



CYBERSECURITY
EXPERTS ON YOUR SIDE

Security is a mindset

Γιάννης Παυλίδης
Presales & Tech Support Manager






30 years of technology

The background is a dark, teal-toned digital landscape. On the left, several bright, glowing teal lines curve upwards and outwards, resembling a stylized wave or a data stream. These lines are composed of many smaller, parallel lines, giving them a textured, wireframe appearance. On the right, there is a complex, multi-layered structure that looks like a futuristic city or a data center. It features various geometric shapes, including cubes and rectangular blocks, some of which are illuminated with a bright teal light. The overall atmosphere is high-tech and futuristic, with a strong emphasis on digital connectivity and data flow.

Cutting Edge-Technology



UEFI Scanner



Exploit
Blocker



LiveGrid®
Protection



Network Attack
Protection




Botnet
Protection



Reputation & Cache



Ransomware
Shield



Advanced
Memory
Scanner



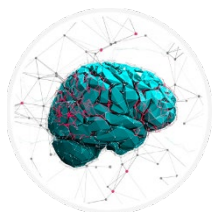
Script
Scanner
(AMSI)



In-product
Sandbox



DNA Detections

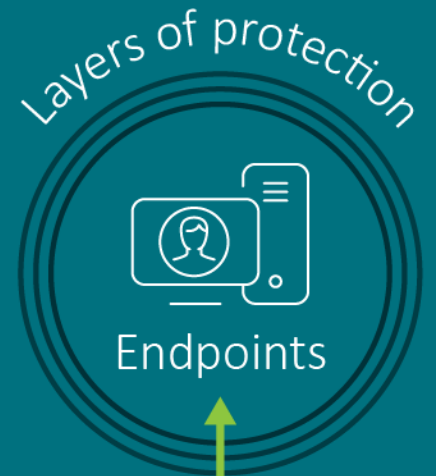
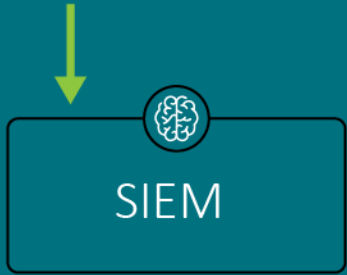


Machine
Learning





Cloud
Malware Scan

- PRE EXECUTION
- EXECUTION
- POST EXECUTION



Mail server

**ESET
ECOSYSTEM**

 Technology
 Product

And then we get a call..

- Κολλήσαμε ransomware
- Το ransomware χτύπησε τον ERP Server
- Το Antivirus δεν έκανε τίποτα
- Το Antivirus δεν ήταν καν εκεί
- Ο server δεν λειτουργεί πλέον

Let the search begin

- Ζητάμε logs από το μηχάνημα που δέχτηκε την επίθεση
- Ξεκινάμε την ανάλυση
- Η ανάλυση τελειώνει πολύ σύντομα

Login statistics:

User name	Remote failed Last	RmtFailCo... ▼
ADMINISTRATOR	21.01.2019 09:50:57	46.264
ADMIN	18.01.2019 17:04:55	10.021
Ndministrato	17.01.2019 15:10:35	7.570
Ndministr...	21.01.2019 10:30:27	7.525
USER	18.01.2019 17:19:26	2.479
TEST	18.01.2019 17:01:03	2.207
administrator	18.01.2019 10:27:30	1.684
SUPPORT	15.01.2019 12:13:09	1.629
SERVER	18.01.2019 17:13:22	1.581
BACKUP	17.01.2019 15:30:15	1.089
INFO	07.01.2019 17:52:02	1.078

Findings

- RDP 3389 on WAN - Firewall: Off
- Shared "C:" with Everyone: Write
- Critical MS Patches missing
- Antivirus without password protection

Isolated incidents?



71% of Ransomware Attacks Targeted Small Businesses in 2018
HealthITSecurity.com - 27 Mar 2019
Beazley researchers analyzed 3,300 ransomware attacks against their ... on RDP



FBI warns companies about hackers increasingly abusing RDP ...
ZDNet - 27 Σεπ 2018
RDP stands for the Remote Desktop Protocol, a proprietary ... on attackers either
guessing login credentials (via a brute-force attack) or by ...
FBI: RDP attacks are still on the rise
CSO Australia - 27 Σεπ 2018

Ransomware To Delete Duplicate Files

exploits or brute-force tactics. In 2018, SamSam was
ities in remote desktop protocols ...



