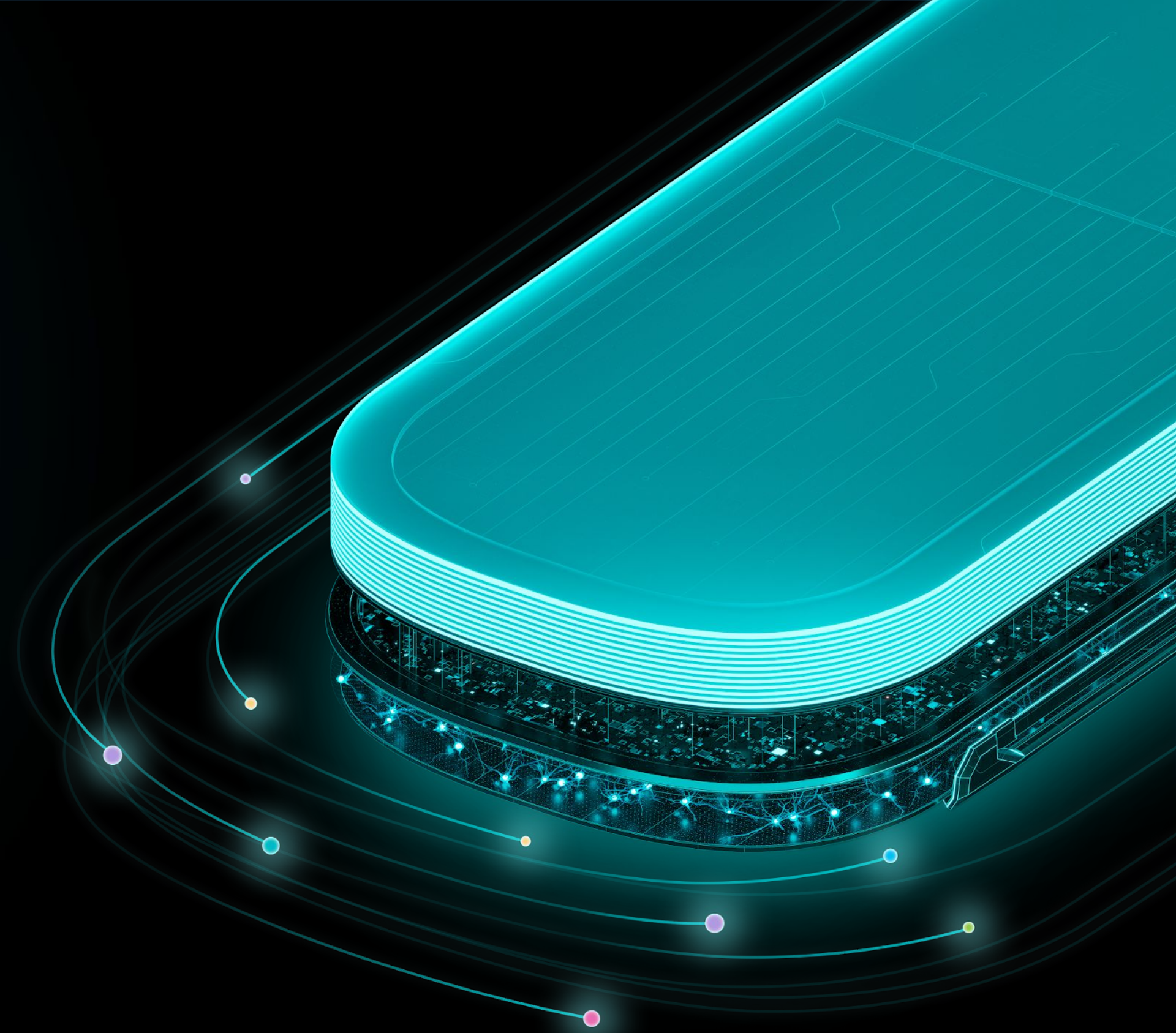


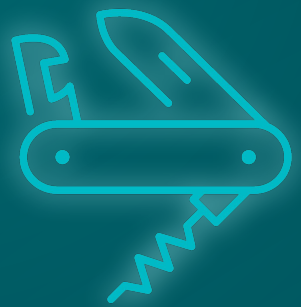
XDR, MDR a ich výhody



ONDREJ KRAJČ

Ondrej.krajc@eset.com

Bezpečnostné výzvy pre organizácie



Komplexnosť
útokov

2,200

Kyber útokov za deň



Regulácie a ich
požiadavky

66%

Očakáva výdaje spojené s
reguláciami



Nedostatok IT
security
odborníkov

49%

Profesionálov priznáva
nedostatky v IT
štruktúre



Finančná
náročnosť

51%

nárast financií v rokoch
2016-2023

Moderný Ransomware



Adversary Gains a Foothold

RDP/RDS Login,
Unpatched Service



Examines Network and Users

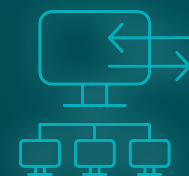
