Integrity360
your security in mind

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

Who is Winning the AI Cyber War?

Ian Porteous

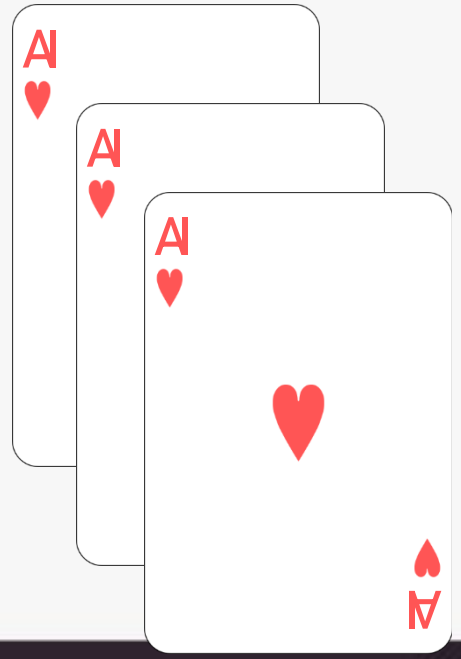
Regional Director, Sales Engineering | Office of the CTO

- Check Point

#SecurityFirstDublin

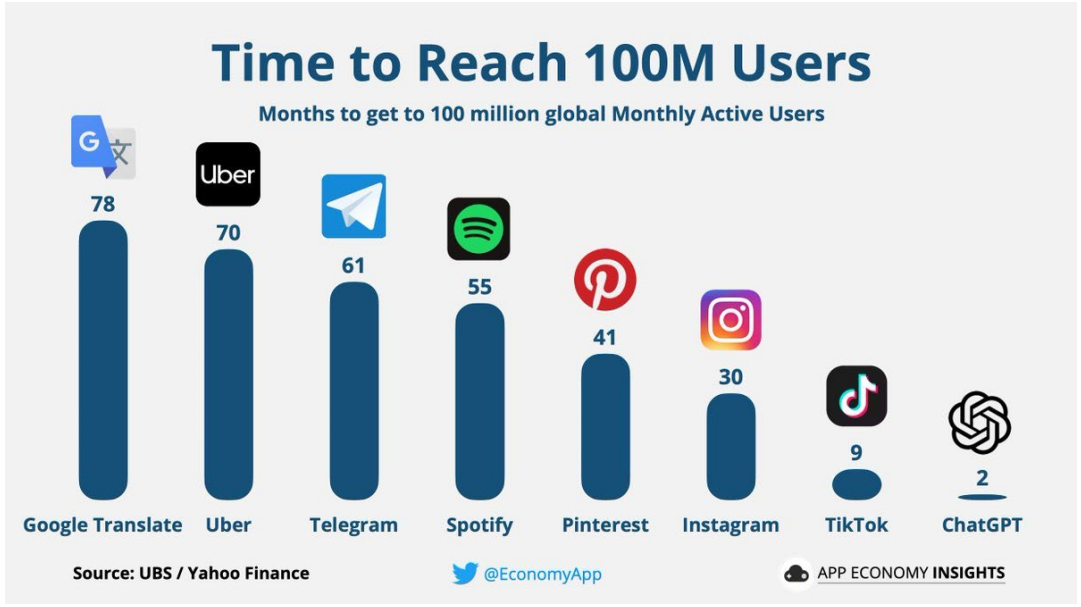
Who is winning the AI Cyber War?

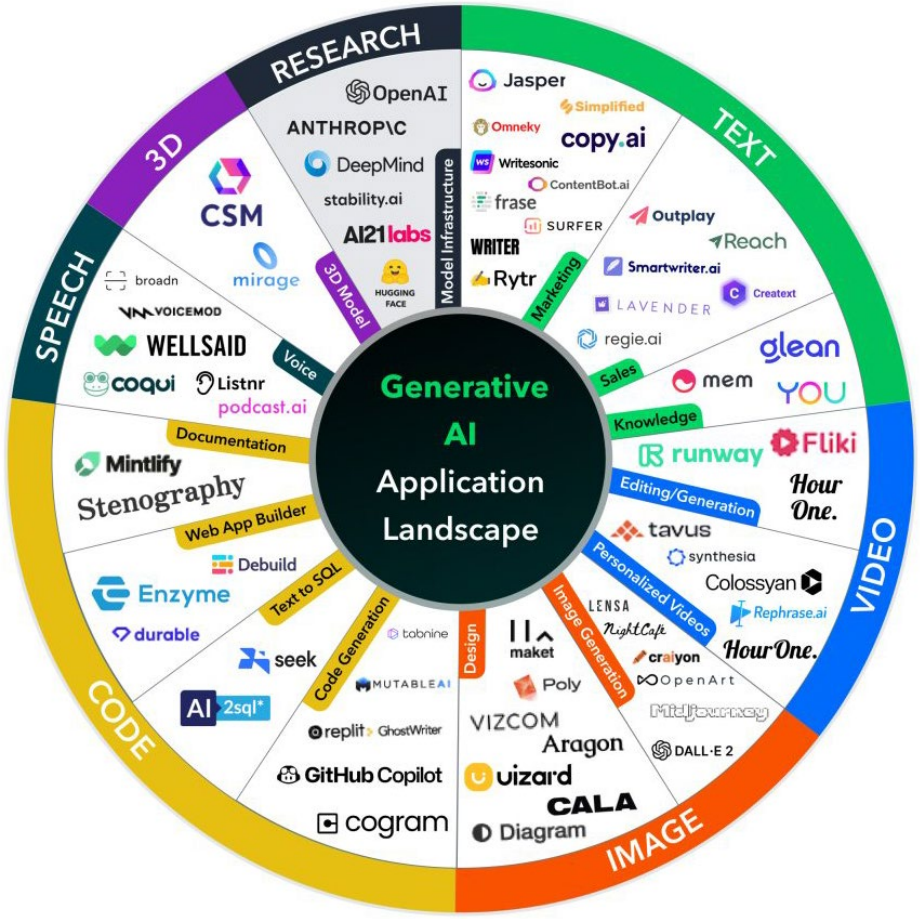
How to stack the deck in your favour



Deryck Mitchelson | Global Chief Information Security Officer

It’s no secret, we’ve ALL been doing it!



