SECURITY DAYS

ESET MDR

14. apríl 2026 / hotel NH Bratislava Gate One

Cybersecurity Progress. Protected. & SME KONFERENCIE

Gabriel BALLA

Product manager

gabriel.balla@eset.com

SECURITY DAYS

Kyberbezpečnostná služba MDR – dnes už AV nestačí

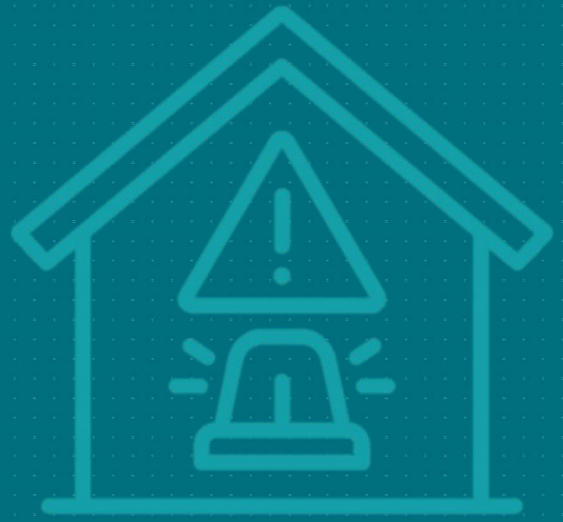
14. apríl 2026 / hotel NH Bratislava Gate One

Cybersecurity Progress. Protected. & SME KONFERENCIE

AV? MDR?

- Ak sa objaví správa o útoku, tak sa spomína zvyčajne:
  - Útočníka si dlho nevšimli
  - Nebol zabezpečený nepretržitý monitoring
  - Sofistikovaný útok nebol odhalený
- MDR ako poistenie – niekedy sa kupuje už neskoro
- Podľa globálnych dát sú firmy pod 1 000 zariadení (SMB) pod väčšou „paľbou“ ako veľké podniky
- Načo je mám potom antivirus?

AV? MDR?



ANTIVIRUS

SECURITY DAYS

AV? MDR?

SECURITY DAYS

AV? MDR?

