APS IT diensten

Voor ICT in het belang van je school

MDR VANUIT DE EU; DE GARANTIE VOOR EEN VEILIGE LEERWEG

Professionaliseringsdag 9 april 2026

- Michael van der Vaart
  - Chief Experience Officer
- Peter Tolboom
  - Partner succes manager

ESET Cybersecurity
Progress. Protected.

APS IT diensten

AL MEER DAN 15 JAAR EEN PARTNERSHIP

APS IT diensten
Voor ICT in het belang van je school

APS IT diensten
Voor ICT in het belang van je school

Wie is ESET?

Global cybersecurity prevention leader

Owned by original founders

Growing YoY for 30+ years

1 billion+ protected internet users

500.000+ business customers

13

Global R&D centers

850

Cybersecurity researchers & Technology experts

750,000

Brand-new & unique suspicious samples received every day

24/7

MDR Service

6 minutes

Mean Time to Respond of ESET MDR

APS IT diensten
Voor ICT in het belang van je school

Gebouwd op vertrouwen, vanuit de EU

Biggest B2B security provider in EU

Owned by original founders

Growing YoY for 30+ years

1 billion+ protected internet users

500.000+ business customers

13

Global R&D centers

850

Cybersecurity researchers & Technology experts

750,000

Brand-new & unique suspicious samples received every day

24/7

MDR Service

6 minutes

Mean Time to Respond of ESET MDR

APS IT diensten

Voor ICT in het belang van je school

De educatie sector vs. Normenkader IBP

- Samen op weg naar een hogere cyberweerbaarheid voor 2030

op de weg naar digitale veiligheid.

APS IT diensten
Voor ICT in het belang van je school

Vijf belangrijke dreigingen om te herkennen en erkennen

- DDoS-aanvallen
- Afhankelijkheid van Leveranciers
- Infostealers
- Phishing
- Ransomware

School CERT door Kennisnet in samenwerking met SIVON

Dreigingsbeeld Cybersecurity primair en voortgezet onderwijs 2025

Kwetsbaarheden herkennen, veiligheid verhogen

ESET Cybersecurity
Progress. Protected.