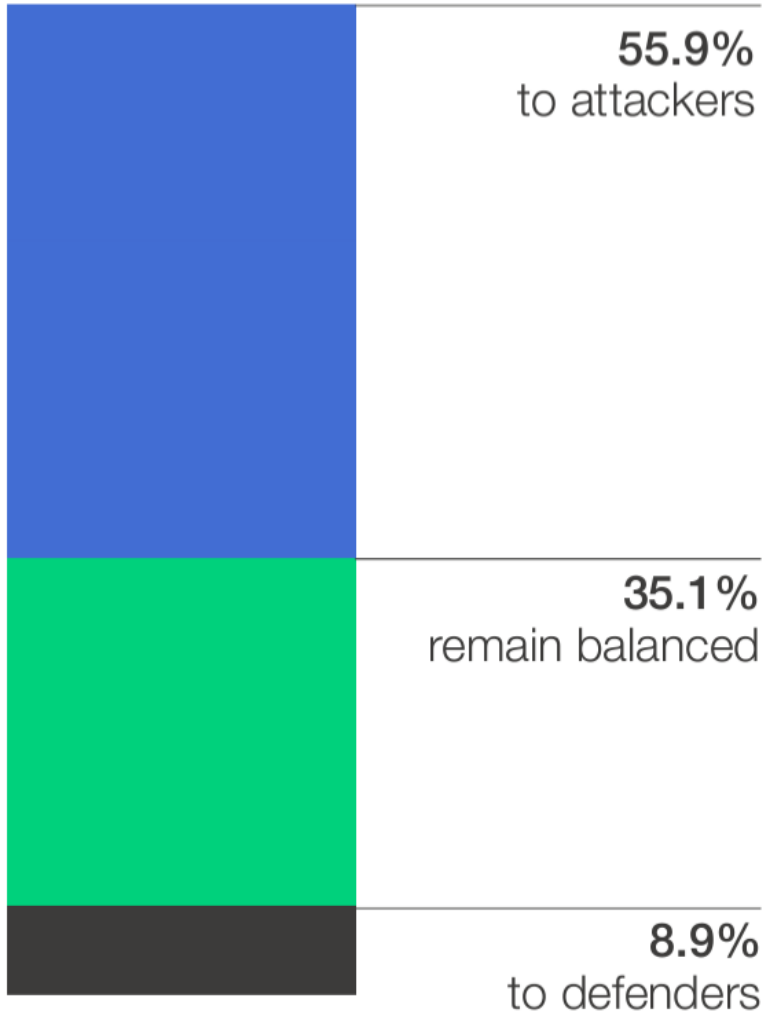


Generative-AI Explosion for Business and Personal

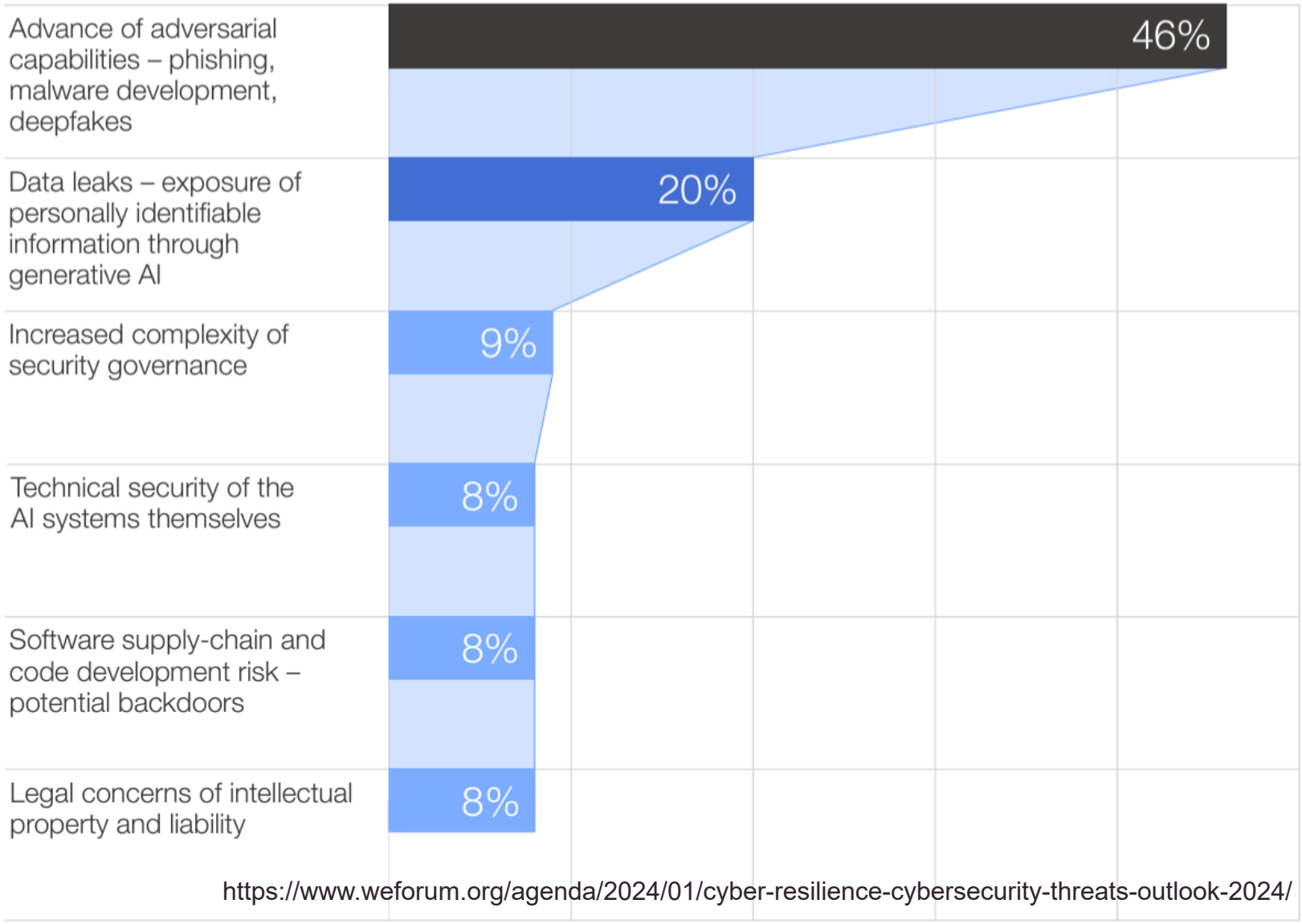
Emerging technologies will exacerbate long-standing challenges related to cyber resilience

WORLD ECONOMIC FORUM

In the next two years, will generative AI provide overall cyber advantage to attackers or defenders?



What are you most concerned about in regards to generative AI's impact on cyber?



https://www.weforum.org/agenda/2024/01/cyber-resilience-cybersecurity-threats-outlook-2024/

Four main points of view when AI meets cyber

AI used by attackers

- Force multiplier
- More targeted
- Increase success rate (test before you do)
- New attacks forms

How to secure AI Usage in my org

- Govern access to AI services & to data
- Secure AI pipeline
- New things: Secure prompts, prevent poisoning, secure the AI models

AI Used for Defense

- Force multiplier
- Precision
- New interface, conversational & generative
- New ways to defend. Better operations

And then, like every organization, your team can leverage AI and be better

More efficient, better operations & quality, growth, development & more

DEEPFAKES / VOICEFAKES / NEWSFAKES

NO LONGER
JUST SCIENCE FICTION

DEEPFAKES

Powered by
Generative Adversarial
Networks (GAN)

#SaveTheVote #DeepFake #KimJongUn
Dictators - Kim Jong-Un

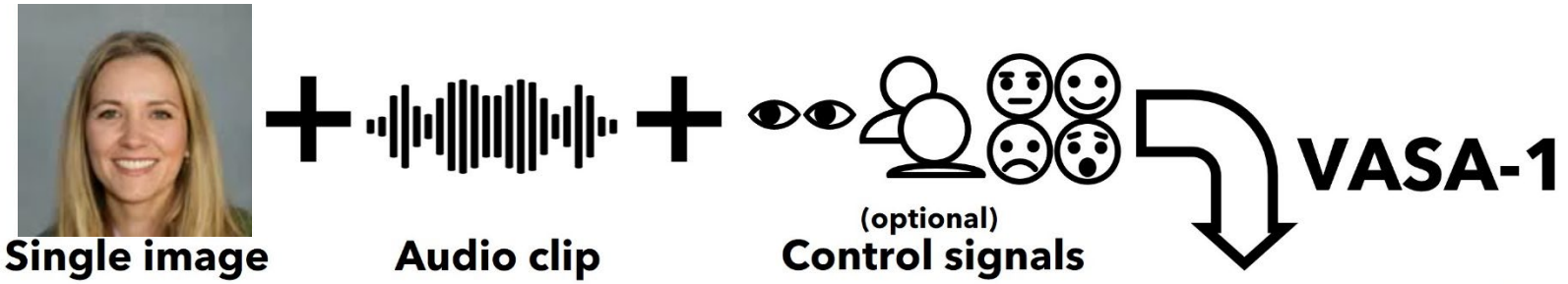
DeepFaceLab
https://github.com/iperov/DeepFaceLab

