

XDR

nástroj, ktorý vidí súvislosti

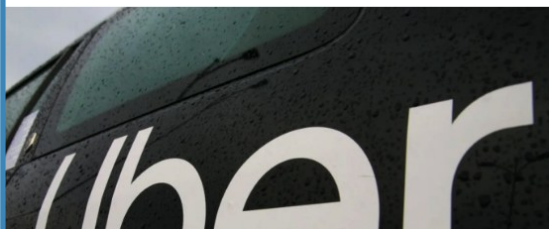
NÁSLEDKY KYBERNETICKÉHO ÚTOKU

Ex-Uber security chief sentenced over covering up hack

5 May 2023

Tom Gerken
Technology reporter

Share Save



REPUTAČNÉ ŠKODY

Hacker igigi ďalej útočí. Najnovšími obeťami sú Union, Denik.cz a Atlas.sk

Cez víkend skopíroval databázu stránky Orangeu. Pred Vianocami napadol weby Unionu a jemu príbuzných finančných domov. Nasledovali Denik.cz a Atlas.sk.

Tomáš Ulej



Kybernetický útok na Jaguar Land Rover stál britskú ekonomiku miliardy libier

22. 10. 2025, 11:45 (aktualizované: 22. 10. 2025, 14:56)



MATERIÁLNE ŠKODY

KYBERNETICKÝ ÚTOK NA OKD A NEMOCNICE? ŠKODY JDOU DO DESÍTEK MILIONŮ

UDÁLOSTI • ONDŘEJ STRATILÍK, 25. 6. 2020



10. okt 2024 o 20:41

Sieť hotelov Marriott zaplatí pokutu pre únik osobných údajov klientov

Prípady úniku osobných údajov sa stali v rokoch 2014 až 2020.

SITA



PRÁVNA ZODPOVEDNOSŤ

AKTUALIZOVANÉ Mall.cz dostal pokutu za únik dát v Česku, zaplatí 1,5 mil. korún



ÚTOKY NIKDY NEBOLI DOSTUPNEJŠIE

BANKING TROJANS/EXPLOIT KITS/MALWARE DROPPERS	
TYPE	PRICE
Emotet Trojan (spreader/malware dropper)	\$1,000
Trickbot Banking Trojan	\$600
TinyNuke	\$6,000
Parasite HTTP RAT	\$500
Generic Exploit Kit	\$2,080/month
Fallout Web Exploit Kit	\$300/week
Drupal RCE Exploit	€71
Android Clipper (SMS stealer)	\$150
Chip POS	\$700

Source: Arbor

RANSOMWARE AND RANSOMWARE-AS-A-SERVICE (RaaS)	
TYPE	PRICE
Generic Ransomware #1	\$225
Generic Ransomware #2	\$660
Inpivx	Ransomware + Panel + Tutorial = \$500 Ransomware-only – \$300 Panel-only – \$200
Ranion-(RaaS)	12 Months – \$900 6 Months – \$490 1 Month – \$120
Megacortex	\$1,000 or €1,000 + 10% of Ransom

Source: Arbor

ZÁKON O KYBERNETICKEJ BEZPEČNOSTI



NAJČASTEJŠIE NEDOSTATKY

- Absencia ucelenej bezpečnostnej architektúry
- Absencia ochrany endpointov (XDR)
- Prítomnosť nástrojov, ktoré však nie sú vyhodnocované
- Absencia SIEM/SOC riešenia
- Absencia dohľadového tímu, absencia pracovného času MKB

Reputačné škody



Materiálne škody



Právna zodpovednosť



Čo sa môže stať?

Keď sa stanete obeťou ransomvérového útoku, odcudzia vám dáta, následne zašifrujú systémy - vo väčšine prípadov s cieľom finančného zisku prostredníctvom vydierania alebo z predaja ukradnutých dát.



- Kybernetické hrozby sa neustále vyvíjajú
- Objavujú sa nové spôsoby útokov
- Opatrenia založené na organizačných opatreniach a „ľudskom faktore“ sú málo účinné
- Mať antivírus nestačí.

Na prienik do prostredia postačuje napríklad phishingový e-mail alebo zneužitá zraniteľnosť.
Nasleduje kompromitácia používateľského účtu alebo zariadenia a útočník získava prvotný prístup do siete.



- Otázkou nie je či sa stanete cieľom útoku, ale otázkou je kedy sa to stane
- Posilňovanie kybernetickej bezpečnosti je nutnosťou, a to aj z legislatívneho hľadiska
- Krokom pre zlepšenie KB je novela ZoKB.

Útočník sa pohybuje v sieti bez vyvolania poplachu, zbiera informácie o infraštruktúre a používateľoch, a to bez viditeľného dopadu na prevádzku. Získava prístup ku kritickým serverom a dátam, prebieha exfiltrácia (tiché kradnutie) dát mimo organizácie. Nasleduje príprava úderu. Zálohy sú znefunkčnené.

Obeť o útoku stále nevie, ransomware je však už distribuovaný v prostredí. Útok je pripravený na spustenie.



- Bez nástrojov nie je možné naplniť legislatívny rámec (ZoKB č. 69/2018 Z.z.)
- Bez nástrojov nie je možná analýza rizík a prijímanie bezpečnostných opatrení
- Bez nástrojov nie je možná správa aktív či riadenie kybernetických hrozieb, rizík a incidentov

Deň "D,,.

