Project Management Institute. Southwest Ohio

Project Management Institute. Dayton/ Miami Valley Ohio

University of CINCINNATI
CARL H. LINDNER COLLEGE OF BUSINESS

#cincysummit24

AI: CYBERSECURITY FRIEND OR FOE?

DAVE HATTER
INTRUST IT

BUSINESS ACUMEN

Project Management Institute. Southwest Ohio

Project Management Institute. Dayton/ Miami Valley Ohio

University of CINCINNATI
CARL H. LINDNER COLLEGE OF BUSINESS

#cincysummit24

HOUSEKEEPING

EACH SESSION IS RECORDED

YOU WILL RECEIVE A LINK TO SLIDES AND THE RECORDING

Project Management Institute. Southwest Ohio

Project Management Institute. Dayton/ Miami Valley Ohio

University of CINCINNATI
CARL H. LINDNER COLLEGE OF BUSINESS

#cincysummit24

SPONSOR:

encore TECHNOLOGIES

AI: CYBERSECURITY FRIEND OR FOE?

Dave Hatter, CISSP, CISA, CISM, CCSP, CSSLP, PMP, ITIL

Cybersecurity Consultant
Intrust IT

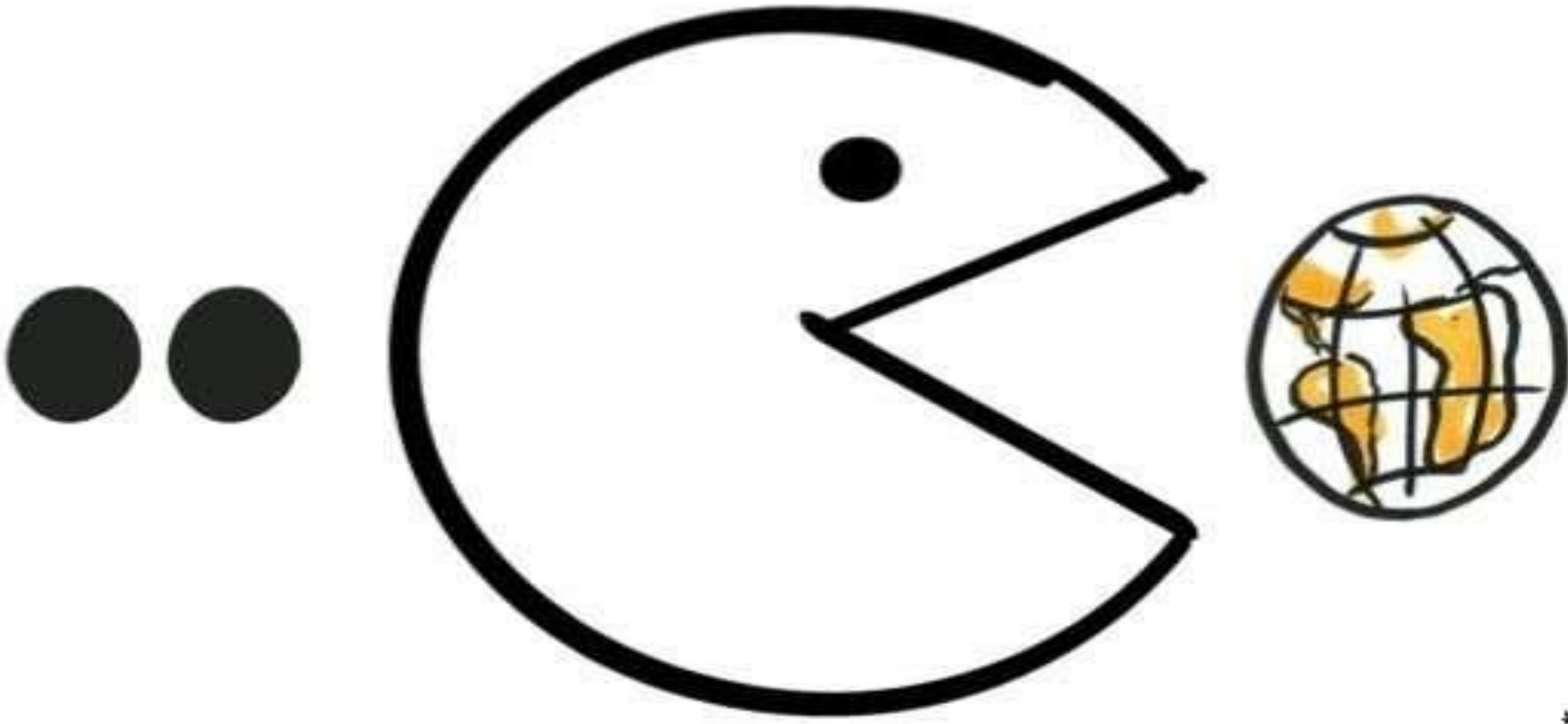
linkedin.com/in/davehatter
twitter.com/davehatter

Agenda

- SDE = cybercrime tsunami
- Disruption and Transformation
- Black Hat AI
- White Hat AI
- Navigating the Future
- Discussion and Q&A


Setting the
Table

Software is eating up the world*



* Marc Andreessen
in Wall Sreet Journal

Microsoft Start

Search the web

CrowdStrike outage reportedly cost over $5.4 billion for top companies alone

Forbes

FORBES > INNOVATION > CYBERSECURITY

Record-Breaking $75 Million Ransom Paid To Dark Angels Gang

TECH

Social Security Add Topic+

2.9 billion records, including Social Security numbers, stolen in data hack: What to know

POLITICO

CYBERSECURITY

The nation's best hackers found vulnerabilities in voting machines — but no time to fix them

Organizers and participants at the DEF CON Voting Village found cyber vulnerabilities in everything from voting machines to e-poll books, but there is no time before the November elections to fully implement their findings.