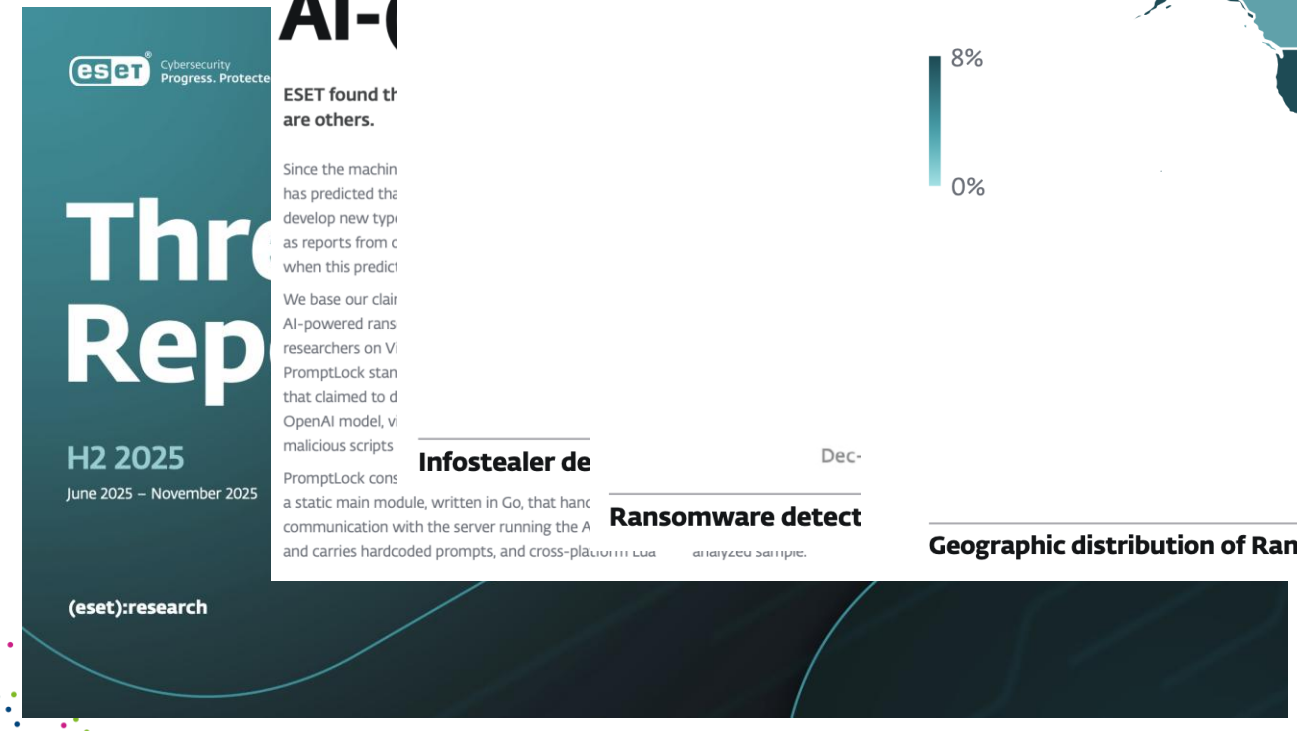
APS IT diensten

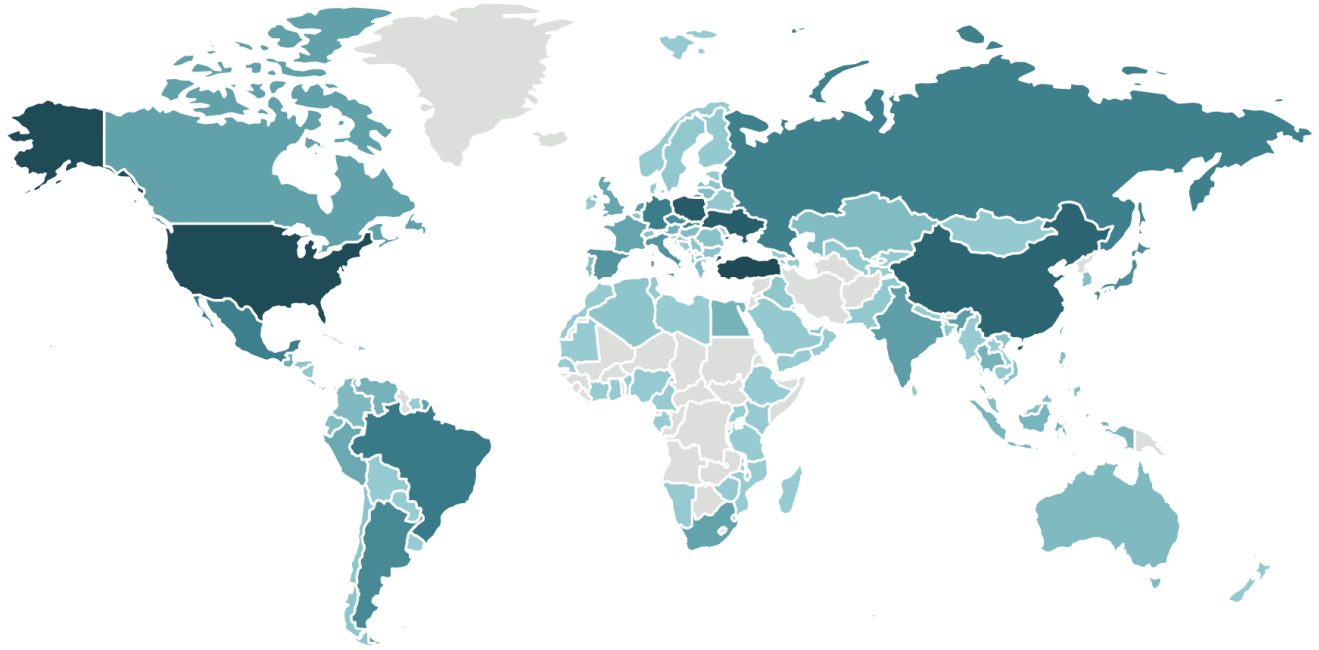
Voor ICT in het belang van je school

ESET's globale inzichten over actuele dreigingen laten dezelfde trends zien

Infostealers

Ransomware





Geographic distribution of Ransomware detections in H2 2025

SECURITY RESEARCH, INNOVATION AND DEEP EXPERTISE

RESEARCH & TECHNOLOGY KEY FACTS

11 RESEARCH AND DEVELOPMENT CENTERS

750,000 NEW AND UNIQUE SUSPICIOUS SAMPLES DAILY

850 TECHNOLOGY EXPERTS

2.5 billion URLS DAILY

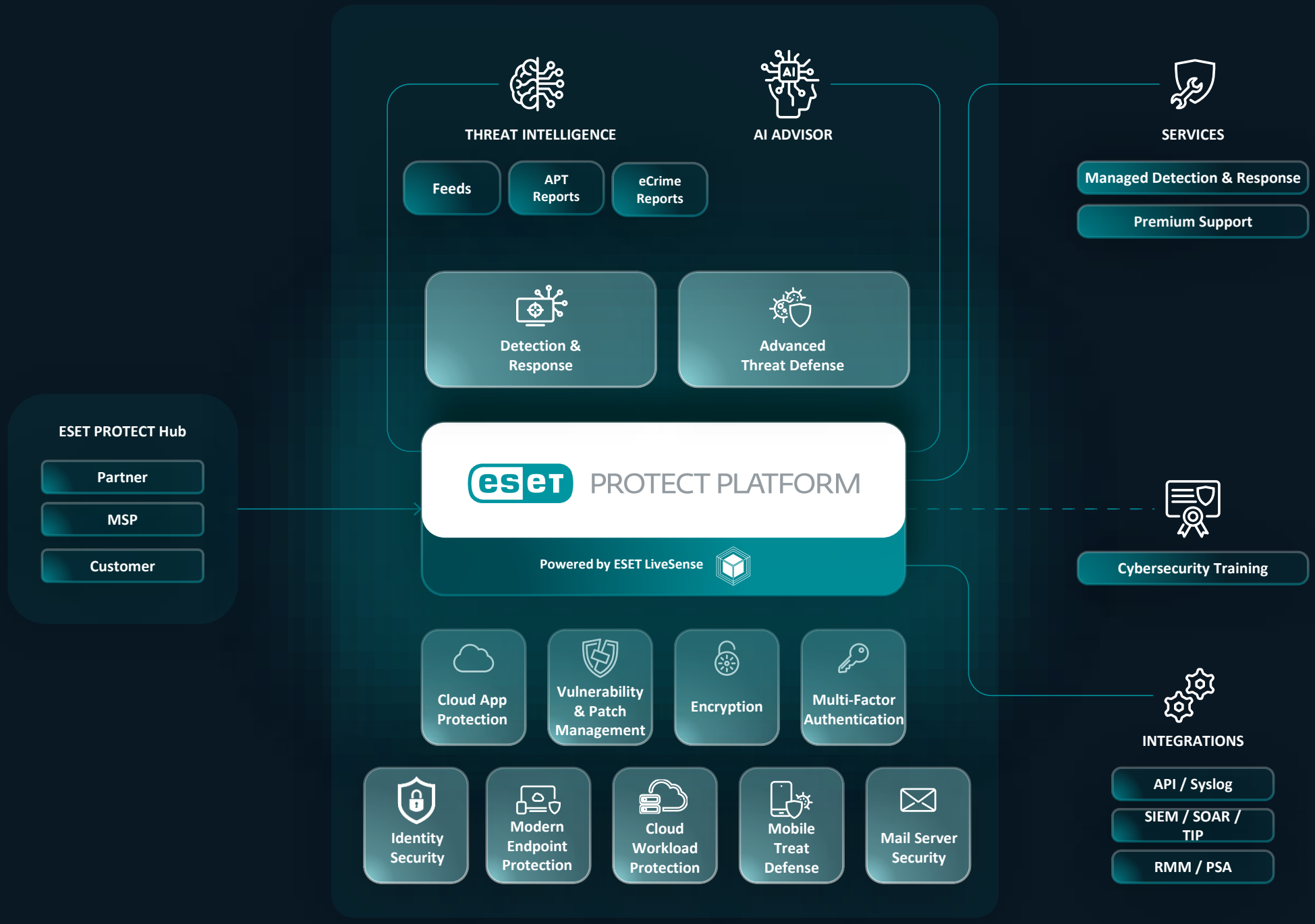
60 million METADATA REDORDS DAILY

SIGNIFICANT CONTRIBUTOR TO

MITRE | ATT&CK®