Používatelia sa nevedia prihlásiť, systémy sú zašifrované, nasleduje vydieranie a hrozba zverejnenia alebo predaja dát. Incident sa stáva závažným problémom s negatívnym dopadom na organizáciu. **Už je neskoro na opatrenia.**

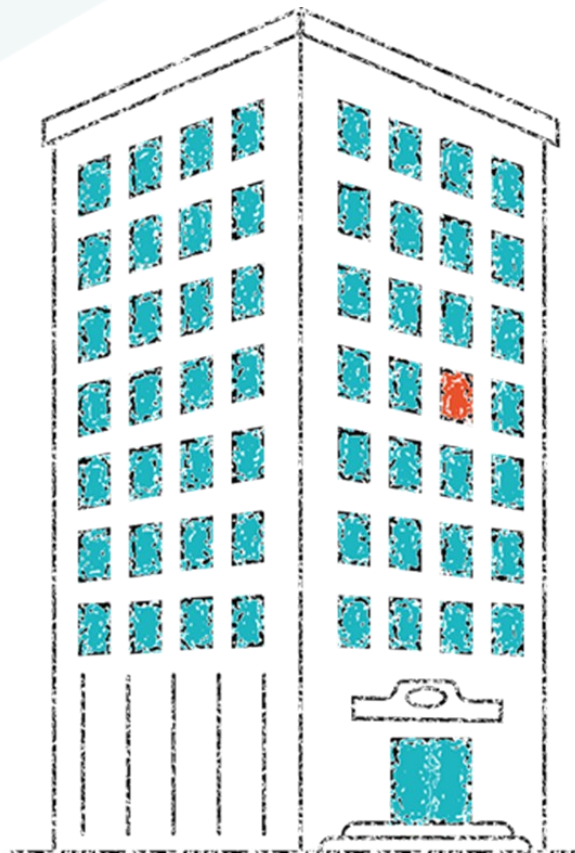


- Po ukončení šifrovania dát sa útok nedá zastaviť a dáta boli exfiltrované dávno pred incidentom
- Zálohy sú kompromitované a náklady na obnovu výrazne presahujú cenu prevencie
- Ďalšie rozhodnutia sa robia pod časovým a finančným tlakom

Čo by pomohlo?

Ochrana koncových bodov, centrálny bezpečnostný monitoring, detekcia pohybu v sieti a incident response plán.

Bezpečnostní specialisti
potrebujú chrániť
kompletne **celý perimeter**



Útočníkom stačí nájsť
jedno slabé miesto

- Centrálny monitoring aktivít a kybernetických incidentov v infraštruktúre nástrojom SOC/**SIEM**.
- Nasadenie ochrany endpointu (XDR) pre efektívnu obranu. XDR nástroj **ESET Inspect** umožní riešiť kybernetickú bezpečnosť v súlade s legislatívou

Bezpečnostný model s centrálnym dohľadom umožní:

- **ochrániť zariadenia** technológiou XDR - **ESET Inspect**, a poskytnúť riadenú reakciu na zistené hrozby
- zber logov, systematické vyhodnocovanie logov z celej infraštruktúry a následnú **koreláciu** bezpečnostných udalostí
- **centrálny monitoring** za použitia **iS Argus 360 SIEM**
- zistiť incident ešte pred vznikom škody
- vytvoriť auditnú stopu a reporting

Čo robí ESET Inspect ?

Zabezpečuje kvalifikovaný dohľad

v súlade s požiadavkami praxe a ZoKB nad udalosťami a incidentmi z prostredia ESET Inspect tak, aby boli výstupy použiteľné pre riadenie kybernetických rizík, interné rozhodovanie a preukázateľnosť plnenia povinností podľa ZoKB.

Priebežne **monitoruje a analyzuje** (systémové aj aplikačné) aktivity na ESET Endpoint a **chráni** pred Zero-Day hrozbami

Odhalí aktivitu, ktorá nemusí byť klasifikovaná ako malware, ale je typická pre prienik - identifikuje reálny incident aj v prípade, ak útočník používa legítimne nástroje

Deteguje potenciálne hrozby a techniky: Malware, Indicators of Compromise (IOC), Techniques Tactics Procedures (TTP) atď.

Udržiava históriu aktivít na koncových bodoch - **Threat Hunting**, zároveň upozorňuje administrátorov systému a ponúka nápravné opatrenia

ESET Inspect poskytuje detailnú telemetriu z endpointov (*procesy, komunikácia, zmeny v systéme, privilegované operácie*).

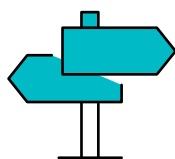
Signály dáva do **kontextu**, koreluje ich v čase a overuje správanie na viacerých úrovniach – nie len podľa jedného alertu.

Výsledok: potvrdenie/ vyvrátenie kompromitácie, odporúčané kroky a remediácia, dopad na aktíva a procesy, auditovateľná dokumentácia, forenzné dôkazy a reporting...

