SECURITY DAYS

AKO VÁM SECURITY SLUŽBY VEDIA NAPOMÔCŤ PRI POSILŇOVANÍ ÚROVNE VÁŠHO ZABEZPEČENIA?

DUŠAN KAŠTAN, ESET

ESET Digital Security Progress. Protected. & SME KONFERENCIE

GARTNER

"In advanced security operations, additional staff members are needed to perform threat hunting and threat intelligence operations,

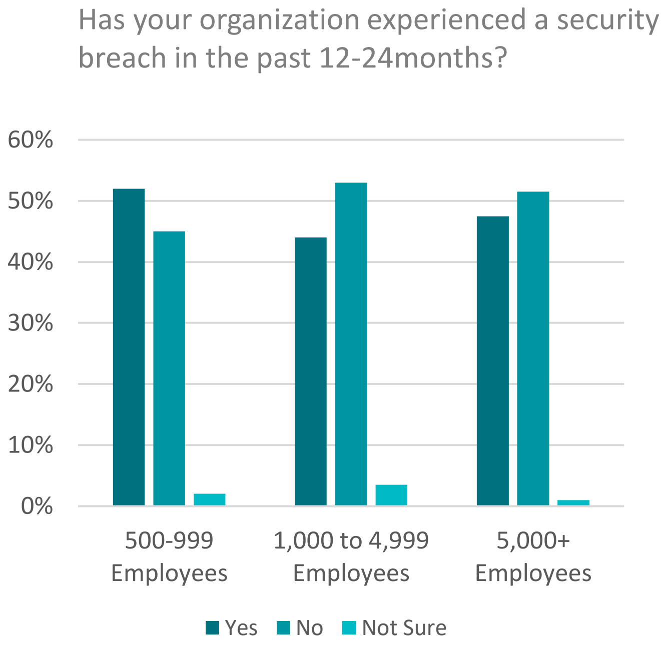
but people with these more specialized skills are especially

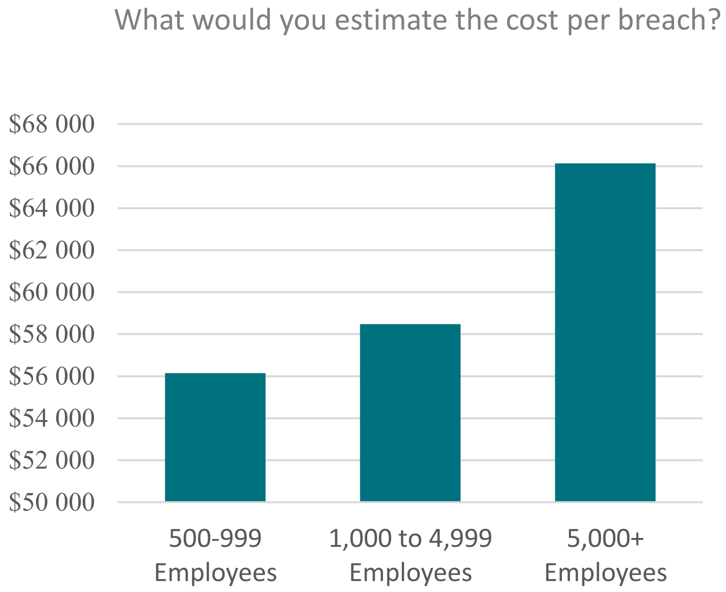
hard to find.

Managed services, such as managed detection and response (MDR), help organizations address this issue. “

Gartner: [2023 Planning Guide for Security], [Richard Bartley and Team], [10 October 2022] ID: G00775183

NO SURPRISE HERE: BREACHES ARE A REALITY





IDC Source: Security Services Market Update Webinar, Q1 2022, IDC Security Services Team, January 2022