NVIDIA GAN
https://thispersondoesnotexist.com/

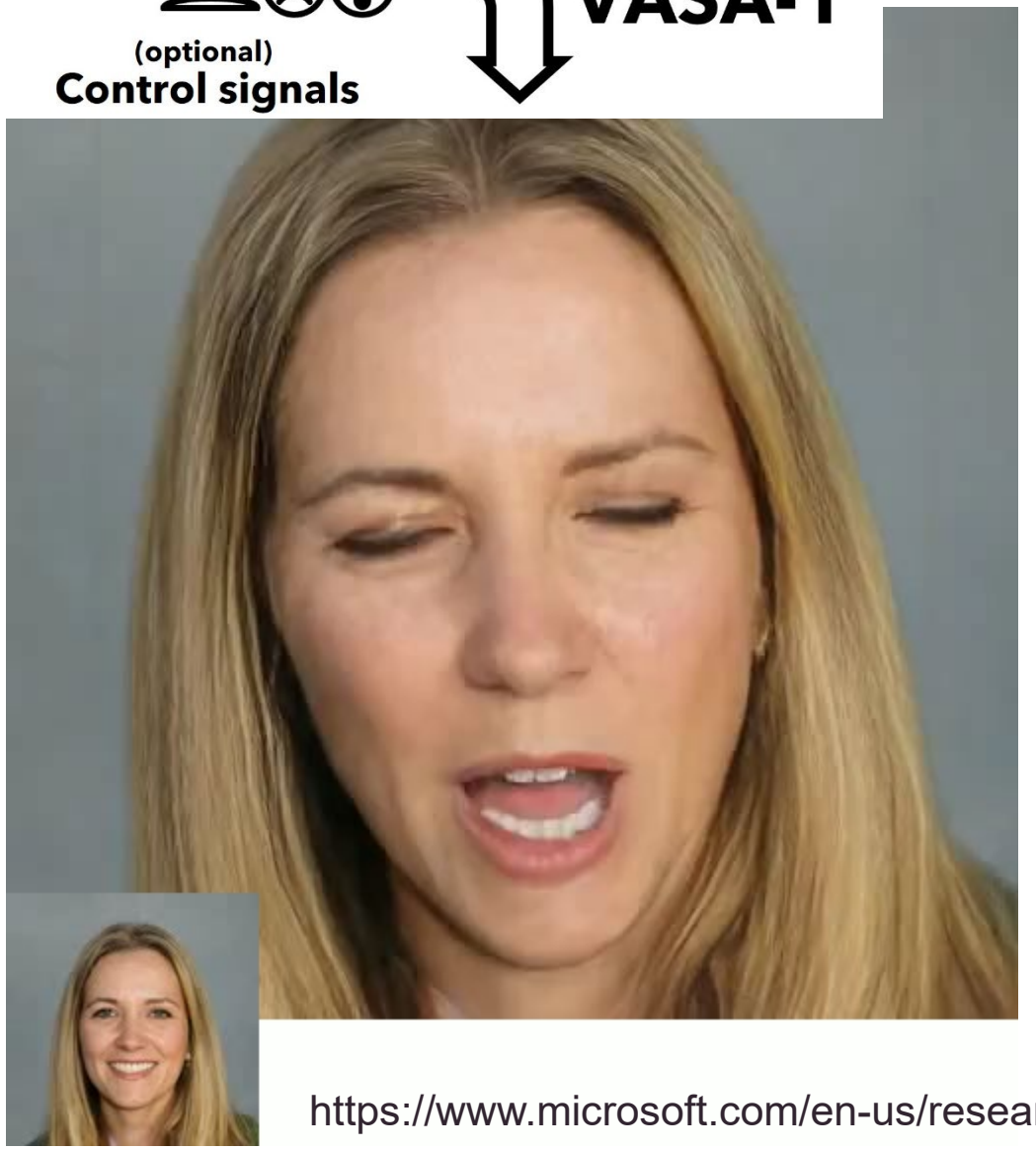
https://www.youtube.com/watch?v=ERQlaJ_czHU

https://www.youtube.com/watch?v=X17yrEV5sl4

https://www.youtube.com/watch?v=oxXpB9pSETo



single portrait photo + speech audio = hyper-realistic talking face video with *precise lip-audio sync*, *lifelike facial behavior*, and *naturalistic head movements*, generated in ***real time***.



https://www.microsoft.com/en-us/research/project/vasa-1/

Could AI Influence Elections?

IS THIS A BUSINESS RISK?

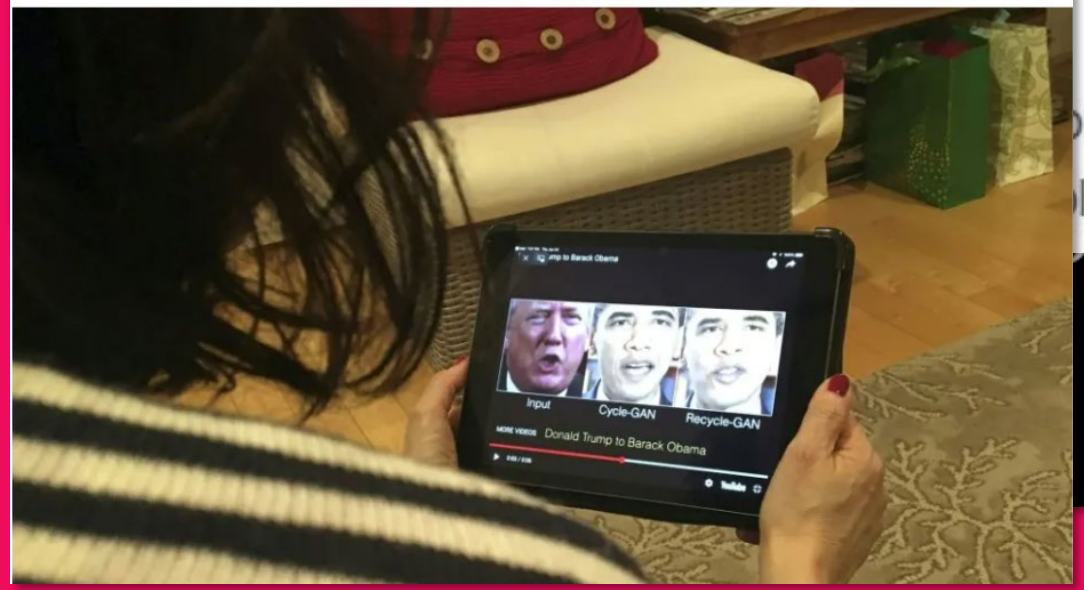
Image if this deepfake technology could impersonate executives live on a video call

It already has

Voice Deepfakes are Coming for your Bank Balance

UK energy boss conned out of £200,000 in 'deep fake' fraud

JAMES WARRINGTON



loses $25 million after
deep fake video call

ong was tricked into paying out USD
logy...

AI DRIVEN PHISHING EPIDEMIC

We are now in an AI-driven Phishing Epidemic

Subject: Nigerian Astronaut Wants To Come Home
Dr. Bakare Tunde
Astronautics Project Manager
National Space Research and Development Agency (NASRDA)
Plot 555
Misau Street
PMB 437
Garki, Abuja, FCT NIGERIA

Dear Mr. Sir,

REQUEST FOR ASSISTANCE-STRICTLY CONFIDENTIAL

I am Dr. Bakare Tunde, the cousin of Nigerian Astronaut, Air Force Major Abacha Tunde. He was the first African in space when he made a secret flight to the Salyut 6 space station in 1979. He was on a later Soviet spaceflight, Soyuz T-16Z to the secret Soviet military space station Salyut 8T in 1989. He was stranded there in 1990 when the Soviet Union was dissolved. His other Soviet crew members returned to earth on the Soyuz T-16Z, but his place was taken up by return cargo. There have been occasional Progrez supply flights to keep him going since that time. He is in good humor, but wants to come home.

In the 14-years since he has been on the station, he has accumulated flight pay and interest amounting to almost $ 15,000,000 American Dollars. This is held in a trust at the Lagos National Savings and Trust Association. If we can obtain access to this money, we can place a down payment with the Russian Space Authorities for a Soyuz return flight to bring him back to Earth. I am told this will cost $ 3,000,000 American Dollars. In order to access the his trust fund we need your assistance.

Consequently, my colleagues and I are willing to transfer the total amount to your account or subsequent disbursement, since we as civil servants are prohibited by the Code of Conduct Bureau (Civil Service Laws) from opening and/ or operating foreign accounts in our names.

Needless to say, the trust reposed on you at this juncture is enormous. In return, we have agreed to offer you 20 percent of the transferred sum, while 10 percent shall be set aside for incidental expenses (internal and external) between the parties in the course of the transaction. You will be mandated to remit the balance 70 percent to other accounts in due course.

Kindly expedite action as we are behind schedule to enable us include downpayment in this financial quarter.

Please acknowledge the receipt of this message via my direct number [redacted] only.

Yours Sincerely, Dr. Bakare Tunde

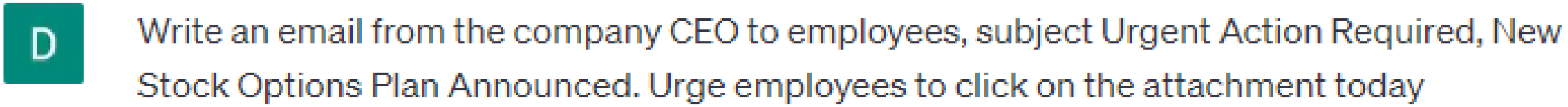
We are now in a Phishing Epidemic

Subject: Urgent Action Required: New Stock Options Plan Announced

Dear [Company Name] Team,

I hope this email finds you well. Today, I have some exciting news to share with all of you. As we continue to grow and thrive as a company, we are constantly seeking ways to reward and recognize the hard work and dedication of our incredible team.

I am thrilled to announce the launch of our new Stock Options Plan, aimed at enhancing our commitment to our employees and aligning our collective interests even further. This plan represents a significant milestone for us, and we believe it will further strengthen our bonds as a united [Company Name] family.



also reinforces our commitment to your personal and professional growth.

If you have any questions or need clarification on any aspect of the Stock Options Plan, please don't hesitate to reach out to our HR department, who will be more than happy to assist you.