Cybercrime Expected To Skyrocket in the Coming Years

Estimated cost of cybercrime worldwide
(in trillion U.S. dollars)

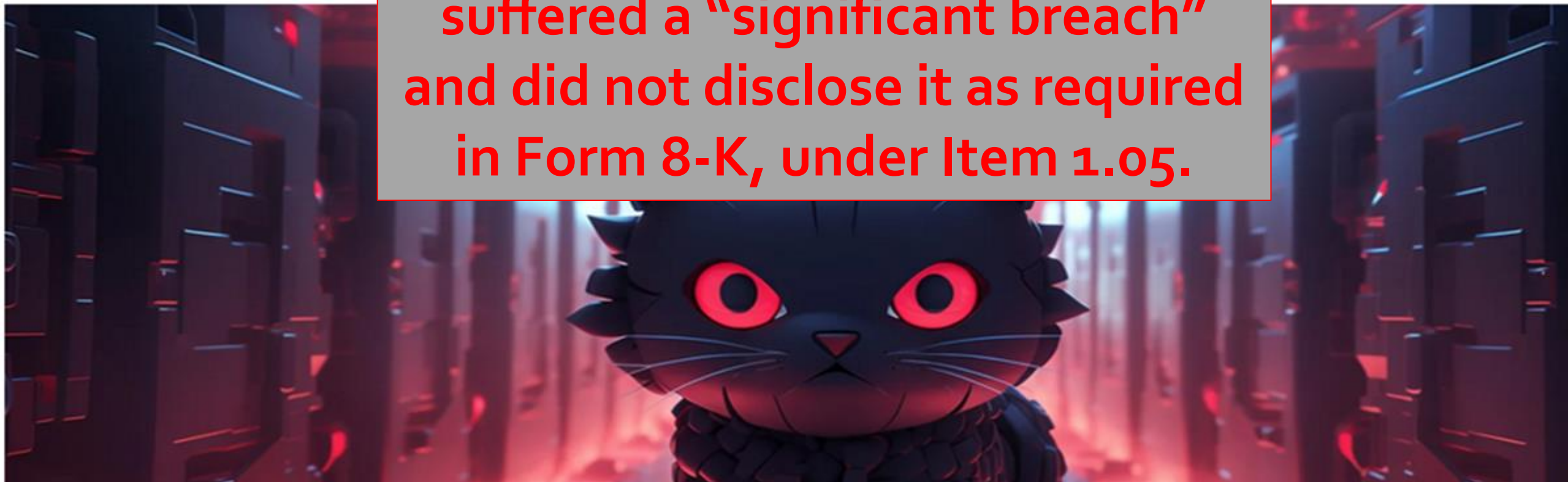
As of November 2022. Data shown is using current exchange rates.
Sources: Statista Technology Market Outlook,
National Cyber Security Organizations, FBI, IMF

Ransomware gang files SEC complaint over victim's undisclosed

By Ionut Ilascu

5, 2023 09:02 PM

In their own words, the attacker told the SEC that MeridianLink suffered a "significant breach" and did not disclose it as required in Form 8-K, under Item 1.05.



INTENT TO KILL | 4:50 PM *by* VICTOR TANGERMANN

Homeland Security Warns of Cyberattacks Intended to Kill People

"The attacks are increasing in frequency and gravity, and cybersecurity must be a priority for all of us."

