# Silnejší spolu:
## ESET technológie v službách SOC providera

Ján Andraško, CEO

14.4.2026

binary CONFIDENCE

ESET Platinum Partner


The IT Security Festival in Central and Eartern Europe
TTN
CY63R53C:_:R17Y
• 7H3 F3W
• 7H3 9R0:_:D

# Binary Confidence

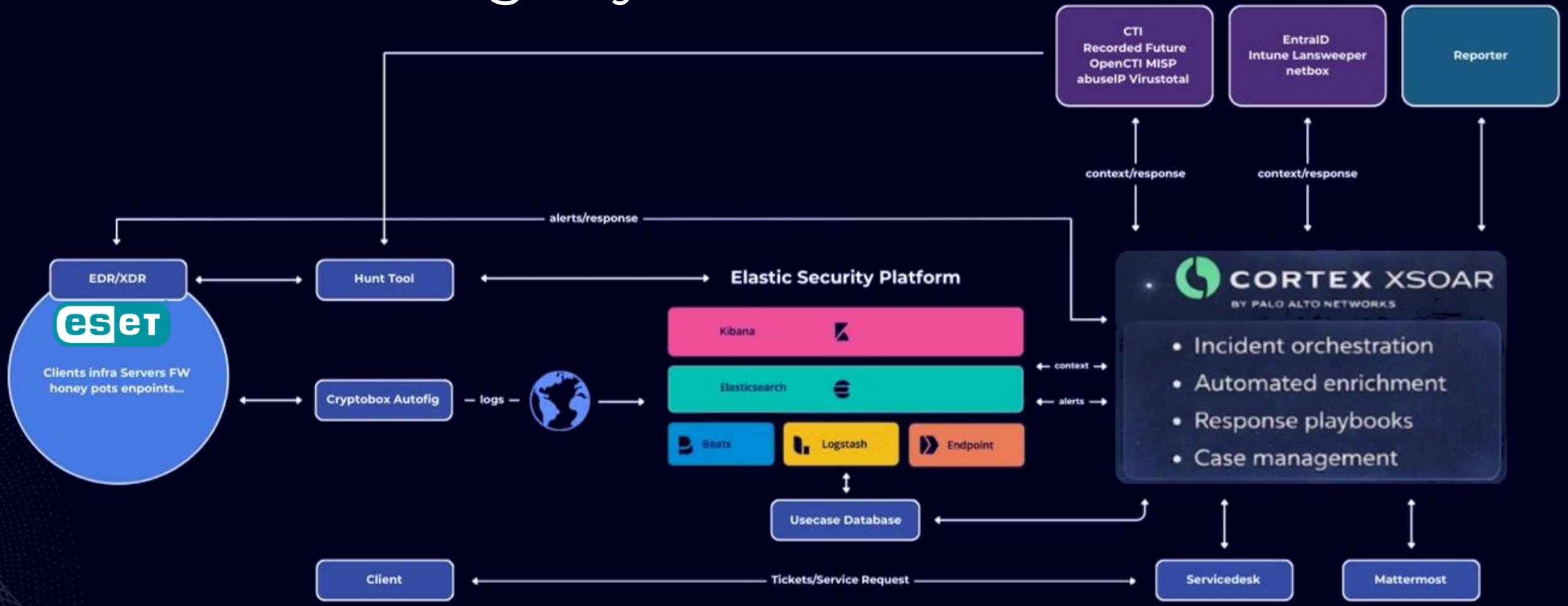
- SOCaaS – Security Operations Centre ako služba
  - Služby detekcie a reakcie 24/7
- Digitálna forenzná analýza
- Implementácia bezpečnostných technológií
  - SIEM, SOAR, EDR, NGFW, ...
- Expertné služby a konzultácie
  - audit, design, NIS, BCM, GDPR, ISO27k, ISAE 3402
- Simulované cvičenia a hry
  - Komerčné aj verejné (Guardians)

ESET® Platinum Partner


JARDIANS
RANGE
INTERNAL
SECURITY


Hello!
TheHive

# Náš technologický stack



# Dashboards

New Incident | Search in Incidents | ?