I want to emphasize that this is a time-sensitive matter, and your prompt attention to this email is greatly appreciated. The deadline for enrollment is [Insert Enrollment Deadline Date], so please ensure you review the details and make an informed decision by that date.

Once again, I want to express my gratitude for your hard work, dedication, and unwavering commitment to our company's success. Our employees are our most valuable asset, and we are excited to take this step forward together.

Thank you for your immediate attention to this important matter, and I look forward to witnessing our continued growth and success as a team.

Warm regards,

[Your Name] CEO, [Company Name]

We are now in a Phishing Epidemic

Subject: Exciting News: New Stock Options Plan Unveiled – **Take Action Today!**

Dear [Company Name] Team,

I hope this message finds you well. We have some fantastic news to share with all of you that underscores our commitment to your success and your future with [Company Name].

Today, I am thrilled to introduce our brand-new Stock Options Plan, a remarkable opportunity designed exclusively for our dedicated team members. This initiative is a testament to our belief in your contributions and our determination to reward your hard work.

Please find the comprehensive details of this plan in the attachment to this email:

refine the message to increase the number of recipients who will click on the attachment

exceptional benefits you stand to gain by participating. We've worked diligently to make this plan as accessible and rewarding as possible.

Your immediate attention to this matter is crucial, as the enrollment deadline is set for [Insert Enrollment Deadline Date]. This is your chance to secure a stake in our shared success, and I urge you to make an informed decision before this date.

If you have any questions or need clarification regarding any aspect of the Stock Options Plan, our dedicated HR team is available to assist you promptly. Your satisfaction and understanding are of utmost importance to us.

We recognize that your time is valuable, and we want to make this process as seamless as possible. As such, we have also organized a series of informational sessions and Q&A sessions over the next few days to address any queries you may have. The schedule for these sessions is included in the attachment.
Our success as a company is a direct reflection of the dedication and expertise of each team member, and this Stock Options Plan is just one way we aim to reciprocate your commitment.

Email security by numbers

75%

1 in 72

30%

$4.89m

IBM estimated cost of BEC Breach

Over 75% of targeted cyberattacks start with an email

AI POWERED HACKTIVISM

AI Developed and

A DDoS attack by itself is

But when you add AI in e dangerous.

Largest blocked DDoS attack was 398 million requests per second

7x Previous

A fully AI-based DDo ation, which isn't good for many reaso

1. It makes the sou
2. Available 24×7. T
3. The error rate is n
4. Fast and efficient de
5. It helps the attacker m ve tasks).
6. Predict outcome (predict

AI POWERED RANSOMWARE

AI Increasing RansomwareThreat

National Cyber Security Centre

Global ransomware threat expected to rise with AI, NCSC warns

AI is expected to heighten the global ransomware threat, says GCHQ's National Cyber Security Centre; New report suggests artificial...

The Record by Recorded Future

British intelligence warns AI will cause surge in ransomware volume and impact

Ransomware attacks will increase in both volume and impact over the next two years due to artificial intelligence (AI) technologies,...

Sky News

Britons must 'strengthen defences' against growing threat of AI-assisted ransomware, cyber security chief warns

Ransomware attacks have already impacted UK services, including in 2017 when the WannaCry virus infected thousands of NHS computers.

AI THREATS FOR SOFTWARE DEVELOPMENT

OWASP Top10 of LLM

LLM01

Prompt Injection

This manipulates a large language model (LLM) through deliberate inputs, causing unintended actions by the LLM. Direct injections overwrite system prompts, while indirect ones manipulate inputs from external sources.

LLM02

Insecure Output Handling

This vulnerability occurs when an LLM output is accepted without scrutiny, exposing backend systems. Misuse may lead to severe consequences like XSS, CSRF, SSRF, privilege escalation, or remote code execution.

LLM03

Training Data Poisoning

Training data poisoning refers to manipulating the data or fine-tuning process to introduce vulnerabilities, backdoors or biases that could compromise the model's security, effectiveness or ethical behavior.

LLM04

Model Denial of Service

Attackers cause resource-heavy operations on LLMs, leading to service degradation or high costs. The vulnerability is magnified due to the resource-intensive nature of LLMs and unpredictability of user inputs.

LLM05

Supply Chain Vulnerabilities

LLM application lifecycle can be compromised by vulnerable components or services, leading to security attacks. Using third-party datasets, pre-trained models, and plugins add vulnerabilities.

LLM06

Sensitive Information Disclosure

LLM's may inadvertently reveal confidential data in its responses, leading to unauthorized data access, privacy violations, and security breaches. Implement data sanitizations and strict user policies to mitigate this.

LLM07

Insecure Plugin Design

LLM plugins can have insecure inputs and insufficient access control due to lack of application control. Attackers can exploit these vulnerabilities, resulting in severe consequences like remote code execution.

LLM08

Excessive Agency

LLM-based systems may undertake actions leading to unintended consequences. The issue arises from excessive functionality, permissions, or autonomy granted to the LLM-based systems.

LLM09

Overreliance

Systems or people overly depending on LLMs without oversight may face misinformation, miscommunication, legal issues, and security vulnerabilities due to incorrect or inappropriate content generated by LLMs.

LLM10

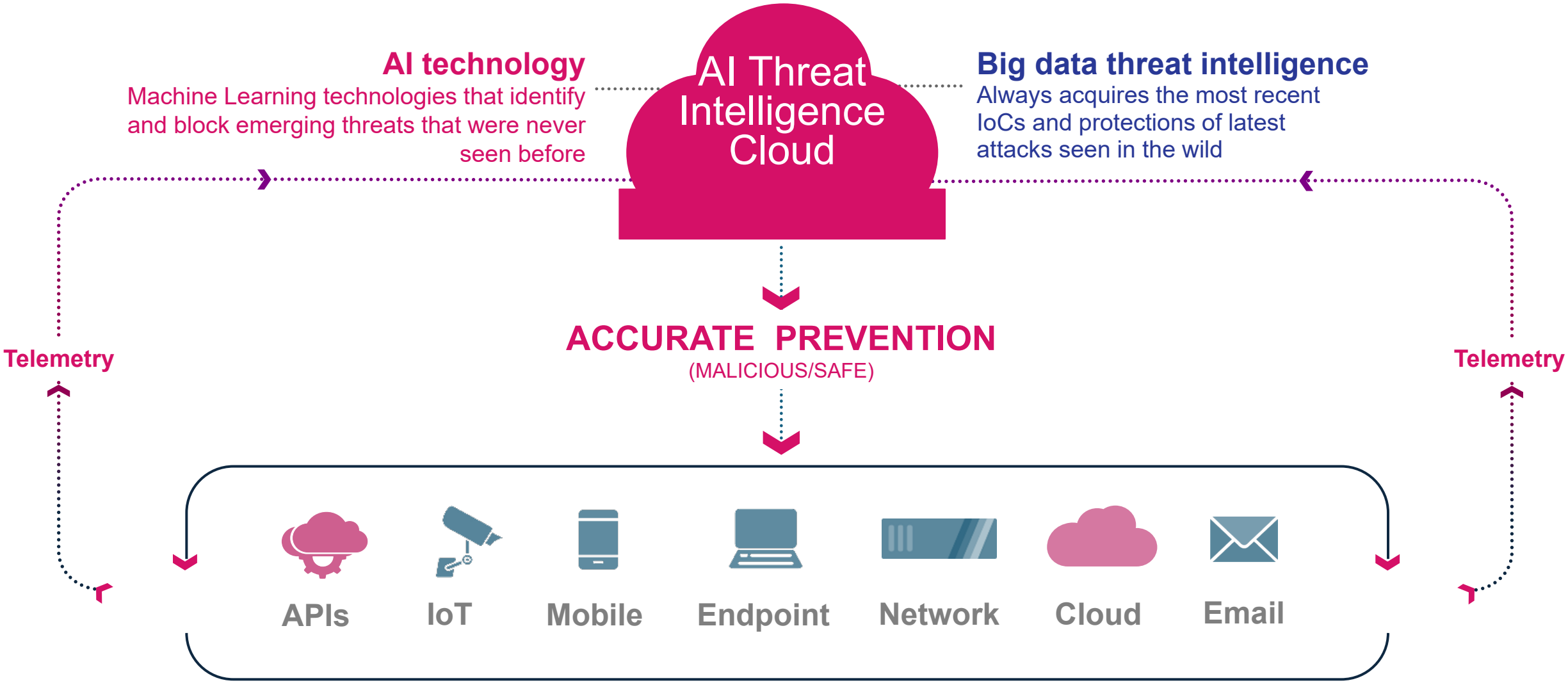
Model Theft

This involves unauthorized access, copying, or exfiltration of proprietary LLM models. The impact includes economic losses, compromised competitive advantage, and potential access to sensitive information.