A year of wiper attacks in Ukraine

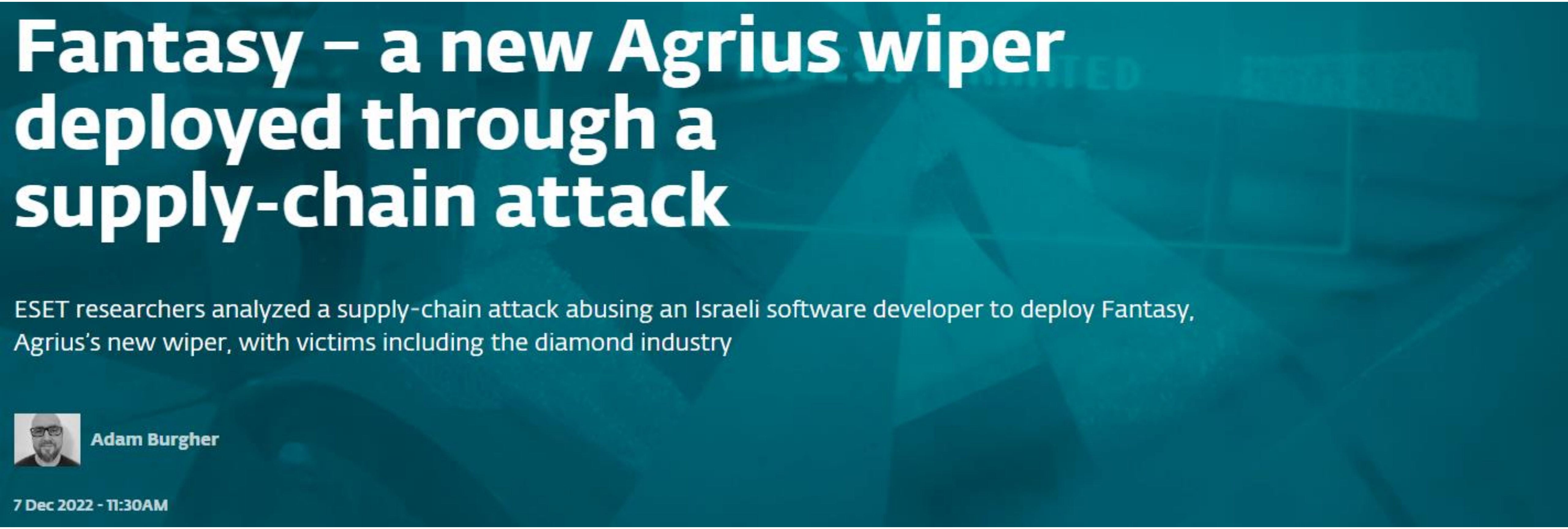
ESET Research has compiled a timeline of cyberattacks that used wiper malware and have occurred since Russia's invasion of Ukraine in 2022

(e):r ESET Research

24 Feb 2023 - 11:30AM

A year of wiper attacks in Ukraine

“On October 11th, 2022, we also identified a previously unknown wiper, which we named **NikoWiper**. This wiper was used against a company in the energy sector in Ukraine. **NikoWiper** is based on the **SDelete Microsoft command line** utility for securely deleting files. “



Fantasy – a new Agrius wiper deployed through a supply-chain attack

ESET researchers analyzed a supply-chain attack abusing an Israeli software developer to deploy Fantasy, Agrius's new wiper, with victims including the diamond industry

