CHECK POINT

Threat Prevention in the Age of AI

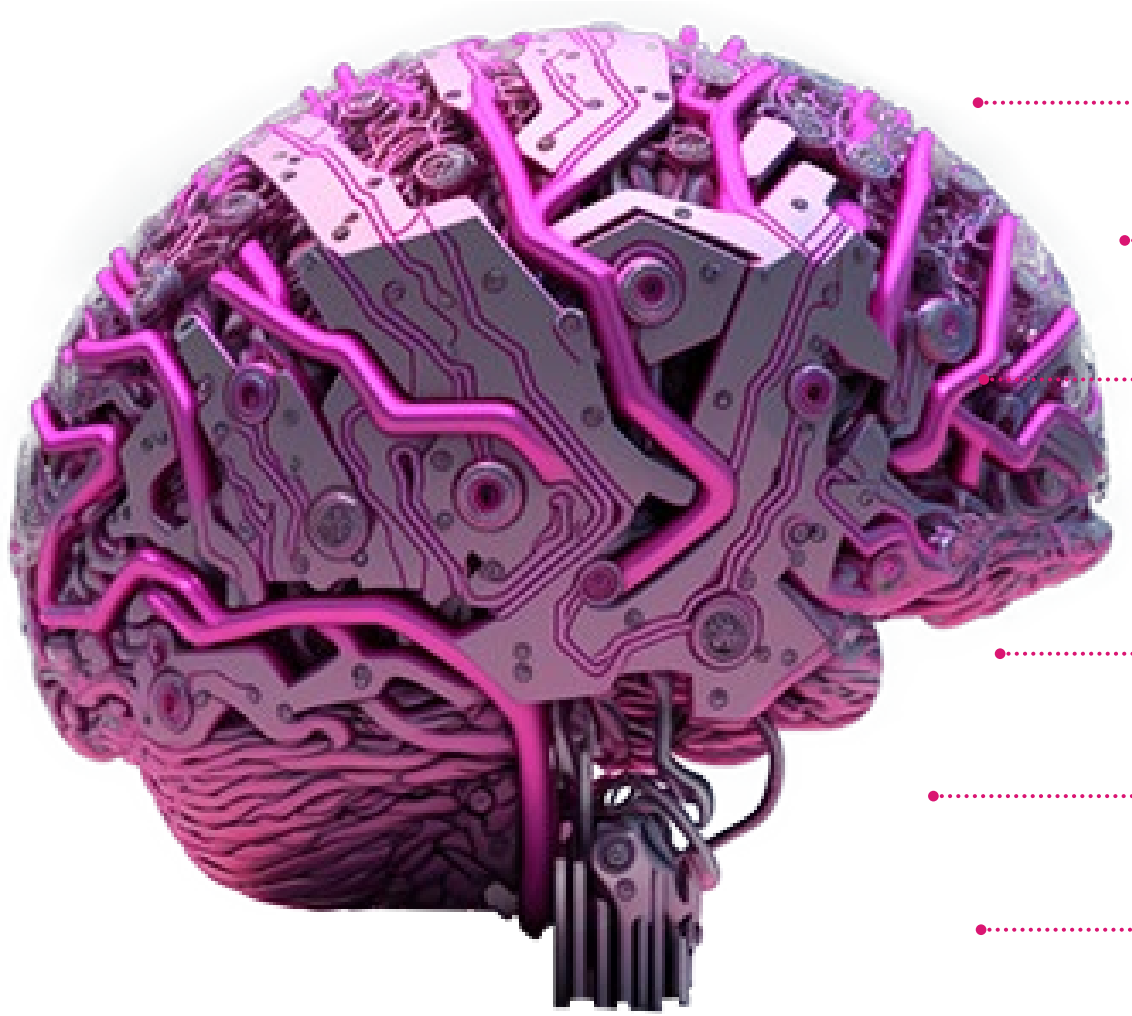
5th InfoCom Security Cyprus 2023

Fanis Tsomis | Security Engineer, Greece & Cyprus

YOU DESERVE THE BEST SECURITY

COLLABORATIVE SECURITY - THREATCLOUD AI

AI is all about your data



Big data threat intelligence:

2,000,000,000
Websites and files inspected

73,000,000
Full content emails

30,000,000
File emulations

20,000,000
Potential IoT devices

2,000,000
Malicious indicators

1,500,000
Newly installed mobile apps

1,000,000
Online web forms

Counted **DAILY!**

Big data threat intelligence

Analyzing big data telemetry and millions of IOCs every day

Check Point's customers & products

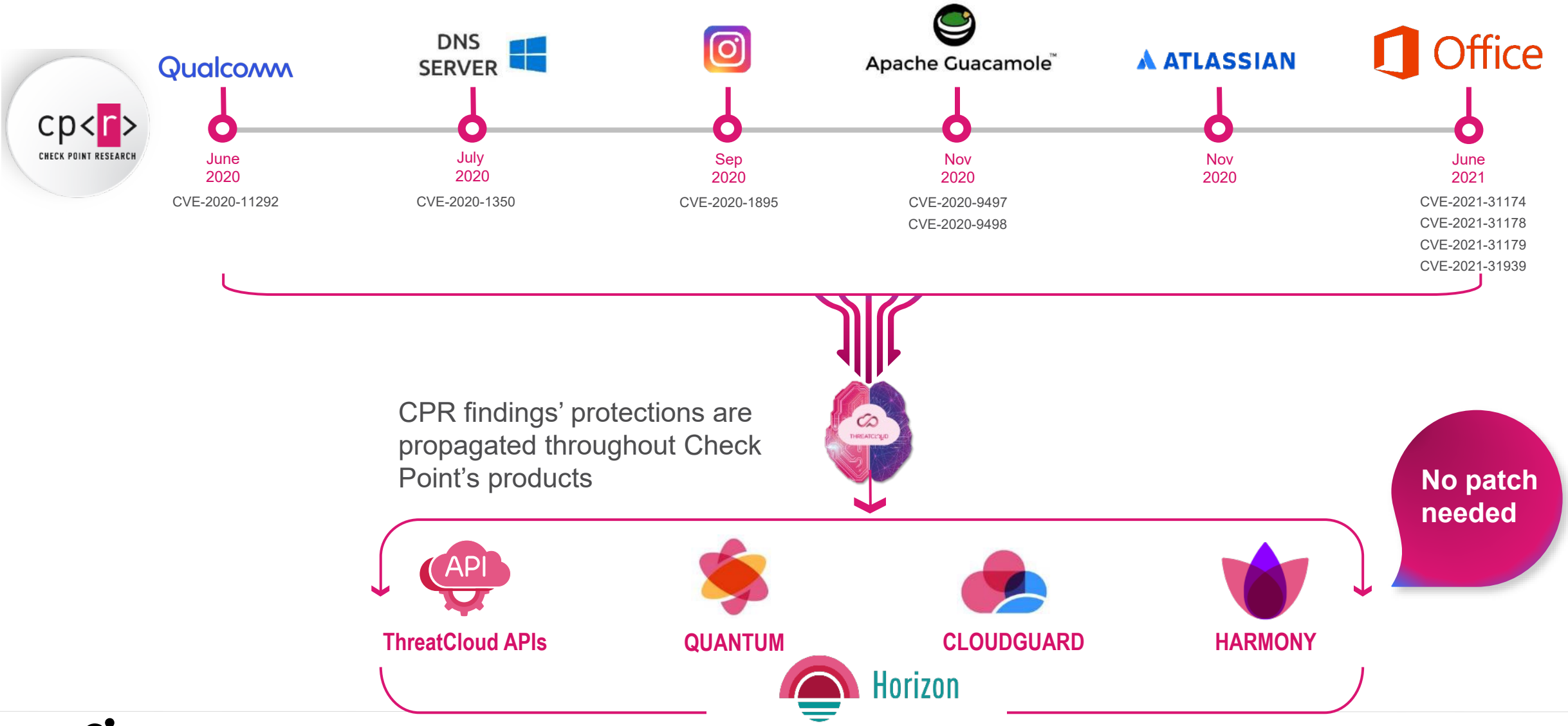
- **150,000** Connected networks
- **Millions of** Endpoint devices
- **2,000,000,000** Websites and files inspected daily

