CHECK POINT

CISO's and Executives need to understand and deal with AI: The Good, The Bad and the Ugly!

Bonus: How to be a better leader!

Pete Nicoletti | Global CISO of Americas

YOU DESERVE THE BEST SECURITY

Speaker Intro Work Life: Pete Nicoletti

Skills: Executive Level Strategy Consulting, Incident Response, BOD Consulting
Product Management, Cyber Security, MSSP Operations, Security Operations, Security Budgeting

Certs and Training: CCSK, CISA, CISSP, SANS GIAC, FCNSP, CCSE

Experience: 20 years at CISO level, 33 years in Information Technology

- CISO – Field, Americas Check Point Software Technologies World Leader in Security
- CISO – Cybraics: Artificial Intelligence and Machine Learning Based Analytics Platform
- CISO - Hertz Global Car Rentals and Sales
- CISO - Virtustream/RSA/EMC/DELL
- VP Security Engineering Terremark/Verizon

Accomplishments:

- Gartner's "most secure cloud design" #1 and #2
- Whitehouse.gov, FBI.Gov, DOT.gov, Veterans Administration, Library of Congress and many more Federal Projects
- Managed two clouds through FedRAMP and eventually to EAL 5
- Book Author/Contributor: "An Intel Reference Design for Secure Cloud" "First 90 Days As CISO" "Security Desk Reference: Content Filtering"
- Secret Service - Miami Electronic Crime Task Force, FBI Infragard Contributor, Started S. Florida ISSA, and BOD for Cloud Security Alliance
- Awarded Top 100 Global CISO in 2017

Real Life: Pete Nicoletti

Why am I passionate about this subject?

I want help you to prevent this:

"Hi, my name is Brian Krebs

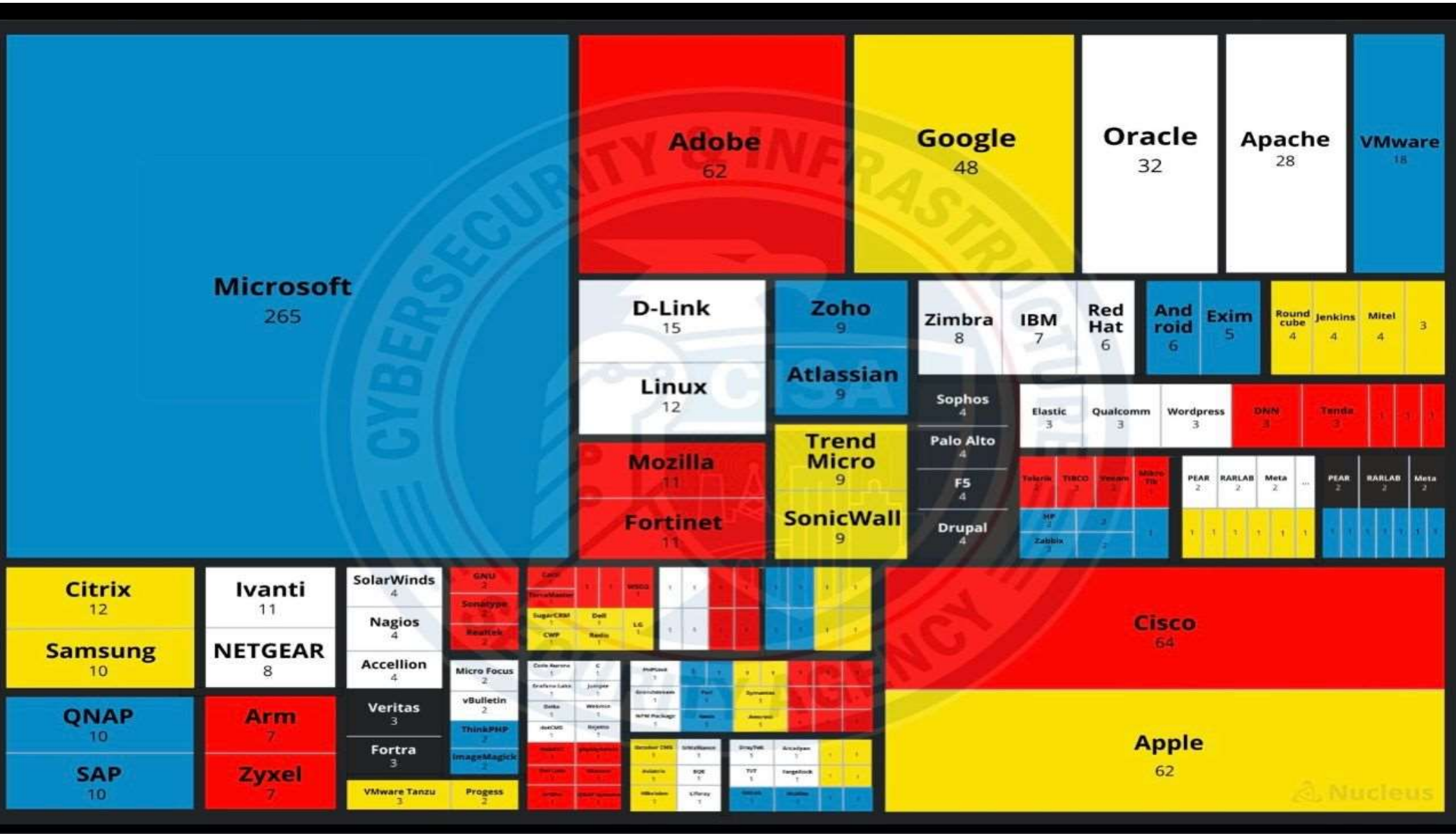
and I would like to

talk to you about your situation"

Don't use this talking point:

"Someone recently told me…"The best defense

still gets scored upon…"


Microsoft
265
Adobe
62
Google
48
Oracle
32
Apache
28
VMware
18
D-Link
15
Linux
12
Zoho
9
Atlassian
9
Zimbra
8
IBM
7
Red Hat
6
And roid
6
Exim
5
Round cube
4
Jenkins
4
Mitel
4
3
Sophos
4
Palo Alto
4
F5
4
Drupal
4
Elastic
3
Qualcomm
3
Wordpress
3
DNN
3
Tenda
3
Mozilla
11
Fortinet
11
Trend Micro
9
SonicWall
9
Citrix
12
Samsung
10
Ivanti
11
NETGEAR
8
QNAP
10
SAP
10
Arm
7
Zyxel
7
SolarWinds
4
Nagios
4
Accellion
4
Veritas
3
Fortra
3
VMware Tanzu
3
GNU
2
Sonatype
2
Realtek
2
Micro Focus
2
vBulletin
2
ThinkPHP
2
ImageMagick
2
Progess
2
Cisco
64
Apple
62
Nucleus

Agenda For Today!

CISO's and Security Pro's need to have awareness of risks & Benefits:

- **Risks and Analysis**
- **Benefits and Analysis**

Need Guidance? Here we go!

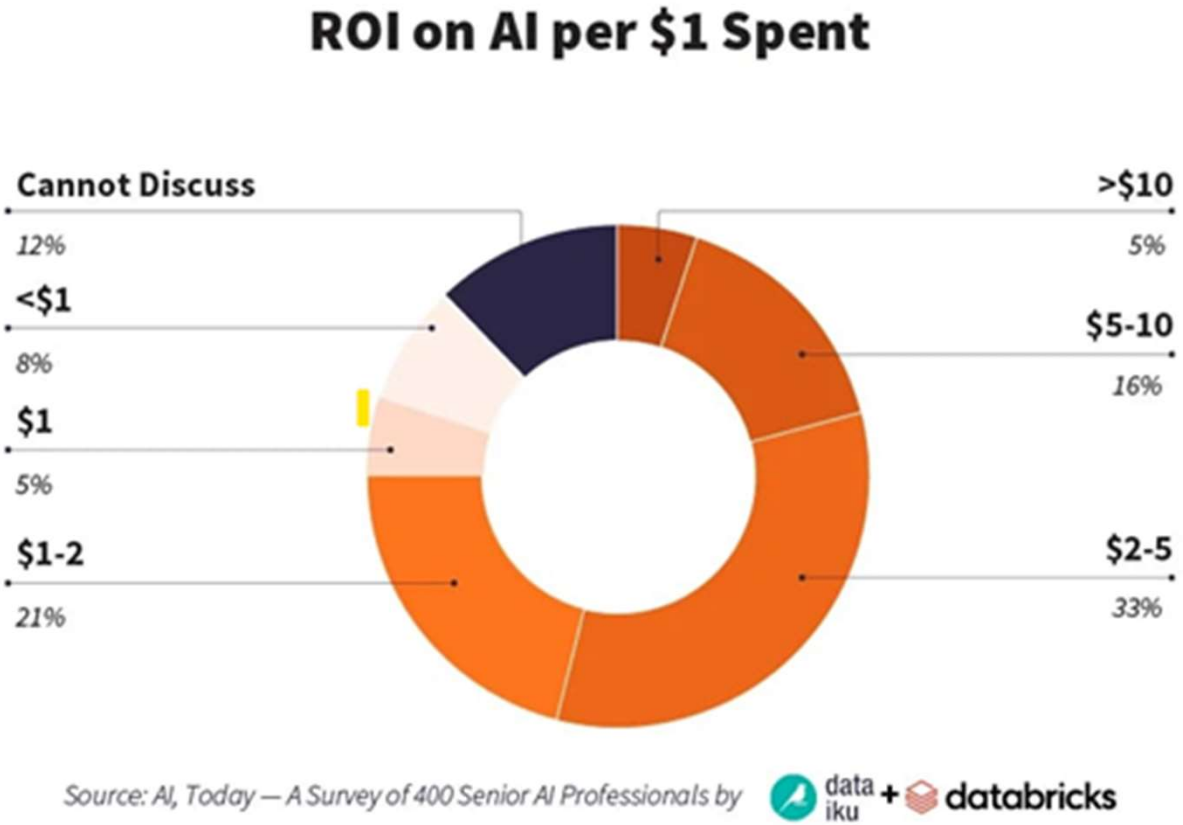
Some examples of AI tools that are of interest to the Business

How AI used used in security tools

Questions to Ask and Plan for AI issues with your Team and Executives

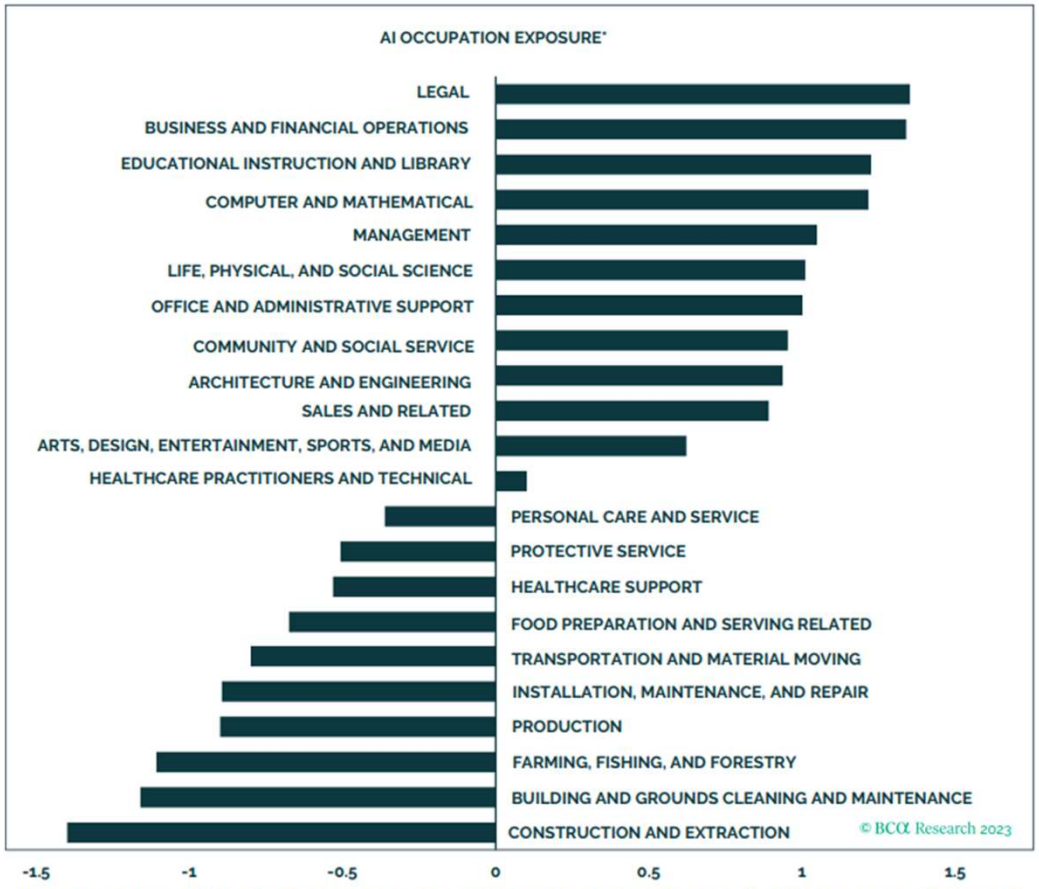
Is the Future "SkyNET" "M3GAN" "I, Robot" or…"J,A.R.V.I.S" ??

Start with some good news:
ROI on AI Investments: Our Goal!



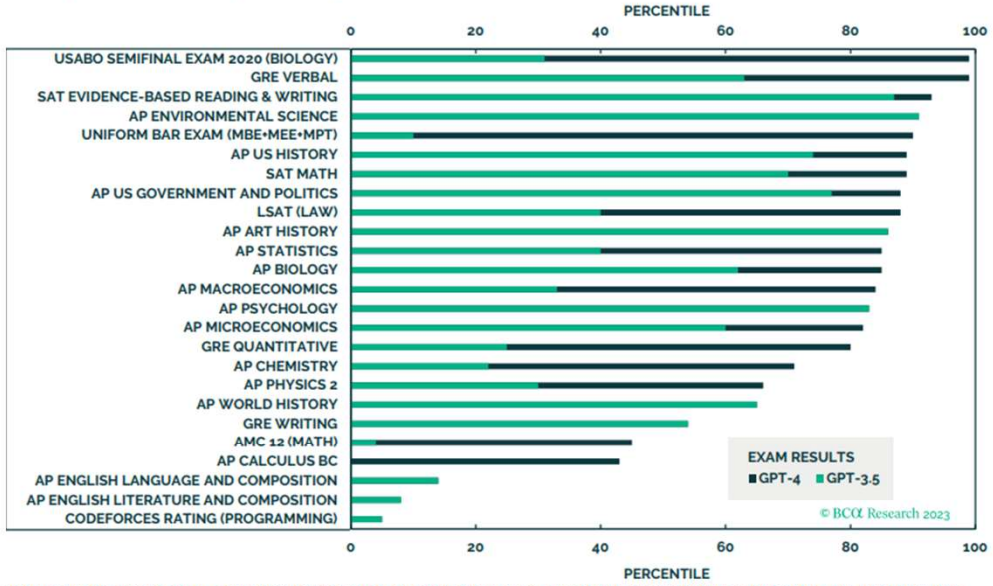
More Good News! tests they pass, and Lawyers Replaced!

AI Has The Potential To Replace Many Tasks Performed By Humans



* MEDIAN SCORE OF OCCUPATIONS (SIX-DIGIT STANDARD OCCUPATIONAL CLASSIFICATION LEVEL) IN EACH OCCUPATION MAJOR GROUP (TWO-DIGIT STANDARD OCCUPATIONAL CLASSIFICATION LEVEL). CALCULATION USING DATA FROM FELTEN ET AL. (ACCESSED ON MAY 1, 2023).
SOURCE: EDWARD FELTEN, MANAV RAJ, AND ROBERT SEAMANS, "OCCUPATIONAL, INDUSTRY, AND GEOGRAPHIC EXPOSURE TO ARTIFICIAL INTELLIGENCE: A NOVEL DATASET AND ITS POTENTIAL USES," *STRATEGIC MANAGEMENT JOURNAL*, (42:12) (2021).

The Capabilities Of AI Keep Improving



NOTE: LOWER BOUND OF EXAM RESULTS SHOWN. ONLY RESULTS OF EXAMS EXPRESSED AS PERCENTILES SHOWN IN THE CHART. FOR THE FULL LIST OF RESULTS, PLEASE CONSULT THE FOLLOWING REPORT: GPT-4 TECHNICAL REPORT, ARXIV:2303.08774 , ARXIV.ORG, CORNELL UNIVERSITY (MARCH 2023).