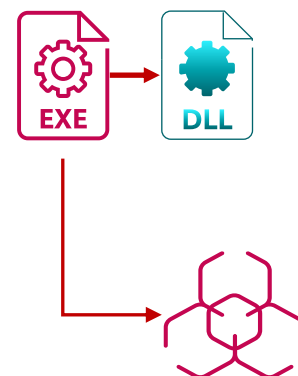
Bez podpory ESET Inspect (XDR)



Minimálna vizibilita



Neistota



Rundll32 spúšťa DLL

Hrozba

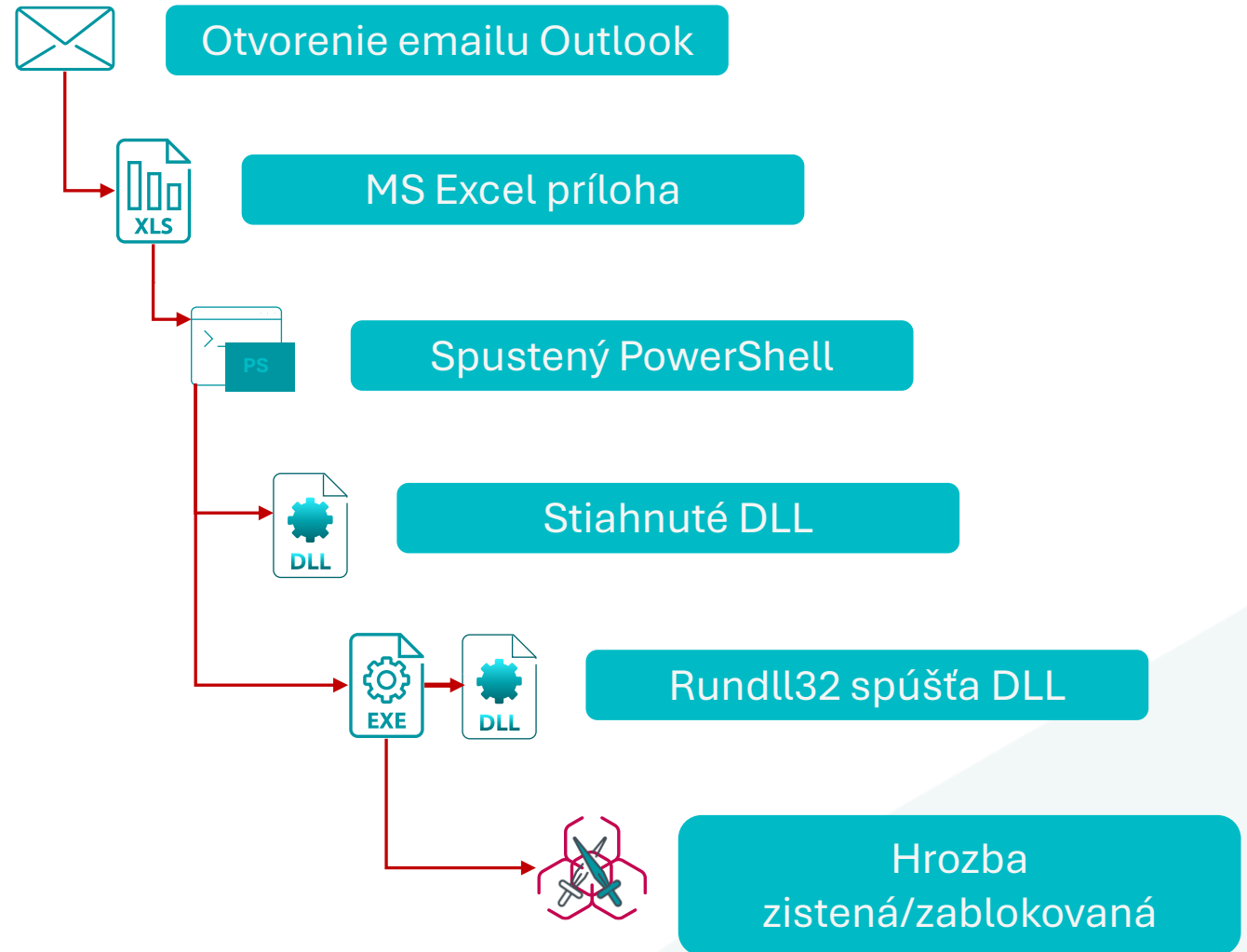
S podporou ESET Inspect (XDR)