DASHBOARDS | REPORTS

My Dashboard | My Threat Landscape | XSOAR Automation Insights | System Health | SLA | Troubleshooting Playbooks | Incidents | API Execution Metrics | Cost Optimization Playbooks | Add dashboard

Date Range: Today

Refresh every 10 minutes | last refreshed: 12/04/2026 16:16:14

[redacted] | Add to Saved queries

## Open VS Closed Alerts

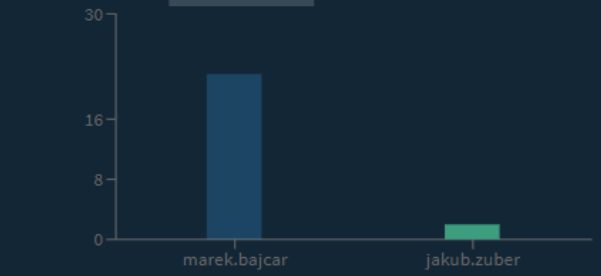
| | |
|---|---|
| Closed | 24 |
| Active | 8 |

## 0

**Unassigned Incidents**

## Incidents Top Close Analysts

marek.bajcar | jakub.zuber




## Actual incidents

marek.bajcar (4)

## Incident Count by Customer

| | |
|---|---|
| [redacted] | 7 |
| [redacted] | 7 |
| [redacted] | 4 |
| [redacted] | 3 |
| [redacted] | 1 |
| [redacted] | 1 |

