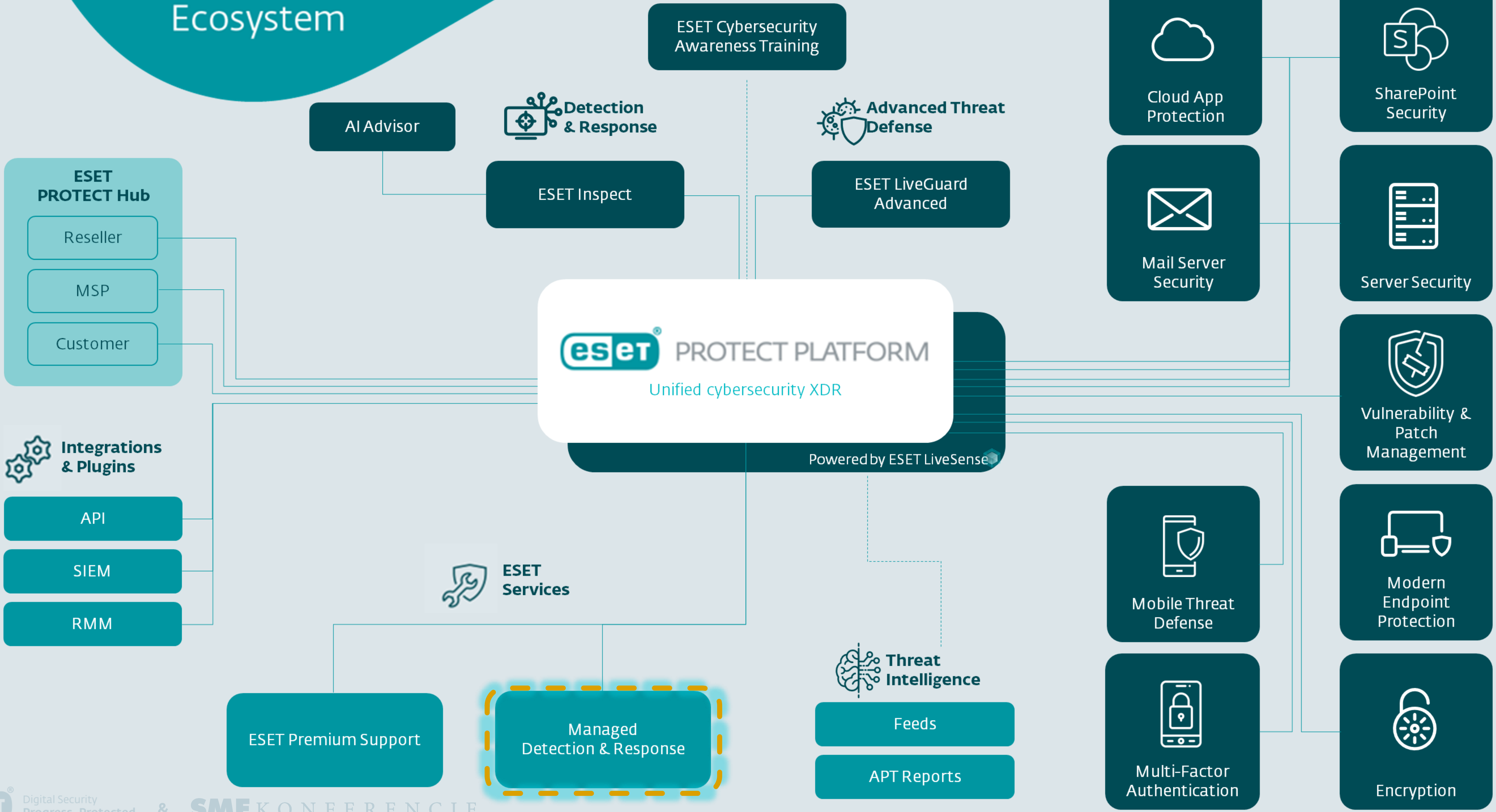
SECURITY DAYS

ESET MDR: TECHNOLÓGIE A STRATÉGIE PRE BEZPEČNÚ BUDÚCNOSŤ

Dušan Kaštan, Core Research and Threat Detection

ESET Digital Security Progress. Protected. & SME KONFERENCIE

ESET PROTECT Ecosystem



ESET Cybersecurity Awareness Training

AI Advisor

Detection & Response

ESET Inspect

Advanced Threat Defense

ESET LiveGuard Advanced

ESET PROTECT Hub

- Reseller
- MSP
- Customer

ESET PROTECT PLATFORM

Unified cybersecurity XDR

Powered by ESET LiveSense

Integrations & Plugins

- API
- SIEM
- RMM

ESET Services

- ESET Premium Support
- Managed Detection & Response

Threat Intelligence

- Feeds
- APT Reports

Cloud App Protection

SharePoint Security

Mail Server Security

Server Security

Vulnerability & Patch Management

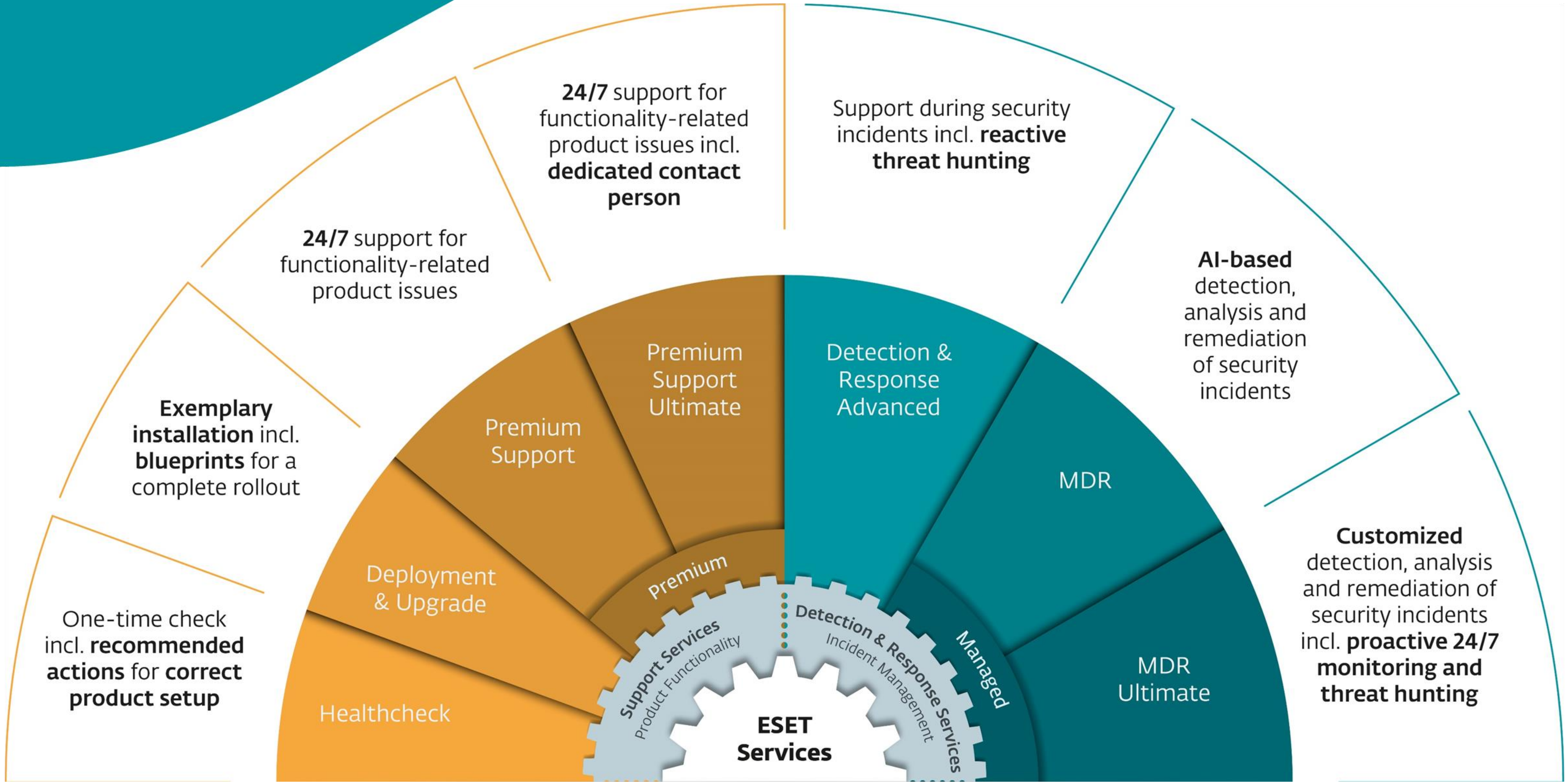
Mobile Threat Defense

Modern Endpoint Protection

Multi-Factor Authentication

Encryption