How can we secure all these?
The good news is that we will have jobs. No silver bullets

FIGHTING AI FIRE WITH FIRE

Threat intelligence is key for AI-based prevention



DEEP LEARNING REDUCES FALSE POSITIVES BY 90%

How AI Deep Learning works vs. Classic Machine Learning

Classic Machine Learning

EXE

Features definition

Certifier
OS
Compiler info
Metadata
Packer
Writable
Permissions
…etc.

Classifier Algorithm

SVM
Random Forest
Decision Trees
...

Malicious?

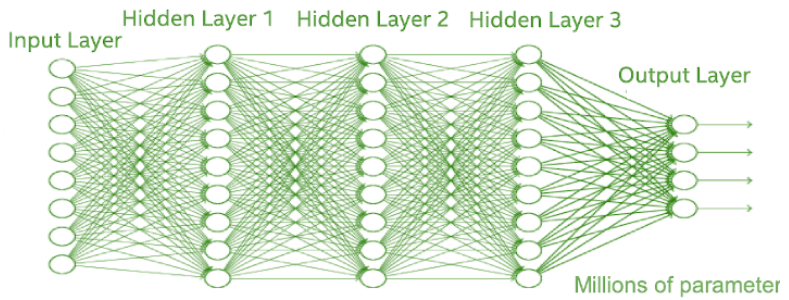
Zero day ransomware (exe)

Deep Learning

EXE

All files' bytes are processed

Natural network

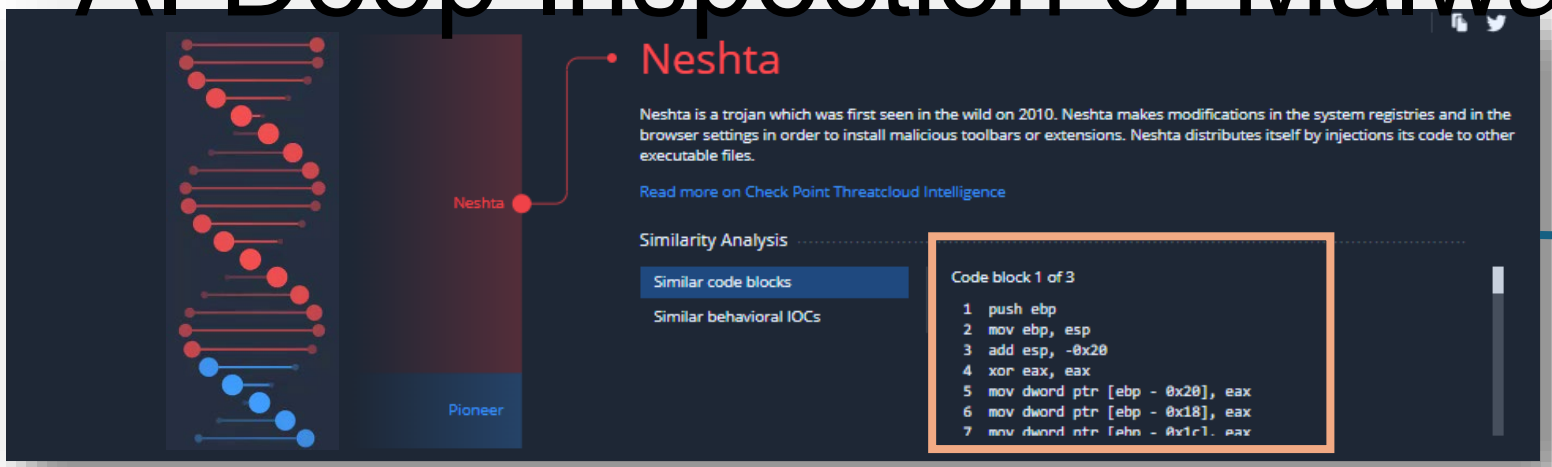


Malicious

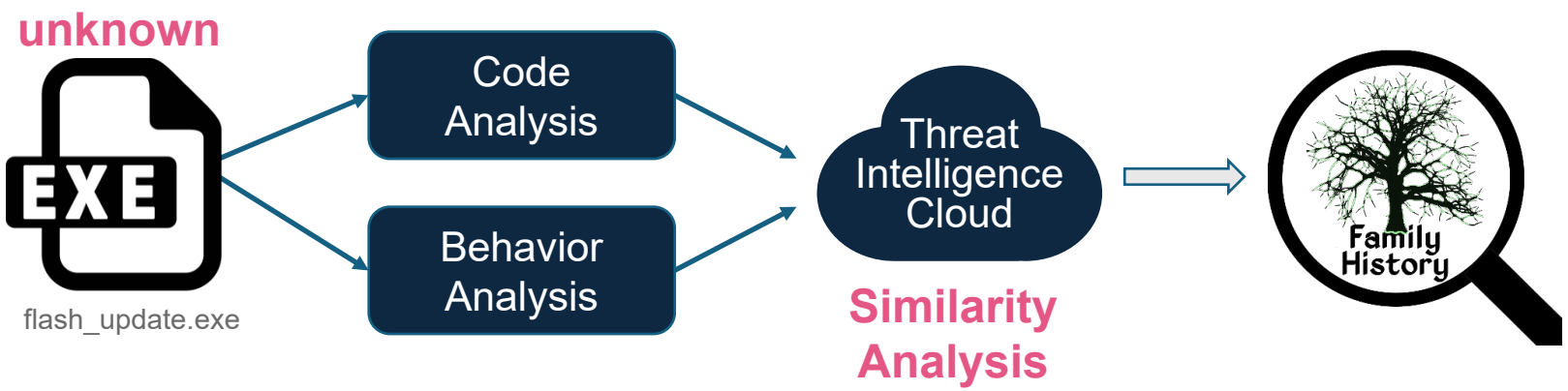
Zero day ransomware (exe)

