2024

The Intersection of Cybersecurity and AI

Nikhil Agarwal

Sr. Architect, Fortanix

FutureGPT

Engineer by Qualification, Architect by Profession, a Hacker at Heart and a Researcher by Passion.

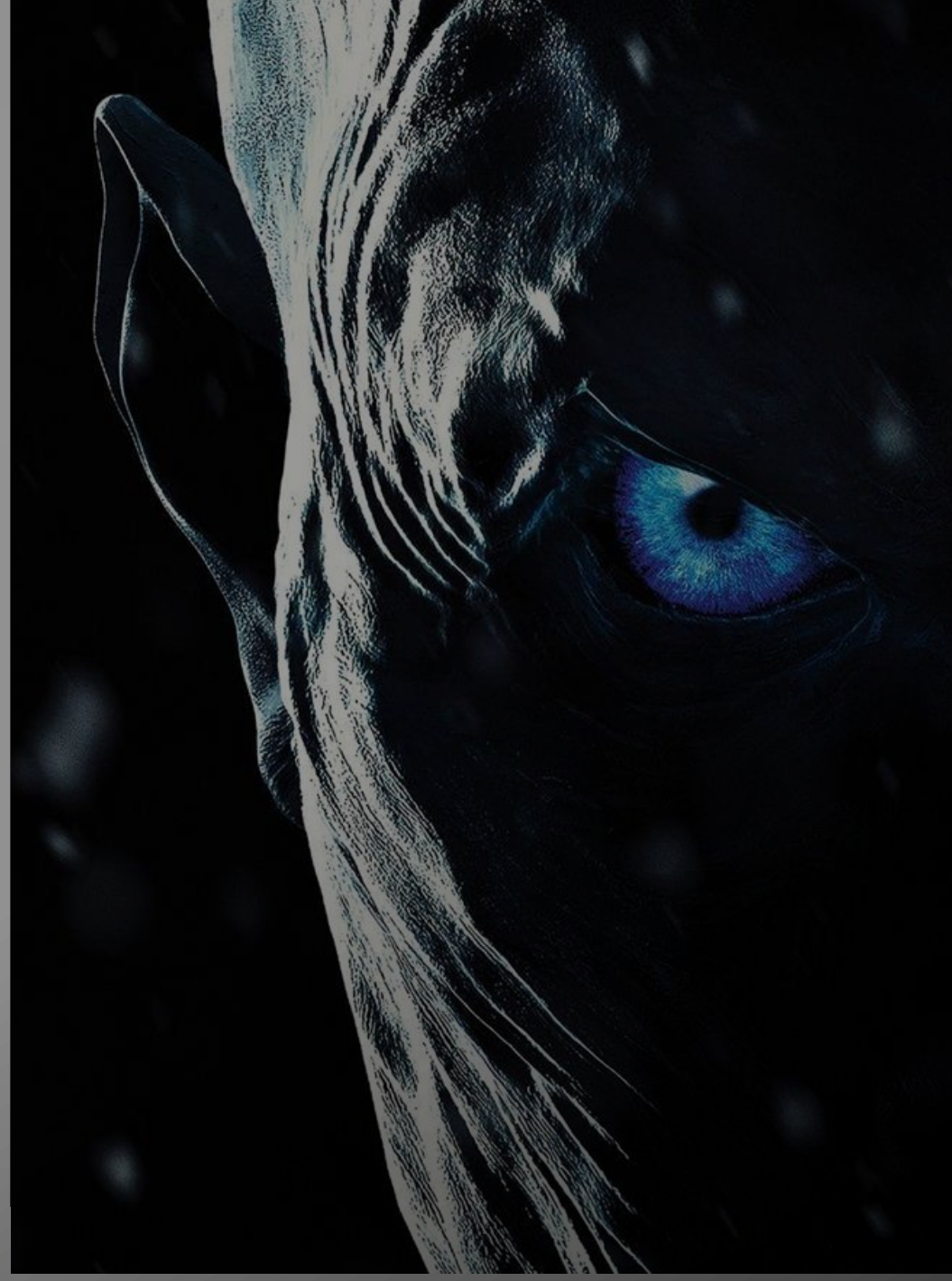
WHO AM I?

Nikhil Agarwal

Sr. Architect, R&D Team – Fortanix Inc.	Technology Enthusiast
Active Red Teamer & Bug Bounty Hunter	Speaker & Author
Love Teaching and building community	Avid Traveler

@REACHTONIKHIL

www.reachtonikhil.com



AGENDA

Current AI Landscape

AI Use cases in Cyber Security

Challenges and Concerns on AI in Cyber Security

Live Demo - Let's fool an LLM?

What is PET?

Protecting AI Workloads using Confidential Computing

Future of AI in Cyber Security

Arts / BUSINESS

THE POWER OF HUMANS AND A.I.

who lives in suburban Detroit. But she chose a sport utility vehicle last fall instead of a mini-van, she said, because "I wanted to be a mom, yet I wanted my own identity."

Mrs. Byer is not alone. Soccer moms and baseball dads, tired of driving mommy-mobiles, are rebelling against their mini-vans. After more than a decade of steadily rising sales, mini-van sales are falling. No one disputes that the mini-vans are roomy, practical and cheaper than most sport utility vehicles and some of the sedans people are buying instead. But more and more people are rejecting the image that mini-vans project.

Cars have always been one way for people to define themselves, and the move away from mini-vans represents a cultural shift as well. In the 80's, when mini-vans were introduced, they became a symbol of the super-mom image of the era. "In our culture right now, there is a lot of tension between what is for me and what is for my kids," said Madelyn Hochstein, president of DYG Inc., a social and market research firm in Danbury, Conn. "The mini-van sort

Markets can't get enough of AI as tech rally passes $4tn

FTSE 100 56.33 | All share 24.21 | Dow Indl 296.58 | Nikkei 225 115.18 | €/£ 1.1520 | €/$ 1.2332

Busi

competition means good deals for buyers. But it also suggests shrinking profits for auto makers in the future, especially for the Chrysler Corporation, which invented the mini-van and has bathed in a river of cash and profit from it.

baby boomer generation, now 51 or slightly younger, are at the stage when, if they became parents, most of their children have grown up. Many of the younger boomers have

Continued on Page D11

In one of those villages, 110 young girls were killed nearly at once, as their elementary school collapsed and buried them under jagged slabs of steel and concrete. At least 2,000

Continued on Page A8

Swift and Slashing, Computer Topples Kasparov

By BRUCE WEBER

In brisk and brutal fashion, the I.B.M. computer Deep Blue unseated humanity, at least temporarily, as the finest chess playing entity on the planet yesterday, when Garry Kasparov, the world chess champion, resigned the sixth and final game of the match after just 19 moves, saying, "I lost my fighting spirit."