Risks and Awareness:

1. Samsung workers made a major error by using ChatGPT
Samsung meeting notes and new source code are now in the wild after being leaked in ChatGPT

Data leaks need to stop: Sensitive information such as confidential business information, code, customer data, and personal information can be leaked.

2. ChatGPT: Exploited twice: The exploit came via a vulnerability in the Redis open-source library. This allowed users to see the chat history of other active users.

Open-source libraries are used “to develop dynamic interfaces by storing readily accessible and frequently used routines and resources, such as classes, configuration data, documentation, help data, message templates, pre-written code and subroutines, type specifications and values,” according to a definition from Heavy.AI. OpenAI uses Redis to cache user information for faster recall and access. Because thousands of contributors develop and access open-source code, it’s easy for vulnerabilities to open up and go unnoticed. Threat actors know that which is why attacks on open-source libraries have increased by 742% since 2019.

Risks and Awareness:

Be Careful…Be Aware…get ready!

1. **Privacy breaches:** Personal information can be disclosed if language models like ChatGPT are not properly configured to protect privacy. This can result in violations of privacy laws and regulations and can damage the reputation of a company. EU Laws are getting Serious!

2. Bias and fairness: Language models like ChatGPT can be trained on biased data, which can result in biased outcomes. This can impact decision-making and lead to discrimination and other unfair outcomes. **New AI Risk: Hallucinations!**

3. **Misinformation:** Language models like ChatGPT can produce incorrect or misleading information, which can have negative consequences, such as spreading false information, making incorrect decisions, and damaging a company's reputation.

4. **Some Models are using dated information**

Risks and Awareness:

How are Hackers using AI?

1. Phishing: Combining Hacked information and Social Network info

2. Code Creation: Easy upgrades to Python

3. Online Profile Creation: (Vid Con IRL!!!)

4. Photos: Creation and Animation

5. Videos and Voice Overs are trivial to create

More Risks and Awareness:

1. Helps write crafted attacks to steal information and deliver ransomware
2. Conduct financial fraud, financial extortion, steal cryptocurrency (crypto wallets)
3. This means Lowering the bar for lower-level cybercriminals, and upping the game for advanced criminals
4. With training it can mimic the writing style/Video of an executive and craft super targeted phishing attacks
5. ChatGPT created Code can do it all: It can find target files, create Zip file and encryption processes easily. It can create new code that has not been seen before. Right now, they are sorta basic, but advances and sophistication are coming!

Benefits and Awareness:

1. **Improved policies.** We can ask ChatGPT to help us improve our security policies. And it's amazing. It's just staggering. And it's very nice. For example, I could ask, "Please give me an updated policy for data governance" and boom, less than five seconds later, you have a complete, new, updated data policy.

2. **Communications.** I can ask ChatGPT 'Please help me to write a communication to our users, explaining X, Y and Z'. I can even ask ChatGPT to explain it in a way that a 12 year-old boy would understand. And ChatGPT will do it. Or if I want to try to explain the latest phishing campaign to my mother, ChatGPT will put the right language together. You get the idea.

3. **Legal Reviews:** have ChatGPT analyze a contract and compare to best practices

4. **Insurance Policy Analysis:** some awesome finding reported

5. **PYTHON Code** creation and improvement

5. Bonus: Love Poems!

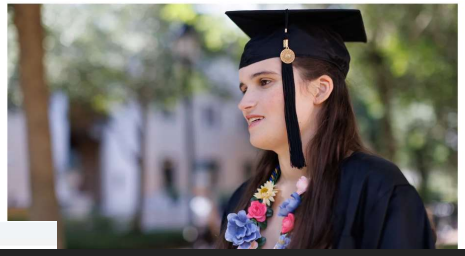
DEEPFAKES, VOICEFAKES, NEWSFAKES, SOCIAL ENGINEERING BOTS

DEEPFAKES, VOICEFAKES, NEWSFAKES, AND BOTS

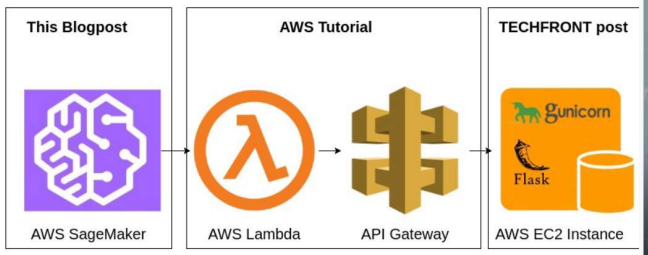
A nonspeaking valedictorian with autism gives her college's commencement speech

May 12, 2022 · 2:44 PM ET

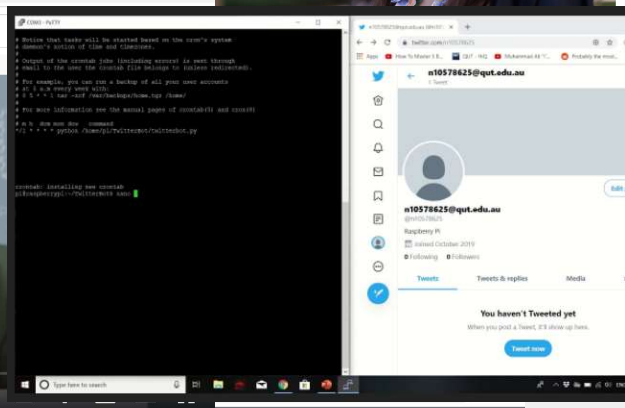
BILL CHAPPELL

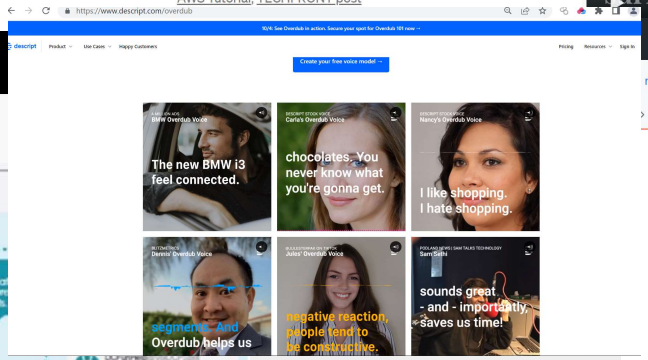


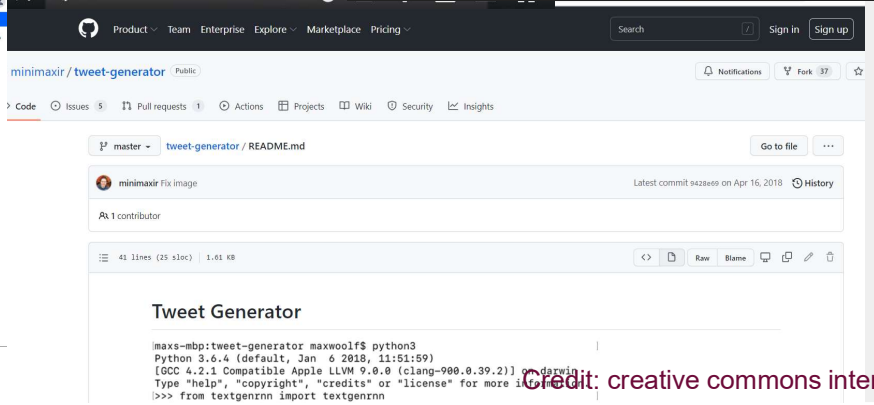
In this blogpost, we will cover the first task in detail. Two others are covered in AWS Tutorial, TECHFRONT post. The final architecture will look like this:



AWS Tutorial, TECHFRONT post







Credit: creative commons internet

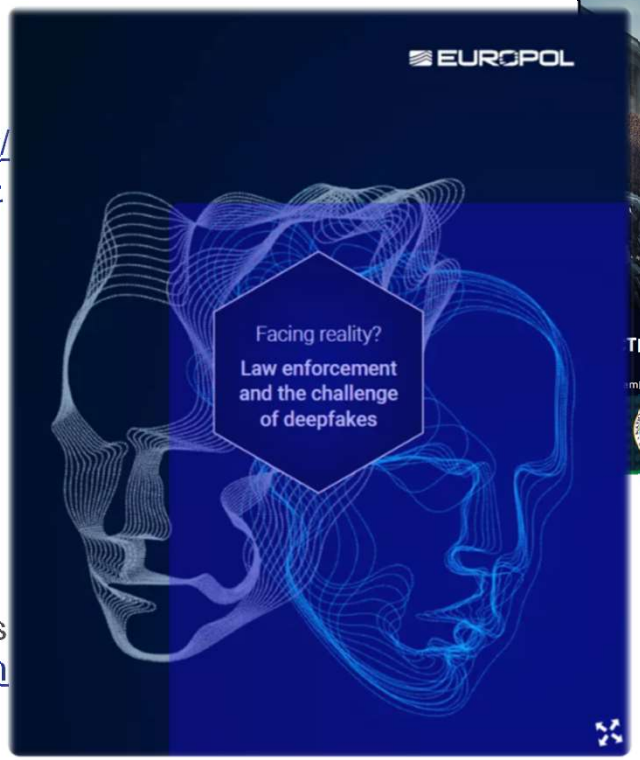
GAI DEEPFAKES WARNINGS

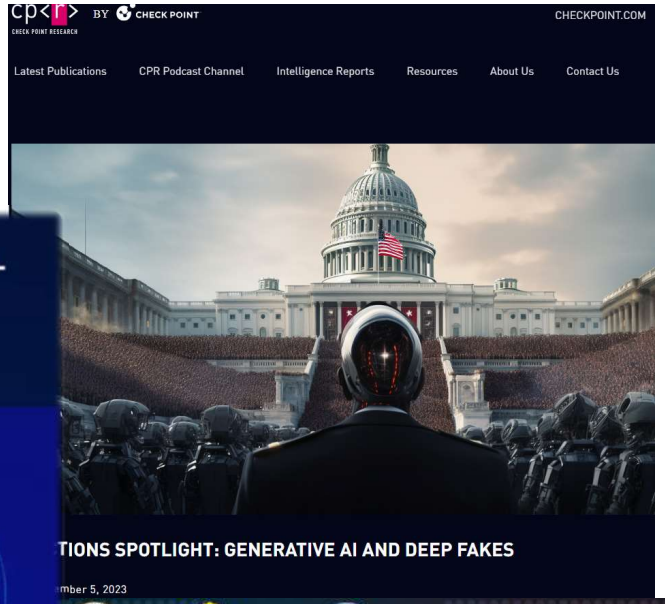
CEO impersonation for financial fraud
https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=1a968bc27559

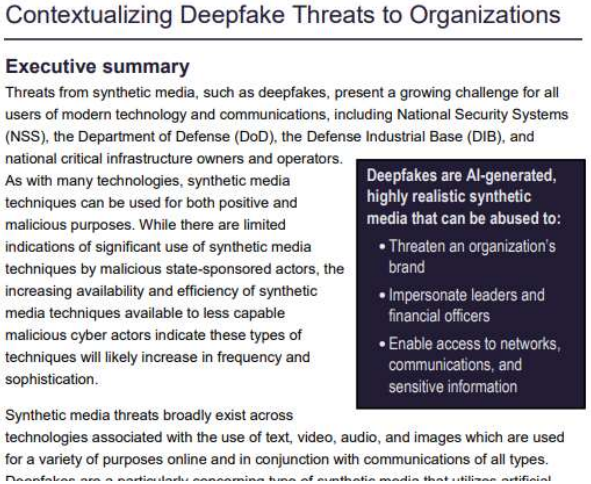
Europol warning use in organized crime
https://www.europol.europa.eu/media-press/newsroom/news/europol-report-finds-deepfake-technology-could-become-staple-tool-for-organised-crime

Check Point Research on GAI and Deepfakes
https://research.checkpoint.com/2023/elections-spotlight-generative-ai-and-deep-fakes/

CISA
https://media.defense.gov/2023/Sep/12/2003298925/-1/-1/0/CSI-DEEPFAKE-THREATS.PDF






Contextualizing Deepfake Threats to Organizations

Executive summary

Threats from synthetic media, such as deepfakes, present a growing challenge for all users of modern technology and communications, including National Security Systems (NSS), the Department of Defense (DoD), the Defense Industrial Base (DIB), and national critical infrastructure owners and operators. As with many technologies, synthetic media techniques can be used for both positive and malicious purposes. While there are limited indications of significant use of synthetic media techniques by malicious state-sponsored actors, the increasing availability and efficiency of synthetic media techniques available to less capable malicious cyber actors indicate these types of techniques will likely increase in frequency and sophistication.

Deepfakes are AI-generated, highly realistic synthetic media that can be abused to:

- Threaten an organization's brand
- Impersonate leaders and financial officers
- Enable access to networks, communications, and sensitive information

Synthetic media threats broadly exist across technologies associated with the use of text, video, audio, and images which are used for a variety of purposes online and in conjunction with communications of all types.

Deep Fake Creation Getting Easier and Evolving:

What are the common techniques used to create deepfakes and how are they evolving?

With just a simple search, you can find lists of reviewed and rated apps:

https://contentmavericks.com/best-deepfake-software/
https://www.rankred.com/best-deepfake-apps-tools/
https://topten.ai/deepfake-app-and-software-review/
https://zapier.com/blog/best-ai-image-generator/

Some of the review sites are undoubtably getting referral money for ones they rank higher, so be aware of that bias.

Most of the tools are trying to be legitimate and use customer provided pictures and video's of only themselves. Other tools let you use other folks' pictures and videos with an approval process that is easy to get around. Companies based outside of US has much lower requirements (FaceApp by Wireless Lab in Russia for example).

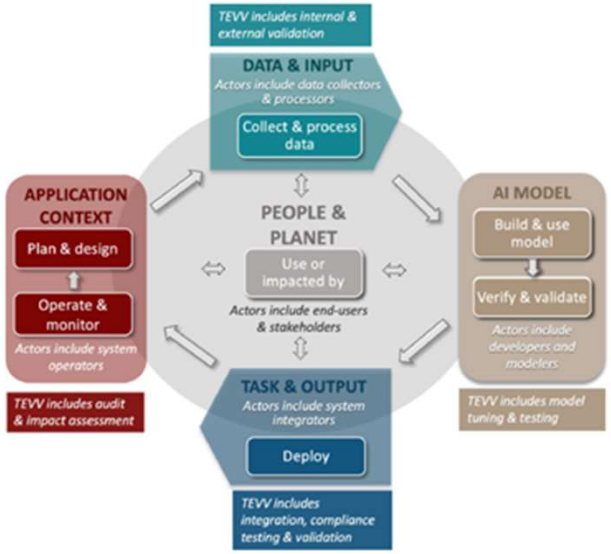
There are apps for Android, Apple and laptops (linux, Apple, MS) that have different features. Some tools require you to upload voice examples, others you can select a stock voice.

In the past 6 months there has been incredible developments in this area. Some tools are super easy to use and have limited outputs, other tools you need to learn a bit more and have very advanced output.

Good Guidance is Available…Review It:

CISO's need to review and embrace the significant amount of good guidance that has recently been released. NIST just released the "AI Risk Management Framework" The AI Risk Management Framework (AI RMF) is intended for voluntary use and to improve the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems.
It has all the appropriate steps that CISO's can use: Framing the Risk, your Audience, AI Risks and Trustworthiness, Effectiveness of the Benefits, the Risk Management Core that describes "Govern, Map, Measure, and Manage" and describes the Risk Management Profiles

Found Here: https://www.nist.gov/itl/ai-risk-management-framework



Counter Measures!:

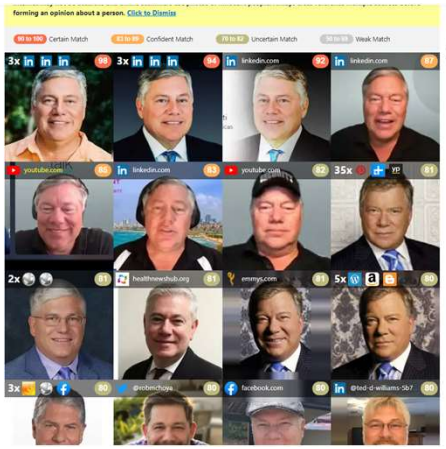
1. **Examine the Pictures used in the profile is using and submit to** www.facecheck.id (Mine pops up William Shatner!) There are many cases where the person is already married, or has an arrest record, or the picture is not from the person who created the profile. 417 million pictures are on line, from Mugshots to good pictures! (I snapped my results and added to research below!)