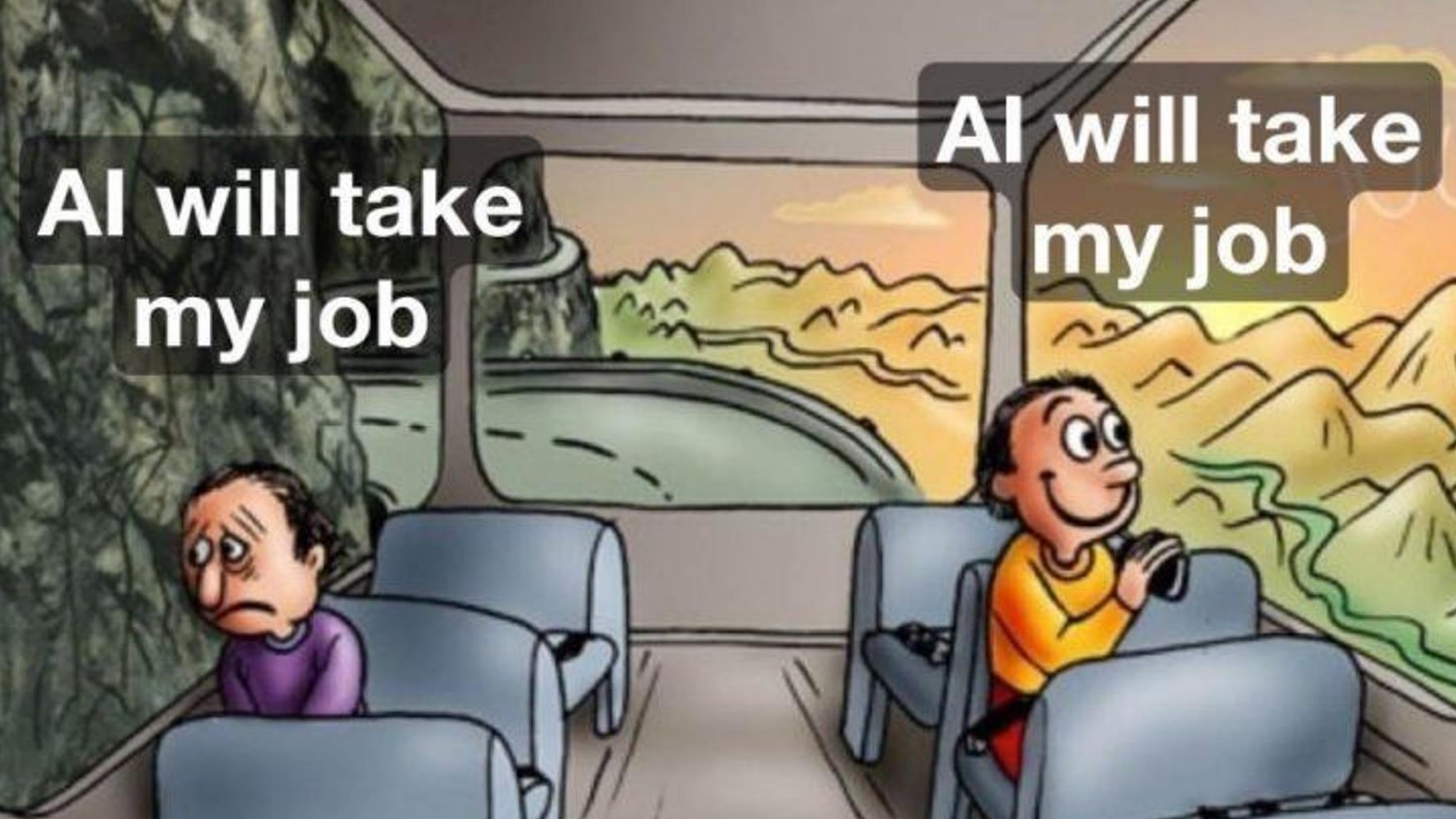
Cybersecurity Challenges

- Skills gap
- Alert fatigue
- Vast and growing attack surface
  - Remote work
  - IoT / ICS / SCADA / OT
- Growing attack sophistication
- Cloud shift
- 3rd Party Risk
- Shadow IT
- Massive data volume
- Compliance & privacy
- Insider threats

Never has a technology made us so excited and terrified at the same time

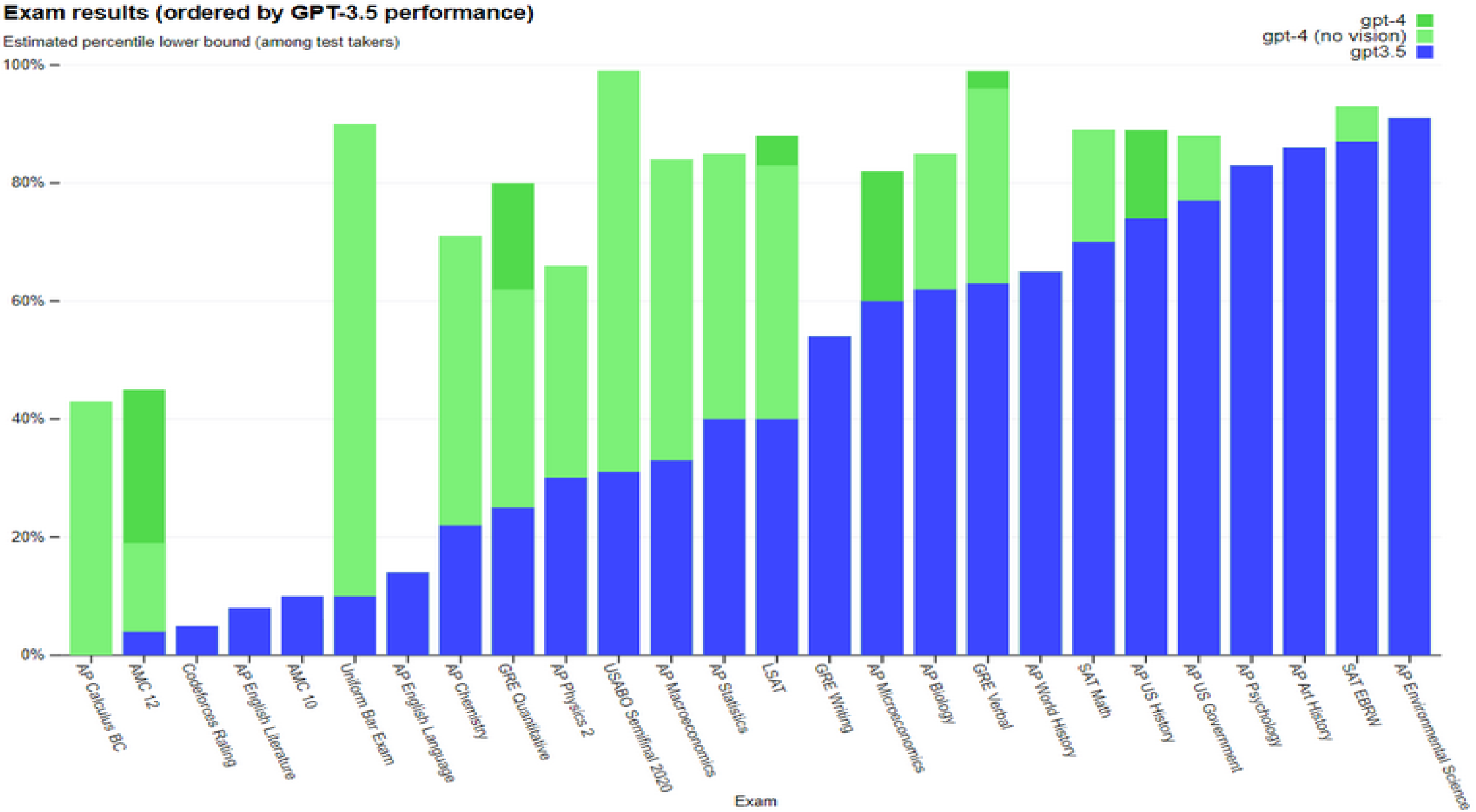
“Any sufficiently advanced technology is indistinguishable from magic.” – Arthur C. Clarke