Adam Burgher

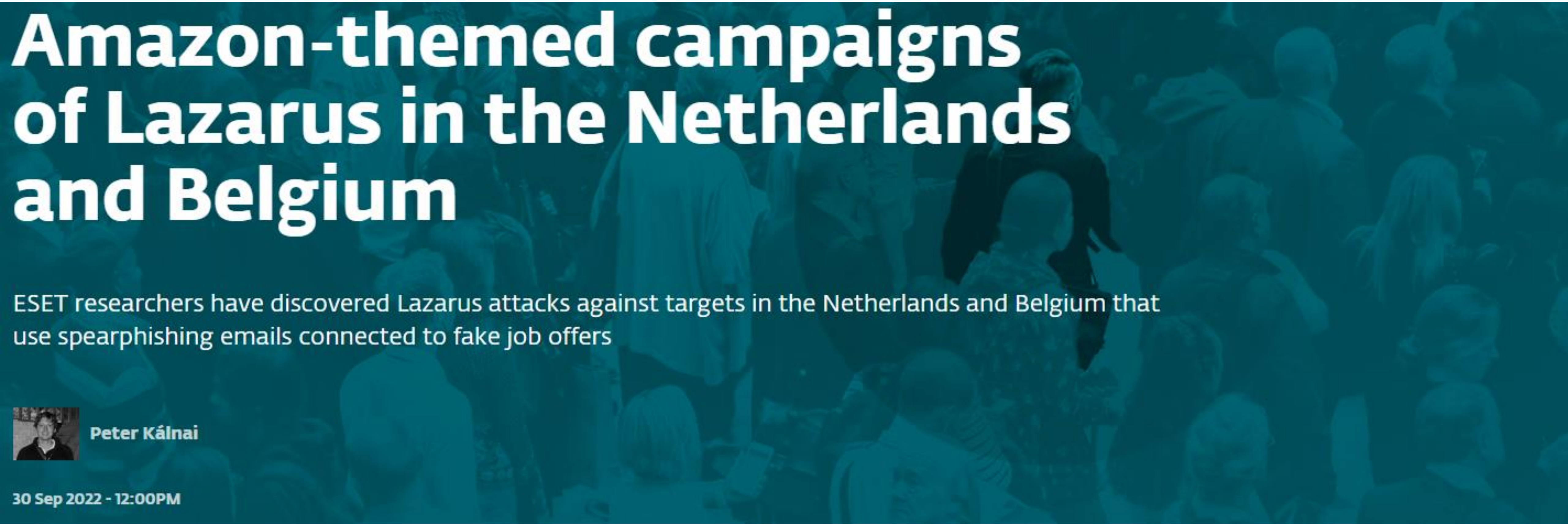
7 Dec 2022 - 11:30AM

Fantasy – a new Agrius wiper deployed through a supply-chain attack

“**Sandals** is a 32-bit Windows executable written in C#/.NET. We chose the name because **Sandals** is an anagram of some of the command line arguments it accepts. It is used to connect to systems in the same network via SMB, to write a batch file to disk that executes the Fantasy wiper, and then run that batch file via **PsExec with this command line string**:

```
PsExec.exe /accepteula -d -u “<username>” -p “<password>”
-s “C:\<path>\<GUID>.bat”
```

“



Amazon-themed campaigns of Lazarus in the Netherlands and Belgium

ESET researchers have discovered Lazarus attacks against targets in the Netherlands and Belgium that use spearphishing emails connected to fake job offers

Peter Kálnai

30 Sep 2022 - 12:00PM

Amazon-themed campaigns of Lazarus in the Netherlands and Belgium

Location folder	Legitimate parent process	Malicious side-loaded DLL	Trojanized project
C:\ProgramData\PTC\	**colorcpl.exe**	colorui.dll	libcrypto of LibreSSL 2.6.5
C:\Windows\Vss\	**WFS.exe**	credui.dll	GOnpp v1.2.0.0 (Notepad++ plug-in)
C:\Windows\security\	**WFS.exe**	credui.dll	FingerText 0.56.1 (Notepad++ plug-in)
C:\ProgramData\Caphyon\	**wsmprovhost.exe**	mi.dll	lecui 1.0.0 alpha 10
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\	**SMSvcHost.exe**	cryptsp.dll	lecui 1.0.0 alpha 10

FINDINGS OF ESET SURVEY

404 respondents from large companies (not only ESET customers)

On average, **91%** use / plan to use Services

68% would prefer the vendor to deploy their products

75% expect their vendor to offer support, consultation and incident response

87% request cybersecurity support 24/7/365

90% prefer response and remediation actions to be included in the monitoring and threat hunting service provided by vendor/3rd party

TRUSTED BY SOME OF THE WORLD‘S BIGGEST PLAYERS

MITSUBISHI MOTORS
Drive your Ambition
T · · ·
Google Play
Canon
FIJI AIRWAYS
de volksbank
Allianz Suisse
DB

✚

Member of the Joint Cyber Defense Collaborative | CISA

RECOGNIZED RESEARCH & DISCOVERIES SERVING CYBERSECURITY

RANSOMWARE WHITE PAPER // 2018 // Author: Stephen Cobb

TLP: WHITE

RANSOMWARE:

an enterprise perspective

Digital Security
Progress. Protected.