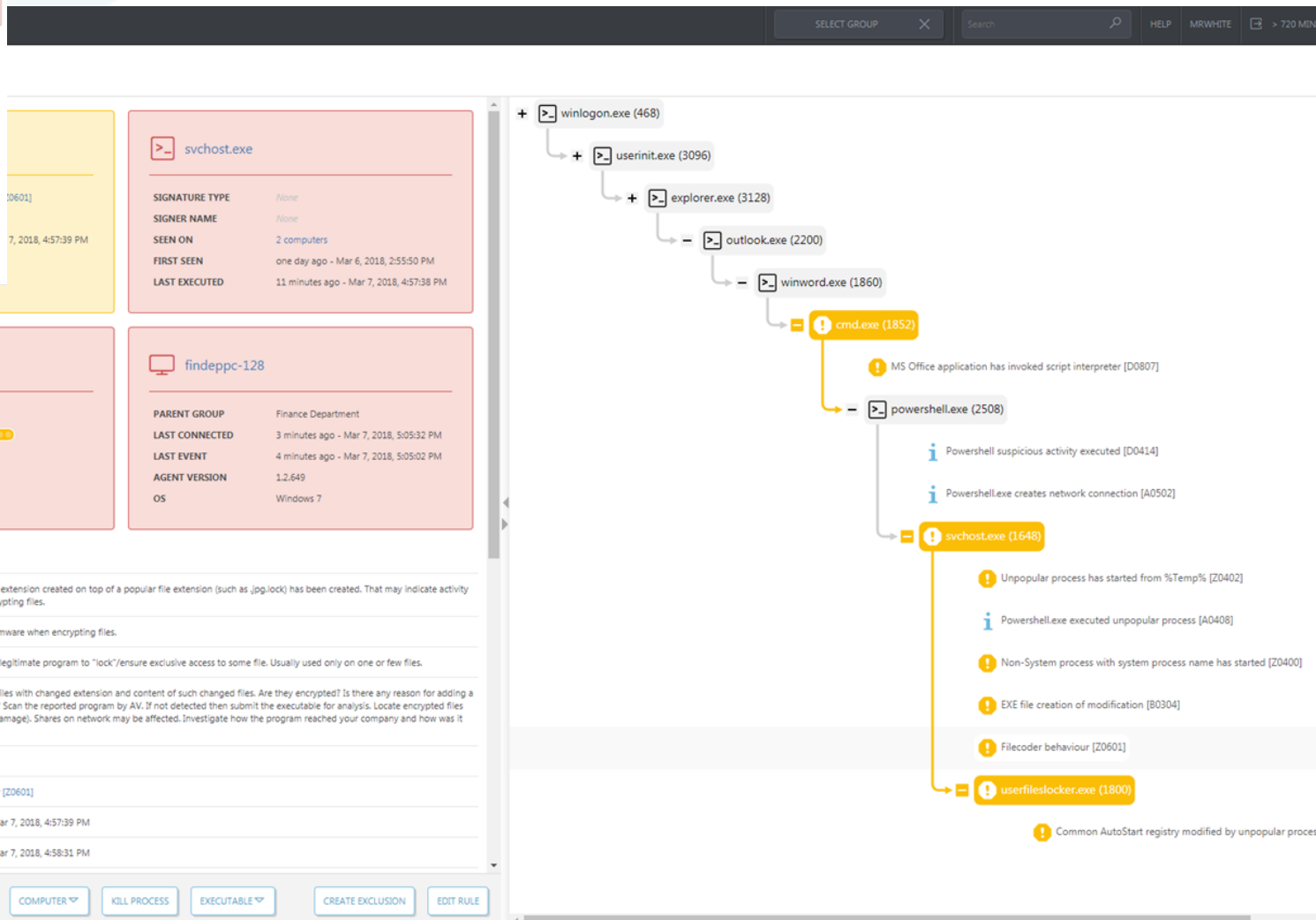
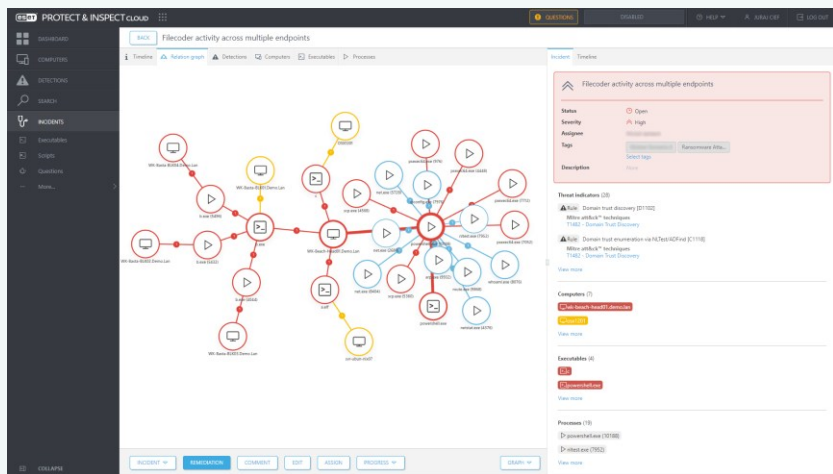
Zvýšená
viditeľnosť



Pokoj v duši :)



ESET Inspect



Jedna konzola

- zjednodušenie
- automatické riešenia
- odporúčané opatrenia
- využívanie AI
- učenie sa z toku dát

