
BLACK KITE
Where Insight Takes Flight
Can We Teach an AI to Speak Fluent Cybersecurity?

Is This Your Next CISO?

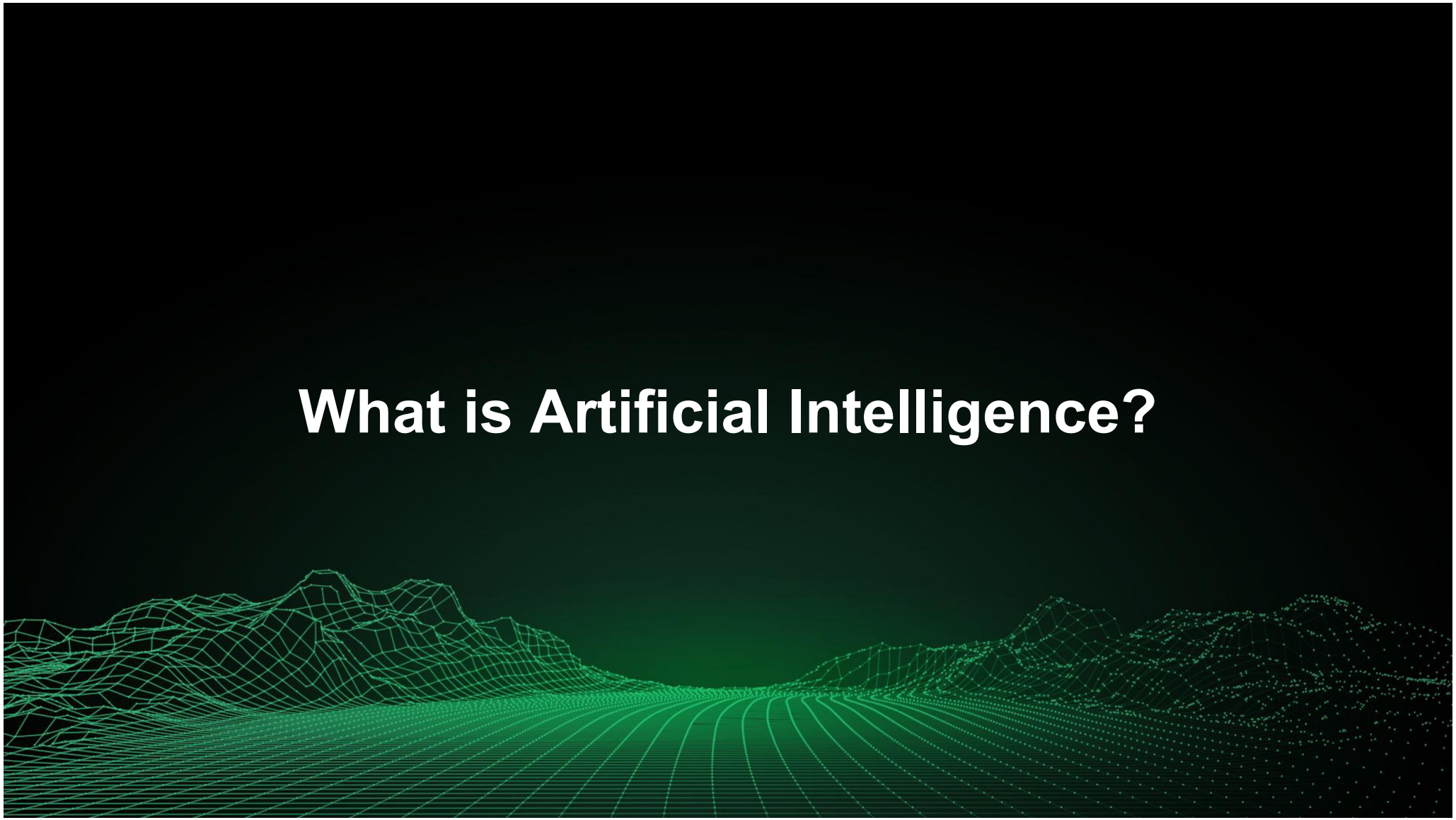
Or … Is This?