“Machine intelligence is the last invention that humanity will ever need to make.” - Nick Bostrom

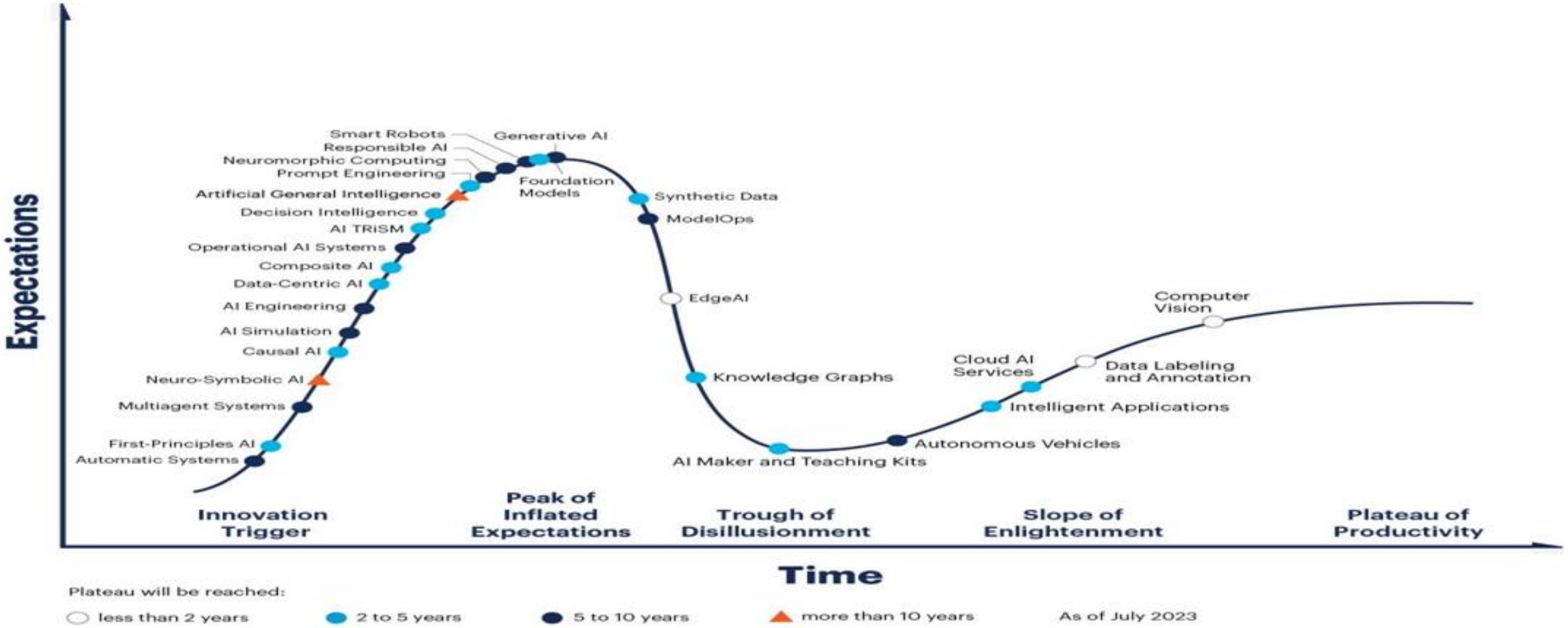

AI will take my job
AI will take my job

OCTOBER 30, 2023

Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence


Exam results (ordered by GPT-3.5 performance)
Estimated percentile lower bound (among test takers)
gpt-4
gpt-4 (no vision)
gpt3.5
100%
80%
60%
40%
20%
0%
AP Calculus BC
AMC 12
Codeforces Rating
AP English Literature
AMC 10
Uniform Bar Exam
AP English Language
AP Chemistry
GRE Quantitative
AP Physics 2
USABO Semifinal 2020
AP Macroeconomics
AP Statistics
LSAT
GRE Writing
AP Microeconomics
AP Biology
GRE Verbal
AP World History
SAT Math
AP US History
AP US Government
AP Psychology
AP Art History
SAT EBRW
AP Environmental Science
Exam