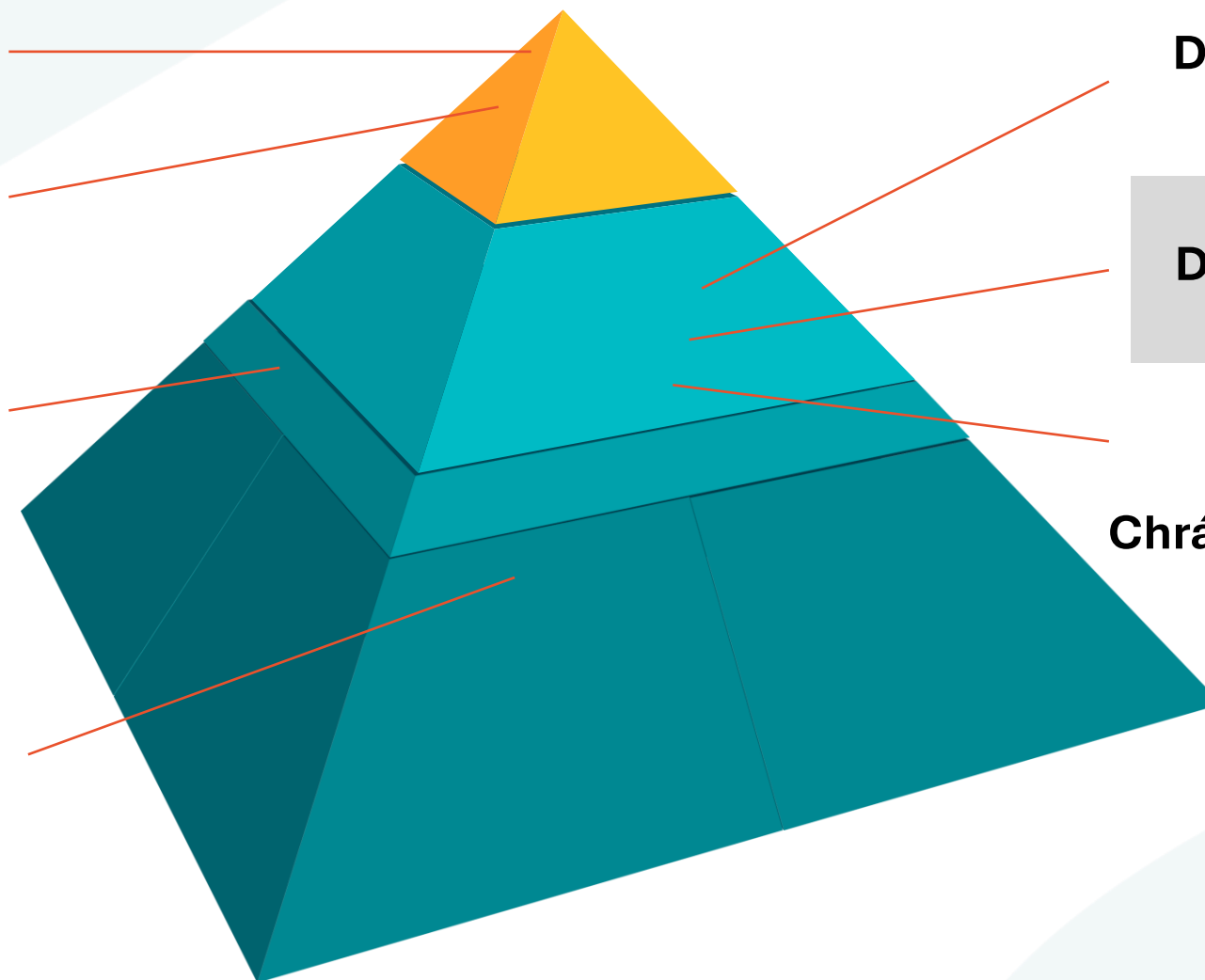
Koncept VIACÚROVNŇOVÉHO ZABEZPEČENIA

iServices
SLA služby / iS SOC

SIEM
iS Argus 360

Analýza v
cloudovom
sandboxe

Viacvrstvová ochrana
na všetkých
platformách



NDR
Detekcia a Reakcia

XDR
Detekcia a Reakcia
ESET Inspect

DLP platforma
Chrání a zabraňuje úniku
citlivých údajov

Koncept VIACÚROVNŇOVÉHO ZABEZPEČENIA

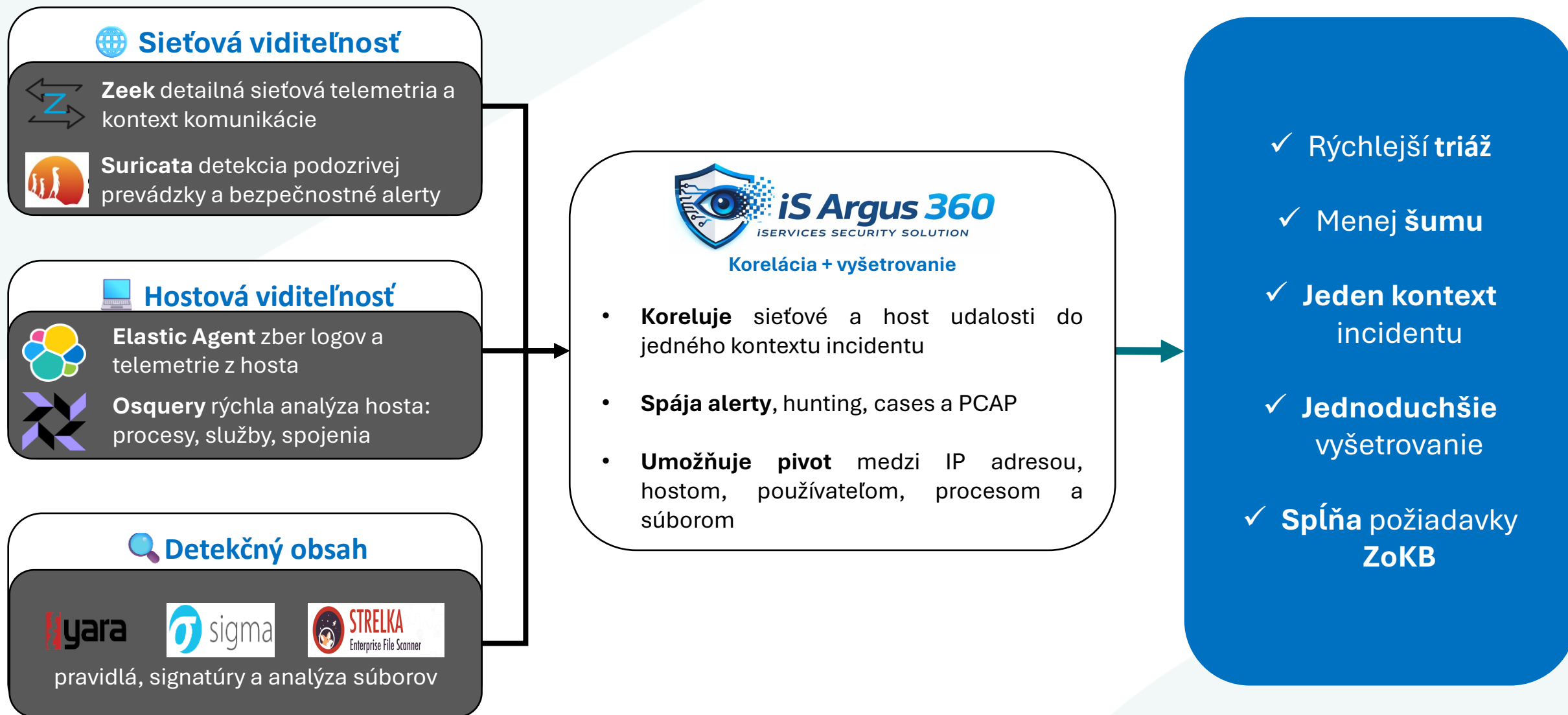




**Centralizovaná viditeľnosť a detekcia
kybernetických hrozieb**

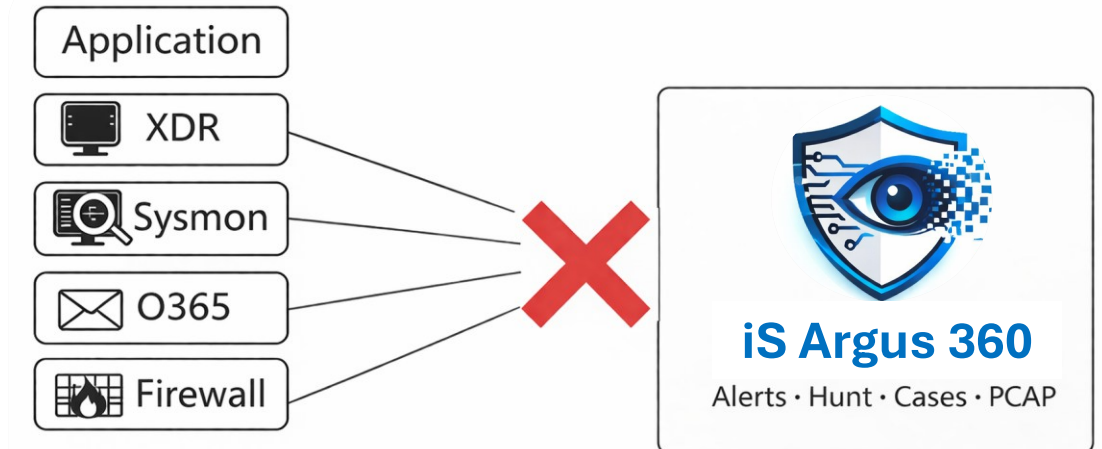


