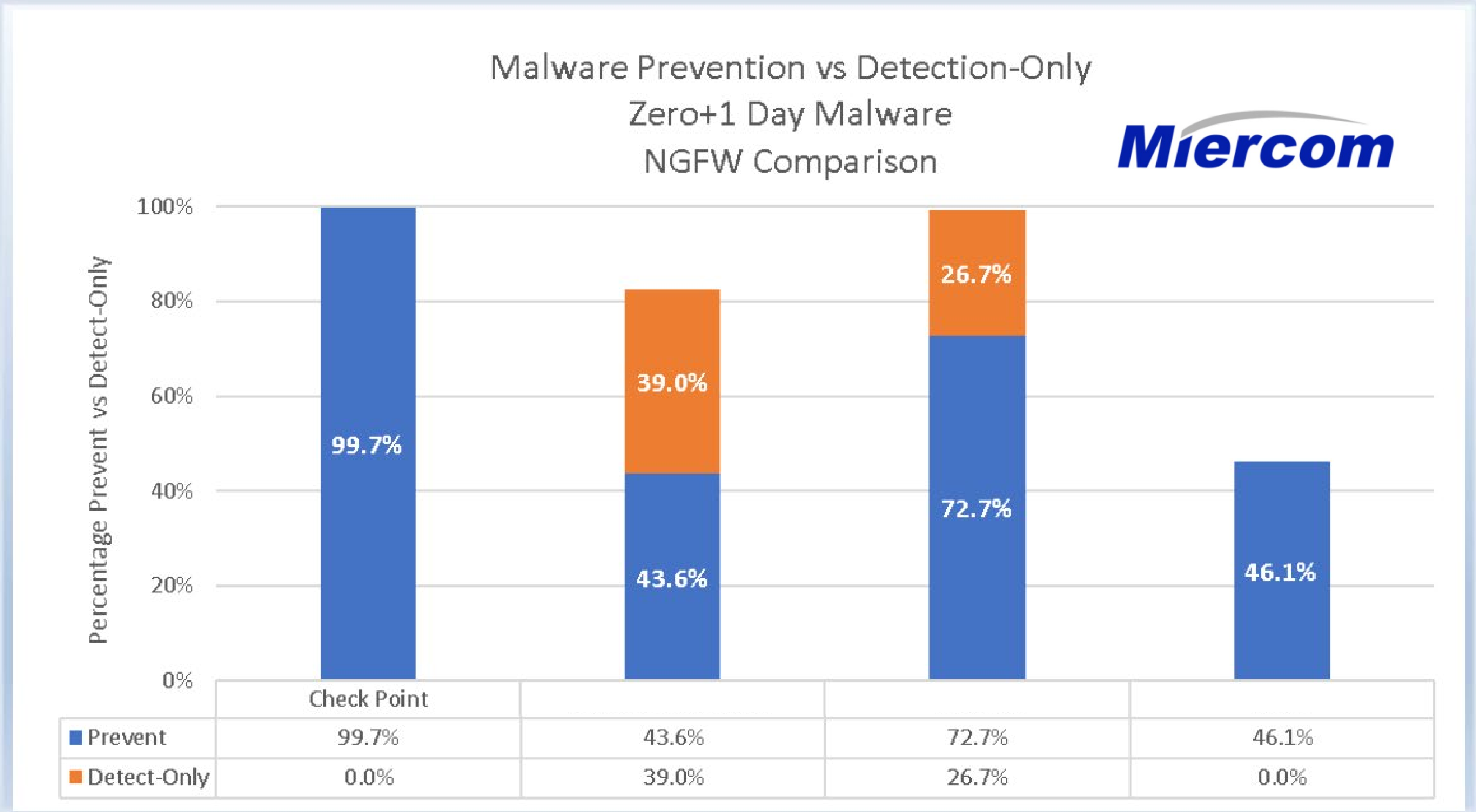
CHECK POINT™

# Leveraging AI in Threat Prevention

13th InfoCom Security 2023

Fanis Tsomis | Security Engineer, Greece & Cyprus

YOU DESERVE THE BEST SECURITY

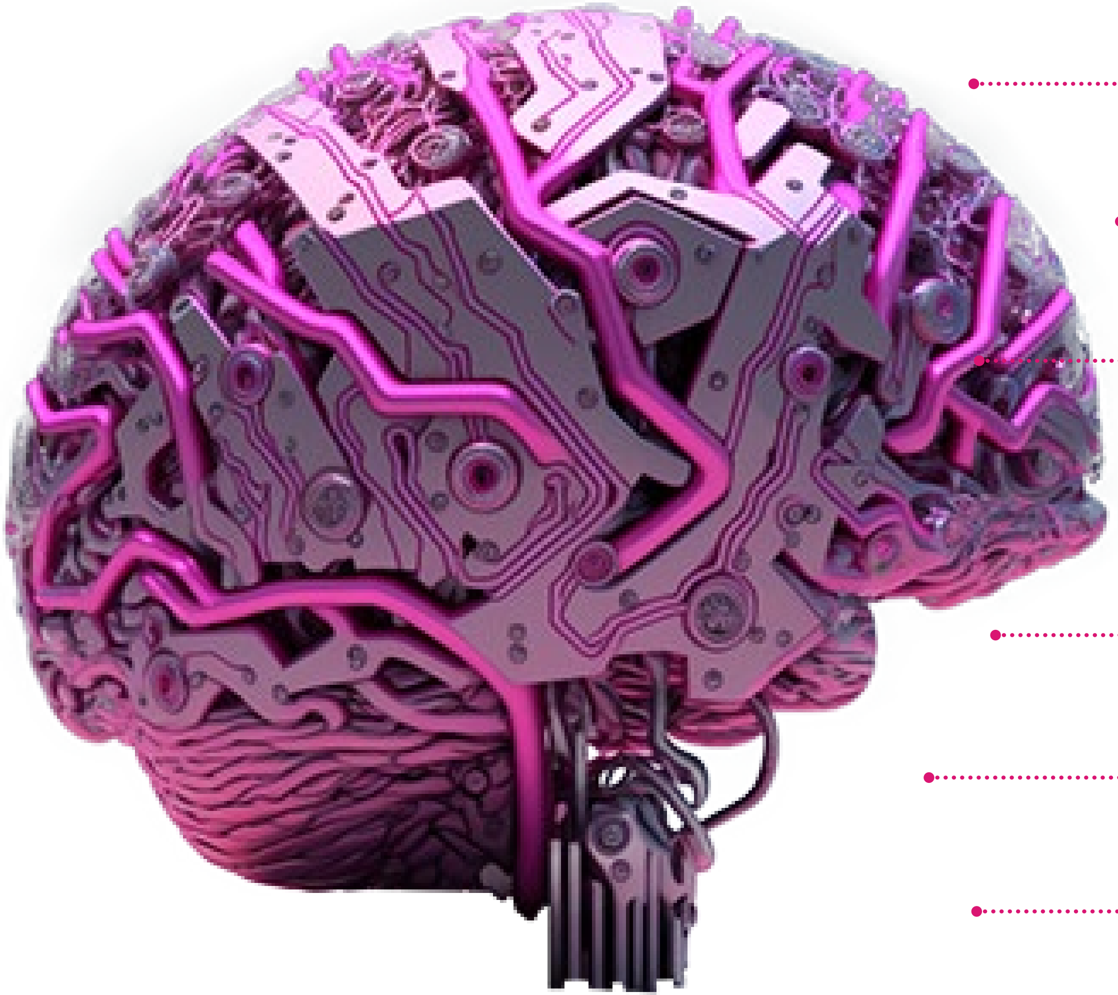


| | Check Point | | | |
|---|---|---|---|---|
| 🟦 Prevent | 99.7% | 43.6% | 72.7% | 46.1% |
| 🟧 Detect-Only | 0.0% | 39.0% | 26.7% | 0.0% |

