



Roglit 25

Trend Micro Vision One

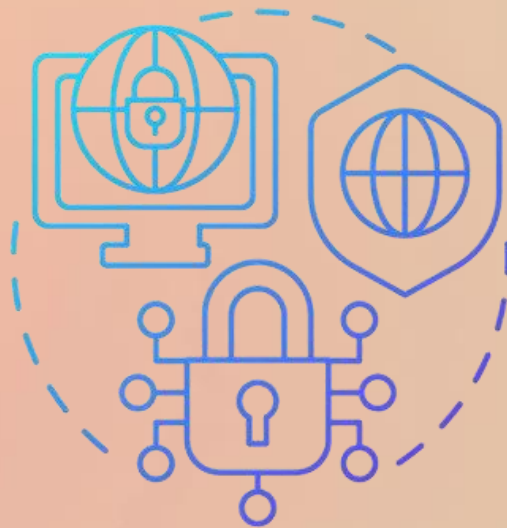
**Ključ do prepoznavanja in zaščite najpomembnejšega.
Referenčna zgodba v UKC Ljubljana**

Mel Pirc, Sistemski inženir

Zavezništvo za močnejši IT ekosistem – Building a Stronger IT Ecosystem



Glavne točke



Varnost ključne
infrastrukture



Trend Micro



Trend Micro Vision One XDR



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



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

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

Zgodba UKC Ljubljana



Potek implemetacije

- Integracija z on-prem storitvami
 - Trend Micro Service Gateway
 - Trend Micro Datacenter Gateway
- Integracija z oblračnimi 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



Roglit 25

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
grožnja

“

CYBERSECURITY | SECURITY NEWSWIRE
Malware was
By Security Staff
Trojan Threatens Financial
America
SECURITY NEWS
of threat detections in Q1 2024
...we'll provide an overview of the trojan and what it does.

JORDAN PEARSON
SECURITY JUN 10, 2024 10:01 AM
Mekot' Ransomware Is 'More Brutal' Than Ever in 2024
Syst'
As the fight against ransomware slogs on, security experts warn of a potential escalation to "real-world violence." But recent police crackdowns are successfully disrupting the cybercriminal ecosystem.
We've recei...
By: Trend Micro Research
July 04, 2024
Read time: 2 min (627 words)

Trend V1 ASRM



Kako in kaj pridobim

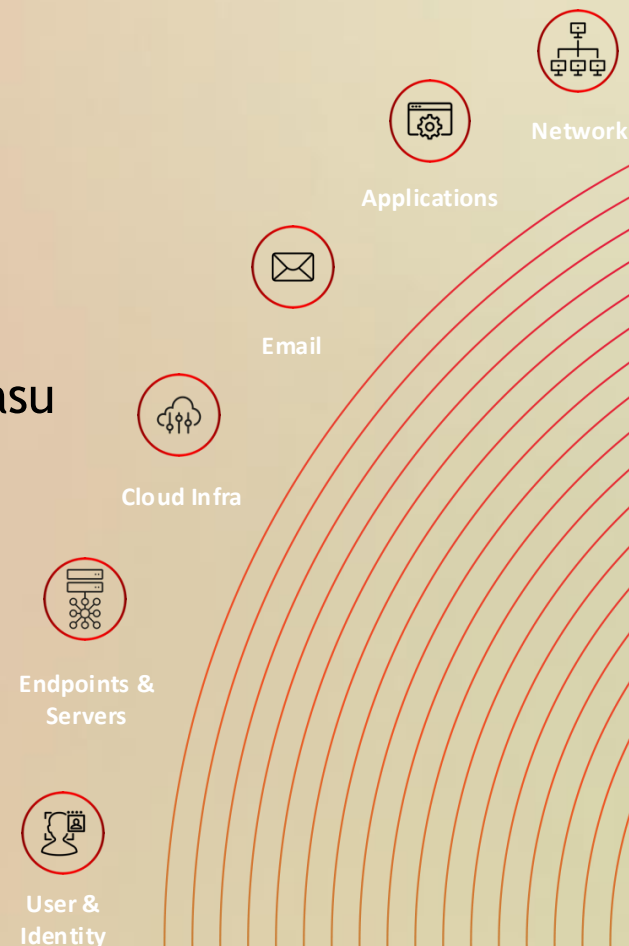
- Odkrivanje znanih in **neznanih** storitev ter njihovih ranljivosti
- Prioritizacija tveganja podjetja in storitev v realnem času
- Proaktivne in avtomatske akcije za zmanjšanje in prekinitev napadov še pred dejansko izvedbo

Ali imamo celovit pregled nad ranljivostmi v svojem okolju?

Kako najbolje izkoristimo ekipo, tehnologijo in čas?

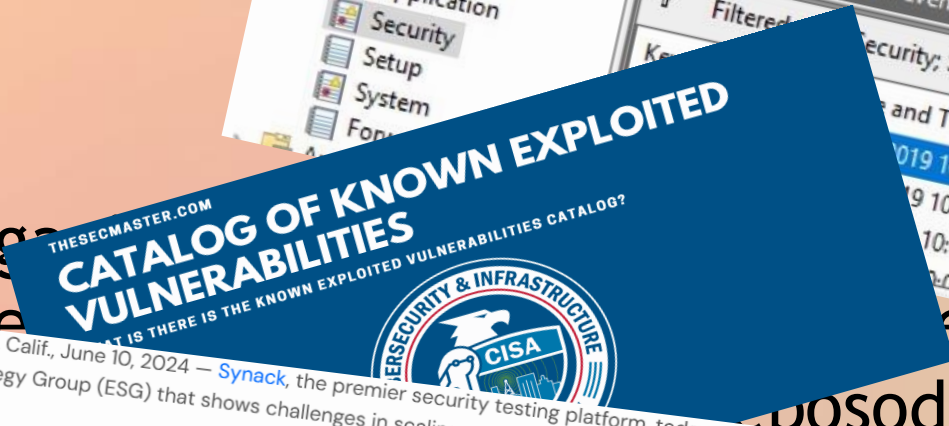
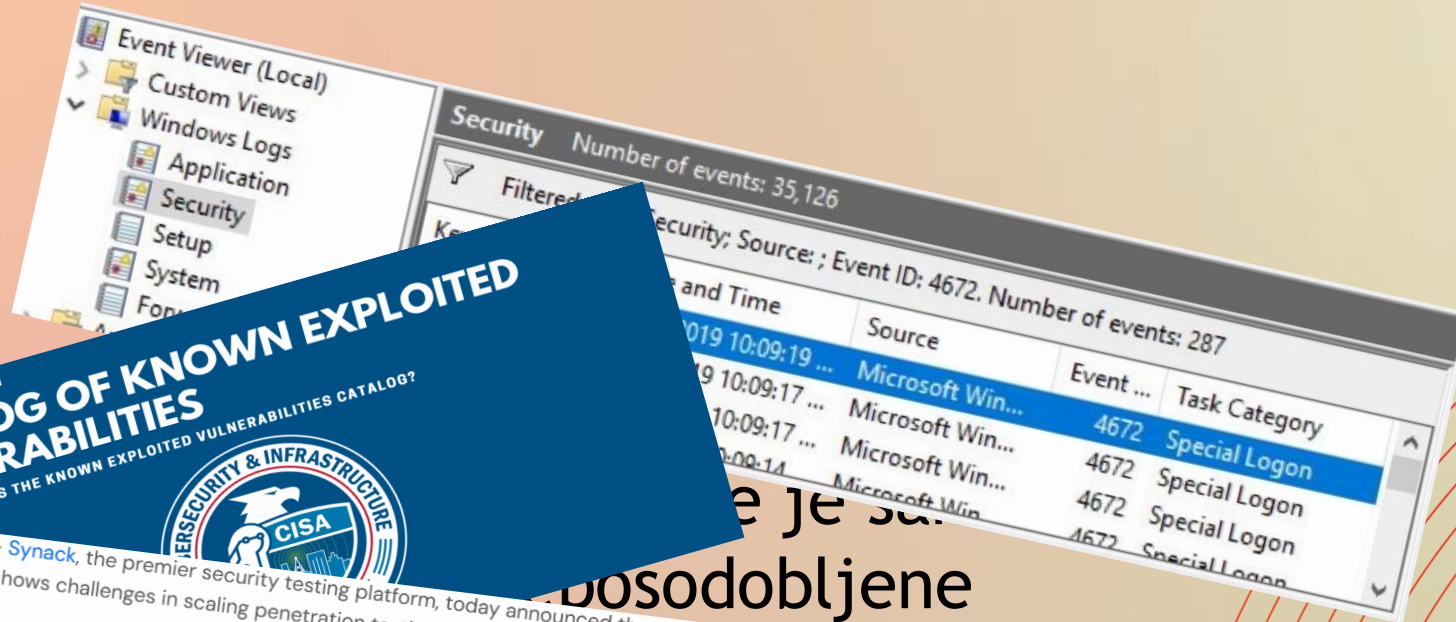
Katere korake moramo narediti, da bi zmanjšali možnosti napada?

Kako in kdaj ukrepamo v primeru kraje dostopnih podatkov?



Trend V1 ASRM

Zakaj



69% orga
kiberne

REDWOOD CITY, Calif., June 10, 2024 — Synack, the premier security testing platform, today announced the results of a survey led by TechTarget's Enterprise Strategy Group (ESG) that shows challenges in scaling penetration testing to meet the needs of large enterprises.

The report commissioned by Synack leverages insights from 200 technical decision-makers at U.S. organizations with at least 1,000 employees. Half of the survey respondents reported it was more difficult to manage their attack surface today than it was a year ago, whether because of third-party risk, data complexity or increasing attacker sophistication.

Other highlights of the report include:

- 58% of enterprises said detecting vulnerabilities is getting more difficult as their attack surface increases in complexity, size and rate of change

Je sa
bosodobljene

Vir: ESG Research, Attack Surface

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**

Hvala za udeležbo in pozornost!

Vprašanja