Architektúra iS Argus 360



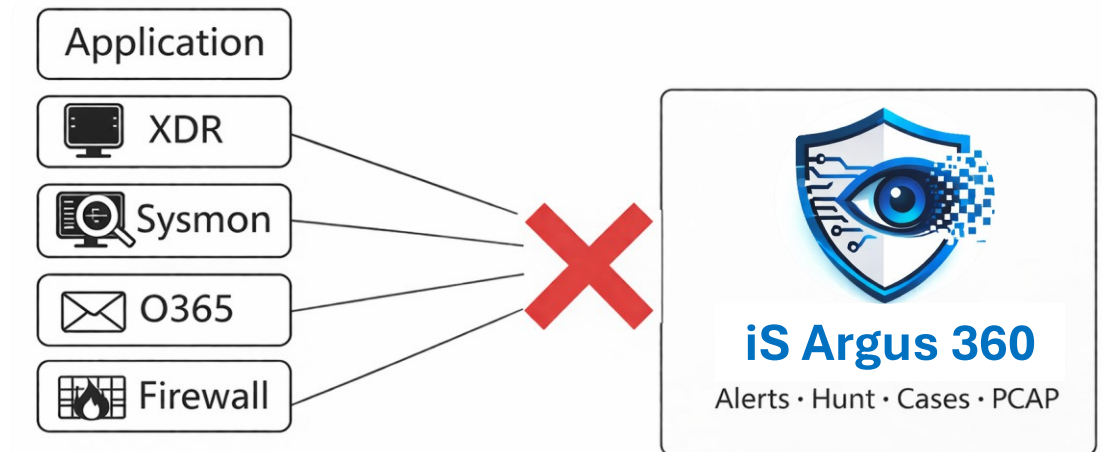
Problém: Fragmentovaná bezpečnostná viditeľnosť

- Dáta sú rozdelené medzi viac systémov
- Korelácia prebieha manuálne
- Vyššie riziko prehliadnutia útoku
- Dlhší čas vyšetrovania



Dôsledky pre biznis:

- Viac času na analýzu incidentov
- Riziko finančných strát
- Problémy s auditom a compliance



Riešenie: iS Argus 360

Riešenie:

- Centralizovaný zber a analýza dát
- Korelácia udalostí v reálnom čase
- Jedno rozhranie pre bezpečnostný monitoring

