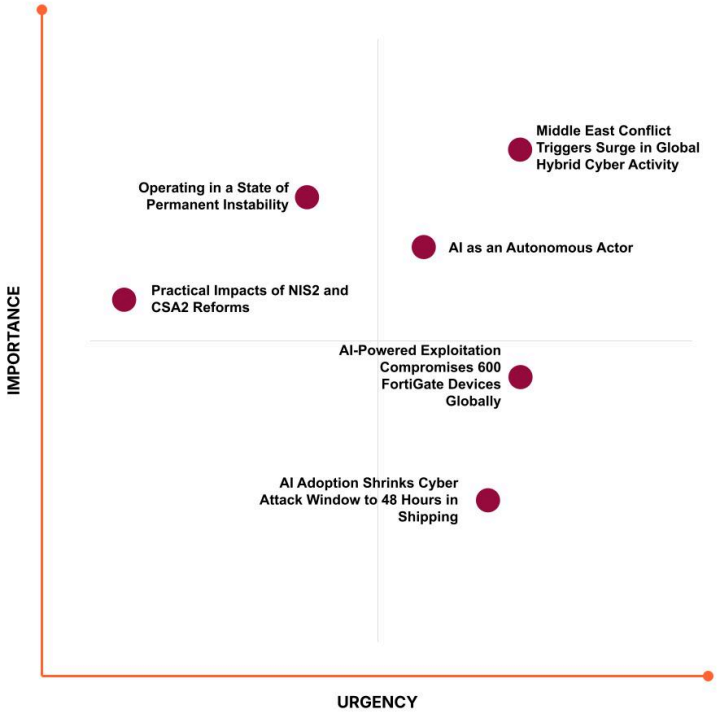
CLOUDFLARE

Cloudflare Cyber Briefing

March 6, 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.

What you need to know:



AI cybersecurity

AI adoption shrinks cyber attack window to 48 hours in shipping

A new report from Cydome warns that AI-driven tools are now weaponizing 60% of newly disclosed vulnerabilities within 48 hours, a massive decrease from previous years. In some cases, automated systems are targeting critical infrastructure within 15 minutes of a flaw being detected, leaving traditional patching cycles obsolete.

CISO's takeaway: Defense must now move at machine speed to match the pace of automated exploitation. Organizations should implement AI-aware traffic inspection to detect anomalous bot behaviors and leverage advanced application firewalling to deploy virtual patches automatically the moment a vulnerability is identified.

Source: SplashTech | Read more →

AI as an autonomous actor

Enterprises have rapidly moved from AI pilots to autonomous agents that execute multi-step tasks and call external APIs without human intervention. This shift has created a governance gap where 64% of billion-dollar companies report significant financial losses due to shadow AI and unmonitored agentic failures.

CISO's takeaway: You must move beyond simple prompt monitoring to a full lifecycle governance model. Implement centralized observability and policy controls for all LLM traffic to prevent data exfiltration by autonomous agents and ensure that shadow AI usage is brought under a secure-by-design framework.

Source: Help Net Security | Read more →

Cyber incidents

Middle East conflict triggers surge in global hybrid cyber activity

Following a coordinated cyber campaign, pro-Iranian hacktivist groups have begun retaliatory strikes against Gulf energy sectors and Western critical infrastructure. Over 60 groups are currently engaged, with ransomware attacks already reported against prominent oil and gas exploration firms.

CISO's takeaway: Geopolitical volatility requires a thoughtful and broad approach. Activating global DDoS mitigation and deploying SASE globally ensures that localized conflicts do not disrupt your global service availability.

Source: Infosecurity Magazine | Read more →

AI-powered exploitation compromises 600 FortiGate devices globally

Amazon security researchers confirmed that a Russian-speaking threat actor successfully used commercial generative AI to automate the compromise of over 600 FortiGate devices across 55 countries. The attackers used AI to refine their exploitation techniques, allowing them to rapidly penetrate edge network devices that had not yet been updated.

CISO's takeaway: Vulnerable edge hardware remains a primary entry point for AI-assisted adversaries. To mitigate this risk, transition away from legacy appliances toward cloud-native zero trust security and use automated WAF rules to protect unpatched vulnerabilities at the network layer.

Source: AWS Security Blog | Read more →

Cyber insights

Operating in a state of permanent instability

As we enter March 2026, the cybersecurity industry is shifting away from "next-gen" marketing toward structural reinforcements that prioritize operational resilience. The convergence of AI speed and geopolitical fragmentation means that trust relationships are increasingly fragile, demanding a machine-speed defense that can handle automated threats.

CISO's takeaway: Strategy must move from detect and respond to a model of sustained resilience that assumes the perimeter is constantly shifting. Consolidating your security stack into a unified connectivity cloud provides the orchestration needed to maintain operations despite high atmospheric cyber instability.

Source: Security Boulevard | Read more →

Practical impacts of NIS2 and CSA2 reforms

The European Commission's new 2026 package transforms cybersecurity certification from a voluntary label into a mandatory risk-management tool. The reforms sharpen reporting requirements for ransomware and expand the "essential entities" list to include providers of digital wallets and strategic dual-use infrastructures.

CISO's takeaway: Compliance doesn't make you secure, but security does make you compliant. Align your reporting playbooks with automated logging and visibility tools

to meet the standardized EU-wide incident response timelines. Confirm that data is only decrypted in your designated region and ensure your supply chain risk management follows the latest unified security standards.

Source: IAPP | Read more →

Cloudflare insights

Introducing the 2026 Cloudflare Threat Report

Today's threat landscape is more varied and chilling than ever: Sophisticated nation-state actors. Hyper-volumetric DDoS attacks. Deepfakes and fraudsters interviewing at your company. Even stealth attacks via trusted internal tools like Google Calendar, Dropbox, and GitHub. Our newest report covers the most current threats and how to protect against them. More can be found here.

The truly programmable SASE platform

As the only SASE platform with a native developer stack, we're giving you the tools to build custom, real-time security logic and integrations directly at the edge. More can be found here.

Evolving Cloudflare's Threat Intelligence Platform: actionable, scalable, and ETL-less

Stop managing ETL pipelines and start threat hunting. Introducing new visualization, automation, and enrichment tools in the Cloudflare Threat Intelligence Platform to turn massive telemetry into instant security posture. More can be found here.

See risk, fix risk: introducing Remediation in Cloudflare CASB

Cloudflare CASB Remediation lets security teams go beyond visibility to fix risky file sharing in Microsoft 365 and Google Workspace directly from Cloudflare One, all in just a few clicks. More can be found here.

CXO events and resources

Join us at our **Trust Forward Summit** on Wednesday, March 25, an exclusive event at RSAC, connecting cybersecurity leaders, AI innovators, and technology executives to tackle the most pressing challenges in digital trust and AI-driven innovation.

Ready to swap conference meetings for a bit of fun? On Night 3 of RSAC, join Cloudflare for an exclusive evening designed for unwinding. At our **CxO Casino Night**, connect with fellow CXOs and visionaries in a relaxed, unscripted lounge atmosphere. Best of all? Every hand dealt supports a charitable cause.

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

- Gartner Security & Risk Summit, March 16–17, Sydney, AU
- secIT by Heise, March 18–19, Hannover, DE
- ISACA LA Spring Conference, March 30–31, Los Angeles, CA, US

Find more resources from the CXO team here:
Liz Morton, Field CISO: Modernizing applications for the AI era: Five pillars for frictionless security

Copyright © 2026 Cloudflare, Inc.
101 Townsend Street, San Francisco, CA 94107

www.cloudflare.com | Community | Privacy Policy | Unsubscribe