NGFW Firewall Security Benchmark 2023

# 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
THREATCLOUD
LIVE CYBER THREAT MAP
9,105,119 ATTACKS ON THIS DAY
DON'T WAIT TO BE ATTACKED PREVENTION STARTS NOW
Malware
Phishing
Exploit

**Check Point's customers & products**

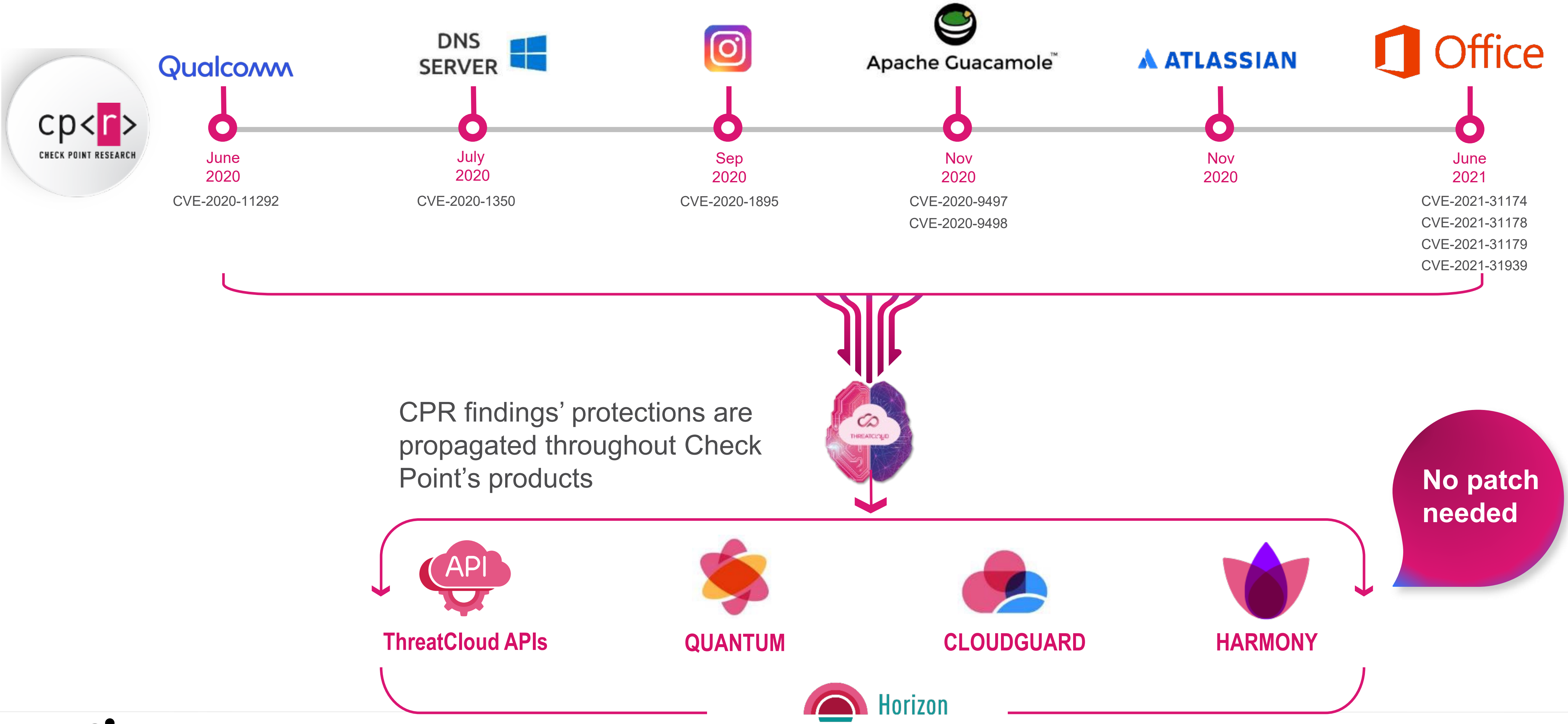
- **150,000 Connected networks**
- **Millions of Endpoint devices**
- **2,000,000,000 Websites and files inspected daily**

**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



June 2020
CVE-2020-11292

July 2020
CVE-2020-1350

Sep 2020
CVE-2020-1895

Nov 2020
CVE-2020-9497
CVE-2020-9498

Nov 2020

June 2021
CVE-2021-31174
CVE-2021-31178
CVE-2021-31179
CVE-2021-31939

CPR findings' protections are propagated throughout Check Point's products

No patch needed

ThreatCloud APIs

QUANTUM

CLOUDGUARD

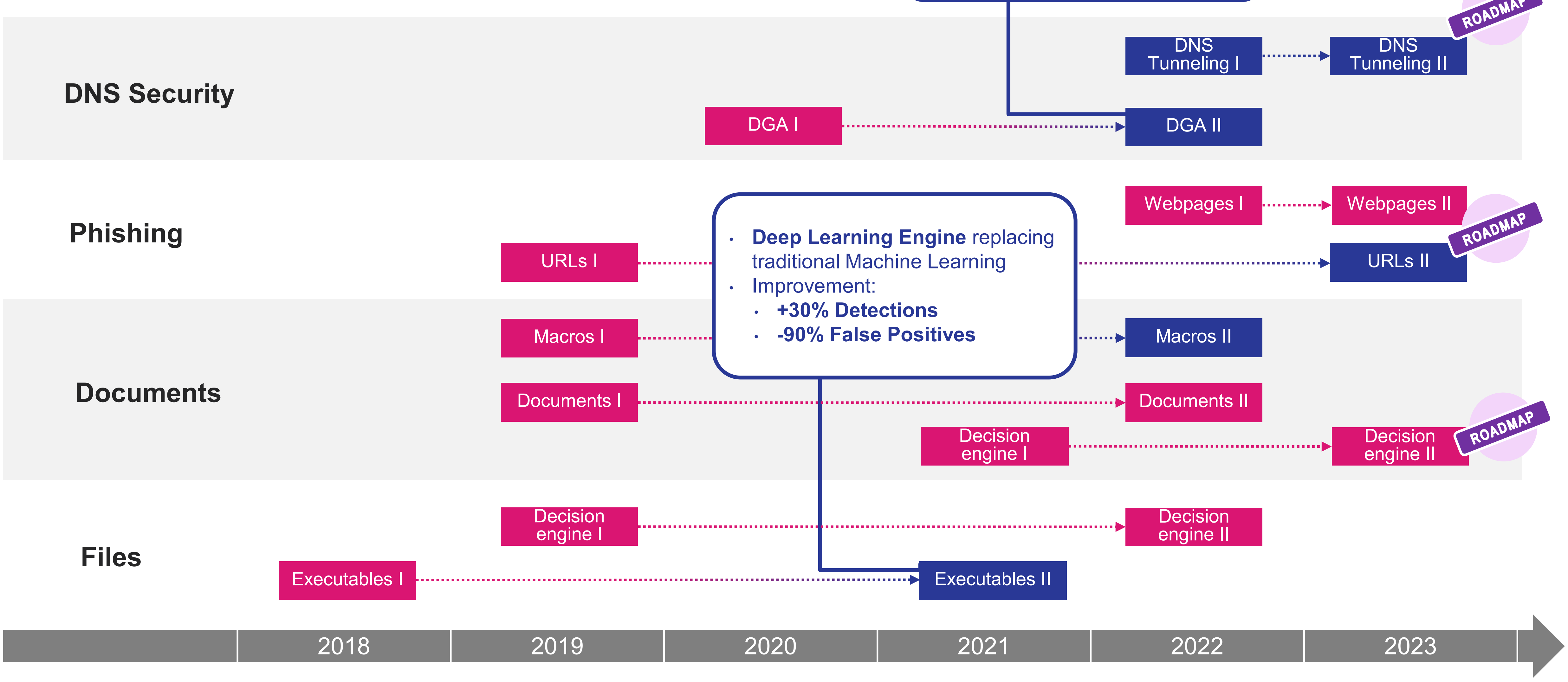
HARMONY

Unified management & security operations

# AI Technology evolution

## From **Classic Machine Learning** to **Deep Learning**

- **Deep Learning Engine** replacing semi-automated AI classification
- Improvement:
  - **+47% Detections**