2. **Most AI Based Text creation tools have No Awareness of Current Events**, as their data used is typically several years old, ask it questions related to new news events to spot an AI based chat

3. **Currently you Can't see back of head in pictures or Video's:** Ask the "person" or thing talking to you to turn around and if they can't… you are done!

4. Have good tools in place to prevent SMS and Phishing scam emails and texts, most companies have, but end-users do not. Free Enduser tool: https://www.zonealarm.com

1. Never click on the links provided by phishing or profile creators…



Deep Fake and Facecheck.ai Testing:

1. A good Article on Deep Fake Analysis:
   https://www.npr.org/2023/04/27/1172387911/how-can-people-spot-fake-images-created-by-artificial-intelligence

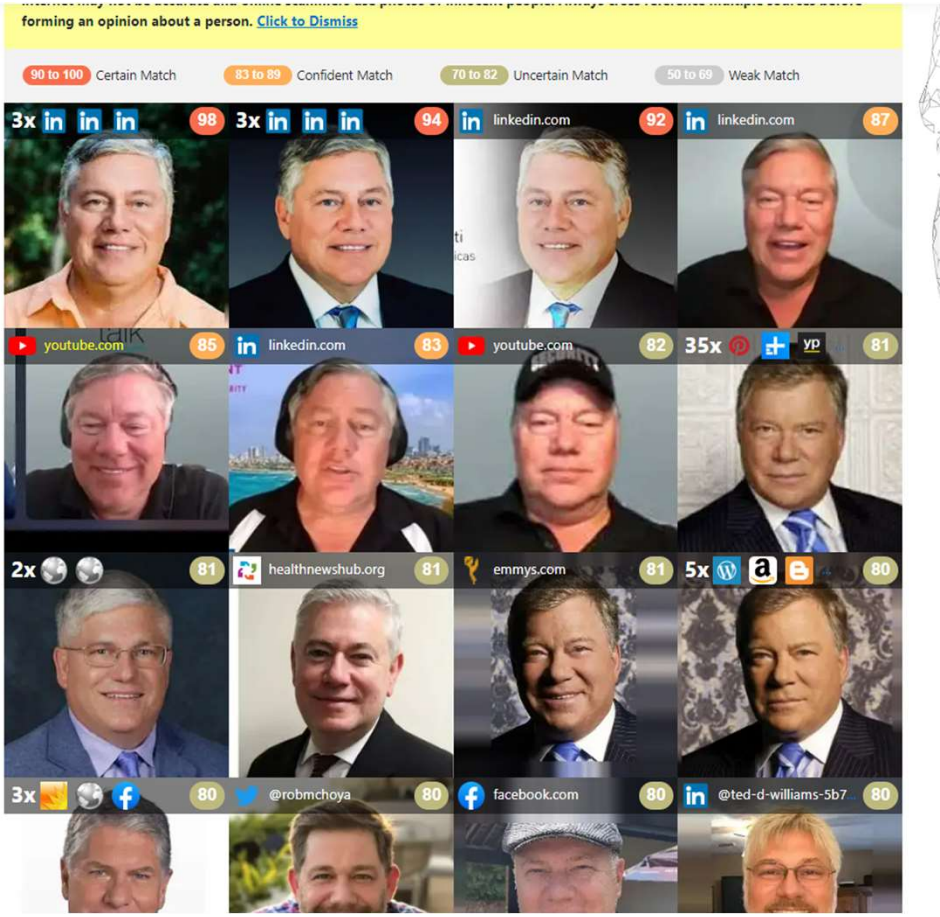
2. An Experts Thoughts:
https://eddyballe.com/deepfake-detection-tools/

- DeepWare AI: Best DeepFake Detection Software
- DuckDuckGoose: Top Deepfake detection programs for businesses
- Sensity AI: Best Deepfake detection services for anyone to use

https://beebom.com/wp-content/uploads/2020/11/AI-fake-face.jpg

How to recognize fake AI-generated images | by Kyle McDonald | Medium

https://kcimc.medium.com/how-to-recognize-fake-ai-generated-images-4d1f6f9

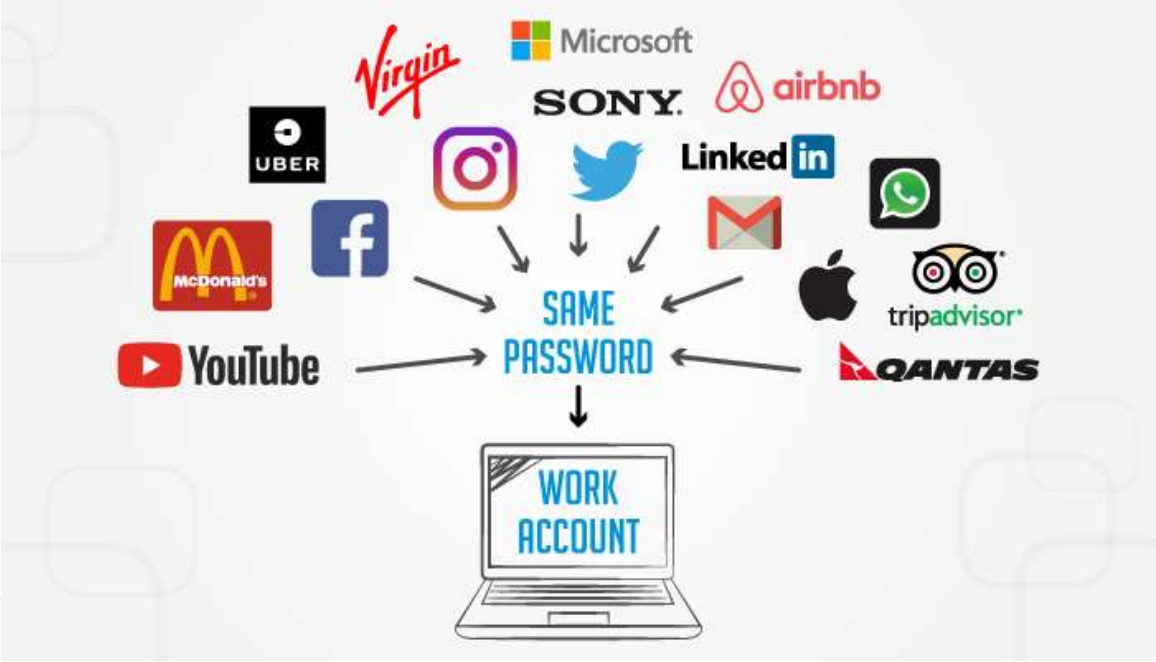


More Counter Measures!:

1. **Don't re-use passwords.** If you use the same password to log into one of their scams, they will take the email address AND the password you just used and try to log into THOUSANDS of other www sites to see where it will work! Always use a unique password for every site. Check out: www.haveibeenpwned.com to see what website you use have been compromised!

2. **Conversations are typically brief**, long AI based conversations currently devolve a bit.

3. **Online Profiles, may use fake information,** or not a real person behind it: If there is real interest in a person, do a video based FTF call, no filters or back grounds! If who you are dealing with can't do that… RUN!!!



How can organizations protect themselves against the potential risks of deepfakes?

1. For money transfers or account changes, use multiple people, during a follow up call/email to validate the transaction.

2. When you get money request/gift card request/weird call/sms/email… Drop the call and call person Directly!

3. Configure your email system to Banner/Label emails/zoom invites coming from external addresses.

4. Use the most advanced Email Phishing prevention tools

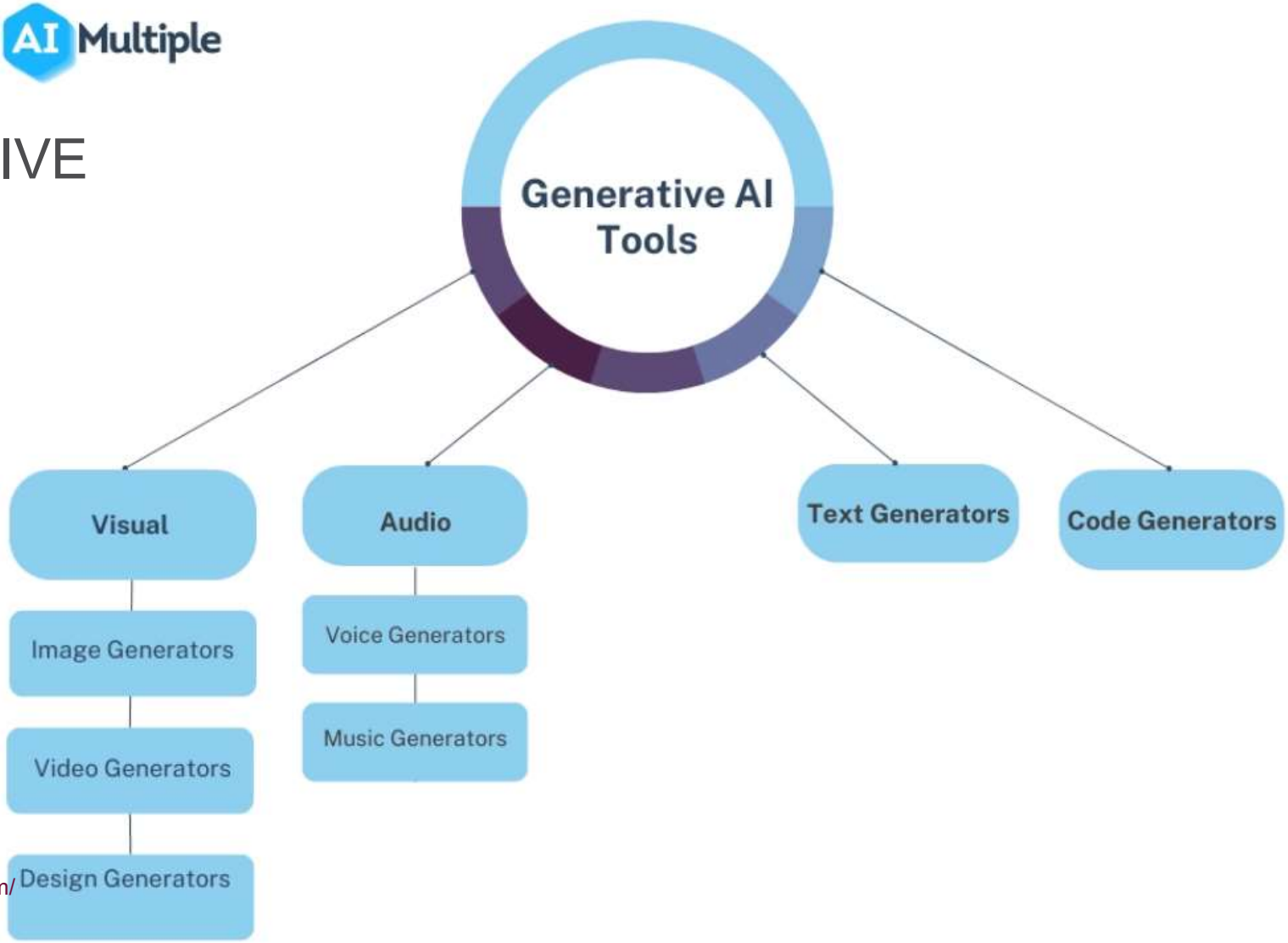
5. Leverage advanced End point tools that prevent malicious code execution and deployment.

6. Use Out of Band Verbal passwords to validate anything important.

7. Use your Spider senses!!!!! Talk with your team and employees. Have a go-to expert.

GENERATIVE AI FOR SECURITY

GENERATIVE AI TOOLS



https://research.aimultiple.com/generative-ai-tools/

CHATGPT (OPENAI) RISK, REWARD, TRADEOFF

CHATGPT (OPENAI) RISK, REWARD, TRADEOFF

TIME SAVINGS: ChatGPT can generate responses quickly and efficiently, which can save time for both the user and the company using the technology.

CUSTOMIZATION: ChatGPT can be customized to fit the needs of the user, allowing for a personalized experience that can improve customer satisfaction and engagement.

SCALE: ChatGPT can handle a large volume of interactions at once, making it an effective solution for companies that need to handle high volumes of customer inquiries.

BIAS: ChatGPT is trained on a large amount of text data, which can contain biases, stereotypes, and offensive language. ChatGPT may perpetuate them in its responses and has potential to manipulate the user.

SAFETY: ChatGPT is not good for decision making. There is risk its responses will be inappropriate for crisis management or healthcare decisions.

ZERO EMPATHY: ChatGPT is an AI language model and lacks the ability to empathize with users. This may result in responses that are impersonal or unsympathetic, which could negatively impact user experience.

ETHICS BYPASS: ChatGPT API with third party software (Telegram) uses OpenAI's GPT-3 model and can circumvent ChatGPT ethics.

FRAGILE: ChatGPT requires extensive training to function effectively, which can be time-consuming and expensive for companies.

CONTEXT PROBLEMS AND BAD FOR DECISION MAKING: ChatGPT can generate responses based only on the information it has been given, it cannot understand the full context of a situation. This can lead to inaccurate or inappropriate responses.

Micki created with
DALL-E and ChatGPT

The Business is Using AI Based Tools, You should know!

1. Meeting BOT's powered by AI:
   https://otter.ai/
   https://www.makeuseof.com/best-ai-meeting-a

WARNING: DO NOT HAVE A MEETING WITH JUST AI MEETING BOTS!

2. Neat developments:
   AI powered Smart Glasses:
https://www.popularmechanics.com/technology/gadgets/a43633762/chatgpt-smart-glasses/

3. https://www.forbes.com/sites/bernardmarr/2023/05/10/15-amazing-re
of-ai-everyone-should-know-about/?sh=2908fb6885e8

How to spot fakes in Content

https://www.forbes.com/sites/bernardmarr/2023/05/25/how-can-you-detect-if-content-was-created-by-chatgpt-and-other-ais/?sh=2a37433f710b

https://www.techopedia.com/detect-deepfakes-tips

AI deepfakes are now as simple as typing whatever you want your subject to say!