The unexpectedly swift denouement to the bitterly fought contest came as a surprise, because until yesterday Mr. Kasparov had been able to summon the wherewithal to match Deep Blue gambit for gambit.

The manner of the conclusion overshadowed the debate over the meaning of the computer's success. Grandmasters and computer experts alike went from praising the match as a great experiment, invaluable to both science and chess (if a temporary blow to the collective ego of the human race) to smacking their foreheads in amazement at the champion's abrupt crumpling.

"It had the impact of a Greek tragedy," said Monty Newborn, chairman of the chess committee for the Association for Computing, which was responsible for officiating the match.

It was the second victory of the match for the computer — there were three draws — making the final score 3½ to 2½, the first time any chess champion has been beaten by a machine in a traditional match. Mr. Kasparov, 34, retains his title, which he has held since 1985, but the loss was nonetheless unprecedented in his career; he has never before lost a multigame match against an individual opponent.

Reuters

Garry Kasparov during the match he lost to Deep Blue yesterday.

Inscrutable Conqueror

Deep (RS/6000 SP) Blue

By ROBERT D. McFADDEN

When it was all over yesterday, when the greatest chess player in history had been crushed, the machine that had done it — I.B.M.'s RS/6000 SP, alias Deep Blue — did the

Computer in the

magnanimous thing: it kept its monastic silence. After days of Man-

beery voice to gloat. Under its smooth metal skin, the chips, wires and electronic circuits were tightly packed and almost alive with invisible blips, but there was not even radiator's clank or gurgle to whispe sympathy, nothing to show a carin or a cruel heart.

Rangers Move On; Knicks Win, Too

The long reach of Adam Graves and Patrick Ewing helped give the Rangers and Knicks dramatic victories in their playoff series yesterday, with the Rangers' triumph over the Devils putting them in the semifinals of the Stanley Cup tournament.

The Devils forced the Rangers to work overtime for their 2-1 victory, but Graves finally delivered it when he circled behind the goal, then swept the puck under goaltender Martin Brodeur, 14 minutes 8 seconds into the extra period. The Rangers won the series in five games.

The Knicks got their second victory in three games against the Heat when Ewing swatted away a potential game-tying basket to preserve a 77-73 victory. Game 4 in the best-

How AI and automation play crucial roles in security ops

TIMES TECHIES

INDUSTRY MOVES TO MINIMISE HYPE, MYTH

Cyber security sector set to consolidate due to AI crime threat

Need for more data on incidents will see a small number of major players, say vendors

Security has become a game of scale. The more data you have about incidents, the greater your efficacy will be as a security vendor... By definition, there are only a few [companies] that can do that.

ChatGPT plays vital role in cybersecurity

The Telegraph

TALK | JOBS | PAN WIN

BEYOND CAMPUS

AI on the future

Artificial intelligence will lead to an estimated two lakh jobs in the near future, writes Omkar Rai. This is a good time to take up the study of AI and machine learning.

Families Emerge Of Tuskegee Sy

By CAROL K

TUSKEGEE, Ala., May 9 — It has been 25 years since the nation learned that more than 400 black men infected with syphilis went untreated for decades in a federally financed experiment in this rural Southern town laced with sandy roads and pine forests.

These men, who are expected to receive a Presidential apology on Friday in Washington, have been the subject of countless academic studies, news articles and books, as well as a play and a made-for-television movie.

Yet their families — the wives and children they may have unwittingly exposed to the disease — have remained largely unseen and unheard, bearing in silence a legacy of anger and shame as well as possible dam-

India is fast emerging as hub for cybersecurity innovations

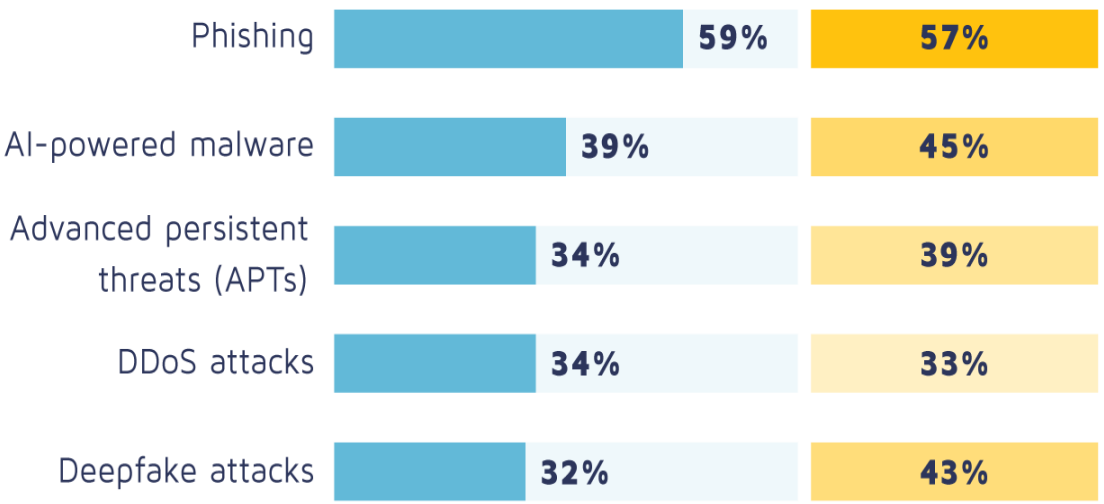
As new malware emerge faster than ever, R&D centres are fighting back

