Cybersecurity and AI Offense -- Defense

1. The classic tug of war of Offense Versus Defense
2. Who will win in the future when both are using AI?
3. Who will use it better, and faster?

Microsoft **CVE-2017-11882** **RCE**

Cybersecurity and AI Offense -- Defense

A. Government AI push

B. CISA Cybersecurity & Infrastructure Security Agency

1. Responsibly use AI to support our mission
2. Assure AI systems
3. Protect critical infrastructure from malicious use of AI
4. Collaborate and communicate on key AI efforts with the interagency, international partners, and the public
5. Expand AI expertise in our workforce

Cybersecurity and AI Offense -- Defense

FIXVIRUS.COM

OVERSITESENTRY

A. Why research and use AI for defense?

1. Attackers have their own LLM AI software – i.e. defense has ChatGPT and Google Bard, Vertex AI, Microsoft Co-Pilot and more
2. The exponential 'doubling' phenomenon
3. Is this feasible with AI capability 'doubling' every so often?

Wormgpt is the attacker LLM

Cybersecurity and AI Offense -- Defense

A. Why research and use AI for defense?

1. Defenders have to find attackers using AI software in their network (activity that looks like attackers) I.e possible threats.
2. Use AI software to spot phishing
3. Spot malware

Cybersecurity and AI Offense -- Defense

A. Offense uses of AI

1. Phishing – no more spelling errors?
2. Malware – more, faster, easier to create
3. Misinformation – Elections and more – also social engineering
4. Deep Fakes – Video using a snippet of a real video -→creates fake videos

Cybersecurity and AI Offense -- Defense

A. Defense uses of AI

1. Analyze – use Machine learning, and other to better effect detection
2. Automation - Deep Learning - tasks
3. Summarize – Incident response – Cases
4. Interact – LLM natural language w/ computer
5. Generate Playbooks – create methods
6. Threat hunting – what if attacker in network now what?
7. Create Proactive instead of reactive solutions

Cybersecurity and AI Offense -- Defense

A. Tools to use

Google's Magika is an open-source, AI-powered tool to aid defenders through file type identification, crucial for detecting malware

Amazon SageMaker enables developers to build, train, and deploy machine learning models quickly and effectively

Trend Micro has enhanced its Vision One platform with Trend Companion, a GenAI tool that automates threat investigations and risk assessments

Cybersecurity and AI Offense -- Defense

A. Tools to use

Palo Alto Networks offers Cortex XSIAM, an AI-driven security operations platform, and has integrated AI into its Prisma Cloud offering

- **SentinelOne's Singularity platform** combines security components for enterprise-wide visibility and real-time threat hunting, with Purple AI enhancing productivity for threat hunters

Darktrace employs a self-learning AI technology that spans detection, prevention, response, and remediation across cloud, applications, email, endpoint, and network environments