TOP GENERATIVE AI TOOLS

Credit: Moti Sagey and Reddit

BATTLE OF THE AI (SHORT LIST)

DEFENDER

Check Point has 72 different AI threat engines in prevention first architecture with ThreatCloud (IOC/TTP data lake)

Effective and efficient for Malware DNA genotyping and analysis

Helps SOC analysts see attack vectors and landscape

Help write good software code

Fix bugs in source code

Auto-write cybersecurity policies and controls based on GRC framework(s)

Gamify cybersecurity training

created with DALL-E

ADVERSARY

Check Point Research saw instances of 5 major attacks created by ChatGPT since its inception

Create Deepfakes and bots

Malware writing for dummies (joke)

Phishing email creation for dummies (again a joke)

Easy to identify attack landscape based on vulnerabilities and find exploits to match (multiphased attacks)

Circumvent AI ethics of GPT-3 by using API with Telegram or other software integration

THREATCLOUD AI: THE BRAIN OF CHECK POINT CYBERSECURITY

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

ACCURATE PREVENTION
(MALICIOUS/SAFE)

Telemetry

Telemetry

ThreatCloud APIs

Quantum
Secure the Network

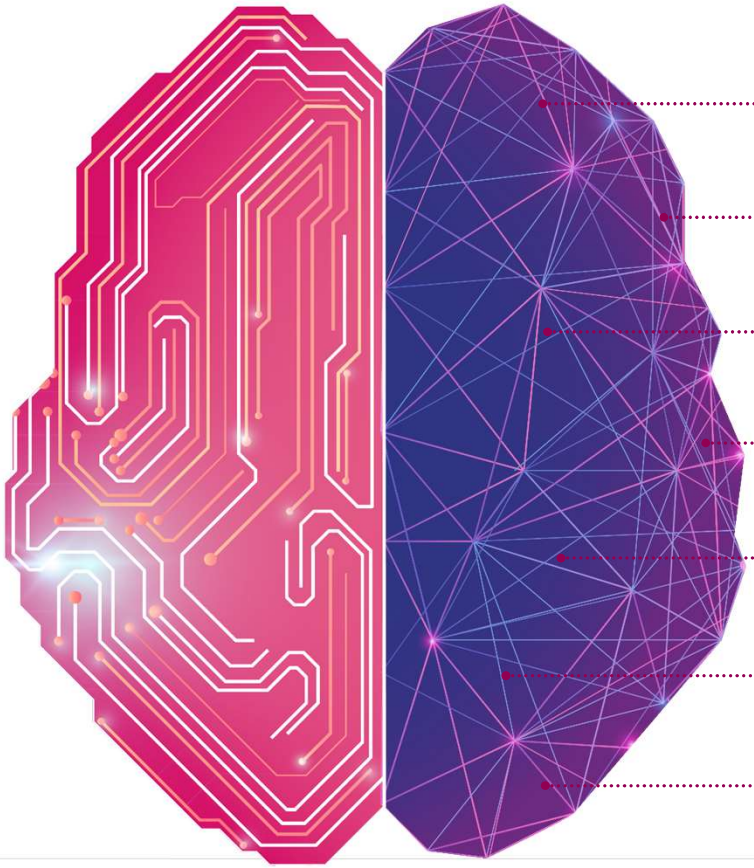
CloudGuard
Secure the Cloud

Harmony
Secure Users & Access

Horizon
Unified Management & Security Operations

*Source – Miercom January 2023

POWER OF AI THREAT INTELLIGENCE



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

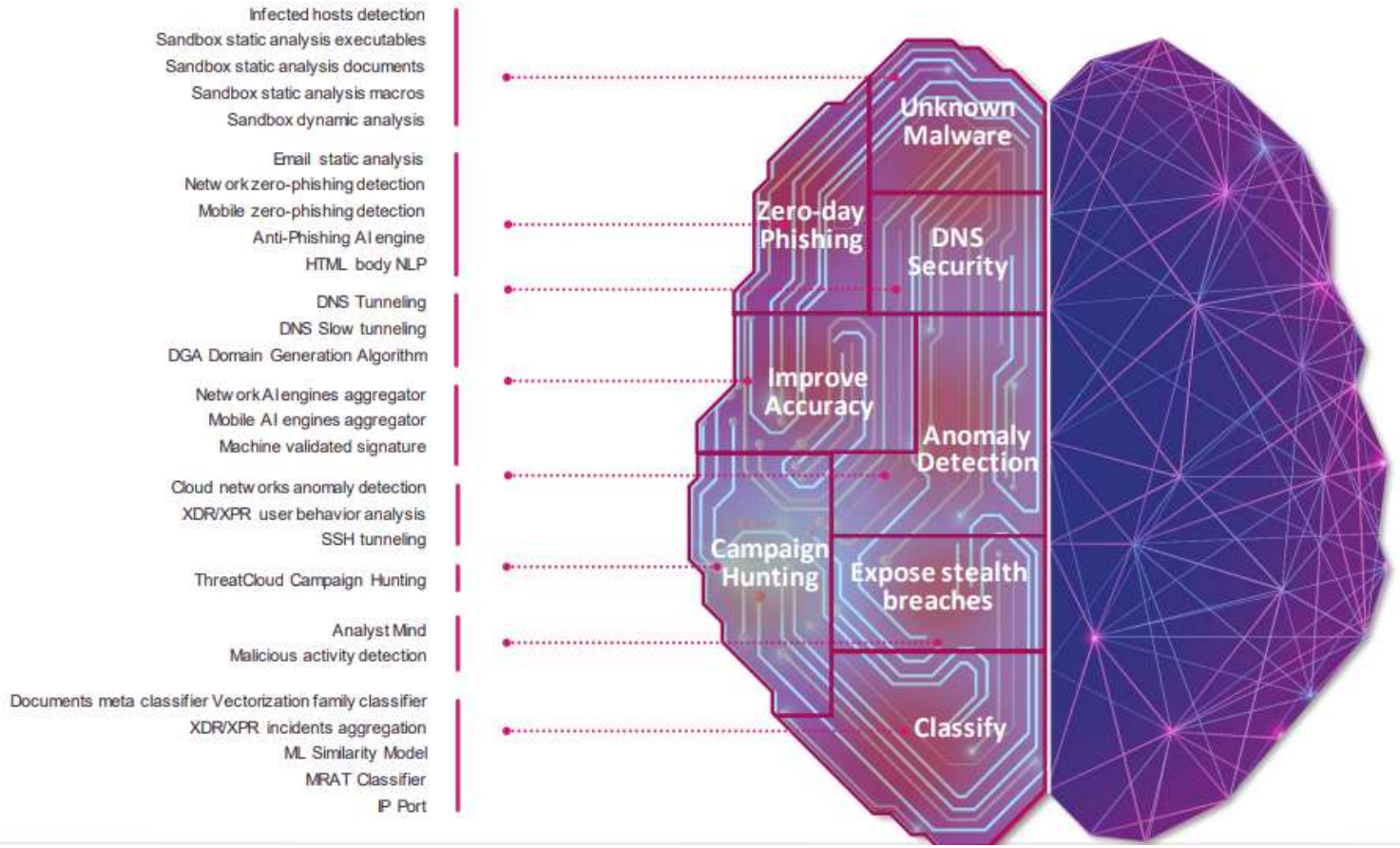
1,500,000
Newly installed mobile apps

1,000,000
Online web forms

Counted **DAILY** !

AI ENGINES

40+ engines across different security functionality



CHECK POINT AI DRIVEN THREAT PREVENTION

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:

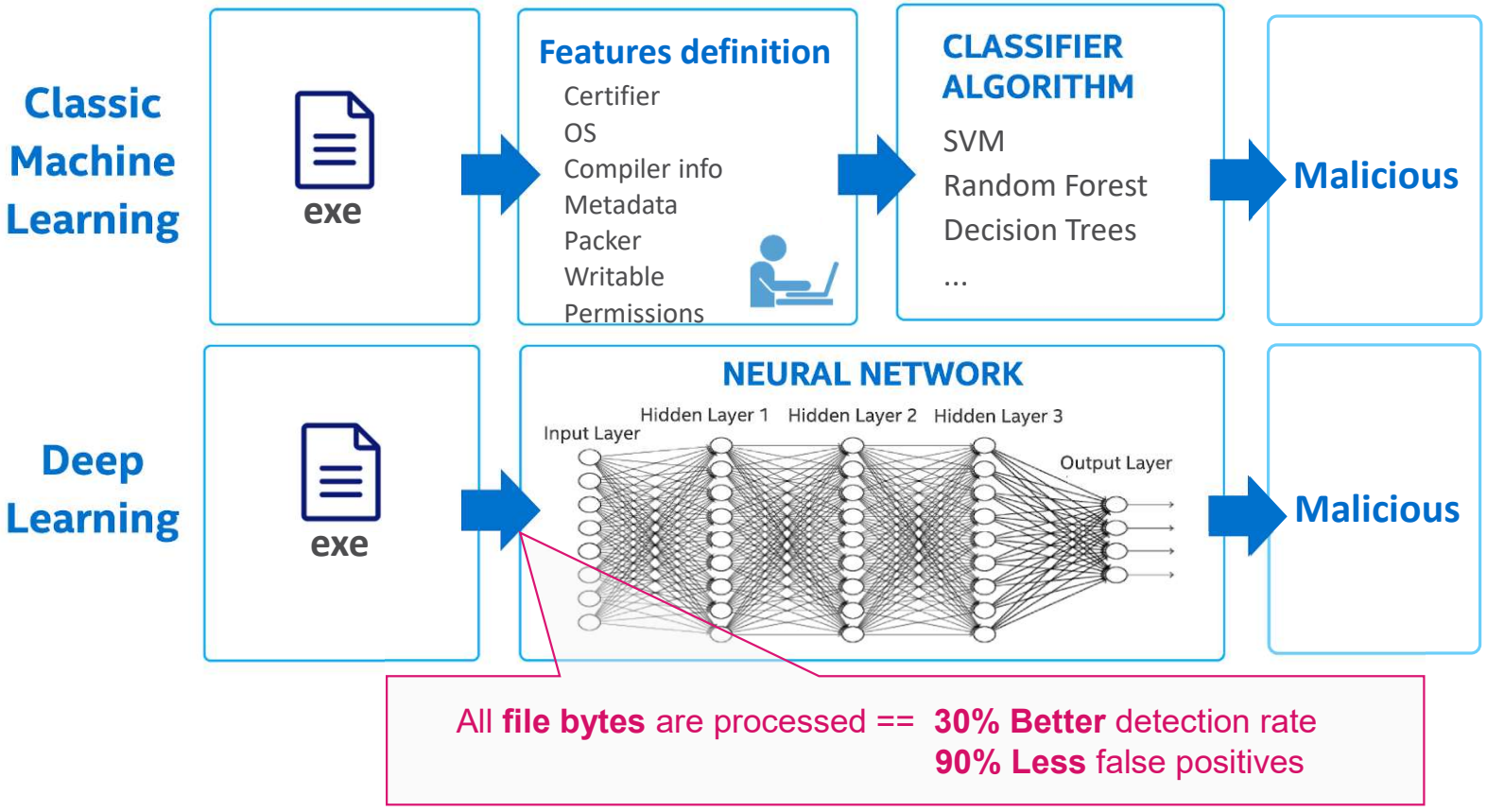
- **Cloud posture** management
- **Zero-trust** and **micro-segmentation**
- **AI-based prevention** on endpoints & servers
- **Analysis of AD** / ADFS / Access token (SAML, OAuth 2.0) & user behaviors
- **Native XDR**

Data leak:

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

BETTER PREVENTION WITH CUTTING-EDGE TECHNOLOGIES

Classic Machine Learning vs. Deep Learning



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

AI-based technologies leveraged by ThreatCloud

30+ examples across different security functionality

Infected hosts detection
Sandbox static analysis
Sandbox dynamic analysis

Email static analysis
Mobile zero-phishing detection
Anti-Phishing AI engine

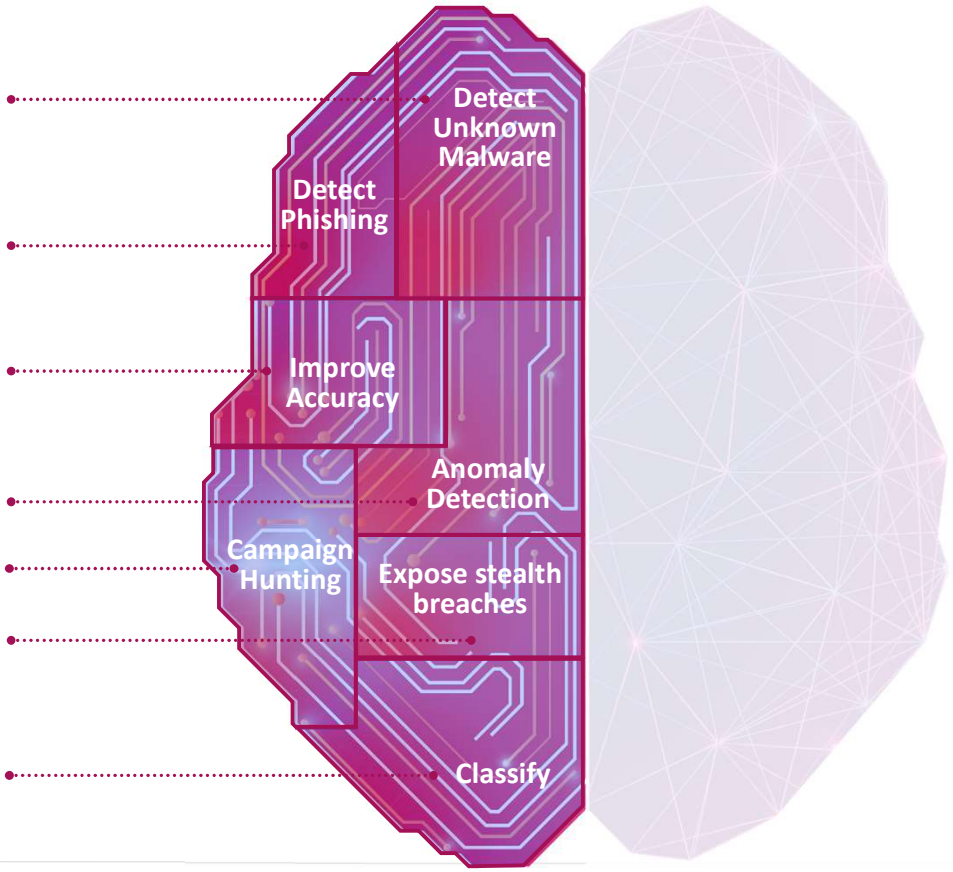
Network AI engines aggregator
Mobile AI engines aggregator
Machine validated signature

Cloud networks anomaly detection

ThreatCloud Campaign Hunting

Analyst Mind
Malicious activity detection

Documents meta classifier Vectorization family classifier
ML Similarity Model
MRAT Classifier

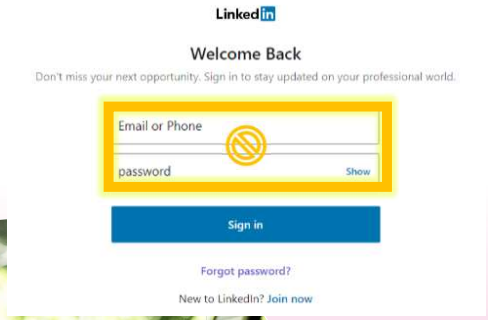


ZERO-DAY PHISHING BLOCKED – IN REAL TIME

Quantum Gateway prevents credential theft in-line, for all browser types

PATENTED

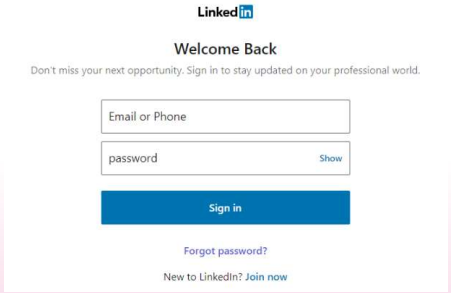
PREVENT CREDENTIALS THEFT
NO CLIENT SOFTWARE NEEDED



4x

 # Blocked new phishing pages

NEWLY SEEN PHISHING SITE



Firewall Provides in-line Protection

Introducing: advanced DNS Security Software Blade

Blocks 5X more Zero-DNS attacks than signature based technologies

Best Security with most innovative AI and Deep Learning Technologies

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

ThreatCloud catches what everyone else missed

3 Examples of malware variants detected by ThreatCloud before VirusTotal

TRICKBOT

12 days before VirusTotal

ZLOADER

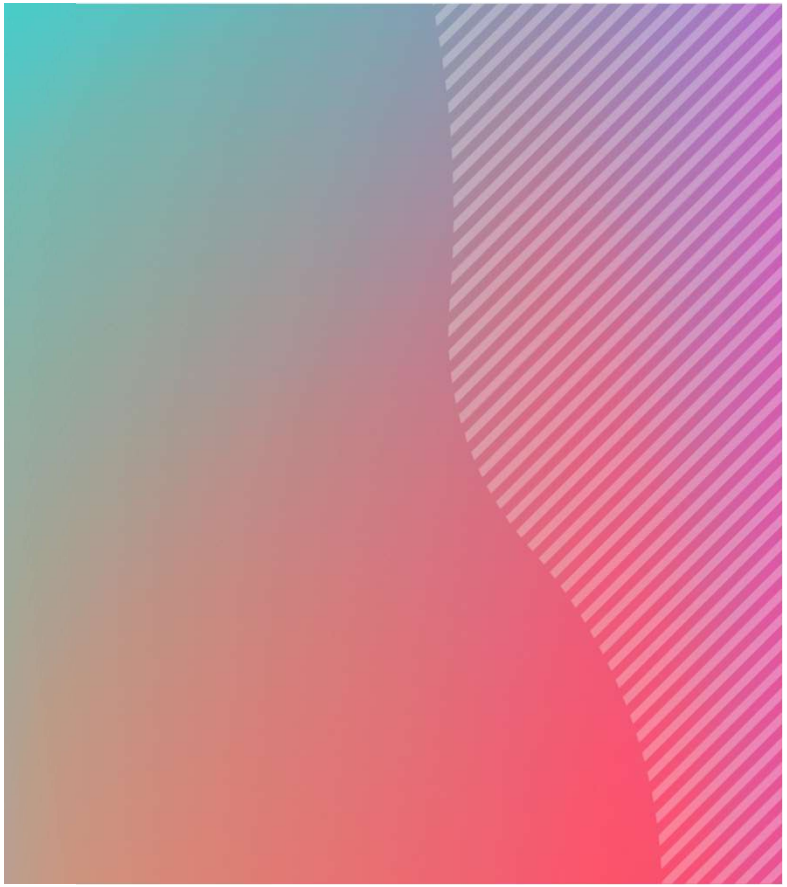
15 days before VirusTotal

HANCITOR

17 days before VirusTotal

THREATCLOUD

THE ONLY PRE-EMPTIVE SECURITY AGAINST LOG4J



CloudGuard AppSec

APPLICATION SELF-PROTECTION

Vendor and Product	Pre-emptive protection before vulnerability published
Check Point CloudGuard AppSec	✓
AWS WAF	✗
Azure WAF	✗
Cloudflare WAF	✗
Imperva WAF	✗
F5 NGINX App Protect	✗
F5 BIG-IP ASM/Advanced WAF	✗
Akamai WAF	✗
Fortinet Fortiweb	✗
ModSecurity	✗