White papers

ESET Threat Intelligence APT reports PREMIUM

Digital Security
Progress. Protected.

THREAT RESEARCH

ACTIVITY SUMMARY

Issue:

AS-2021-0007

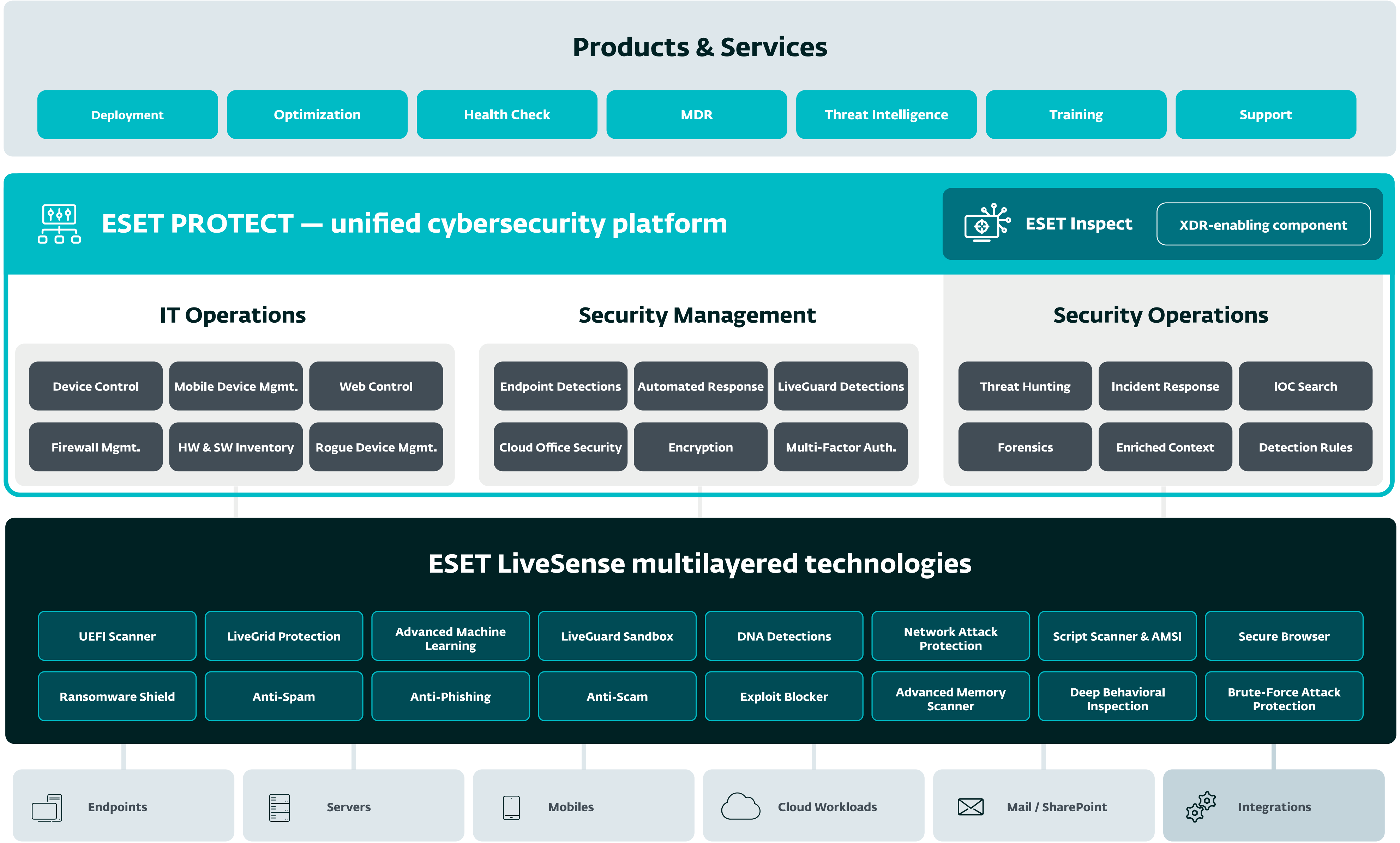
1 April – 15 April, 2021

* This report and its contents have been provided for distribution within your organization only

APT reports PREMIUM

ESET is one of the most active **MITRE ATT&CK** contributors, and one of the most referenced sources.