DNS Security

DGA I → DGA II

DNS Tunneling I → DNS Tunneling II ROADMAP

Phishing

URLs I → URLs II ROADMAP

Webpages I → Webpages II

- **Deep Learning Engine** replacing traditional Machine Learning
- Improvement:
  - **+30% Detections**
  - **-90% False Positives**

Documents

Macros I → Macros II

Documents I → Documents II

Decision engine I → Decision engine II ROADMAP

Files

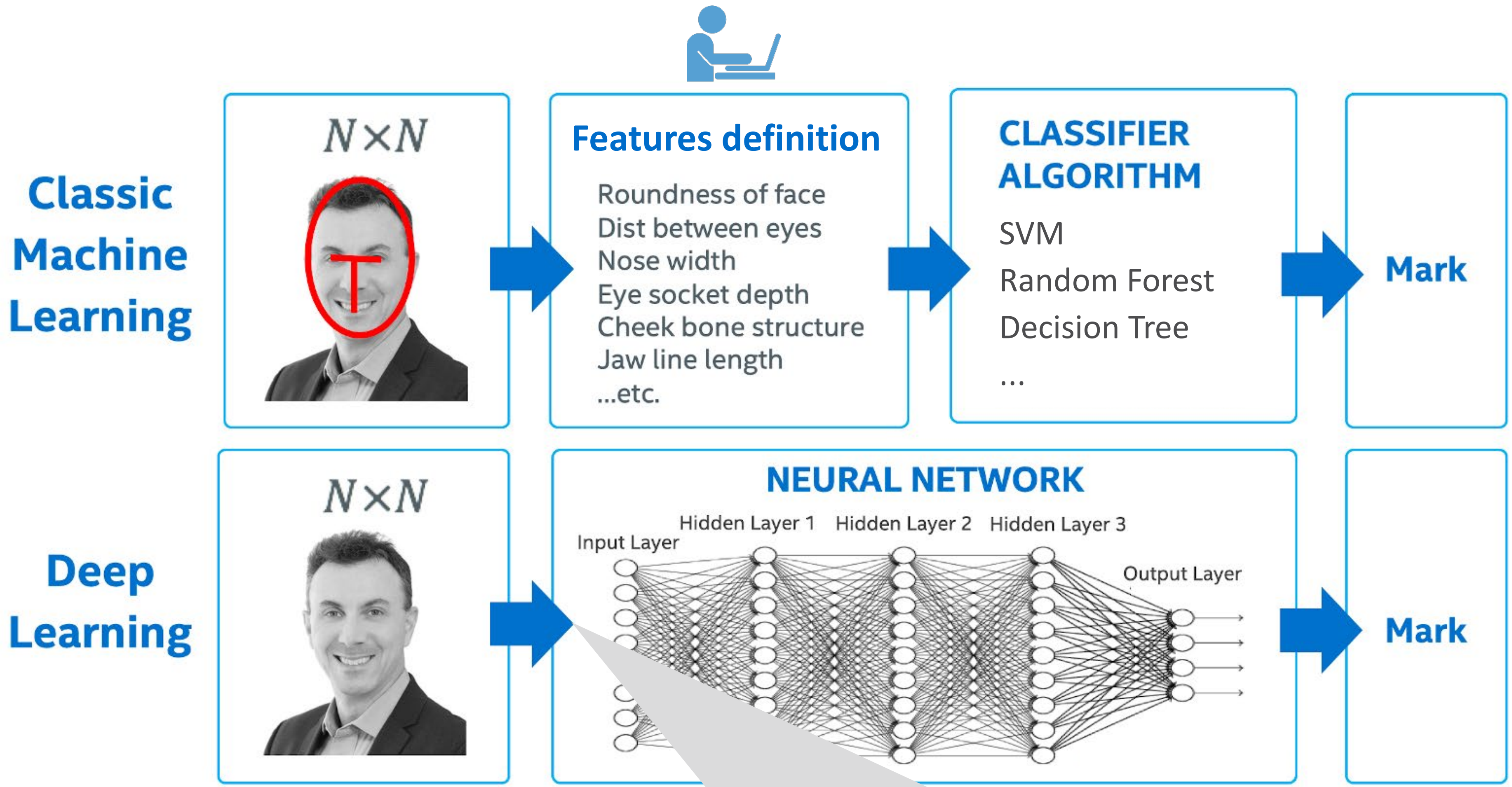
Decision engine I → Decision engine II

Executables I → Executables II

2018 2019 2020 2021 2022 2023

# BETTER PREVENTION WITH CUTTING-EDGE TECHNOLOGIES

## Classic Machine Learning vs. Deep Learning



**Classic Machine Learning**

$N \times N$

**Features definition**

Roundness of face
Dist between eyes
Nose width
Eye socket depth
Cheek bone structure
Jaw line length
...etc.

**CLASSIFIER ALGORITHM**

SVM
Random Forest
Decision Tree
...