SECURITY DAYS

Prostredie MDR

SILA ESET PROTECT & Inspect

Hĺbková viditeľnosť hrozieb a útokov: **aké, kde** a **ako?**

+

Vedomosti **ESET expertov**

ESET má **špičkových** bezpečnostných výskumníkov monitorujúcich hrozby **24/7**

=

ESET MDR

Najvyššie hodnotená spravovaná bezpečnostná služba pre **vašu ochranu**

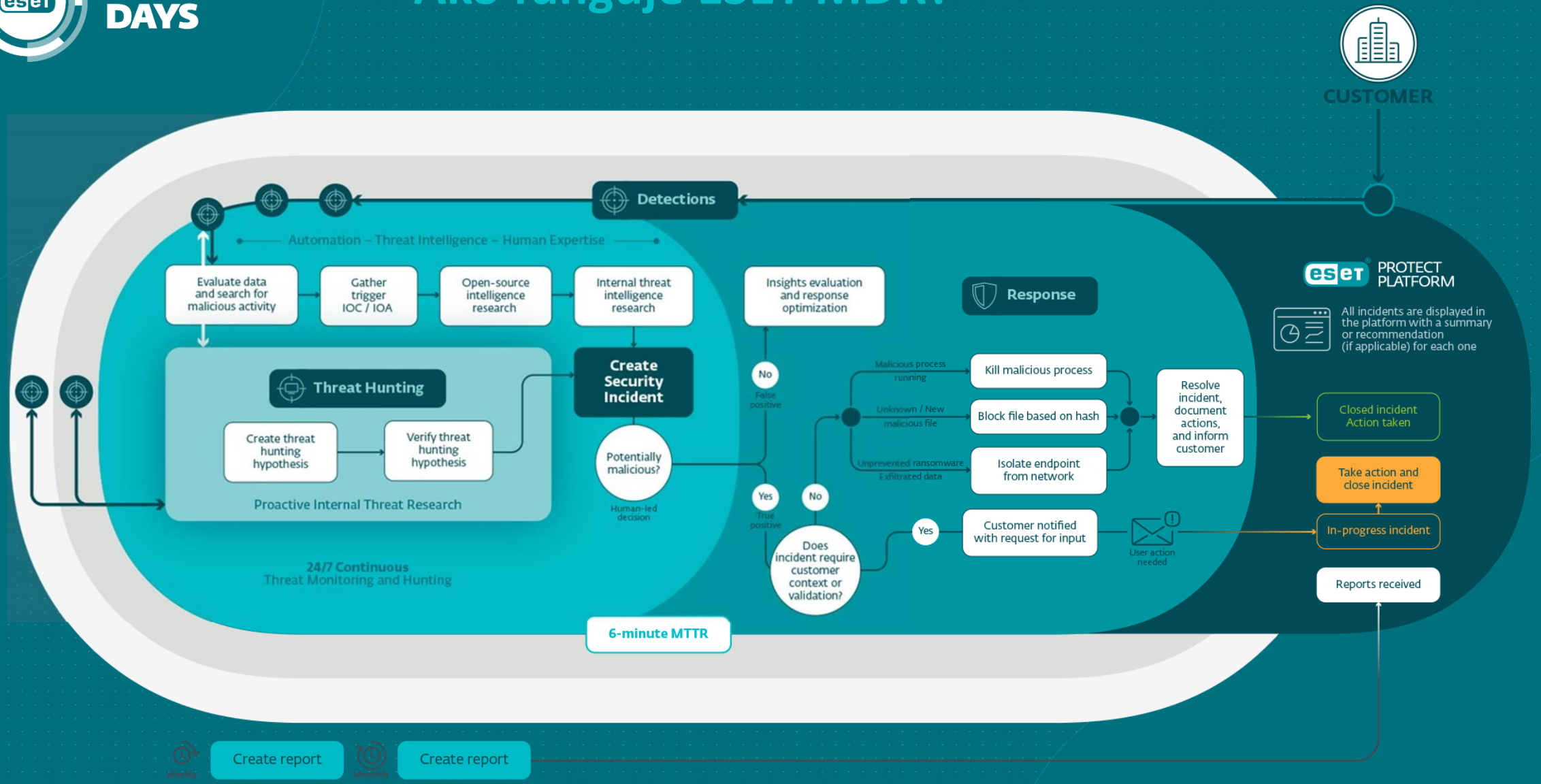
Čo je bežné očakávanie zákazníkov?