ESET SERVICES



One-time check incl. **recommended actions** for **correct product setup**

Exemplary installation incl. **blueprints** for a complete rollout

24/7 support for functionality-related product issues

24/7 support for functionality-related product issues incl. **dedicated contact person**

Support during security incidents incl. **reactive threat hunting**

AI-based detection, analysis and remediation of security incidents

Customized detection, analysis and remediation of security incidents incl. **proactive 24/7 monitoring and threat hunting**

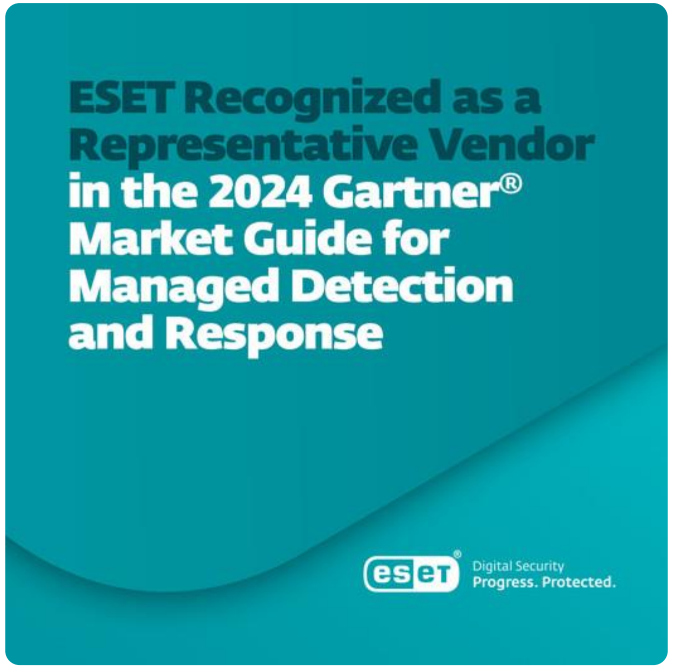
Analyst Recognitions

ESET PROTECT MDR

Market & Overall Leader

According to MDR Leadership Compass 2023

ESET is Overall & Market Leader for MDR
KuppingerCole



ESET Recognized as a Representative Vendor in the 2024 Gartner® Market Guide for Managed Detection and Response

eset® Digital Security Progress. Protected.