Ransomware Hits Garage of Canada
BleepingComputer - 28 Mar 2019
The attack happened on Tuesday, but the
computers running RDP and try to brute-



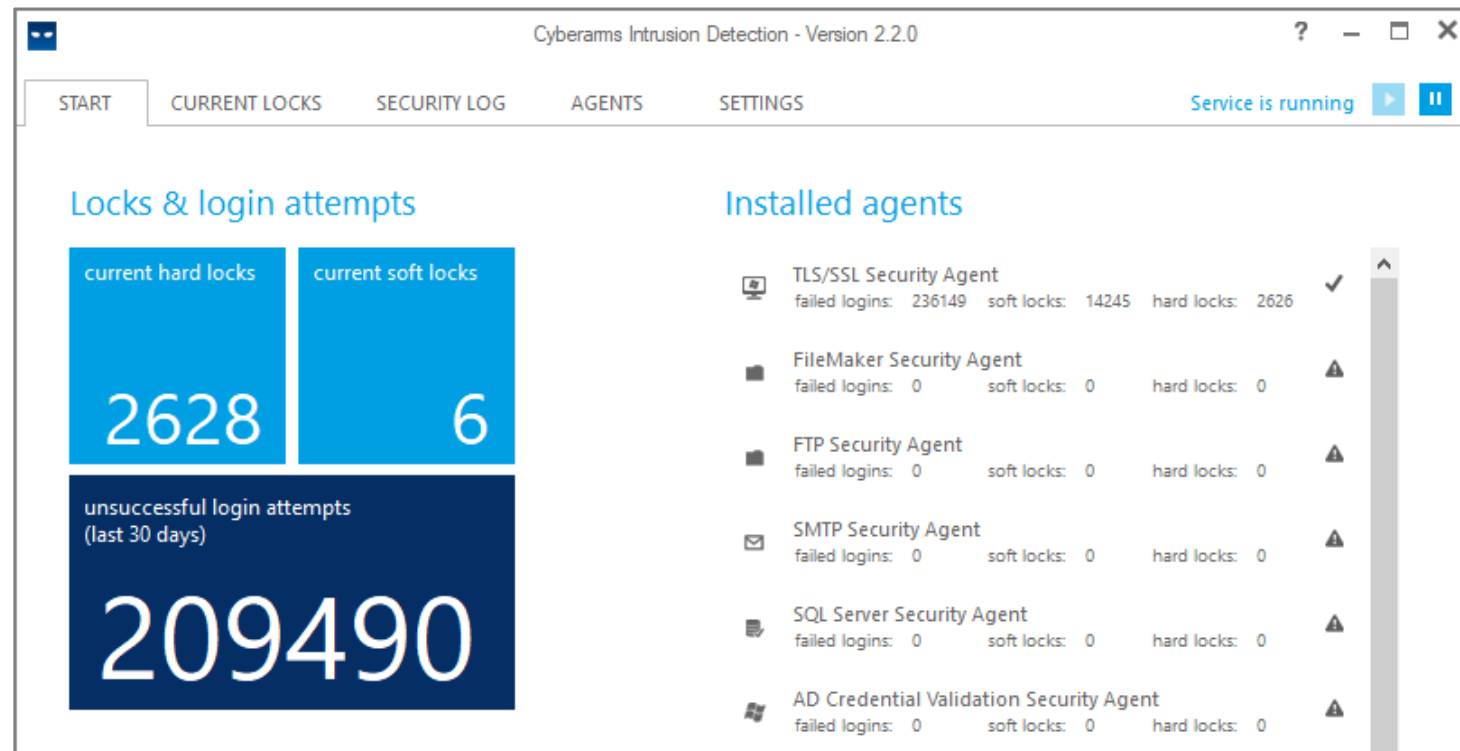
Experience an RDP attack? It's your fault, not Microsoft's
CSO Online - 7 Νοε 2018
You don't need to put a VPN around RDP to protect it. ... like CrySis, that attempt
brute-force guessing attacks against accessible RDP services.

... Increase...

to brute force

ak password to get access," says Beazley. "Businesses ...

But, nobody is going to target us!



Think Security!

