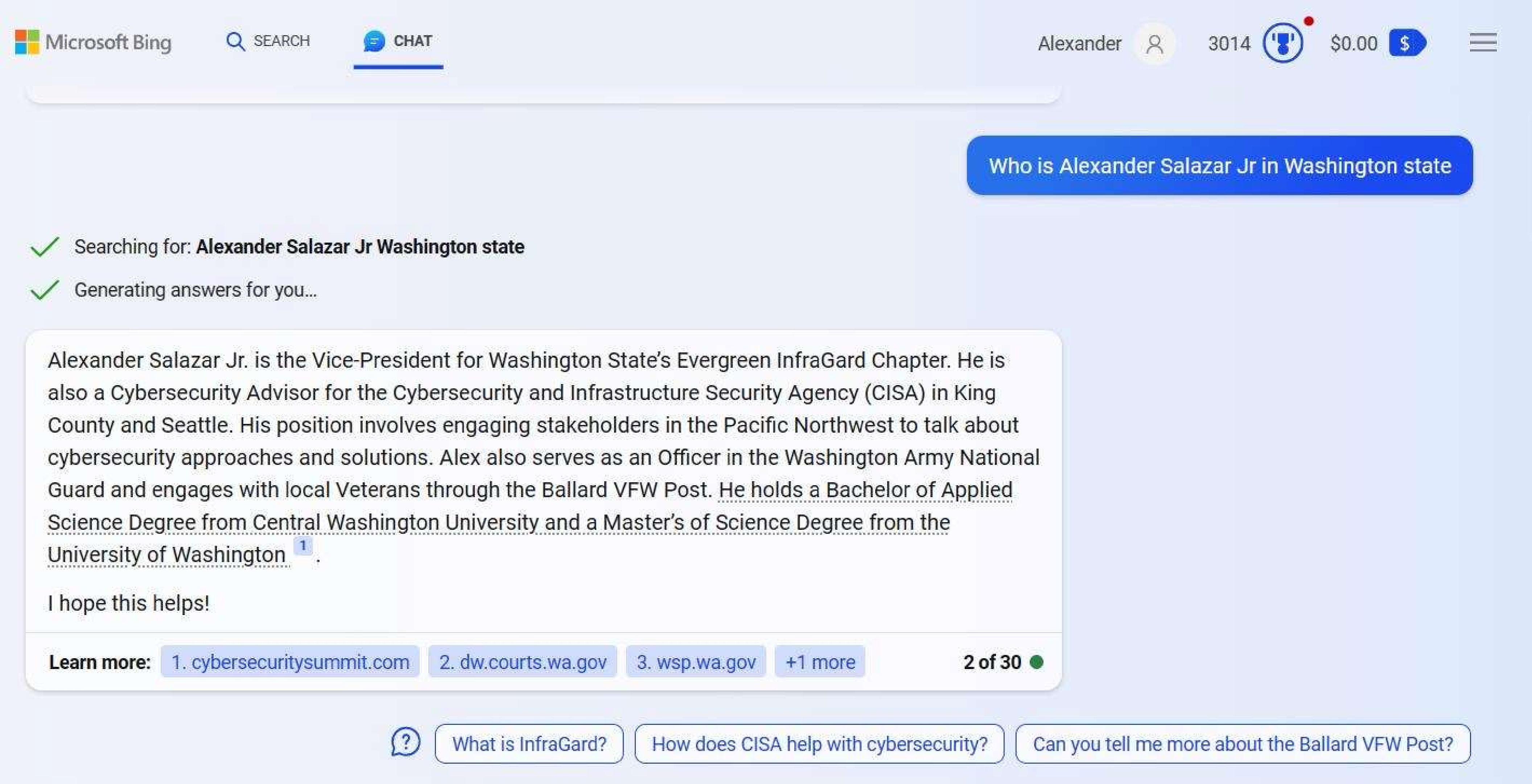
ARTIFICIAL INTELLIGENCE: What is it & what does it mean for Cybersecurity?

Alexander Salazar Jr, MSc, CISSP
Cybersecurity Advisor
CISA Region 10, Seattle & King County

Who is Alexander Salazar?



Who is Alexander Salazar Jr in Washington state

✓ Searching for: **Alexander Salazar Jr Washington state**

✓ Generating answers for you…

Alexander Salazar Jr. is the Vice-President for Washington State's Evergreen InfraGard Chapter. He is also a Cybersecurity Advisor for the Cybersecurity and Infrastructure Security Agency (CISA) in King County and Seattle. His position involves engaging stakeholders in the Pacific Northwest to talk about cybersecurity approaches and solutions. Alex also serves as an Officer in the Washington Army National Guard and engages with local Veterans through the Ballard VFW Post. He holds a Bachelor of Applied Science Degree from Central Washington University and a Master's of Science Degree from the University of Washington [1].

I hope this helps!

Learn more: 1. cybersecuritysummit.com 2. dw.courts.wa.gov 3. wsp.wa.gov +1 more **2 of 30** ●

What is InfraGard?
How does CISA help with cybersecurity?
Can you tell me more about the Ballard VFW Post?

