Több csatornából származó CTI információk feldolgozása a gyakorlatban

Előadó:
Orosz Nándor
Projekt- és szolgáltatásigazgató
RelNet Technológia Kft.

RelNet technológia

1

TRENDEK

AI generálta káros kódok

01

Signatúra alapú felismerés korlátai, előtérbe kerül a viselkedési minták elemzése

Káros kód életciklus lerövidül

02

Évente 270'000 új kód
= életciklus 36h!

Nagyobb halakra spéci csali

03

Egyedi támadások, többfajta párhuzamosan, figyelemelterelésnek

MSP-k lettek a fő célpont

04

Ha sikeres a törés, sok adat egyszerre érhető el

Az exponenciális növekedés miatt a manuális működés a jövőben a közepes vállalatoknak sem lesz fenntartható

Értékelemzés

05

Melyik vulnerability-t érdemes kihasználni, befektetés/nyereség

Kiberbűnözés

06

Ha külön ország lenne, harmadik lenne a rangsorban, csak USA és Kína előzné meg, jelenleg már 5-7%-a világ összes GDP-jének

Legjövedelmezőbb ág, jobb, mint az avokádó 😊

AMIT TAPASZTALTUNK:

- kihasznált sérülékenység, kiépített hátsó ajtó, de kivárnak, hogy mézesbödön-e, nem történik effektív káros tevékenység
- a hátsó ajtón keresztül tesztelik, hogy milyen gyorsan frissülnek a patch-ek
- vagy tartaléknak hagyták, mert vannak eredményesebben törhető találataik,
- vagy maguknak hajtják végre a frissítést, hogy mások ugyan azzal a sérülékenységgel ne tudjanak bemenni…

CTI - ITS

Védekező oldalról át kell állítani a nézetet a támadó oldalra

Skybox dióhéjban

- tűzfal szabályrendszer optimalizáció
- támadási felület folyamatos ismerete/ felügyelete
- sérülékenység menedzsment