BIG IMPROVEMENT IN QUALITY OF INDIA'S CYBER TALENT

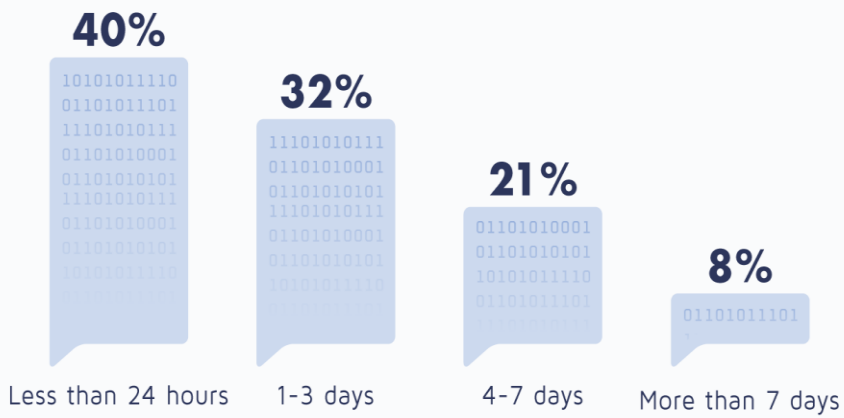
THE **AI CYBER THREAT**

More than **1 in 6 cybersecurity specialists** worked for companies that **suffered AI-fueled cyberattacks**. **Medium-sized** companies were **41% more likely** than micro, small, and large companies to **experience them**.

Most Commonly Seen AI-Fueled Cyberattacks

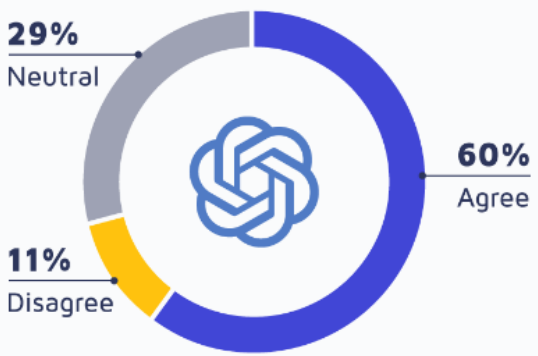


How long did it take your company to detect and respond to the AI-powered cyberattack?

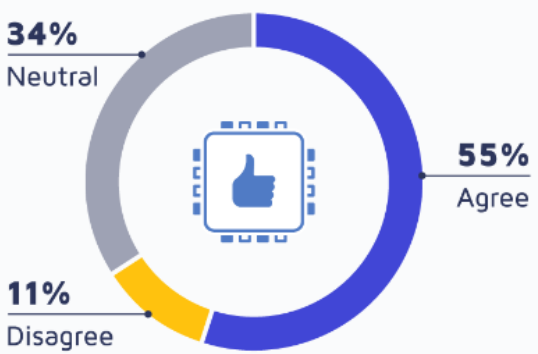


Do you agree or disagree with the following statements?

ChatGPT will be used for cyberattacks in 2023.

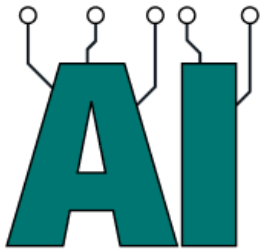


AI's benefits in cybersecurity outweigh its drawbacks.



https://www.beyondidentity.com/resources/cyber-pros-weigh-in-on-ai-impact

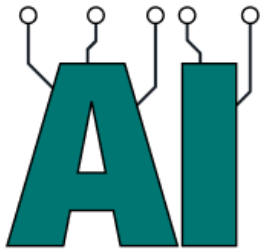
In 2022



the market size for AI in cybersecurity was

$17 billion

By 2032



is projected to reach an impressive

$102 billion

48.9%

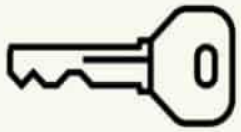
of global executives and security experts consider AI and machine learning as potent tools to combat modern cyber threats.

44%

of global organizations are already leveraging AI to detect security intrusions.