MITRE | ATT&CK®



Products & Services

Deployment | Optimization | Health Check | MDR | Threat Intelligence | Training | Support

ESET PROTECT — unified cybersecurity platform

ESET Inspect

XDR-enabling component

IT Operations

- Device Control
- Mobile Device Mgmt.
- Web Control
- Firewall Mgmt.
- HW & SW Inventory
- Rogue Device Mgmt.

Security Management

- Endpoint Detections
- Automated Response
- LiveGuard Detections
- Cloud Office Security
- Encryption
- Multi-Factor Auth.

Security Operations

- Threat Hunting
- Incident Response
- IOC Search
- Forensics
- Enriched Context
- Detection Rules

ESET LiveSense multilayered technologies

- UEFI Scanner
- LiveGrid Protection
- Advanced Machine Learning
- LiveGuard Sandbox
- DNA Detections
- Network Attack Protection
- Script Scanner & AMSI
- Secure Browser
- Ransomware Shield
- Anti-Spam
- Anti-Phishing
- Anti-Scam
- Exploit Blocker
- Advanced Memory Scanner
- Deep Behavioral Inspection
- Brute-Force Attack Protection

Endpoints | Servers | Mobiles | Cloud Workloads | Mail / SharePoint | Integrations

CHOOSE THE LEVEL OF SERVICE THAT FITS YOUR ORGANIZATION‘S REQUIREMENTS SECURITY SERVICES

ACTIVITY	STANDARD SECURITY SUPPORT	DETECTION AND RESPONSE ESSENTIAL	DETECTION AND RESPONSE ADVANCED	DETECTION AND RESPONSE ULTIMATE
	Best effort	Guaranteed by SLA	Guaranteed by SLA	Guaranteed by SLA
Malware: missing detection	✓	✓	✓	✓
Malware: cleaning problem	✓	✓	✓	✓
Malware: ransomware infection	✓	✓	✓	✓
False positive	✓	✓	✓	✓
General: Suspicious behavior investigation	✓	✓	✓	✓
Basic file analysis	–	✓	✓	✓
Detailed file analysis	–	✓	✓	✓
Digital forensic	–	✓	✓	✓
Digital forensic incident response assistance	–	✓	✓	✓
Support – rules	–	–	✓	✓
Support – exclusions	–	–	✓	✓
General: ESET Inspect (EI) security related question	–	–	✓	✓
EI: Initial Optimization	–	–	✓	✓
EI: Threat Hunting (on-demand)	–	–	✓	✓
EI: Threat Monitoring	–	–	–	✓
EI: Threat Hunting (proactive)	–	–	–	✓
Deployment & Upgrade	–	–	–	✓

CHOOSE THE LEVEL OF SERVICE THAT FITS YOUR ORGANIZATION‘S REQUIREMENTS
SECURITY SERVICES

ACTIVITY	STANDARD SECURITY SUPPORT	DETECTION AND RESPONSE ESSENTIAL	DETECTION AND RESPONSE ADVANCED	DETECTION AND RESPONSE ULTIMATE
	Best effort	Guaranteed by SLA	Guaranteed by SLA	Guaranteed by SLA
Malware: missing detection	✓	✓	✓	✓
Malware: cleaning problem	✓	✓	✓	✓
Malware: ransomware infection	✓	✓	✓	✓
False positive	✓	✓	✓	✓
General: Suspicious behavior investigation	✓	✓	✓	✓
Basic file analysis	–	✓	✓	✓
Detailed file analysis	–	✓	✓	✓
Digital forensic	–	✓	✓	✓
Digital forensic incident response assistance	–	✓	✓	✓
Support – rules	–	–	✓	✓
Support – exclusions	–	–	✓	✓
General: ESET Inspect (EI) security related question	–	–	✓	✓
EI: Initial Optimization	–	–	✓	✓
EI: Threat Hunting (on-demand)	–	–	✓	✓
EI: Threat Monitoring	–	–	–	✓
EI: Threat Hunting (proactive)	–	–	–	✓
Deployment & Upgrade	–	–	–	✓