+1

## Active Incidents Assigned by User

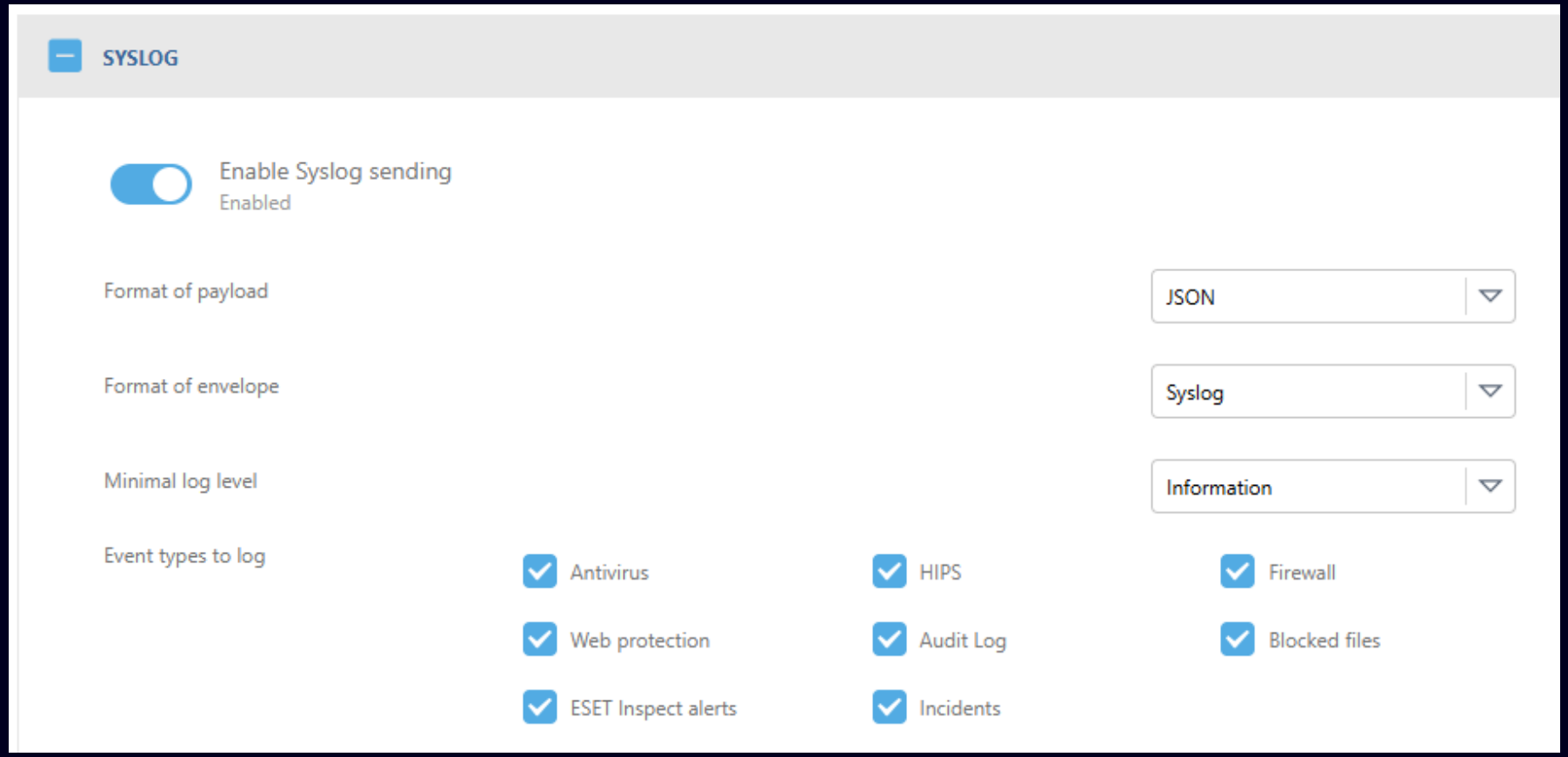
*Showing Top 4 results*

| Name | Owner | WorkStart | Analyst Note |
|---|---|---|---|
| [redacted] | [redacted] | [redacted] | XSOAR |
| [redacted] - Removal of BAT/KillWin.NPD and Win64/Agent.IGY from removable drive on [redacted] | marek.bajcar | 12/04/2026 12:25:49 | |
| [redacted] - PUA Win32/FusionCore Detections and Deletions on [redacted] | marek.bajcar | 12/04/2026 14:14:11 | 2026-04-12T12:38: incident number # XSOAR |
| [redacted] - Chrome download attempt of Win32/Yandex.AE and cached malicious module f_003166 on [redacted] | marek.bajcar | 12/04/2026 15:37:44 | 2026-04-12T14:01: incident number # XSOAR |

## Unassigned Incident

| ID ↓ | Name | Type | Severity | Status | Owner | Roles | Playbook | Occurred | SLA |
|---|---|---|---|---|---|---|---|---|---|

# Fáza 1




2025-01-30T15:09:00.847Z 52779ddf-68b5-48c4-ba85-0e30015bebfc ERAServer 41 - - ï»¿{"event_type" : "Audit_Event","ipv4" : "","ipv6" : "","hostname" : "","source_uuid" : "691883d2-015f-4413-abc0-318c39e512a3","os_name" : "","occured" : "30-Jan-2025 15:08:06","group_name" : "","group_description" : "","severity" : "Information","domain" : "Incidents","action" : "Create","target" : "0c76bd63-3aee-5fc7-84bb-b22f49ec97a6","detail" : "Incident \"Code Injection and Suspicious Executable Dropped on DESKTOP-F3GHDS4\" created","user" : "","result" : "Success"}

# Fáza 1

2025-01-30T15:09:00.847Z 52779ddf-68b5-48c4-ba85-0e30015bebfc ERAServer 41 - - ï»¿{"event_type" : "Audit_Event","ipv4" : "","ipv6" : "","hostname" : "","source_uuid" : "691883d2-015f-4413-abc0-318c39e512a3","os_name" : "","occured" : "30-Jan-2025 15:08:06","group_name" : "","group_description" : "","severity" : "Information","domain" : "Incidents","action" : "Create","target" : "0c76bd63-3aee-5fc7-84bb-b22f49ec97a6","detail" : "Incident \"Code Injection and Suspicious Executable Dropped on DESKTOP-F3GHDS4\" created","user" : "","result" : "Success"}

---

eset.incident.name: "Code Injection and Suspicious Executable Dropped on DESKTOP-F3GHDS4" AND domain: "Incidents" AND event.action : "Add"

---

incident: {"object": {"name": "services.exe", "type": "Process"}}

incident: {"object": {"name": "deploymentservice.exe", "type": "Process"}}

incident: {"object": {"name": "Rule - Injection from an unpopular process [F0415]", "type": "Detection"}}

incident: {"object": {"name": "Rule - Suspicious executable with .exe extension was dropped [B0304]", "type": "Detection"}}