- **Dozens of external feeds and crawling the www and social media**

- **Unique ML algorithms detecting 650,000 suspicious domains daily**

Patented

Instant protection from the most significant unknown software vulnerabilities



Best security with most innovative AI and Deep Learning technologies

Zero-Day Phishing
New Software Blade

4 X More attacks blocked compared to **Signature** based technologies

40% Zero-phishing attacks **MISSED** by other **AI** based technologies

Advanced DNS Security
New Software Blade

5 X More attacks blocked compared to **Signature** based technologies

47% Zero-DNS attacks **MISSED** by other **AI** based technologies

Blocking never-seen-before Phishing Attacks

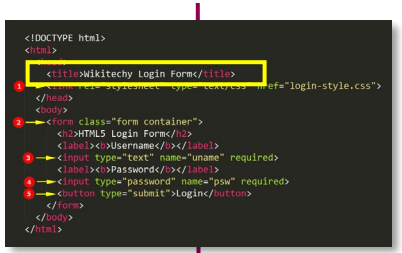
PATENTED

AI-based analysis of 300 phishing indicators in email & web

- IP REPUTATION
- ✓ URL REPUTATION
- SUBJECT CONTEXT
- URL EMULATION
- ✓ HTML INSPECTION
- NLP
- DOMAIN REPUTATION
- ✓ LOOKALIKE FAVICON
- ✓ BRAND IMPERSONATION

+300 indicators

#1 GATEWAY WEB INSPECTION

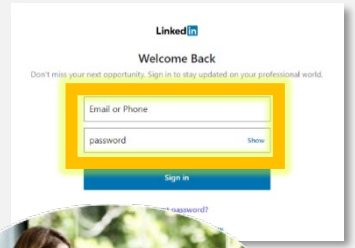


#2 CHECK POINT'S INJECTION

GET

RESPONSE

#3 BROWSER INSPECTION (BY INJECTED CODE)