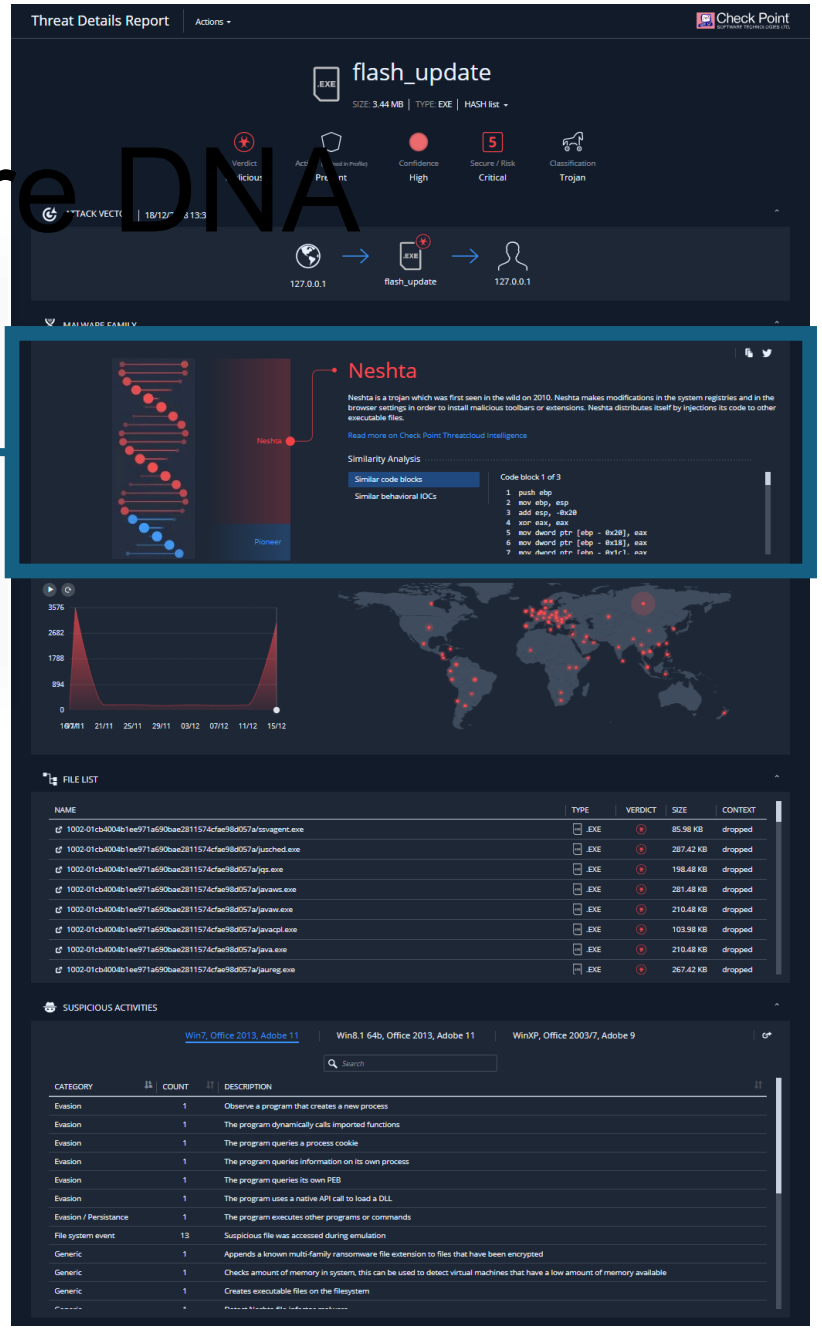
Blocks **30%** more attacks

AI Deep Inspection of Malware DNA



AI Classification of Unknown Genes





PREVENTATIVE AI IN ACTION

AI technologies leveraged by Check Point Threat Intelligence

70+ engines across different security functionality protecting all vectors

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

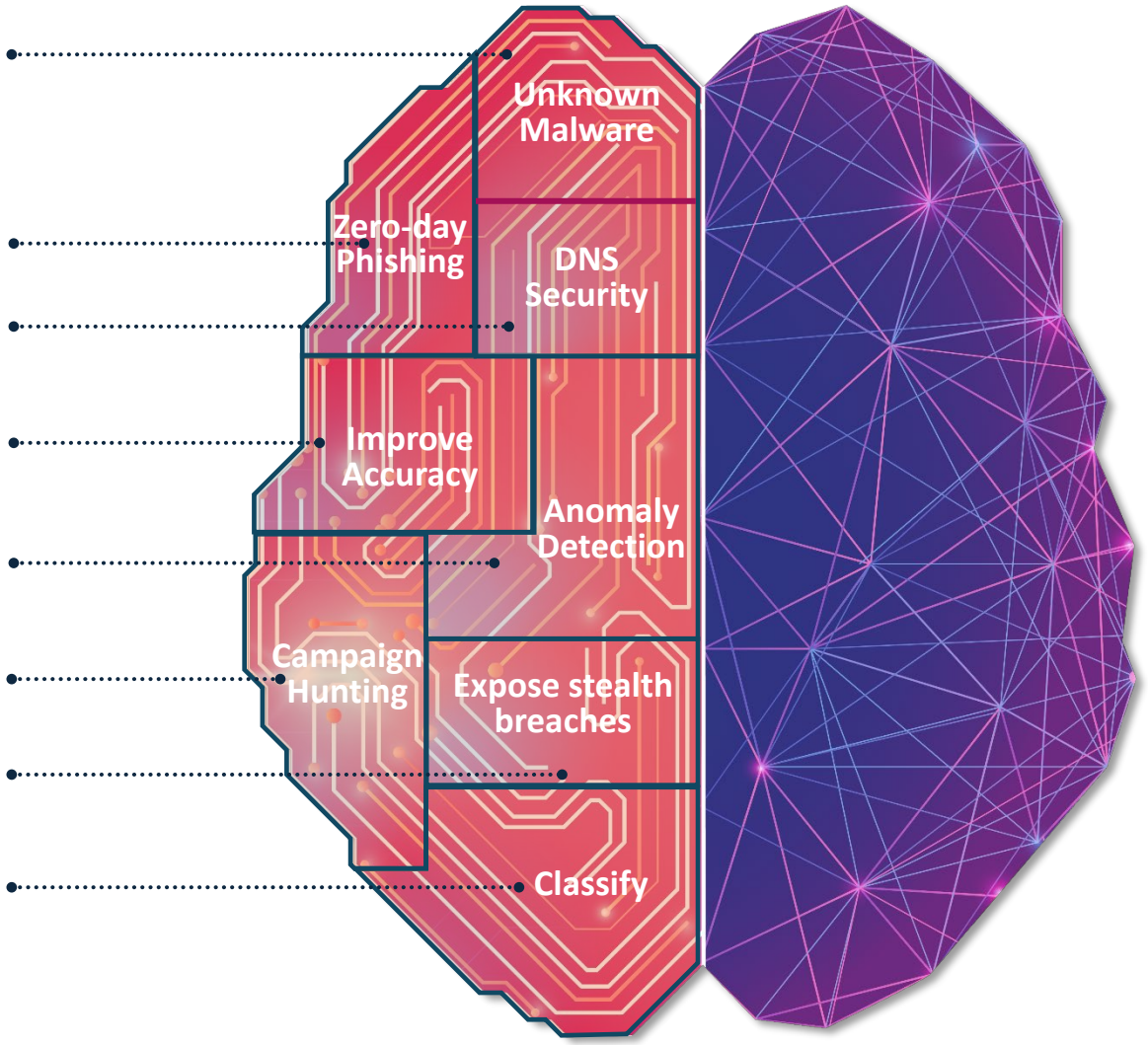
Network AI engines aggregator
Mobile AI engines aggregator
Machine validated signature