CLOUDGUARD

Quantum Security Gateway Architecture

Quantum

Attack Indicator

Querying & Sharing

THREATCLOUD

Evasion Resistant Sandbox | Zero-day AI Security Engines | Threat Intelligence Bank

CLOUD | NETWORK | MOBILE | ENDPOINT | IOT

THREAT PREVENTION PARALLEL PROCESSING MODULES

Intelligence Based Prevention | Behavioral Enforcement | Inline File Sanitization

DYNAMIC WORKLOADS

NETWORK PARALLEL PROCESSING

Active Traffic Streaming

Stateful Inspection & Multi-Layer Policy

Accelerated packet path

VIRTUAL MGMT PLANE

Real-Time Log & Event Correlation

HyperSync™

Lights Out Management

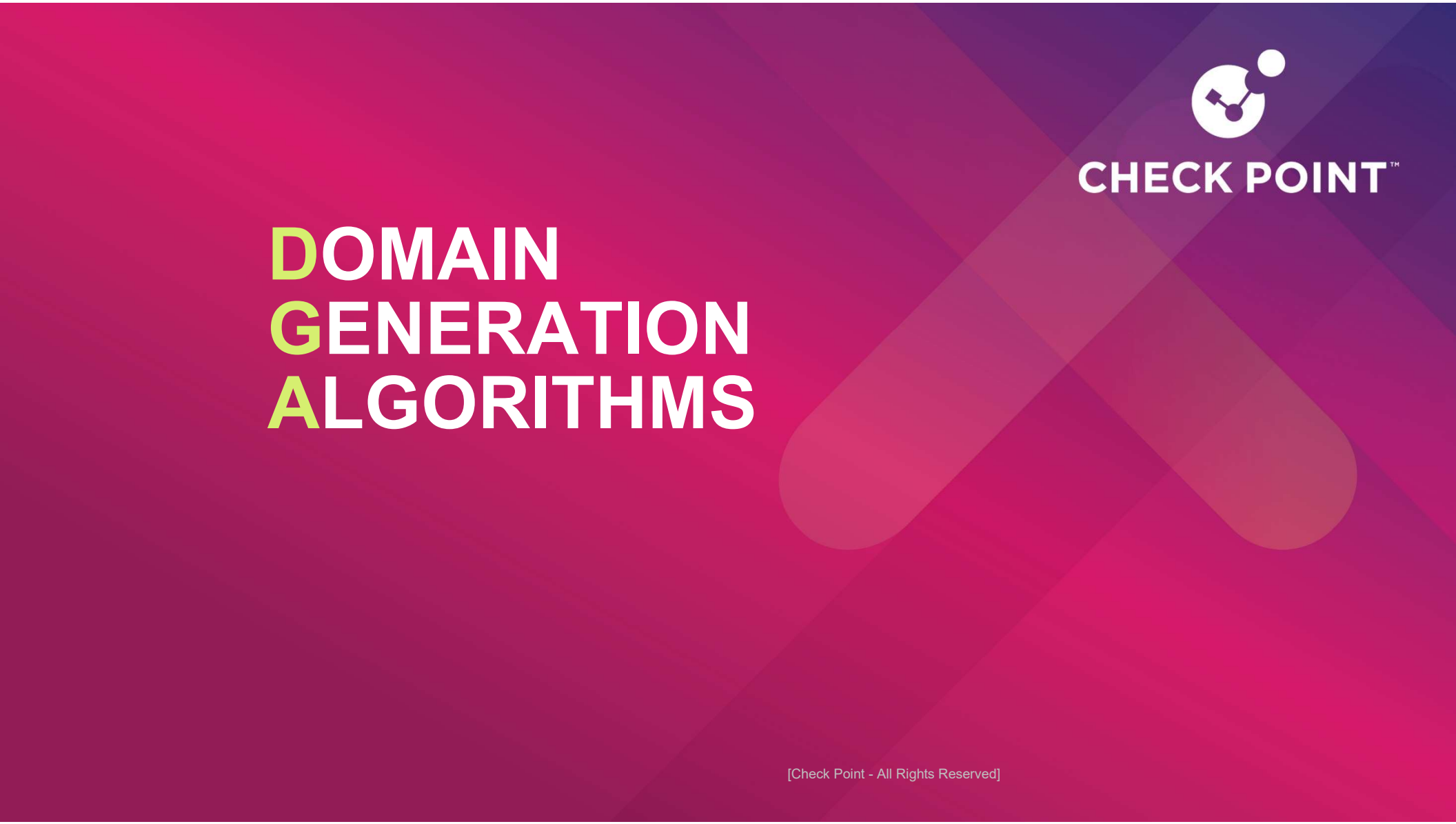
MODULAR HARDWARE TO CUSTOMIZE GATEWAY TO SECURITY NEEDS

Gen II | Gen III | Gen IV | Gen V

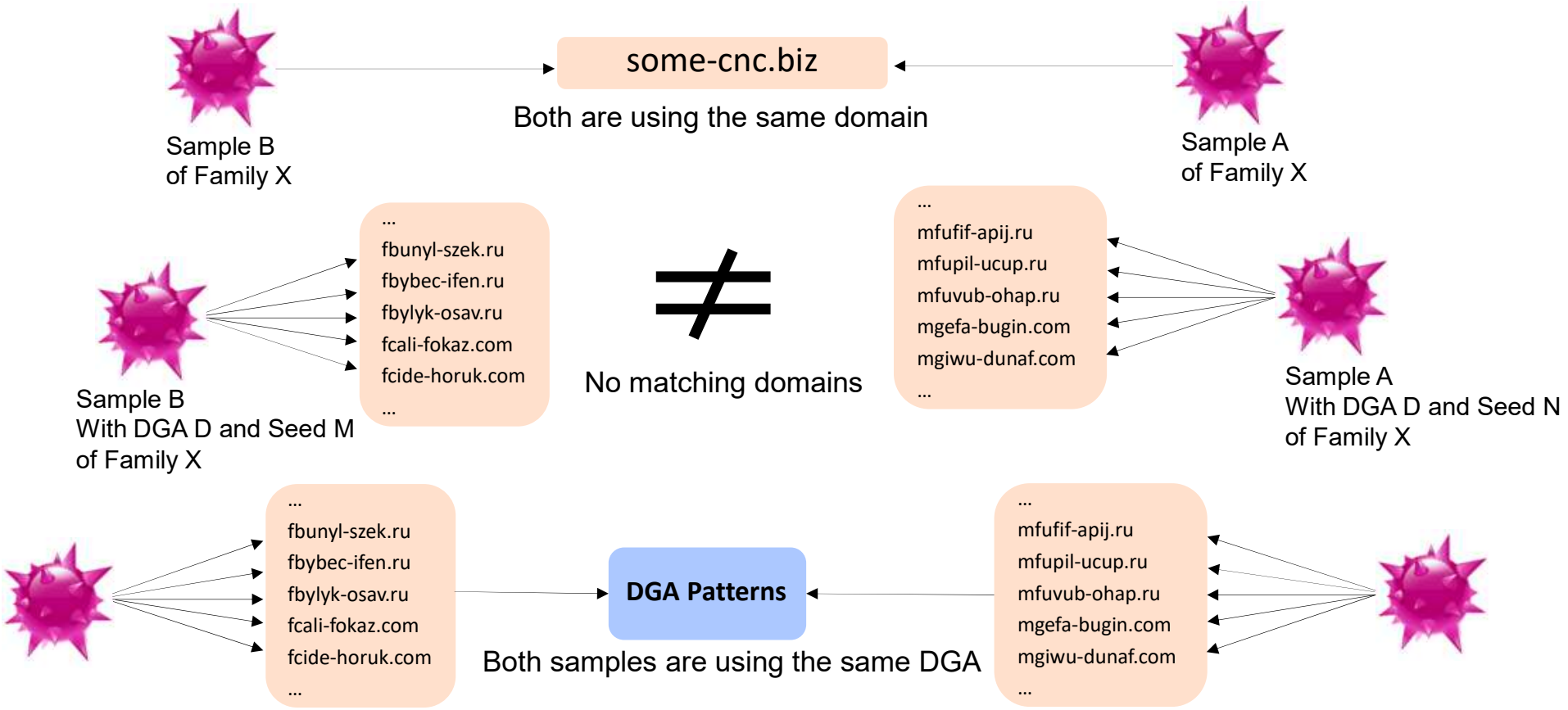
How We Deliver Best Security with Deep-Learning

New approaches for DNS Security and Zero-Day prevention

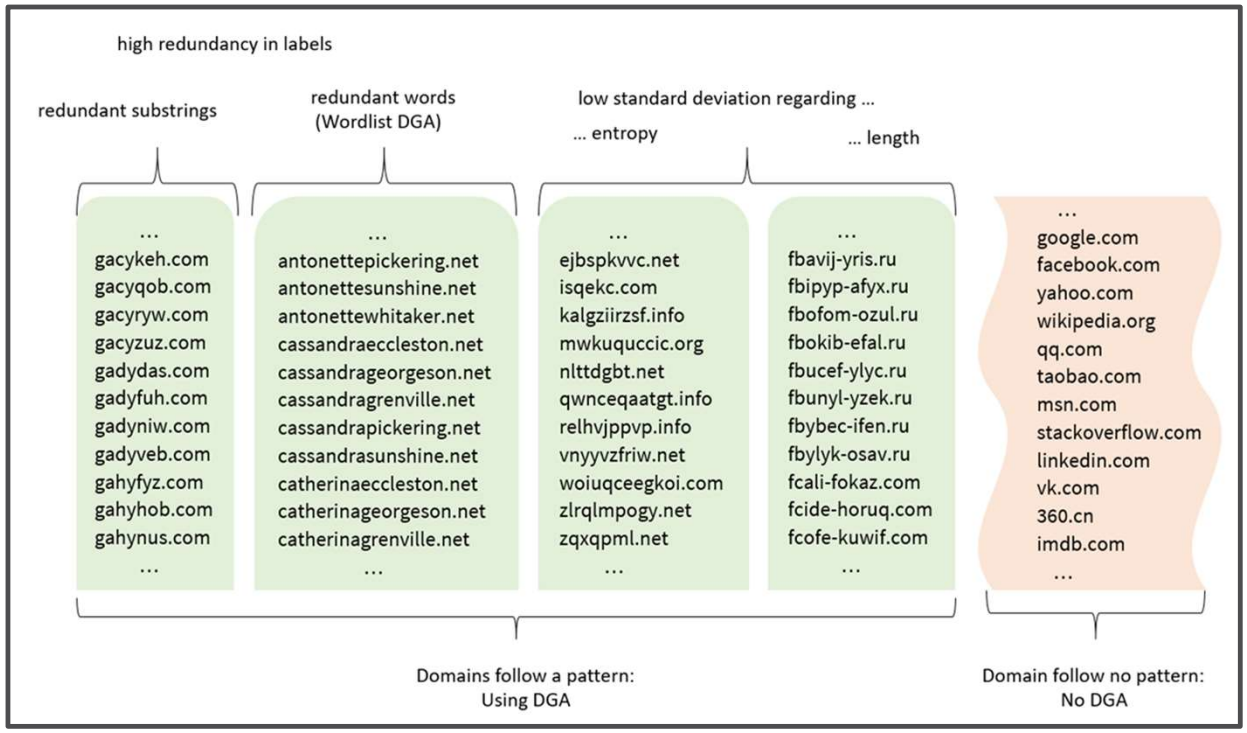
- Domain DGA
  - Prevention **on X6** the number of customers GWs
  - Prevention on a **wider variety** of malwares
- DNS Tunneling
  - Preventing **X32 sophisticated attacks**
  - The main engine that was able to detect
- Less labor and costs



DGA-Based Malware Operations (Channel Skipping)



Domain Generation Algorithms



20 Millions

80eloa543qyui62w.ga
fqxhvxnlivs.com
hcg6q70pqvahcuq.gq
zvfxpjpvlrj.cn
bcbnprjwry2.net
ju2ymymh4zlsk.com
lkry2vwbd.com
1qwabcdefghijk.us
8dfabcdefghij.us
8dfabcdefghijk.us
8dfabcdefghijkl.us
8dfabcdefghijklmn.us
8dfabcdefghijklm.us
7w6yatsvx0piayrq.tk

- Here some domain generation algorithms reverse-engineered from real malware.
- Zloader malware: https://github.com/baderj/domain_generation_algorithms/tree/master/zloader

DGA use in Malware

- Prior to DGA - hardcoded IP addresses or Domains – was easier to trace
- Millions new every day
- Never seen before
- Not listed as malicious
- Harder to block
- Harder to affiliate malware families
- Reputation Databases less effective - Stale data, DGAs change fast

- Consequence:
  - Overcome security solutions using high-velocity covert channels
  - Malware is able to exfiltrate data, pull instructions, download more malware

What are today's solutions?

- DGA reversing labs
  - Reversing the top malwares
  - Running in emulation to capture domains (changing seed time/date)
  - DGAs Feeds
- Anti-Bot Signatures
  - Less effective on encrypted traffic
  - Less effective on zero-days (unknown malware)
- 3rd party feeds
  - Not necessarily containing DGAs