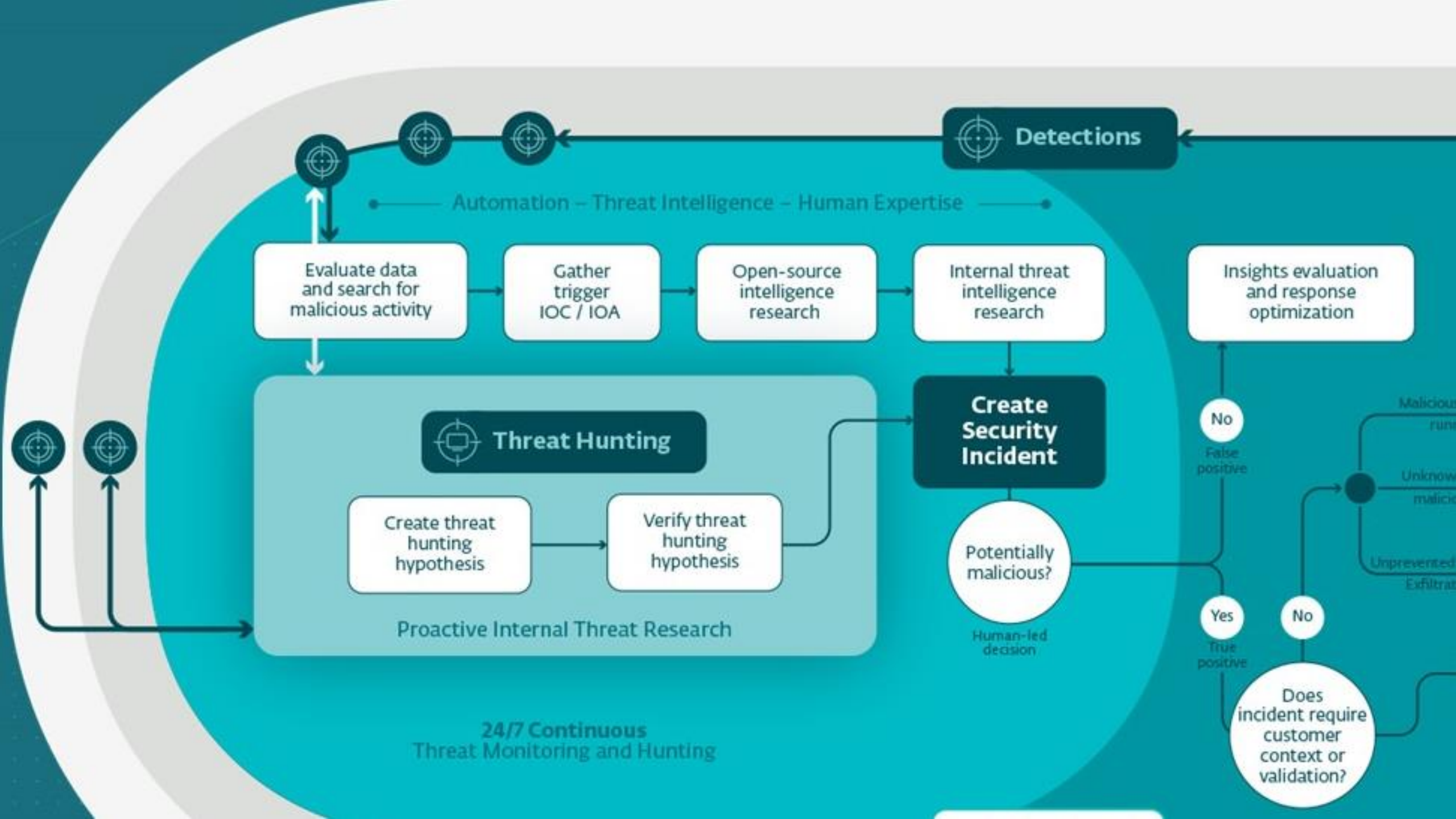
- SOC výstupy bez SOC-u
- Riešenie, ktoré zastaví útoky na moju firmu
- Je dostupná 24/7/365
- Informuje ma o útokoch a poradí mi, ako sa tomu vyhnúť v budúcnosti
- Poskytne mi prehľad, čo sa dodáva cez službu
- Poskytne mi sumáre, reporty - hlásenia, ktoré viem použiť pre manažment
- Poskytne mi rýchlu pomoc, ak nastane incident alebo ak budem mať otázky ohľadne incidentu