Agenda

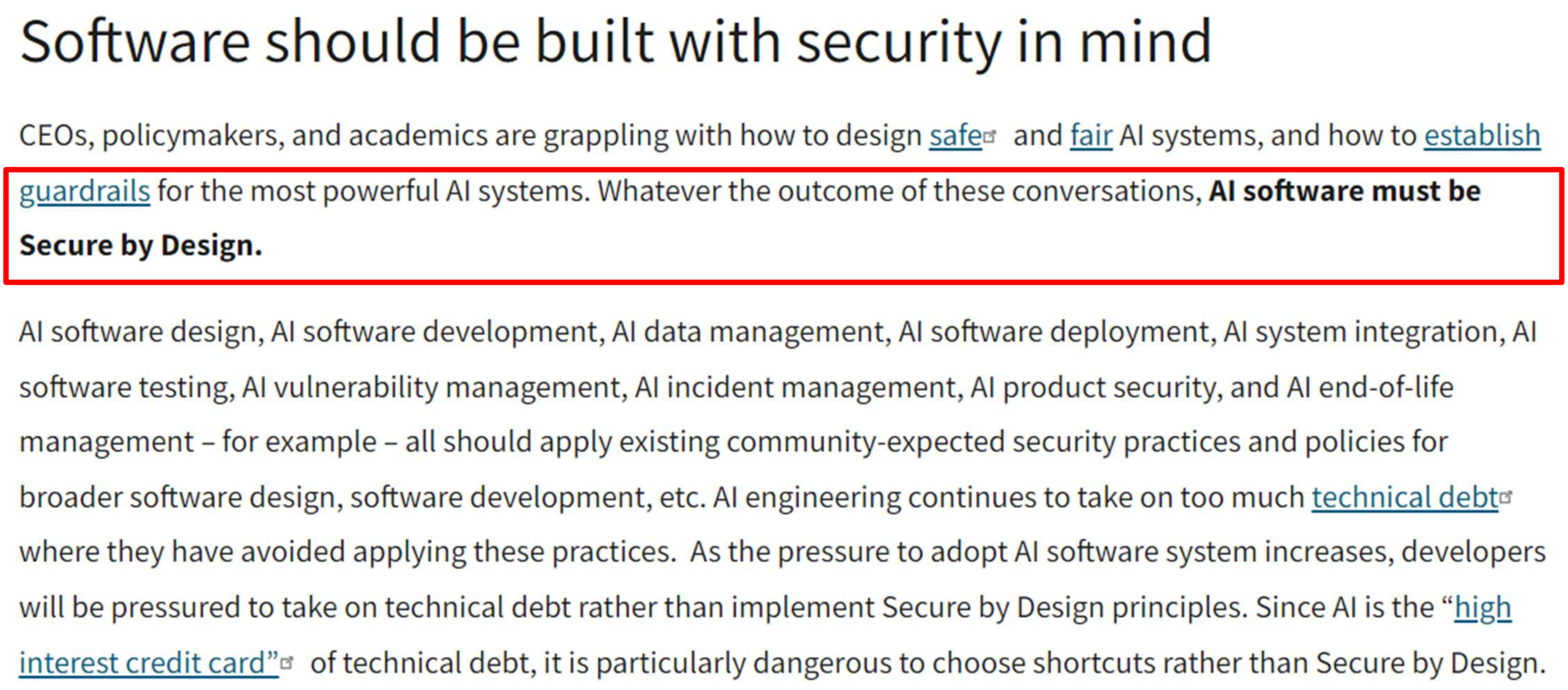
First:

- Artificial Intelligence (AI) vs. Machine Learning (ML)
  - AI is not new.
- How does AI learn?
  - Examples of its application.

Then:

- The Good
- The Bad

CISA Official Statements



Software should be built with security in mind

CEOs, policymakers, and academics are grappling with how to design safe and fair AI systems, and how to establish guardrails for the most powerful AI systems. Whatever the outcome of these conversations, **AI software must be Secure by Design.**

AI software design, AI software development, AI data management, AI software deployment, AI system integration, AI software testing, AI vulnerability management, AI incident management, AI product security, and AI end-of-life management – for example – all should apply existing community-expected security practices and policies for broader software design, software development, etc. AI engineering continues to take on too much technical debt where they have avoided applying these practices. As the pressure to adopt AI software system increases, developers will be pressured to take on technical debt rather than implement Secure by Design principles. Since AI is the "high interest credit card" of technical debt, it is particularly dangerous to choose shortcuts rather than Secure by Design.