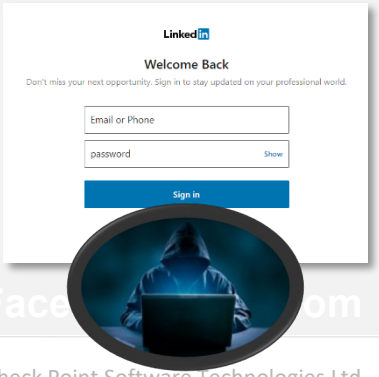


GET

RESPONSE

Quantum
Secure the Network

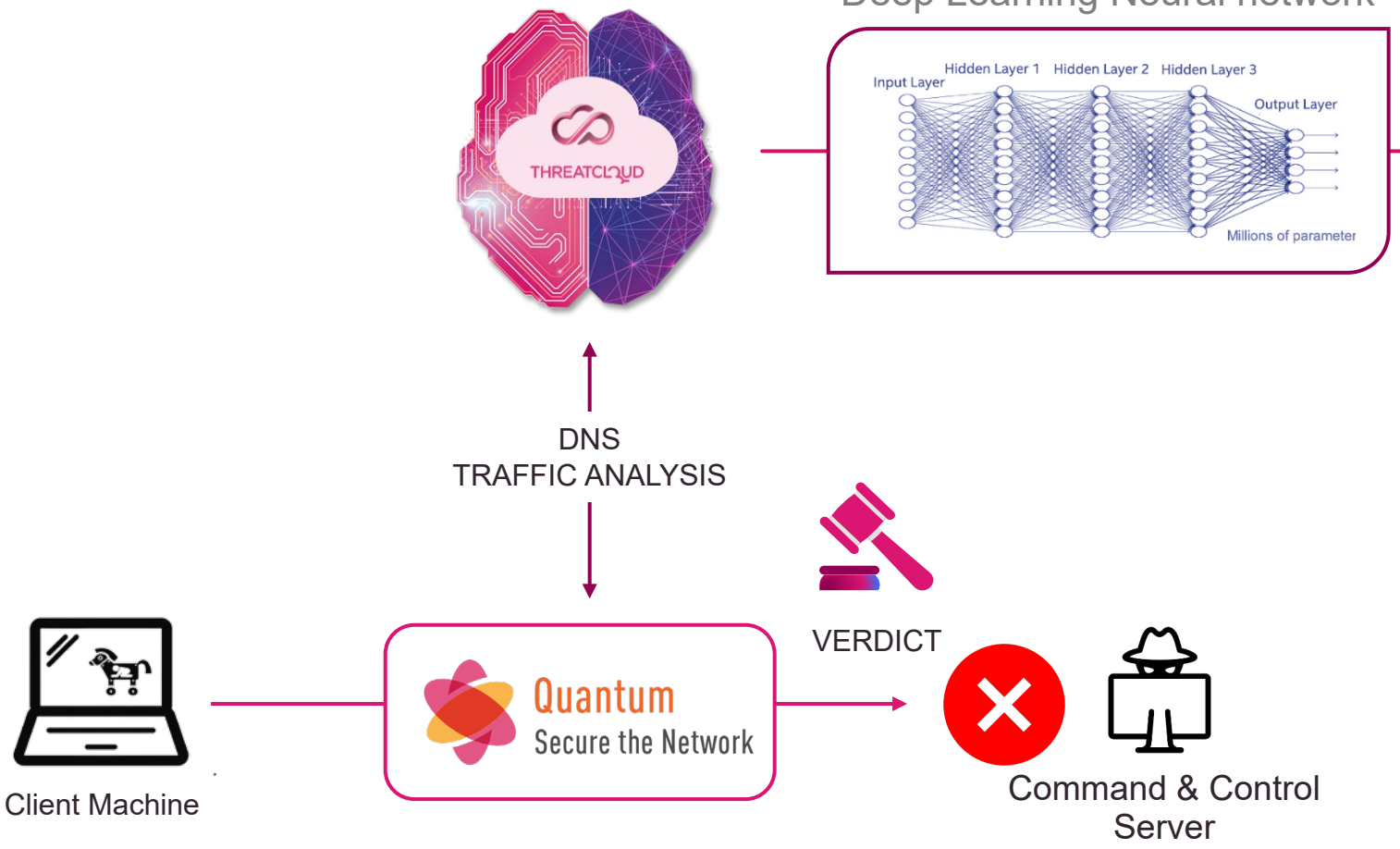
PHISHING SITE
LinkedInscam.com



Prevents 5X more sophisticated DNS attacks

Block C&C communications and Data theft with Deep Learning engines

PATENTED



#1 DGA (Domain Generation Algorithm)

#2 DNS Tunneling

```
6a57jk2ba1d9keg15cbg.appsync-api.eu-west-1.avsvmcloud.com
7sbvaemscs0mc925tb99.appsync-api.us-west-2.avsvmcloud.com
gq1h856599gqh538acqn.appsync-api.us-west-2.avsvmcloud.com
ihvpgv9psvq02ffo77et.appsync-api.us-east-2.avsvmcloud.com
k5kcubuassl3alrf7gm3.appsync-api.eu-west-1.avsvmcloud.com
mhdosoksaccf9sni9icp.appsync-api.eu-west-1.avsvmcloud.com
```

```
f5534496-1a85-4844-8bc0-e9edc537ea40.server-26.deeponlines.com
f5534496-1a85-4844-8bc0-e9edc537ea40.server-34.deeponlines.com
f5534496-1a85-4844-8bc0-e9edc537ea40.server-5.deeponlines.com
f5534496-1a85-4844-8bc0-e9edc537ea40.server-98.deeponlines.com
f5534496-1a85-4844-8bc0-e9edc537ea40.server-73.deeponlines.com
f5534496-1a85-4844-8bc0-e9edc537ea40.server-82.deeponlines.com
f5534496-1a85-4844-8bc0-e9edc537ea40.server-15.deeponlines.com
f5534496-1a85-4844-8bc0-e9edc537ea40.server-59.deeponlines.com
```