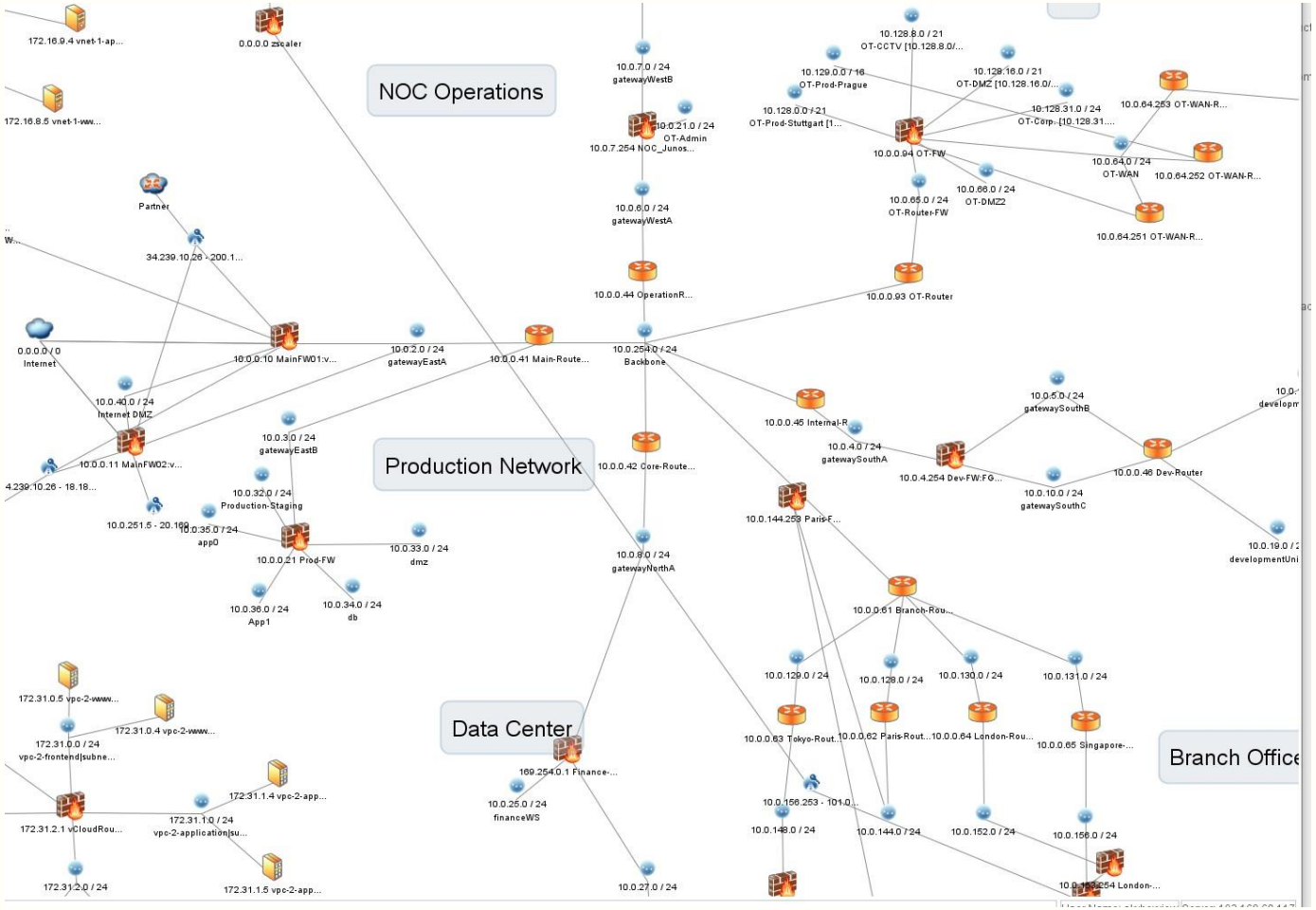
Topológia tudatosság vs CVSS

Automatizált beavatkozás a menedzselt tűzfalak konfigurációiba

Mivel van topológia és átsúlyozott sérülékenységek, ezért végrehajtható egy támadás-szimuláció

4

TOPOLÓGIA-TUDATOSSÁG



INTELLIGENCE FEEDEK

35 különböző adatforrás

Integráció többféle sérülékenység vizsgáló eszközzel

Qualys Cloud Platform
Rapid7 Nexpose
Tenable Nessus
Tripwire IP360
OpenVAS integráció folyamatban

IPS (Intrusion Prevention System) adatbázisok, folyamatos frissítéssel

Check Point IPS,
Palo Alto Networks,
Cisco Sourcefire,
McAfee IPS (Trellix),
…

Vulnerability Control + Content update előfizetés Skybox-szon belül

Sérülékenység-kihasználási figyelmeztetések

Expliot-DB,
AlienVault OTX,
X-Force Exchange

Egyéb szakértői adatbázisok és kutatói publikációk

CISA Known Exploited Vulnerabilities
MITRE CVE
CERT & ICS CERT
First.org EPSS
Security researchers via social media
Published vulnerabilities and exploits

További frissülő adatbázisok

NIST NVD,
Red Hat CVE Database

Gyártói ajánlások, jó gyakorlatok, hardening

Fortinet,
Check Point,
Cisco,
Juniper
VMware,
Red Hat,
Microsoft,
IBM,
Mozilla,
…

GYAKORLATI PROJEKT TAPASZTALATOK, MEGOLDANDÓK

Assetek azonosítása, CMDB egyértelműség

- több rendszer is képes asset jellegű adatok kezelésére, ki kell jelölni egy hiteles CMDB adatforrást, amihez az összes többi rendszer igazodik
- asset duplikációk megszűntetése, egyedi azonosítók
- IP-cm nem tökéletes a célra, mert kioszthtató másik eszköznek is
- nem látható, hogy egy IP-cím mögött eszköz / port vagy kiajánlott szolgáltatás van