Who am I? …

- I am an SVP at Black Kite, a security ratings service vendor – we help companies manage third party risk
- I am a prolific and proficient evangelist
  - **I think about ‘stuff’ and talk about the ‘stuff’ I think about**
- 15-year Gartner veteran
- I’ve advised and spoken to 50,000+ people about cybersecurity and IT risk management
- I’ve run strategic planning workshops for hundreds of organizations
- I’ve spent my career chasing cool technology

- What the heck is Artificial Intelligence (AI) and why should you care?
- How can and will AI impact Cybersecurity professionals?
- Can AI ever replace humans? And should they?

What is Artificial Intelligence?



“Parents” of Artificial Intelligence

Charles Babbage

Ada Lovelace

Alan Turing

What is Artificial Intelligence?

ar·ti·fi·cial in·tel·li·gence

/ˈärdəˌfiSH(ə)l ənˈteləj(ə)ns/

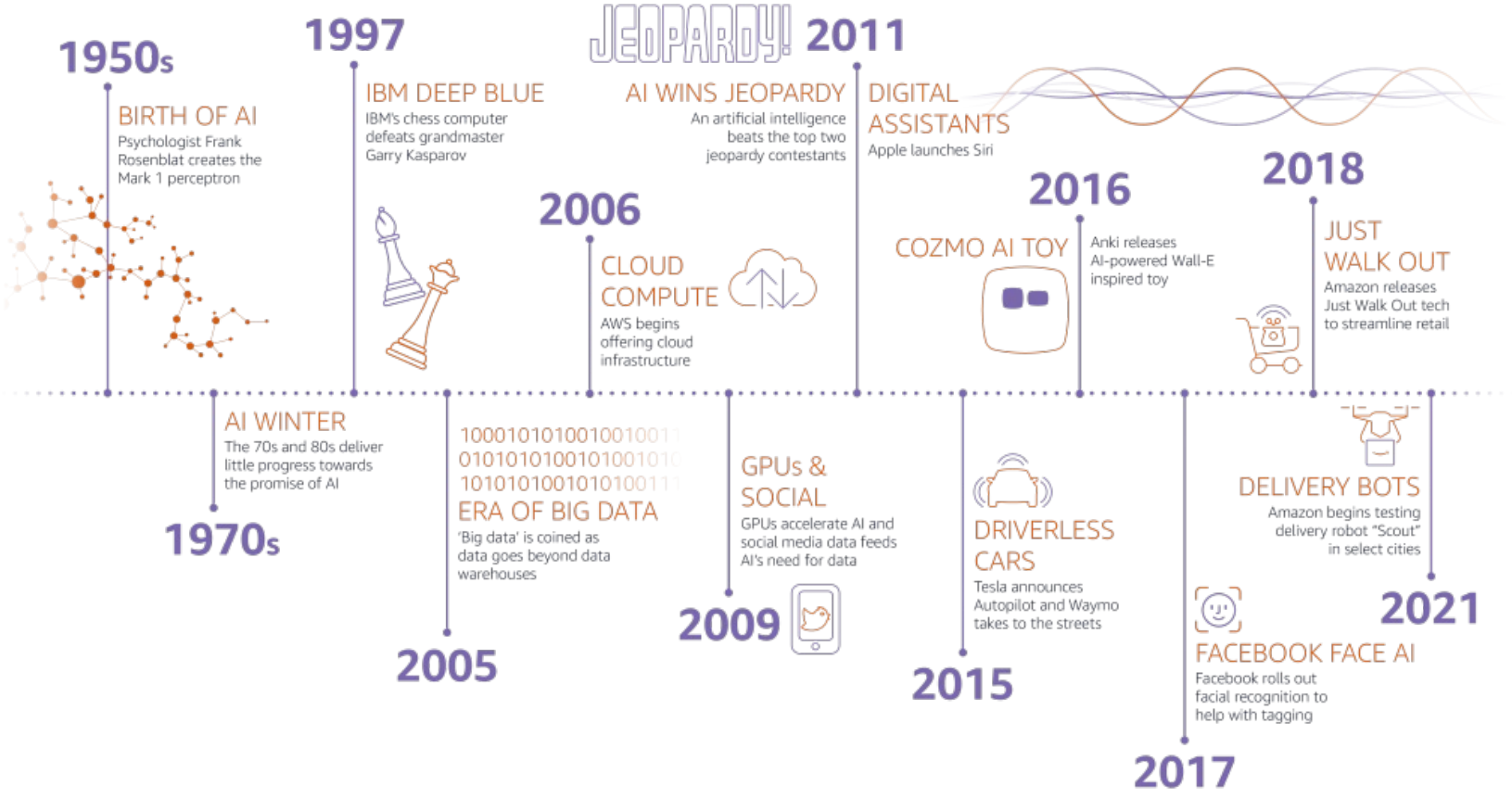
noun

noun: **artificial intelligence**; noun: **AI**

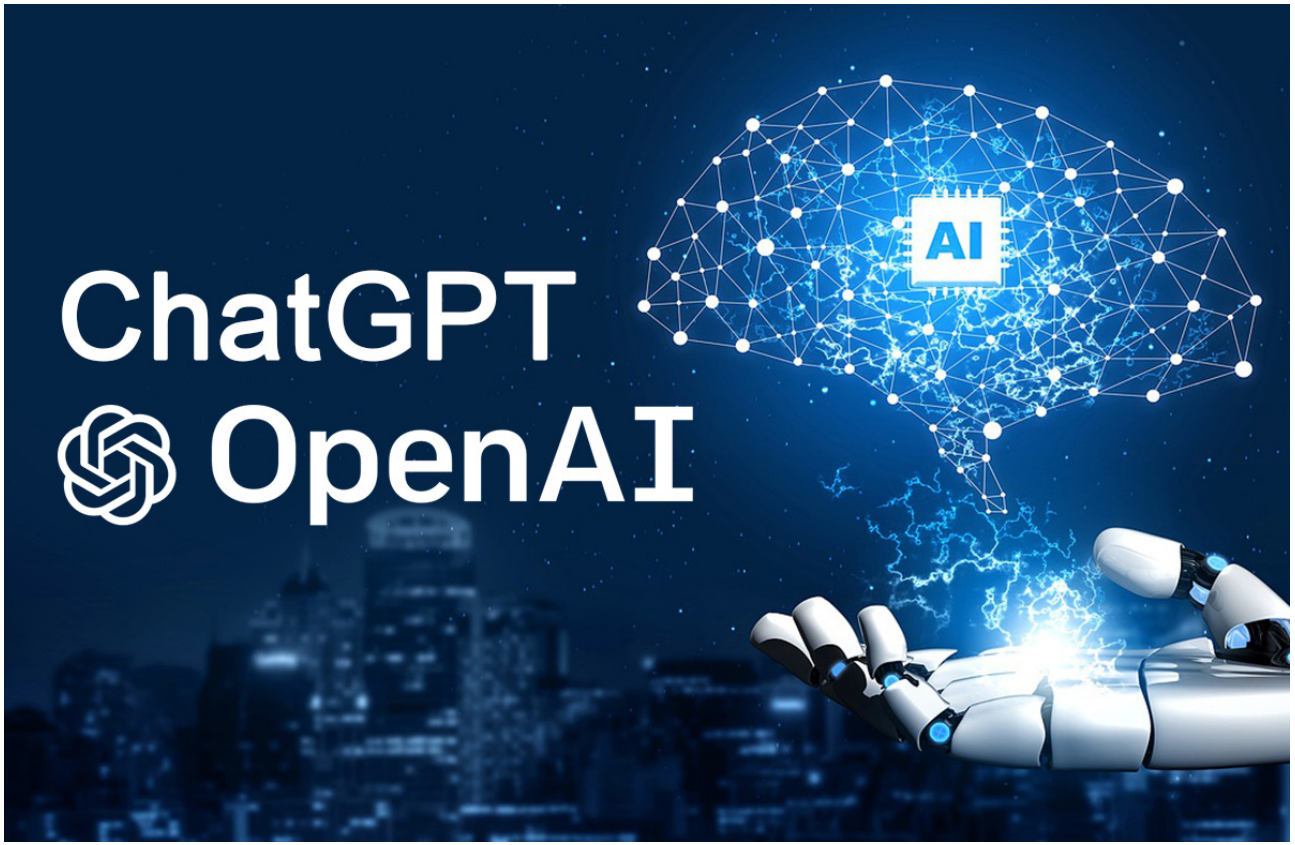
the theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.

