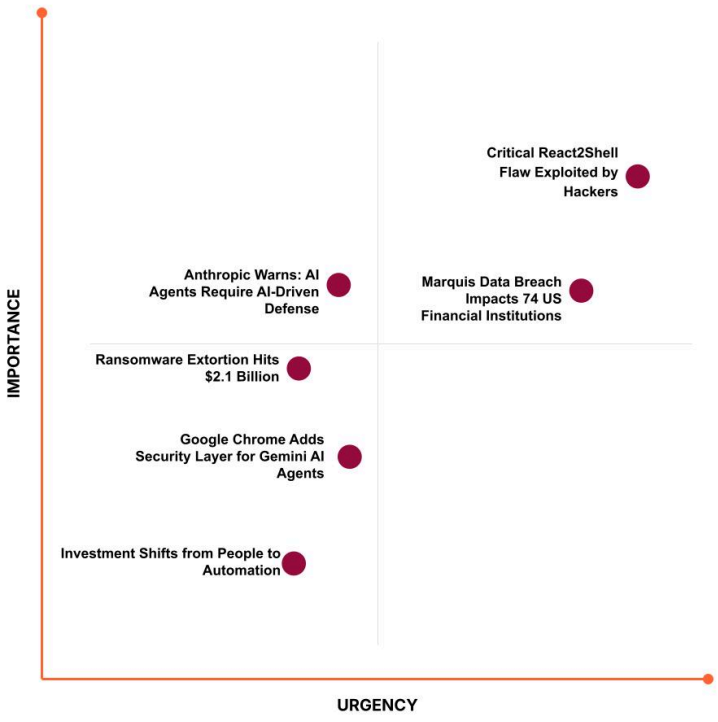
CLOUDFLARE

Cloudflare Cyber Briefing

December 12, 2025

Welcome to the Cloudflare Cyber Briefing from our Field CXO team, helping leaders stay ahead in a fast-moving cyber landscape of threats, technology shifts, and criminal tactics.

What you need to know:



AI cybersecurity

Google Chrome adds security layer for Gemini AI agents

Google is rolling out a new security architecture within Chrome designed to sandbox and scrutinize the actions of its Gemini agentic AI features, aiming to prevent these autonomous agents from being hijacked by malicious web content.

CISO's takeaway: Browser-based AI agents introduce a new attack surface where the browser itself acts on behalf of the user; do not rely solely on client-side sandboxes. Enforce strict isolation to contain potential agent compromises.

Source: Google | Read more →

Anthropic warns: AI agents require AI-driven defense

Anthropic's latest security guidance argues that as AI agents become more autonomous and capable of rapid action, traditional static defenses will fail. They advocate for deploying "defensive AI" to counter the speed and scale of attacks launched by adversarial AI agents.

CISO's takeaway: Fighting fire with fire is no longer optional — CISOs must integrate AI-enabled detection at the edge to identify and block machine-speed attacks that human analysts cannot catch in time.

Source: Anthropic | Read more →

Cyber incidents

Critical React2Shell flaw exploited by hackers

Hours after disclosure, a critical Remote Code Execution (RCE) vulnerability in React Server Components, dubbed "React2Shell," was added to CISA's KEV list following confirmed active exploitation by Chinese threat actors targeting unpatched web servers.

CISO's takeaway: The window between disclosure and exploitation has effectively vanished — you cannot wait for patch cycles. Implement virtual patching at the WAF level immediately to block exploit attempts against known CVEs before they reach your origin.

Source: CISA | Read more →

Marquis data breach impacts 74 US financial institutions

A significant supply chain breach at vendor Marquis has exposed sensitive data across 74 US banks and credit unions. Attackers compromised the third-party provider to gain downstream access to financial institution data, bypassing direct perimeter defenses.

CISO's takeaway: Your vendor's security posture is your own; implicit trust in third-party connections is a liability. Enforce zero trust access for all external partners and audit their access privileges strictly to prevent cascading supply chain breaches.

Source: BleepingComputer | Read more →

Cyber insights

Ransomware extortion hits $2.1 billion

A new FinCEN report reveals that ransomware gangs extorted over $2.1 billion between 2022 and 2024. Despite law enforcement disruptions, the profitability of ransomware continues to drive sophisticated, high-value targeting of critical sectors.

CISO's takeaway: Ransomware is an economic engine that isn't slowing down, and perimeter defense is insufficient. Shift focus to "assuming breach" and implementing zero trust architectures to prevent the lateral movement that turns an intrusion into a payout, while ensuring a swift response to potential incidents.

Source: FinCEN | Read more →

Investment shifts from people to automation

New research from the European Union Agency for Cybersecurity (ENISA) reveals a decisive pivot in cybersecurity spending, with organizations increasingly diverting budgets from hiring to technology and outsourcing as the global talent shortage makes scaling human teams impossible.

CISO's takeaway: The "people-first" defense model is breaking under the weight of the skills gap — you cannot hire your way to security. Aggressively consolidate tools and implement automated policy enforcement to maintain resilience without needing to increase headcount.

Source: ENISA | Read more →

Cloudflare insights

Cloudflare outage on December 5, 2025

On December 5, 2025, at 08:47 UTC (all times in this blog are UTC), a portion of Cloudflare's network began experiencing significant failures. The incident was resolved at 09:12 (~25 minutes total impact), when all services were fully restored. More can be found here.

The Internet is constantly changing in ways that are difficult to see

Stay up to date with the recent trends and statistics of the Internet at https://radar.cloudflare.com/.

In case you missed it...

Find more resources from the CXO team below:

Dan Kent, Field CTO for Public Sector: An AI chatbot playbook for government — How to build, protect, and govern AI-powered assistants. Read more.