**Mark**

**Deep Learning**

$N \times N$

**NEURAL NETWORK**

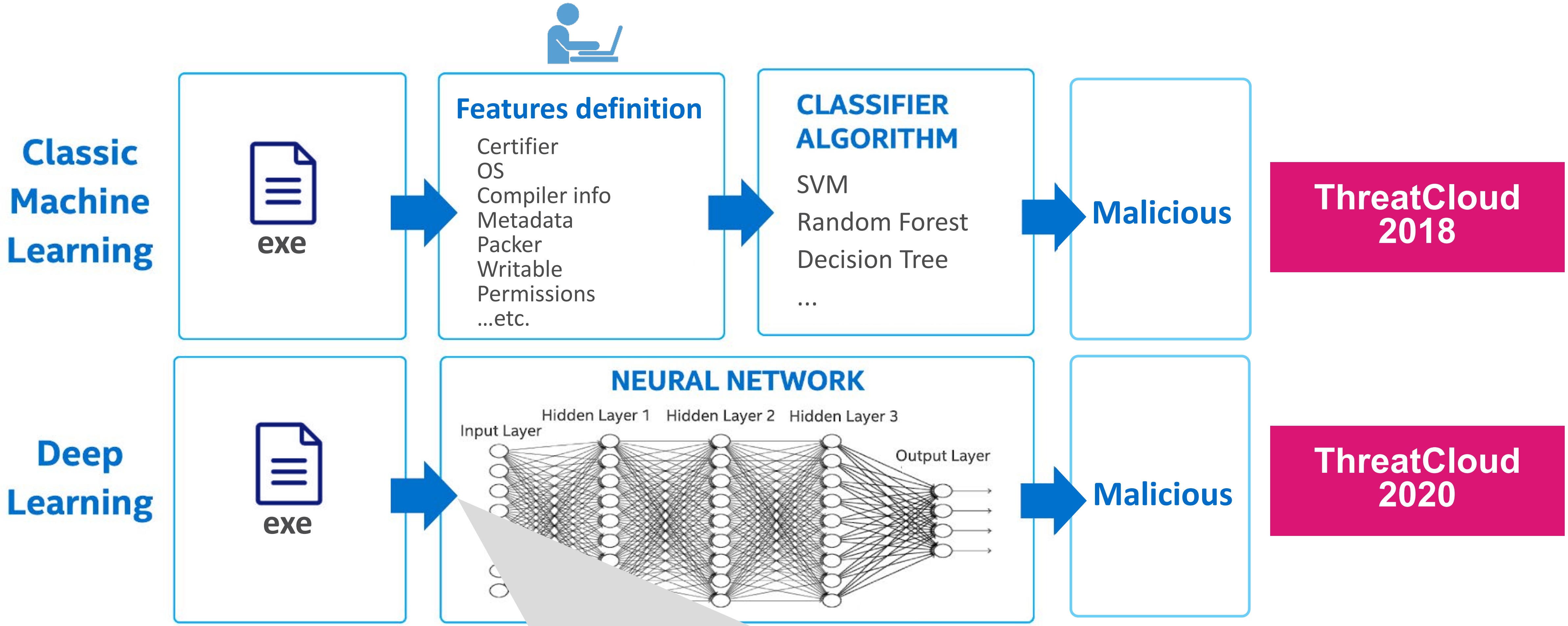
**Mark**

All **image pixels** are processed == higher accuracy

* Source: Intel, May 2020

# BETTER PREVENTION WITH CUTTING-EDGE TECHNOLOGIES

## Classic Machine Learning vs. Deep Learning



**Classic Machine Learning**

exe

**Features definition**

Certifier
OS
Compiler info
Metadata
Packer
Writable
Permissions
...etc.

**CLASSIFIER ALGORITHM**

SVM
Random Forest
Decision Tree
...

**Malicious**

**ThreatCloud 2018**

**Deep Learning**

exe

**NEURAL NETWORK**

**Malicious**

**ThreatCloud 2020**

All **file bytes** are processed == **30% Better** detection rate
**90% Less** false positives

* Source: Intel, May 2020

# Best security with most innovative AI and Deep Learning technologies

Quantum
Cyber Security Platform
Titan release
CHECK POINT™

## Zero-Day Phishing
**New** Software Blade

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

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

## Advanced DNS Security
**New** Software Blade

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

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

# Blocking never-seen-before Phishing Attacks

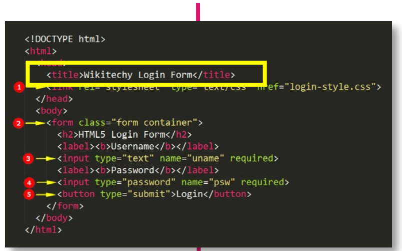
PATENTED

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



```
<!DOCTYPE html>
<html>
  <head>
    <title>Wikitechy Login Form</title>
1 → <link rel="stylesheet" type="text/css" href="login-style.css">
  </head>
  <body>
2 → <form class="form container">
      <h2>HTML5 Login Form</h2>
      <label><b>Username</b></label>
3 →   <input type="text" name="uname" required>
      <label><b>Password</b></label>
4 →   <input type="password" name="psw" required>
5 →   <button type="submit">Login</button>
    </form>
  </body>
</html>
```

#3 BROWSER INSPECTION (BY INJECTED CODE)

#2 CHECK POINT'S INJECTION

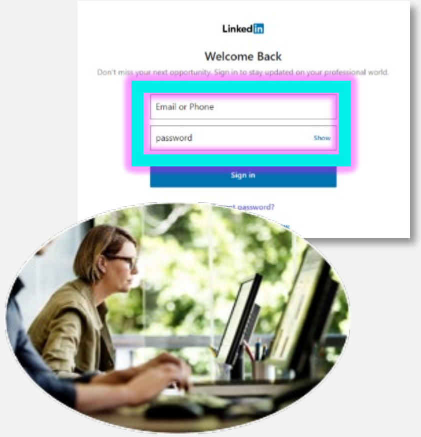
GET

RESPONSE

```
document.getElementById(div).
else if (i==2)
{
    var atpos=inputs[i].indexOf("@");
    var dotpos=inputs[i].lastIndexOf(".");
    if (atpos<1 || dotpos<atpos+2 ||
    document.getElementById('errEmail').
    else
    ment.getElementById(div).
```

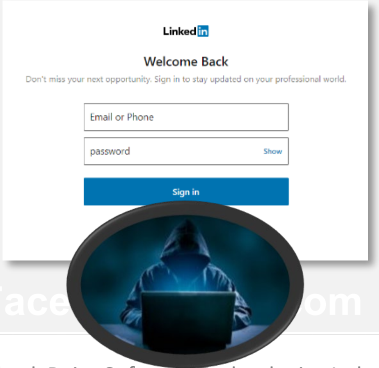
GET

RESPONSE


Linked in
Welcome Back
Don't miss your next opportunity. Sign in to stay updated on your professional world.
Email or Phone
password
Show
Sign in
Forgot password?

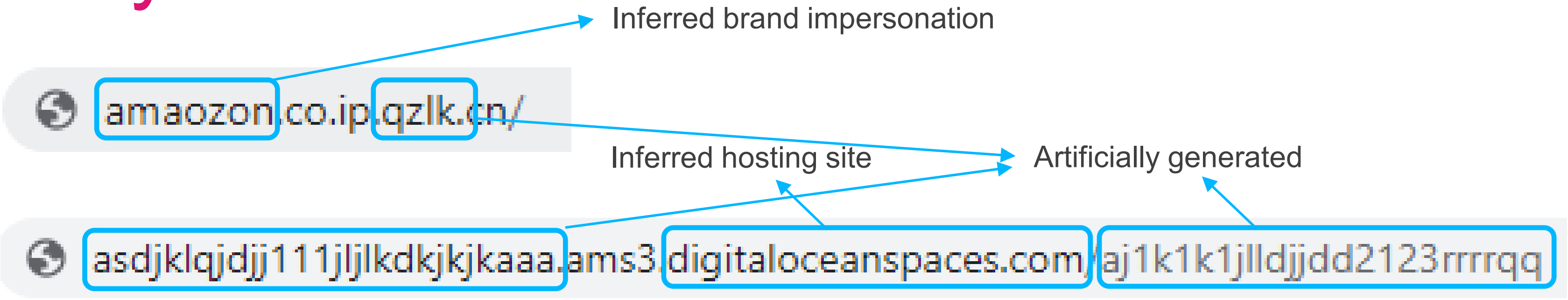
Quantum
Secure the Network

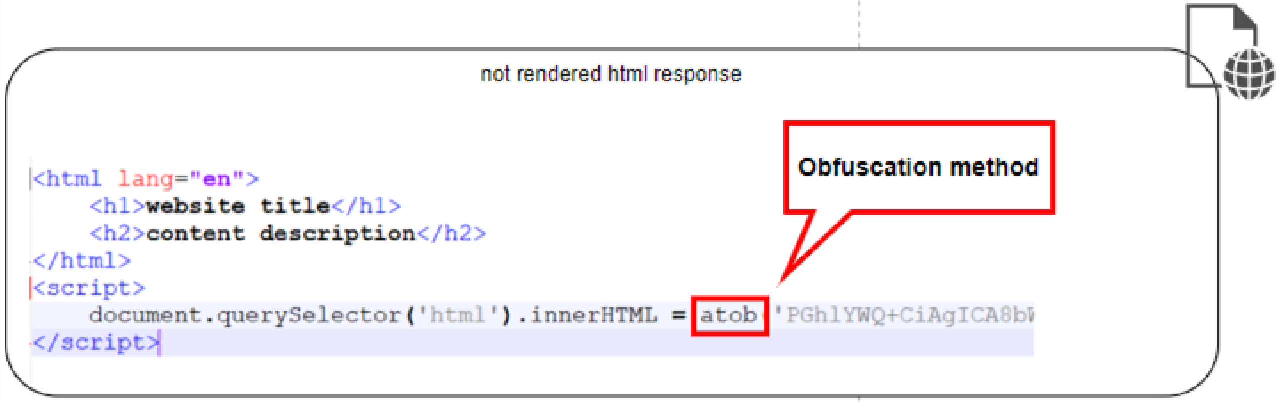
PHISHING SITE
LinkedInscam.com


Linked in
Welcome Back
Don't miss your next opportunity. Sign in to stay updated on your professional world.
Email or Phone
password
Show
Sign in

