CLOUDFLARE

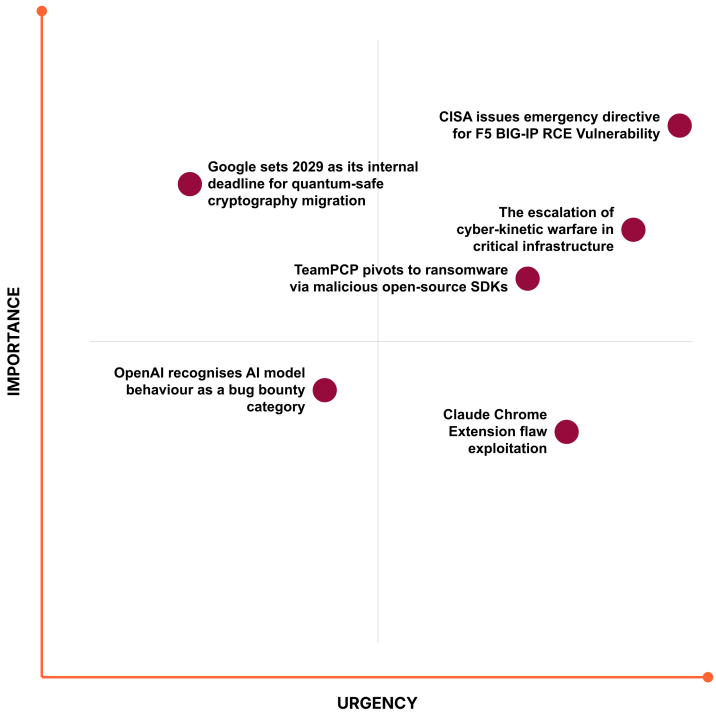
# Cloudflare Cyber Briefing

**April 3, 2026**

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.

The **2026 Cloudflare Security Signals Report** is now available. This year's report provides a map to hidden fault lines, the enterprise risks that only emerge as speed, scale, and disruption increase.  Discover ways to identify and address these fault lines before they become major ruptures.

## What you need to know:




# AI cybersecurity

## Claude Chrome Extension flaw exploitation

A vulnerability in Anthropic's Claude Chrome Extension, codenamed ShadowPrompt, chained an overly permissive origin allowlist with a DOM-based cross-site scripting flaw in a third-party CAPTCHA component to allow any website to inject prompts silently into the AI assistant, without any user interaction. The attacker required only that the target visited a malicious page; the assistant then acted on attacker-controlled instructions with the permissions of the signed-in user.

**CISO's takeaway:** Browser-based AI assistants are privileged software running inside the corporate browser. CISOs whose endpoint policy permits third-party AI browser extensions should treat them with the governance discipline applied to privileged executables: controlled allowlists, enforced via a secure gateway with real-time content inspection that blocks malicious page content before it reaches the extension. Pairing that with a data loss prevention layer covering AI-bound traffic adds a second line of defense if a session is silently hijacked.

Source: The Hacker News | Read more →

---

## OpenAI recognizes AI model behavior as a bug bounty category

OpenAI has expanded its bug bounty program to cover design-level AI risks explicitly, including model abuse, jailbreaking, prompt manipulation leading to material harm,

and safety-relevant behavioral failures — recognizing that vulnerabilities in AI systems extend beyond implementation flaws to how the model itself responds to adversarial inputs. The program rewards external researchers for finding weaknesses that traditional CVE processes were not designed to capture.

**CISO's takeaway:** Vendor security due diligence for AI tools should now include questions about responsible disclosure program covering model behavior. Organizations that deploy AI models with access to sensitive data or customer-facing interactions need visibility into how those models respond to adversarial inputs — both from external users and from malicious content the model may encounter. A security layer positioned between users and AI models that monitors inputs for adversarial patterns, enforces output policies, and produces audit logs of model interactions provides a compensating control that operates independently of the model's internal guardrails.

Source: SecurityWeek | Read more →

# Cyber incidents

### TeamPCP pivots to ransomware via malicious open-source SDKs

Following a string of supply chain compromises involving popular SDKs, the TeamPCP group has officially partnered with the "Vect" ransomware-as-a-service operation. The group is now leveraging previously harvested credentials from their supply chain attacks to deploy ransomware across multiple sectors simultaneously.

**CISO's takeaway:** Supply chain hygiene is now a real-time requirement; use automated API protection to discover hidden dependencies and enforce strict schemas, ensuring that compromised third-party code cannot exfiltrate sensitive data or communicate with unauthorized command-and-control servers.