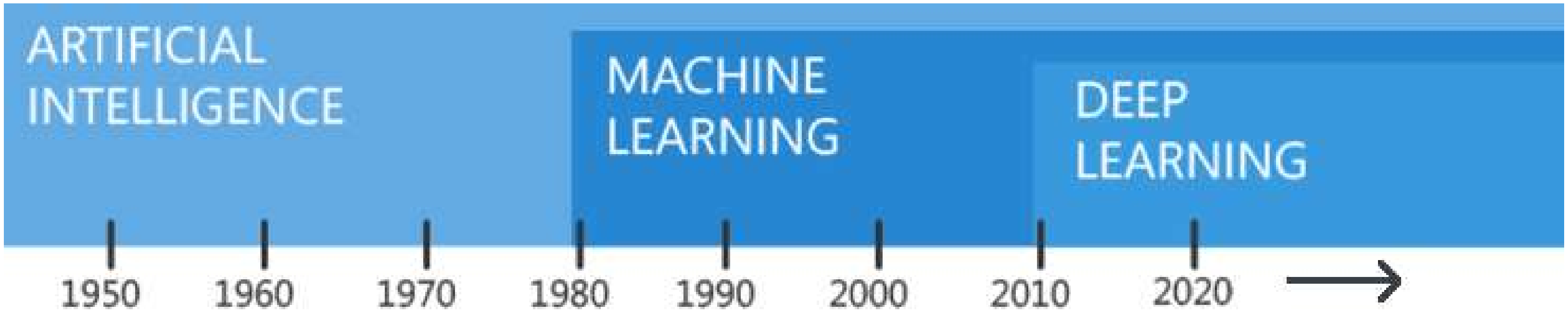
Source: https://www.cisa.gov/news-events/news/software-must-be-secure-design-and-artificial-intelligence-no-exception

IMPORTANT: Work-In-Progress

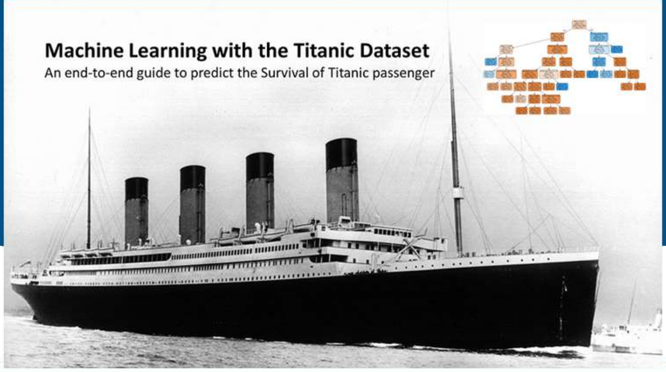
AI vs. ML

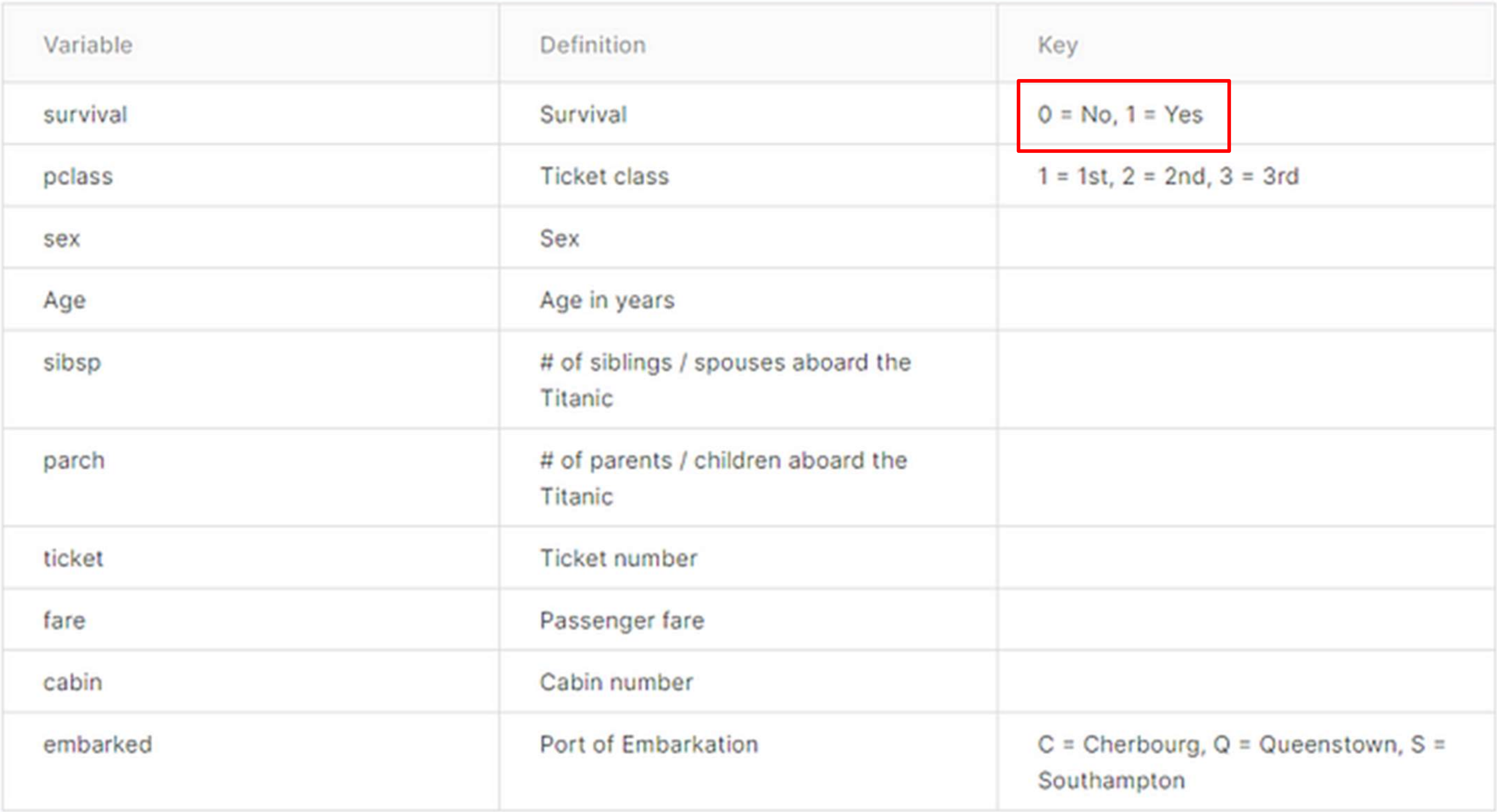
Important Clarification!