Hype Cycle for Artificial Intelligence, 2023



Source: Gartner

Gartner

New Security Challenges

- AI-driven Attacks
- AI-driven Social engineering
- AI adoption

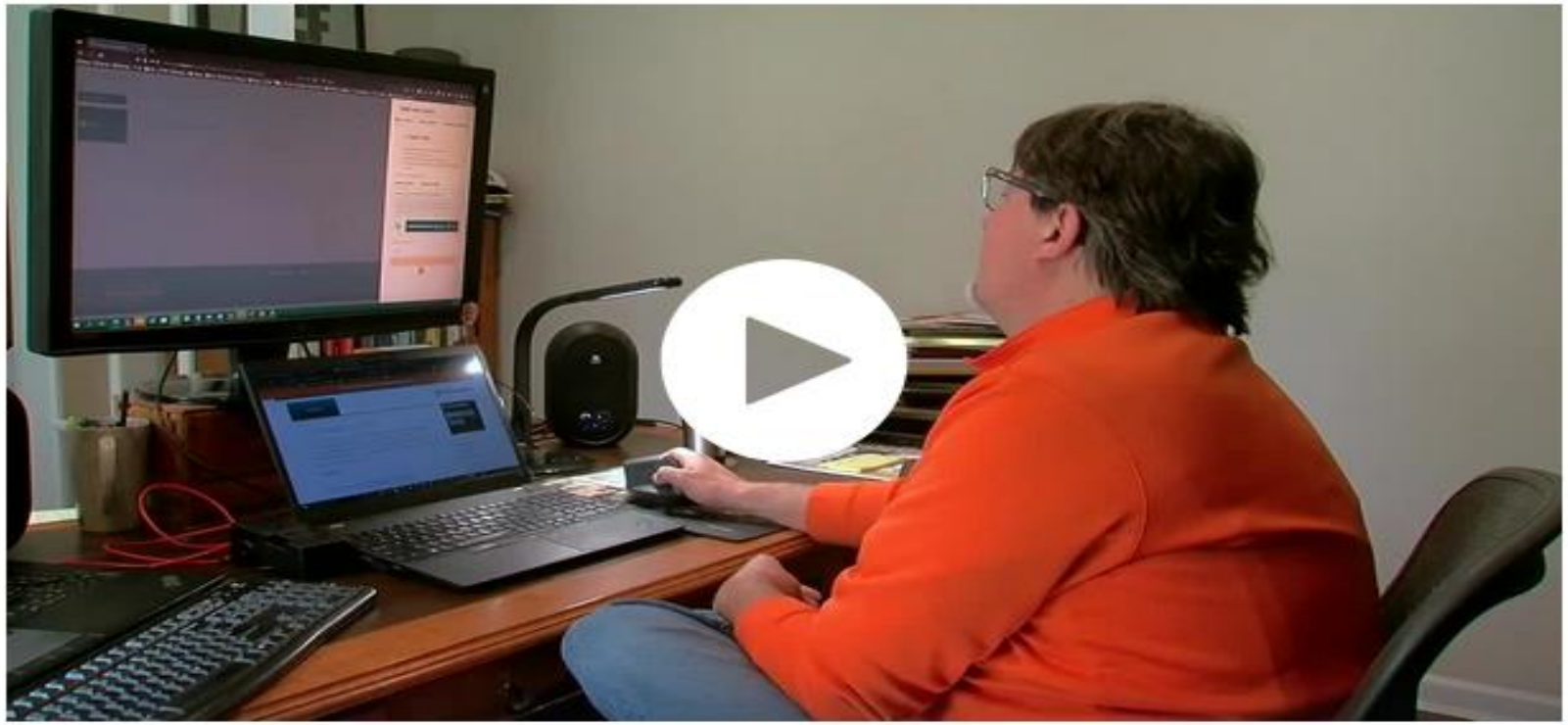
Figure 1: ENISA Threat Landscape 2022 - Prime threats

Black Hat AI

- Social Engineering Attacks
- Automated Hacking
- Password Cracking
- Evasion of Detection Systems
- Targeted Malware Creation
- Data Poisoning
- Exploiting AI Systems

Listen how AI can clone your voice, use it in phishing scams

Reporter's words recorded, then turned into the "Grandparent scam"



Scammers can now use AI to clone your voice, then make scam phishing phone calls to relatives. We find out how easily it can be done, and what it sounds like.

Don't Waste Your Money

Exploiting AI Systems

- Adversarial attacks
- Data poisoning
- Prompt injection
- Backdoor attacks on AI models

Cybersecurity Evolution

- Rule based tools
- Machine learning
- Deep learning / AI

AI-Driven Tools

- Sentinel One
- MS Security Copilot
- Cisco Stealthwatch
- Palo Alto Networks WildFire
- Splunk
- IBM Watson for Cyber Security
- Nessus

White Hat AI

- Network Protection
- Endpoint protection
- Application security
- Anomalous user behavior
- Automation
- Testing
- Simulating attacks

White Hat AI

- Enhanced EPP/MDR
- Security Information and Event Management (SIEM)
- Phishing Detection and Prevention
- Threat Detection and Analysis
- Behavioral Analytics
- Vulnerability Management

White Hat AI

- Predictive Threat Intelligence
- Automated Incident Response
- Identity and Access Management (IAM)
- User Training
- Content Generation
- Chatbots for Security Assistance

Identify

Timestamp	User	Action	Description
11/14/2023 12:40	user_1	LOGIN_FAILURE	Generic action
11/14/2023 12:40	user_8	LOGIN_FAILURE	Generic action
11/14/2023 12:40	privileged_user	PRIVILEGED_LOGIN	Privileged user logs in
11/14/2023 12:40	privileged_user	COPY_SENSITIVE_CONTENT	Files copied
11/14/2023 12:40	privileged_user	PRIVILEGED_LOGOUT	Privileged user logs out
11/14/2023 12:40	user_8	LOGIN_FAILURE	Generic action
11/14/2023 12:40	privileged_user	ACCOUNT_DELETION	Privileged user account is deleted
11/14/2023 12:40	user_4	PASSWORD_CHANGE	Generic action
11/14/2023 12:40	user_8	LOGIN_FAILURE	Generic action