Source Oxford English Dictionary

Evolution of AI



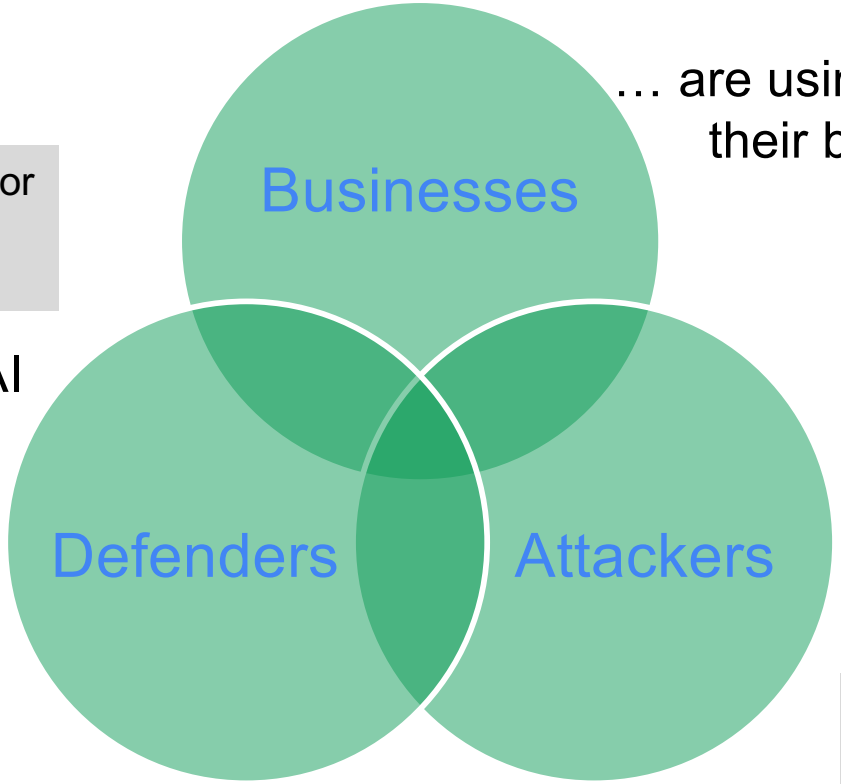
Evolution of AI



Testing of Artificial Intelligence

Turing Test

AI Impacts Cybersecurity in Three Ways



… are using AI to grow their business.

And they probably aren't talking to you about it

And of course every vendor uses AI to solve all you problems

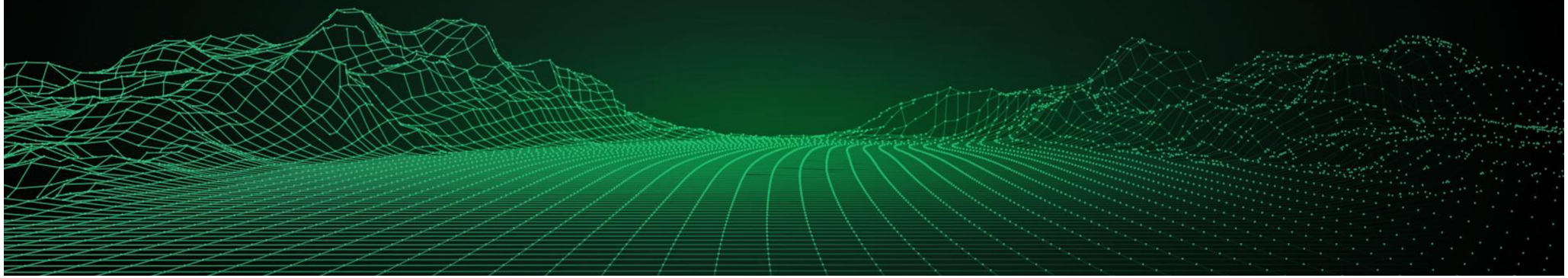
… are using AI keep the bad actors at bay