PRIORITY AI USE CASES IN CYBERSECURITY

AI Reduces the Total Response Time but is Limited by Simplistic AI Deployments



49% of breaches involved stolen credentials*

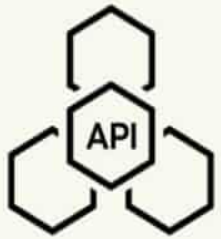
Identity & Credential Attacks

Digital Fingerprinting

74% of breaches include human element*

Phishing & Social Engineering

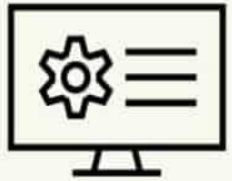
Phishing Simulation & Detection



49-day average to patch critical vulnerabilities*

Vulnerability Management

CVE Tools and Workflows



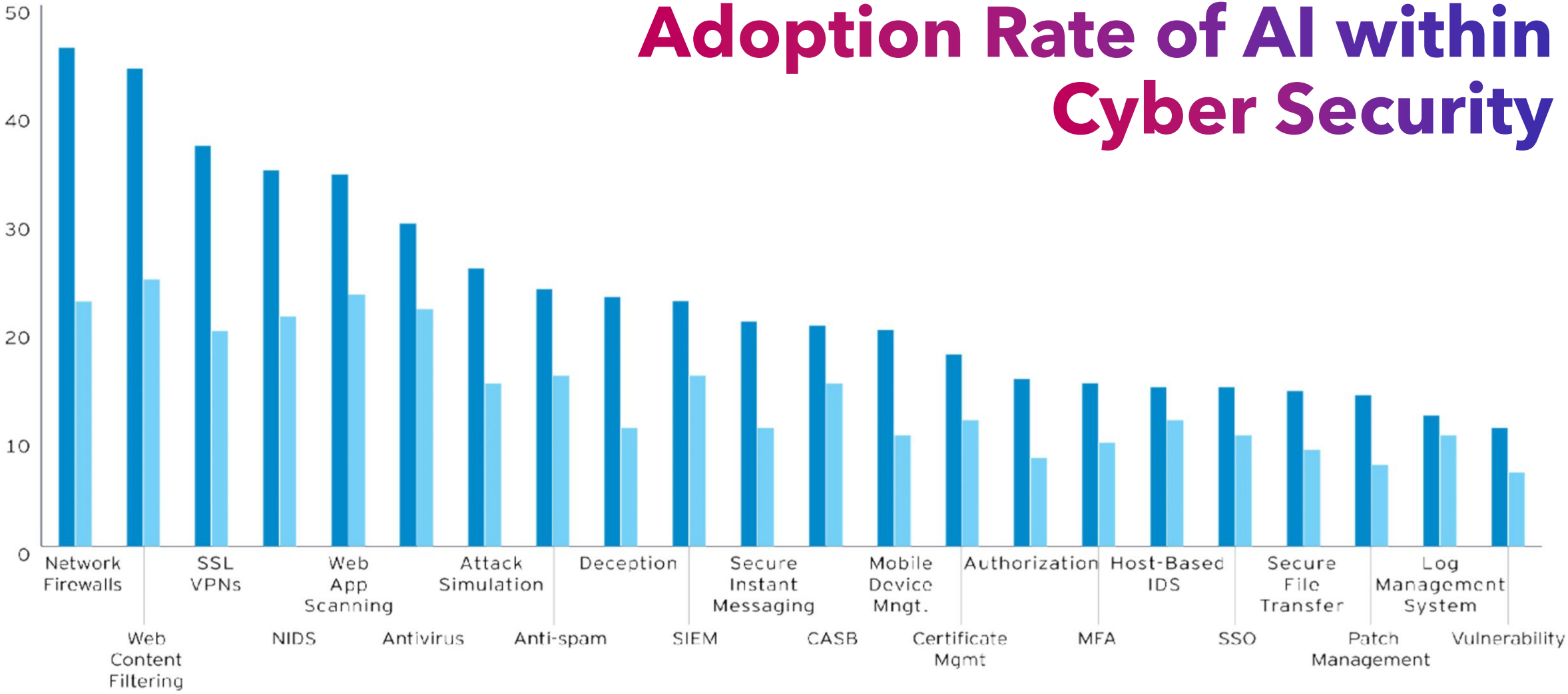
Up to 70% of cloud incidents are misconfigurations