- Artificial Intelligence makes use of…
  - Machine Learning makes use of…
    - Deep Learning makes use of…
      - Data



Data


Machine Learning with the Titanic Dataset
An end-to-end guide to predict the Survival of Titanic passenger



Variable	Definition	Key
survival	Survival	0 = No, 1 = Yes
pclass	Ticket class	1 = 1st, 2 = 2nd, 3 = 3rd
sex	Sex	
Age	Age in years	
sibsp	# of siblings / spouses aboard the Titanic	
parch	# of parents / children aboard the Titanic	
ticket	Ticket number	
fare	Passenger fare	
cabin	Cabin number	
embarked	Port of Embarkation	C = Cherbourg, Q = Queenstown, S = Southampton

AI Applications

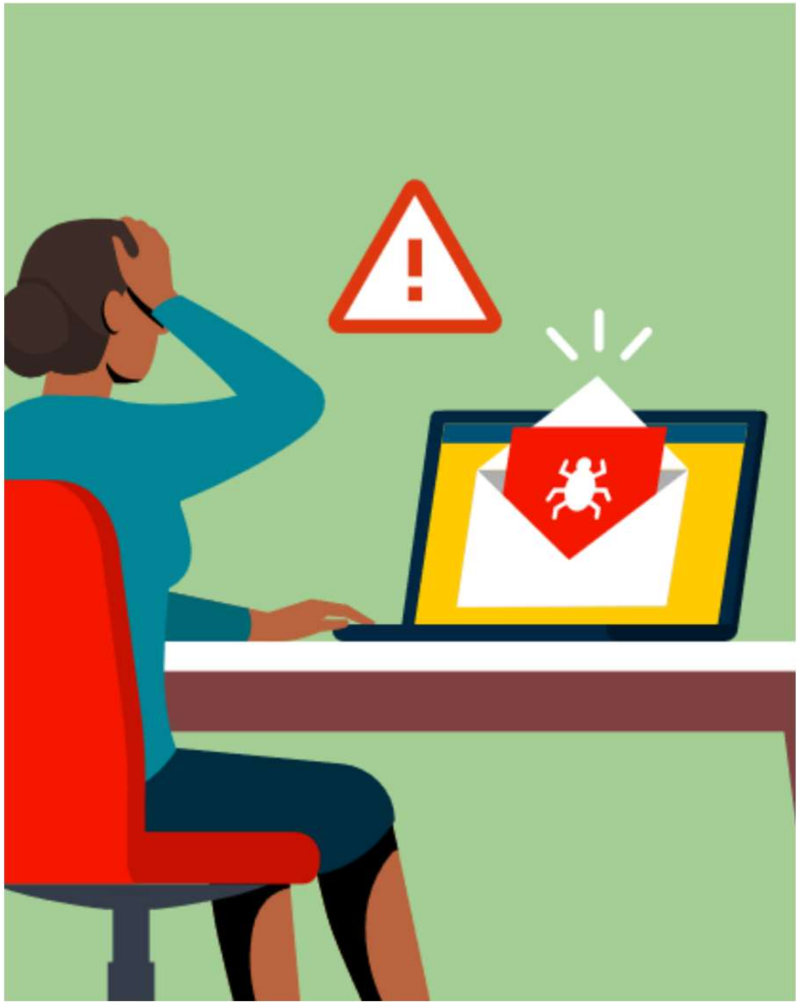
- What is real-time learning?
- Application examples:
  - ChatGPT (OpenAI)
  - Bing Chat (Microsoft)
  - Bard (Google)
- What is GPT?
  - What is an LLM?

The Good, The Bad, and…The Rest

- Phishing
  - Translation and Grammar
- Education/Skills
- Vulnerability information

Phishing (bad)

- Look for bad grammar! Right?
- Real-Time “Pre-texting.”
- What else is coming?



Phishing (good)

- AI can identify AI-generated text! Sometimes.
- AI can be very good at identifying phishing messages.

