Meta Eyes Enterprise Spend With Muse for Small Business Launch

The new offering aims to put Meta’s new agent to work for the roughly 200 million brands that operate on its platform. https://www.adweek.com/social-marketing/meta-muse-for-small-business-enterprise/

OpenAI Takes On Meta’s Muse With Dots, an Always-On AI Agent

The agents run on their own cloud computers and can connect to more than 4,000 apps. https://www.adweek.com/media/openai-takes-on-metas-muse-with-dots-an-always-on-ai-agent/

Reco Raises $55 Million for Agentic Security

The company will use the funds to expand its sales, partnerships, channels, and customer support teams.

The post Reco Raises $55 Million for Agentic Security appeared first on SecurityWeek.

https://www.securityweek.com/reco-raises-55-million-for-agentic-security/

Hackers Use ChatGPT Custom GPTs in ClickFix Attacks

The personalized versions of ChatGPT were used to impersonate legitimate products and trick users into executing PowerShell commands.

The post Hackers Use ChatGPT Custom GPTs in ClickFix Attacks appeared first on SecurityWeek.

https://www.securityweek.com/hackers-use-chatgpt-custom-gpts-in-clickfix-attacks/

Pentagon Personnel Agency Data Breach Impacts 3 Million People

The data breach affects the Defense Manpower Data Center (DMDC), which maintains personnel records for the Department of Defense.

The post Pentagon Personnel Agency Data Breach Impacts 3 Million People appeared first on SecurityWeek.

https://www.securityweek.com/pentagon-personnel-agency-data-breach-impacts-3-million-people/

Alphabet’s Wing Hires Minjae Ormes as Head of Marketing

She arrives as the drone delivery service is helping brands like Walmart, DoorDash, and PepsiCo take to the skies. https://www.adweek.com/brand-marketing/alphabets-wing-hires-minjae-ormes-as-head-of-marketing/

Rig Security Emerges From Stealth With $12M to Tackle Agentic AI Identity Risks

Rig provides an identity dependencies graph to distinguish between legitimate users and rogue AI agents

The post Rig Security Emerges From Stealth With $12M to Tackle Agentic AI Identity Risks appeared first on SecurityWeek.

https://www.securityweek.com/rig-security-emerges-from-stealth-with-12m-to-tackle-agentic-ai-identity-risks/

TikTok’s Partnership With All Things Go Shows What Discovery Looks Like IRL

The indie music festival teamed up with TikTok LIVE. https://www.adweek.com/brand-marketing/tiktok-partnership-all-things-go-discovery/

Four Cyber Threats Harboring Big Plans for the Future

– AI, supply-chain exposure, quantum computing and geopolitical conflict are testing security programs. Preparing for disruption must become part of day-to-day operations.

The post Four Cyber Threats Harboring Big Plans for the Future appeared first on SecurityWeek.

https://www.securityweek.com/four-cyber-threats-harboring-big-plans-for-the-future/

OpenAI Calls Off GPT-6.1 Astra Launch, Details Safety Cases for Frontier Training

The GPT-6.1 Astra model was slated to debut in ChatGPT and Codex in October, but it fell short of expectations.

The post OpenAI Calls Off GPT-6.1 Astra Launch, Details Safety Cases for Frontier Training appeared first on SecurityWeek.

https://www.securityweek.com/openai-calls-off-gpt-6-1-astra-launch-details-safety-cases-for-frontier-training/