SINCE 2015, ESET EXPERTS PROUDLY PARTICIPATE IN

LOCKED SHIELDS


THREAT INTELLIGENCE
AI ADVISOR
SERVICES
Feeds
APT Reports
eCrime Reports
Managed Detection & Response
Premium Support
Detection & Response
Advanced Threat Defense
ESET PROTECT Hub
Partner
MSP
Customer
ESET PROTECT PLATFORM
Powered by ESET LiveSense
Cybersecurity Training
Cloud App Protection
Vulnerability & Patch Management
Encryption
Multi-Factor Authentication
INTEGRATIONS
Identity Security
Modern Endpoint Protection
Cloud Workload Protection
Mobile Treat Defense
Mail Server Security
API / Syslog
SIEM / SOAR / TIP
RMM / PSA

CLOUD OFFICE SECURITY

Microsoft 365

Google Workspace

EXCHANGE ONLINE AND GMAIL EMAIL PROTECTION

- ANTISPAM
- ANTI-MALWARE
- ANTI-PHISHING
- CLOUD SANDBOXING
- EMAIL QUARANTINE

TEAMS PROTECTION

- ANTI-MALWARE
- CLOUD SANDBOXING
- TEAM FILES QUARANTINE

ONE DRIVE BUSINESS AND GOOGLE DRIVE PROTECTION

- ANTI-MALWARE
- CLOUD SANDBOXING
- ONEDRIVE FILESQUARANTINE
- ONE NOTE PROTECTION

SHAREPOINT ONLINE PROTECTION

- ANTI-MALWARE
- CLOUD SANDBOXING
- SHAREPOINT FILES QUARANTINE

ESET CLOUD OFFICE SECURITY

In 2025, **on top of native protection** in Microsoft 365 and Google Workspace,
ESET Cloud Office Security detected and blocked threats that other solutions missed.
It provides an extra layer of defense against sophisticated and evasive attacks.