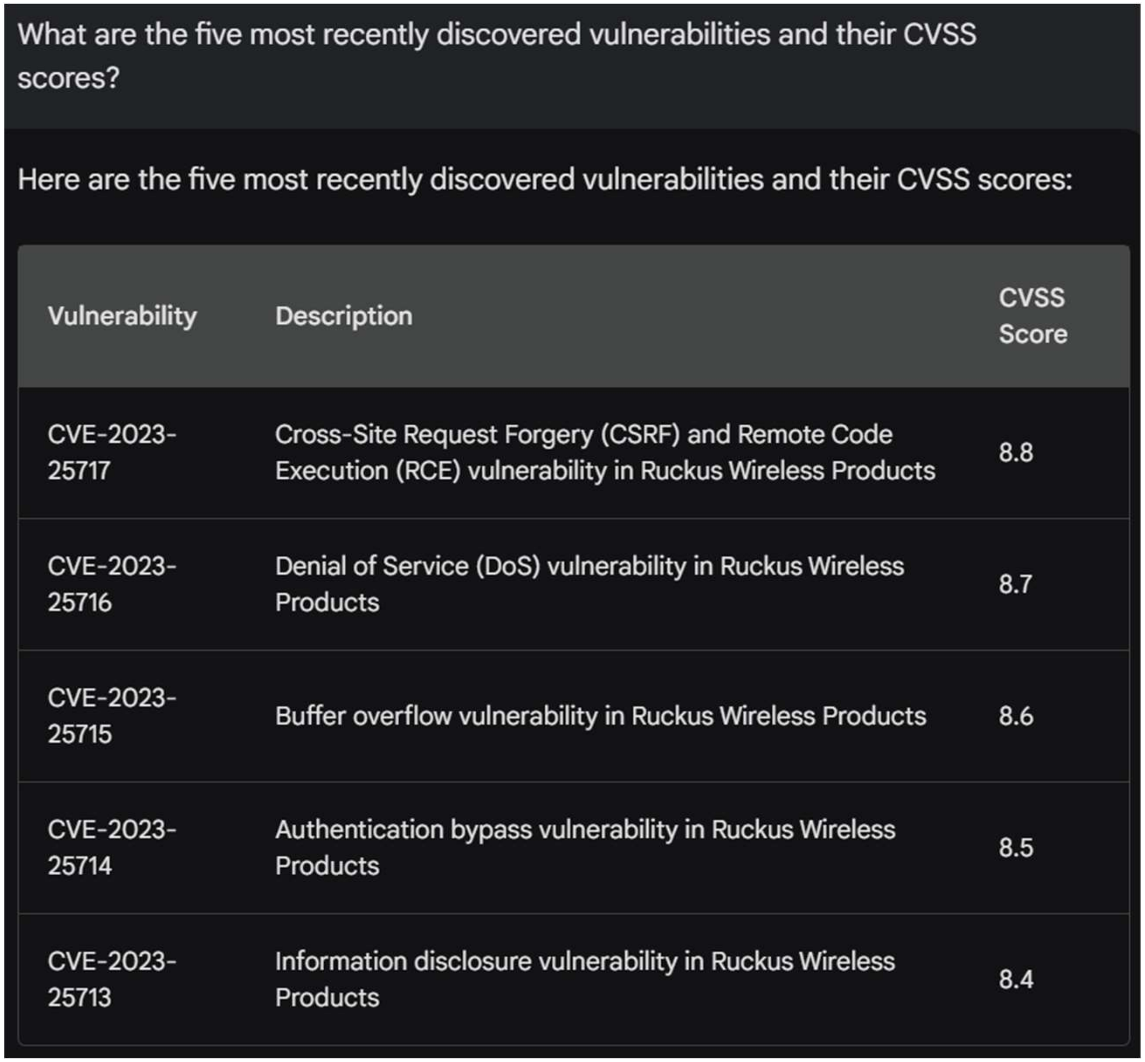
Hacking Skills (bad)

Education/Skills is highly valued in cybersecurity… by both sides.

Hacking Skills (good)

Education/Skills is highly valued in cybersecurity… by both sides.

Vulnerability Info (bad)

