Artificial Intelligence with Check Point - Security and Strategy

Sep 2023

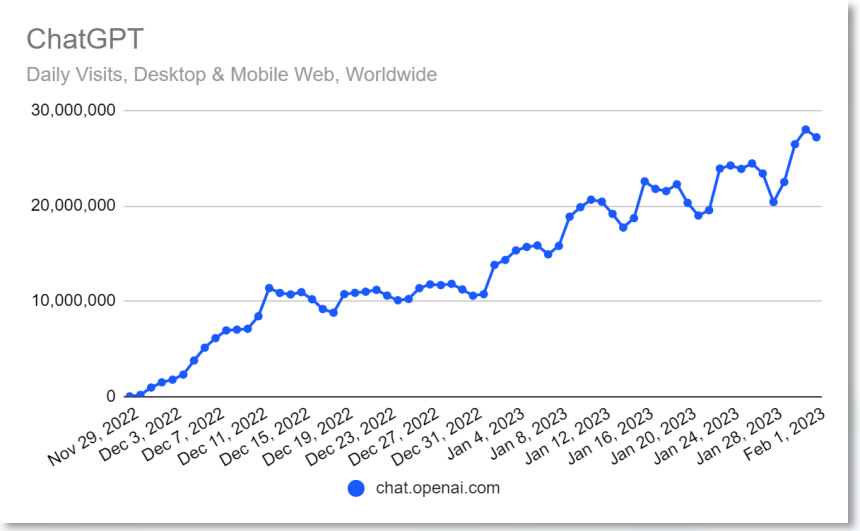
Yaniv Shechtman | Head of Product Management, Threat Prevention

Dan Karpati | Chief Technologist, Threat Prevention

YOU DESERVE THE BEST SECURITY

The year of AI

Adoption rate (daily visits)



similarweb

100M users

Jun, 2023

Market landscape

ChatGPT

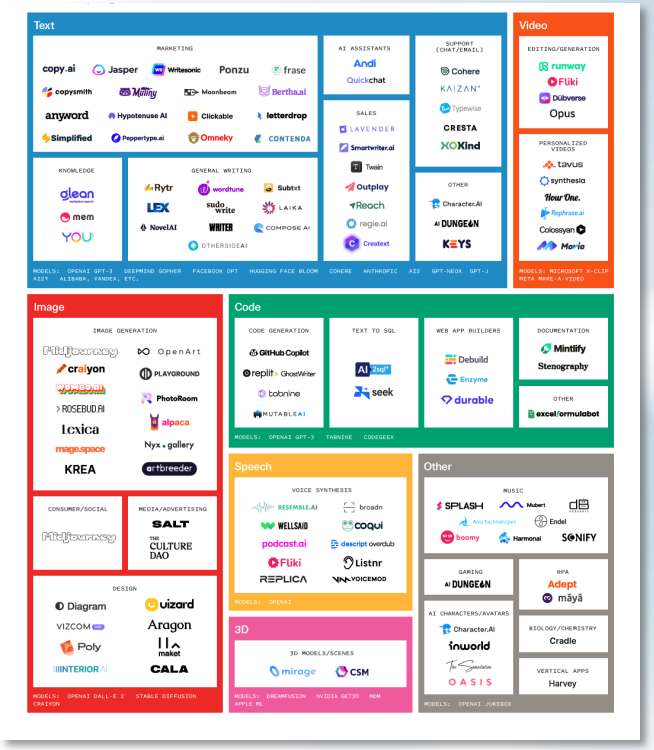
GPT-4 is OpenAI's most advanced system, producing safer and more useful responses

Bard AI

Google Cloud advances generative AI at I/O: new foundation models, embeddings, and tuning tools in Vertex AI

Meta AI

Introducing LLaMA: A foundational, 65-billion-parameter large language model



Lots of progress across all AI frameworks, GenAI is at the front

The human element of Generative-AI (GenAI)

As human beings:

- Flood of GenAI outputs and ideas
- Inaccurate information goes deep (looks real) and wide (all over the place)
- Deliberate fake and manipulative information
- Modernizations of jobs – redefine your profession as ‘me plus my co-pilot’

The New York Times

GPT-4 Is Exciting and Scary

Today, the new language model from OpenAI may not seem all that dangerous. But the worst risks are the ones we cannot anticipate.

How hackers use ChatGPT to code Ransomware attack?

Check Point Software Technologies, Ltd.
76.7K subscribers

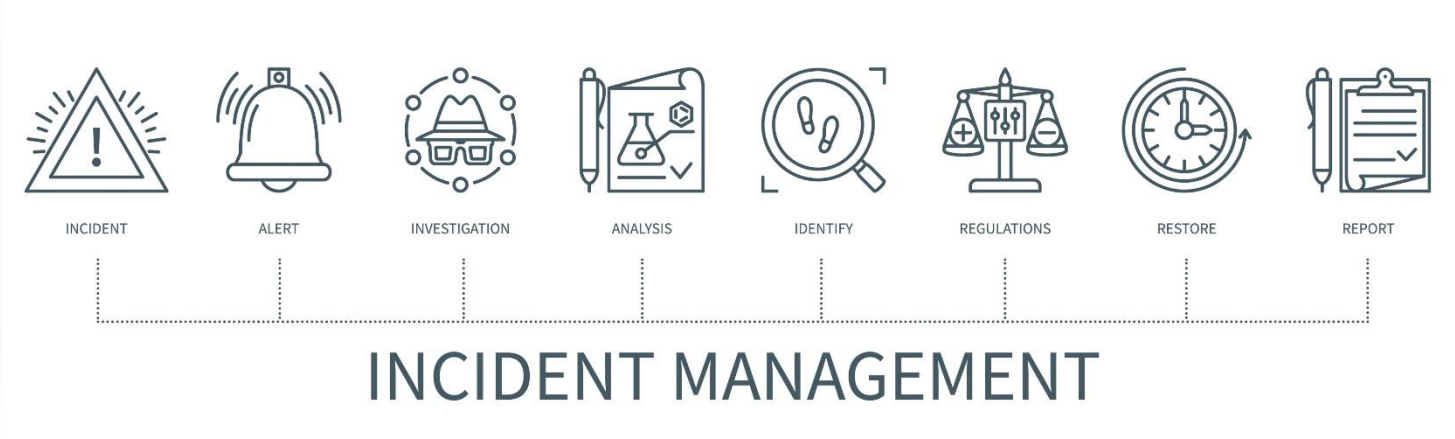
Subscribe

Where AI and Cyber meet

Attacks

Security & Prevention

Automation



On the CISO’s agenda

What we hear from you

- Securing the **Digital Transformation**
- The impact of **Generative-AI**
- **Zero-trust** across network and cloud
- **Consolidation** of security solutions and **ROI** of their investment
- **Prevent** company extortion

