BLACK CELL
Protecting critical infrastructures

A hálózat sötét oldala – forgalomfigyelés belülről

Bevezetés

A kibertámadások növekvő kifinomultsága miatt, a digitális infrastruktúrák megfelelő védelméhez már nem elegendők a hagyományos biztonsági megoldások.

A Network Security Monitoring (**NSM**) mélyreható vizibilitást és elemzést nyújt, aminek köszönhetően sokkal hatékonyabban tudjuk **észlelni**, **kezelni** és **megelőzni** a fenyegetéseket.

A monitorozás fontossága

- A hálózati viselkedés megértése: Az **NSM** segít megismerni a hálózat normál működését (**baseline**), így észlelhetjük azokat az **eltéréseket**, amelyek rosszindulatú tevékenységre vagy technikai problémára utalhatnak.
- Fejlett védelmi ökoszisztéma: A **folyamatos monitorozás és elemzés** révén a szervezetek alkalmazkodni tudnak a **folyamatosan változó** fenyegetésekhez, ami összességében egy sokkal robusztusabb védelmi ökoszisztémát eredményez.
- Proaktív védekezés: **Képes felismerni** azokat a fenyegetéseket, amelyek a **hagyományos** szignatúra alapú rendszerek **nem** feltétlenül detektálnak.
- Behatolások korai észlelése: Lehetővé teszi a rosszindulatú tevékenységek azonosítását **már a kezdeti szakaszban**, minimalizálva ezzel a lehetséges károkat.

A monitorozás fontossága

- Incidensreagálás: A **részletes hálózati naplózás** és a forgalom értelmezése megfelelő **kontextust** és adatokat biztosít a hatékony incidensvizsgálathoz és az incidensekre való megfelelő reagáláshoz.
- Threat Hunting: A hálózati forgalom folyamatos elemzésével **proaktívan kereshetővé** válnak a kompromittálódásra utaló jelek (IOC-k).
- Belső fenyegetések észlelése: Az NSM képes azonosítani a szervezet **hálózatán belüli** rendellenes viselkedést, ami akár rosszindulatú belső munkatársakra vagy feltört fiókokra is utalhat.

A monitorozás fontossága

- Szabályozási megfelelés: Számos jogszabály és keretrendszer **előírja** a magas szintű biztonsági felügyeletet és naplózási képességeket. Az NSM **segít megfelelni** ezeknek a követelményeknek.

- Adatvesztés megelőzése: A hálózati forgalom megfigyelésével a szervezetek észlelhetik és megakadályozhatják az **érzékeny adatok** jogosulatlan kiszivárgását a hálózatról.

- Sérülékenységkezelés: Az NSM-ből származó adatok rávilágíthatnak az ismert **sebezhetőségek** elleni **támadási kísérletekre**, ezzel segítve a frissítések ütemezését és priorizálását.

Hogyan monitorozzuk a forgalmat

Az NSM a tükrözött hálózati forgalom passzív monitorozását látja el.

- Beavatkozás nélküli elemzés: A **passzív** monitorozás során az eszközök a hálózati forgalom másolatát kapják meg, anélkül, hogy aktívan beavatkoznának vagy módosítanák az eredeti adatfolyamot. Ez biztosítja, hogy **semmilyen hatással** ne legyen a hálózat **teljesítményére** vagy **stabilitására**.

- Átfogó vizibilitás: A tükrözött forgalom elemzésével a biztonsági eszközök **széleskörű vizibilitást** kapnak a hálózati kommunikációra, beleértve az úgynevezett „**kelet-nyugat**" forgalmat is, amelyet a hálózati határvédelmi rendszerek gyakran figyelmen kívül hagynak.

- Historikus adatok rögzítése: Lehetővé teszi a hálózati forgalom időbeli rögzítését és tárolását. Ez elengedhetetlen az incidensek **visszamenőleges elemzéséhez**, a trendek azonosításához és a megfelelőségi követelmények teljesítéséhez.

Hogyan monitorozzuk a forgalmat

Az NSM a tükrözött hálózati forgalom passzív monitorozását látja el.