… will use any tools they can get to 'win'

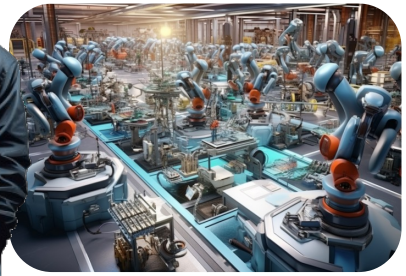
They are using ALL of the tools you are and then some

Artificial Intelligence and Cybersecurity

The Business Perspective



AI in Business



Automated Operations

Informed Decision Making

Enhanced Productivity

Recruitment And Talent Sourcing

Adopting A Customer-Centric Approach

Predictions for Artificial Intelligence

Through 2026, more than $10 billion will have been invested in AI startups that rely on foundation models (large AI models trained on huge amounts of data).

By 2026, 30% of new applications will use AI to drive personalized adaptive user interfaces, up from under 5% today.

By 2026, AI-driven product and customer experience (CX) analytics tools will be the primary source of insight for 40% of digital product enhancements, up from 10% today.

By 2027, over 35% of software will use AI-based digital twins as user personas for user experience (UX) development through the product life cycle, up from less than 5% today.

By 2027, nearly 15% of new applications will be automatically generated by AI without a human in the loop, up from zero percent today.

Source Gartner: Predicts 2023: AI's Profound Impact on Products and Services

Sample ‘Hack’ of Business AI

Sample ‘Hack’ of Business AI

Manipulate the Input … Change the Output

Manipulate the Input … Change the Output

Three Moves for CISOs to Secure AI

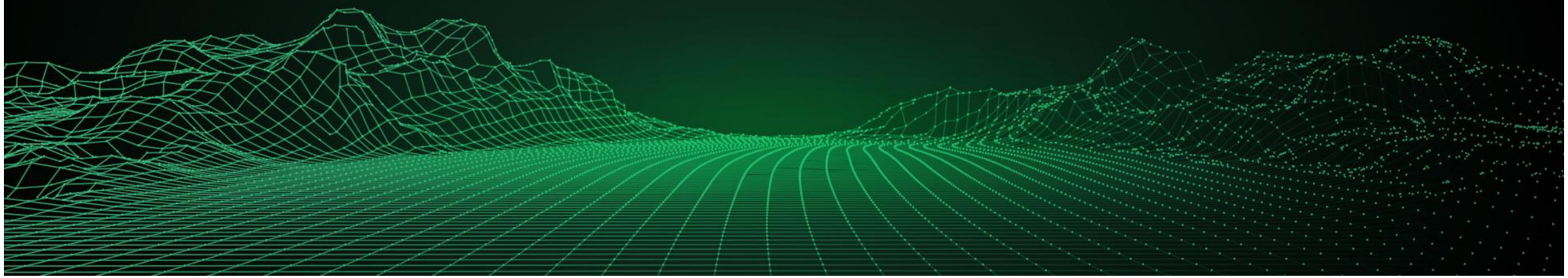
Adopt data protection programs to address AI-specific threats without impeding AI development.