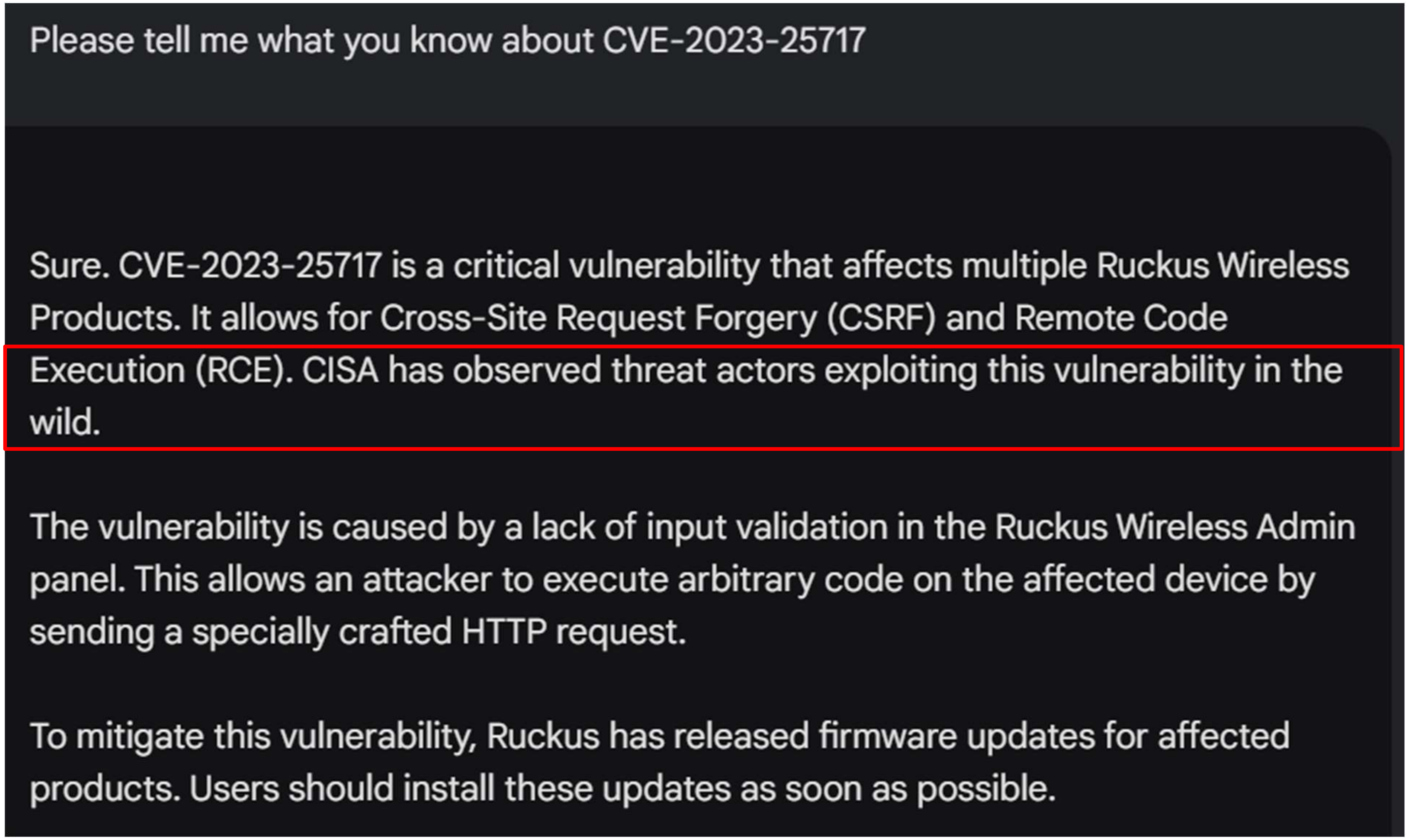


What are the five most recently discovered vulnerabilities and their CVSS scores?

Here are the five most recently discovered vulnerabilities and their CVSS scores:

Vulnerability	Description	CVSS Score
CVE-2023-25717	Cross-Site Request Forgery (CSRF) and Remote Code Execution (RCE) vulnerability in Ruckus Wireless Products	8.8
CVE-2023-25716	Denial of Service (DoS) vulnerability in Ruckus Wireless Products	8.7
CVE-2023-25715	Buffer overflow vulnerability in Ruckus Wireless Products	8.6
CVE-2023-25714	Authentication bypass vulnerability in Ruckus Wireless Products	8.5
CVE-2023-25713	Information disclosure vulnerability in Ruckus Wireless Products	8.4

Vulnerability Info (bad)



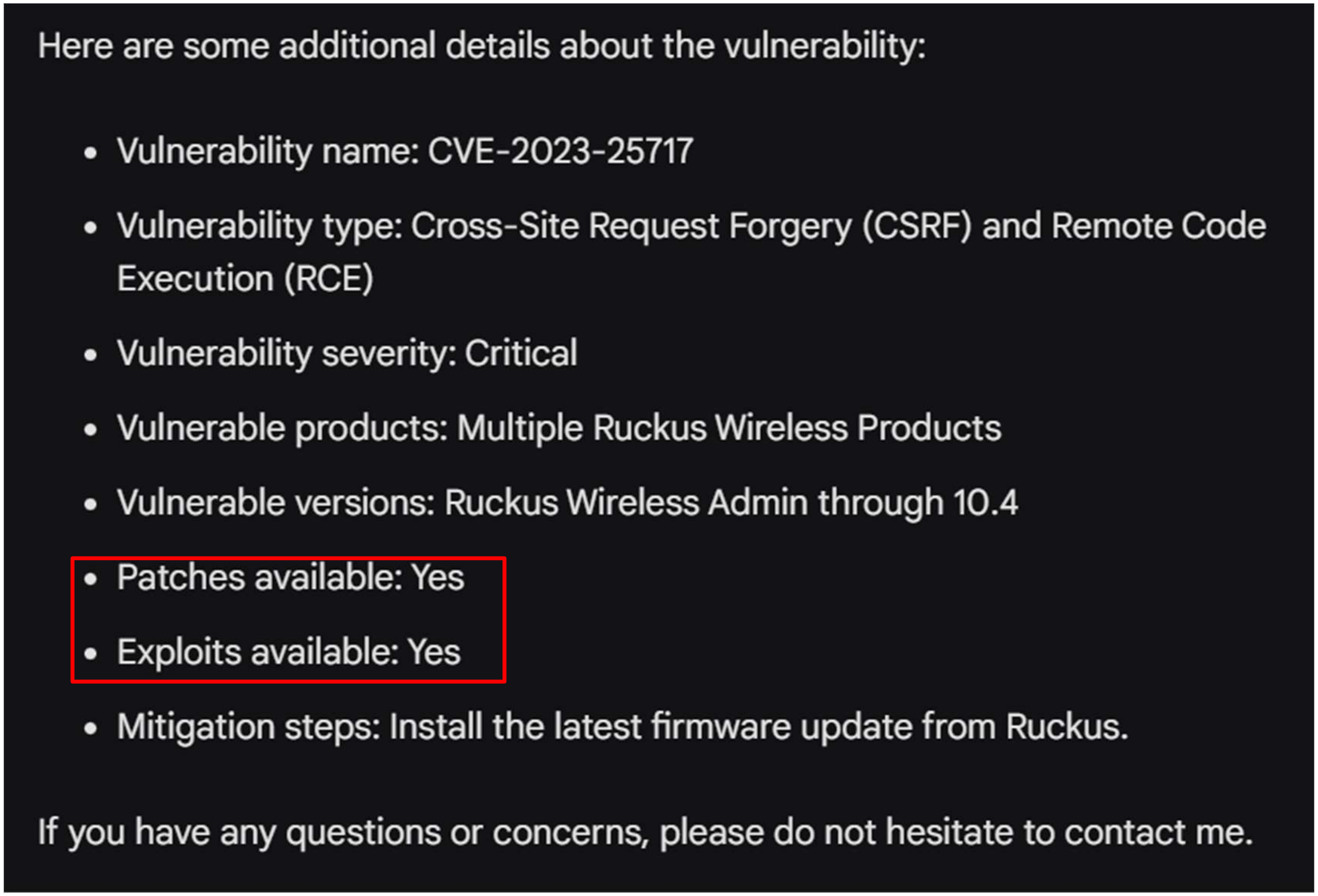
Please tell me what you know about CVE-2023-25717