ML

AI Benefits

- Real-time Response
- Reduced False Positives
- Automated Incident Response
- Advanced Threat Detection (Zero Day)
- Predictive Security

AI Benefits

- Natural language
- Breach attack simulation (BAS)
- Cost Savings
- Continuous Learning
- Scalability

AI Benefits

In a recent study to measure the productivity impact for "new in career" analysts, participants using Security Copilot demonstrated **44 percent more accurate responses and were 26 percent faster across all tasks.**[3]

According to the same study:

- **86 percent** reported that Security Copilot helped them improve the quality of their work.
- **83 percent** stated that Security Copilot reduced the effort needed to complete the task.
- **86 percent** said that Security Copilot made them more productive.
- **90 percent** expressed their desire to use Security Copilot next time they do the same task.

99%

Basic security hygiene protects against 99% of attacks

Enable multifactor authentication (MFA)

Apply Zero Trust principles

Use extended detection and response (XDR) and antimalware

Keep up to date

Protect data

← Outlier attacks on the bell curve make up just 1% →

Figure 1—Evolution of the SOC

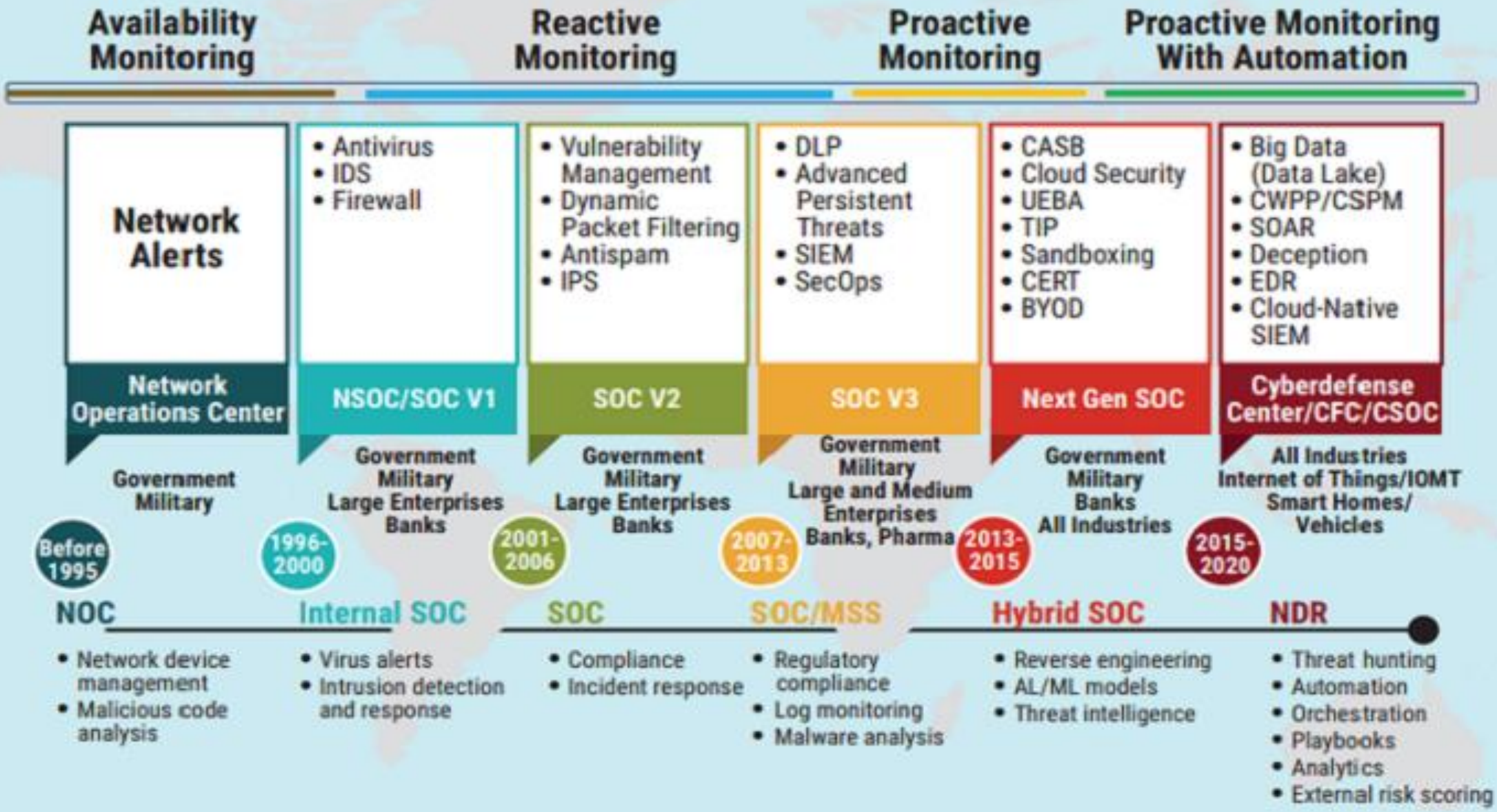
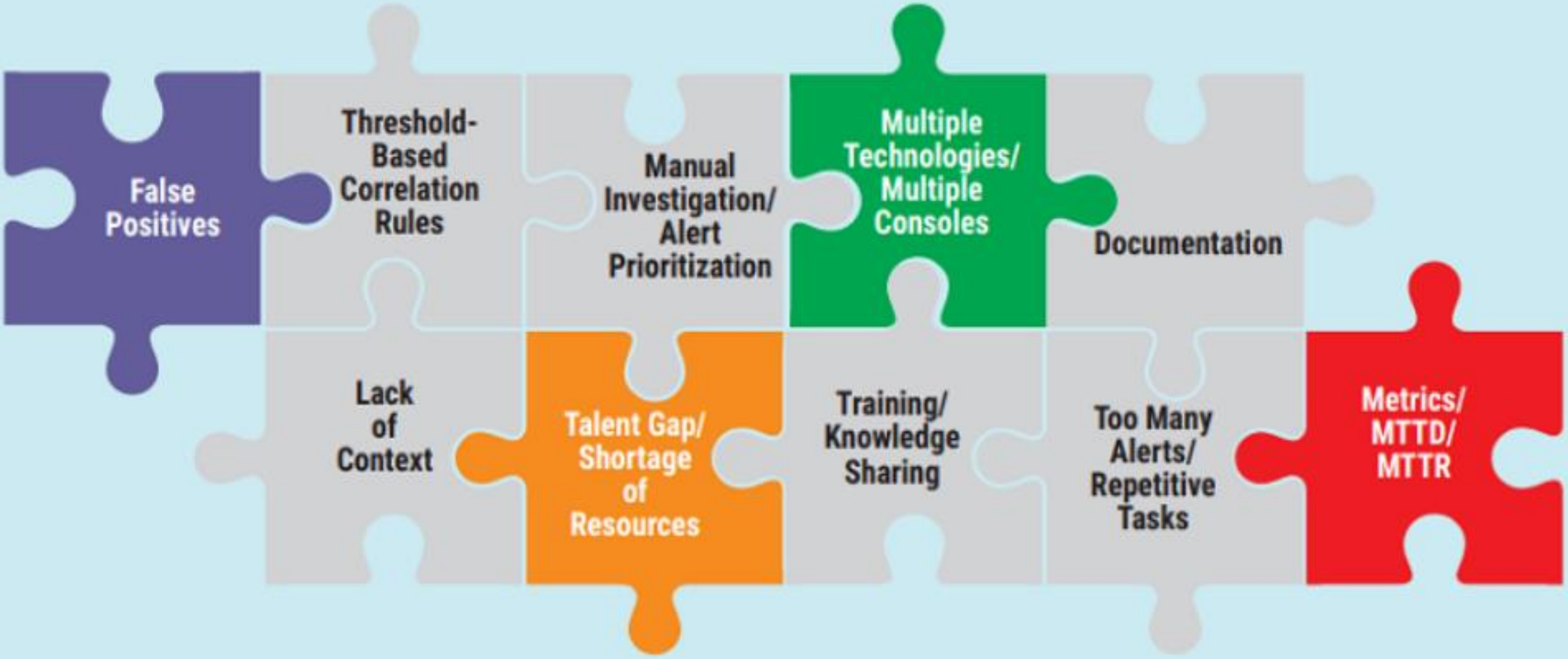
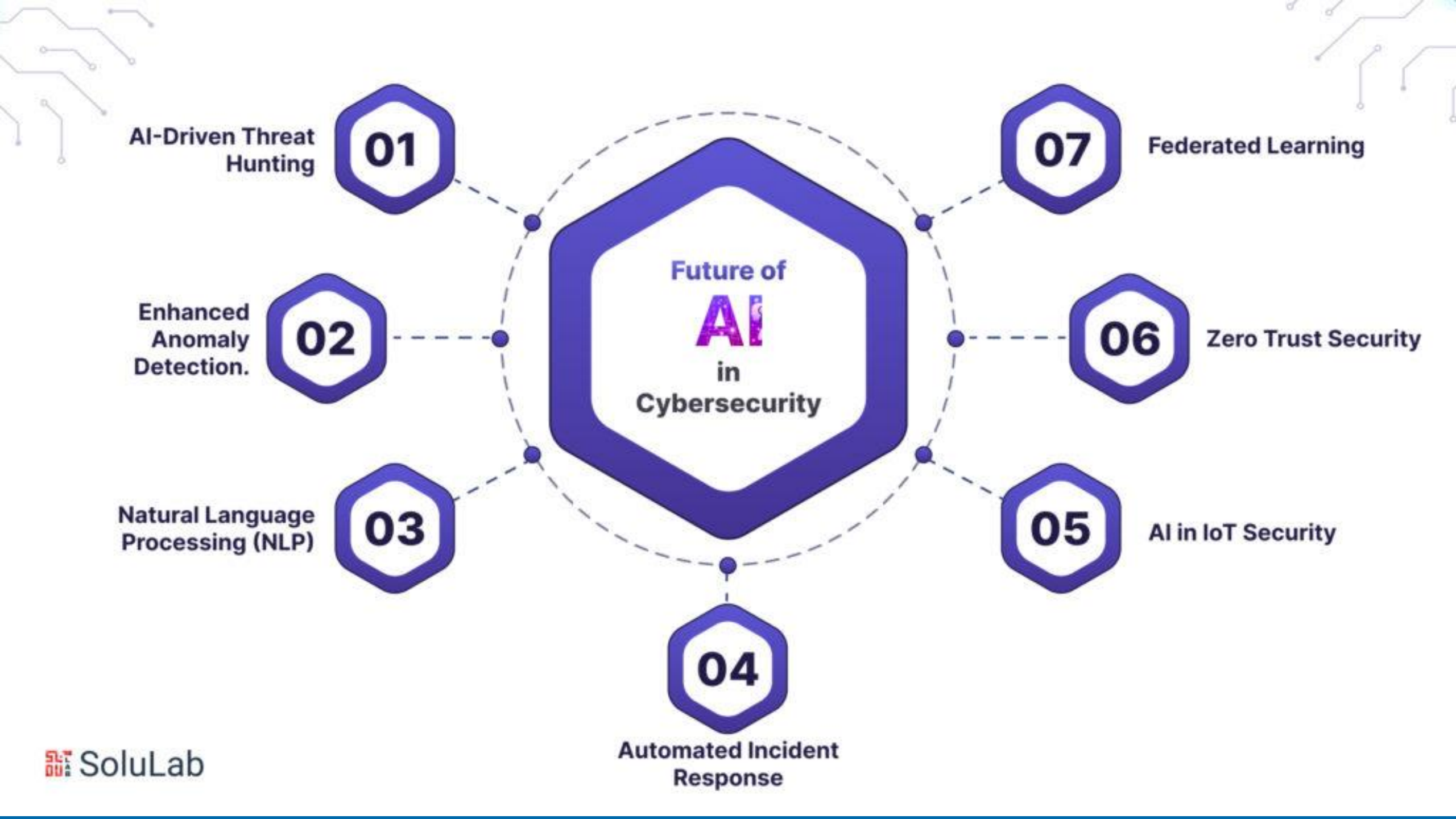