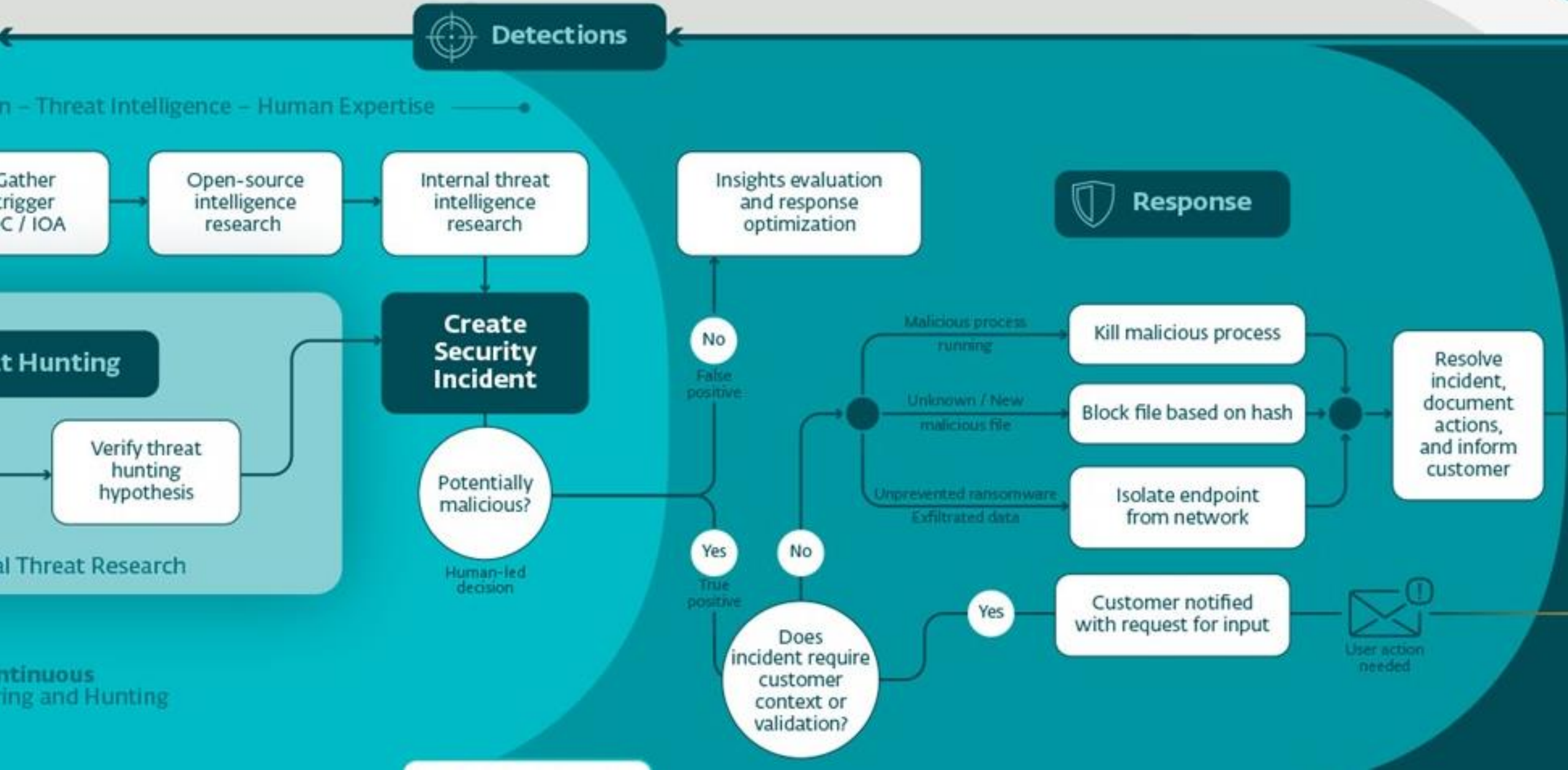
Celosvetové výzvy SOC tímov

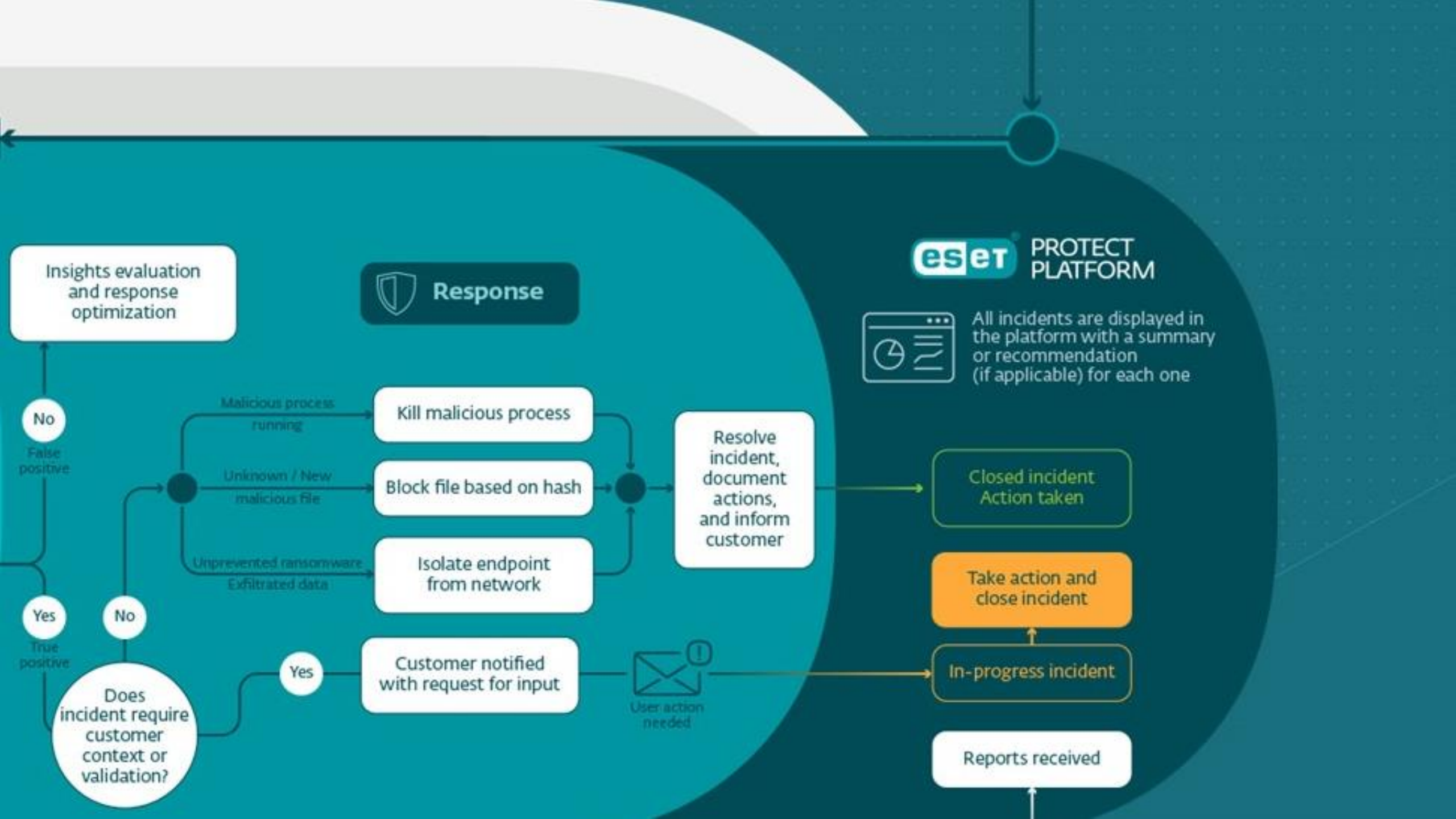
- Stále sa meniace prostredie
- Neustála potreba vzdelávania
- Drahé nástroje (napr. SIEM a SOAR)
- Málo bezpečnostných expertov a vysoký dopyt zo strany firiem
- Lojalita – lovci talentov a náborári
- Príliš veľa dát, hlásení a alarmov
- Vyhorenie