1,300,000

Email threats detected

3,000,000

Phishing emails blocked

200,000,000

Spam emails captured

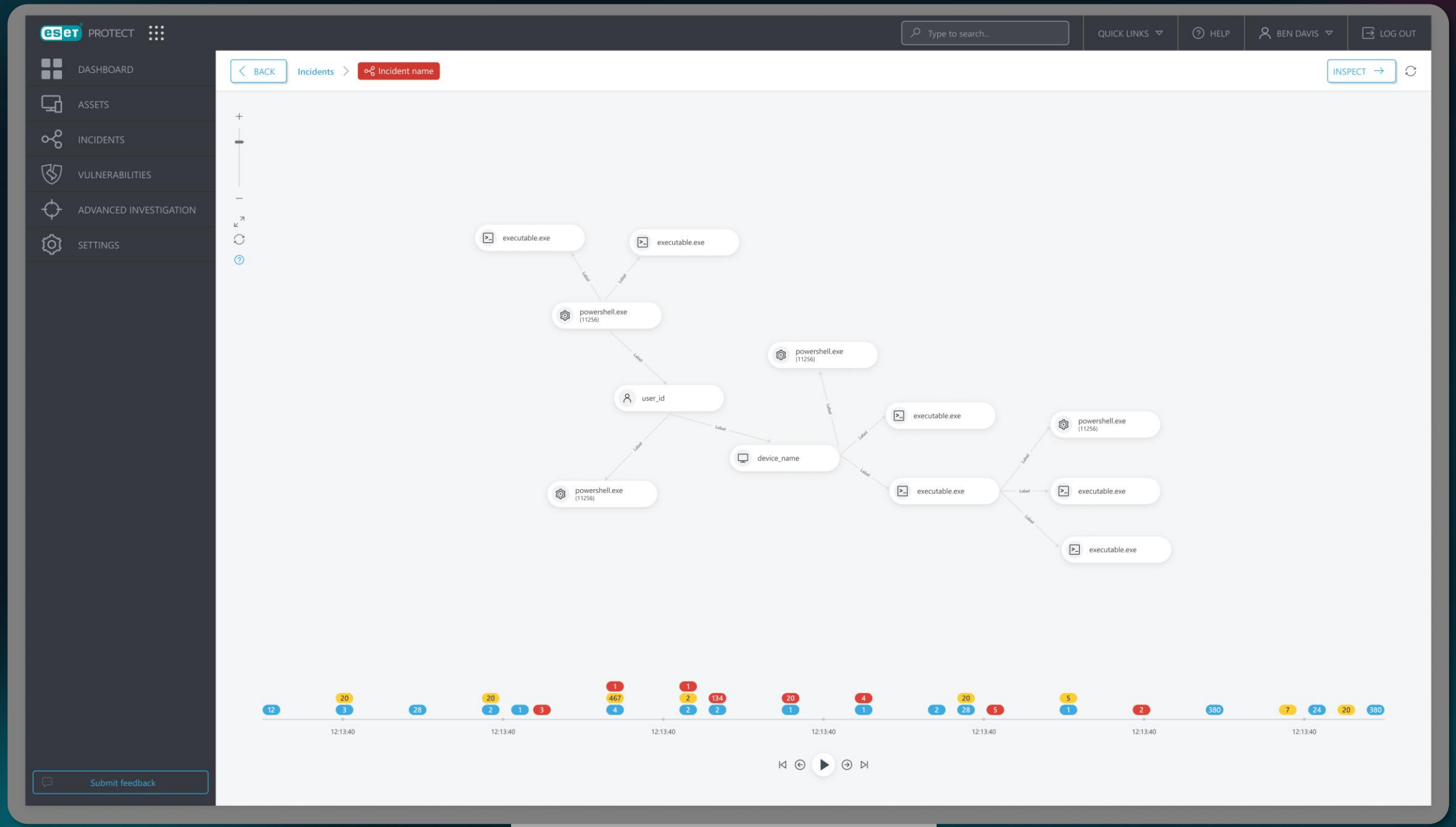
600,000

Non-email threats originated from OneDrive, SharePoint, Teams and Google Drive

APS IT diensten
Voor ICT in het belang van je school

Wat is MDR -> Managed Detection & Response en hoe helpt het onze school?

- Kwetsbaarheden herkennen
- Automatisch patchen
- Infostealers
- Geavanceerde Phishing detectie
- Ransomware beveliging en herstel
- 24/7 Monitoring & Response



Contents

1. Summary 5
2. Timeline 7
10
22
33
41
41
50
65
74
81
89

Cybersecurity
Progress. Protected.

ESET Incident Report

Incident ID - 08976654

Incident created: January 7, 2025
Incident created: January 7, 2025

Timeline

Incident Timeline provides a clear chronological overview of all key events and actions taken during the incident, helping to understand its progression and impact.

14/07/2025 11:48 — Detection: Set File as Hidden [M0304] – HIGH severity

MITRE ATT&CK:

Computer list

List of all affected computers with basic identification and protection status.

Name	Parent group	OS name	Protection status
eset-apollo-wks-1	Workstations – HQ	Windows 11 Pro	Isolated
eset-apollo-wks-1	Workstations – HQ	Windows 11 Pro	Isolated

Incident summary

On 8 April 2025, an attempt to access the corporate server via API was detected. The incident involved the use of compromised login credentials from an external environment. The attacker attempted to execute unknown binaries via PowerShell. ESET PROTECT automatically blocked the executions and isolated 12 devices from the internal network.