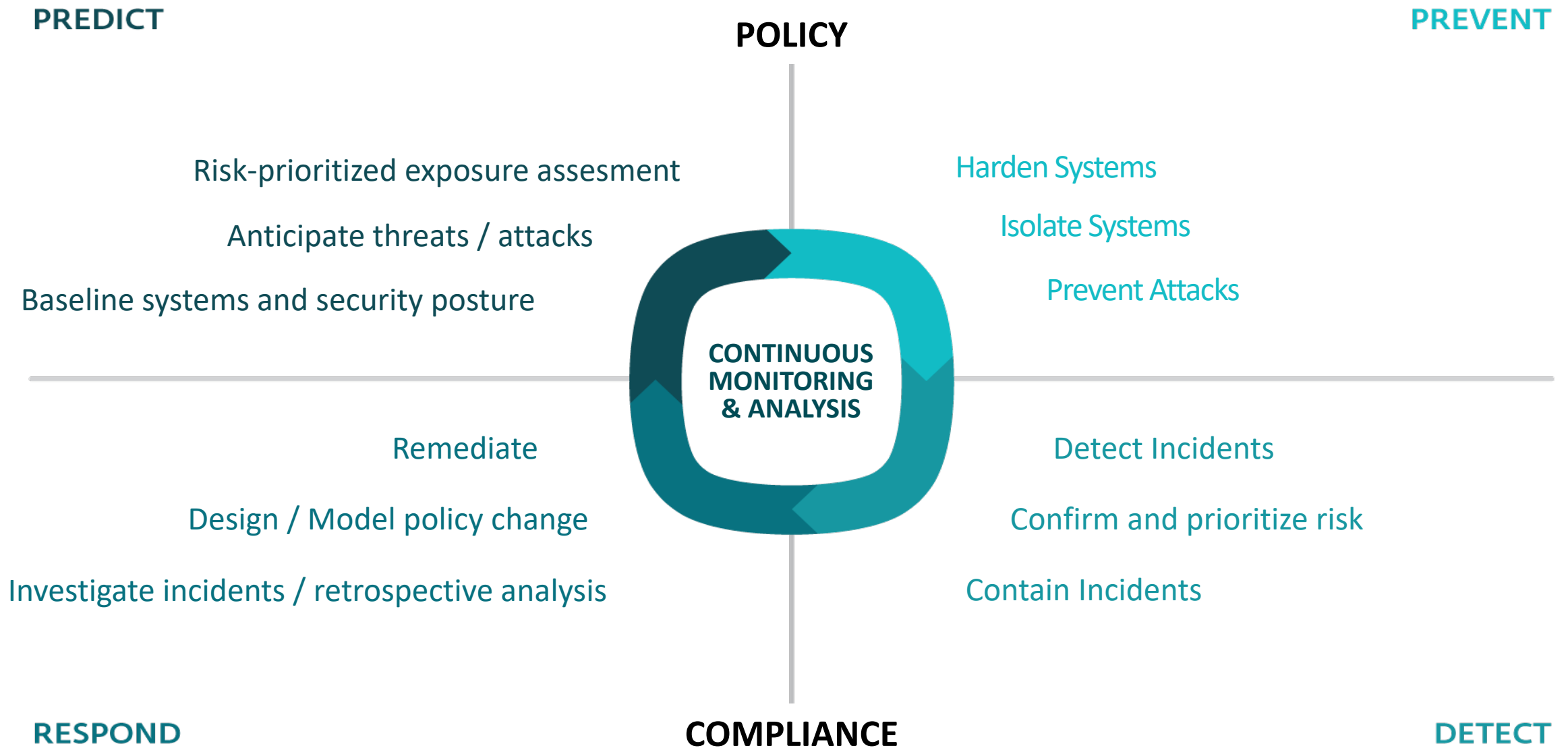
- Server has a “key”
- Attackers have millions of keys
- Attackers will find our key
- Key is only *one* layer of security, what's next?

Find the balance, ask yourself

- I need RDP just for me, should I enable Firewall?
- Can I use a VPN connection?
- I have a Terminal Server, should I use MFA?
- Can I protect my Antivirus with a password?
- Does my Backup work?
- Should I pay ransom?

..but not only for RDP!