Ako funguje ESET MDR?

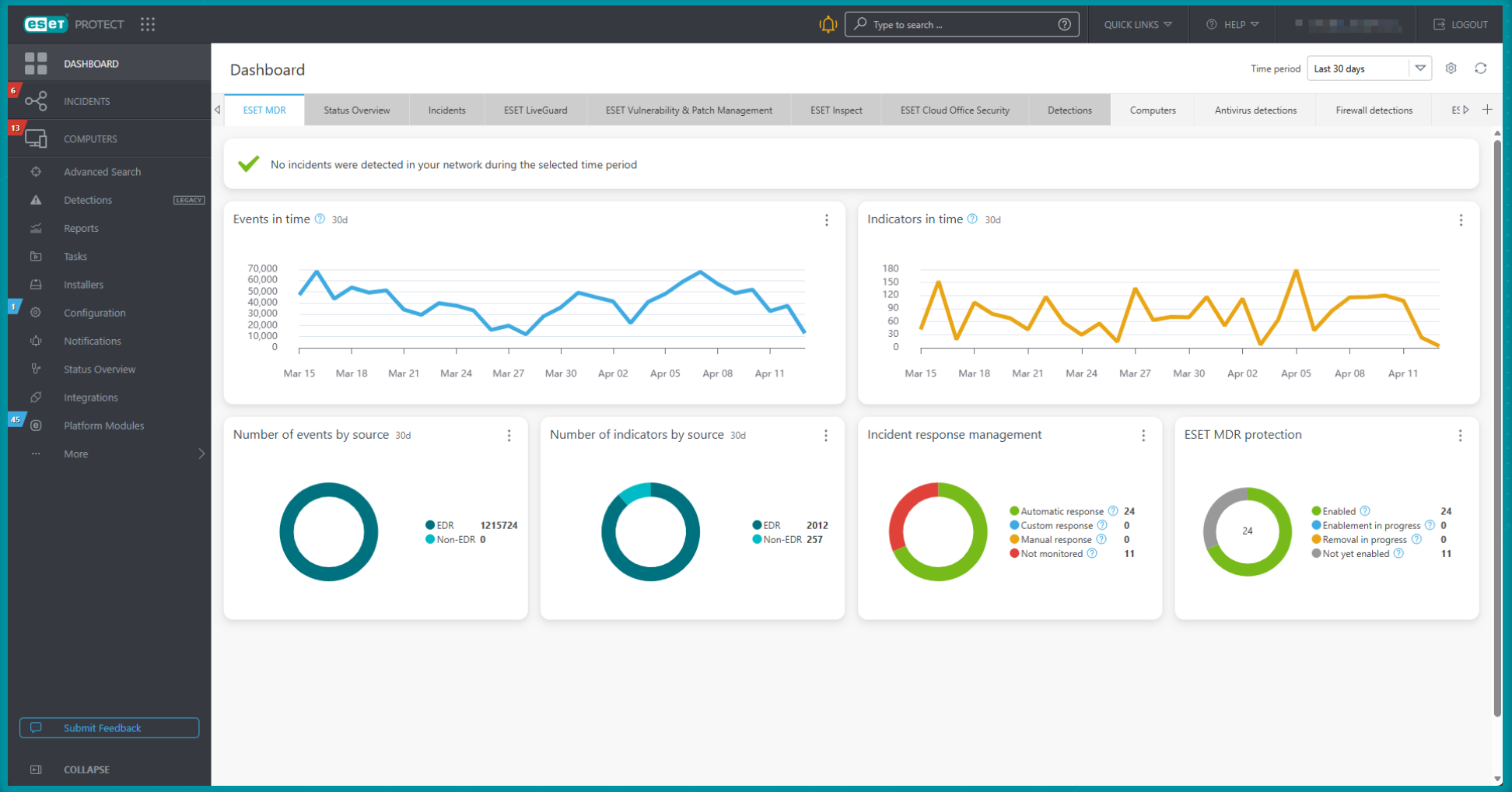



Detections
Automation – Threat Intelligence – Human Expertise
Evaluate data and search for malicious activity
Gather trigger IOC / IOA
Open-source intelligence research
Internal threat intelligence research
Insights evaluation and response optimization
Threat Hunting
Create threat hunting hypothesis
Verify threat hunting hypothesis
Proactive Internal Threat Research
Create Security Incident
Potentially malicious?
Human-led decision
No
False positive
Yes
True positive
No
Does incident require customer context or validation?
24/7 Continuous
Threat Monitoring and Hunting