High Severity Incident

Incident Name	API Source Test – Unauthorized Access Attempt
Incident ID	INC-2025-000234
Author	Apollo Connect (SOC Analyst)
Status	Open – monitoring in progress
Created time	08/04/2025, 10:14 UTC
Closed time	Pending
Response	Incident detected and isolated within **2** hours. Expected resolution within **24** hours.
Affected hosts & identities	12 Hosts 5 Identities
Tags	Default tag Default tag Default tag

Recommended steps

Below is a summary of the recommended actions to contain the current incident and reduce the risk of similar attacks in the future.

1. **Apply security patches on all affected servers and endpoints**
   a. Verify patch applicability for Windows 10/11 endpoints (KBXXXXXXX).
   b. Patch affected servers with the latest cumulative updates.
   c. Reboot all systems to complete patch installation.
   Benefit: Closes vulnerabilities used in the attack.
   Risk if skipped: Attackers can re-exploit known flaws.

2. **Block all malicious IPs, domains, and hashes identified during this incident**
   a. Block IP ranges 116.83.1.29 and 121.93.44.121 at the network perimeter.
   b. Blacklist all malicious domains in ESET LiveGuard Cloud Reputation (appendix B).
   c. Add malicious file hashes to endpoint blocklists.
   Benefit: Stops C2 traffic and lateral movement.
   Risk if skipped: Attackers may maintain persistence and exfiltrate data.

3. **Reset passwords and invalidate tokens for all compromised accounts**
   a. Force password reset for all accounts flagged in this incident (see Appendix C).
   b. For domain accounts: perform KRBGT account reset twice, waiting 10 hours between resets.
   Benefit: Cuts off adversary access.
   Risk if skipped: Stolen credentials will remain usable.

IN PROGRESS

De Educatie sector verdient MDR, maar het niveau is vaak nog “antivirus”

- Aanvallers gebruiken al lang geen virussen meer
- Aanvallers gedragen zich als beheerders in het netwerk
- Aanvallers gebruiken vaak een gelekt (beheer)account en doen zich voor als “Henk de admin”
- Aanvallers kiezen graag een moment dat er weinig aandacht is voor hun verkenningsessie (Reconnessaince) als “Henk de admin”
- Het gijzelen van het netwerk (Ransomware) is vaak pas de allerlaatste stap
- Wat daaraan vooraf ging is het enige waar je een aanvaller had kunnen onderscheppen
- Sommige aanvallers kiezen niet alleen voor een gijzeling van data die tegen betaling teruggekocht kan worden
- Gevoelige gegevens worden ook gebruikt voor afpersing tegen een datalek