ESET is representative vendor for MDR
Gartner

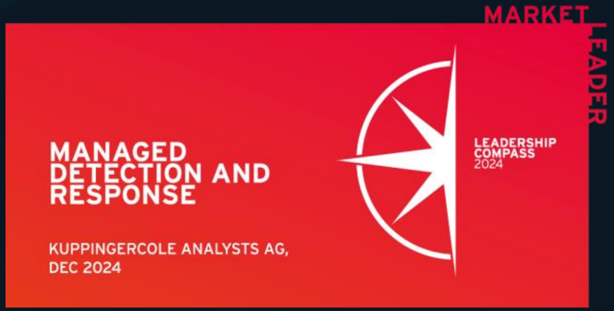
QUOTE FROM REPORT:
IDC: ESET Evolves with AI, MDR, Threat Intelligence, and Integrations.

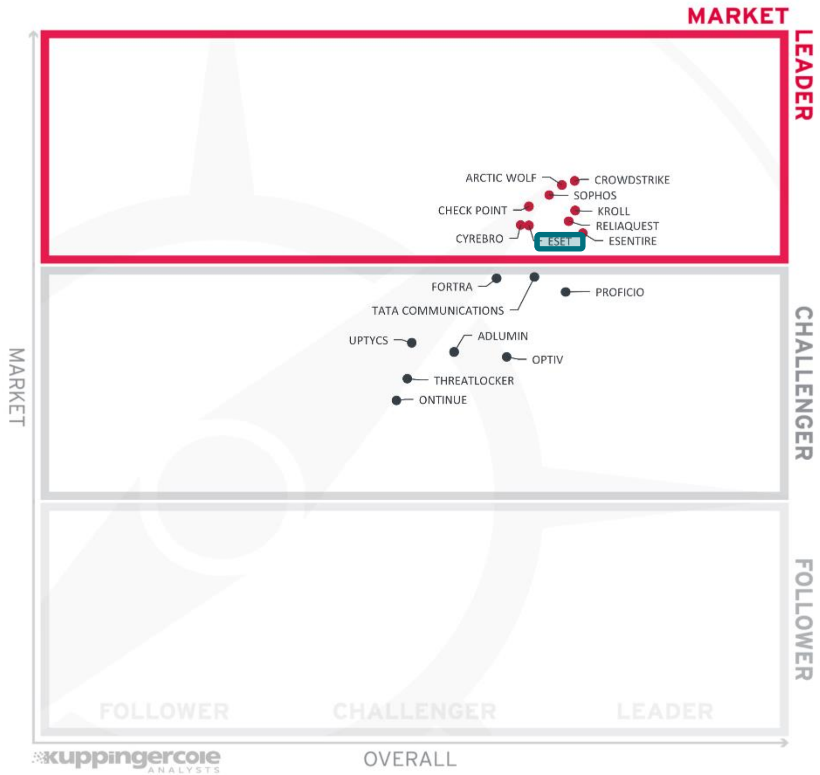
"While many of the cybersecurity behemoths continue to slug it out for market share and mindshare, and cybercriminals and nation state actors continue to develop ever more effective ways to breach company networks, **ESET goes steadily about its business of developing an integrated platform of world-class security solutions backed by world-class security research."**