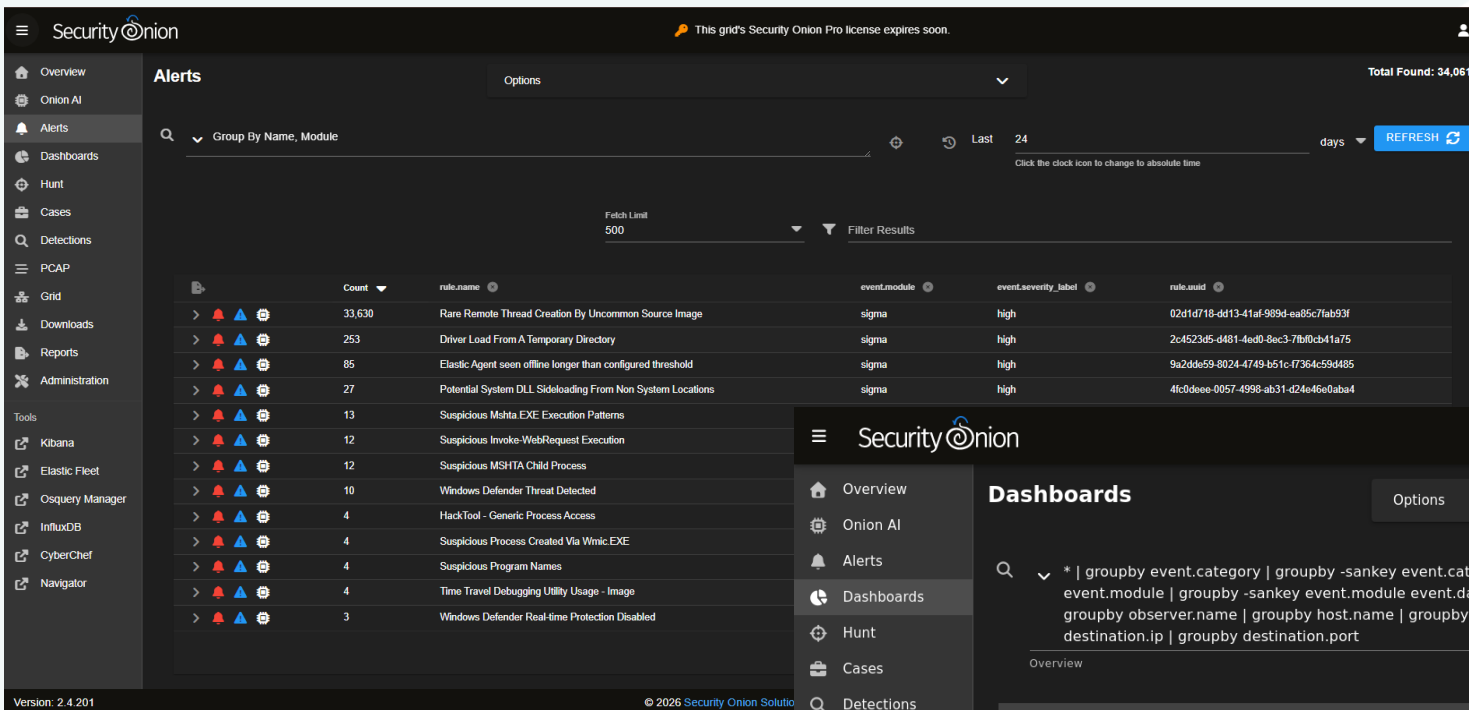


Bez iS Argus 360

- ☐ Nesplnené požiadavky ZoKB
- ☐ Fragmentácia
- ☐ Chýbajúci context
- ☐ Dlhší čas analýzy
- ☐ Viac šumu
- ☐ Manuálna analýza

iS Argus 360

- ✓ Pomáha plniť požiadavky ZoKB
 - ✓ Menej šumu
 - ✓ Rýchlejšia triáž
- ✓ Jasný obraz incident
- ✓ Lepšia viditeľnosť
- ✓ Rýchlejšia reakcia