CHOOSE THE LEVEL OF SERVICE THAT FITS YOUR ORGANIZATION'S REQUIREMENTS SECURITY SERVICES

ACTIVITY	STANDARD SECURITY SUPPORT	DETECTION AND RESPONSE ESSENTIAL	DETECTION AND RESPONSE ADVANCED	DETECTION AND RESPONSE ULTIMATE
	Best effort	Guaranteed by SLA	Guaranteed by SLA	Guaranteed by SLA
Malware: missing detection	✓	✓	✓	✓
Malware: cleaning problem	✓	✓	✓	✓
Malware: ransomware infection	✓	✓	✓	✓
False positive	✓	✓	✓	✓
General: Suspicious behavior investigation	✓	✓	✓	✓
Basic file analysis	–	✓	✓	✓
Detailed file analysis	–	✓	✓	✓
Digital forensic	–	✓	✓	✓
Digital forensic incident response assistance	–	✓	✓	✓
Support – rules	–	–	✓	✓
Support – exclusions	–	–	✓	✓
General: ESET Inspect (EI) security related question	–	–	✓	✓
EI: Initial Optimization	–	–	✓	✓
EI: Threat Hunting (on-demand)	–	–	✓	✓
EI: Threat Monitoring	–	–	–	✓
EI: Threat Hunting (proactive)	–	–	–	✓
Deployment & Upgrade	–	–	–	✓

CHOOSE THE LEVEL OF SERVICE THAT FITS YOUR ORGANIZATION‘S REQUIREMENTS SECURITY SERVICES

ACTIVITY	STANDARD SECURITY SUPPORT	DETECTION AND RESPONSE ESSENTIAL	DETECTION AND RESPONSE ADVANCED	DETECTION AND RESPONSE ULTIMATE
	Best effort	Guaranteed by SLA	Guaranteed by SLA	Guaranteed by SLA
Malware: missing detection	✓	✓	✓	✓
Malware: cleaning problem	✓	✓	✓	✓
Malware: ransomware infection	✓	✓	✓	✓
False positive	✓	✓	✓	✓
General: Suspicious behavior investigation	✓	✓	✓	✓
Basic file analysis	–	✓	✓	✓
Detailed file analysis	–	✓	✓	✓
Digital forensic	–	✓	✓	✓
Digital forensic incident response assistance	–	✓	✓	✓
Support – rules	–	–	✓	✓
Support – exclusions	–	–	✓	✓
General: ESET Inspect (EI) security related question	–	–	✓	✓
EI: Initial Optimization	–	–	✓	✓
EI: Threat Hunting (on-demand)	–	–	✓	✓
EI: Threat Monitoring	–	–	–	✓
EI: Threat Hunting (proactive)	–	–	–	✓
Deployment & Upgrade	–	–	–	✓