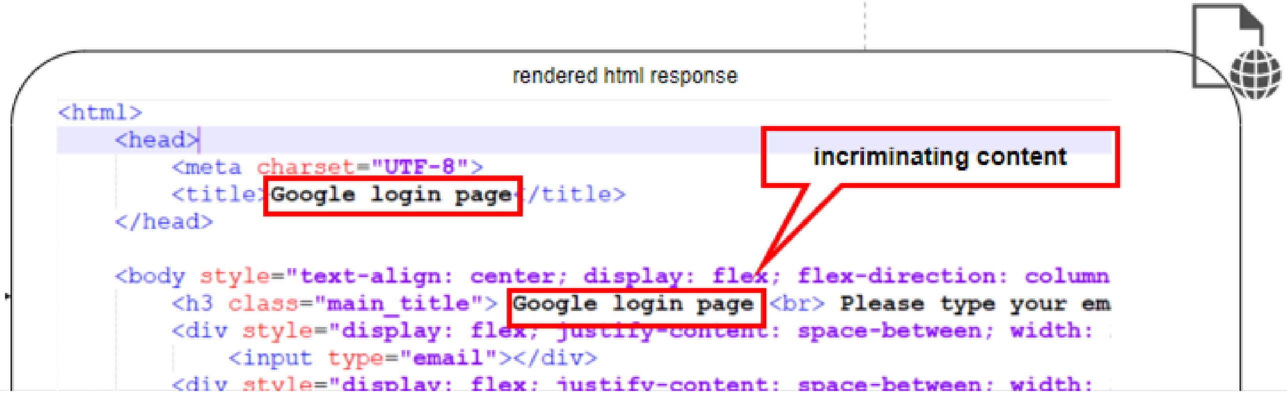
# More of Web Security

- Deep Learning Engine for malicious URLs
- Dynamic Web Emulation ROADMAP
- Local brand impersonation ROADMAP


Inferred brand impersonation
amaozon.co.ip.qzlk.cn/
Inferred hosting site
Artificially generated
asdjklqjdjj111jljlkdkjkjkaaa.ams3.digitaloceanspaces.com/aj1k1k1jlldjjdd2123rrrrqq


not rendered html response

```
<html lang="en">
    <h1>website title</h1>
    <h2>content description</h2>
</html>
<script>
    document.querySelector('html').innerHTML = atob('PGhlYWQ+CiAgICA8b
</script>
```


rendered html response

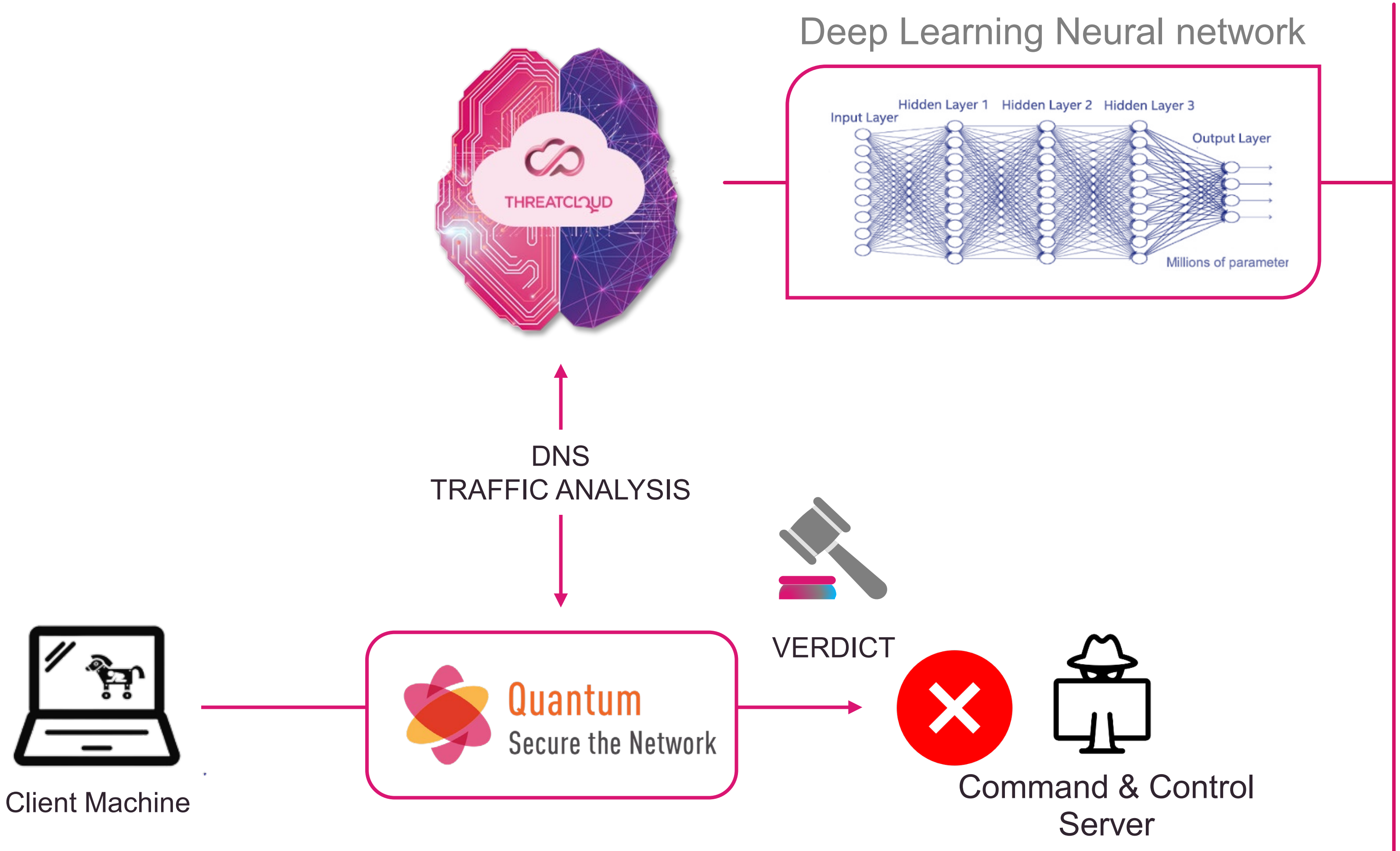
```
<html>
    <head>
        <meta charset="UTF-8">
        <title>Google login page</title>
    </head>

    <body style="text-align: center; display: flex; flex-direction: column
        <h3 class="main_title"> Google login page <br> Please type your em
        <div style="display: flex; justify-content: space-between; width:
            <input type="email"></div>
        <div style="display: flex; justify-content: space-between; width:
```