ESET is commended for MDR offering
IDC

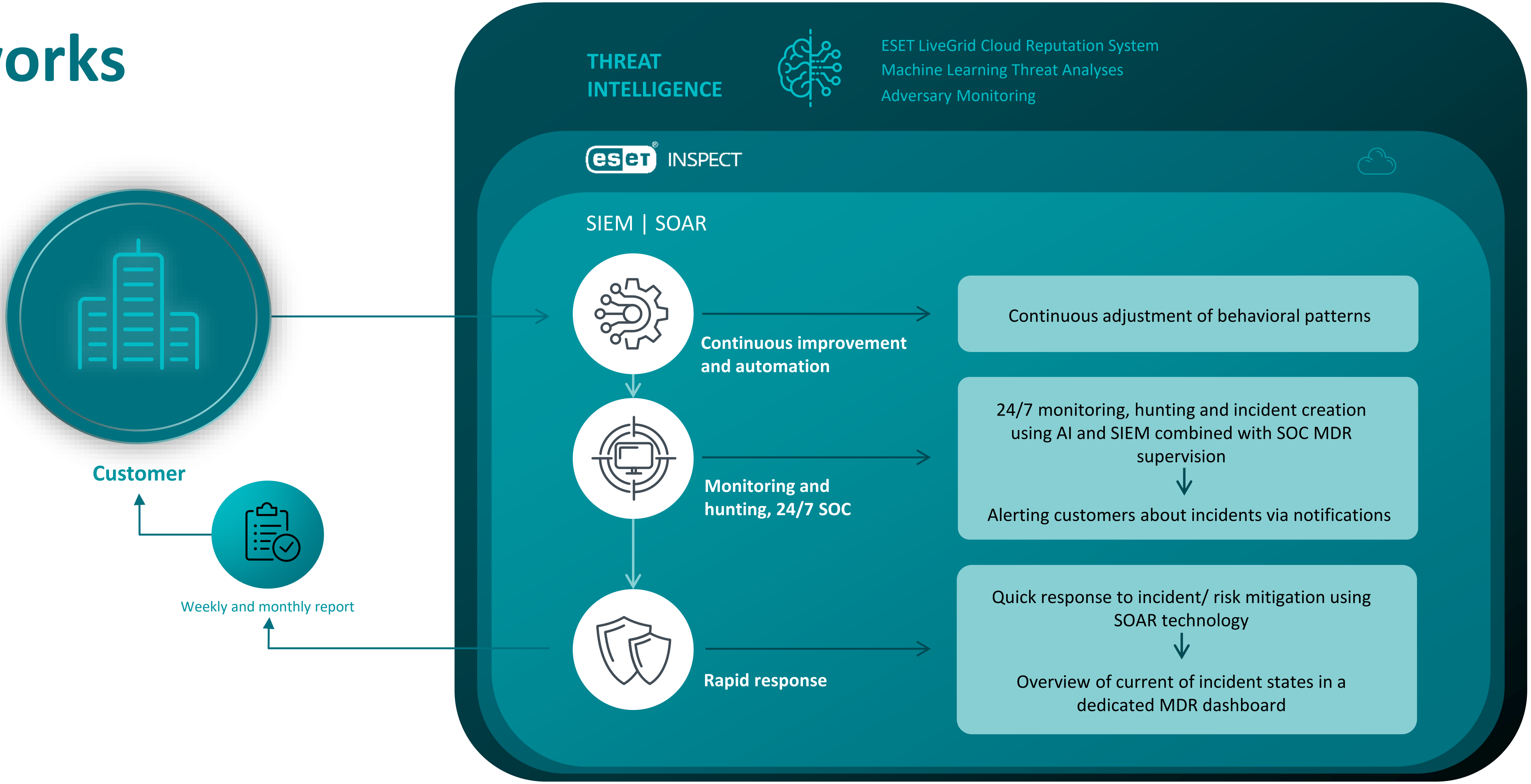
kuppingercole ANALYSTS

ESET has been recognized as both a **Market Leader** and a **Product Leader** in the **2024 MDR Leadership Compass.**


MARKET
LEADER
MANAGED DETECTION AND RESPONSE
KUPPINGERCOLE ANALYSTS AG, DEC 2024
LEADERSHIP COMPASS 2024



How ESET MDR works



THREAT INTELLIGENCE

ESET LiveGrid Cloud Reputation System
Machine Learning Threat Analyses
Adversary Monitoring

ESET INSPECT

SIEM | SOAR

Continuous improvement and automation → Continuous adjustment of behavioral patterns

Monitoring and hunting, 24/7 SOC → 24/7 monitoring, hunting and incident creation using AI and SIEM combined with SOC MDR supervision ↓ Alerting customers about incidents via notifications