Figure 2—SOC Challenges



AI Concerns

- False Positives and Negatives
- Model Bias
- Lack of Transparency
- Complexity
- Ethics
- Resources
- Regulatory and Compliance Issues


Future of
AI
in
Cybersecurity
01
AI-Driven Threat Hunting
02
Enhanced Anomaly Detection.
03
Natural Language Processing (NLP)
04
Automated Incident Response
05
AI in IoT Security
06
Zero Trust Security
07
Federated Learning

SoluLab

AI Future

- The genie is out of the bottle
- Tools are readily available to bad actors
- Attacks will increase in:
  - Speed
  - Quality
  - Sophistication

AI Future

- AI can’t replace human security professionals
  - Enhances their work
  - Fills skills and resource gaps
  - Speeds detection and mitigation
  - Augments capabilities
  - Leads to more job satisfaction
  - Focus on key gaps first
- Ask questions like:
  - Will your tools id and block what's new?
  - Will you help us meet compliance needs?
  - What signals success in your AI platform?

Additional Resources

- https://www.nist.gov/artificial-intelligence/executive-order-safe-secure-and-trustworthy-artificial-intelligence
- https://www.cisa.gov/sites/default/files/2023-11/2023-2024_CISA-Roadmap-for-AI_508c.pdf
- https://www.nist.gov/itl/ai-risk-management-framework
- https://www.nist.gov/artificial-intelligence/artificial-intelligence-safety-institute
- https://ai.gov/naiac/
- https://www.cisa.gov/news-events/news/dhs-cybersecurity-and-infrastructure-security-agency-releases-roadmap-artificial-intelligence
- https://www.cisa.gov/resources-tools/resources/roadmap-ai
- https://www.isaca.org/resources/artificial-intelligence
- https://www.nist.gov/cyberframework
- https://chat.openai.com/chat

For more information:

- Bruce Schneier:@schneierblog
- US-CERT: @USCERT_gov
- SecurityWeek: @SecurityWeek
- Center for Internet Security: @CISecurity
- MSRC: @msftsecresponse
- NIST Cyber: @NISTcyber
- Intrust IT: @IntrustIT
- CISA: CISAgov
- MSRC: @msftsecresponse
- Microsoft Secure: @msftsecurity
- RSA: @RSAsecurity
- Mikko Hypponen: @mikko
- CSOnline: @CSOonline
- Me: @DaveHatter


WE ARE NO LONGER
SECURING COMPUTERS
WE ARE SECURING SOCIETY.

Q & A

"Cybersecurity is national security"
- NSA Director General Paul Nakasone

intrust IT

THANK YOU!

Dave Hatter, CISSP, CISA, CISM, CCSP, CSSLP, PMP, ITIL

linkedin.com/in/davehatter | twitter.com/davehatter

Get our checklist:
https://www.intrust-it.com/cyber-security/cyber-essentials-checklist/

Ask about our no-cost, no-obligation vulnerability assessment

Catch Tech Friday live on 55KRC at 6:30 AM every Friday on 550 AM or http://55krc.iheart.com

Catch Cyber Monday live on WTVG at 6:30 AM and Tech Support at 9:00AM every Monday on 13 ABC or https://www.13abc.com/

Project Management Institute. Southwest Ohio

Project Management Institute. Dayton/ Miami Valley Ohio

University of CINCINNATI
CARL H. LINDNER COLLEGE OF BUSINESS

#cincysummit24

UP NEXT:

TRACK 1: WAYS OF WORKING, RM 1410

BU8ILDING A WINNING SOLUTION: DESIGNING A TECHNOLOY REFRESH PROJECT
-DAVID GROTE

TRACK 2: AI FOR TODAY/TOMORROW, RM 3240

A CEO'S PERSPECTIVE ON AI AND VIRTUAL TEAMS
-ALEX YASTREBENETSKY

TRACK 3: PEOPLE, PROCESS, TECHNOLOGY, RM 3265

CI+AI: THE NEW FORMULA LEVERAGIN AI TO CONINUOUS IMPROVEMENT
-STEVEN JONES

SUMMIT 2024 SURVEY

PDU ID: CO43T542S
PDU TYPE: BUSINESS ACUMEN
GO TO PMI.ORG FOR SUBMISSION