Config Analysis and Copilot

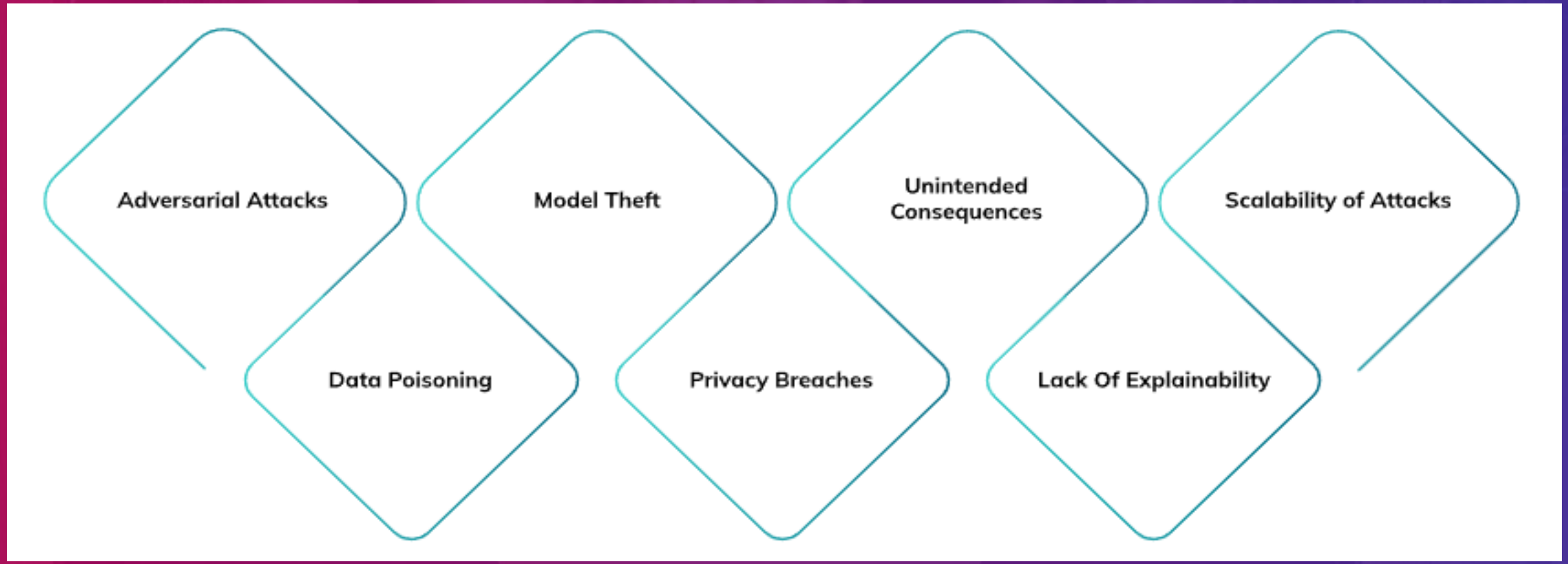
Requirements Generation

credits - NVidia

Adoption Rate of AI within Cyber Security

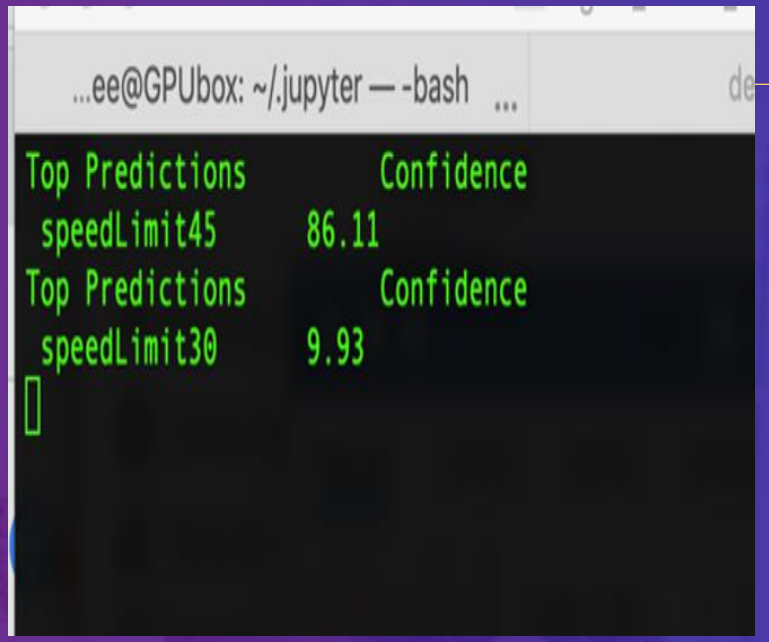


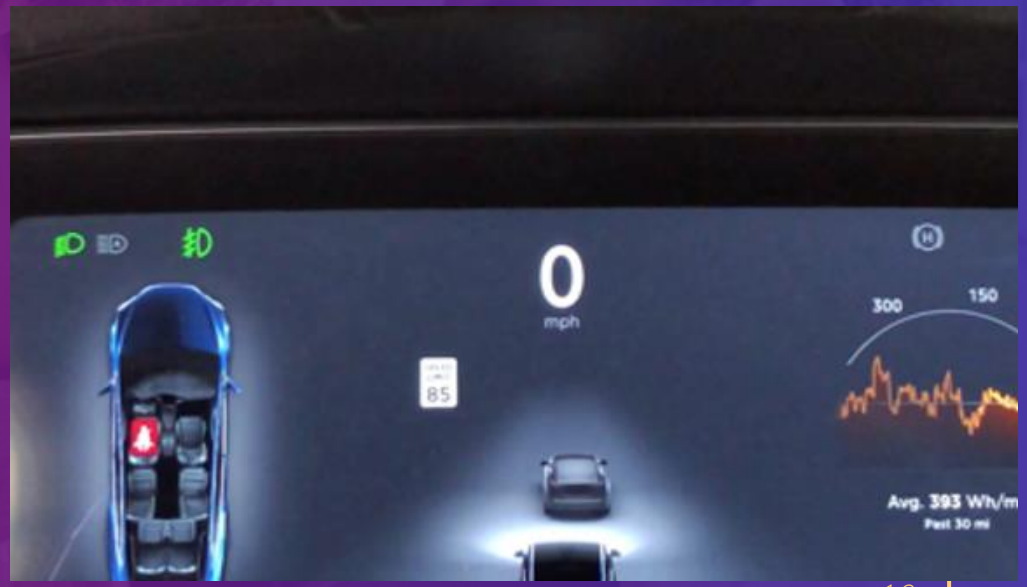
Key Cybersecurity Risks for AI



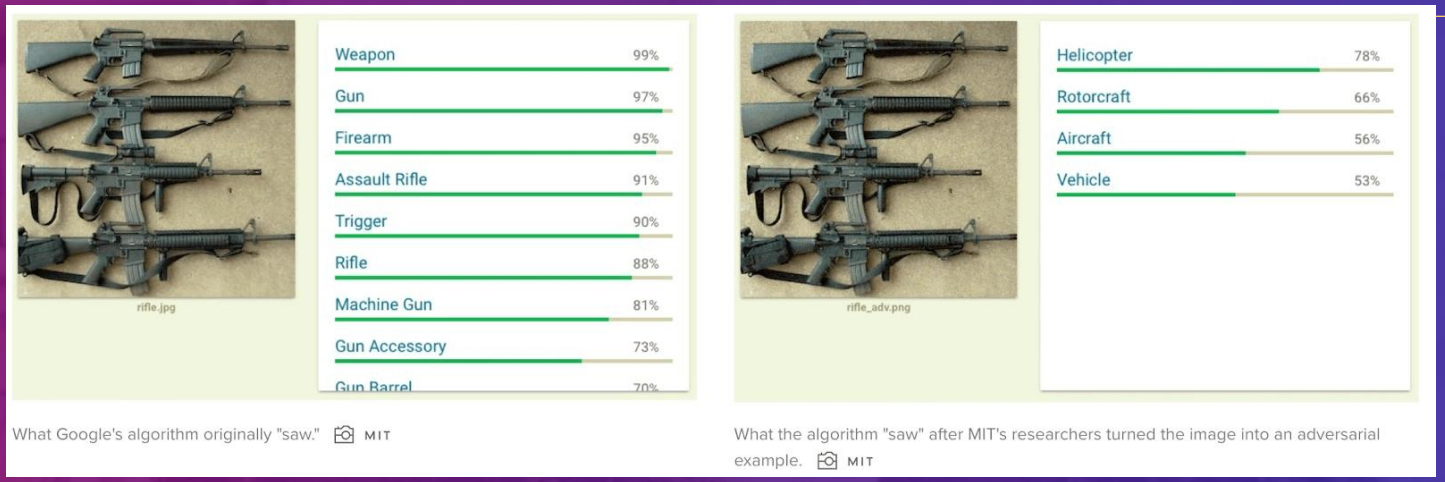
Tricking Tesla Model S

For example, conveniently placed stickers managed to trick a Tesla Model S into recognizing a stop sign as an "Added Lane" sign. In any traffic, that would most likely crash it. Also, stickers managed to trick its algorithm into seeing 85 instead of 35 on a speed limit sign. Check out the modified sign on the figure below!