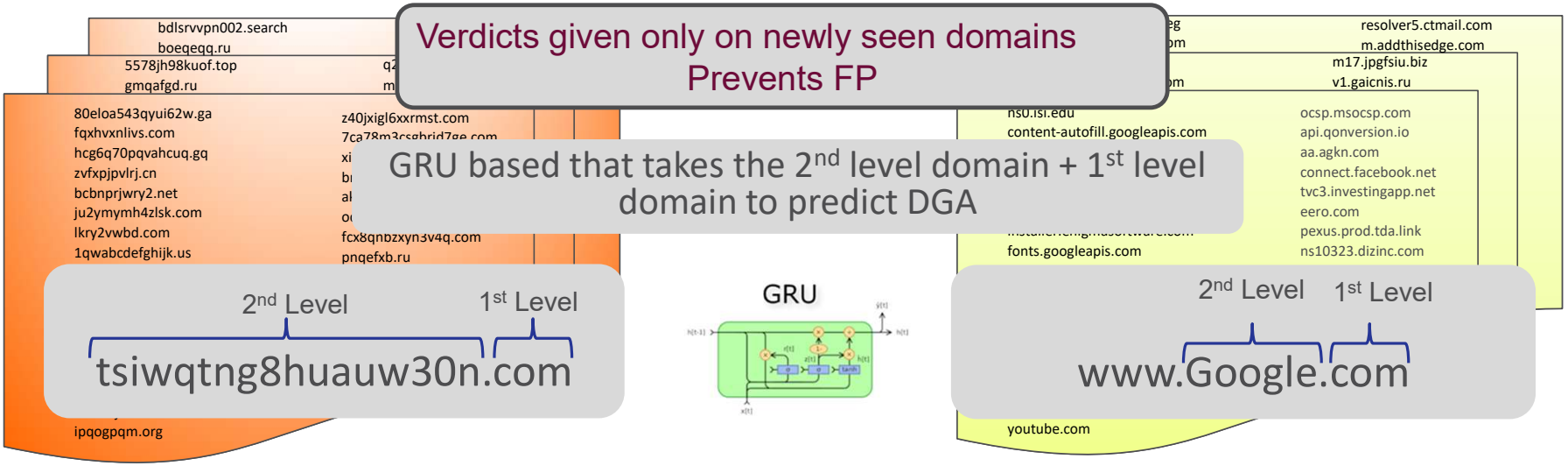
DeepDGA – Deep Learning - How it works

Malicious

Benign

Verdicts given only on newly seen domains
Prevents FP

GRU based that takes the 2nd level domain + 1st level domain to predict DGA



700,000 samples

DGA lab indicators

Known Algorithms synthesized data

Training: 5M samples

Prevents Zero days
No malware reversing
Wider coverage
Low cost

1,700,000 samples

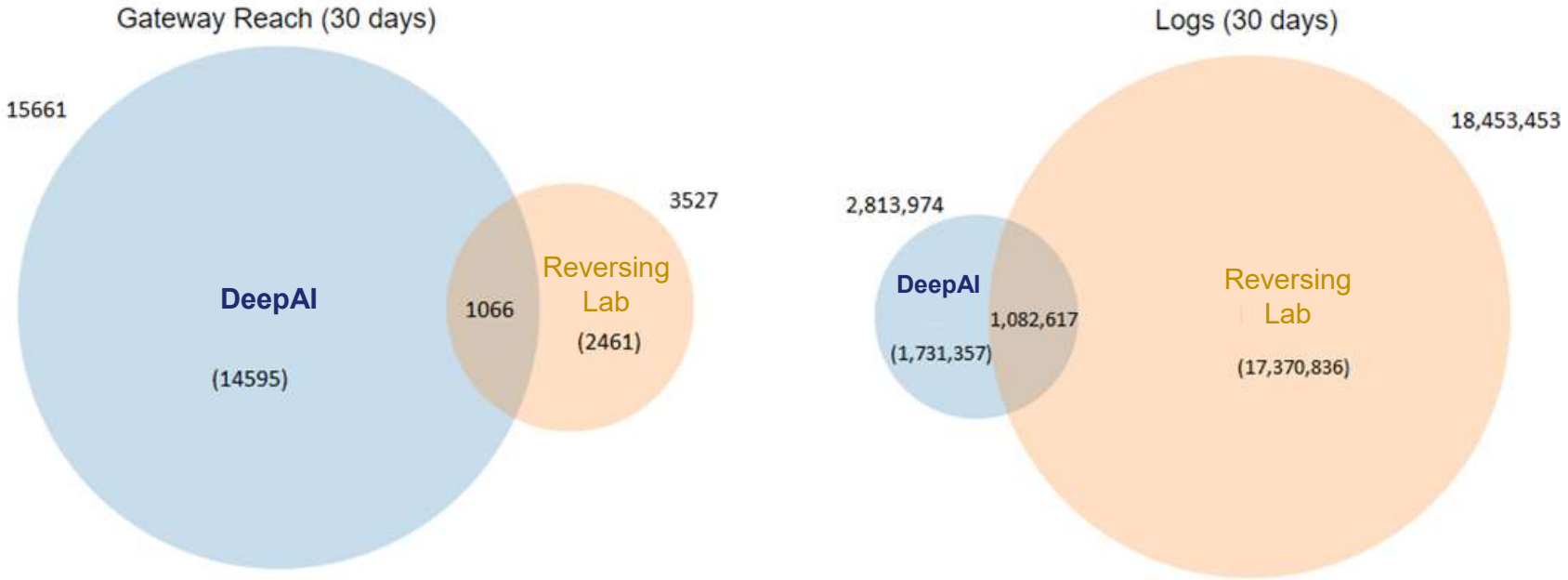
GW DNS requests (Akamai data)

Training: 50M samples

X6 more impacted customers GW's

Much wider spread covering a variety of malware types

Provider	Reversing Lab	DeepDGA
Impacted GWs	2,461	14,595
Logs	17,370,836	1,731,357
Unique IOCs upload	528K	135K



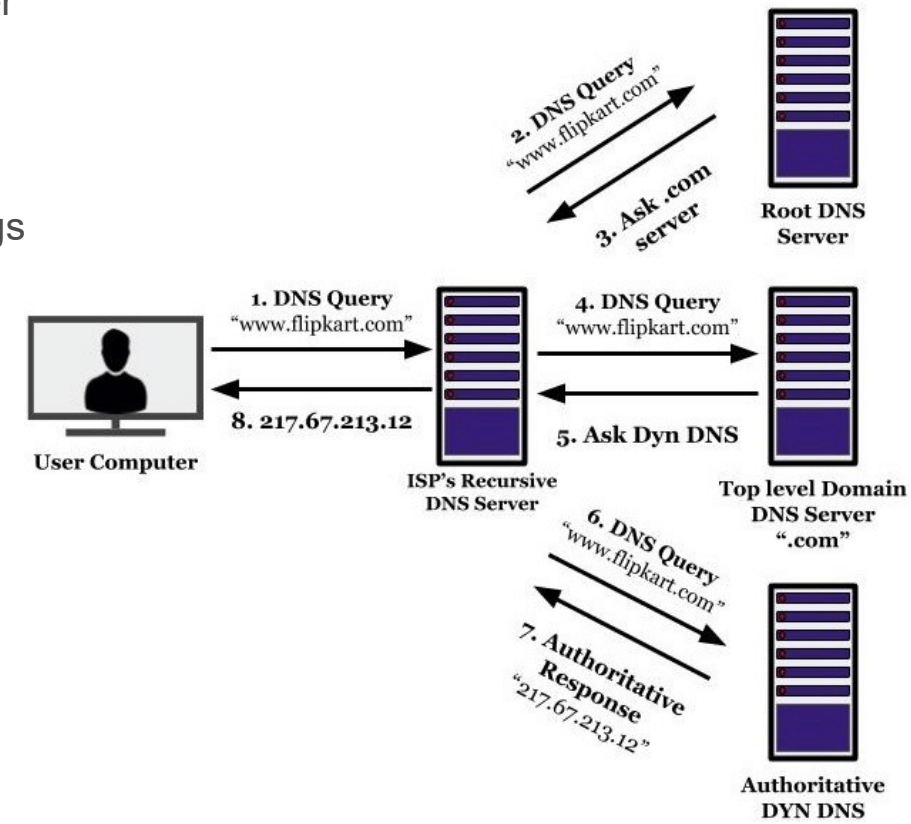
DNS TUNNELING

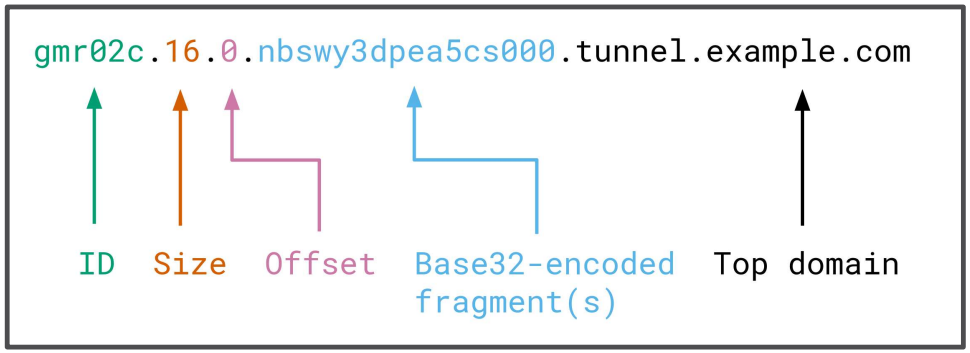
CHECK POINT™

DNS Tunneling

DNS has an amazing property: it'll make its way from server to server until it figures out where it's supposed to go

To get traffic off a secure network, it simply has to send messages to *a* DNS server, which will happily forward things through the DNS network until it gets to *your* DNS server





Examples: DNS Tunneling - Famous Attacks

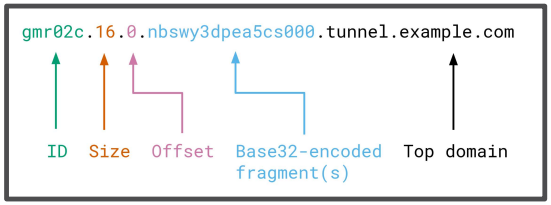
SolarWinds - SunBurst

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

Glupteba

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

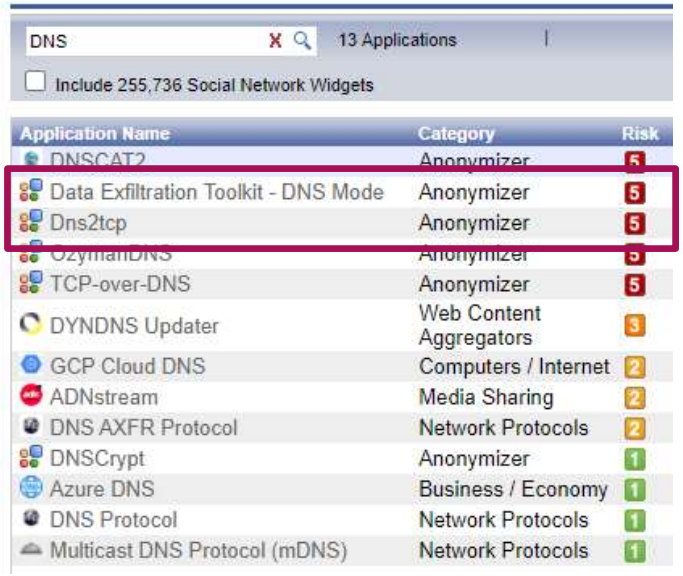
Example Attack – OilRig DNS Tunneling



Time	DST PORT	Dns Request name	Dns Response IPv6	Info
2019-03-07 15:31:34	53	n.n.c.BEE796C48ADE497DA0A1.ntpupdateserver.com		Standard query 0x37fc AA…
2019-03-07 15:31:34	65089	n.n.c.BEE796C48ADE497DA0A1.ntpupdateserver.com	a67d:db8:a2a1:7334:7654:4325:370:2aa3	Standard query response …
2019-03-07 15:31:34	53	aHR0cDovLzE3M 0.d.BEE796C48ADE497DA0A1.ntpupdateserver.com		Standard query 0x142f AA…
2019-03-07 15:31:34	64088	aHR0cDovLzE3M 0.d.BEE796C48ADE497DA0A1.ntpupdateserver.com	a67d:db8:85a3:4325:7654:8a2a:370:7334	Standard query response …
2019-03-07 15:31:34	53	i4xNi4xMDcuMT 1.d.BEE796C48ADE497DA0A1.ntpupdateserver.com		Standard query 0x35ec AA…
2019-03-07 15:31:34	53	i4xNi4xMDcuMT 1.d.BEE796C48ADE497DA0A1.ntpupdateserver.com	a67d:db8:85a3:4325:7654:8a2a:370:7334	Standard query response …
2019-03-07 15:31:34	53	I4L3VwbG9hZC9 2.d.BEE796C48ADE497DA0A1.ntpupdateserver.com		Standard query 0x554d AA…
2019-03-07 15:31:34	59636	I4L3VwbG9hZC9 2.d.BEE796C48ADE497DA0A1.ntpupdateserver.com	a67d:db8:85a3:4325:7654:8a2a:370:7334	Standard query response …
2019-03-07 15:31:34	53	WMGxPTFVSUVVV 3.d.BEE796C48ADE497DA0A1.ntpupdateserver.com		Standard query 0x1b97 AA…
2019-03-07 15:31:34	60039	WMGxPTFVSUVVV 3.d.BEE796C48ADE497DA0A1.ntpupdateserver.com	a67d:db8:85a3:4325:7654:8a2a:370:7334	Standard query response …
2019-03-07 15:31:34	53	TlBUa0pNTVU0N 4.d.BEE796C48ADE497DA0A1.ntpupdateserver.com		Standard query 0x2f34 AA…
2019-03-07 15:31:34	60504	TlBUa0pNTVU0N 4.d.BEE796C48ADE497DA0A1.ntpupdateserver.com	a67d:db8:85a3:4325:7654:8a2a:370:7334	Standard query response …
2019-03-07 15:31:34	53	FhGSnBZMnNnUl 5.d.BEE796C48ADE497DA0A1.ntpupdateserver.com		Standard query 0x6b0e AA…
2019-03-07 15:31:34	56492	FhGSnBZMnNnUl 5.d.BEE796C48ADE497DA0A1.ntpupdateserver.com	a67d:db8:85a3:4325:7654:8a2a:370:7334	Standard query response …
2019-03-07 15:31:34	53	c1bmJHbHphQSU 6.d.BEE796C48ADE497DA0A1.ntpupdateserver.com		Standard query 0x479e AA…
2019-03-07 15:31:34	54818	c1bmJHbHphQSU 6.d.BEE796C48ADE497DA0A1.ntpupdateserver.com	a67d:db8:85a3:4325:7654:8a2a:370:7334	Standard query response …
2019-03-07 15:31:34	53	zZCUzZC8yOTgz 7.d.BEE796C48ADE497DA0A1.ntpupdateserver.com		Standard query 0x7844 AA…
2019-03-07 15:31:34	56095	zZCUzZC8yOTgz 7.d.BEE796C48ADE497DA0A1.ntpupdateserver.com	a67d:db8:85a3:4325:7654:8a2a:370:7334	Standard query response …
2019-03-07 15:31:34	53	Yjk4My0wYWNkL 8.d.BEE796C48ADE497DA0A1.ntpupdateserver.com		Standard query 0xd217 AA…
2019-03-07 15:31:34	61107	Yjk4My0wYWNkL 8.d.BEE796C48ADE497DA0A1.ntpupdateserver.com	a67d:db8:85a3:4325:7654:8a2a:370:7334	Standard query response …
2019-03-07 15:31:34	53	TQyZGItOWQ4Ni 9.d.BEE796C48ADE497DA0A1.ntpupdateserver.com		Standard query 0xc69d AA…
2019-03-07 15:31:34	56976	TQyZGItOWQ4Ni 9.d.BEE796C48ADE497DA0A1.ntpupdateserver.com	a67d:db8:85a3:4325:7654:8a2a:370:7334	Standard query response …
2019-03-07 15:31:34	53	0wYjA5NmFmNWY 10.d.BEE796C48ADE497DA0A1.ntpupdateserver.com		Standard query 0xbed9 AA…
2019-03-07 15:31:34	62742	0wYjA5NmFmNWY 10.d.BEE796C48ADE497DA0A1.ntpupdateserver.com	a67d:db8:85a3:4325:7654:8a2a:370:7334	Standard query response …
2019-03-07 15:31:34	53	zNjl8fFRleHQg 11.d.BEE796C48ADE497DA0A1.ntpupdateserver.com		Standard query 0xf3d0 AA…
2019-03-07 15:31:34	53054	zNjl8fFRleHQg 11.d.BEE796C48ADE497DA0A1.ntpupdateserver.com	a67d:db8:85a3:4325:7654:8a2a:370:7334	Standard query response …
2019-03-07 15:31:34	53	d3JpdHRlbiB0b 12.d.BEE796C48ADE497DA0A1.ntpupdateserver.com		Standard query 0xf4e0 AA…
2019-03-07 15:31:34	55808	d3JpdHRlbiB0b 12.d.BEE796C48ADE497DA0A1.ntpupdateserver.com	a67d:db8:85a3:4325:7654:8a2a:370:7334	Standard query response …
2019-03-07 15:31:34	53	yBmaWxlLnR4dA 13.d.BEE796C48ADE497DA0A1.ntpupdateserver.com		Standard query 0xe2d4 AA…
2019-03-07 15:31:34	53475	yBmaWxlLnR4dA 13.d.BEE796C48ADE497DA0A1.ntpupdateserver.com	a67d:db8:85a3:4325:7654:8a2a:370:7334	Standard query response …
2019-03-07 15:31:34	53	0K.14.d.BEE796C48ADE497DA0A1.ntpupdateserver.com		Standard query 0x5732 AA…
2019-03-07 15:31:34	54857	0K.14.d.BEE796C48ADE497DA0A1.ntpupdateserver.com	a67d:db8:85a3:4325:7654:8a2a:370:7334	Standard query response …
2019-03-07 15:31:34	53	n.15.f.BEE796C48ADE497DA0A1.ntpupdateserver.com		Standard query 0xfb12 AA…
2019-03-07 15:31:34	56265	n.15.f.BEE796C48ADE497DA0A1.ntpupdateserver.com	a67d:db8:85a3:4325:7654:8a2a::	Standard query response …

What do we do today?