CHOOSE THE LEVEL OF SERVICE THAT FITS YOUR ORGANIZATION‘S REQUIREMENTS PREMIUM SUPPORT

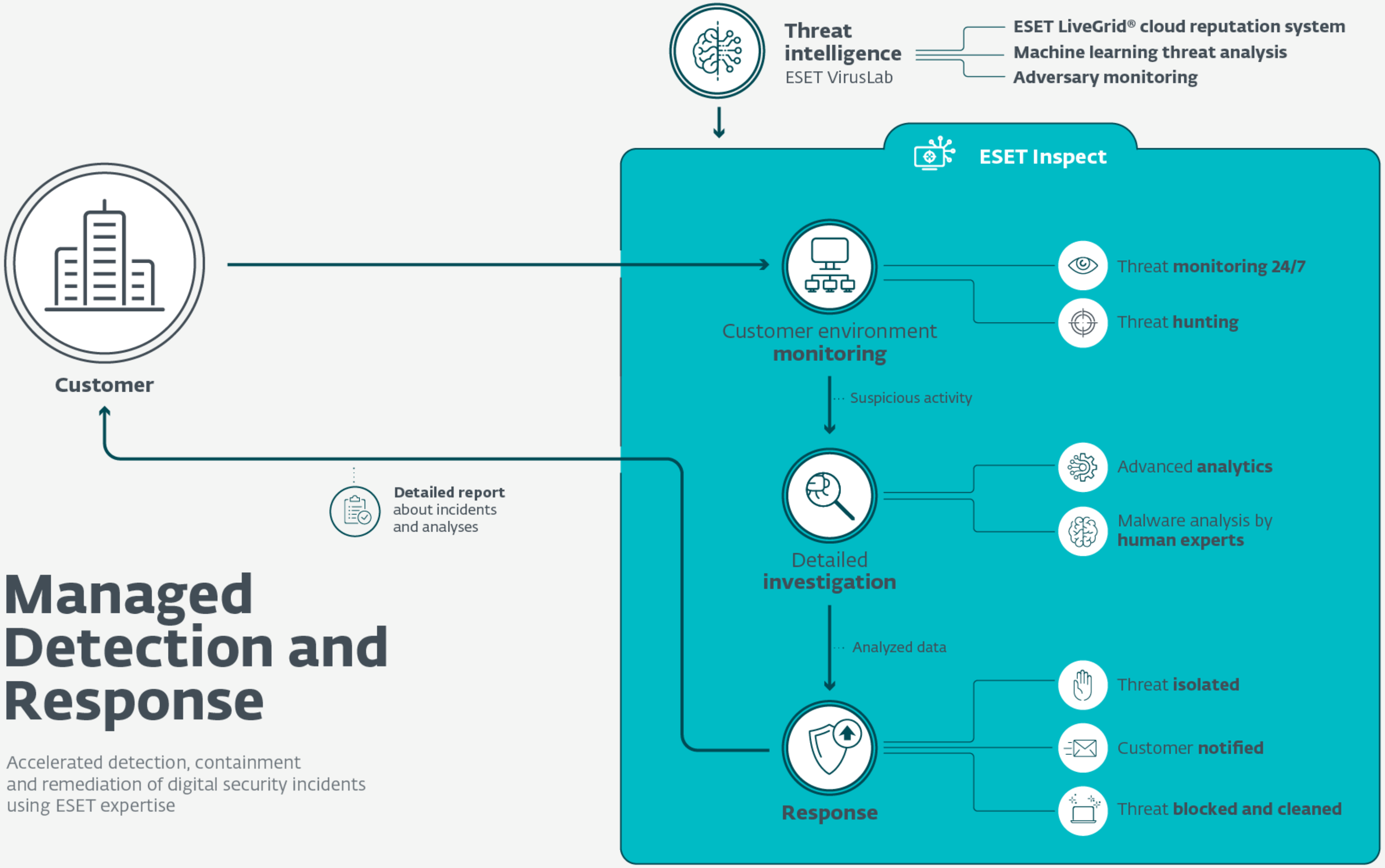
	STANDARD SUPPORT	PREMIUM SUPPORT ESSENTIAL	PREMIUM SUPPORT ADVANCED
Critical Severity (A) Response Time	Best effort	2 hours	2 hours
Serious Severity (B) Response Time	Best effort	4 hours	4 hours
Common Severity (C) Response Time	Best effort	24 hours	24 hours
Support availability	7:00-18:00, business days only	365/24/7	365/24/7
Customer Contacts	Limited	Unlimited	Unlimited
Priority call queuing	–	✓	✓
Number of tickets eligible for premium treatment	–	Limited	Unlimited
Dedicated account manager	–	–	✓
Priority access to development teams	–	–	✓
Proactive Informative Services	–	–	✓
Deployment/Upgrade	–	–	✓
HealthCheck	–	–	✓

CUSTOMER CHALLENGES (PAIN POINTS)

- Resources
- Expertise
- Business continuity
- Product set-up
- Costs
- Procurement
- Compliance
- Heterogenous environment
- Time
- Complexity
- Learning curve

ESET SOLUTION TO CUSTOMER CHALLENGES

- Expertise
- Faster response
- Complexity managed
- Business continuity
- Resources allocated
- Reduced risk



Managed Detection and Response

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

ADDITIONAL RECOMMENDED SERVICES

ESET Threat Intelligence

Extend your security intelligence from local network to global cyberspace.