Living off the land



Downloads other utilities



Escalate Privileges /Steal Credentials



Moves Across Network



Find and Exfiltrate Files

Allows for Extortion



Deploy Encryption

Ransomware



Demand Payment

Extortionware



Adversary Gains a Foothold

RDP/RDS Login,
Unpatched Service



Examines Network and Users

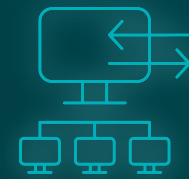
Living off the land



Downloads other utilities



Escalate Privileges /Steal Credentials



Moves Across Network



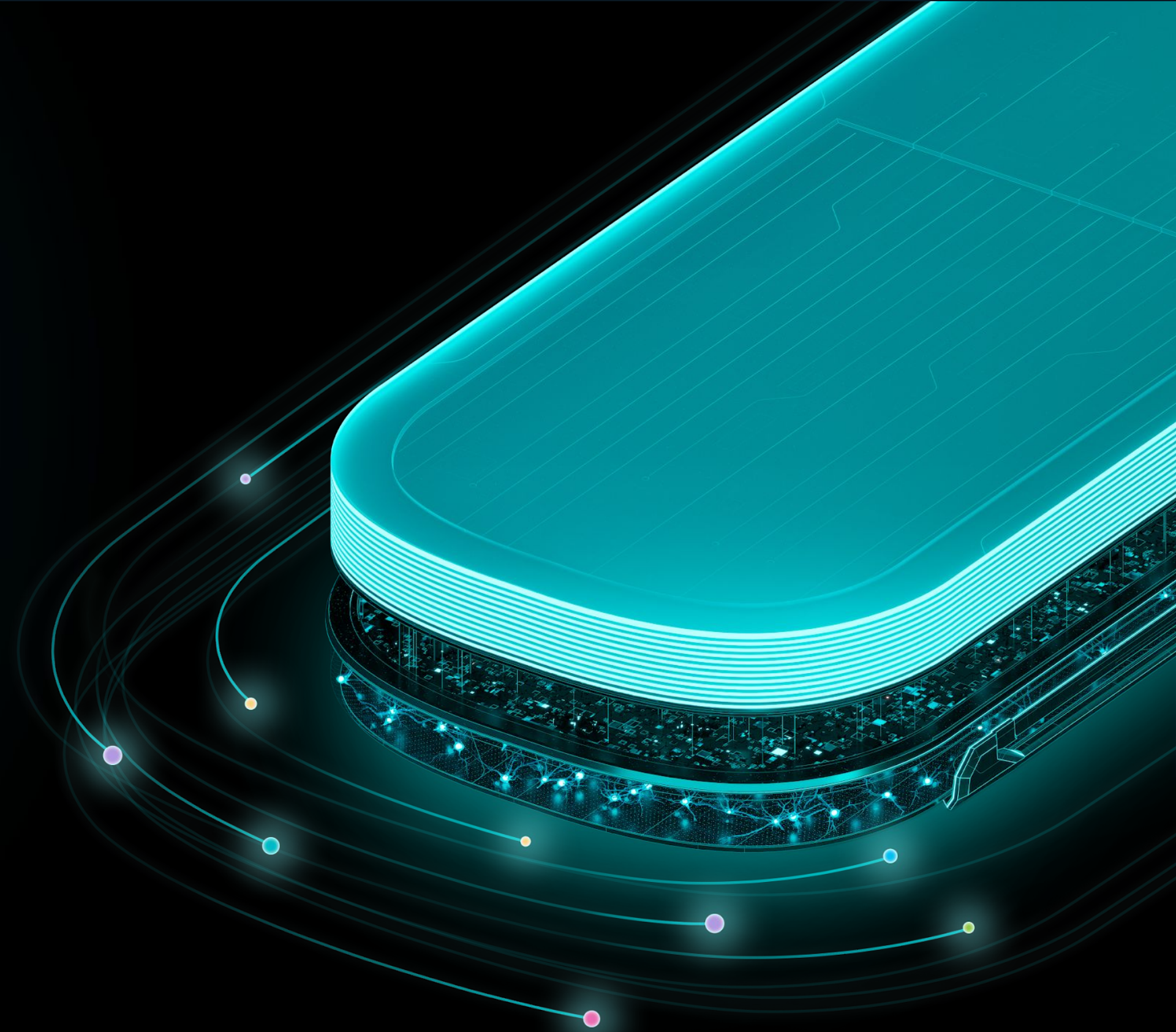
Find and Exfiltrate Files

Allows for Extortion



Demand Payment

XDR



Bežná viditeľnosť AV ochrany:



minimálna viditeľnosť



neistota



PowerShell Launched

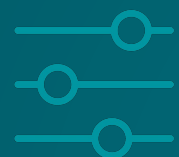


Threat Detected/Blocked

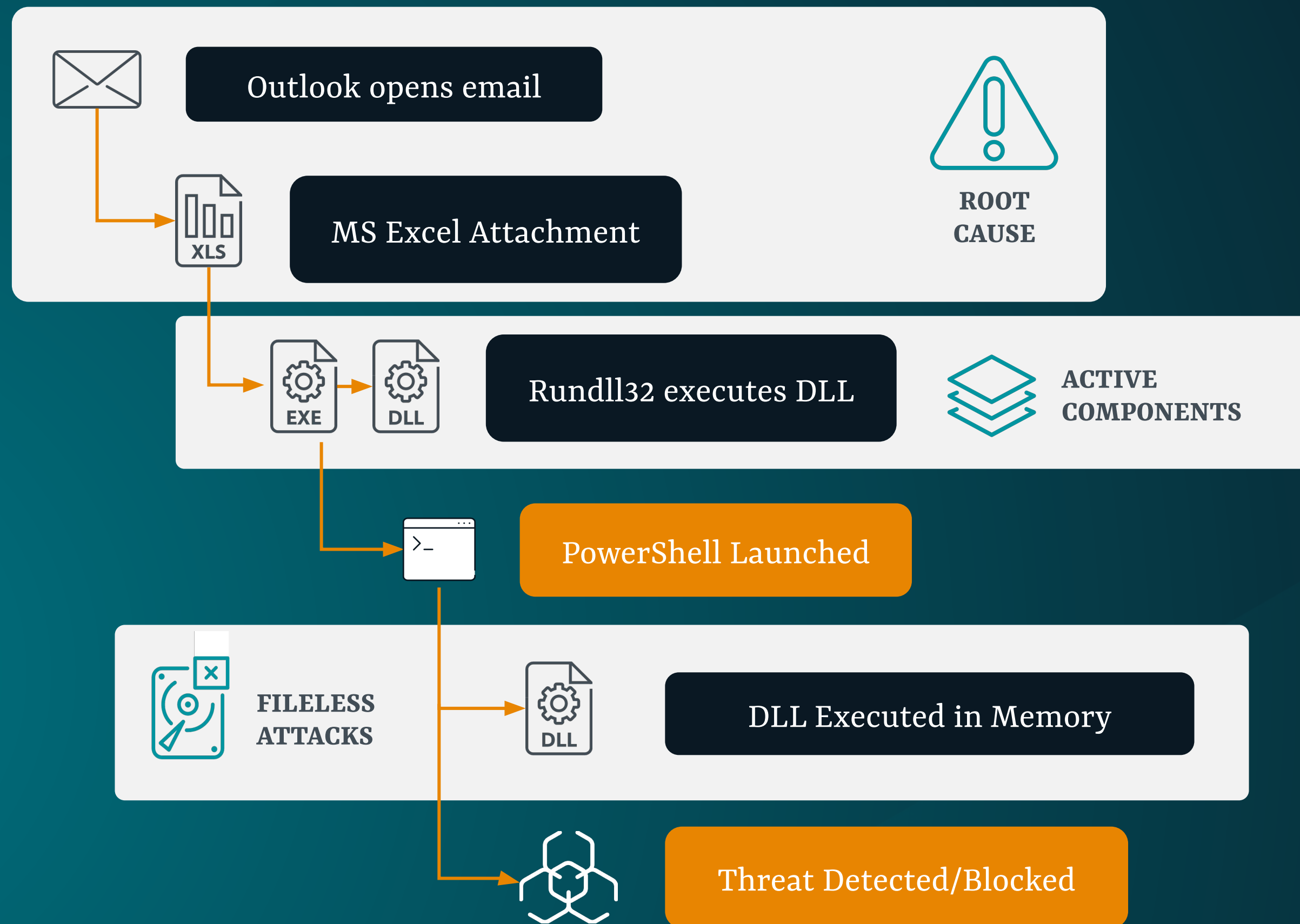
S ESET Inspect riešením:



zvýšená viditeľnosť



dodatočná kontrola

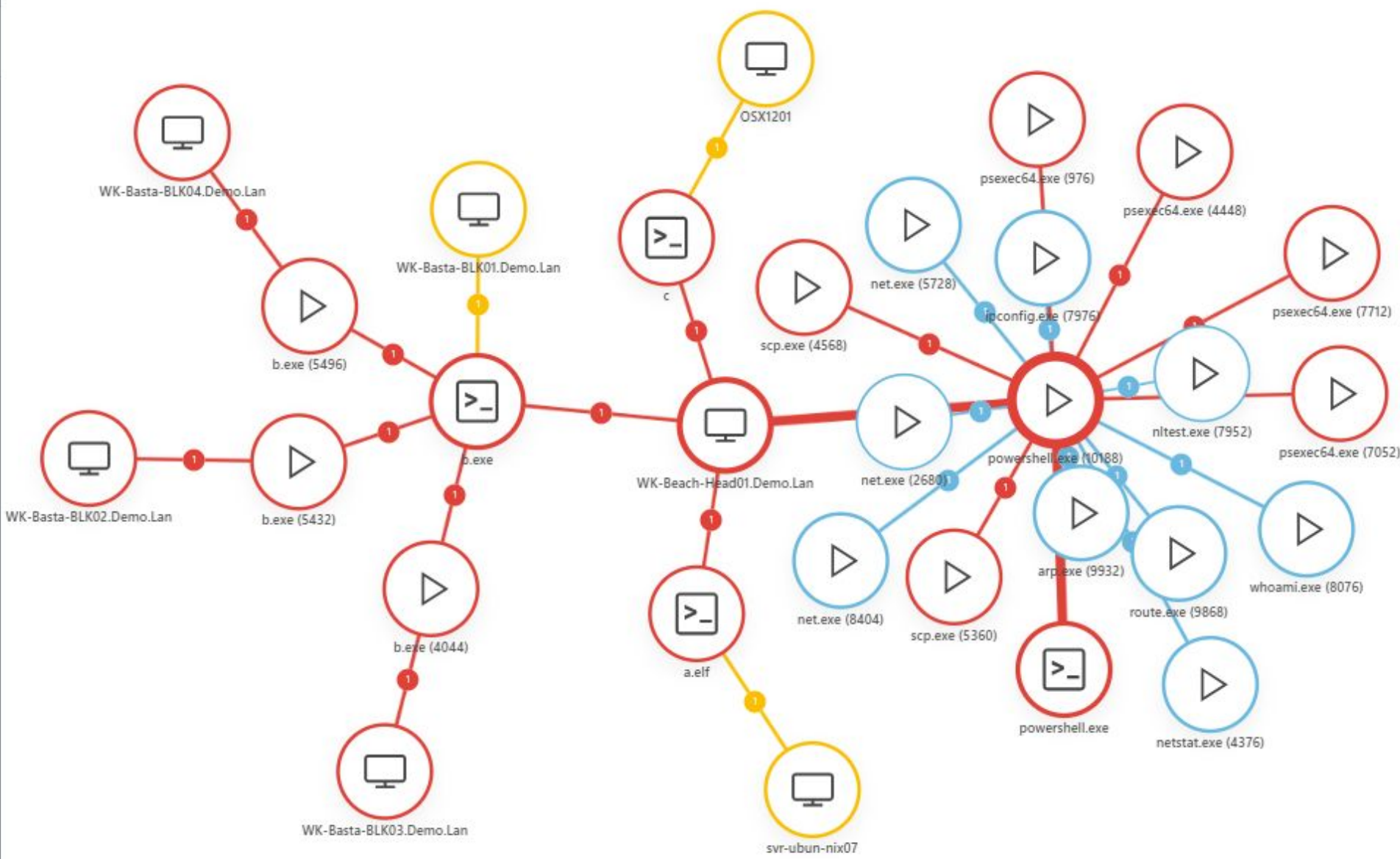


- DASHBOARD
- COMPUTERS
- DETECTIONS
- SEARCH
- INCIDENTS
- Executables
- Scripts
- Questions
- More...

BACK

Filecoder activity across multiple endpoints

- Timeline
- Relation graph
- Detections
- Computers
- Executables
- Processes



- Incident
- Timeline

Filecoder activity across multiple endpoints

Status

Open

Severity

High

Assignee

Michal Jankech

Tags

Gartner Scenario 2

Ransomware Atta...