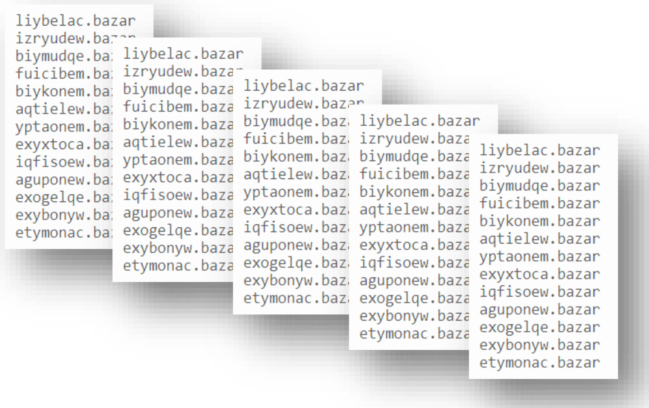
# Prevents 5X more sophisticated DNS attacks

PATENTED

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

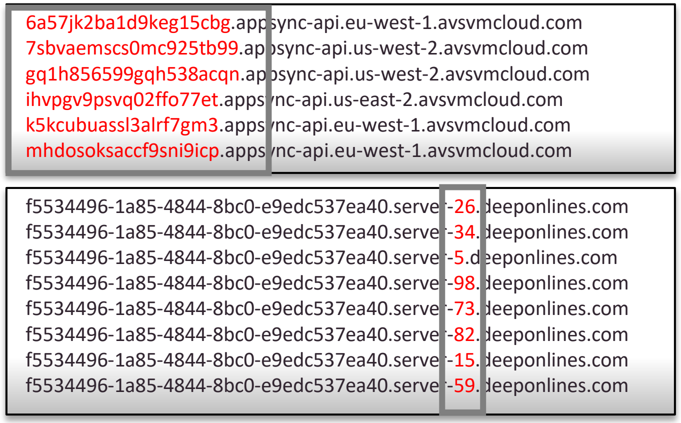


## #1 DGA (Domain Generation Algorithm)



```
liybelac.bazar
izryudew.bazar
biymudqe.bazar
fuicibem.bazar
biykonem.bazar
aqtielew.bazar
yptaonem.bazar
exyxtoca.bazar
iqfisoew.bazar
aguponew.bazar
exogelqe.bazar
exybonyw.bazar
etymonac.bazar
```