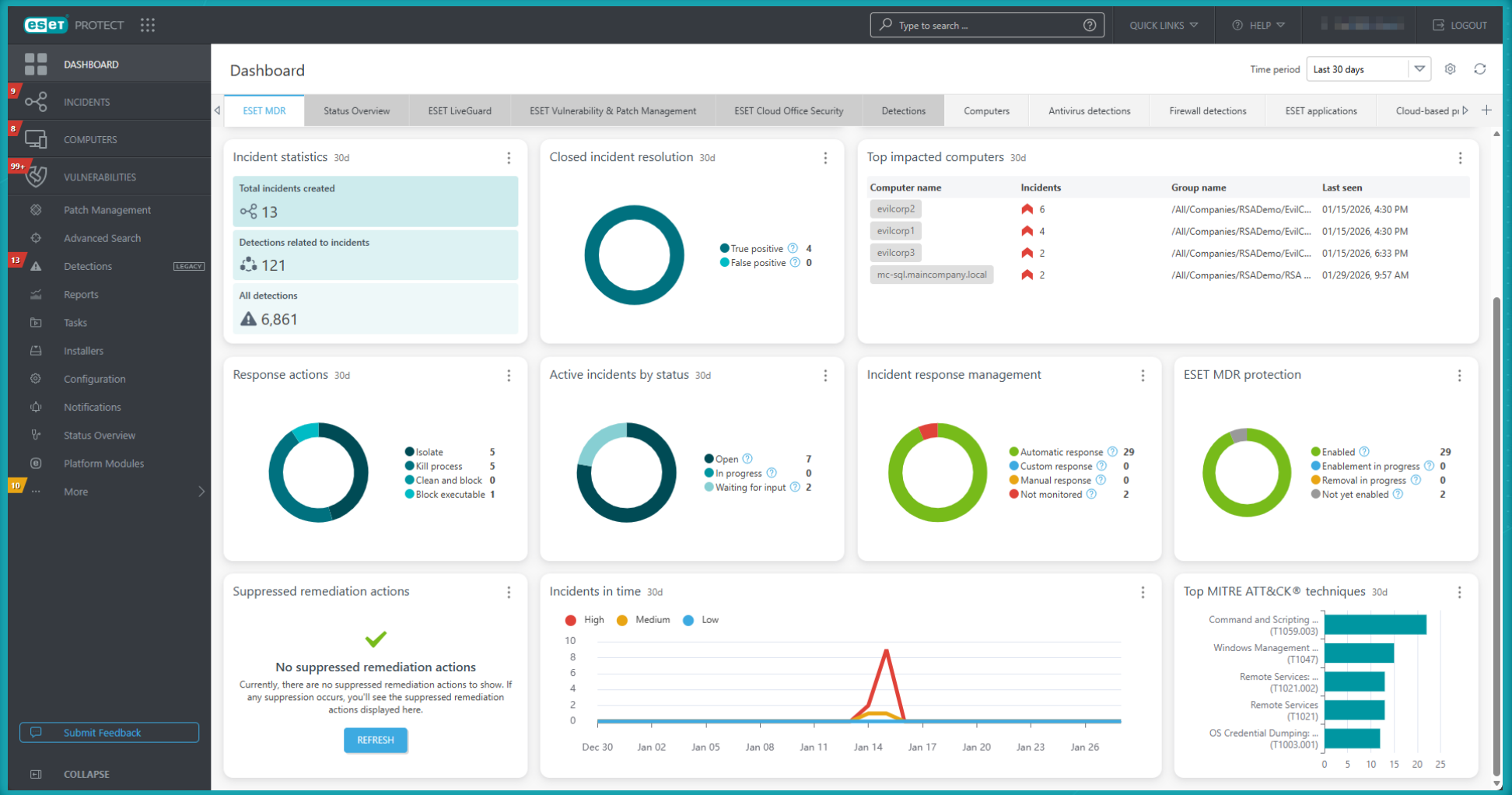

Detections
n – Threat Intelligence – Human Expertise
Gather
rigger
C / IOA
Open-source intelligence research
Internal threat intelligence research
t Hunting
Verify threat hunting hypothesis
al Threat Research
Create Security Incident
Potentially malicious?
Human-led decision
ntinuous
ing and Hunting
Insights evaluation and response optimization
No
False positive
Yes
True positive
No
Does incident require customer context or validation?
Yes
Customer notified with request for input
User action needed
Response
Malicious process running
Kill malicious process
Unknown / New malicious file
Block file based on hash
Unprevented ransomware Exfiltrated data
Isolate endpoint from network
Resolve incident, document actions, and inform customer


Insights evaluation and response optimization
Response
ESET PROTECT PLATFORM
All incidents are displayed in the platform with a summary or recommendation (if applicable) for each one
No
False positive
Malicious process running
Kill malicious process
Unknown / New malicious file
Block file based on hash
Unprevented ransomware
Exfiltrated data
Isolate endpoint from network
Resolve incident, document actions, and inform customer
Closed incident
Action taken
Take action and close incident
Yes
True positive
No
Does incident require customer context or validation?
Yes
Customer notified with request for input
User action needed
In-progress incident
Reports received

Prostredie MDR bez incidentov



Prostredie MDR s incidentom



SECURITY DAYS

Reporting

ESET MDR Weekly Report

Weekly report: September 02, 2024 - September 08, 2024
Created: September 09, 2024; 09:09:13; UTC+1:00

ESET MDR

Incident overview

All incidents from all sources according to severity

2	2	0	0
All incidents	High ↑ increase	Medium without change	Low without change

Incidents according to status

Key insight into the progression of incidents within the incident cycle

Resolved 2 ↑

Resolved - Incidents where an issue was identified and addressed by ESET MDR

Incident pipeline

An overview of all detections, total incidents, and incidents resulting from detections, providing insight into service efficiency

	All detections	Detections related to incidents	Created incidents
September 2	2	0	0
September 3	7	0	0
September 4	36	5	2
September 5	5	0	0
September 6	2	0	0
September 7	0	0	0

Čo je bežné očakávanie zákazníkov?

- ✓ SOC výstupy bez SOC-u
- ✓ Riešenie, ktoré zastaví útoky na moju firmu
- ✓ Je dostupná 24/7/365
- ✓ Informuje ma o útokoch a poradí mi, ako sa tomu vyhnúť v budúcnosti
- ✓ Poskytne mi prehľad, čo sa dodáva cez službu
- ✓ Poskytne mi sumáre, reporty - hlásenia, ktoré viem použiť pre manažment
- ✓ Poskytne mi rýchlu pomoc, ak nastane incident alebo ak budem mať otázky ohľadne incidentu

Budúce kroky – roadmapa pre ESET MDR

Zjednodušená cesta aktivácie a nainštalovanie služby

Manažovanie integrácii – identita, firewall, CWP, e-mail a NDR

Incident response – hĺbková analýza, komplexný, post-mortem reporting


eset
SECURITY
DAYS