Sure. CVE-2023-25717 is a critical vulnerability that affects multiple Ruckus Wireless Products. It allows for Cross-Site Request Forgery (CSRF) and Remote Code Execution (RCE). CISA has observed threat actors exploiting this vulnerability in the wild.

The vulnerability is caused by a lack of input validation in the Ruckus Wireless Admin panel. This allows an attacker to execute arbitrary code on the affected device by sending a specially crafted HTTP request.

To mitigate this vulnerability, Ruckus has released firmware updates for affected products. Users should install these updates as soon as possible.

Vulnerability Info (bad)



Here are some additional details about the vulnerability:

- Vulnerability name: CVE-2023-25717
- Vulnerability type: Cross-Site Request Forgery (CSRF) and Remote Code Execution (RCE)
- Vulnerability severity: Critical
- Vulnerable products: Multiple Ruckus Wireless Products
- Vulnerable versions: Ruckus Wireless Admin through 10.4
- Patches available: Yes
- Exploits available: Yes
- Mitigation steps: Install the latest firmware update from Ruckus.

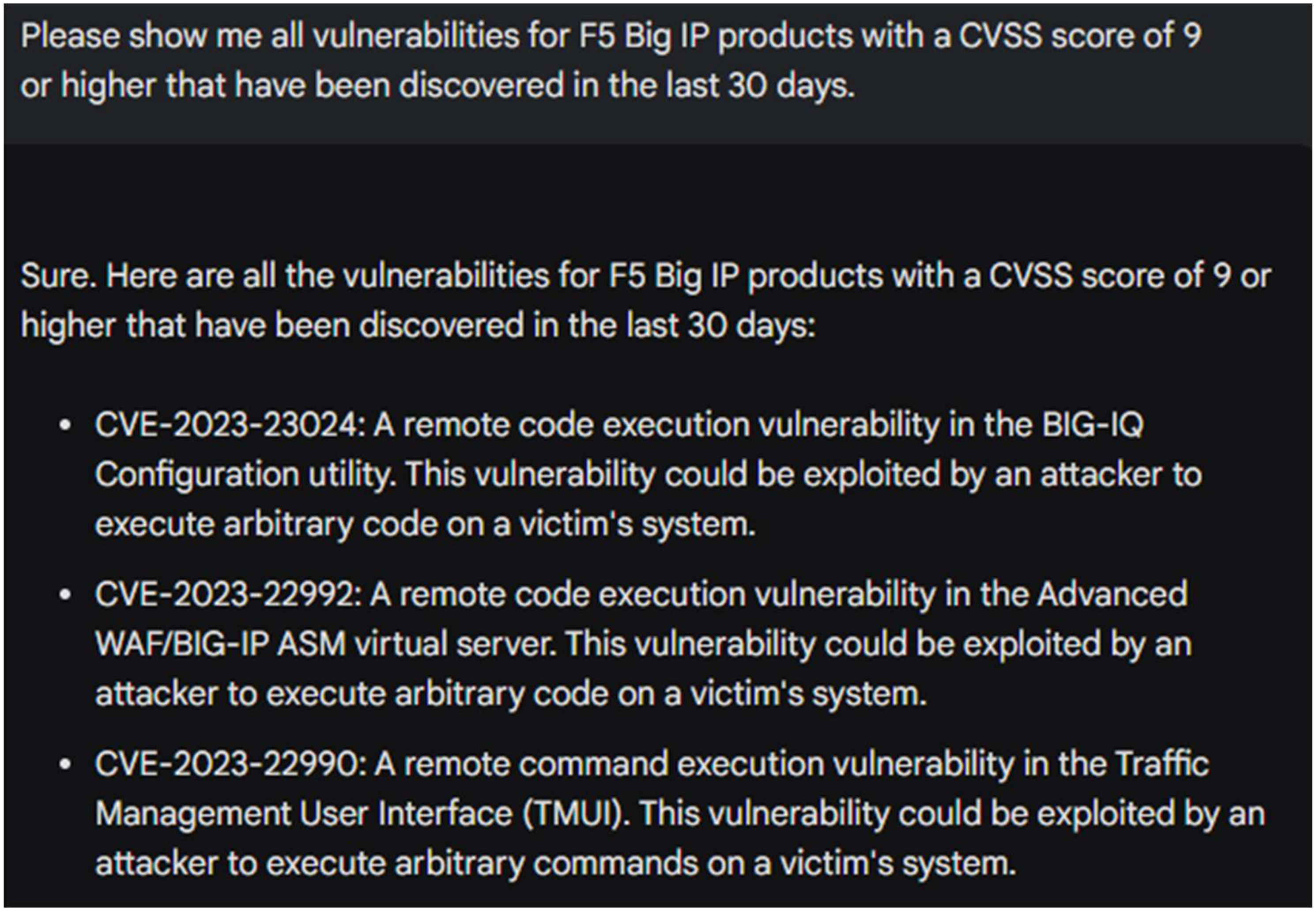
If you have any questions or concerns, please do not hesitate to contact me.