COMPLETE SECURITY OPERATIONS AS A SERVICE
WITH PREVENTION-FIRST APPROACH TO MDR

PREVENTION FOCUSED

Best practices to improve defenses and prevent future attacks

SIMPLICITY

24*7x365 service by our elite experts

ELEVATE SECURITY

Advanced threat prevention powered by AI-based analytics

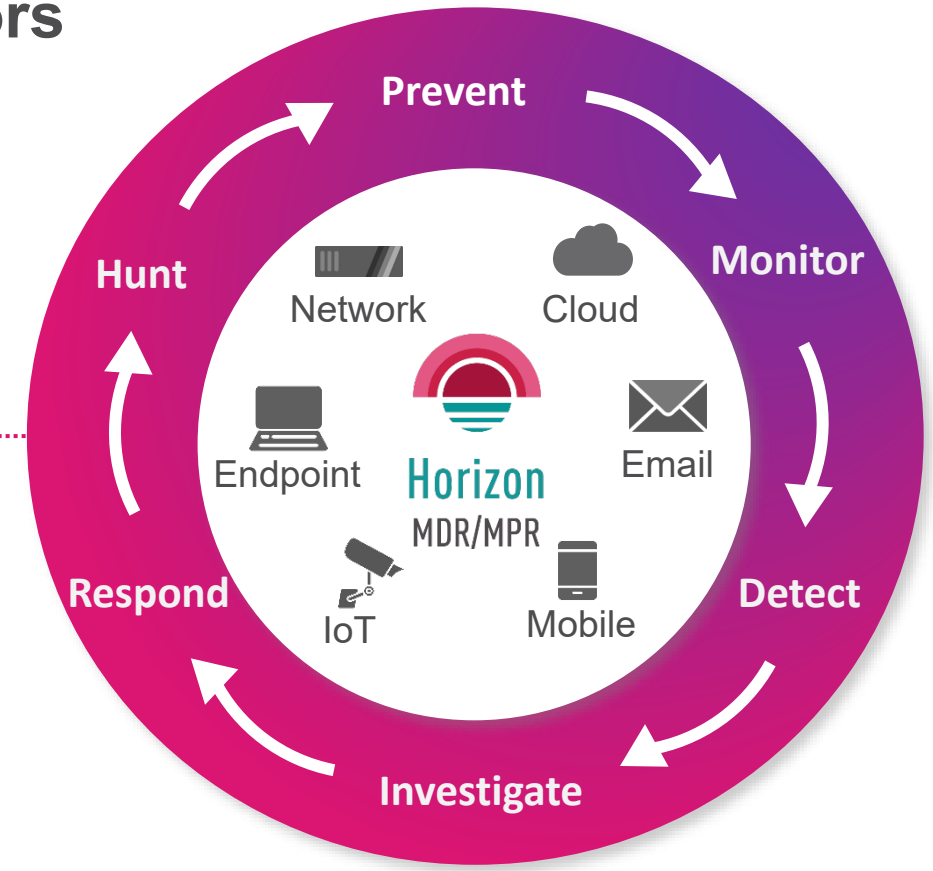
ONE SOLUTION

Prevent, monitor, detect, investigate, and remediate attacks

End-to-end Security Operations Service

One solution across all attack vectors

- Prevent threats and attacks
- Full-cycle investigation
- Automated remediation



AI TECHNOLOGY
Identify and block threats

BIG DATA THREAT INTELLIGENCE
Most recent IoCs

AI-BASED TECHNOLOGIES LEVERAGED BY THREATCLOUD

40+ engines across different security functionality

Infected hosts detection
Sandbox static analysis executables
Sandbox static analysis documents
Sandbox static analysis macros
Sandbox dynamic analysis

Email static analysis
Network zero-phishing detection
Mobile zero-phishing detection
Anti-Phishing AI engine
HTML body NLP