incident: {"object": {"name": "DESKTOP-F3GHDS4", "type": "Computer"}}

incident: {"object": {"name": "deploymentservice.exe", "type": "Executable"}}

# Fáza 1

incident: {"object": {"name": "DESKTOP-F3GHDS4", "type": "Computer"}}

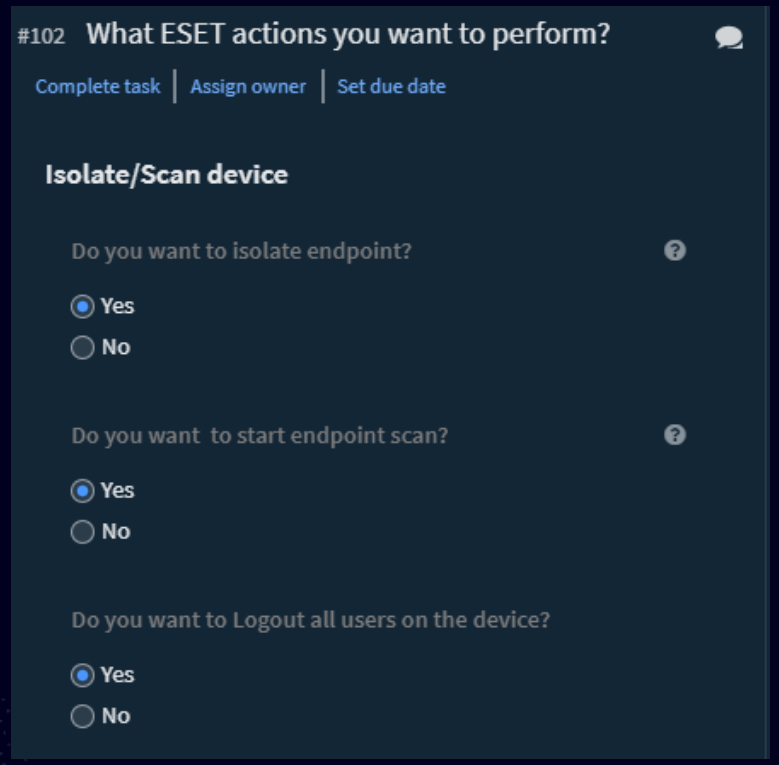
---

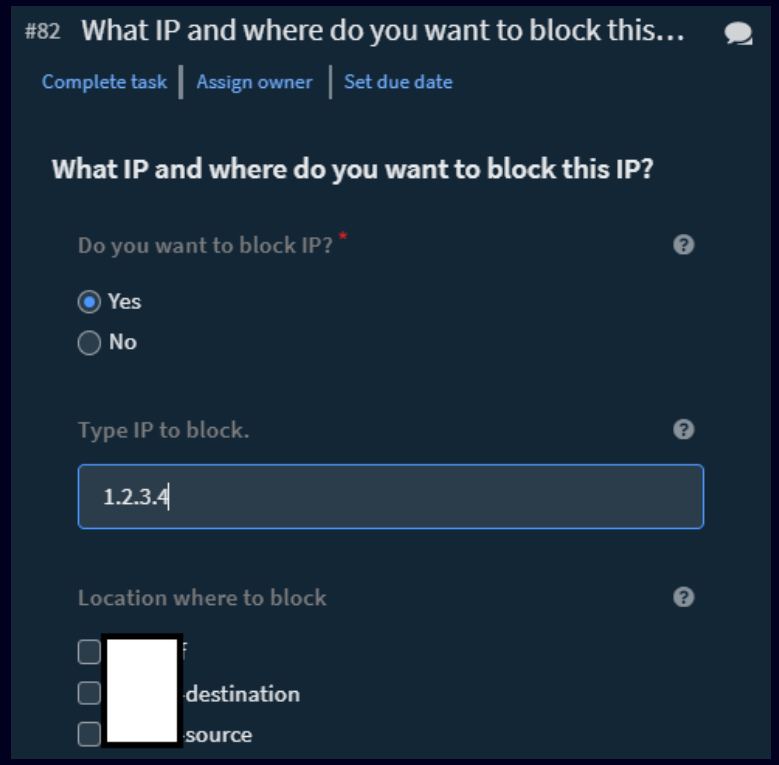
NOT eset.event_type: "Audit_Event" AND NOT eset.event_type: "Information_Event"
AND host.hostname : DESKTOP-F3GHDS4