Security Onion Alerts

Options

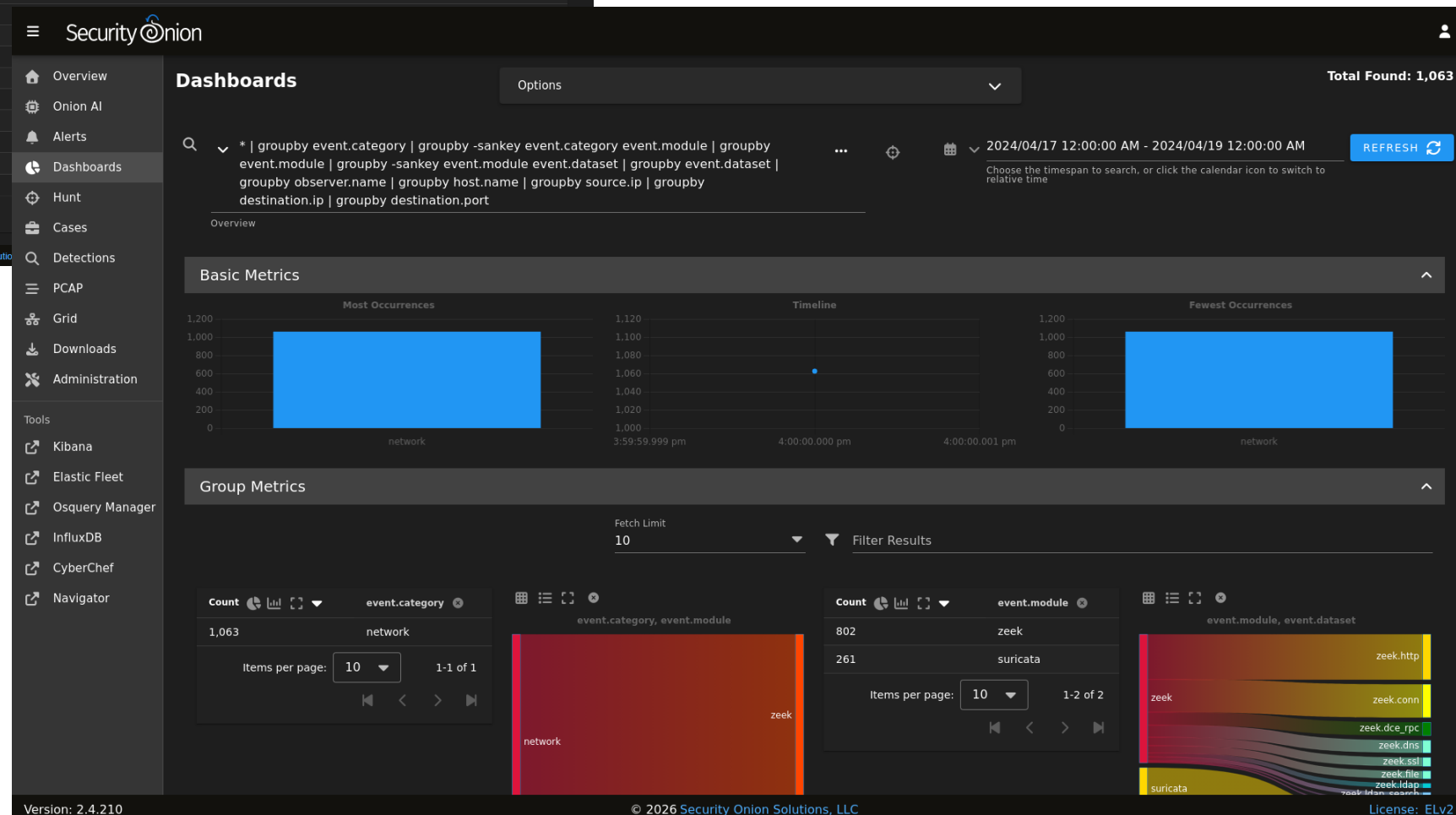
Total Found: 34,061

Group By Name, Module

Fetch Limit: 500

Count	rule.name	event.module	event.severity_label	rule.uuid
33,630	Rare Remote Thread Creation By Uncommon Source Image	sigma	high	02d1d718-dd13-41af-989d-ea85c7fab93f
253	Driver Load From A Temporary Directory	sigma	high	2c4523d5-d481-4ed0-8ec3-7fb0cb41a75
85	Elastic Agent seen offline longer than configured threshold	sigma	high	9a2dde59-8024-4749-b51c-f7364c59d485
27	Potential System DLL Sideloaded From Non System Locations	sigma	high	4fc0deee-0057-4998-ab31-d24e46e0aba4
13	Suspicious Mshta EXE Execution Patterns			
12	Suspicious Invoke-WebRequest Execution			
12	Suspicious MSHTA Child Process			
10	Windows Defender Threat Detected			
4	HackTool - Generic Process Access			
4	Suspicious Process Created Via Wmic.EXE			
4	Suspicious Program Names			
4	Time Travel Debugging Utility Usage - Image			
3	Windows Defender Real-time Protection Disabled			

Version: 2.4.201



Security Onion Dashboards

Options

Total Found: 1,063

* | groupby event.category | groupby -sankey event.category event.module | groupby event.module | groupby -sankey event.module event.dataset | groupby event.dataset | groupby observer.name | groupby host.name | groupby source.ip | groupby destination.ip | groupby destination.port

Overview

Basic Metrics

Most Occurrences

Timeline

Fewest Occurrences

Group Metrics

Fetch Limit: 10

Filter Results

Count: 1,063

event.category: network

Items per page: 10

1-1 of 1

Count: 802

event.module: zeek

Items per page: 10

1-2 of 2

Count: 261

event.module, event.dataset: zeek

Items per page: 10

1-2 of 2

Count: 10

event.module, event.dataset: zeek

Items per page: 10

1-2 of 2

Version: 2.4.210

© 2026 Security Onion Solutions, LLC

License: ELv2

- Visibility
- Detection
- Investigation
- Response



Viditeľnosť

Compliance

Detekcia

Reakcia

Otázky

Procesy

Aký je Váš súčasný proces zisťovania a vyšetrovania incidentov ?

Akú viditeľnosť máte do správania používateľov ?

Akým výzvam čelíte pri monitorovaní útokov na vaše prostredie ?

Aké percento varovaní je skutočné a zaslúži si detailnú analýzu ?

Aké sú vaše nároky na dodržiavanie požiadaviek na uchovávanie záznamov
/ log manažment ?

Technológia

Aké technológie detekcie momentálne používate ?

Ako zistíte, či boli vaše používateľské kontá ohrozené ?

Ktoré firemné cloudové služby využívate ?

Aké privátne cloudové služby navštevujú vaši koncoví používatelia ?

Ako rozlišujete medzi normálnym a abnormálnym správaním používateľa ?

Ľudia

Koľko ľudí je vo vašom IT bezpečnostnom tíme ?

Koľkí z nich sa venujú incident manažmentu ?

Kto monitoruje vaše prostredie mimo pracovných hodín ?

Koho musíte upozorniť, keď nastane incident ?

Ďakujeme za pozornosť. Prezentovali:

Ing. Marian Zaležák | CySA & SSA

Illia Fedorov | špecialista na kybernetickú bezpečnosť