DNS Tunneling
DNS Slow tunneling
DGA Domain Generation Algorithm

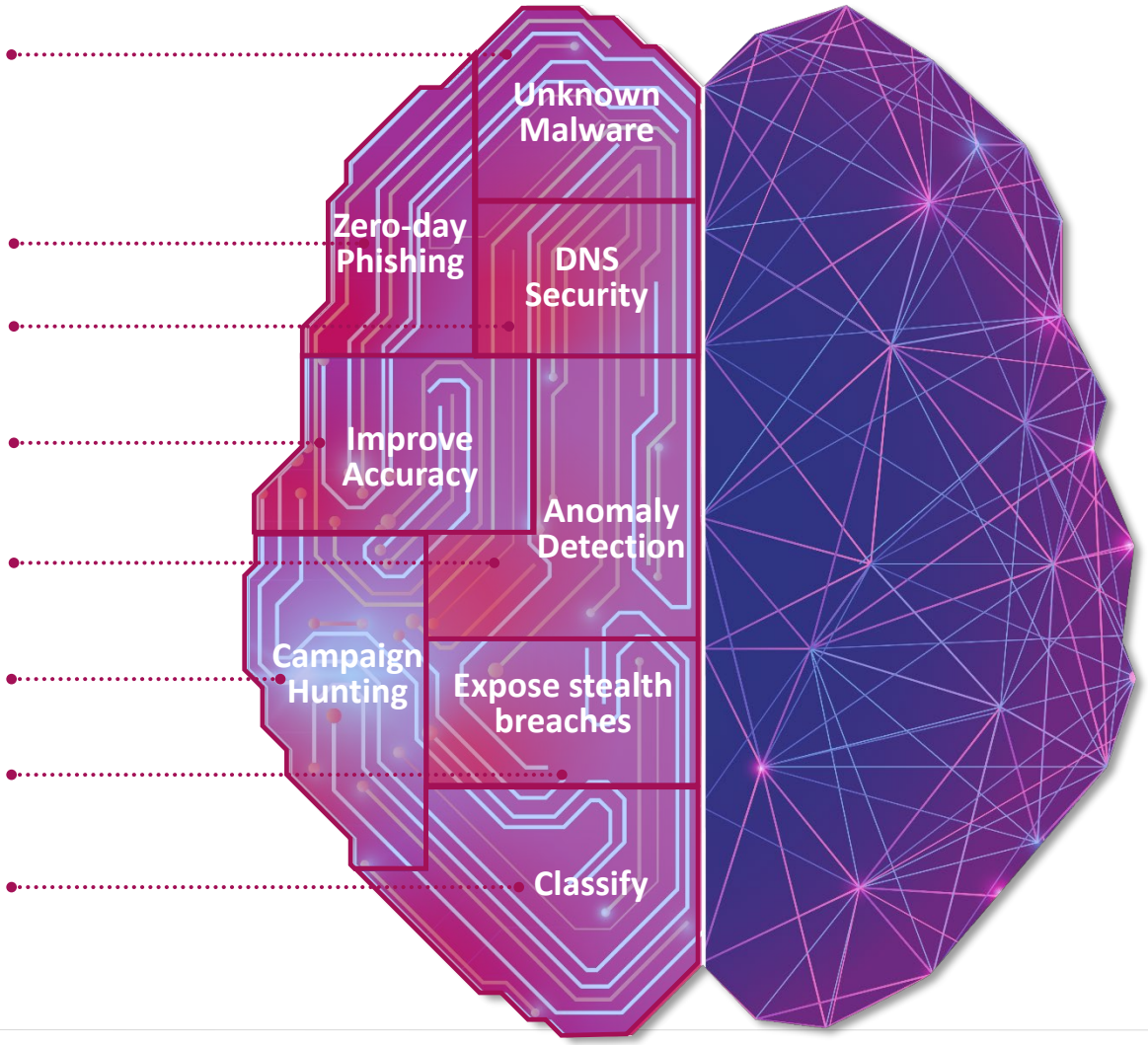
Network AI engines aggregator
Mobile AI engines aggregator
Machine validated signature