Source: Help Net Security | Read more →

---

### CISA issues emergency directive for F5 BIG-IP RCE vulnerability

The Cybersecurity and Infrastructure Security Agency (CISA) has added a critical remote code execution vulnerability in F5 BIG-IP Access Policy Manager to its Known Exploited Vulnerabilities catalog. Attackers are actively leveraging the flaw to gain initial access, prompting a remediation deadline of March 30, 2026, for all federal agencies.

**CISO's takeaway:** This incident underscores the systemic risk of exposing critical network appliances and management interfaces to the public Internet. Organizations

should immediately prioritize protecting their infrastructure by transitioning to identity-aware access controls that verify every request before it reaches the network, while simultaneously deploying automated web application protection to provide virtual patching against exploit attempts while official updates are validated.

Source: Cyber Security News | Read more →

# Cyber insights

## Google sets 2029 as its internal deadline for quantum-safe cryptography migration

Google has announced 2029 as its deadline for completing the migration to quantum-safe cryptography across its infrastructure, citing the accelerating timeline for cryptographically relevant quantum computing and the active "harvest now, decrypt later" threat model — in which state-level adversaries are collecting encrypted traffic today to decrypt it once quantum capability matures. The announcement follows the 2024 finalization of NIST post-quantum standards including ML-KEM and ML-DSA.

**CISO's takeaway:** A 2029 internal deadline from Google is a practical benchmark. The program starts with inventory: map TLS versions, cipher suites, and key exchange mechanisms across Internet-facing services, data-at-rest encryption on sensitive stores, and any long-lived encrypted archives. Modern network edge infrastructure, including TLS termination with hybrid post-quantum key exchange using ML-KEM alongside classical elliptic curve algorithms, supports this migration on externally facing traffic without requiring application changes, making it a practical first step while longer-term cryptographic library migrations progress.

Source: Google's The Keyword | Read more →

---

## The escalation of cyber-kinetic warfare in critical infrastructure

Security insights from the ongoing conflicts in the Middle East and Europe demonstrate that digital attacks on hospitals and energy grids are now a standard component of modern warfare. These "cyber-kinetic" events prove that digital disruption is no longer just about data theft but about creating physical chaos and weakening national resilience.

**CISO's takeaway:** For organizations operating critical infrastructure, business continuity must be built on a global anycast network that can absorb hyper-volumetric strikes and maintain service availability even when domestic networks are under heavy duress.

Source: SecurityWeek | Read more →

# Cloudflare insights

### Sandboxing AI agents, 100x faster

We're introducing Dynamic Workers, which allow you to execute AI-generated code in secure, lightweight isolates. This approach is 100 times faster than traditional containers, enabling millisecond startup times for AI agent sandboxing. More can be found here.

---

### Custom Regions give organizations precise control over where data is processed

We are expanding Regional Services with new predefined regions and the launch of Custom Regions. Customers can now define precise geographical boundaries for data processing, tailored to meet their compliance and performance needs. More can be found here.

---

### Launching Cloudflare's Gen 13 servers: trading cache for cores for 2x edge compute performance

Cloudflare's Gen 13 servers double our compute throughput by rethinking the balance between cache and cores. Moving to high-core-count AMD EPYC™ Turin CPUs, we traded large L3 cache for raw compute density. By running our new Rust-based FL2 stack, we completely mitigated the latency penalty to unlock twice the performance. More can be found here.

# CXO events and resources

The Intelligent Age has arrived. It brings the potential of agentic AI, but also a new risk equation of global attacks and a fracturing geopolitical cloud. Join us at Connect on Tour London on April 15 to learn how to navigate this shift. We will show you how to move from complexity to confidence by simplifying your stack and securing your future.

**Come chat with Cloudflare's Field CXO team at the following events:**

- Optivcon Dallas, April 7, Parker, TX,US
- GITEX Africa, April 7–9, Marrakech, Morocco

- IATA World Data Symposium, April 8–9, Singapore, SG
- RH-ISAC Cyber Intelligence, April 13–15, Austin, TX, US
- Immerse New York, April 14, New York City, NY, US
- OptivCon Toronto, April 16, Toronto, CA
- SINETSilicon Valley, April 21, Mountain View, CA, US
- Immerse Montreal, April 22, Montreal, CA
- Immerse Minneapolis, April 23, Minneapolis, MN, US

Find more resources from the CXO team here.