Tükrözési megoldások:

- SPAN portok: Hálózati switchek beépített funkciója, amely lehetővé teszi, hogy a forgalmat egy vagy több forrásportról vagy VLAN-ról lemásoljuk, és egy kijelölt célportra küldjük.
- Hálózati TAP-ek: Fizikai hardvereszközök, amelyeket közvetlenül a hálózatba illeszthetünk be. A TAP-ek másolatot készítenek a hálózati forgalomról anélkül, hogy az eredeti adatfolyamot befolyásolnák.
- Virtuális TAP-ek (vTAP-ek): A hagyományos TAP-ek virtuális megfelelői, amelyek lehetővé teszik a virtuális gépek közötti forgalom megfigyelését.

NSM komponensek

Két kulcsfontosságú komponense van:

- Suricata:

Nyílt forráskódú, hatékony és gyors hálózati behatolásérzékelő rendszer (**IDS**), behatolásmegelőző rendszer (IPS) és hálózati biztonsági elemző motor.

- Zeek:

Nyílt forráskódú hálózati biztonsági **elemző** keretrendszer, amely a hálózati forgalom **mélyreható elemzésére** fókuszál. A Zeek részletes naplókat generál a hálózati eseményekről, ami elengedhetetlen a komplex vizsgálatokhoz és a hálózati viselkedés mély megértéséhez.

Ezeket jól kiegészítik az alábbi komponensek:

- NSM Threat Intel Feed
- Detection-as-Code (testreszabás, automatizálás)
- Gépi tanulás
- További protokollértelmezők, ideértve olyan OT protokollokat is, mint: MODBUS, MMS, IEC 104, GOOSE, BACnet, stb.
- További protokollok: Igény esetén lehetőség van további protokollértelmezők fejlesztésére.

NSM komponensek

Suricata - IDS

Behatolásérzékelő rendszer (IDS): A Suricata képes detektálni a kártékony vagy gyanús **mintázatokat** a hálózati forgalomban.

Szignatúra alapú észlelés: Előre definiált szabályok és **szignatúrák** alapján észleli az ismert fenyegetéseket.
Ezt a képességet az **NSM-TIF** jelentősen fokozza.

Anomália-alapú detektálás: A hagyományos szignatúrák mellett képes felismerni a normál hálózati viselkedéstől való eltéréseket is. Ezek az **anomáliák** új vagy ismeretlen fenyegetésekre utalhatnak.

Szabálynyelv: A Suricata egy rugalmas és hatékony szabálynyelvet használ, amellyel egyedi detektálási szignatúrákat definiálhatunk.

NSM komponensek

Zeek - Elemző

Mélyreható csomagelemzés: A Zeek képes a mélyreható csomagelemzésre (**Deep Packet Inspection**, DPI), ami azt jelenti, hogy az alkalmazási rétegig lebontva elemzi a hálózati forgalmat. Ennek köszönhetően olyan részletes információkhoz juthatunk, amelyek a felületesebb vizsgálatok során rejtve maradnának (például csak a fejlécek vizsgálata esetén).

Protokollelemzés: A Zeek kiemelkedően jól teljesít a **protokollelemzésben**. Képes számos protokollt, például a HTTP, SMTP, DNS és SSH protokollokat értelmezni (**parsing**), hogy azokból releváns információkat nyerjen ki.

Viselkedéselemzés: A Zeek a kommunikációs **mintázatok** elemzésével képes a gyanús vagy kártékony hálózati **viselkedéseket** azonosítani.

Szkriptnyelv: A Zeek fejlett szkriptnyelvet biztosít, amellyel testreszabható az elemzés és egyedi naplók hozhatók létre.

DPI vs Szignatúra

Table JSON

iec104

Field	Value
iec104.apdu_type	I
iec104.asdu_address	1
iec104.asdu_length	10
iec104.asdu_type	46
iec104.confirm	false
iec104.cot	6
iec104.execute	false
iec104.indeterminate0	false
iec104.indeterminate3	false
iec104.ioa	393,261
iec104.ioa_num	1
iec104.longpulse	false
iec104.origin	0
iec104.persistent	false
iec104.rec_num	13,738
iec104.select	true
iec104.send_num	2
iec104.shortpulse	false
iec104.state_off	true
iec104.state_on	false
iec104.uid	Co9CgxhpQZGwiiVO4

A kulcsinformációk kinyerését, értelmezését követően azt strukturált formában tárolhatjuk.

Az ilyen adathalmazban már kereshetünk, elemezhetjük azt, vagy akár gépi tanulási algoritmusokat vethetünk be rajta.

```
0000  bc 24 11 cb 30 1a bc 24  11 e0 f1 1d 08 00 45 00   ·$··0··$ ·····E·
0010  00 44 ac 65 40 00 40 06  72 b3 c0 a8 4d 24 c0 a8   ·D·e@·@· r···M$··
0020  4d 26 97 88 09 64 21 e6  14 08 5c 85 b7 bc 80 18   M&···d!· ··\·····
0030  00 f9 1b d2 00 00 01 01  08 0a bc af aa ce ff 29   ·····)
0040  ba 18 68 0e 04 00 54 6b  2e 01 06 00 01 00 2d 00   ··h···Tk ·····-··
0050  06 81                                             ··
```

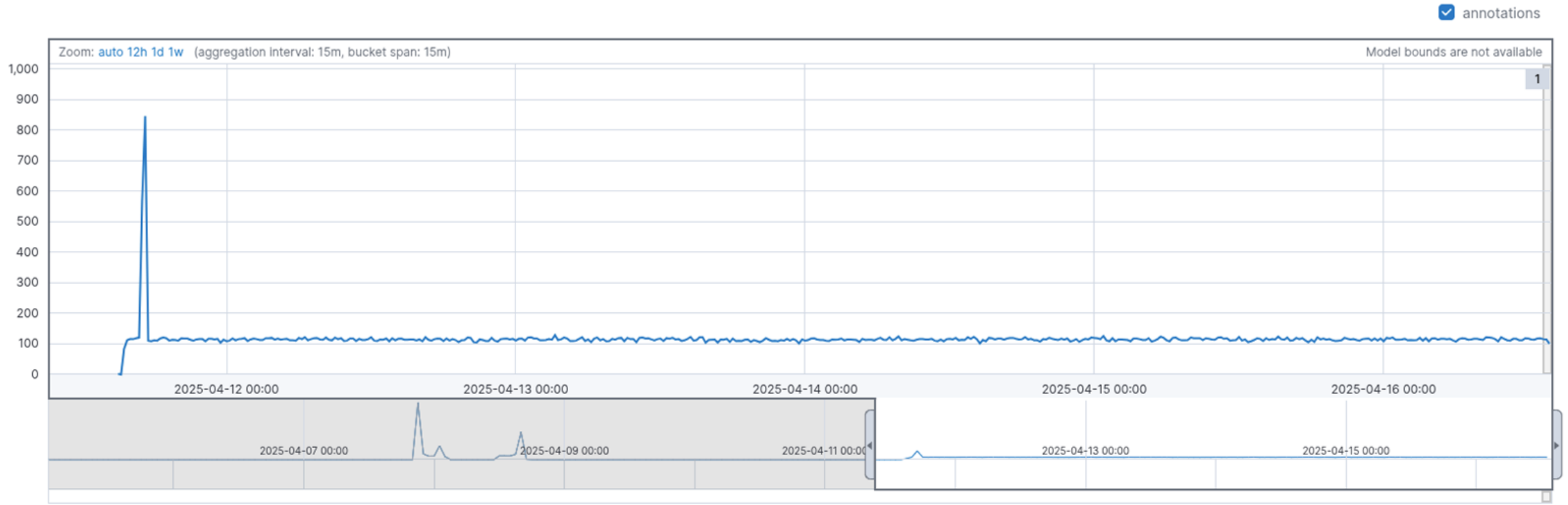
Field	Value
message	{"sourceIP":"192.168.77.36","sourcePort":38792,"destinationIP":"192.168.77.38","destinationPort":2404,"ts":1744807686.395425,"uid":"Co9CgxhpQZGwiiVO4","asdu_length":10,"apdu_type":"I","send_num":2,"rec_num":13738,"ioa_num":1,"cot":6,"asdu_type":46,"origin":0,"asdu_address":1,"confirm":false,"ioa":[393261],"state_on":[false],"state_off":[true],"indeterminate0":[false],"indeterminate3":[false],"shortpulse":[false],"longpulse":[false],"persistent":[false],"execute":[false],"select":[true]}

Gépi tanulás

Detects high count of network denies.

Forecast

Single time series analysis of count



Annotations Total: 1

Összefoglaló

A **Suricata** a **szignatúra alapú** IDS riasztásokat biztosítja, a **Zeek protokollértelmezés** segítségével biztosítja a kontextust az elemzésekhez.

Kiegészítik, nem pedig helyettesítik egymást.

Hatékonyságuk fokozható threat intel adatforrással (**NSM Threat Intel Feed**), kiegészítő **protokollértelmezőkkel** és **gépi tanulással**.