Cloud networks anomaly detection
XDR/XPR user behavior analysis
SSH tunneling

ThreatCloud Campaign Hunting

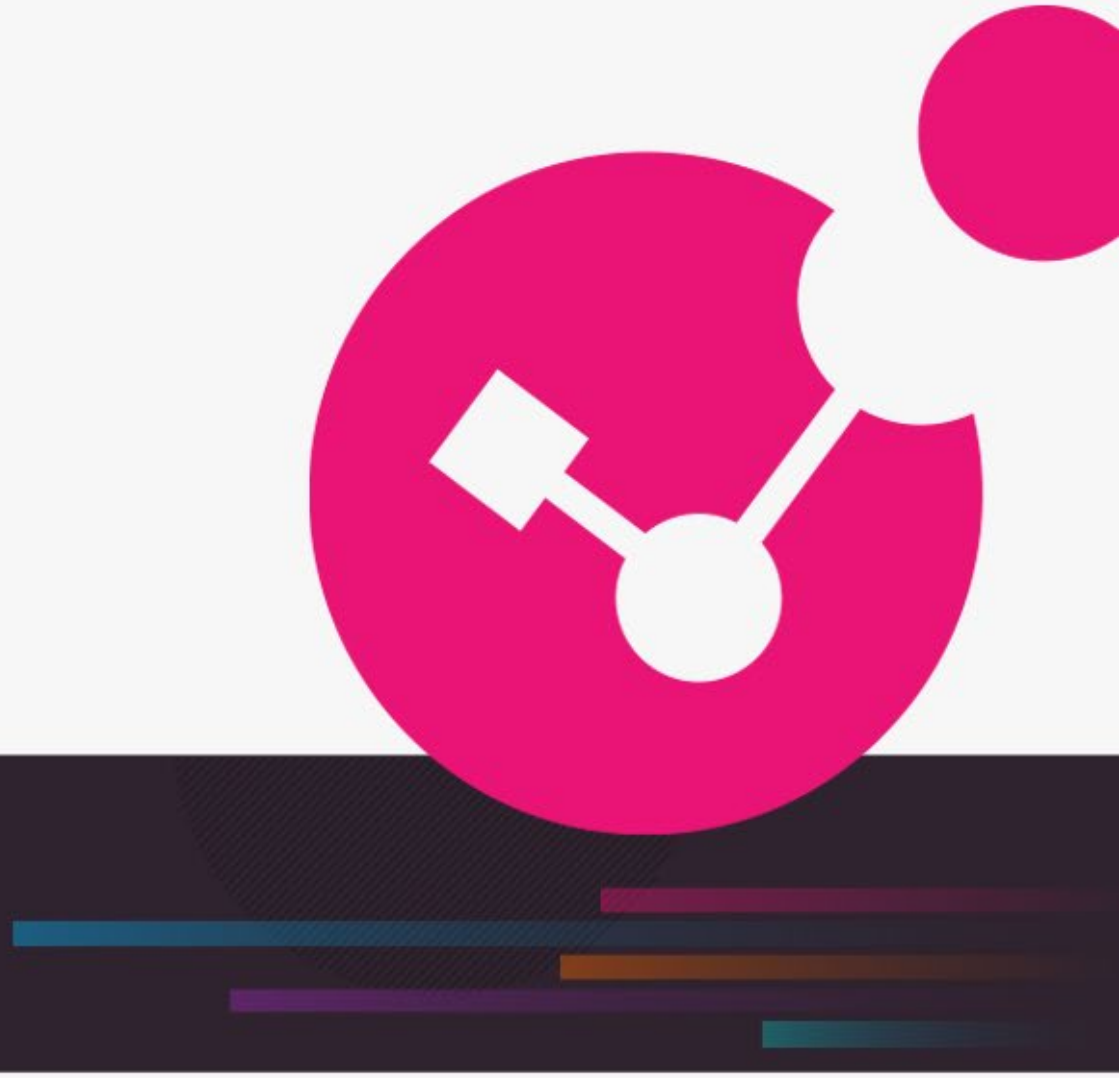
Analyst Mind
Malicious activity detection

Documents meta classifier Vectorization family classifier
XDR/XPR incidents aggregation
ML Similarity Model
MRAT Classifier
IP Port



CHECK POINT™

Thank you!



YOU DESERVE THE BEST SECURITY