prepoznavanja in zaščite najpomembnejšega.
Referenčna zgodba v UKC Ljubljana

Mel Pirc, Sistemski inženir

Zavezništvo za močnejši IT ekosistem – Building a Stronger IT Ecosystem

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Glavne točke



Varnost ključne infrastrukture

Trend Micro

Trend Micro Vision One XDR

Roglit25

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Začnimo na začetku

Naša kritična infrastruktura?

- Naše okolje:
  - Delovno okolje oz. končni uporabniki (računalniki, mobilni telefoni itd.)
  - Elektronska pošta in ostale storitve
  - Strežniško okolje
  - Omrežje (IT/OT)




Začnimo na začetku

Uporabljamo rešitve za zaščito?

- AV – Antivirus
- EDR – Endpoint Detection Response
- XDR – Extended Detection Response
- NDR – Network Detection Response

RISK = **THREAT** + **IMPACT** + **VULNERABILITY**

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Trend Micro V1

- Platforma za razširjeno odkrivanje in odziv na grožnje v našem okolju
- Celovita rešitev za zaščito celotnega okolja – “štiri točke” našega okolja
- Proaktivna zaščita in integracija – “third party”
- Optimizacija obveščanja in zmanjšanje števila opozoril
- Hibridni način – on-premise <-> SaaS
- NIS2 skladnost

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Zgodba UKC Ljubljana

Obstoječe okolje

- Rešitve:
  - Trend Micro Apex One (on-prem)
  - Trend Micro Office Scan (on-prem)
  - Trend Micro Deep Security

- Manjkajoče funkcionalnosti
  - Zmanjšana vidljivost (več ločenih konzol) – sinergija med produkti
  - Nezmožnost avtomatskih akcij
  - Zaščita O365 okolja kot celota

Zgodba UKC Ljubljana

Novo okolje

- Rešitve
  - Trend V1 Standard Endpoint Protection
  - Trend V1 XDR
  - Trend V1 ASRM
  - Trend V1 Sandbox
  - Trend Email and Collaboration Security (O365)
  - + Trend Micro on-prem A1 in Deep Security

- Pridobljene funkcionalnosti
  - Korelacija med produkti
  - ASRM modul
  - Definicija avtomatskih akcij na nivoju vseh produktov
  - Sandbox analiza in blokiranje
  - Integracija z O365 in NIS2 skladnost

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Zgodba UKC Ljubljana

Potek implemetacije

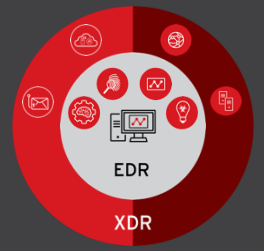
- Integracija z on-prem storitvami
  - Trend Micro Service Gateway
  - Trend Micro Datacenter Gateway
- Integracija z oblačnimi storitvami
  - API
- Distribucija XDR agentov
- Vzpostavitev avtomatskih akcij
- Vzpostavitev analize (Sandboxing)

- **Nadzor, prilagoditve, še enkrat nadzor, in še enkrat prilagoditve**

Gradniki rešitve

Trend Vision One Sandboxing

Trend Vision One ASRM



Roglit25

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Trend V1 Sandboxing

Kako in kaj pridobim

- Samodejno ali ročno (submission)
- Obdelava v realnem času
- Datoteke in URL naslovi
- Blokiranje (t.i. “suspicious object list”)
- Možnost avtomatskih akcij - blokiranje (požarna pregrada)

Kako preverjamo vsebino datoteke ki je morda zlonamerna?	Znamo centralno ukrepati ko se napad z zlonamernim izvajanjem izvede?
Ali učinkovito ščitimo naše okolje pred sumljivimi in neznanimi datotekami?	Kako lahko izboljšam varnost našega okolja?

Trend V1 Sandboxing

Zakaj

“

Izsiljevalska pro
grožn
“

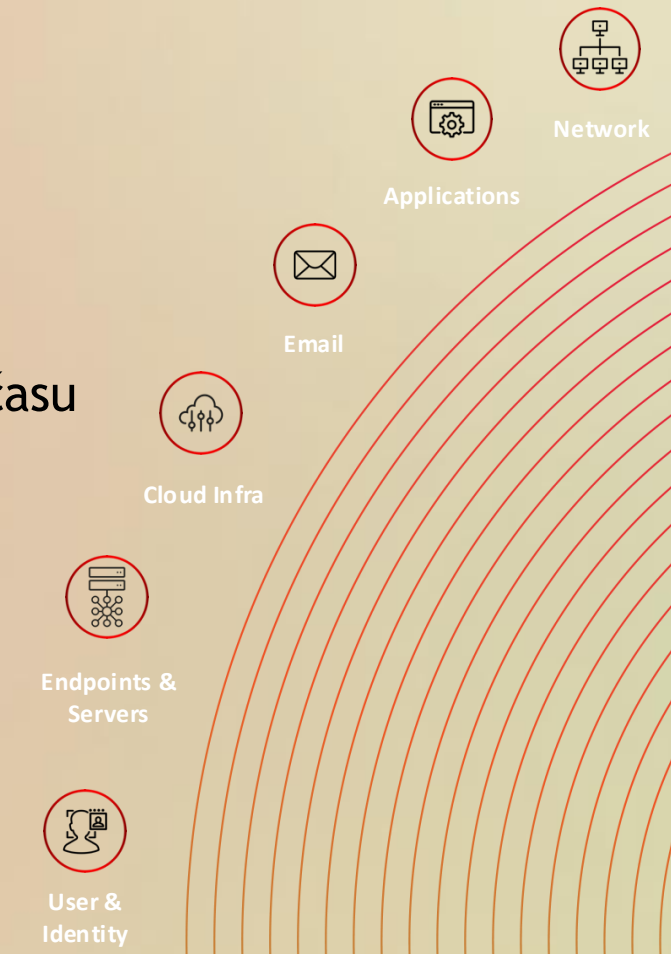
ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Trend V1 ASRM