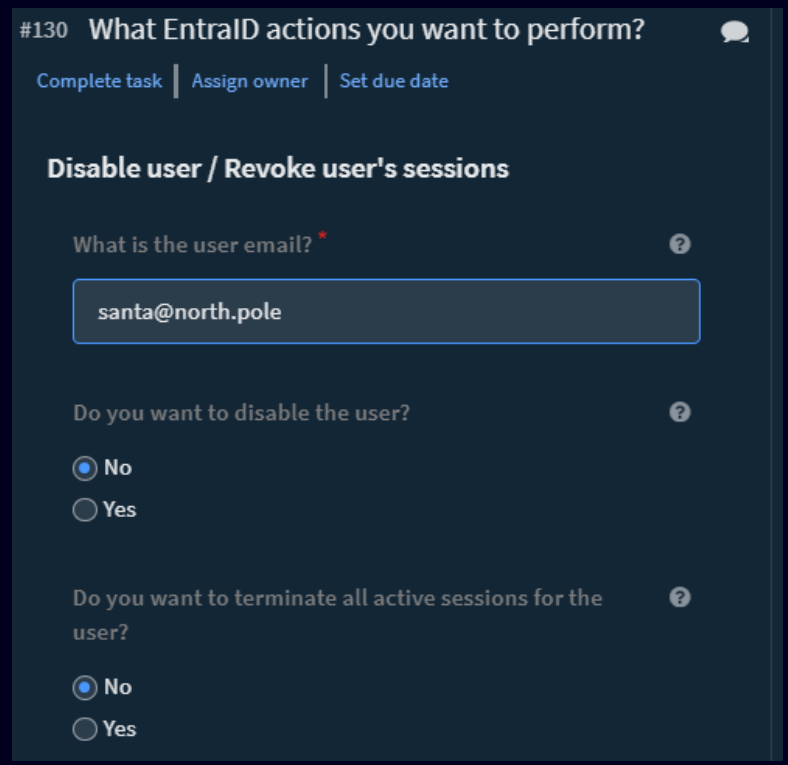
---

ip: 172.16.2.5 | id: a24ad982-c9a1-45ac-8d0d-[redacted]<br>hostname: DESKTOP-F3GHDS4 | executable: d:\deploymentservice\deploymentservice.exe | domain: AD<br>name: deploymentservic | trigger_event: %SYSTEM%\tssdis.exe (APC queue)<br>object_uri: - | name: Injection from an unpopular process [F0415] |

ip: 172.16.2.5 | id: a24ad982-c9a1-45ac-8d0d-[redacted]<br>hostname: DESKTOP-F3GHDS4 | executable: d:\deploymentservice\deploymentservice.exe | domain: AD<br>name: deploymentservic | trigger_event: d:\deploymentservic\deployment\actual\rdpextension.exe<br>object_uri: - | name: Suspicious executable with .exe extension was dropped [B0304] |


#102 What ESET actions you want to perform?
Complete task
Assign owner
Set due date
Isolate/Scan device
Do you want to isolate endpoint?
Yes
No
Do you want to start endpoint scan?
Yes
No
Do you want to Logout all users on the device?
Yes
No


#82 What IP and where do you want to block this...
Complete task
Assign owner
Set due date
What IP and where do you want to block this IP?
Do you want to block IP? *
Yes
No
Type IP to block.
1.2.3.4
Location where to block
destination
source


#130 What EntraID actions you want to perform?
Complete task
Assign owner
Set due date
Disable user / Revoke user's sessions
What is the user email? *
santa@north.pole
Do you want to disable the user?
No
Yes
Do you want to terminate all active sessions for the user?
No
Yes

## Default section

| | |
|---|---|
| User | |
| User Domain | |
| Host Name | |
| SIEM Alert Original Ti... | |
| SIEM Rule Name | |
| SIEM Alert Reason | |
| SIEM Alert URL | |
| SIEM Event Action | |
| SIEM Rule Category | |
| SIEM Rule Description | |
| SIEM Rule tags | |
| Kibana Alert Ancestor... | |
| Kibana Alert Ancestor... | |
| Kibana Signal Index | |
| Kibana Space | |
| Tags | eset incident |

## LDAP section

| | |
|---|---|
| LDAP sAMAccountN | |
| LDAP Title | |
| LDAP Department | |
| LDAP Company | |
| LDAP Manager | |
| LDAP Mail | |
| LDAP Member Of | |

## Lansweeper section

Enrich IP from Lansweeper

## EntraID section

| | |
|---|---|
| User City | Bratislava 5 |
| User Company Name | |
| User Creation Time | |
| User Department | |
| User Job Title | |
| User Last Password C... | |
| User Mail Nickname | |
| User Mobile Phone | |
| Office Location | |
| User Principal Name | |
| Mail Proxy Address | |

## InTune section

| | |
|---|---|
| O365 Device Name | |
| O365 Device Complia... | compliant |
| O365 Device Encryption | true |
| O365 Device OS | Windows |
| O365 Device OS Version | 10.0.22631.4460 |
| O365 Device Manufact... | Dell Inc. |
| O365 Device Model | XPS 13 9340 |

## ESET section

Eset Info

| ESET Object Type | ESET Object Name |
|---|---|
| Detection | Antivirus - Malware: Eicar |
| Computer | |

ESET Device UUID

## ESET Detections

ESET Detections

| Hostname | ESET Rule Name | ESET Process Executable | ESET Object URI |
|---|---|---|---|
| | Eicar | C:\Program Files\Notepad++\notepad++.exe | file:///C:/Users/ /AppDa 1@2024-12-16_090459.tmp |
| | Eicar | C:\Program Files\Notepad++\notepad++.exe | file:///C:/Users/ /OneDri a.s/Desktop/eicar.txt |