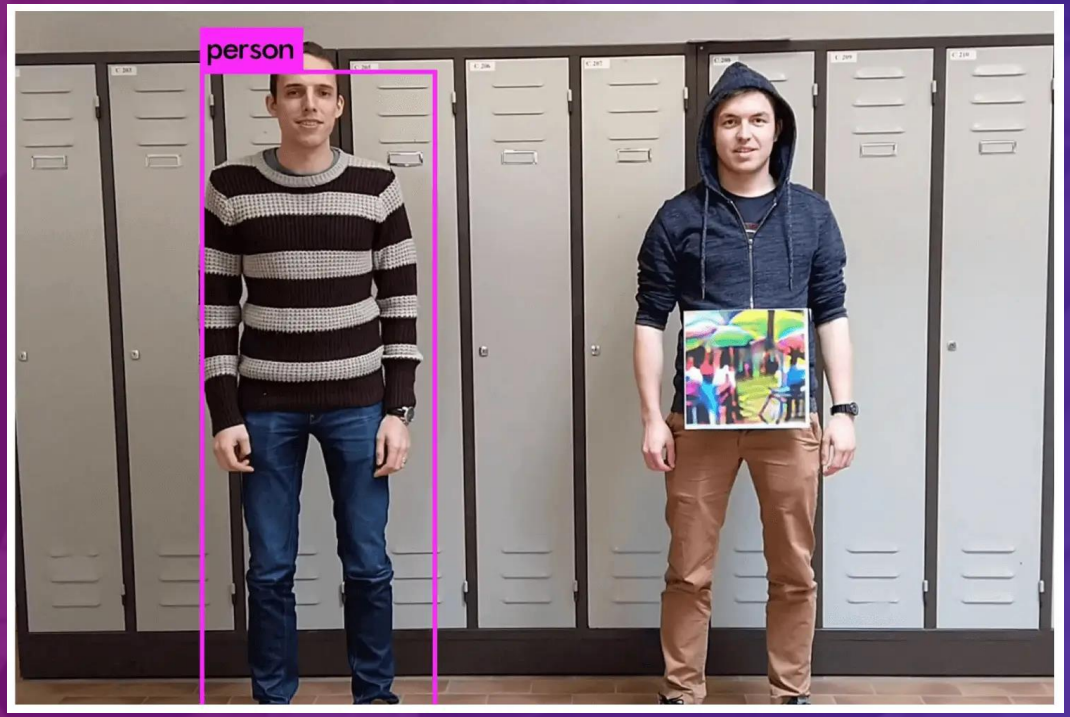
Video Surveillance Fails



What Google's algorithm originally "saw." MIT

What the algorithm "saw" after MIT's researchers turned the image into an adversarial example. MIT

In most cases, machine learning algorithms can be fooled by manipulating the underlying pixels of an image. These changes are invisible to humans, but they lead the algorithm astray. Take a look below to see how the methods can make AI see a helicopter on a photo with four automatic weapons

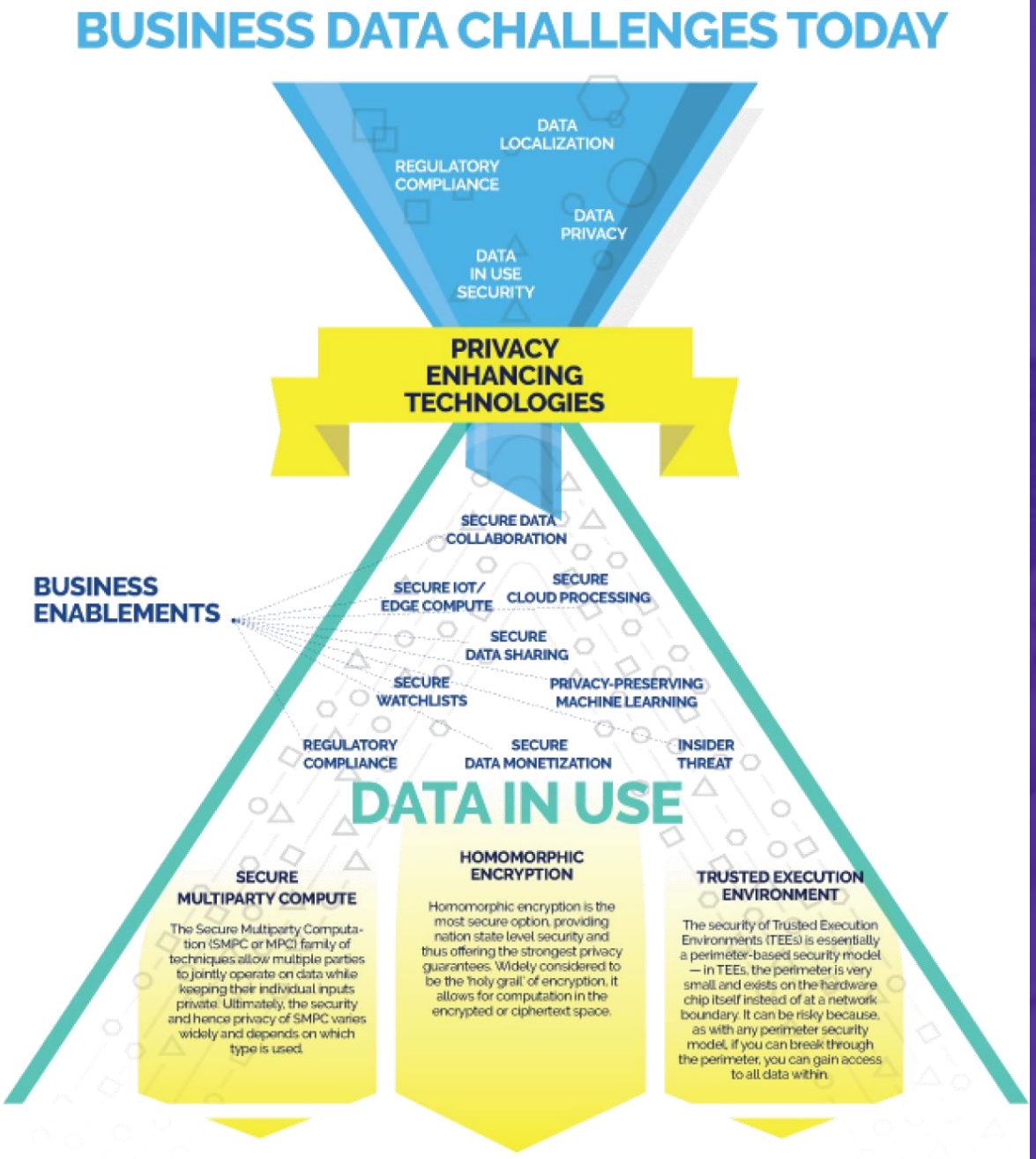


Live Demo

Let's fool an AI?

