TAKTIK TECHNOLOGIES

MONTHLY IT/SECURITY BRIEFING

JULY 2026 EDITION

On target, every month: the threats we're tracking, what our technology partners are shipping, and the practical moves that keep your business locked in and protected.

◎ IN THE CROSSHAIRS: TOP CYBER NEWS, LAST 30 DAYS

NATION-STATE ACTIVITY

Nine countries warn: Russian state hackers targeting routers

Cybersecurity agencies from the U.S. and eight allied nations issued a joint advisory that Russian state actors are exploiting vulnerable and poorly configured routers to infiltrate critical infrastructure networks. If your edge devices haven't been patched or hardened lately, now is the time.

CREDENTIAL EXPOSURE

Mega-leaks put billions of passwords back in play

Researchers reported a colossal leak of roughly 24 billion records including usernames and passwords, and separately warned that criminals have compiled a database of about 30,000 working Fortinet logins. Both stories underline the same lesson: assume reused passwords are already compromised and enforce MFA everywhere.

LAW ENFORCEMENT WIN

FBI takes down "Outsider" phishing-as-a-service network

With help from Google and Lumen, the FBI dismantled a China-based phishing-as-a-service operation blamed for nearly $1.9 billion in losses since 2023 — a reminder that phishing remains the most profitable crime on the internet.

AI-POWERED ATTACKS

Attackers are now "vibe-coding" their tooling

Huntress researchers documented an intrusion in which the attacker used an AI-generated PowerShell script to map an entire Active Directory environment after gaining RDP access with stolen credentials. AI is compressing the time from break-in to full network reconnaissance.

PATCH PRIORITIES

Actively exploited flaws: ColdFusion, Exchange, Joomla

CISA flagged active exploitation of a critical Adobe ColdFusion flaw (CVE-2026-48282) and of Joomla form/event extensions used for remote code execution, while an on-prem Microsoft Exchange vulnerability is being triggered through crafted emails. Patch these first if they're in your environment.

BREACH WATCH

Third-party breaches keep biting big brands

Supermarket giant Lidl notified customers across three countries after attackers stole data from a service provider, and a ransomware group claims to hold Deutsche Bank data. Vendor risk is business risk — see FortifyData's update below for tools that help.

◎ PARTNER INTEL

WHAT OUR TECHNOLOGY PARTNERS ANNOUNCED THIS MONTH

CHECK POINT

Check Point will embed OpenAI's frontier cyber models directly into its security products and managed services through the OpenAI cyber partner program, aiming at faster threat prevention and remediation. It also announced an upcoming Amazon Bedrock AgentCore integration, made its Cloud Firewall available on the new AWS European Sovereign Cloud, and achieved FedRAMP and GovRAMP authorization for U.S. public-sector customers.

New Check Point exposure-management research finds critical vulnerabilities have doubled as AI floods security teams with alerts — yet fewer than 1 in 12 truly demand urgent action. Q2 financial results arrive July 30.

METER NETWORKS

Meter launched a $100 million Partner Growth Fund — rebates, spiffs, migration incentives, and MDF for partners building practices on its managed networking platform. Meter was also recognized as a Visionary on the 2026 Gartner Magic Quadrant and announced a strategic partnership with Spectrotel to deliver fully managed, subscription-based enterprise networks end to end.

FORTIFYDATA

Atlanta's own FortifyData rolled out AI-powered enhancements for Continuous Threat Exposure Management (CTEM): a dynamic risk map, automated prioritization, and autonomous remediation planning that charts the fastest path to a stronger risk score. Its new TPRM AI Auditor analyzes vendor SOC 2, HECVAT, and SIG reports in minutes — a timely capability given that roughly 30% of breaches now involve a third party.

BROADVOICE

Broadvoice launched GoEngage and AI Analyst for its GoContact platform: GoEngage handles inbound voice interactions autonomously with a natural cadence, while AI Analyst gives contact-center leaders instant answers to operational questions. Broadvoice research cites up to a 250% return on contact-center AI investments, and the company sponsored Customer Contact Week in Las Vegas, June 22–25.

AWARE FORCE

Aware Force continues to publish twice-monthly, company-branded security awareness content, with recent editions covering AI chat data leakage, tightening cyber-insurance fine print, and the deepfake threats facing schools and families — the only awareness program built to protect employees at work and at home.

THREATMATIC

Threatmatic's lightweight endpoint agent and S/Channel platform deliver real-time Zero Trust enforcement: millisecond policy changes, application and bandwidth control by user, group, or device,

and instant blocking of malware command-and-control traffic. Ask TakTik about a demo of instantaneous ZTNA for your environment.

BEFORE THE BREACH

Before the Breach announces its Cyber Boot Camp.

Want to strengthen your organization's cyber readiness with a hands-on, real-world training experience designed to elevate teams before an incident ever occurs? The Before the Breach Cyber Boot Camp delivers practical defense strategies, threat-response skills, and expert-led sessions that help businesses build a proactive security posture.

BLACKSTONE & CULLEN

Blackstone & Cullen announces Level42: AI-powered requirements management — 60+ modules, one platform.

Level42 sits on top of the AI tools your team already uses and adds the thing they're missing: governance, structure, and a real institutional memory. It captures requirements, maps your process, and flags compliance gaps automatically, instead of living in someone's inbox or a doc nobody updates. Teams using it have seen up to 10x efficiency gains on the same work.

◎ SECURITY & AI TIPS AND TECHNIQUES

◉ HARDEN THE EDGE THIS QUARTER

With state actors actively hunting misconfigured routers, audit every internet-facing device: change default credentials, disable unused remote-management services, update firmware, and log outbound traffic from network gear.

◉ TREAT EVERY PASSWORD AS ALREADY LEAKED

Billions of fresh credentials are circulating. Require phishing-resistant MFA on email, VPN, and admin accounts, deploy a password manager company-wide, and run a quarterly review to kill shared logins and stale accounts from former staff and vendors.

◉ ADD A MONEY-MOVEMENT CALLBACK RULE

AI voice cloning has made "the CEO called me" unreliable. Institute a hard rule: no wire, payroll change, or gift-card purchase happens on the strength of a call, text, or email alone — verify through a second, known-good channel every time.

◉ SET GUARDRAILS ON WORKPLACE AI

Employees are pasting contracts, code, and customer data into chatbots. Publish a one-page AI use policy: approved tools, data that may never leave the building, and a review step before AI-generated content goes to a client. Prefer business-tier AI accounts where your data is not used for training.

◉ VERIFY BEFORE YOU TRUST AI OUTPUT

AI is a force multiplier for defenders too — use it to draft policies, summarize logs, and triage alerts — but keep a human in the loop. Treat AI output like a junior analyst's first draft: useful, fast, and always in need of a review.

◎ TAKTIK NEWS & ANNOUNCEMENTS

FROM THE TAKTIK TEAM

TAKTIK AI GOVERNANCE FRAMEWORK NOW AVAILABLE

TakTik Technologies announces availability of the TakTik AI Governance Framework document. Email sales@taktiktechnologies.com to request a copy.

NEW SERVICE: THIRD-PARTY RISK MANAGEMENT

TakTik announces availability of its Third-Party Risk Management service. Third-party breaches continue to increase and are a real vulnerability to most businesses. Email sales@taktiktechnologies.com to request information about the service or to schedule a 30-minute consultation.

BOOK YOUR Q3 SECURITY REVIEW

Midyear is the perfect time to pressure-test your defenses. Reply to this newsletter or contact your TakTik representative to schedule a complimentary Q3 security posture review.