Segregate data to enable AI development without compromising cybersecurity

Make AI data and model vendors a priority in your third-party risk management program

Artificial Intelligence and Cybersecurity

The Defender Perspective



Trends in AI (Cybersecurity Context)

- Security concerns are seen as a major barrier to AI development, but AI workers want security to be more involved in the development process.
- The traditional software development life cycle (SDLC) can be augmented to protect against some, but not all AI threats.
- CISOs cannot go it alone. They have a role in protecting data and systems using AI; however, cybersecurity should not have sole/primarily responsibility.
- CISOs face a hiring challenge — as few as 2% of cybersecurity professionals possess the required AI skills.

AI is THE Buzzword in Cybersecurity

Ask vendors three questions

1. What do you do better with AI?
2. What does AI enable you to do now that you couldn’t or didn’t do before?
3. What does AI enable you to do that your competitors can’t or don’t do?

Advantages and Disadvantages

Advantages

- Getting past the noise
- Managing huge amounts of data
- Learning from mistakes
- Automating complex but easy tasks
- Much better at assessing behavioral anomalies
- More adaptable than people or static tools

Disadvantages/Problems

- AI will not get rid of people
- They aren't very good where data is bad or missing
- AI can be fooled by smart attackers AND their AI tools
- AI can be, and in fact are, biased
- AI isn’t now and may never be truly and fully autonomous

Good News!

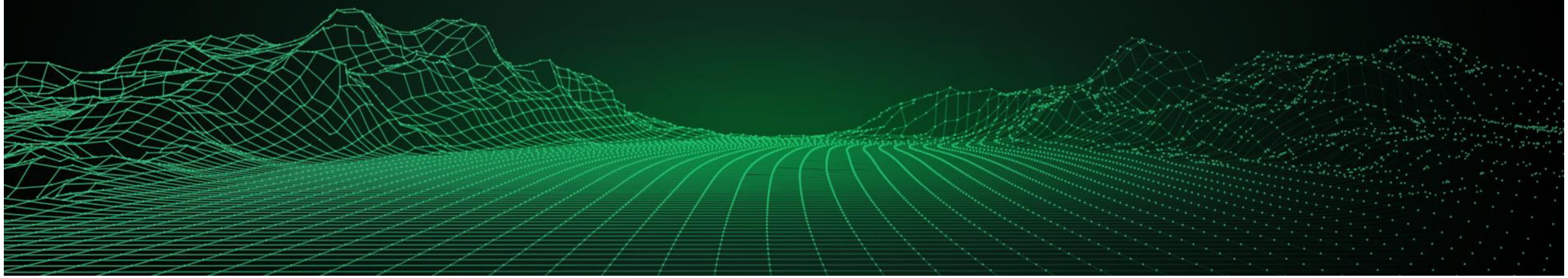
AI is Improving … Rapidly and Relentlessly

Areas Where Defenders Can Leverage AI

Threat & anomaly detection	Identity analytics & fraud detection	Compliance, privacy, & risk management	Bot mitigation
Data discovery & categorization	Breach & attack simulation	Asset discovery	Policy automation
	Security orchestration	Behavioral analytics	

Artificial Intelligence and Cybersecurity

The Attacker Perspective



What About the Adversary?

Test malware's success against AI-based defenses

Poison AI with inaccurate data

Map existing AI models

- Create deepfake data
- Build better malware
- Create & launch stealth attacks
- AI-supported password/CAPTCHA-hacks
- Generative Adversarial Networks (GANs)
- Human impersonation on social media
- Weaponizing AI frameworks vs. hosts
- Deep exploits
- ML-enabled penetration testing tools

Conclusions & Recommendations

- Artificial Intelligence is getting better all the time, but it's not a panacea
- AI has many benefits, but many limitations
- It's unlikely that AI will be CISOs soon (and I would be scared)
- Effective AI will result from partnerships with humans
- Work with your business stakeholders to understand use and plans for AI and share risks with business stakeholders
- Remember the bad guys have AI & no ethics - they will always be ahead

Questions?

Contact Me

Jeffrey.Wheatman@Blackkite.com

linkedin.com/in/jnwheatman/

BlackKite.com/Blog

blackkite.com/risk-and-reels-podcast/

Jeffrey N Wheatman
SVP, Cyber Risk Evangelist