## NetBox section

Enrich IP from Netbox

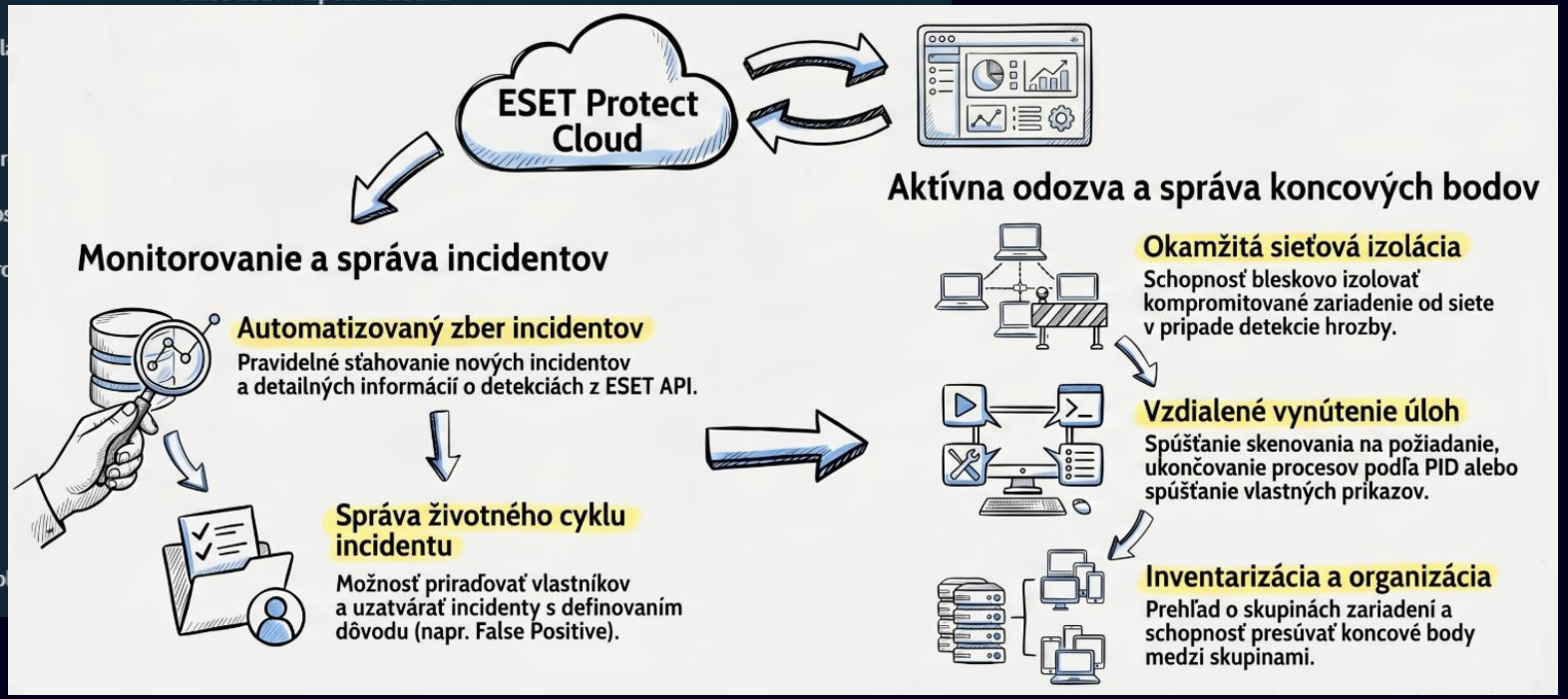
# Fáza 2 (Inspect Incident API)

**Eset-Protect-Cloud-incidents-API**
Custom Integration for ESET Protect Cloud environment.

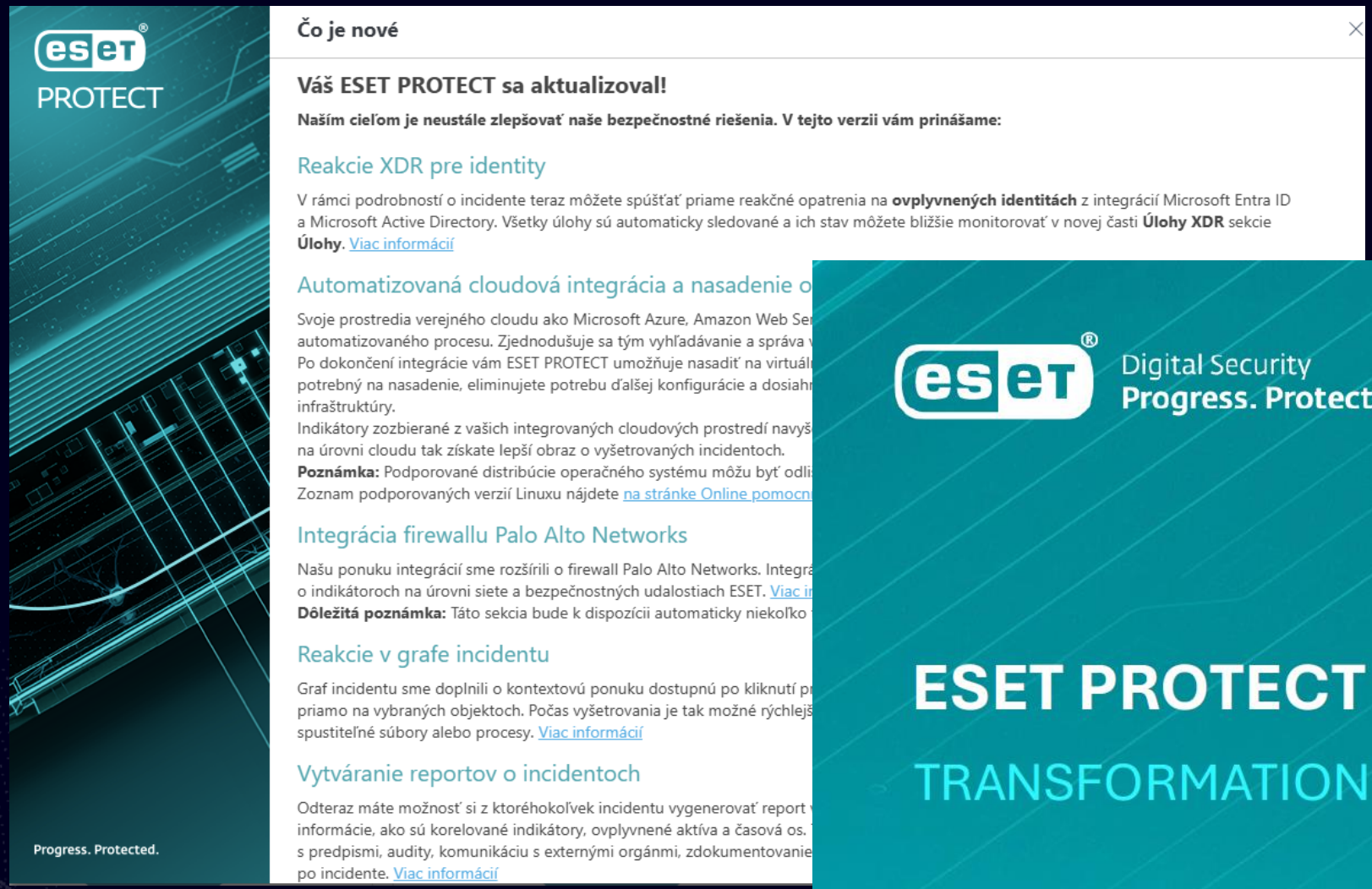
Hide commands

This integration imports events as incidents

| | |
|---|---|
| eset-assign-incident | |
| eset-block-process | Block process on device via ESET agent. |
| eset-close-incident | Close ESET Inspect incident. |
| eset-end-network-isol | |
| eset-get-device | |
| eset-list-detection-per | |
| eset-list-device-groups | |
| eset-list-devices-in-gr | |
| eset-logout-users | |
| eset-move-device | |
| eset-run-command | |
| eset-scan-device | |
| eset-start-network-iso | |



# Fáza 3 (OpenXDR)




# Fáza 3 (vlastný AI asistent)

☆ #1047593 BIC - PowerShell Invoke-Expression and External Connections to aka.ms and we…

Actions | Search in Incidents

Incident Info | Incident Details | AI Summary | Manage customers notes | War Room | Work Plan | Show empty fields

## Evidence & Threat Intel

| Field/Value | Significance | RF Intel |
|---|---|---|
| **whatsapp.root.exe** SHA1: FA0E790D2E787751C1179FEFC47DBF9DD5D92ED1 | Legitimate WhatsApp Desktop from Microsoft Store (WindowsApps path with Store package ID 5319275a) | No RF hits |
| **pwsh.exe** SHA1: 663586E86C615C53C4871AA27E0B9B16E008A2D9 | PowerShell 7 from %PROGRAMFILES%\powershell\7\ — standard install path | No RF hits |
| **pwsh.exe cmdline** | VS Code shell integration script using Invoke-Expression — expected behavior for VS Code terminal | N/A |
| **web.whatsapp.com** | Legitimate WhatsApp web domain | Score: **20/100** — benign (Intel Card) |
| **aka.ms** | Microsoft URL shortener / redirect service | Score: **24/100** — benign (Intel Card) |
| **Host: bic-sk-l069** | Windows 11 Pro, IP: **192.168.11.246**, Public IP: **46.229.238.250** | N/A |
| **msedgewebview2.exe** SHA1: 111FB1359D39C3FB568A8066BA47523895A10DD1 | Edge WebView2 v146.0.3856.97 — used by WhatsApp Desktop for rendering | No RF hits |
| **svchost.exe** SHA1: 1E12A6ECEA737511B246DDBC41E62620FEDD56DC | System service (NetworkService context) handling DNS for WhatsApp | No RF hits |

## Verdict: True Positive - Benign

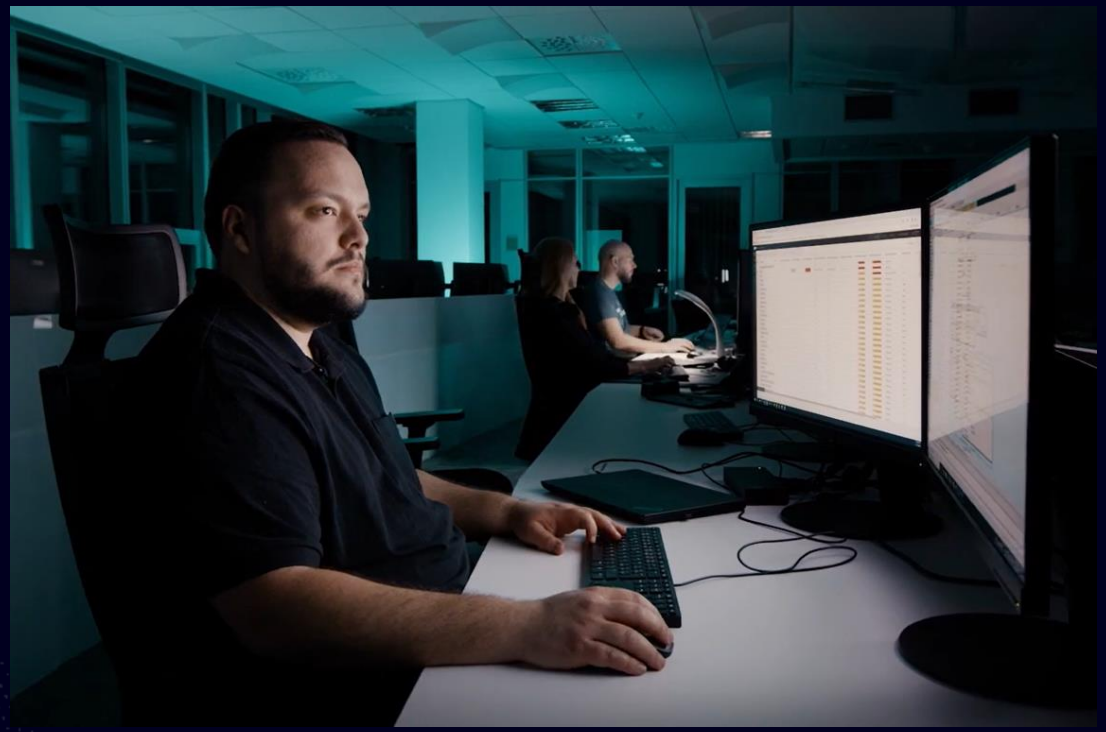
- **Priority:** Standard
- **Confidence:** 97%
- **Reasoning:** All detections trace back to two benign activities: **(1)** WhatsApp Desktop (legitimate Microsoft Store applicatic
  PowerShell 7 with its standard shell integration script (which uses Invoke-Expression), making expected external connect
  processes, no code execution outside expected paths, no persistence, no lateral movement. This is standard developer/u

## Exception/Rule Proposal

- **Reason:** The WhatsApp URL detection rules ("Testing whatsapp URL", "Testing whatsapp URL (1)", "Testing whatsapp URL
  WhatsApp Desktop user. The VS Code + PowerShell Invoke-Expression alert is a known benign pattern for VS Code termin

**WhatsApp rules** — recommend disabling or tuning the custom ESET Inspect rules named "Testing whatsapp URL*" and "Access t
intelligence.

# MDR vs SOC



# Ďakujem za pozornosť.

**Ján Andraško**

www.binaryconfidence.com
jan.andrasko@binconf.com


GUARDIANS
powered by
binary
CONFIDENCE
AFTERMOVIE
SLOVENSKA
TandemTrace
CLICO
HudsonRock
eset
NEXTECH