APS IT diensten

Voor ICT in het belang van je school

APS IT diensten

Voor ICT in het belang van je school

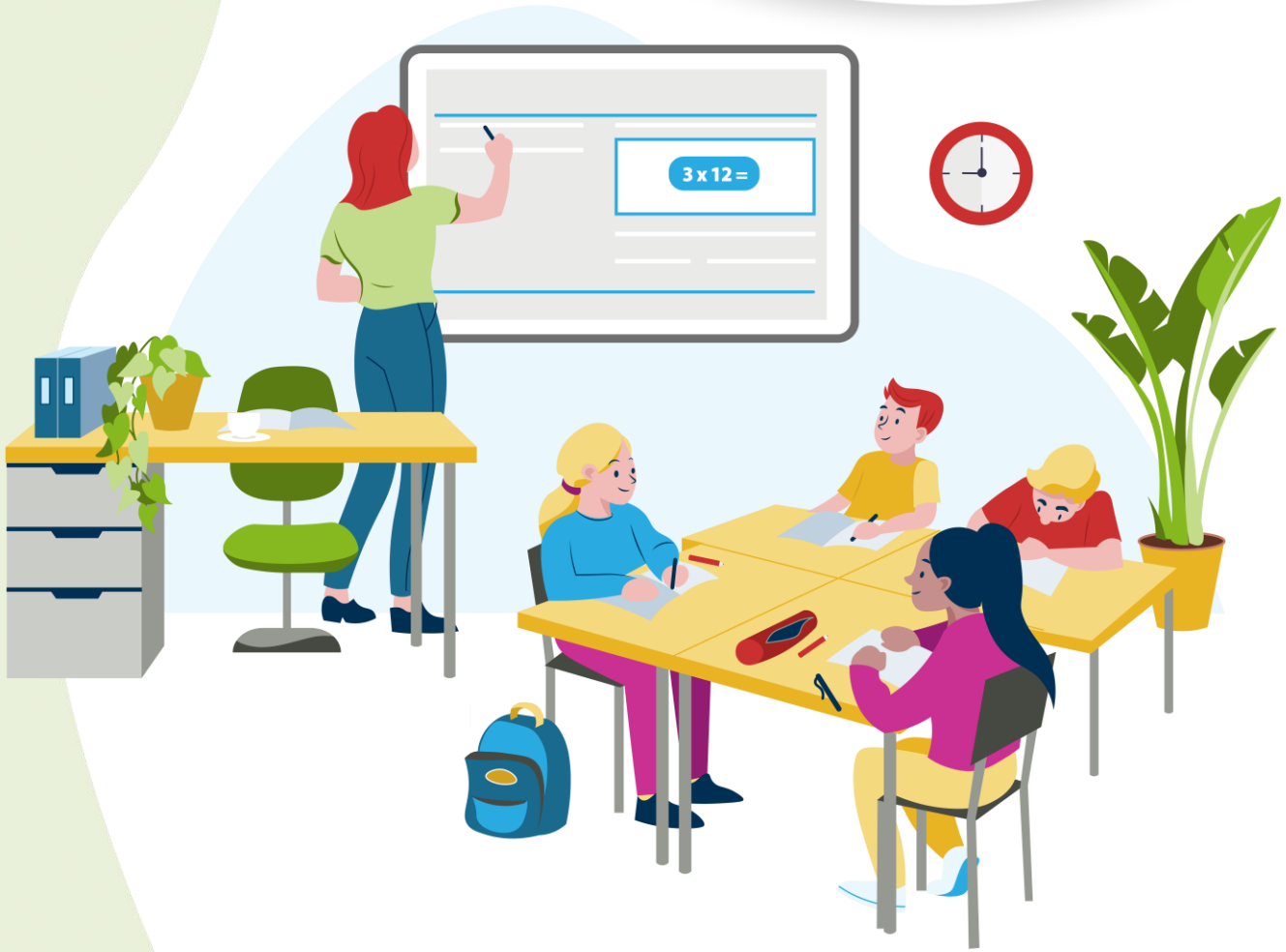
Managed Detection & Response 24/7 – 365 dagen binnen 6 minuten

- Wij zijn wakker
- Wij zijn alert
- Wij acteren zo snel mogelijk in de eerste stappen van de aanval (Reconnessaince)
- Wij hebben de mogelijkheid om ”Henk de admin” zijn account te pauzeren/disablen op alle portalen
- Wij hebben de mogelijkheid om de computers, server of systemen te isoleren van het netwerk
- Wij werken graag samen met partners/klanten in het gezamenlijk optreden tijdens een incident
- Wij werken samen om de omgeving weerbaar te maken met beveiligingsadviezen
- ESET is internationaal betrokken bij het verdedigen van klanten binnen iedere sector (ook defensie)
- ESET levert ook dreigingsinformatie op statelijk niveau voor de verdeging tijdens conflicten

APS IT diensten

Voor ICT in het belang van je school

Q&A
Aske us anything



- Michael van der Vaart
  - Chief Experience Officer
- Peter Tolboom
  - Partner succes manager

APS IT-diensten
Voor ICT in het belang van je school

APS IT-diensten
Zwarte Woud 2
3524 SJ Utrecht

www.apsitdiensten.nl

T 030 2856 870
M info@apsitdiensten.nl