November 2024 Meetup - Peer Group Discussions

Agenda

Introduction (3 mins)
- 20 seconds / person
- Feel free to drop your LinkedIn profile in chat so we can connect each other further

Exercise (20 mins)
- Review the prompt
- Recap on key concepts
- Group discussion

Readout
- Select a rep from our group to share key insights/takeaway in the main room

Discussion Prompt

- *How does the role of data in AI systems change the attack surface? How can security professionals adjust their thought processes around this?*
- *Does the CIA triad (confidentiality, integrity, and availability) still apply to AIML systems? Why or why not?*

Team Fraser

How does the role of data in AI systems change the attack surface? How can security professionals adjust their thought processes around this?	In ML systems, everything is ABOUT the data - lack of transparency in the data, but all usable	Over-index on just using, with little regard for security	Trust AI to be reliable, in traditional software this is obvious, but in AI reliability isn't obvious	No watchdog about what is dangerous - we lack a CVE equivalent for AI or dependency checkers (hopefully will come)			
	Ordinary security practices, shifting left, old rules still hold for AI	Security is likely to need to use AI to test AI, which involves bootstrapping trust	Software + data security is a journey, a process	LLM acts with the privileges of the user			
Does the CIA triad (confidentiality, integrity, and availability) still apply to AIML systems? Why or why not?							

Team Robin + Audrey

How does the role of data in AI systems change the attack surface? How can security professionals adjust their thought processes around this?							
Does the CIA triad (confidentiality, integrity, and availability) still apply to AIML systems? Why or why not?	yes, esp with model dependencies etc. What happens if a link in the chain fails (availability), Integrity can also be compromised - Man in the middle	Access controls are not clear in the AIML space esp. with lack of understanding of the dependency. Indexed data could be compromised :)	With RAG patterns a small change can have wider reaching influence				

Team Susanna

How does the role of data in AI systems change the attack surface? How can security professionals adjust their thought processes around this?	Data increases attack surface	LLM guardrails - always potential for sensitive data disclosure	Data can be weaponized - not just hardware/network elements				
	Data minimization may not be practical to prevent sesitive disclosure - big data training	Makes attack surface more complex - data may be compromised before training even begins					
Does the CIA triad (confidentiality, integrity, and availability) still apply to AIML systems? Why or why not?	Integrity - Bias, how do we fight?	PII industries - credit risk, insurance, etc. Confidentiality becomes inportant					
	AI as critical infrastructure - Availability attacks compromise critical functions	Integration of other standards					

Team Dimitri + Claire

• **How does the role of data in AI systems change the attack surface? How can security professionals adjust their thought processes around this?**	You need production-like data in a lower environment	Focused a lot on tooling - but not so much data security	Supports productivity	Some professionals uncofmortable as not familair with it, rely on frameworks	Knowledge gaps	Need to change how to approach security	
Does the CIA triad (confidentiality, integrity, and availability) still apply to AIML systems? Why or why not?	Data is data! So yes, it applies	Depends on your architecture	Still applies because we have AI agents being viewed which should be considered an entity (like your PC etc.) you should apply controls to protect the information	The integrity is more important in the AI world			