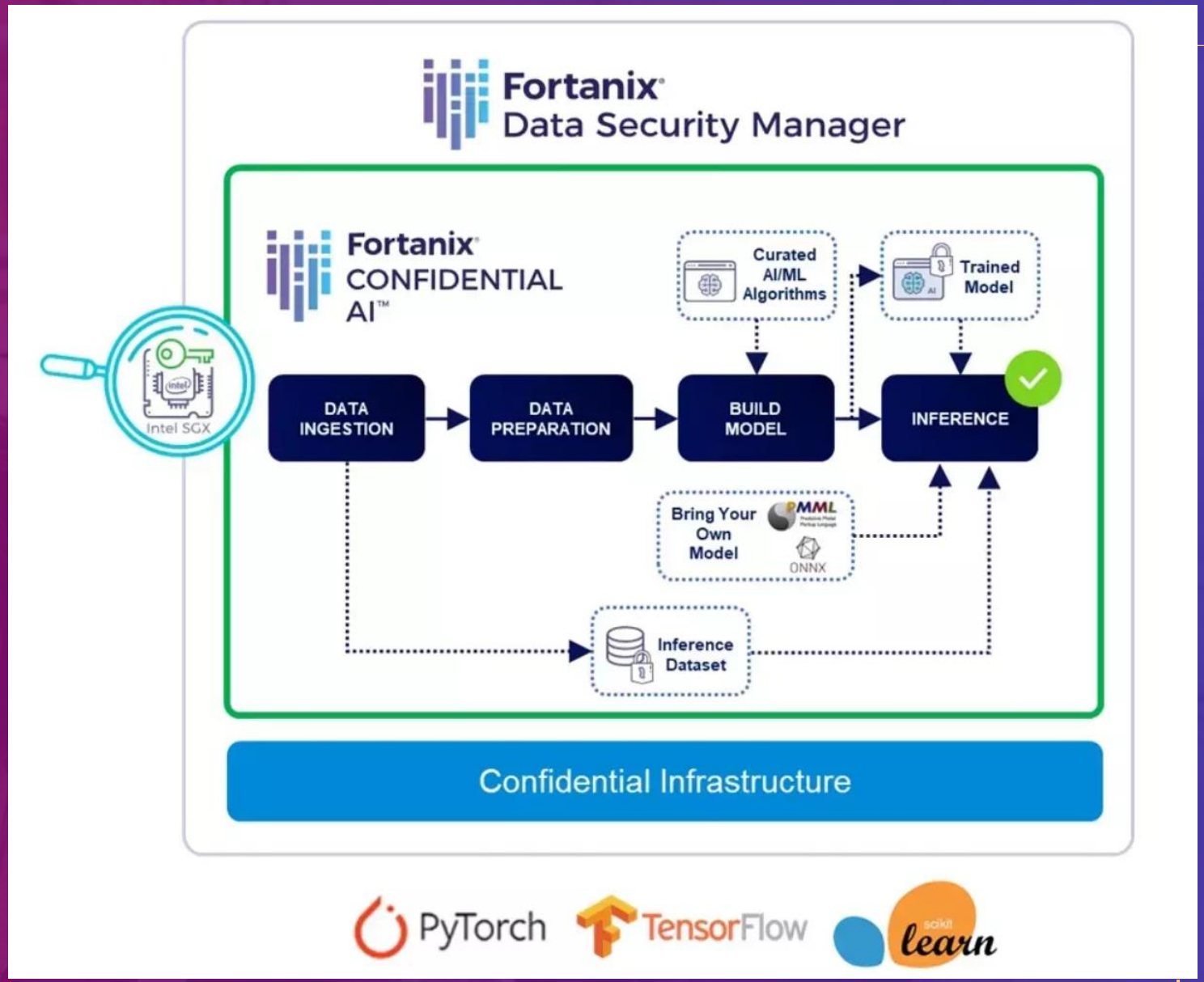
What are privacy-enhancing technologies (PETs)?

Privacy-enhancing technologies (PETs) are a broad range of technologies (hardware or software solutions) that are designed to extract data value in order to unleash its full commercial, scientific and social potential, without risking the privacy and security of this information.



Protecting Sensitive Data and AI Models

with Confidential Computing



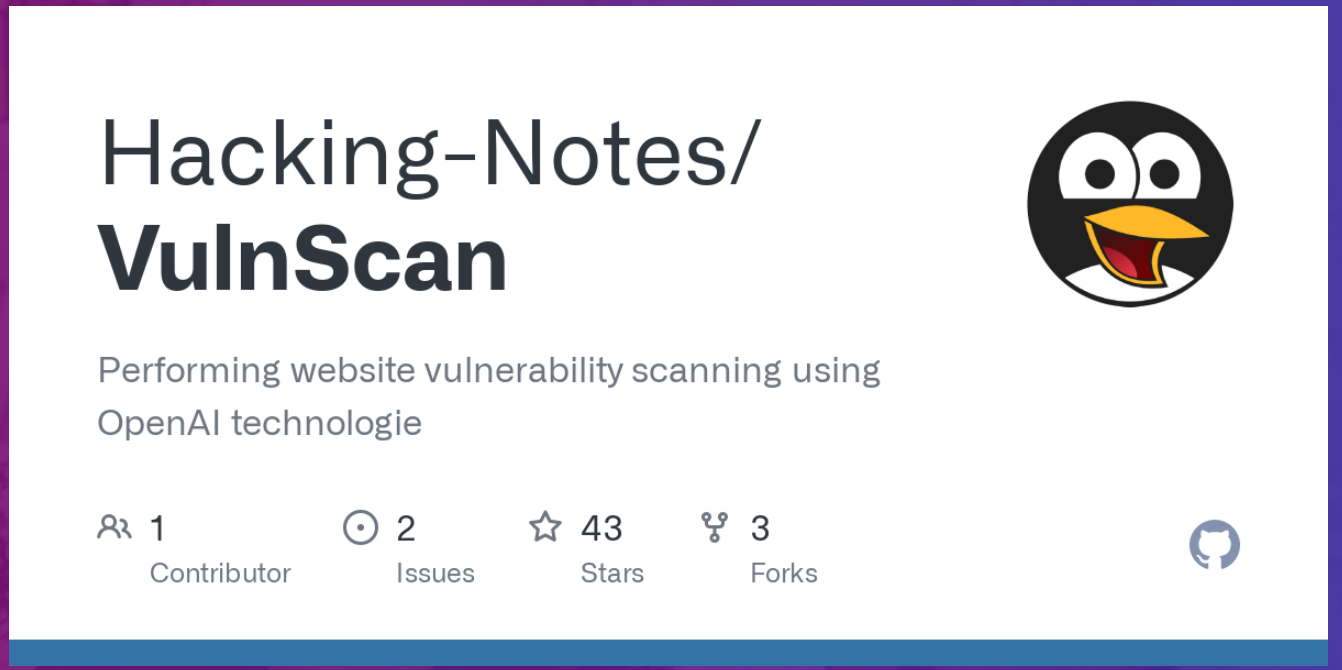
How do I hack using AI?