Select tags

Description

None

- Threat indicators (28)
- Rule

Domain trust discovery [D1102]

Mitre att&ck™ techniques

T1482 - Domain Trust Discovery
- Rule

Domain trust enumeration via NLTest/ADFind [C1118]

Mitre att&ck™ techniques

T1482 - Domain Trust Discovery

View more

- Computers (7)
- wk-beach-head01.demo.lan

osx1201

View more

- Executables (4)
- c

powershell.exe

View more

- Processes (19)
- powershell.exe (10188)

nltest.exe (7952)

View more

Problémy



Komplexita nástrojov



Únava z veľkého množstva upozornení



**Nedostatok
kvalifikovaných ľudí**



Limitovaný čas na reakciu

The background is a dark blue, almost black, field filled with a complex pattern of glowing blue and white binary digits (0s and 1s). These digits are arranged in a way that suggests a three-dimensional grid or a data stream flowing through space. Faint, light blue grid lines are visible, creating a sense of depth and structure. The overall effect is one of high-tech digital connectivity and data processing.

MDR

(služby riadenej bezpečnosti)

Čo je MDR?

Managed Detection & Response je služba pod vedením odborníkov monitorujúcich a reagujúcich na škodlivú aktivitu vo vašej infraštruktúre.



Prečo **MDR** mení pravidlá hry?

je účinné riešenie na zvládnutie výziev spojených s detekciou a reakciou na hrozby pre zákazníkov

Gartner:

klúčovou hodnotou, ktorú poskytovatelia MDR prinášajú, sú služby, inak príliš zložité a nákladné na to, aby ich klienti vykonávali sami:

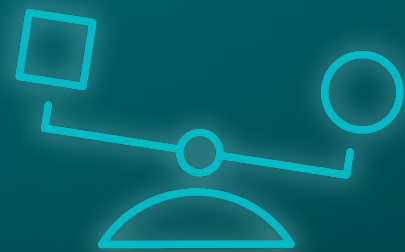
- Analýza rozličných telemetrických údajov
- AI/ML a ľudská interpretácia bezpečnostných incidentov
- Včasné usmernenie ohrozenia
- Rôzne úrovne reakcie/nápravy



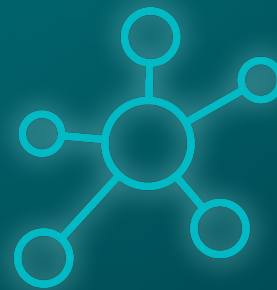
Ako vie **ESET MDR** pomôcť?



**Posilnenie
bezpečnosti**



Skúsení ľudia



**Cross-industry
viditeľnosť**



**Úspora
nákladov**



**Napĺňanie
regulácií**

Ako ESET MDR funguje?



Zákazník



reporting

THREAT
INTELLIGENCE



ESET LiveGrid Cloud Reputation System
Machine Learning Threat Analyses
Adversary Monitoring

eset INSPECT



SIEM | SOAR



Neustále zlepšovanie a
automatizácia

Continuous adjustment of behavioral patterns



Monitoring and
hunting, 24/7 SOC

24/7 monitoring, hunting a incident creation
za použitia AI a SIEM kombinovaných so SOC
MDR dohľadom

Upozornenie zákazníka cez notifikácie



Urýchlená reakcia

Quick response to incident/ risk mitigation
using SOAR technology

Overview of current of incident states in a
dedicated MDR dashboard

Špecifikácie ESET MDR služieb

	MDR	MDR Ultimate
24/7 Expert-Led Continuous Threat Monitoring, Hunting, Triage and Response	✓	✓
Global Threat Intelligence Team	✓	✓
Behavior Patterns and Exclusions Optimization	✓	✓
Behavior Patterns Library	✓	✓
Tailored Reporting	✓ Standard	✓ Advanced
Historical & Customized Threat Hunting		✓
Attack Vectors Visibility		✓
Digital Forensic Incident Response (DFIR) Assistance		✓
Dedicated Incident Response Lead		✓
Expert Assistance for MDR Alerts, with More Context		✓

Čím je **ESET MDR** unikátna:

20 min.

čas potrebný na
detekciu a reakciu

600+

R&D expertov v 13
centrách

24/7

threat management

35 rokov

Skúseností v
cybersecurity

podpora

39 jazykov

110M+

Po celom svete

Ďakujem za pozornosť