ESET Authorized Training Center

Online training platform for improving the skill-set of your sales force and customer care representatives.

ESET THREAT INTELLIGENCE DATA FEEDS

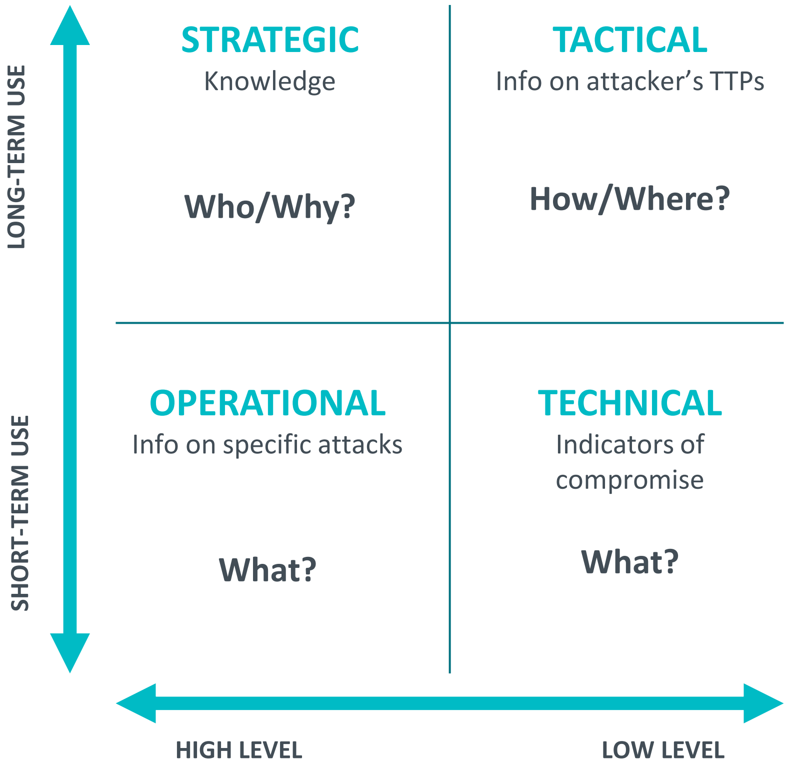
Provides real-time global knowledge gathered by ESET experts on targeted attacks, advanced persistent threats, zero-days and botnet activities.

Shared in the form of **data feeds**:

- **JSON and STIX** v2.0 formats
- Via **TAXII** server, updated several times every hour
- Indicators of Compromise (**IoCs**)
- **Out-of-the-box integrations** with Threat Intelligence Platforms

- **Botnet** Feed
- **Domain** Feed
- **URL** Feed
- **Malicious Files** Feed
- **IP** Feed
- **APT** Feed

ESET THREAT INTELLIGENCE
APT Reports PREMIUM



LONG-TERM USE

SHORT-TERM USE

STRATEGIC
Knowledge

Who/Why?

TACTICAL
Info on attacker’s TTPs

How/Where?

OPERATIONAL
Info on specific attacks

What?

TECHNICAL
Indicators of compromise

What?

HIGH LEVEL

LOW LEVEL

- Reports cover threat actors we track
- **Activity Summary Reports**
- **Technical Analysis Reports**
- **Monthly Overview Reports**
- WLS pre-publication access (where possible)
- IOCs available via MISP, STIX/TAXII
- YARA rules
- MITRE ATT&CK mapping
- Retrospective intelligence
- Access to analysts

SECURITY
DAYS

Ďakujem za pozornosť

Digital Security
Progress. Protected. & SME KONFERENCIE