GenAI serves the attackers

GenAI is good for SOC tasks

Effective security prevention requires AI Deep Learning

AI STRATEGY

AI Strategy Pillars

Pillar 1 – Shaping the "next normal" of human experience

- Natural language human-machine Interfaces
- GenAI for extreme automation of usability and productivity

Pillar 2 – Unparalleled Threat Prevention

- AI-powered Security and Threat Prevention to find anomalies
- Unprecedented scale, speed and efficiency

Pillar 3 – Security of AI technology

- Secure vulnerabilities in the AI Technology
- Attackers will use AI

Pillar 4 – Scaling AI across the organization

- Data first mind-set
- Automate, scale and re-use across the org

5 Principles for a Winning AI Engine (at Check Point)

#1

Addresses a Significant Problem

#2

Utilizes Cutting-Edge Technology

#3

Easy to Explain

#4

Enables Fast Integration

#5

Includes a 2-Year Warranty

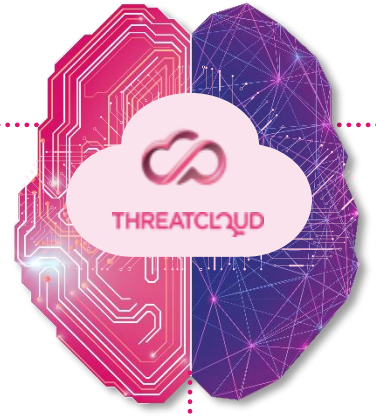
UNPARALLELED THREAT PREVENTION POWERED BY AI

ThreatCloud: AI brain behind Check Point Security

99.7%
Security effectiveness
BEST RESULT IN THE INDUSTRY*

AI technology

40+ AI and Machine Learning technologies that identify and block emerging threats that were never seen before



Big data threat intelligence

Always acquires the most recent IoCs and protections of latest attacks seen in the wild

Telemetry

ACCURATE PREVENTION

(MALICIOUS/SAFE)

Telemetry

ThreatCloud APIs

Quantum
Secure the Network

Horizon
Unified Management & Security Operations

CloudGuard
Secure the Cloud

Harmony
Secure Users & Access

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

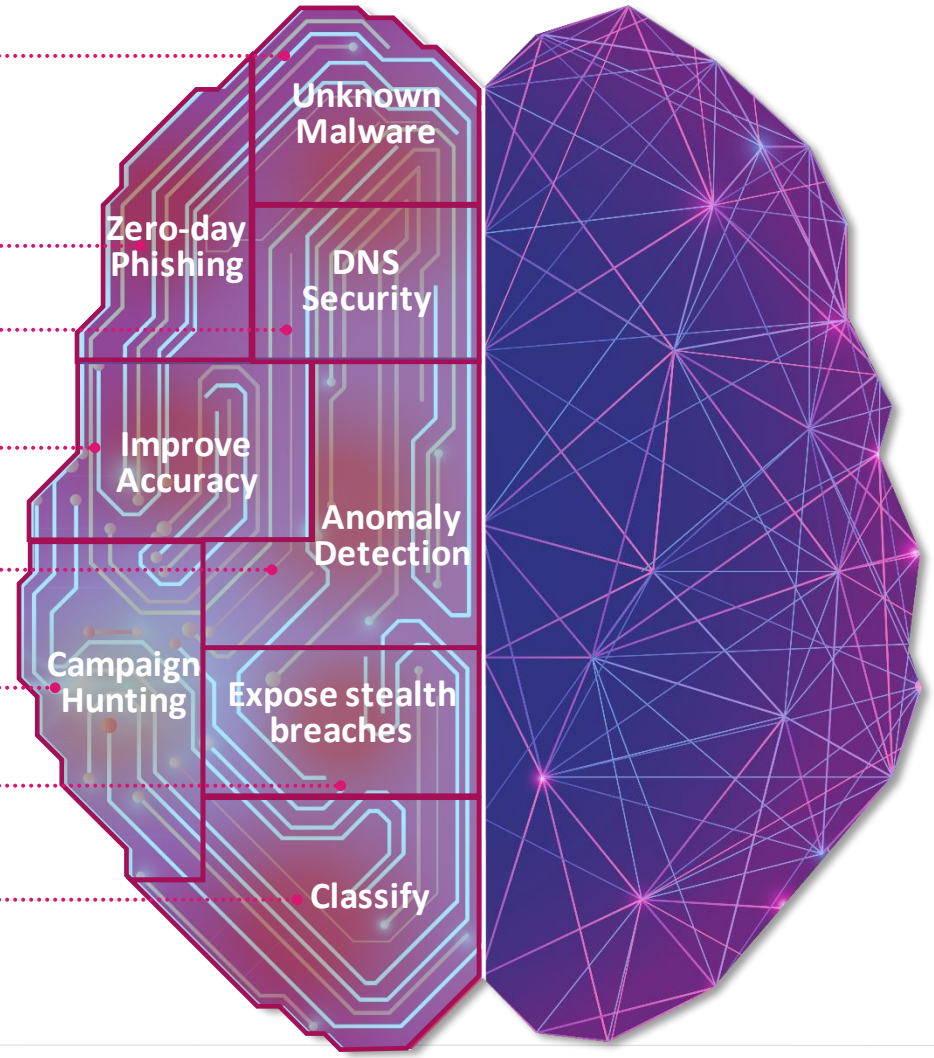
Network AI engines aggregator
Mobile AI engines aggregator
Machine validated signature

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

ThreatCloud Campaign Hunting

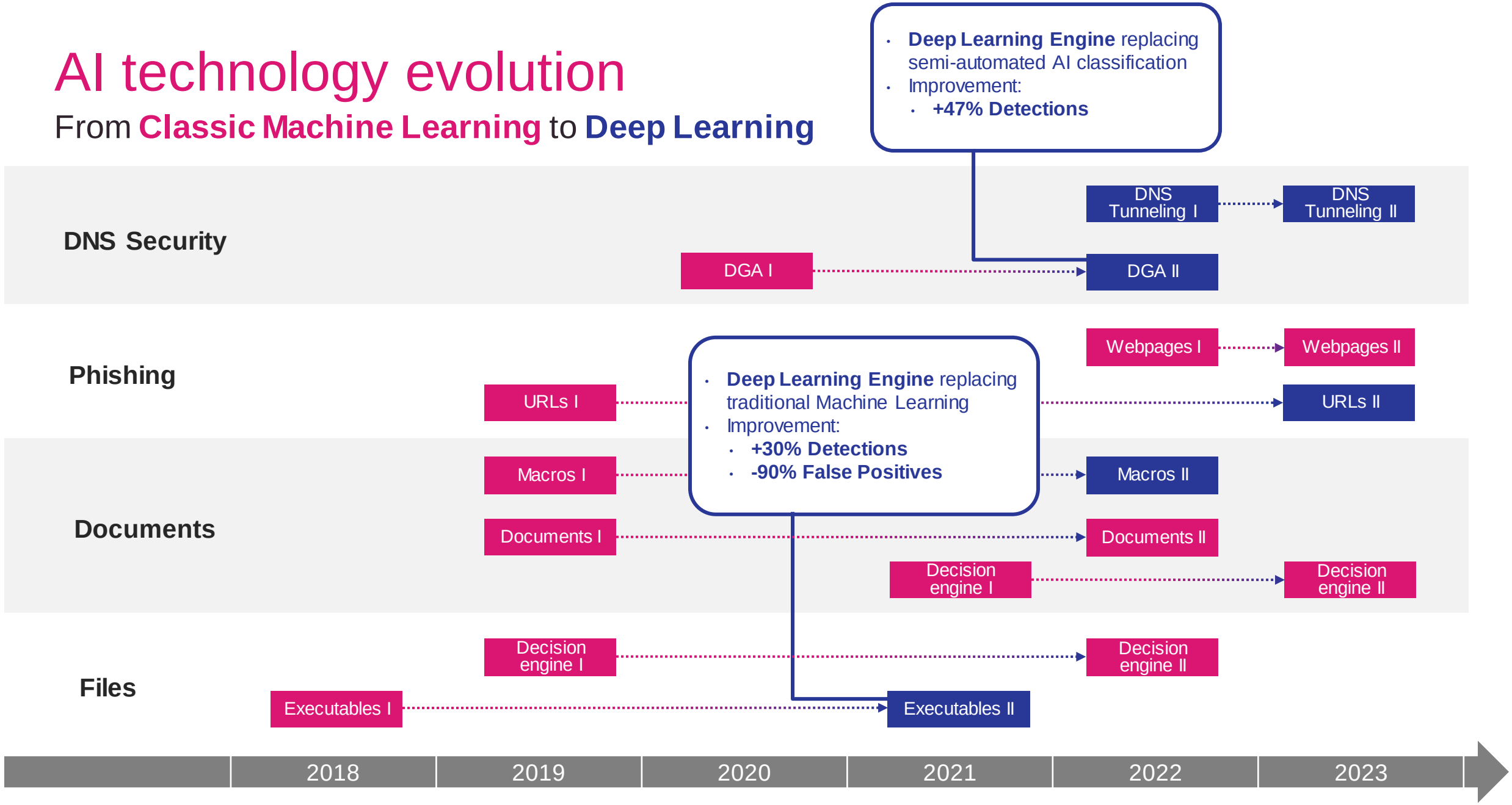
Analyst Mind
Malicious activity detection

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



AI technology evolution

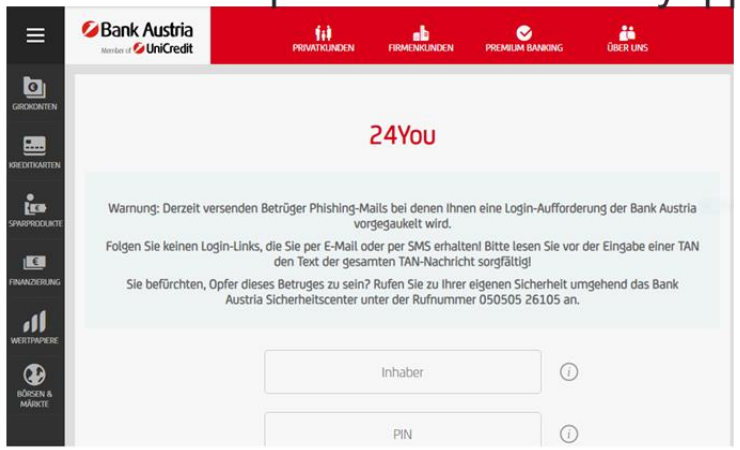
From **Classic Machine Learning** to **Deep Learning**

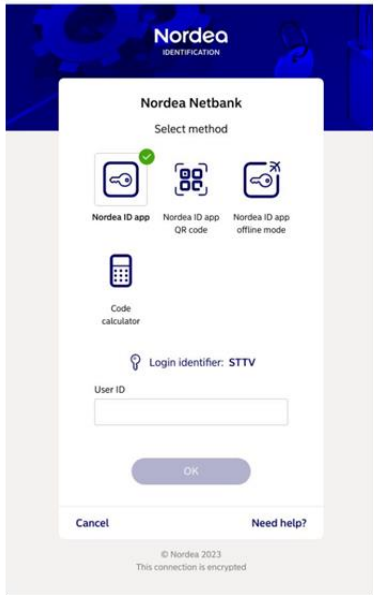


Local brand spoofing – Banking apps and websites

bankraiffeisen-ch.web.app

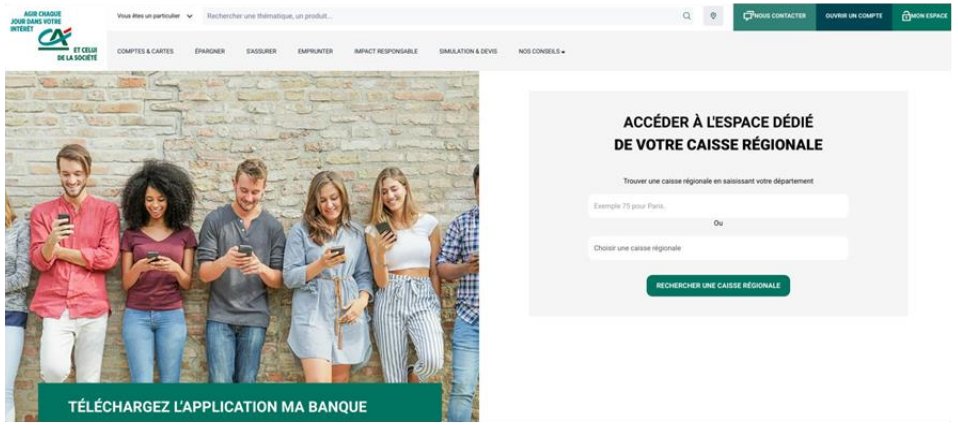
online-bankaustria-at-eservices2023psdi754465.codeanyapp.com





serviceappnetnordea.xyz/serv/netbank/nordea/Login/

erf-iepnz.formstack.com/forms/caixa



creditagricole-otp.172-232-56-179.plesk.page/44394

Blocking never-seen-before Phishing Attacks

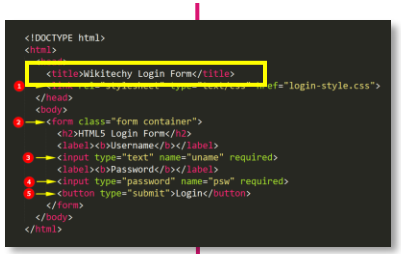
PATENTED

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



#3 BROWSER INSPECTION (BY INJECTED CODE)

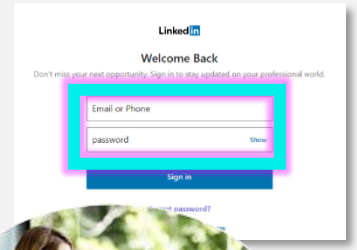
#2 CHECK POINT'S INJECTION

GET →

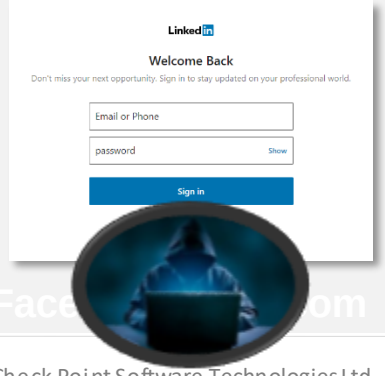
← RESPONSE

GET →

← RESPONSE



PHISHING SITE
LinkedInscam.com



The most comprehensive Zero-Day Phishing solution

Brands

- Local brand impersonation
- Brand phishing domain name
- Lookalike favicon
- Title brand similarity
- Copyright brand similarity
- Website impersonation
- Source code similarity

URLs

- Deep URL analysis
- Known malicious URL
- Path similarity
- Compromised website
- URL categories
- URL popularity
- Special TLD

Reputation

- IP reputation
- URL reputation
- Registrant reputation
- Domain reputation
- ThreatCloud graph (ROADMAP)

Domain

- Newly registered domain
- Real estate registrant
- Suspicious Regex
- Registered anonymously
- Domain classification
- Domain popularity

Cutting edge / deep analysis

- In browse (PATENTED)
- NLP
- Protections engine
- HTML model
- Static web emulation
- Dynamic web emulation

AI Based

Deep Learning

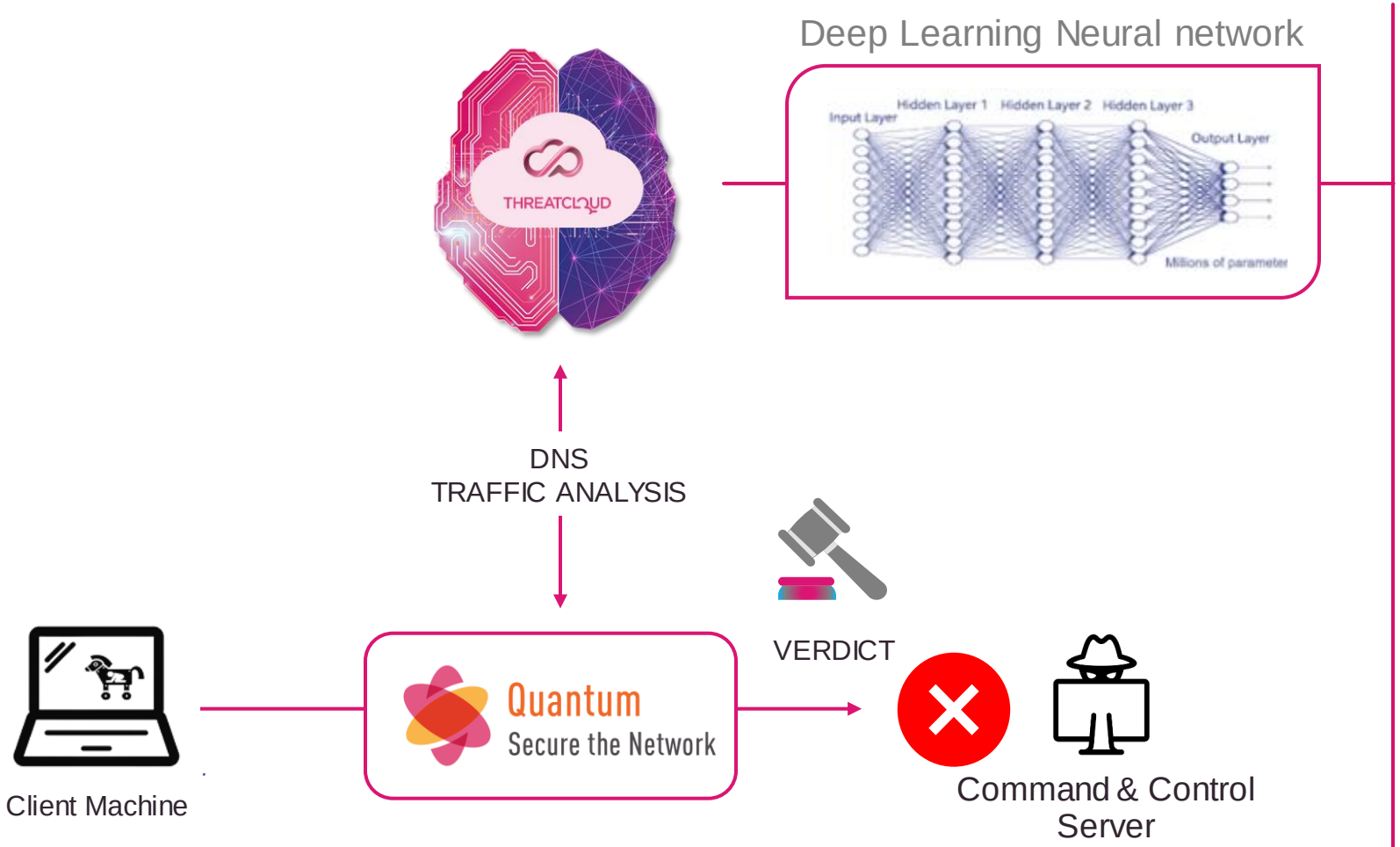
Patented

Harmony Connect | Harmony Endpoint | Harmony Mobile | Harmony Email | Quantum

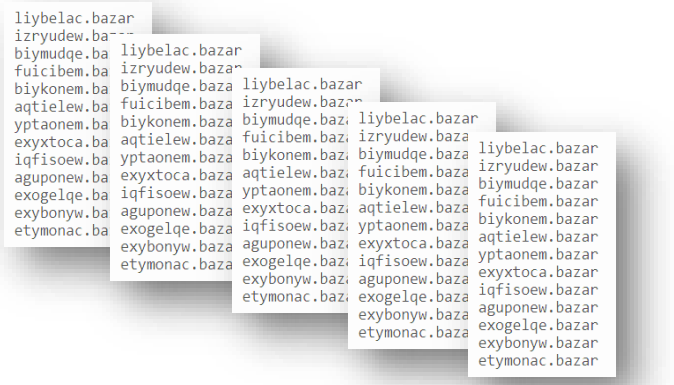
Prevents 5X more sophisticated DNS attacks

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

PATENTED



#1 DGA (Domain Generation Algorithm)



#2 DNS Tunneling

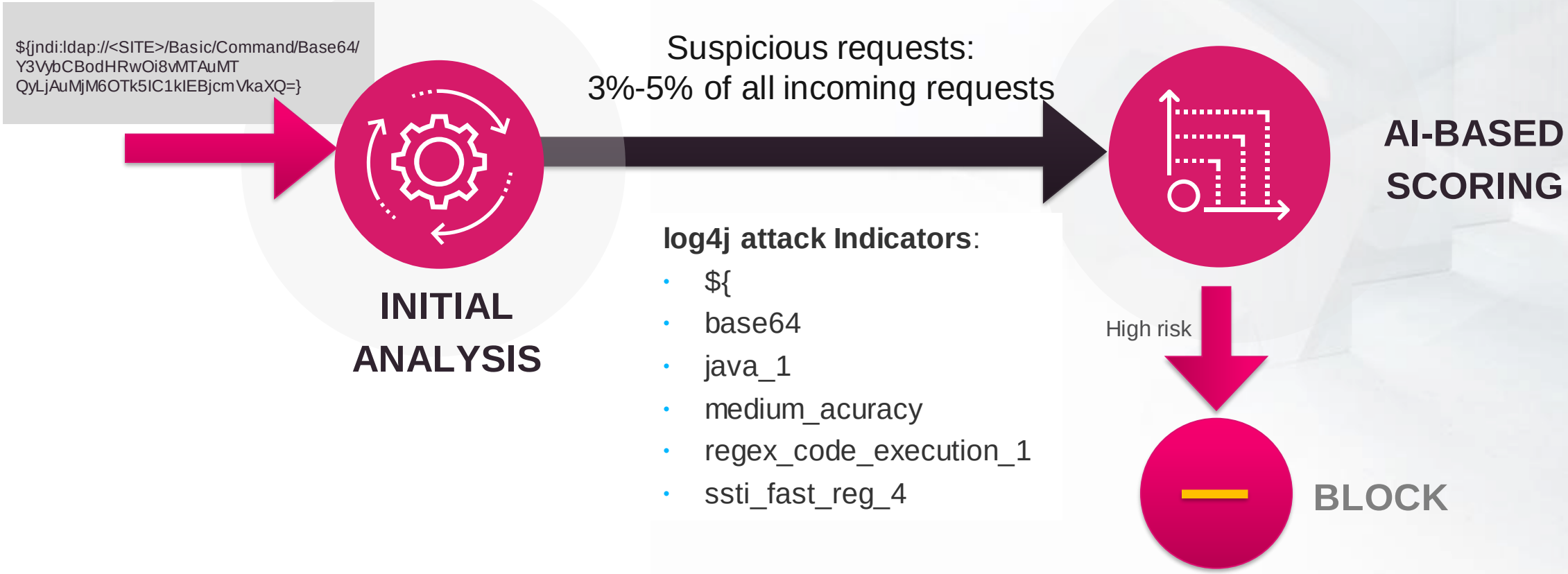
6a57jk2ba1d9keg15cbg.appsync-api.eu-west-1.avsvmcloud.com
7sbvaemscs0mc925tb99.appsync-api.us-west-2.avsvmcloud.com
gq1h856599gqh538acqn.appsync-api.us-west-2.avsvmcloud.com
ihvpgv9psvq02ffo77et.appsync-api.us-east-2.avsvmcloud.com
k5kcubuassl3alrf7gm3.appsync-api.eu-west-1.avsvmcloud.com
mhdosoksaccf9sni9icp.appsync-api.eu-west-1.avsvmcloud.com

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

How 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



Preventing malicious Code Packages

At the earliest stage possible of the CI/CD pipeline

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

CHECK POINT prevention

Step 1: Download locally

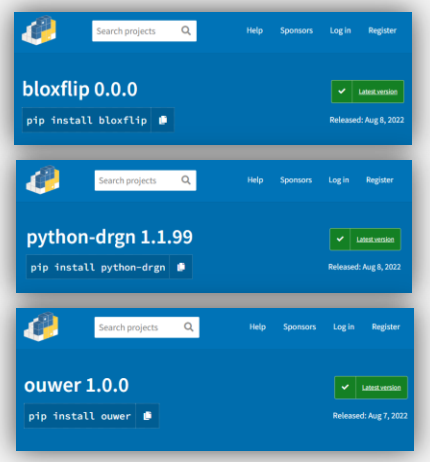
Step 2: Commit to CI pipeline

CHECK POINT + Other vendors

Step 3: Testing (including security)

Step 4: Deploy to staging and production

Actual preventions by Check Point:



Known vulnerable packages:

Visibility on code packages traffic:

GEN-AI AND CYBER SECURITY

ChatGPT - Risks

- ChatGPT usage has cyber security Implications.
- Employees are eager to take advantage of Generative AI

- Risks:
  - Leakage of sensitive data
  - Leakage of code
  - Supply chain attack (code poisoning)
  - Leakage via 3rd party SaaS plugins (AI-based)

- Opportunities:
  - Data-Leakage solutions, Hashing PII data
  - Prompt inspection with AI
  - Local LLM – privacy, security, costs

Security Operations will be Augmented & Automated

Generative AI can assist in automating security operations daily tasks

- Threat Intelligence:
  - Analyze news - identify emerging threats and patterns
- Incident Response:
  - Categorize, prioritize, and analyze security incidents
  - Automated workflows & incident response
- Security Policy:
  - Ensuring policies enforced consistently across the organization
  - Alert policy violations
  - Recommend remediation & actions
  - Create zero-trust networks
  - Resolve tickets
  - Assist projects
  - Optimize resources - activate security blades on demand

- **"Why many users complain about Zoom connectivity?"**
- **"Am I impacted by CVE-2023-4852?"**
- **"Please solve ticket SR84215"**

Enterprises will isolate their Data in walled gardens

- Data will become an intellectual-property
- Enterprises will harness data-first strategy
- Companies will isolate their data
- Enterprises will accumulate huge amounts of raw data
- Un-reasonable to upload to cloud (amounts, privacy, regulations)
- More local processing AI power – at the Edge

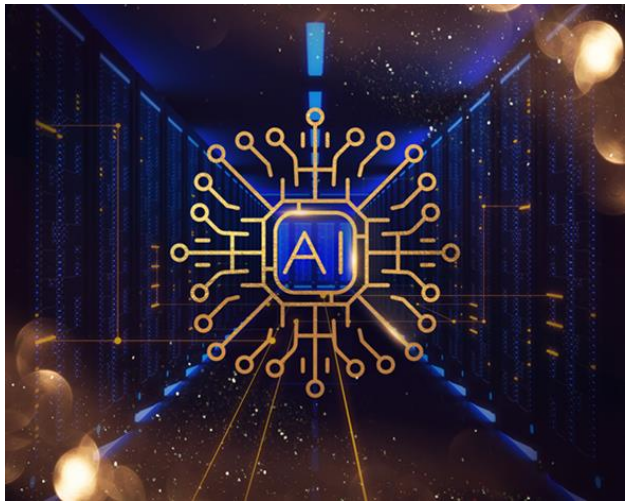
Opportunities:

- GPUs (LLMs) @ Edge
- Personalized adaptive security, Whitening traffic

New types of attacks will emerge

- AI models becoming a target
- Adversaries re-engineer how AI trained & operates
- Guess weaknesses by the input and results
- Poison the data trained, mis-information, unbalanced data
- Offensive Cyber, DeepFake (voice, video, chat, e-mail)

- Opportunities:
  - Polymorphic protections with GenAI – gain resiliency
  - AI ‘Shield’



Machine-to-machine interactions (Auto-GPT)

- Generative-AI will replace back-office tasks
- Human roles will be automated
- Future will be machine-to-machine (AI-to-AI) interactions
  - E.g. call center: customer support request will trigger actions in multiple systems
- AI will code, build and deploy fixes
- AI will instantiate infrastructure..
- Attackers can fool systems to orchestrate devastating attacks
- .. harmless workloads could freak out

Opportunities:

- Prompt security – input & output..
- Identify intent

Data Becomes a Strategy

- Data mindset
  - **Data-first** mind-set = competitive edge
  - Reinforcement Learning Human Feedback (RLHF)

- AI mindset in products operations
  - Code generation
  - Code testing
  - Protections generation
  - Performance optimization
  - AI @ edge (GPUs at firewalls, endpoints) - privacy, security, Costs

AI projects – 2024 motion

ROADMAP

Project 1: XPR Incident Summary

- Provide textual summarization, specific insights, chat interface to ask follow-up questions and remediation suggestions for XPR incident

Project 2: Smart1 Admin Management Co-pilot

- AI-powered "Admin Co-pilot" to automate policy change requests. For example – a ticket request to allow a new finance member to access Salesforce will be resolved with GenAI access rules into existing policy

Project 3: Generative Security Policy (based on seen activity)

- Automatically generate a hardened policy for servers based on logs from XPR. Will allow the prevention of zero-day attacks such as Log4j, Proxyshell (Exchange) & MOVEit

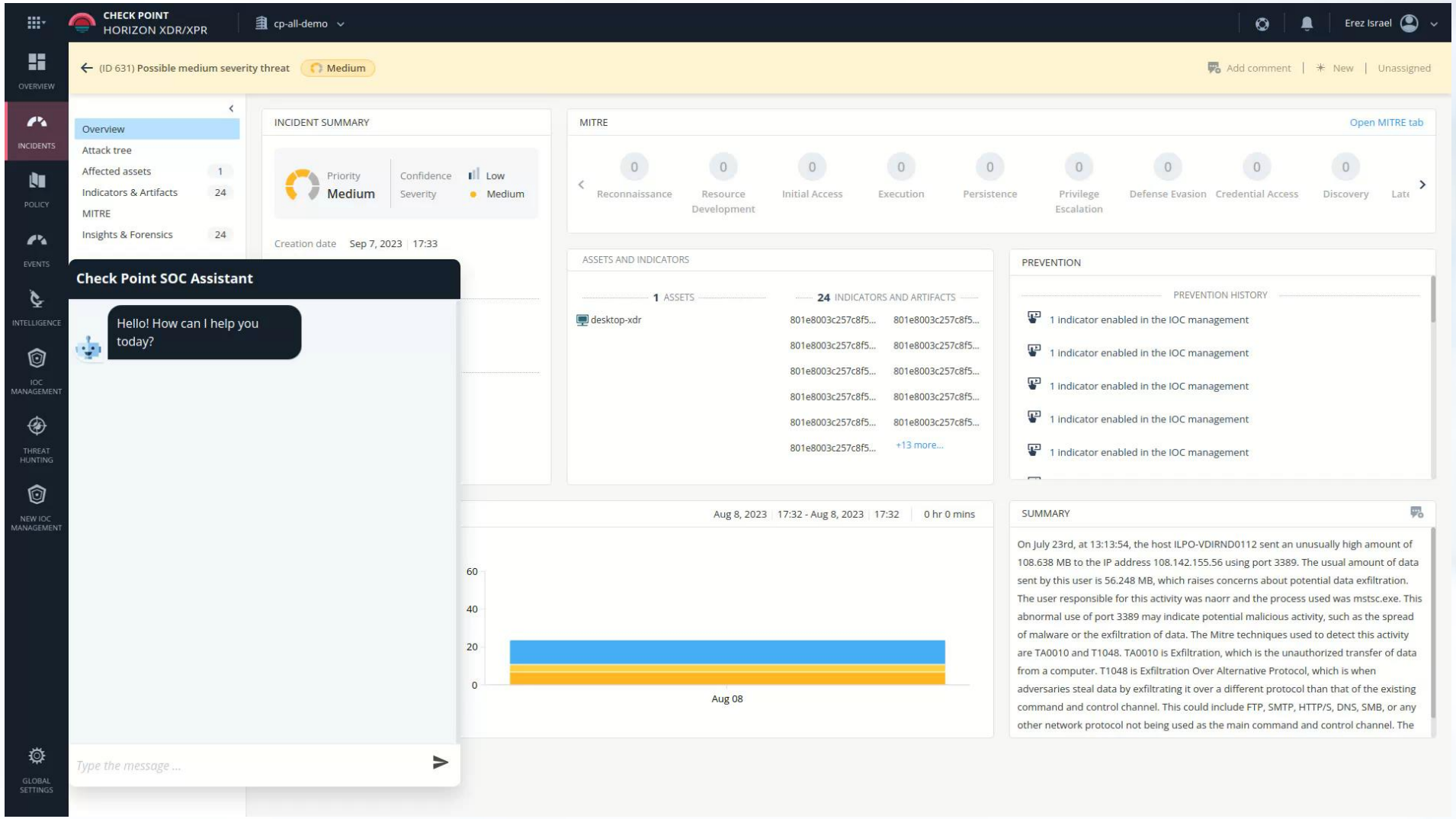
Project 4: AFW – zero-trust network (segmentation)

- Automatic firewall policy generation based on network traffic, creating network segmentation with access rules

Project 5: GenAI for IPS

- Automatically generate IPS protections that are able to cover new attacks quickly based on few traffic samples

Project 1 demo



Project 2 demo

portal.checkpoint.com/dashboard/smart-1cloud#/policy

QUANTUM SMART-1 CLOUD | Workspace MT2 | Albert Khavinson | CHECK POINT INFINITY PORTAL

Install Policy | Discard | Session | Publish

WELCOME | POLICY | CONNECT GATEWAYS | LOGS & EVENTS | SETTINGS | GLOBAL SETTINGS

Standard

- Access Control
  - Policy
  - NAT
- Threat Prevention
  - Custom Policy
  - Autonomous Policy
    - Policy
    - File Protections
    - Settings
  - Exceptions
- HTTPS Inspection
  - Policy

Access Tools
- VPN Communities

Install Policy | Actions

No.	Name	Source	Destination	VPN	Services & App...	Action	Time	Track	Install On	Comments
1	Cleanup rule	Any	Any	Any	Any	Drop	Any	None	Policy Tar...	

Summary | Logs

Drop | Rule 1

Cleanup rule

Comment:

Created by: System
Date created: 17-Nov-22 03:43
Expiration time: Never
Hit Count: 0 (0%, Zero)

Additional Rule Info:
Ticket Number:
Ticket Requester:

Search... | New...

Object Categories

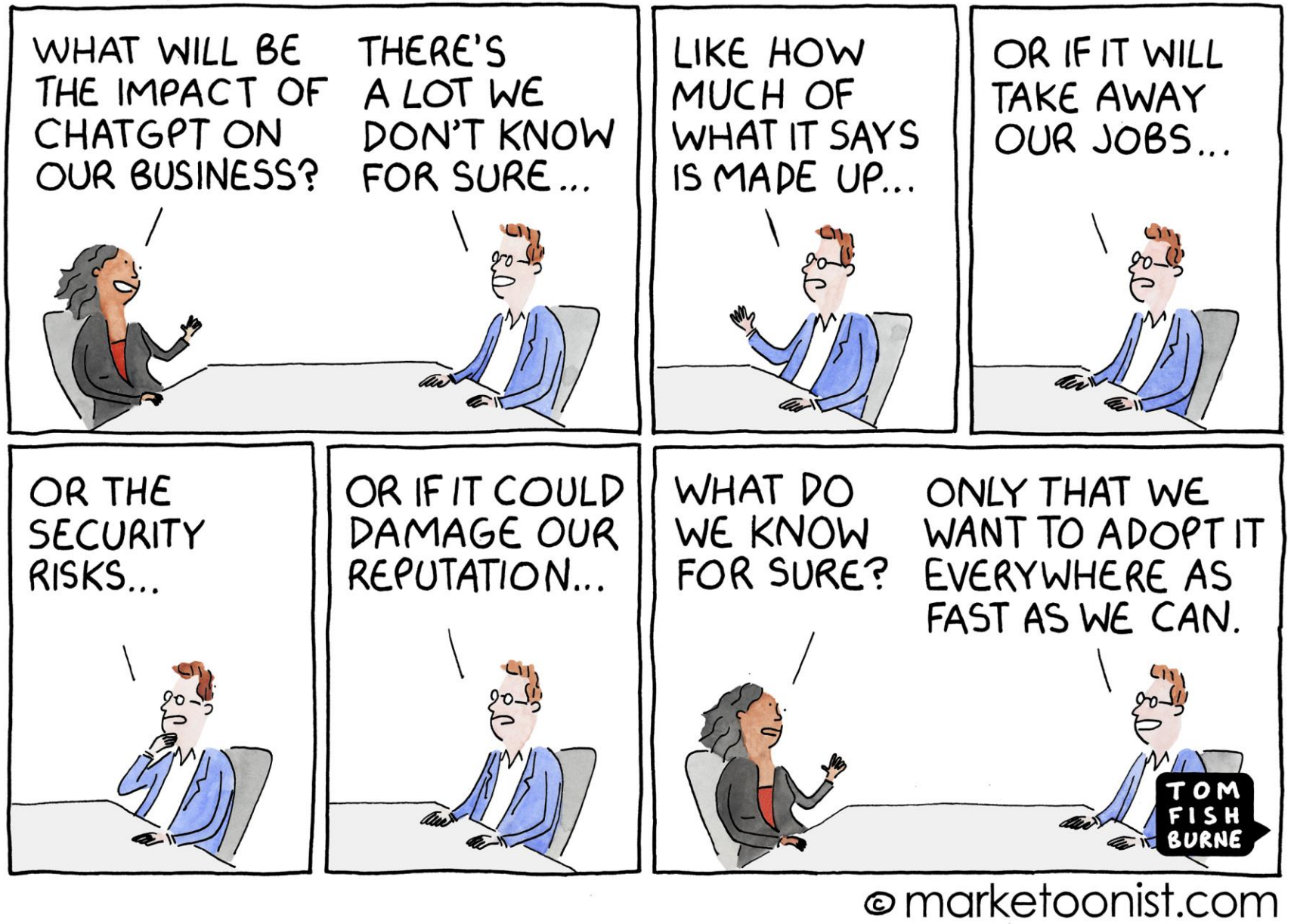
Network Objects	19
Services	523
Applications/Categories	10181
VPN Communities	2
Date Types	62
Users/Identities	1
Servers	1
Time Objects	3
UserCheck Interactions	15
Limit	4

Objects | Validations

No tasks in progress | Open in full SmartConsole | No changes

Challenges in adopting AI for prevention

- AI is as good as your data
- Balance between data collection and privacy
- Skill shortage
- Easy to claim, hard to prove
- Contextual understanding of what is ‘good’ and what is ‘bad’ (values based)



AI-driven Threat Prevention stops all cyber attacks

3CX · JBS · COLONIAL PIPELINE CO. · Exchange · Kaseya · LOG4J

Reconnaissance → Resource Development → Initial Access → Execution → Persistence → Privilege Escalation → Defense Evasion → Credential Access → Discovery → Lateral Movement → Collection → Command and Control → Exfiltration → Impact

Entry points:

- **Social engineering**
- **Supply chain**
- SW and Protocols **Vulnerabilities**
- **Cloud misconfigurations**

Gaining persistence:

- **Zero-trust** access & strong policies
- **AI-based prevention** for malware, docs, phishing
- Blocking **C&C** communication
- **Cloud posture** management & workload protection
- Server **hardening**
- **Shift-left** source code & developers
- **Native XDR** – network, endpoints, servers, cloud, mobile, email, AD, more

Lateral movement:

- **Cloud posture** management
- **Zero-trust** and **micro-segmentation**
- **AI-based prevention** on endpoints & servers
- **Analysis of AD** / ADFS / Access token (SAML, OAuth 2.0) & user behaviors
- **Native XDR**

Data leak:

- **Cloud posture** management
- **AI-based prevention** on endpoints & servers
- **Gateway IPS / Anti-BOT** protections
- **Native XDR**
- **DLP**
- **NDR**

CHECK POINT™

Thank you!

YOU DESERVE THE BEST SECURITY