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



AI Blocking zero-day malware

Zero-day malware
“AveMaria” RAT
May 2022

First seen by a
customer in Italy

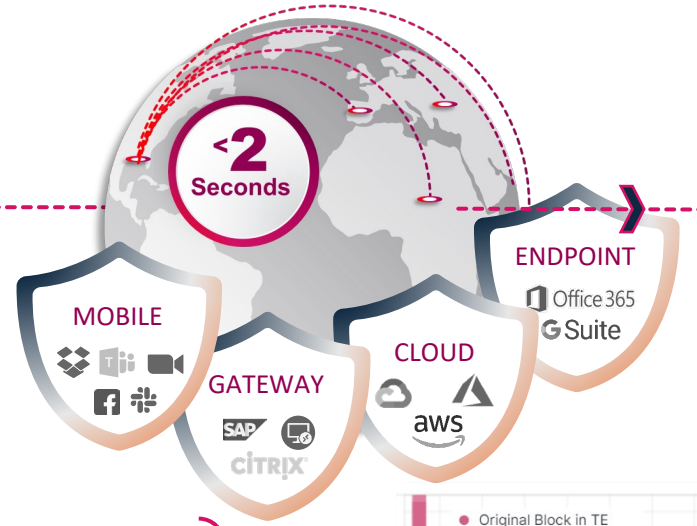
Detected as malicious
in seconds

Synced in real-time to all
enforcement points
worldwide

Prevented in dozens
of other countries
within 3 hours

Security Gateway

Threat Intelligence Cloud



Security Gateway

70+ Decision Engines

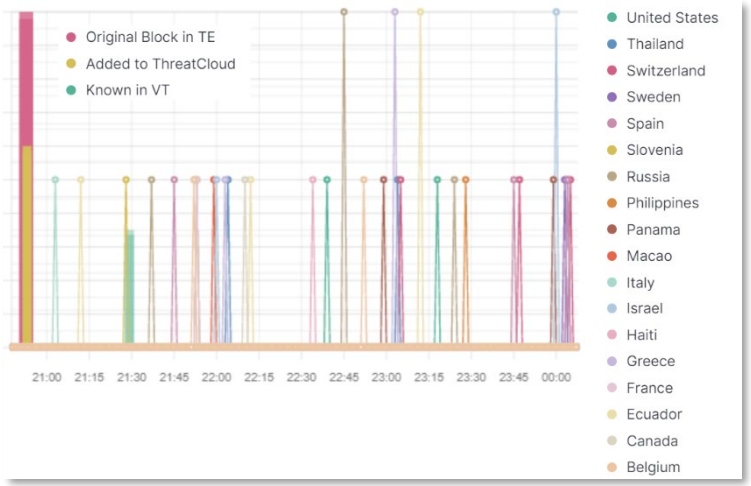
Deep Learning

File Reputation

Machine Learning

Emulation Runtime

Verdict Engine
Machine Learning Based

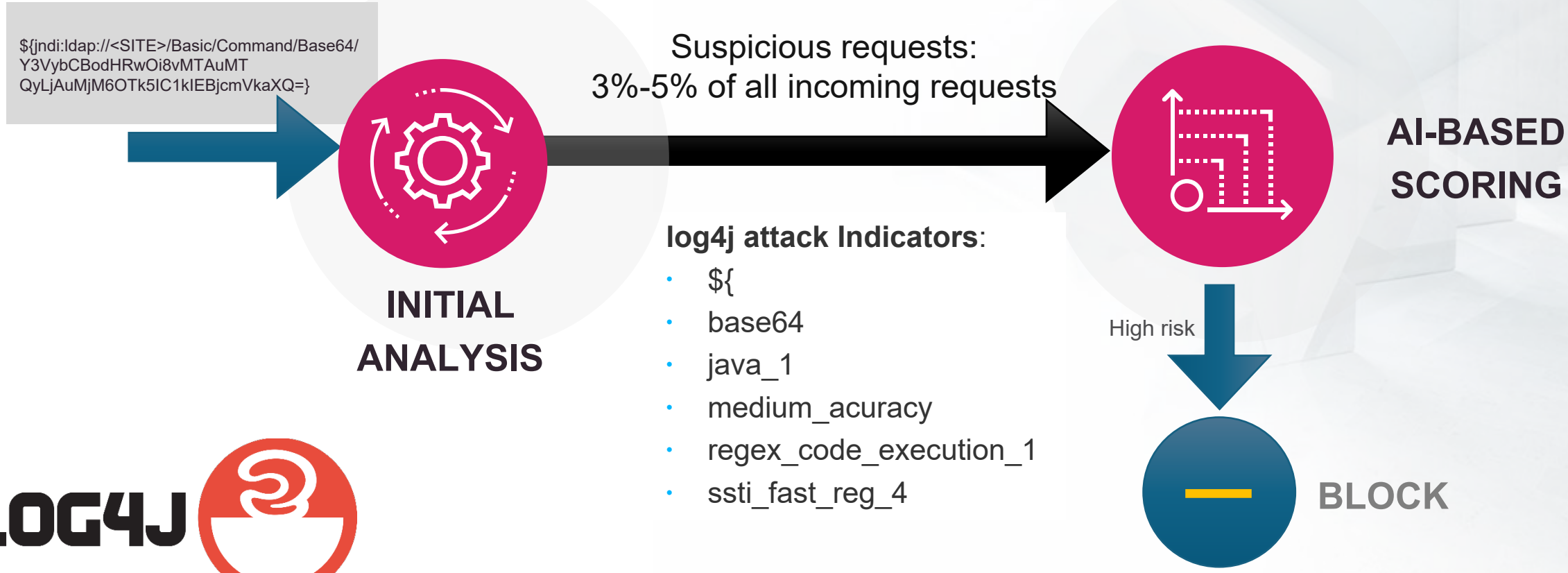


AI Powering Web & API Security

How AI AppSec uniquely preempts exploitation of Apache server zero-day vulnerabilities

- Initial payload analysis
- Base64 decoding (avoid evasions)
- Collection of telemetry/statistics

- Low reputation (single suspicious request)
- Application awareness – uncommon content
- Indicator scoring – multiple indicators of attack



LOG4J

AI Blocking never-seen-before Phishing Attac

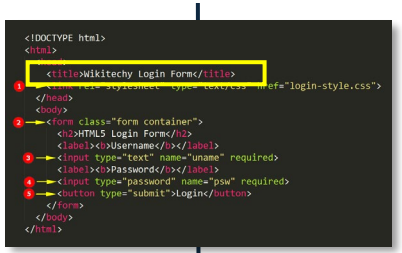
PATENTED

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

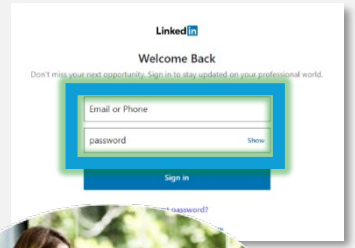


#2 CHECK POINT'S INJECTION

GET

RESPONSE

#3 BROWSER INSPECTION (BY INJECTED CODE)

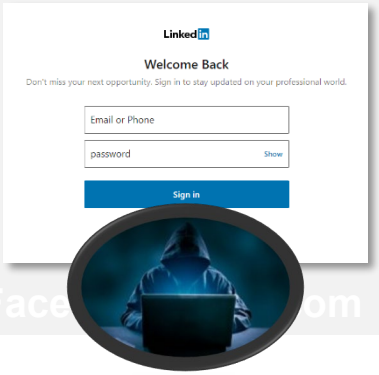


GET

RESPONSE

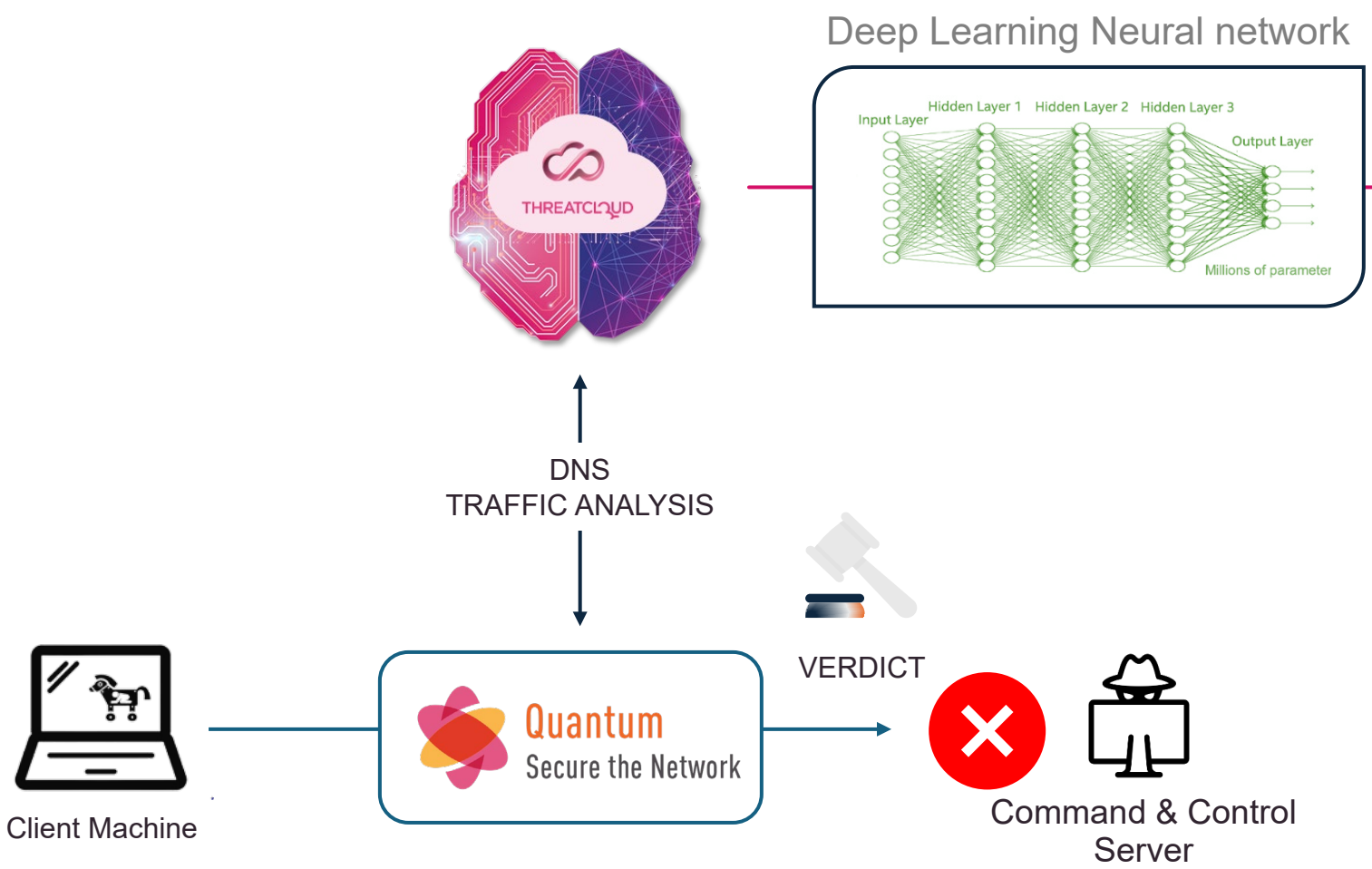
Quantum
Secure the Network

PHISHING SITE
LinkedInscam.com

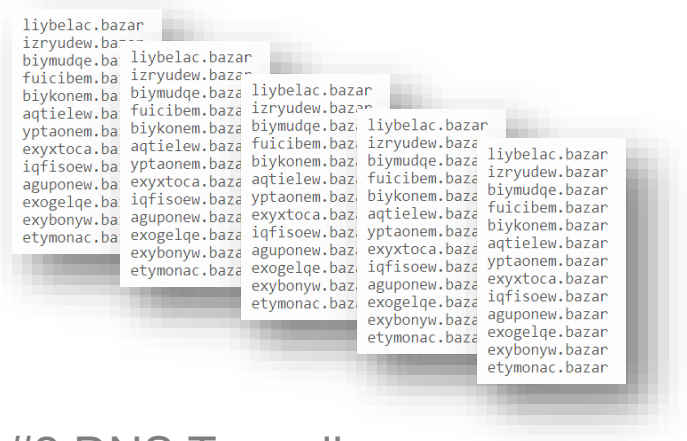


AI Preventing 5X more sophisticated DNS attacks

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



#1 DGA (Domain Generation Algorithm)