- Signatures – network application control (APPI)
  - Tools/applications/anonymizers



- IPS Signatures
  - DNS Tunneling – mechanism built inside the GW

Signature ID	Signature Name	Hits last 30 days
8589622049	Malicious Activity Over DNS Tunneling	XXXXX
7596623894	DNS Tunneling	XXXXX
8044502309	SSH Over DNS Tunneling	XXXXX

Deep DNS Tunneling – How it works

Deep Neural Network with 2 objectives:

1. Compress and reconstruct the subdomain (encoder decoder architecture based on GRU)
2. For known tunneling domains, fail the reconstruction (change the mathematics of the loss function)

Bad

150K

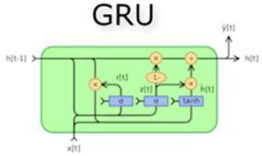
Known DNS Tunneling Tools

o0axdqw2fhdaiyjmpyfztxoia1h5kkcrbsrgqpc9fl**.k2h4.com**
acfsnui7geismdxwansql59rlcjkhc34syupzetume**.k2h4.com**
z9dw9kus6vksnlxlu5tirlniweoxrsjbduwmh8rl**.k2h4.com**

good vs. bad X 1,000

(Unsupervised)

GRU



Good

100,000,000

Subdomains

amplify.outbrain.com
hangouts.google.com
ampcid.google.com
pull-flv-l16-tt01.tiktokcdn-us.com
cookie-matching.mediarithmics.com
vms-eu.boldchat.com
edgedl.me.gvt1.com
t.wayfair.com
duckduckgo.com

Identify tunneling attacks as these attacks do not behave in the standard manner of subdomains – they encode payload into the subdomains…

Teach the network how the structure of legitimate subdomain looks like

Algorithm is able to detect zero day attacks

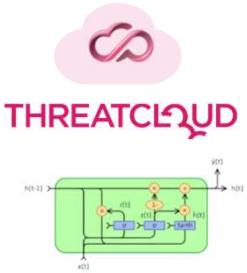
Deep DNS Tunneling – How it works in production

1. Aggregate results in a 4 hours window
2. Group by 1st + 2nd level domains
3. For each group, calculate:
   A. The amount of unique '**look like tunneling**' subdomains (model score > threshold)
   B. The amount **unique** subdomains
   C. Total amount of requests to domain (**not unique**)
4. Logic to decide if a tunneling domain:
   A. A/C > 50% (3 out of 5)
   B. A>2 (A = 3)
   C. B/C distinct domain ratio (5 out of 6)

   (it will remove FP on popular domains that are used for both "tunneling look alike traffic" and legitimate purpose)

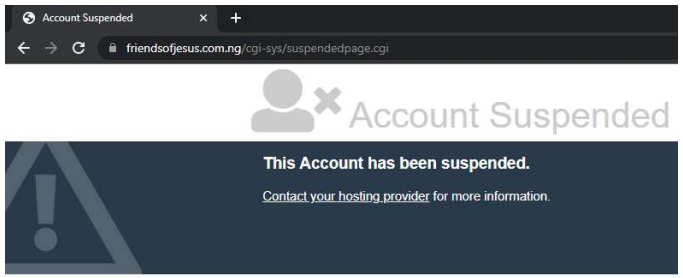
- qweuiyqwiey.googleme.com
- uqyekc68123.googleme.com
- jfejkdz12312.googleme.com
- www.googleme.com
- beta.googleme.com
- beta.googleme.com

DeepDNS – Detected Samples



8xp0-vzzh8i-wni58xp0-vzzh8i-wni58xp0-vzzh8i-wni5.**friendsofjesus.com.ng**
8oh0-uuqj6m-qdm28oh0-uuqj6m-qdm28oh0-uuqj6m-qdm2.**friendsofjesus.com.ng**
x2.**friendsofjesus.com.ng**
5un0-eexu3r-sve95un0-eexu3r-sve95un0-eexu3r-sve9.**friendsofjesus.com.ng**
8en1-bvks1v-zqr98en1-bvks1v-zqr98en1-bvks1v-zqr9.**friendsofjesus.com.ng**
9ut9-kicn1g-muz69ut9-kicn1g-muz69ut9-kicn1g-muz6.**friendsofjesus.com.ng**
9mp7-mjeb6w-ogy19mp7-mjeb6w-ogy19mp7-mjeb6w-ogy1.**friendsofjesus.com.ng**
du.**friendsofjesus.com.ng**
fa.**friendsofjesus.com.ng**
3pl0-mdeo3h-gof43pl0-mdeo3h-gof43pl0-mdeo3h-gof4.**friendsofjesus.com.ng**
oh.**friendsofjesus.com.ng**
3y.**friendsofjesus.com.ng**
1ow9-onux8m-vru91ow9-onux8m-vru91ow9-onux8m-vru9.**friendsofjesus.com.ng**
7ck9-abhg5n-ady67ck9-abhg5n-ady67ck9-abhg5n-ady6.**friendsofjesus.com.ng**
3vb9-rxxl1x-vis63vb9-rxxl1x-vis63vb9-rxxl1x-vis6.**friendsofjesus.com.ng**
5lx9-dpus4t-rkt45lx9-dpus4t-rkt45lx9-dpus4t-rkt4.**friendsofjesus.com.ng**
ma.**friendsofjesus.com.ng**
0gz5-waeo5g-jxc70gz5-waeo5g-jxc70gz5-waeo5g-jxc7.**friendsofjesus.com.ng**
2sj8-lygf7z-sej22sj8-lygf7z-sej22sj8-lygf7z-sej2.**friendsofjesus.com.ng**

o0axdqw2fhdaiyjmpyfztxoia1h5kkcrbsrgqpc9fl.**k2h4.com**
acfsnui7geismdxwansql59rlcjkhc34syupzetume.**k2h4.com**
v31pl0uwygyblhxogyd2pdr827ojve9wyhrcvqyh3s.**k2h4.com**
z9dw9kus6vksnlxlu5tirlniweoxrsjbduwmh8rl.**k2h4.com**
jyr2bfaarlfjdy7w77x8ptuj1xvvhma4iphjht3w.**k2h4.com**



DeepDNS Tunneling – GW Stats Hits

- In the past 30 days:
  - 32k log hits seen in 474 GW's
  - In most cases it was the only vendor to catch
  - Only 2 out of over 14,500 ioc's were also found by another vendor

DeepDNS – Attack Simulation of a Recent Blog

- Run the malware on VM, malware generates DNS traffic
- Matches the domain and format posted in the blog
- Tunnel detected by DeepDNS

```
11111.593421518.4653c1e56c8de52d154450c01d728e4573d953f24d98482bbea3a635a27f0a.dev42.bancodobrasil.dev
11111.593421518.4653c1e56c8de52d154450c01d728e4573d953f24d98482bbea3a635a27f0a.dev42.bancodobrasil.dev
11112.593421518.d27aaf3d8c2640347a8c140150768046c15e5fb62eb5b32b052f5e87ba5a47.dev42.bancodobrasil.dev
```

11111[.]593421518[.]4653c1e56c8de52d154450c01d728e4573d953f24d98482bbea3a635a27f0a[.]dev42[.]bancodobrasil[.]dev

(Packet Number, Machine ID, Hex Encoded Payload, Domain Name)

- https://blogs.blackberry.com/en/2022/06/symbiote-a-new-nearly-impossible-to-detect-linux-threat

Check Point: The LEADING Global Cyber Security Company

GLOBAL LEADER
100,000+ CUSTOMERS,
88+ COUNTRIES, 6,200+ PARTNERS

6,000+
EMPLOYEES WORLDWIDE,
TOP TALENT

CUTTING-EDGE TECHNOLOGIES
OVER 30 YEARS OF EXPERTISE,
INDUSTRY'S MOST VISIONARY PLAYER

TRADED ON NASDAQ
1996 I CHKP

INNOVATION LEADERSHIP
HIGHEST NUMBER OF AI REAL-TIME
PREVENTION TECHNIQUES

WORLD'S BEST EMPLOYER
BY FORBES,
#1 CYBER SECURITY VENDOR

TRUSTED BY
FORTUNE 500

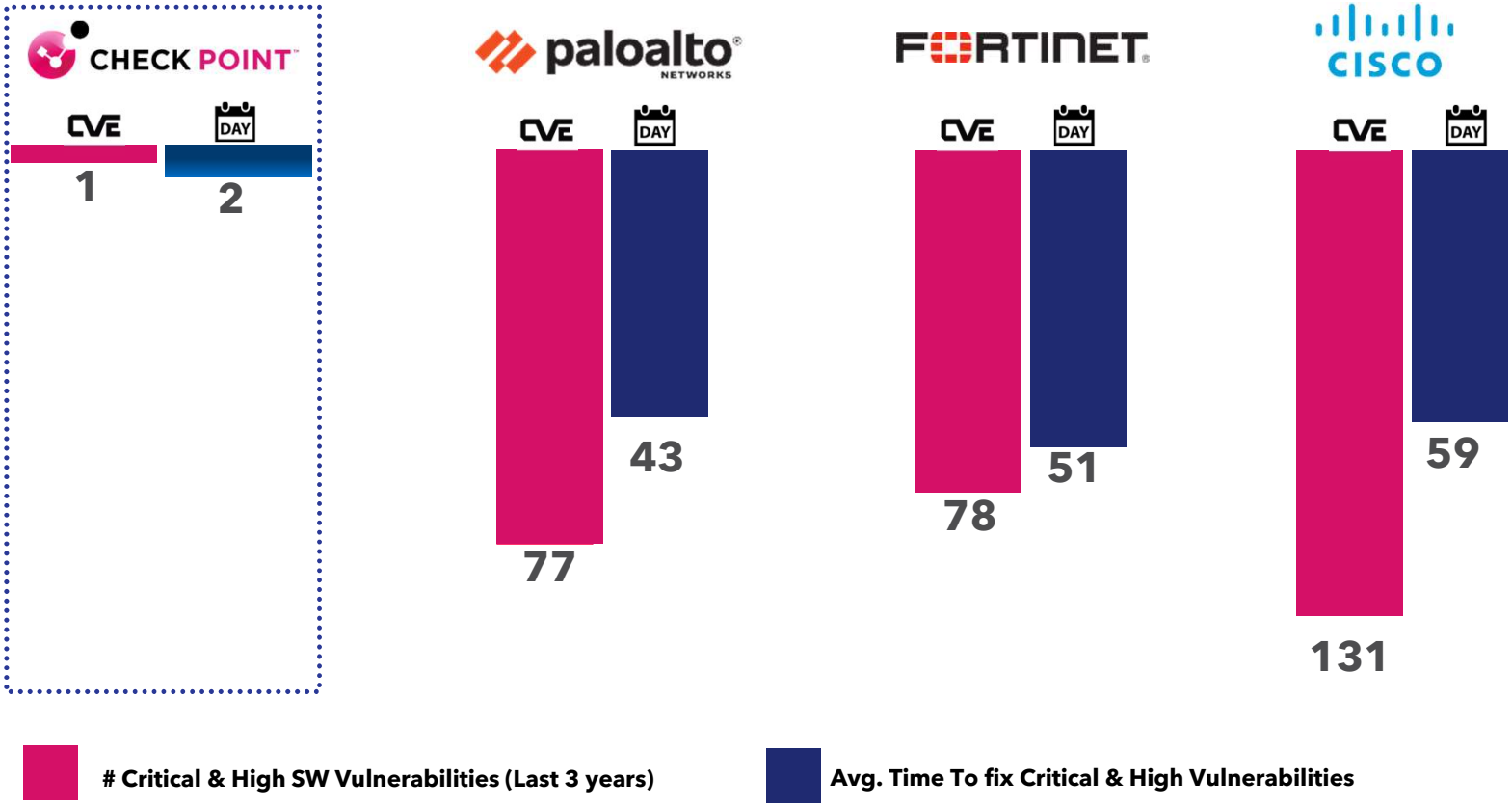
30 Years of Recognition

NETWORK	Gartner	**22 times Security Leader in Magic Quadrant**
	Gartner	**Customers' Choice for Unified Threat Management**
	NSS LABS	**Highest cyber prevention score in Breach Prevention**
ENDPOINT & EMAIL	MITRE ENGENUITY	**Highest coverage of detected attacking techniques**
	AV-TEST	**Top Product Scoring: 17.5 / 18**
	FORRESTER	**a leader in the Email Security Forrester Wave™**
MOBILE	IDC	**Highest Mobile security value**
CLOUD	Leader WINTER 2023	**CloudGuard, Leader in 5 customer choice grids**

COMPREHENSIVE SECURITY WITH FASTEST RESPONSE TIME TO VULNERABILITIES

95X
less High-Profile Vulnerabilities

26X
Faster Response

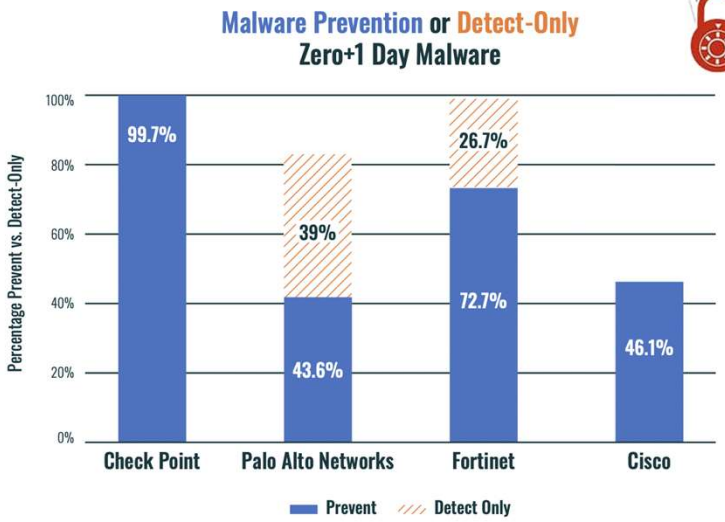


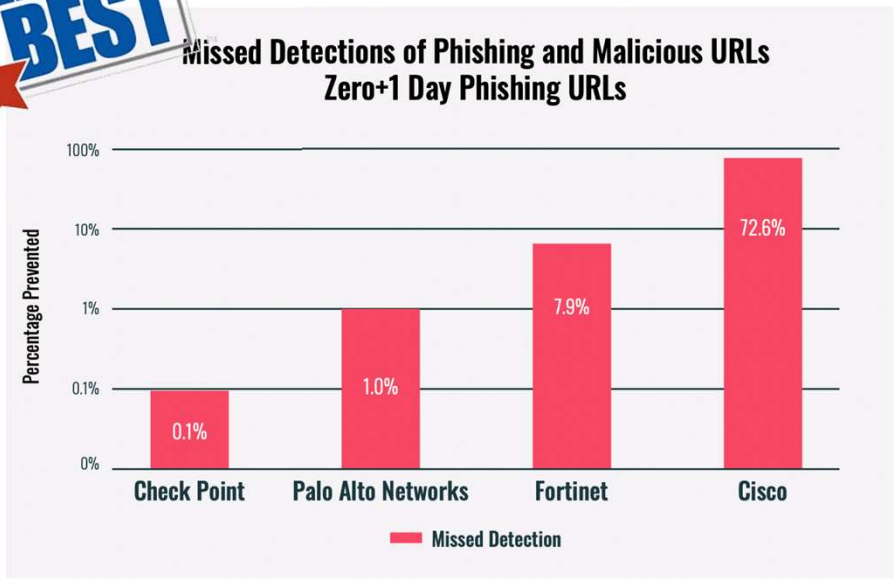
 # Critical & High SW Vulnerabilities (Last 3 years)

Avg. Time To fix Critical & High Vulnerabilities

Source: vendors security advisories web pages & https://tiny.cc/urgency
Updated July 1st 2023

COMPREHENSIVE SECURITY VALIDATED BY 3RD PARTY (MIERCOM): THE BEST PROTECTION AND VALUE TO OUR CUSTOMERS





Read the full report at https://tiny.cc/miercom23

Advice to CISO's and Business Leaders:

For business leaders, adopt a baby steps approach. Don't rush into it without dictating policy and safeguards following a risk assessment/project prioritization process.