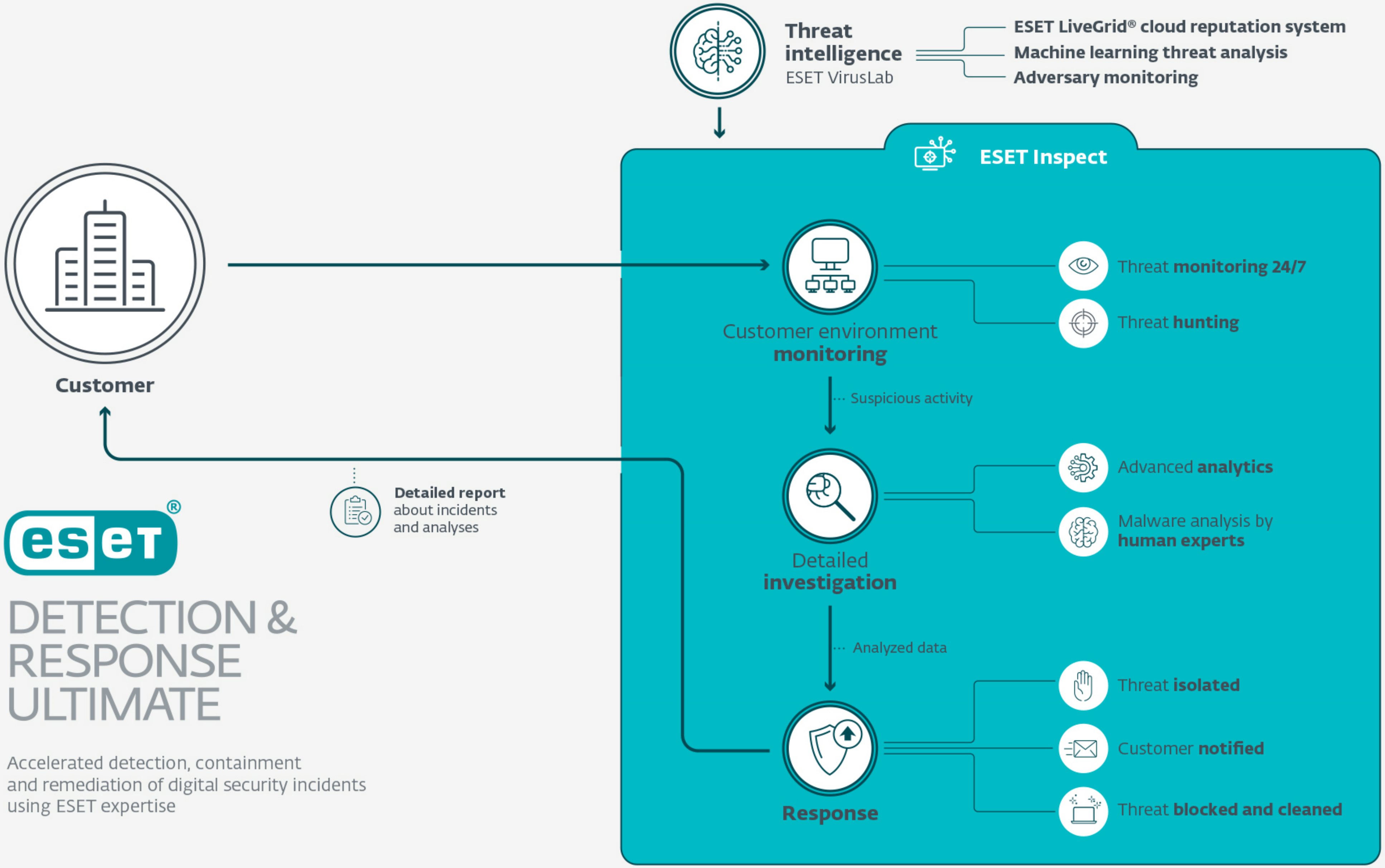
Rapid response → Quick response to incident/ risk mitigation using SOAR technology ↓ Overview of current of incident states in a dedicated MDR dashboard

Customer

Weekly and monthly report

DETECTION & RESPONSE ULTIMATE

Accelerated detection, containment and remediation of digital security incidents using ESET expertise



Threat intelligence
ESET VirusLab

- **ESET LiveGrid® cloud reputation system**
- **Machine learning threat analysis**
- **Adversary monitoring**