Kako in kaj pridobim

- Odkrivanje znanih in **neznanih** storitev ter njihovih ranljivosti
- Prioritizacija tveganja podjetja in storitev v realnem času
- Proaktivne in avtomatske akcije za zmanjšanje in prekinitev napadov še pred dejansko izvedbo

Ali imamo celovit pregled nad ranljivostmi v svojem okolju?	Kako najbolje izkoristimo ekipo, tehnologijo in čas?
Katere korake moramo narediti, da bi zmanjšali možnosti napada?	Kako in kdaj ukrepamo v primeru kraje dostopnih podatkov?

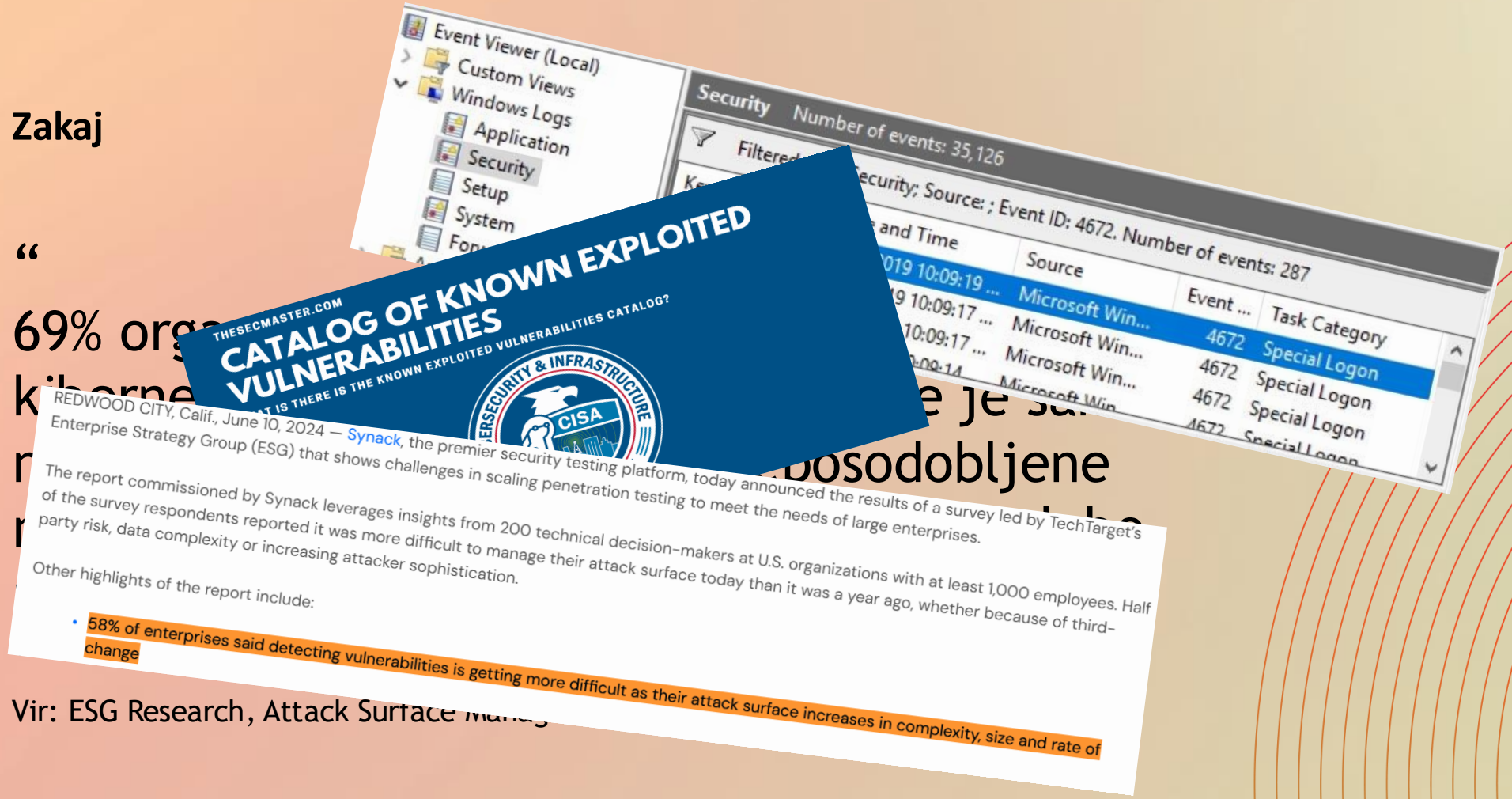


Trend V1 ASRM

Zakaj

“

69% org
ki
n



bosodobljene

Vir: ESG Research, Attack Surface

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Roglit 25

Definirajmo našo kritično infrastrukturo

Implementirajmo ustrezne rešitve Trend Micro V1

Zaupajmo,da Vision One postane naš zaveznik pri zaščiti najpomembnejšega in nam omogoči miren spanec

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Roglit 25

Hvala za udeležbo in pozornost!

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Roglit 25

Vprašanja

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company