Adaptive Security Architecture



How ESET fits in Adaptive Security Architecture

PREDICT

POLICY

PREVENT

ESET Endpoint Security

ESET Virtualization Security

ESET Security Management Center

ESET Secure Authentication

ESET Endpoint Encryption

CLOSING
THE LOOP

ESET Threat Intelligence
ESET Virus Radar
WeLive Security

ESET Security Management Center

NEW ESET Enterprise Inspector

NEW ESET Dynamic Threat Defense

RESPOND

COMPLIANCE

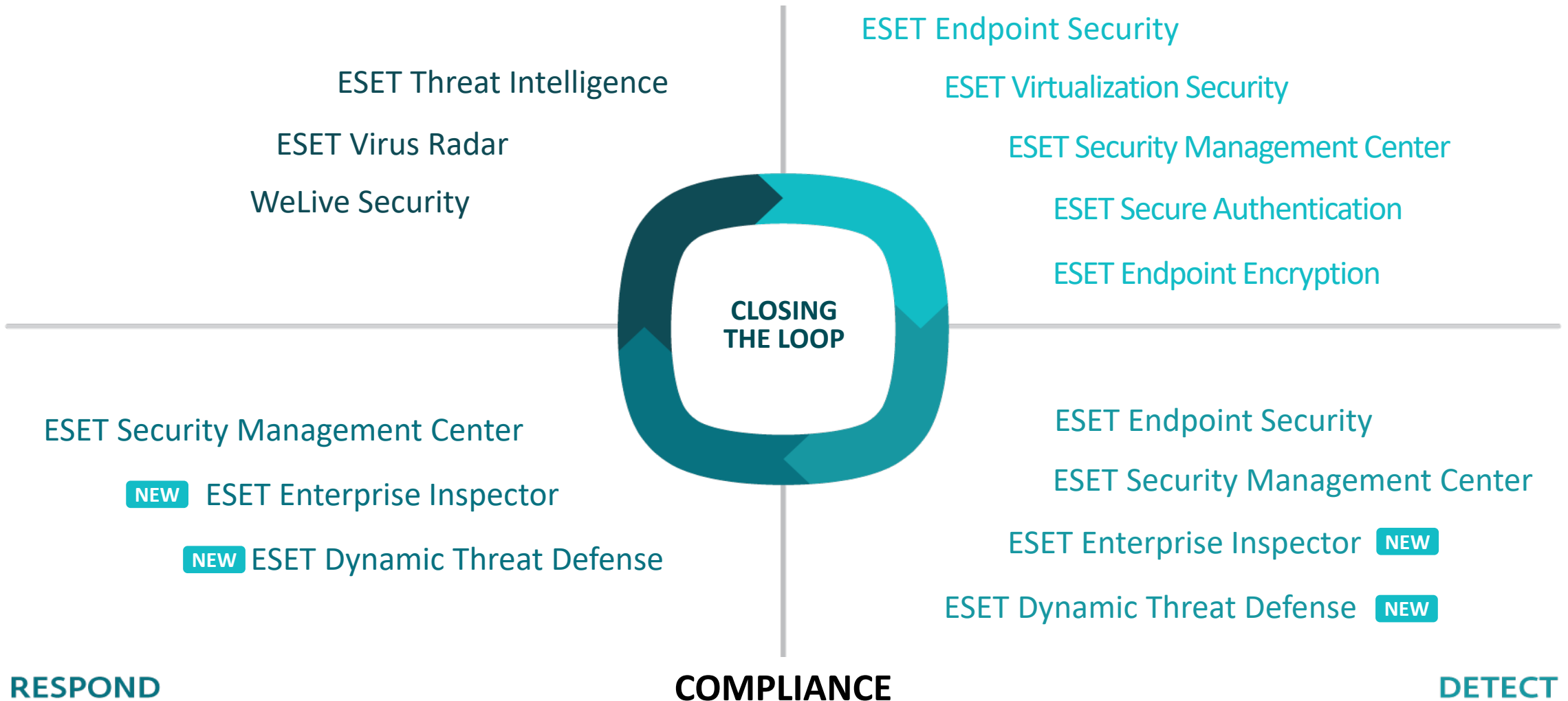
ESET Endpoint Security

ESET Security Management Center

ESET Enterprise Inspector **NEW**

ESET Dynamic Threat Defense **NEW**

DETECT





CYBERSECURITY
EXPERTS ON YOUR SIDE

Thank you!

Γιάννης Παυλίδης
ESET Hellas