Hálózati láthatóság

- a modellben a „szigetek” felszámolása, manuális hozzárendelés
- architekturális gondolkodás – külön Collectorok elhelyezése a nem összenyitható alhálózatokban

Adatforrások

- több irányból bejön ugyan az a sérülékenység jelzés (túl sok info)
- egy jól hardenelt hálózati eszközt pl. a Rapid7 egy általános szervernek azonosít (túl kevés info)

GYAKORLATI PROJEKT TAPASZTALATOK, MEGOLDANDÓK

Adatgazdagítás

- felelős személy hozzárendelése
- az átsúlyozott sérülékenységet hozzá kell rendelni az assethez

A mitigáláshoz change folyamat indítás

- Skybox saját Change Manager moduljában
- SNOW vagy egyéb ticketing / SM rendszer integráció
- SOAR integráció

Interfészek

- átgondoltan kell mozgatni az asset és a vulnerability jellegű adatokat
- gyári API-k
- xml
- „jól bevált CSV”

EGYÉB LEHETŐSÉGEINK

Adatbővítés pl. üzleti tranzakciós adatokkal Fraud Prevention

- azonnali átutalási rendszerekben tizedmásodpercek vannak a döntésre
- **adatgazdagítás:** a tranzakciós adatok mellé a döntéshez egyéb, pl. monitoring/ hálózatos/ L7 adatok is kellenek
- tranzakció-tudatosság
- Skybox felé API-n keresztül átadható a Fraud Prevention rendszer felől a kért tűzfalszabály-módosítás

Kézi engedélyezés vagy automatizmus

Bankok és nagy infrastruktrúra szolgáltatók már az automatizmus irányába mozdulnak

Orchestrator (karmester) igény megjelenik

További adatforrás: NAD/NDR hálózati anomália észlelés (pl. Flowmon ADS, ExtraHop, Vectra)

VALIDÁCIÓS MEGOLDÁS

De jó lenne, ha ténylegesen egy eszköz az ismert sérülékenységeken végig is lépkedne
nem-destruktív módon,
hozzáférések megszerzésével, jogosultsági szint növelésével
mert akkor az **nem szimuláció lenne, hanem validáció.**

Van ilyen megoldás: PENTERA

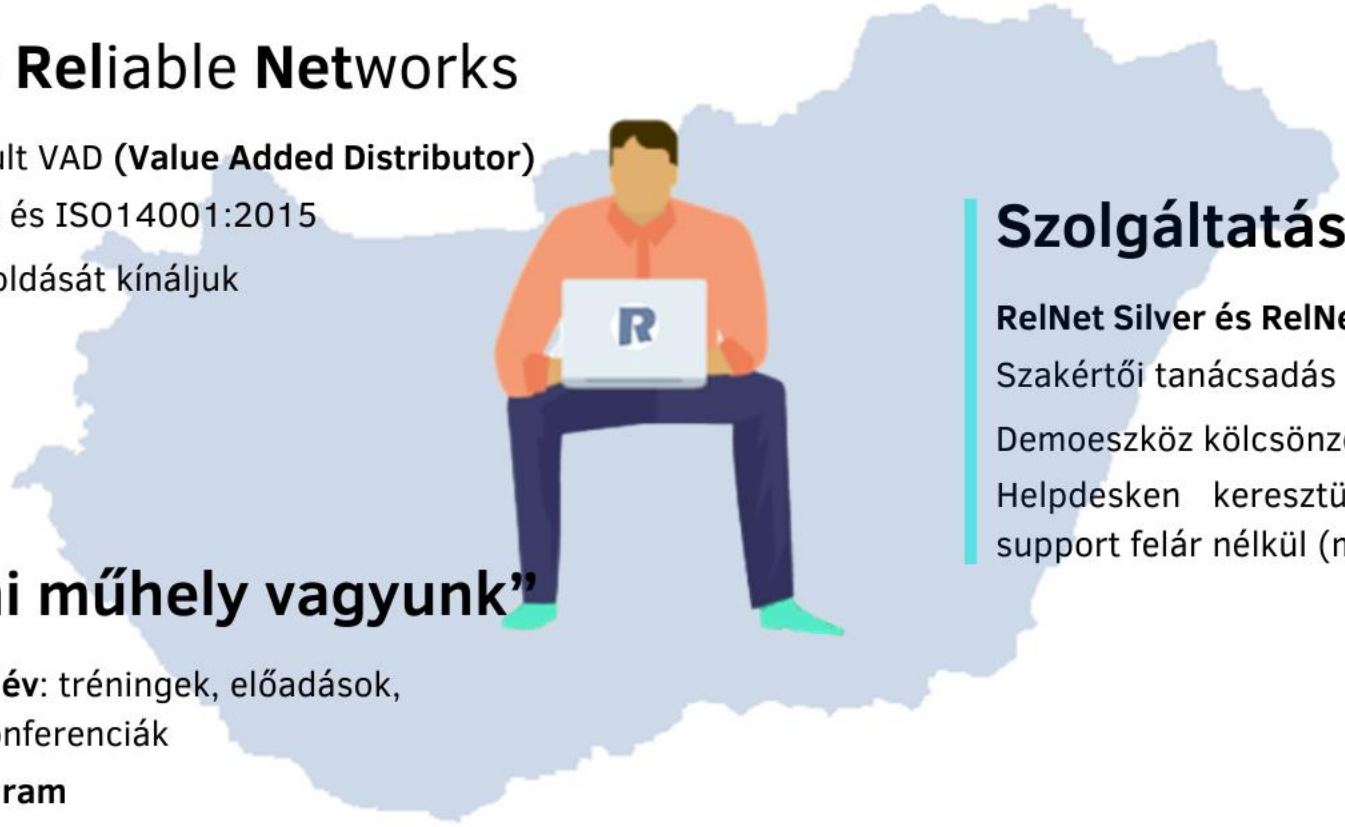
BEMUTATKOZÁS

RelNet = Reliable Networks

2004-ben alakult VAD **(Value Added Distributor)**

ISO 9001:2015 és ISO14001:2015

24 gyártó megoldását kínáljuk



„Szakmai műhely vagyunk”

~50 esemény /év: tréningek, előadások, workshopok, konferenciák

eLearning program

Szolgáltatásaink

RelNet Silver és RelNet Gold támogatások

Szakértői tanácsadás

Demoeszköz kölcsönzés + POC

Helpdesken keresztül **7/24 magyar nyelvű** support felár nélkül (már 1 licensz vásárlásától)

E-LEARNING

Skybox – A kiberfenyegetések menedzsmentje egyszerűen

Bővebben

Skybox – Az IT/OT konvergencia kockázatcsökkentése

Bővebben

Skybox Security – CTEM – Folyamatos kitettség- és fenyegetésmenedzsment

Bővebben

Pentera – Penetrációs tesztelés és biztonsági validáció

Bővebben

Pentera Demo – Támadási vektorok felvázolása és sérülékenységek osztályozása

Bővebben

Pentera viszonteladóknak 1 – Értékesítési folyamat

Bővebben

Pentera viszonteladóknak 2 – Demózási technikák ügyfelek számára

Bővebben

Pentera viszonteladóknak 3 – 'Proof of Value' nap az ügyféllel

Bővebben

Pentera viszonteladóknak 4 – Pentera Surface és partnerprogram

Bővebben

Pentera – A biztonsági validáció lényege és előnyei

Bővebben

ELVIHETŐ GONDOLATOK

Tranzakció tudatosság

Orchestrator funkció

Topológia tudatosság

+1 Szimuláció vs. validáció

KÉRDÉSEK

Köszönöm a figyelmet!

Orosz Nándor
Projekt- és szolgáltatásigazgató
RelNet Technológia Kft.

+36 30/288 0953

norosz@relnet.hu