## #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
```

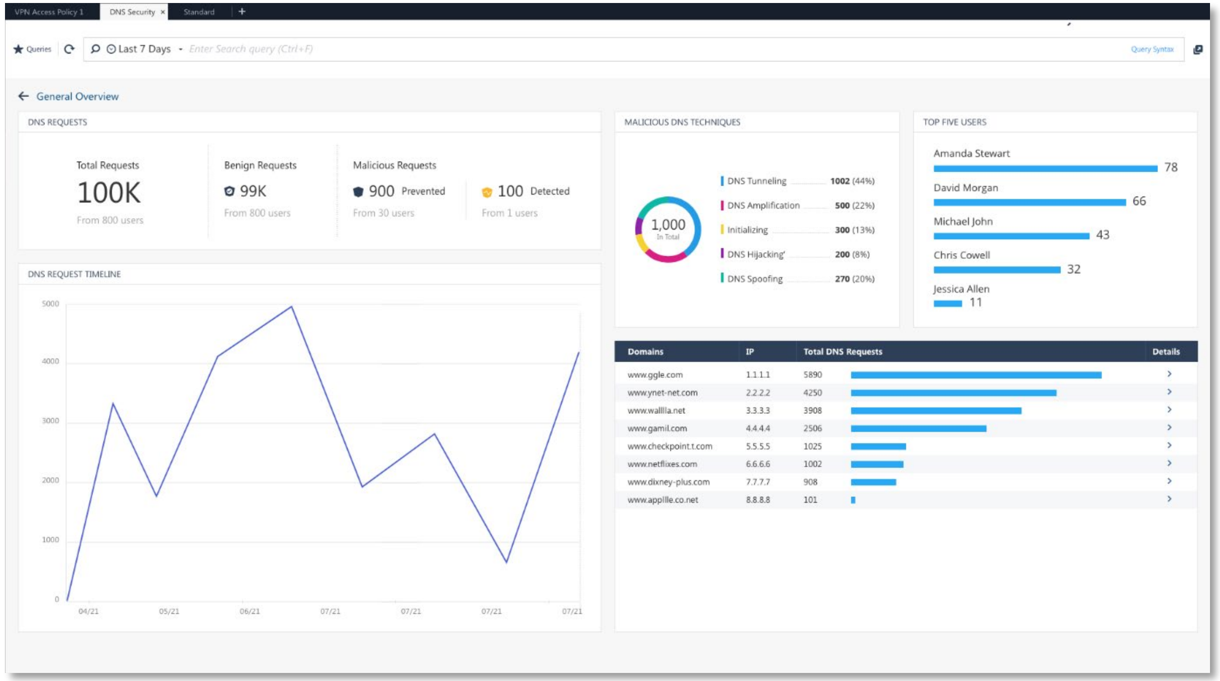
# More of DNS Security

ML/Deep Learning DNS engines:

- Ultra-slow tunneling JOIN EA
- CNAME cloaking
- Look-alike domains and
- Brand impersonation
- Dangling
- DNS Integrity

ROADMAP

Dedicated DNS Security dashboard: ROADMAP



VPN Access Policy 1 | DNS Security × | Standard | +

Queries | Last 7 Days | Enter Search query (Ctrl+F) | Query Syntax

General Overview

DNS REQUESTS

Total Requests 100K From 800 users

Benign Requests 99K From 800 users

Malicious Requests 900 Prevented From 30 users | 100 Detected From 1 users

DNS REQUEST TIMELINE

MALICIOUS DNS TECHNIQUES

1,000 In Total

| | |
|---|---|
| DNS Tunneling | 1002 (44%) |
| DNS Amplification | 500 (22%) |
| Initializing | 300 (13%) |
| DNS Hijacking' | 200 (8%) |
| DNS Spoofing | 270 (20%) |

TOP FIVE USERS

| | |
|---|---|
| Amanda Stewart | 78 |
| David Morgan | 66 |
| Michael John | 43 |
| Chris Cowell | 32 |
| Jessica Allen | 11 |

| Domains | IP | Total DNS Requests | Details |
|---|---|---|---|
| www.ggle.com | 1.1.1.1 | 5890 | > |
| www.ynet-net.com | 2.2.2.2 | 4250 | > |
| www.walllla.net | 3.3.3.3 | 3908 | > |
| www.gamil.com | 4.4.4.4 | 2506 | > |
| www.checkpoint.t.com | 5.5.5.5 | 1025 | > |
| www.netflixes.com | 6.6.6.6 | 1002 | > |
| www.dixney-plus.com | 7.7.7.7 | 908 | > |
| www.appllle.co.net | 8.8.8.8 | 101 | > |

THREATCLOUD

# New Machine Learning

“CADET”

“HUNTRESS”

“CAMPAIGN HUNTING”

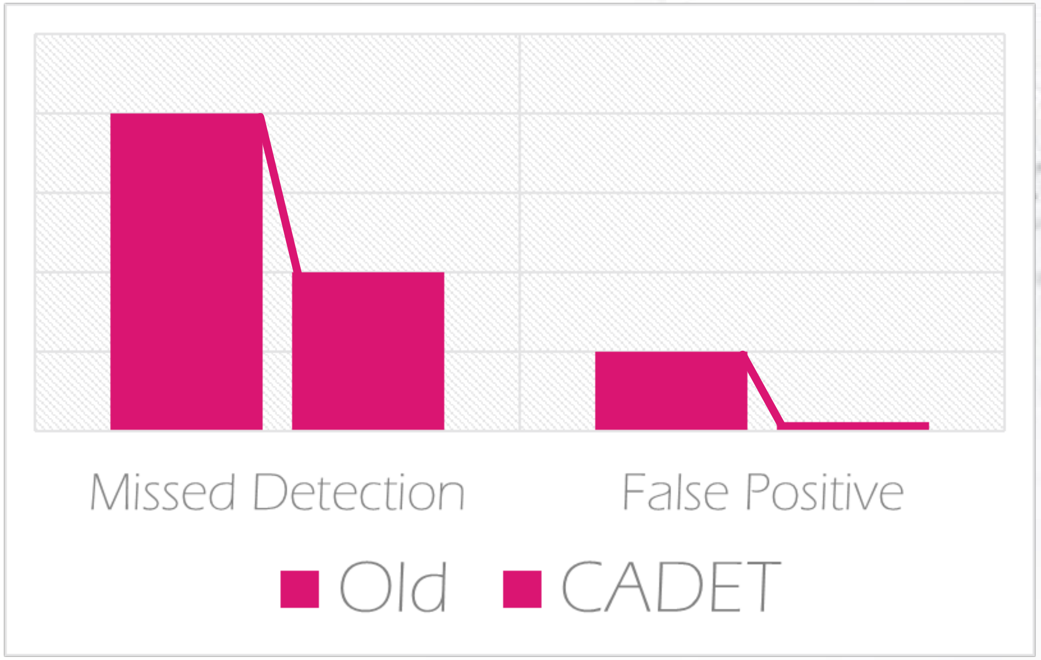
PREVENT UNKOWN ATTACKS

HIGHER CATCH RATES

LOWER FALSE POSITIVES

# “CADET”

# CONTEXT AWARE DETECTION

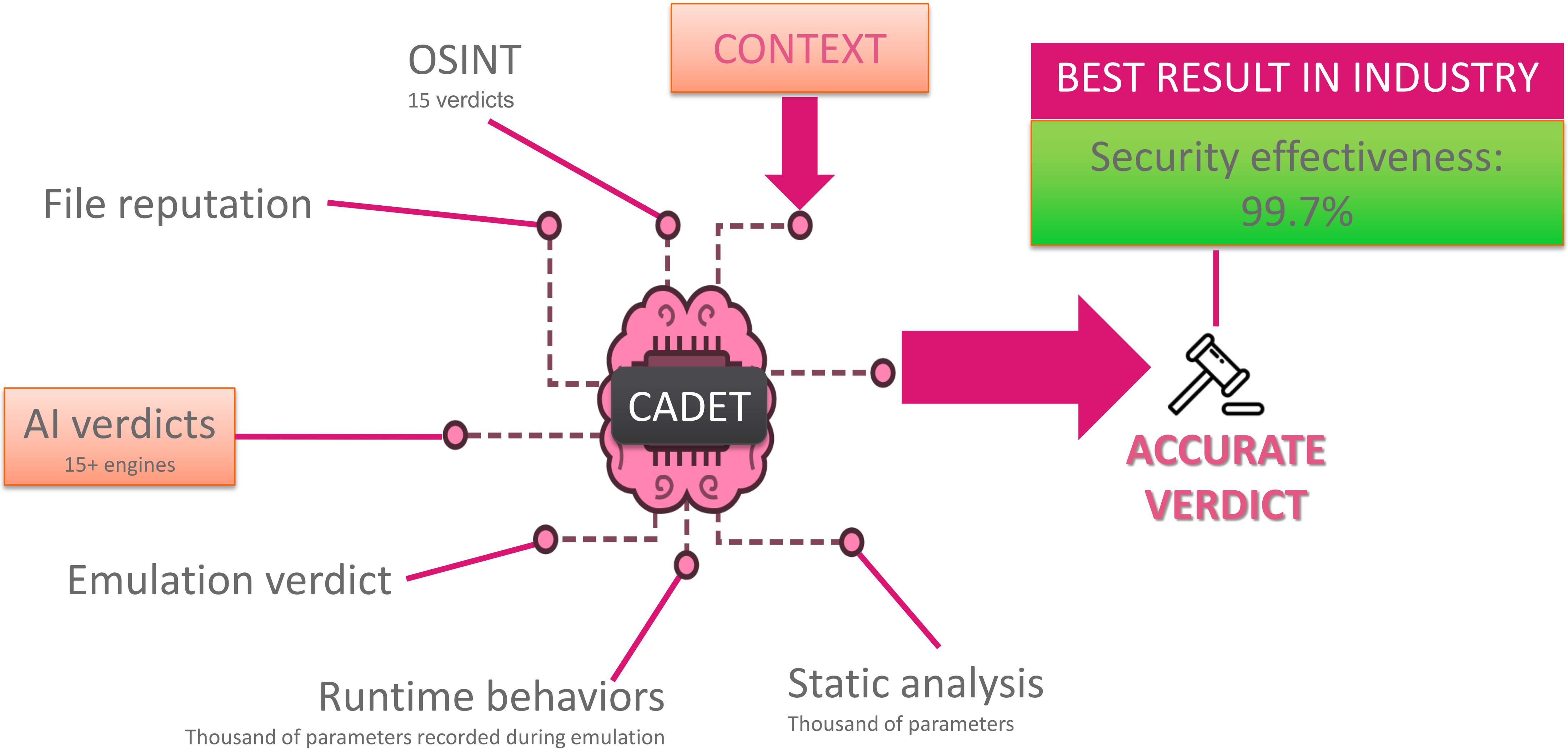


Look at full context of the inspected element

Extract parameters from the environment

THOUSANDS of discrete Indicators → ONE Accurate Verdict

# CADET: The ML of MLs



OSINT

15 verdicts

CONTEXT

BEST RESULT IN INDUSTRY

Security effectiveness: 99.7%

File reputation

AI verdicts

15+ engines

CADET

ACCURATE VERDICT

Emulation verdict

Runtime behaviors

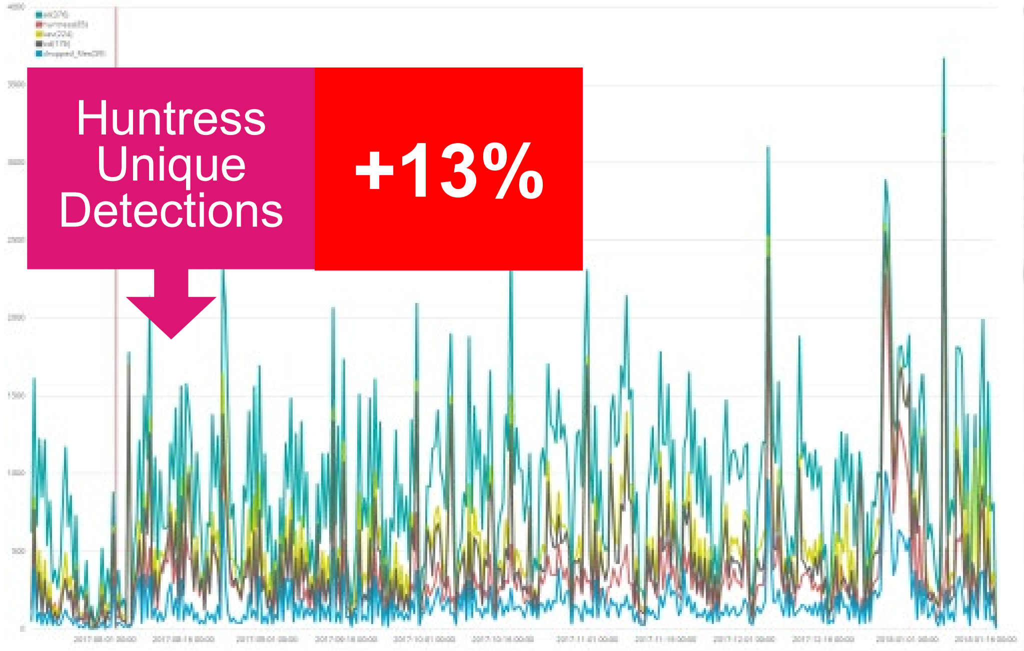
Thousand of parameters recorded during emulation

Static analysis

Thousand of parameters

# “HUNTRESS”

# UNCOVER MALICIOUS EXECUTABLES



Huntress Unique Detections

+13%

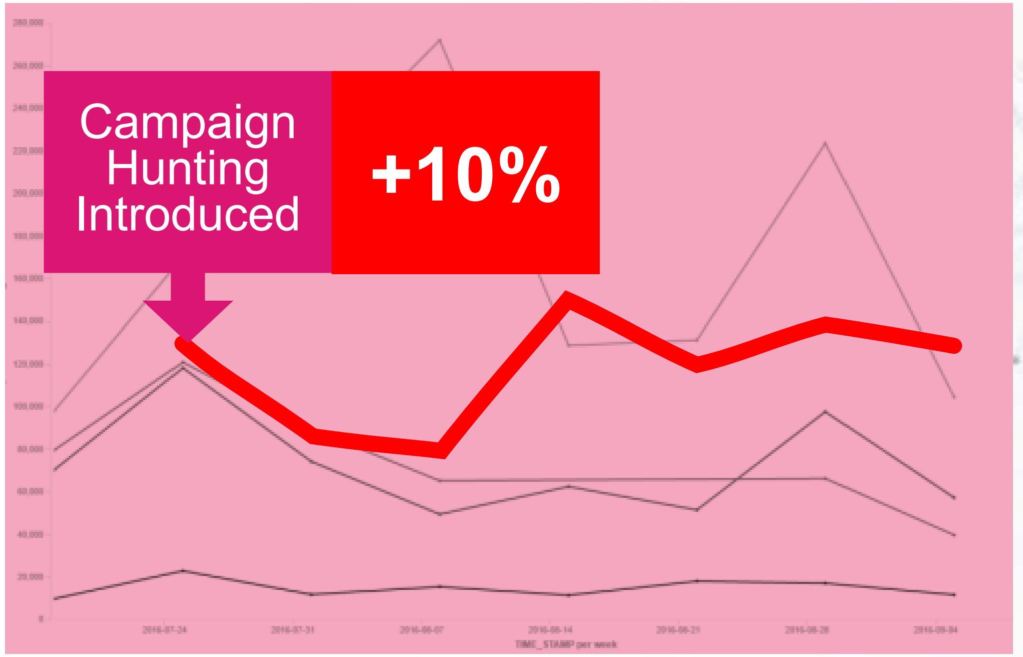
Dynamically analyze executables in a Sandbox to collect system API calls

Apply Machine Learning to reach malicious verdict based on behaviors

Feedback loop for continued learning

# “CAMPAIGN HUNTING”

# PREDICTIVE THREAT INTELLIGENCE



Expose unknown bots and malicious domains

Attribute attacks to campaigns

Enrich threat intelligence for predictive campaign prevention

# 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**

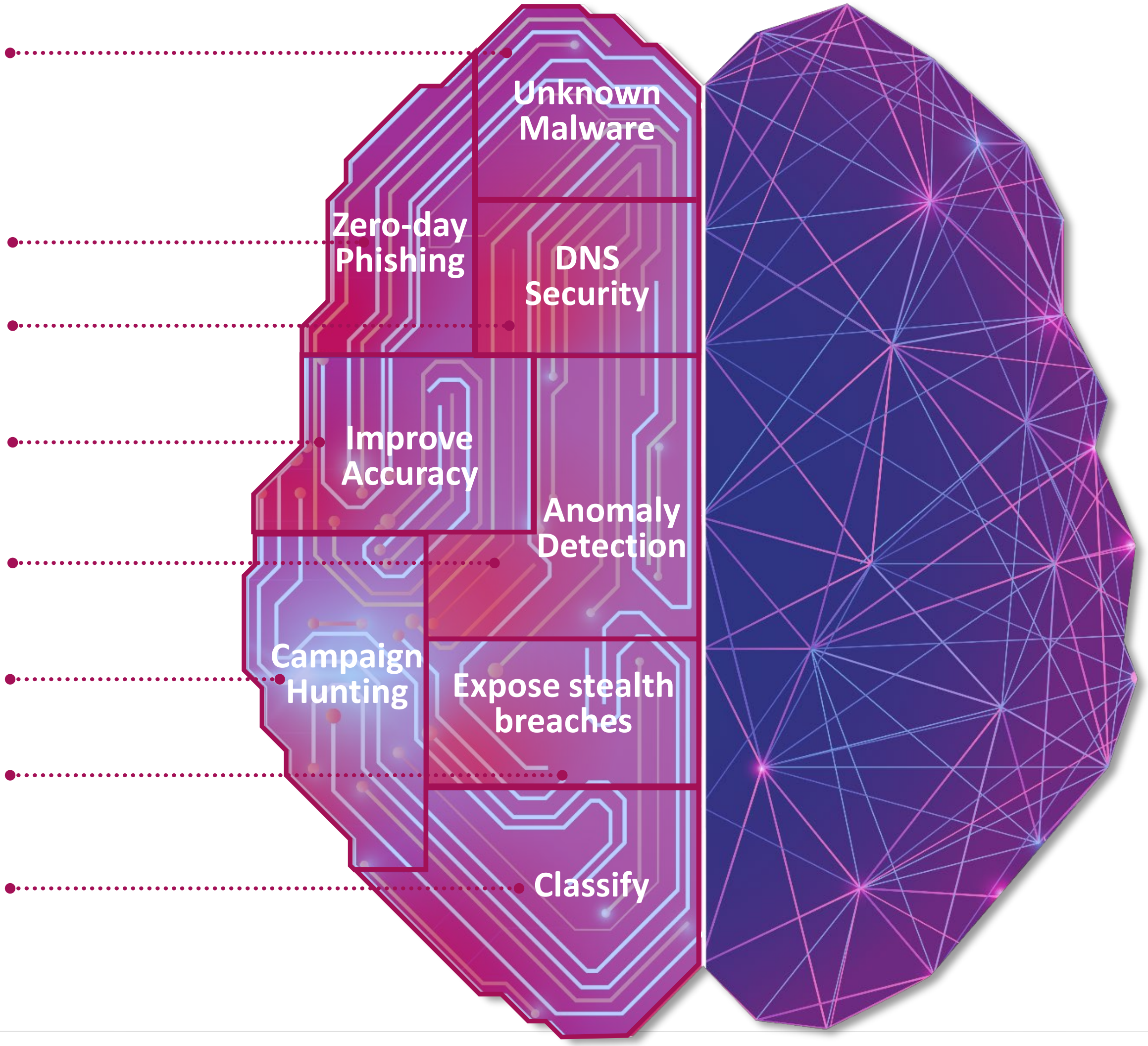
Network AI engines aggregator
Mobile AI engines aggregator
Machine validated signature

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