Day 50

Exploitation Analyst

AI powered solutions for OT Security Tasks:

Cybersecurity Threat Landscape Report - ChatGPT & Gemini & Perplexity:

1. AI Tools Accelerate Attack Crafting: Malicious actors—ranging from script kiddies to state-backed groups—are increasingly using LLMs like ChatGPT and Gemini to enhance their attacks. These tools assist in generating phishing messages, malware code, reconnaissance scripts, and even ransomware components with minimal coding skills required. This accelerates the speed and scale of attacks.

2. State-Backed Abuses of Gemini: Google's Threat Intelligence Group reports that government-linked APTs from Iran, China, and North Korea are leveraging Gemini for various stages of their campaigns—like scripting, lateral movement planning, vulnerability research, payload development, and evasion techniques—though not yet pioneering new methods.

3. Surge in Jailbreaking and Prompt Injection: Underground forums and dark web communities have seen a spike in "jailbreaking" techniques—users successfully bypassing LLM safety controls. Prompt injection methods, including cleverly disguised inputs embedded within data or early-stage prompts, are further enabling the misuse of these tools for illicit purposes.

4. Complacency and Rising Risk in AI Adoption: Enterprise deployment of GenAI tools like ChatGPT, Gemini, and Copilot is rising rapidly—over 40% of organizations have already adopted them. However, a lack of awareness or oversight is breeding security complacency. Experts warn that by 2027, up to 40% of breaches could stem from improper GenAI use, via prompt injections, data leaks, or misuse.

5. Dual Role: AI as Both Threat and Shield: While LLMs are being weaponized by attackers, they're also valuable assets for defenders. Organizations employ ChatGPT, Gemini, and similar tools for threat intelligence—scanning forums, dark web, news sources to produce trend analyses, risk summaries, and actionable security advice.