Customer

ESET Inspect

Customer environment **monitoring**

- Threat **monitoring 24/7**
- Threat **hunting**

Suspicious activity

Detailed **investigation**

- Advanced **analytics**
- Malware analysis by **human experts**

Analyzed data

Response

- Threat **isolated**
- Customer **notified**
- Threat **blocked and cleaned**

Detailed report about incidents and analyses

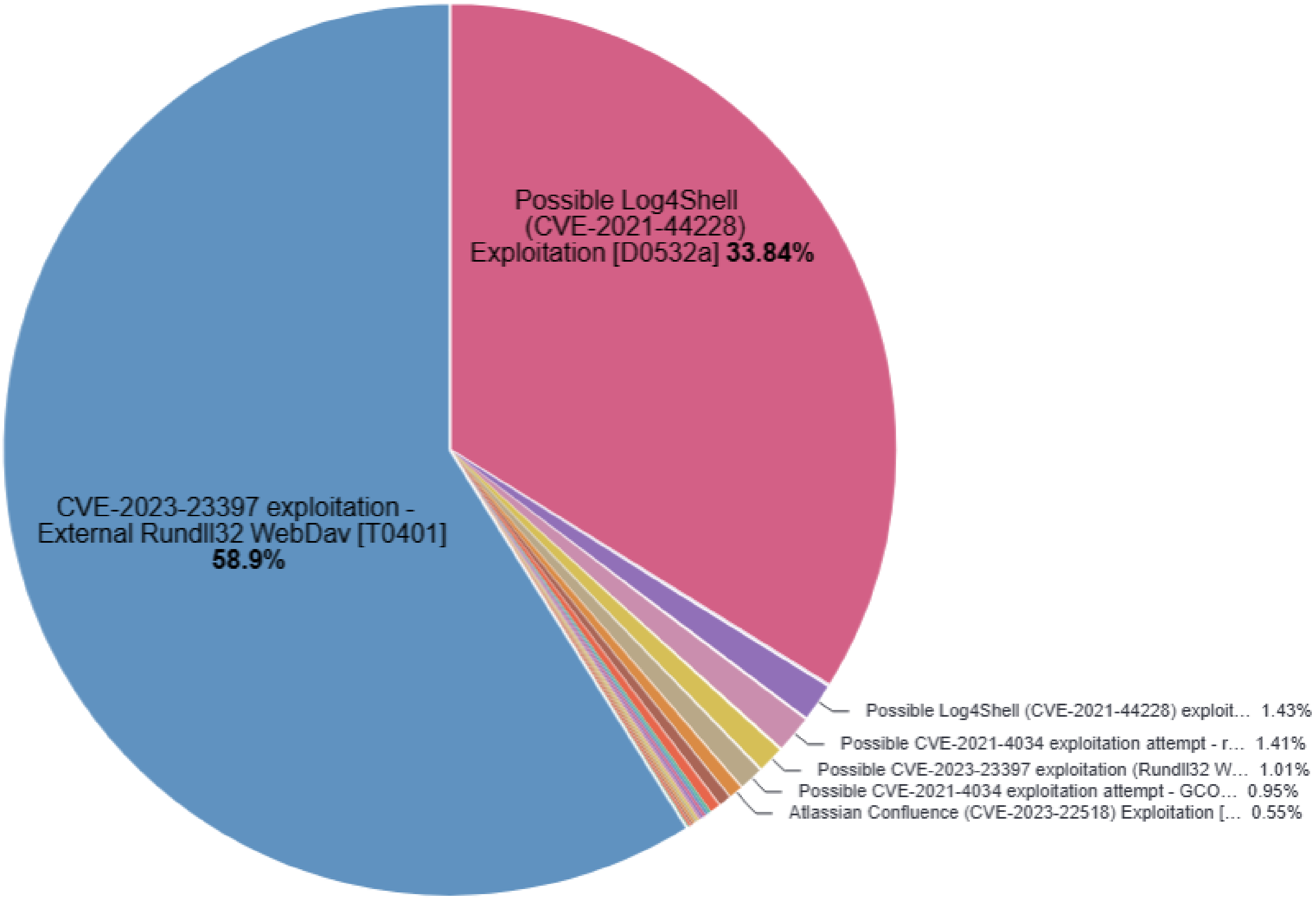
Initial access

- Valid credentials
  - VPNs
  - MS SQL servers
  - RDPs
- Web shells
- Vulnerabilities

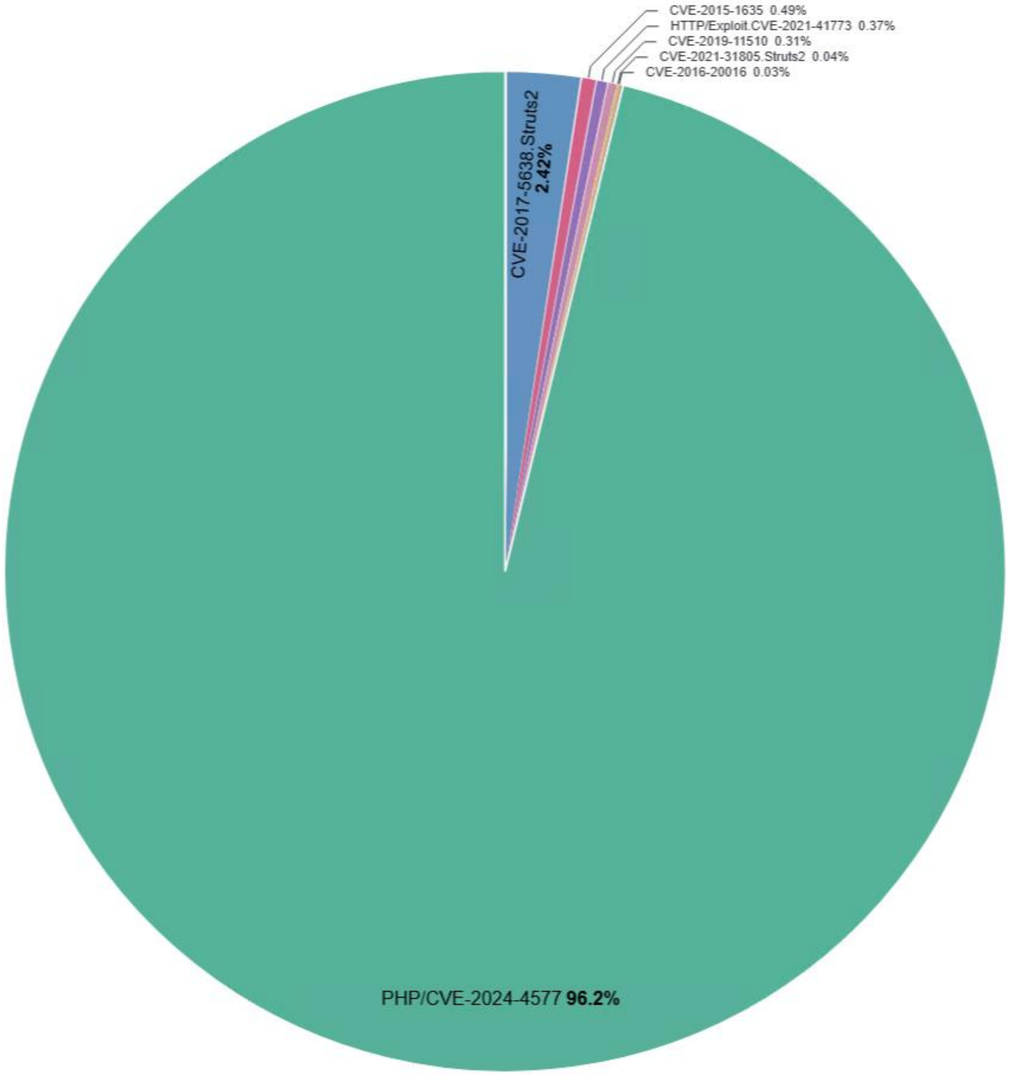
Targeted vulnerabilities

- Edge devices - FWs, VPNs, …
- Microsoft Exchange vulnerability (CVE-2021-26855)
- Veeam vulnerability (CVE-2023-27532)
- Veritas Backup Exec (CVE-2021-27876, CVE-2021-27877, CVE-2021-27878)
- FortiClient EMS vulnerability (CVE-2023-48788)

Targeted vulnerabilities



Targeted vulnerabilities



Infostealers | Commodity malware

- PXA Stealer – Python malware
- hxxps[://]tvdseo[.]com
    - "Compilazione di video e immagini protetti da copyright.exe"
- Credentials from Web Browsers

Credential access

- Web browsers
- Locally stored
- lsass

Credential access

- Parent name: wmiprvse.exe
  - /Q /c copy "C:\Users\<<redacted>>\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies" "C:\Windows\Temp\<<epoch time>>“
  - /Q /c copy "C:\Users\<<redacted>>\AppData\Local\Google\Chrome\User Data\Default\Login Data" "C:\Windows\Temp\<<epoch time>>"

LOLBins

- Powershell
- RMMs and likes (MeshAgent, …)
- ssh
- PsExec
- RDP
- WMI
- WinRM

HackTools | PUA | PUsA

- Cobalt Strike, Meterpreter, Empire, …
- Impacket
- PowerSploit
- Nirsoft, …
- Process Hacker, Gmer, …

Impacket

- Parent name: wmiprvse.exe
  - cmd.exe /Q /c <<command>> \ 1> \\127.0.0.1\ADMIN$\__<timestamp value> 2>&1

Impacket

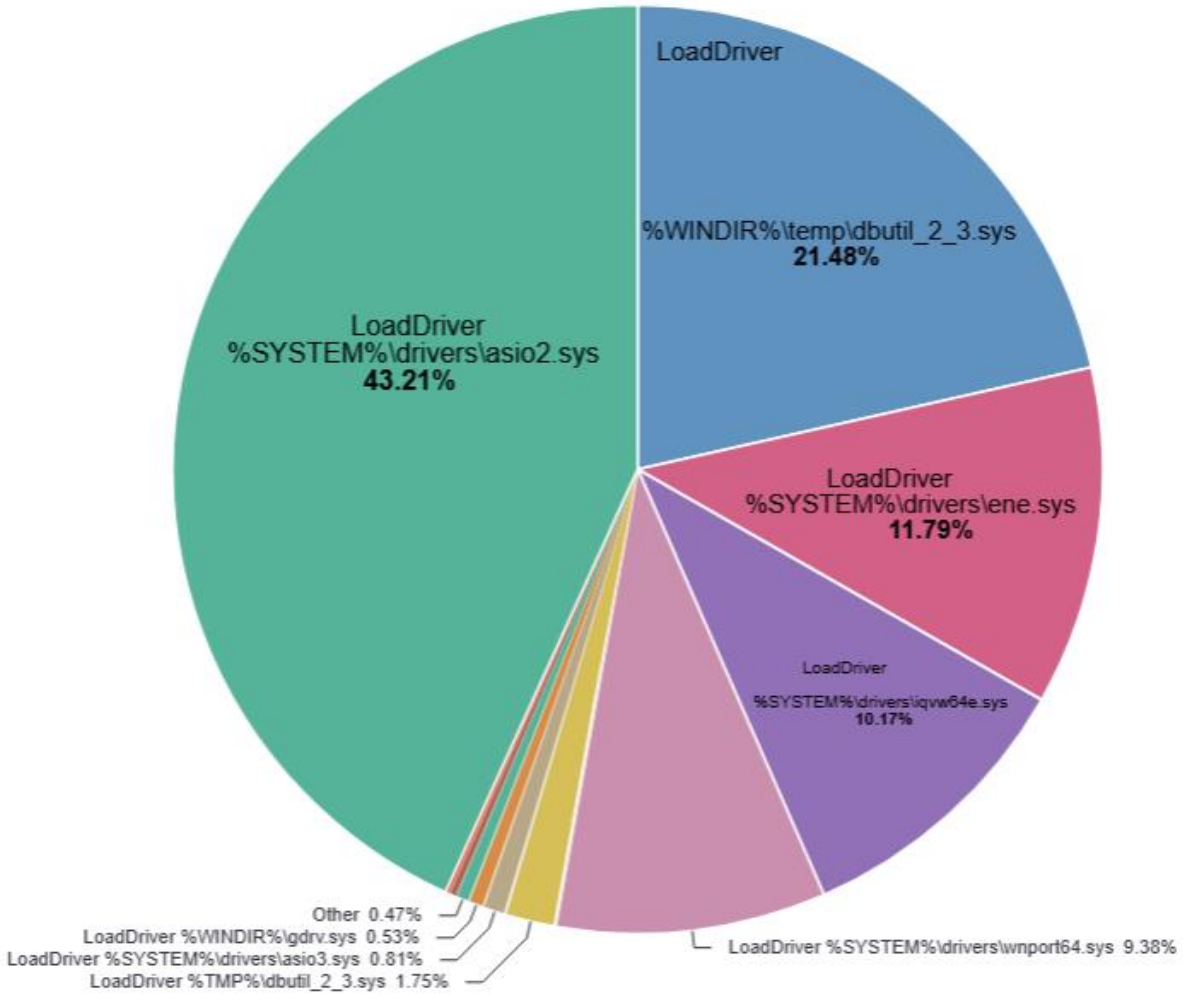
- Parent name: services.exe

  -
    ```
    /Q /c echo dir C:\Users\<<redacted>>\.ssh ^> \\<<redacted>>\C$\__output 2^>^&1 > C:\WINDOWS\afCBqXqx.bat & C:\WINDOWS\system32\cmd.exe /Q /c C:\WINDOWS\afCBqXqx.bat & del C:\WINDOWS\afCBqXqx.bat
    ```

Defense evasion

- EDR killers
  - Loading of drivers
  - BYOVD
- EDR silencers

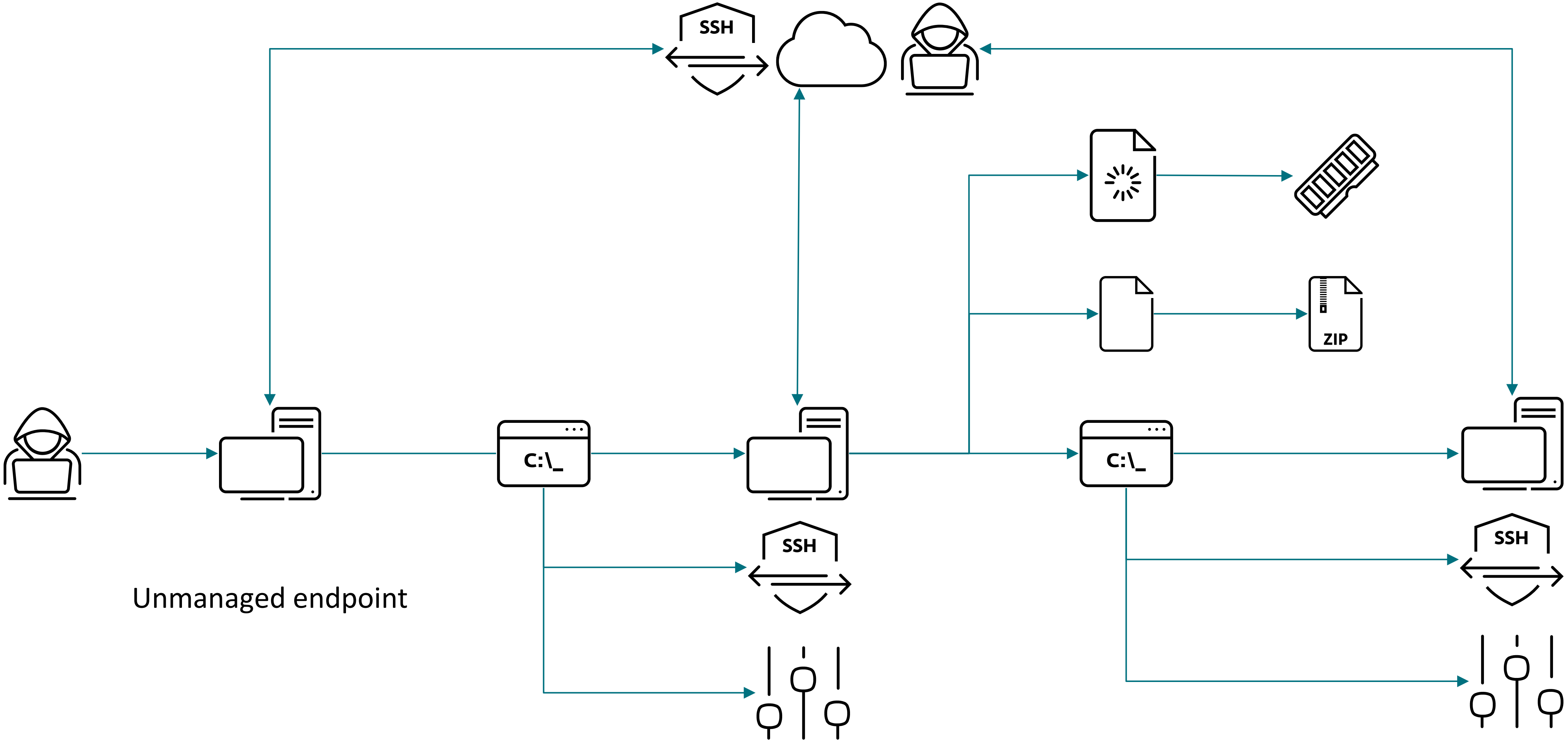
Vulnerable drivers



Still seen in the wild

- USB drive as initial vector
- Cracked software
- Keygens
- Windows activators
- Torrent downloads

APT attack



Unmanaged endpoint

Managed by ESET MDR

Managed by ESET MDR

APT attack - TTPs

- [T1059] Command and Scripting Interpreter
- [T1053.005] Scheduled Task/Job: Scheduled Task
- [T1021.004] Remote Services: SSH
- [T1560.001] Archive Collected Data: Archive via Utility
- [T1570] Lateral Tool Transfer
- [T1105] Ingress Tool Transfer
- [T1021.006] Remote Services: Windows Remote Management

SECURITY DAYS

Ďakujem

Digital Security
Progress. Protected.

&

SME KONFERENCIE