AI Powered Ethical Hacking Tools

https://github.com/beryllium sec/nebula

AI Powered Ethical Hacking Tools

https://github.com/Hacking-Notes/VulnScan

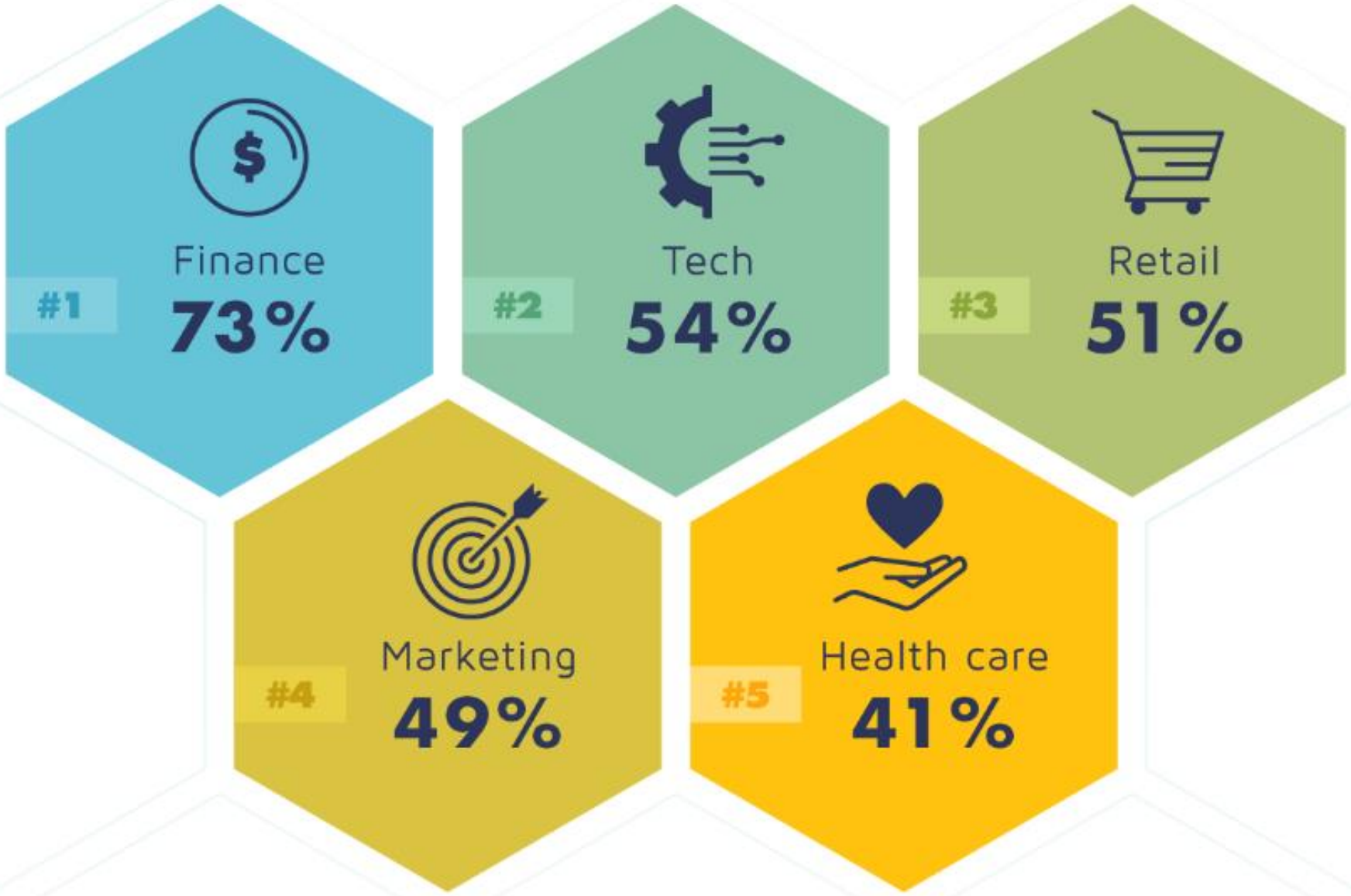


Future of AI in Cybersecurity

AI's future in cybersecurity is very exciting, with a lot of room for growth and new ideas. With more use cases and applications, AI's role in cybersecurity is likely to grow. One potential area where AI could be integrated with other technologies is blockchain and the Internet of Things (IoT).

As AI keeps getting more and more important in cybersecurity, there will be a growing need for people who know how to use AI in cybersecurity. These professionals will need to have a deep understanding of both cybersecurity and AI technologies.

Top 5 Industries Hiring for AI Cybersecurity Skills



FutureGPT

TY/Q&A

@REACHTONIKHIL

www.reachtonikhil.com