#2 DNS Tunneling

```
6a57jk2ba1d9keg15cbg.app sync-api.eu-west-1.avsvmcloud.com
7sbvaemscs0mc925tb99.ap sync-api.us-west-2.avsvmcloud.com
gq1h856599gqh538acqn.ap sync-api.us-west-2.avsvmcloud.com
ihvpgv9psvq02ffo77et.apps nc-api.us-east-2.avsvmcloud.com
k5kcubuassl3alrf7gm3.apps nc-api.eu-west-1.avsvmcloud.com
mhdosoksaccf9sni9icp.apps nc-api.eu-west-1.avsvmcloud.com
```

```
f5534496-1a85-4844-8bc0-e9edc537ea40.serve -26. eeponlines.com
f5534496-1a85-4844-8bc0-e9edc537ea40.serve -34. eeponlines.com
f5534496-1a85-4844-8bc0-e9edc537ea40.serve -5.d eponlines.com
f5534496-1a85-4844-8bc0-e9edc537ea40.serve -98. eeponlines.com
f5534496-1a85-4844-8bc0-e9edc537ea40.serve -73. eeponlines.com
f5534496-1a85-4844-8bc0-e9edc537ea40.serve -82. eeponlines.com
f5534496-1a85-4844-8bc0-e9edc537ea40.serve -15. eeponlines.com
f5534496-1a85-4844-8bc0-e9edc537ea40.serve -59. eeponlines.com
```

AI Preventing malicious Code Packages

Securing Software Supply Chains at the earliest stages of the CI/CD pipeline

User wants to use a new code package from a known repository

Step 1: Download locally

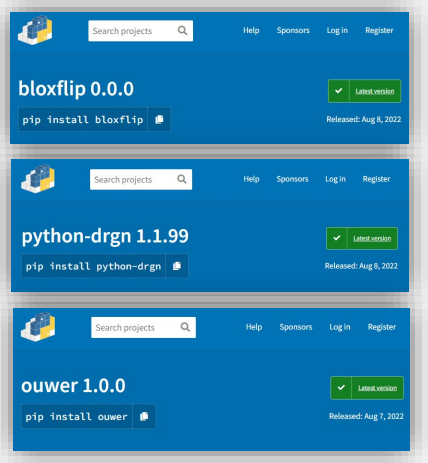
Step 2: Commit to CI pipeline

Step 3: Testing (including security)

+ Other vendors

Step 4: Deploy to staging and production

Actual preventions by Check Point:



Known vulnerable packages:

AXIOS

pandas

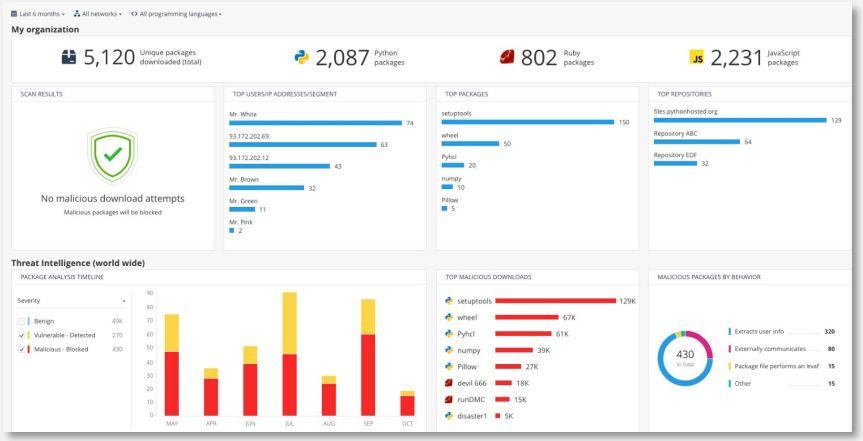
NumPy

wheel

Express

scikit learn

Visibility on code packages traffic:



Try Check Point's AI For 14 days for Free

Microsoft SECURITY CHECKUP | EMAIL PROTECTION | OVERVIEW

AVANAN

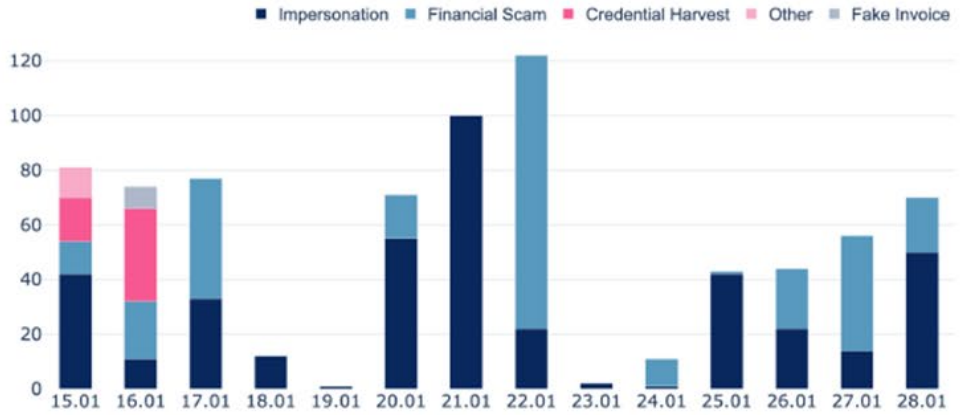
These graphs provide an overview of the detected phishing emails and how they were handled by the policy.

Total Security Events **5874**

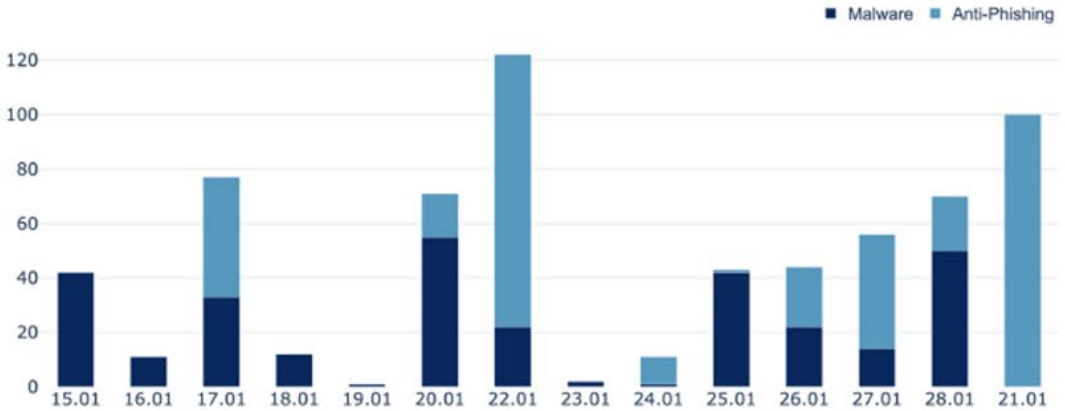
Out of which:

Phishing	Malware	Spam	Other
325	458	1458	1234

Top Phishing Detection Reasons

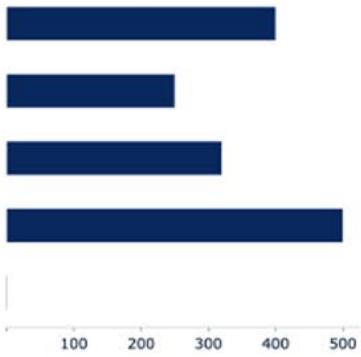


Events Trend



Top Attacked Users

VIP	User Name	User Email
♛	David aaa	david@avananXXX1.com
	David	david@2.com
♛	aaa	david@3.com
	Joseph	david@avana41.com
	Davido	david@avanan51.com

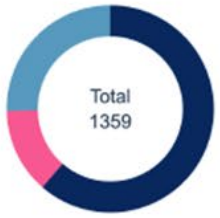


Scanned Elements

Emails
3589

Attachments
1000

Security Events by Enforcement



Log security Event	834
Warning Banner	344
Quarantine	181

Thank you!

Ian Porteous

Regional Director, Sales Engineering | Office of the CTO

Check Point

YOU DESERVE THE BEST SECURITY