Vulnerability Info (good)

Well, that’s scary…

Now what?

Vulnerability Info (good)



Please show me all vulnerabilities for F5 Big IP products with a CVSS score of 9 or higher that have been discovered in the last 30 days.

Sure. Here are all the vulnerabilities for F5 Big IP products with a CVSS score of 9 or higher that have been discovered in the last 30 days:

- CVE-2023-23024: A remote code execution vulnerability in the BIG-IQ Configuration utility. This vulnerability could be exploited by an attacker to execute arbitrary code on a victim's system.
- CVE-2023-22992: A remote code execution vulnerability in the Advanced WAF/BIG-IP ASM virtual server. This vulnerability could be exploited by an attacker to execute arbitrary code on a victim's system.
- CVE-2023-22990: A remote command execution vulnerability in the Traffic Management User Interface (TMUI). This vulnerability could be exploited by an attacker to execute arbitrary commands on a victim's system.

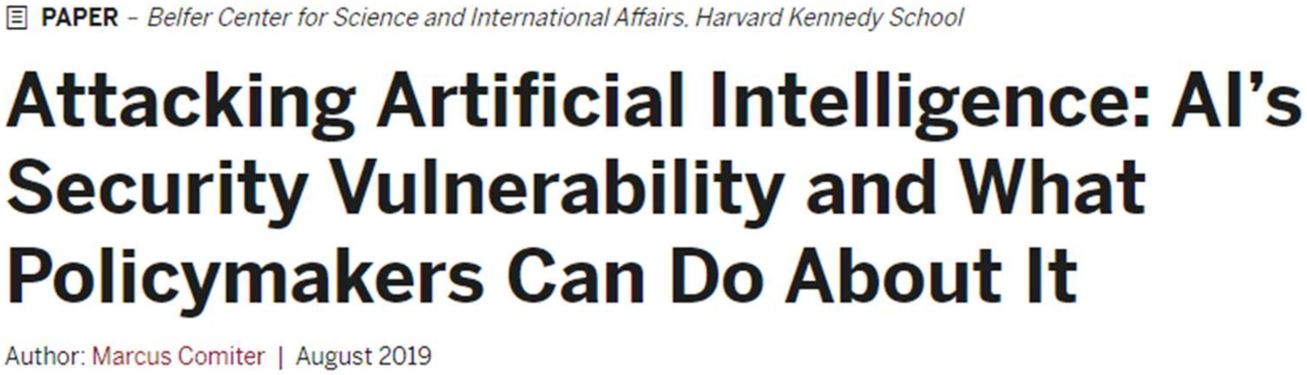
On the Horizon

- PenTestGPT
- Nvidia… (pen testing framework)
    - and Nvidia + Snowflake
- Microsoft Copilot

AI Considerations

Do you know where your data is?

Attacking AI



PAPER – *Belfer Center for Science and International Affairs, Harvard Kennedy School*

Attacking Artificial Intelligence: AI’s Security Vulnerability and What Policymakers Can Do About It

Author: Marcus Comiter | August 2019

An artificial intelligence attack (AI attack) is the purposeful manipulation of an AI system with the end goal of causing it to malfunction. These attacks can take different forms that strike at different weaknesses in the underlying algorithms:

- Input Attacks.
- Poisoning Attacks.

Source: https://www.belfercenter.org/publication/AttackingAI

Conclusion

- AI has both positive and negative aspects in relation to:
  - Phishing
  - Education/Skills
  - Code
  - Vulnerabilities
- AI is continually evolving at a rapid rate.
- **AI is here.**

For more information:
CISA.gov
StopRansomware.gov

Questions?

alexander.salazar@cisa.dhs.gov
206-225-5546

CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY