TECHNICAL LEVEL

BIRD ROCK SYSTEMS

GET A TASTE OF WHAT YOU MIGHT HAVE MISSED AT THIS YEARS BLACK HAT BRIEFINGS*

TASTE OF BLACK HAT

2023

*Briefs not on this menu are available on request! Our team has recordings of all the briefings, ask your Account Manager which you would like a taste of: https://www.blackhat.com/us-23/briefings/schedule/index.html

Keynote: Guardians of the AI Era: Navigating the Cybersecurity Landscape of Tomorrow

History, AI capabilities in security drizzled with discussions on reshaping the Cybersecurity Landscape, Generalized Keynote. Excellent Appetizer!

Keynote: Forward Focus: Perspectives on AI

Forward thoughts on the future of AI with an extra helping of challenges, regulation, and legal issues for the future complemented with what it means in security. Generalized Keynote recommended to order alongside the first briefing.

Devising and Detecting Phishing: Large Language Models (GPT3, GPT4) vs. Smaller Human Models (V-Triad, Generic Emails)

Research into AI made to pair with spear-phishing. Researcher goes into detail about how AI can be used to create highly targeted phishing campaigns with scary success rates. Served in a university setting.

Me and My Evil Digital Twin: The Psychology of Human Exploitation by AI Assistants

A flavorful helping on AI, shown to exploit human “cognitive levers” to manipulate people. An interesting serving of this being a case study involving GPT-4 socially engineering a human to bypass visual Captcha.

The Integration Cyber Security and Insurance: The Journey of Cysurance

A light dish that takes to the recent history of CyberInsurance and its trends. Tasty sprinkles of the trend of cyberinsurance premiums and their companies fight to reduce risk and cost! Recommended to pair with an order of “Bridging Cyber and Insurance."

Bridging Cyber and Insurance

A supplemental dish that takes you back to the history of Cyber and Insurance with an extra helping of compliance.

AI Assisted Decision Making of Security Review Needs for New Features

SDLC (Software Development Life Cycle) related. Delicious demonstration of NLP (Natural Language Processing) in SDLC programs and how it can be used to make judgements on legal, privacy, and general engineer reviews. A management favorite!

Evasive Maneuvers: Trends in Phishing Evasion & Anti-Evasion

A culinary delight on the latest creative tactics and evasion techniques used by threat actors to set up under the radar phishing sites. Includes a side dish of historical methods to bypass phishing defenses and detecting cutting-edge campaigns. Great pairing with the previous item!

Compromising LLMs: The Advent of AI Malware

An exotic new strain of malware corrupting AI. Observe as the chef demonstrates how new and existing malware can run entirely inside of LLMs like ChatGPT!

mTLS: When Certificate Authentication is Done Wrong

A quick but filling snack about the new novel attacks on mTLS authentication with none of the fattening crypto. Finished with a look on implementation vulnerabilities and information leakages!

The Yandex Leak: How a Russian Search Giant Uses Consumer Data

A healthy look into Russian Yandex’s 45GB source code leak! Garnished with information on Yandex’s services and behavioral analytics. Don’t let the Yandex’s data collection burn your tongue!