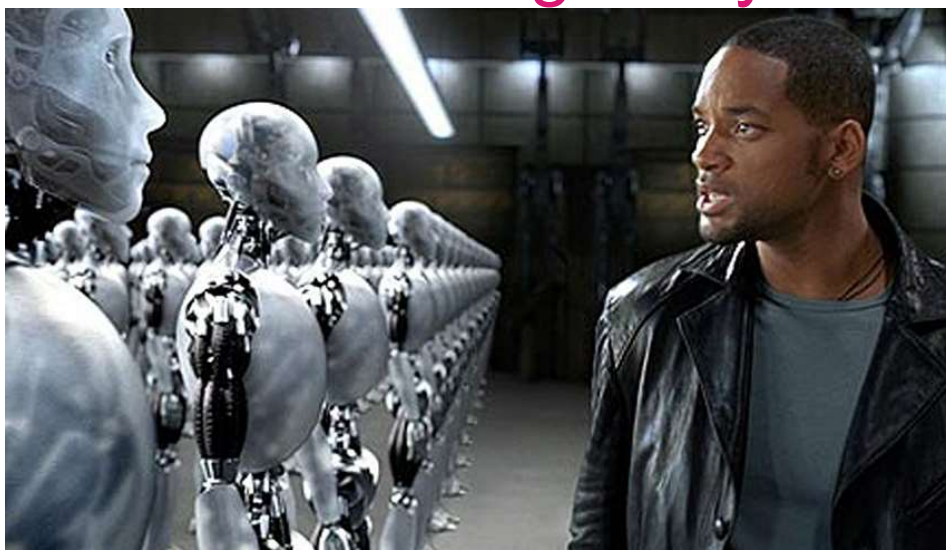
- Pick some easy projects, and get some fast wins!
- Adopt its use into existing policies.
- Communicate: Share do's and don'ts with all employees via the Security Awareness programs.
- Supply Chain Risk awareness: Review contracts to ensure no co-mingling, or use of your data to help competitors
- Monitor/Enforce: Ensure that PII or critical data is not getting exposed to AI platforms that didn't obtain the required level of trust according to the sensitivity levels. Leverage enforcement mechanisms such as DLP + WAP (Web application and API protections) security capabilities.

Questions to Bring Home and Discuss with your Team:

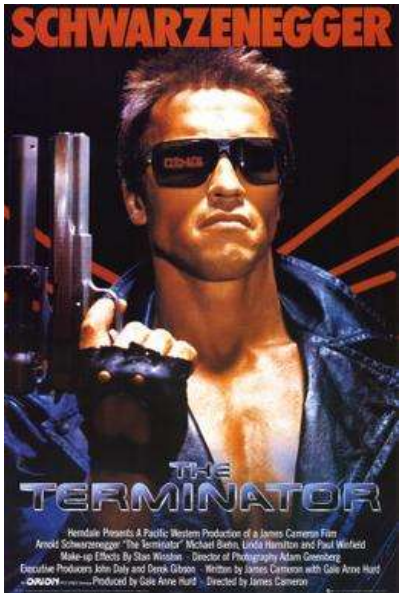
Artificial Intelligence Risks and Issues

- As a CISO whose company is using AI tools, let's start by discussing some of the positive capabilities you are seeing and supporting.
- What AI technologies are you using at your organization? How are they adding value?
- Are you leveraging any of the AI Related Guidance from NIST or others?
- What should CISOs communicate to employees, execs, boards?
- Have you created organizational policies around the use of generative AI? Are you allowing it?
- Now, lets go the dark side, where do you see you company at risk by leveraging AI tools?
- From an external threat landscape perspective, how is AI impacting attack capabilities and patterns?
- Have the advances in generative AI changed how you're thinking about the threat landscape? Is it shifting your security posture? Are you looking at changing or enhancing tools and or processes?
- What are best practices to vet legitimate AI technologies? What are the hard questions security leaders should ask?
- What is your thinking on vendors in your supply chain using AI technologies? Are you looking for them to leverage AI?
- What are you doing to monitor and put security controls around this?

When is the Singularity?



NS-5 Robots in I, Robot



SKYNET and The Terminator

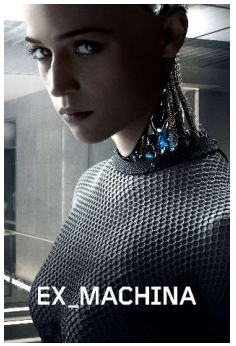
J.A.R.V.I.S

M3GAN

ARISA

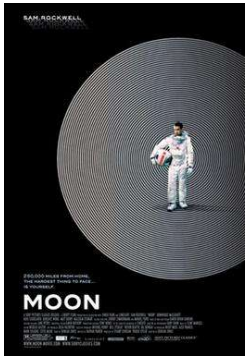
2001

Blade Runner



Ex Machina

Metropolis



MOON

CHECK POINT

Thank You! Danke! Gracias! Merci! Grazie! תודה!

petern@checkpoint.com

https://www.linkedin.com/in/petenicoletti/

PETE'S AI DISCUSSION MEDIA APPEARANCES:

GMA segment was extended to an **ABC News Nightline** feature & online article informing about the rapid increase in malicious actors utilizing Artificial Intelligence to imitate human voices.

Pete's in-person interview with **CBS LA**. **CBS LA's Evening News with Norah O'Donnell** as part of their "***Age of AI series***" on July 12th, and it was later showcased again in an extended interview on the **CBS Morning Show** on July 19th.

The coverage didn't stop there! The interview was syndicated across the US appearing in **over 1,000 instances** in top markets such as San Francisco, Las Vegas, Austin, New York City, Washington and many others.

Live interviews with Fox12 Oregon

- https://www.youtube.com/watch?v=9TqjHdWD1u4&t=29s
- https://www.youtube.com/watch?v=Fgm1Fk90Z4I&t=658s
- https://www.youtube.com/live/t8pceEuKn3E?si=CPyiktvq4OhZ-sAx

CISO to CISO Interview: Inside the CISO's Office: Dive in with Pete Nicoletti, a hacker's worst nightmare - YouTube
Interview with Vox- print- https://www.vox.com/technology/2023/9/15/23875113/mgm-hack-casino-vishing-cybersecurity-ransomware
1.Comments on IT Brew- : https://www.itbrew.com/stories/2023/09/14/mgm-resorts-hit-by-alleged-ransomware-attack
2.KTNLV- Broadcast- https://mms.tveyes.com/PlaybackPortal.aspx?SavedEditID=4f924f35-f192-4831-b063-99dd938dcaed
3.WVON- radio- https://mms.tveyes.com/PlaybackPortal.aspx?SavedEditID=ecd571d9-e932-4bbc-a7e3-4a8f73ed77d0
4.Fox 13: https://www.fox13now.com/the-place/software-to-avoid-getting-scammed
5.News 12 Hudson Valley - https://bronx.news12.com/ransomware-attack-targets-commack-school-district
6.WEF Byline: https://www.weforum.org/agenda/2023/08/6-ways-to-reduce-cybersecurity-spend-without-compromising-security/
7.And two comments on Tech Republic: https://www.techrepublic.com/article/microsoft-apple-spyware/ and https://www.techrepublic.com/article/check-point-hackers-usb/

What Are The “Killer Apps” Everyone Should Know about?

ChatGPT
Let’s start with a quick recap of the viral sensation that is ChatGPT. It is a conversational interface for OpenAI’s GPT-3 large language model, which has recently been made available to the public as a free research preview. In response to text prompts such as questions or instructions, it will output text in any form, including prose, poetry, and even computer code.

Dall-E 2
Another OpenAI project, which together with ChatGPT is responsible for kick-starting the current wave of consumer interest in generative AI. This one takes text prompts and transforms them into computer graphics (images, photos, drawings, paintings, etc.).

Stable Diffusion 2
This is another text-to-image generative AI application. Unlike Dall-E 2, its source code, as well as details on the training data and weighting used by its algorithms, are openly available to the public, and the application can be downloaded and installed on your own computer rather than only being accessible through a proprietary cloud portal as is the case with OpenAI’s projects.

Lumen5
An AI-powered video creation tool that enables anyone to easily create education, marketing, or business video content using a simple drag-and-drop interface.

Soundraw
Automated music generator – create royalty-free AI music by simply making decisions about the genre of music you want to create, the instruments that will be used, the mood you want to create, and the length of the track. Then sit back and let the AI compose unique tracks.

Looka
This is a tool that makes it easy to brand your business by using AI to create unique and distinctive logos that convey your company style and messaging. This tool makes it a doddle to start creating customized marketing material even if you don’t have any design skills.

Podcastle
An audio recording and editing platform with integrated AI tools that helps you create clear, super-smooth recordings that sound as if they’ve been edited professionally, automating tasks like cleaning up messy sounds and creating transcripts.

Gen-1
Cloud-based text-to-video platform that creates new videos from ones that you upload, using text prompts to apply the edits and effects that you desire, or create animations from storyboard mock-ups. This tool was also developed by the creators of Stable Diffusion.

Lalal.ai
This tool uses a neural network system called Phoenix to automate audio source separation. This involves extracting elements such as vocals, music, or even specific instrumental tracks like drumbeats or basslines from any audio or video content.

Deep Nostalgia
Do you have historic family photographs of distant relatives or ancestors who you’d like to see in motion? This innovative tool lets you animate the faces in family photos so you can see them smile, blink, and laugh, just as if you had recorded a video of them back in the day.

Murf
This is a text-to-speech engine that makes it simple to create natural-sounding synthetic vocal recordings in 15 languages from a choice of over 100 voices and dialects. This output can easily be incorporated into automated marketing or video content, automating the process of creating narration and voiceovers.

Legal Robot
This tool is designed to automatically translate complex and confusing “legalese” into straightforward language that can be understood by anyone. Useful both for laypeople wanting to make sure they understand legal documents and for legal professionals to ensure that their contracts and documents are written in terms that anyone can understand.

Cleanup.Pictures
This AI tool lets you retouch images by removing unwanted objects, defects, or even people, using a process known as “inpainting” to help you create the perfect image.

Fireflies
This tool plugs into popular video conferencing tools like Zoom, Teams, or Webex and automates the process of taking notes and creating transcriptions. It also analyzes conversations to provide insights into the dynamics and decision-making that are going on in your conversations.

Krisp
Another conferencing application, this one uses algorithms to remove background noises, echo, and other distracting elements in real-time, ensuring that you always come across in a clear and professional manner.

DEEPFAKES AND INFLUENCE BOTS RESOURCES

https://github.com/iperov/DeepFaceLab

https://www.rand.org/blog/2020/01/artificial-intelligence-and-the-manufacturing-of-reality.html

https://mitsloan.mit.edu/ideas-made-to-matter/how-do-online-bots-shift-opinions

https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2740/RAND_RR2740.pdf

https://arstechnica.com/tech-policy/2016/12/op-ed-five-unexpected-lessons-from-the-ashley-madison-breach/

https://www.ftc.gov/system/files/documents/reports/social-media-bots-advertising-ftc-report-congress/socialmediabotsreport.pdf

https://foreignpolicy.com/2019/08/12/8-ways-to-stay-ahead-of-influence-operations/

https://www.wired.com/story/law-makes-bots-identify-themselves/

https://venturebeat.com/2020/09/30/how-bots-threaten-to-influence-conversations-ahead-of-the-2020-u-s-elections/

https://www.fastcompany.com/90390287/this-ai-generates-fake-news-about-anything-you-want-try-it

https://www.forbes.com/sites/bernardmarr/2023/05/24/the-29-best-and-free-chatgpt-and-generative-ai-courses-and-resources/?sh=1e1819054a6f

The human side of generative AI: Creating a path to productivity | McKinsey

MORE INFLUENCE BOTS RESOURCES

https://www.forbes.com/sites/robpegoraro/2020/08/07/from-russia-with-lure-why-were-still-beset-by-bots-and-trolls-pushing-disinformation/?sh=2546610e5542

https://www.pewresearch.org/internet/2018/04/09/bots-in-the-twittersphere/

https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search.html

https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/

https://cyber.fsi.stanford.edu/io/

https://ieeexplore.ieee.org/document/7490315

https://www.rand.org/pubs/research_reports/RR2705.html

https://asiatimes.com/2021/02/collectively-countering-chinas-influence-operations/

https://www.reuters.com/article/us-china-robots-idUSKBN1AK0G1

https://www.darkreading.com/threat-intelligence/how-china-and-russia-use-social-media-to-sway-the-west/d/d-id/1334108

https://www.recordedfuture.com/china-social-media-operations/

AI/ML/ANN ALGORITHMS RESOURCES

https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/

https://www.brookings.edu/blog/techtank/2019/01/03/artificial-intelligence-and-bias-four-key-challenges/

https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms

https://cio.economictimes.indiatimes.com/news/corporate-news/google-ai-researchers-abrupt-exit-sparks-ethics-bias-concerns/79591079

https://plato.stanford.edu/entries/ethics-internet-research/

https://aif360.mybluemix.net/

http://sciencepolicy.duke.edu/content/forget-killer-robots%E2%80%94bias-real-ai-danger

https://www.technologyreview.com/2017/07/12/150510/biased-algorithms-are-everywhere-and-no-one-seems-to-care/

https://cacm.acm.org/magazines/2020/3/243021-dilemmas-of-artificial-intelligence/fulltext

https://www.scu.edu/ethics/all-about-ethics/artificial-intelligence-and-ethics/

https://journalofethics.ama-assn.org/article/ethical-dimensions-using-artificial-intelligence-health-care/2019-02

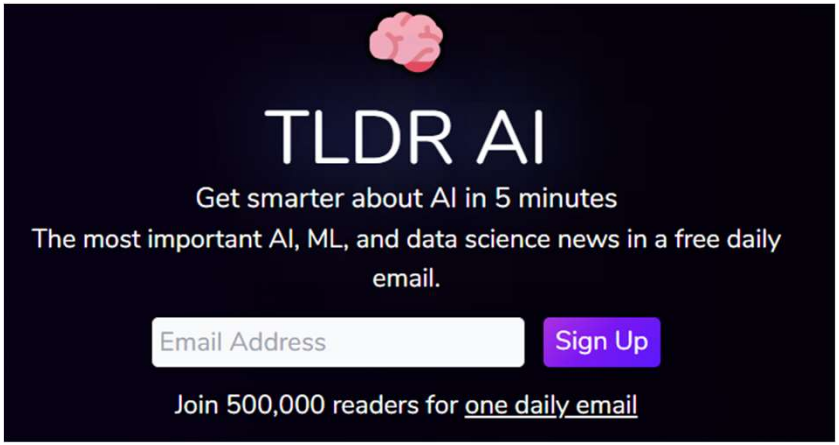
https://plato.stanford.edu/entries/ethics-ai/

https://www.forbes.com/sites/bernardmarr/2023/05/24/the-29-best-and-free-chatgpt-and-generative-ai-courses-and-resources/?sh=1e1819054a6f

Sign Up for these AI Newsletters!

TLDR: Get smarter about AI in 5 minutes (tldr.tech)
https://tldr.tech/ai

CB Insights:
https://www.cbinsights.com/newsletter/



Subscribe | FryAI (fry-ai.com)
https://www.fry-ai.com/subscribe?ref=M6mKsLv16q

CYBERSECURITY/NATIONAL SECURITY RESOURCES

https://www.aspi.org.au/report/weaponised-deep-fakes

https://www.rand.org/multimedia/audio/2020/10/23/using-ai-to-tackle-disinformation-online.html

https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT473/RAND_CT473.pdf

https://www.foreignaffairs.com/articles/2018-10-04/what-clausewitz-can-teach-us-about-war-social-media

https://comprop.oii.ox.ac.uk/

https://redy.ssri.duke.edu/news/don%E2%80%99t-believe-your-eyes-or-ears-weaponization-artificial-intelligence-machine-learning-and

https://www.cbc.ca/news/world/china-hong-kong-national-security-law-1.5633277

https://www.fbi.gov/investigate/counterintelligence/the-china-threat

http://www.homelandsecuritynewswire.com/dr20210209-deepfake-detectors-can-be-defeated-researchers-show-for-the-first-time

https://www.brookings.edu/research/fighting-deepfakes-when-detection-fails/

https://www.lanl.gov/discover/publications/national-security-science/2020-winter/deepfakes.php

https://www.media.mit.edu/projects/detect-fakes/overview/

https://hai.stanford.edu/blog/using-ai-detect-seemingly-perfect-deep-fake-videos

https://www.nextgov.com/emerging-tech/2019/08/darpa-taking-deepfake-problem/158980/

https://www.fastcompany.com/90273352/maybe-its-time-to-take-away-the-outdated-loophole-that-big-tech-exploits

Paul Rosenzweig book ‘Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World’

Bobby Akart book ‘Cyber Warfare’

Dr. Chase Cunningham book ‘Cyber Warfare – Truth, Tactics, and Strategies’

CHECK POINT

Thank You! Danke! Gracias! Merci! Grazie! תודה!

petern@checkpoint.com

https://www.linkedin.com/in/petenicoletti/