MAY 2026

REGIONAL THREAT REPORT
EUROPE

STEPHANIE SCHNEIDER

CYBER THREAT
INTELLIGENCE ANALYST

MICHAEL KOSAK

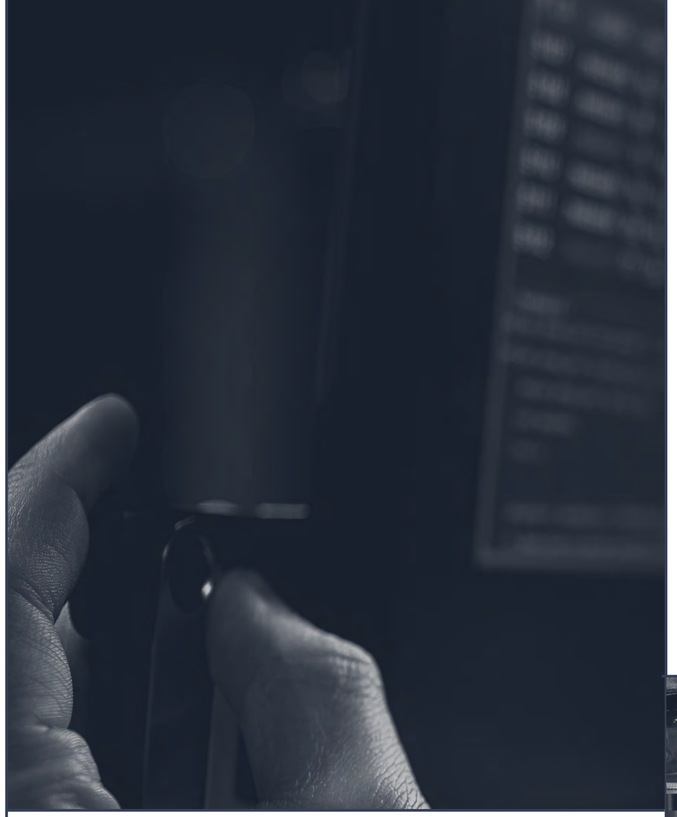
DIRECTOR OF THREAT
INTELLIGENCE

The Regional Threat Report delivers strategic insights from the LastPass Threat Intelligence, Mitigation & Escalation (TIME) Team into the evolving cyber threat landscape across key global markets. Each edition provides a concise, intelligence driven overview of the most significant threats affecting organizations within a specific region, including Europe, Asia-Pacific, and North America.

For more cybersecurity insights, visit the LastPass Threat Intel blog or listen to The Phish Bowl podcast featuring the LastPass TIME team.

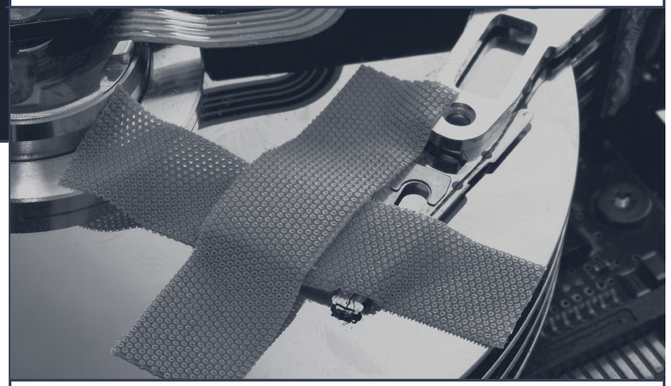
WHAT'S ON TAP THIS MONTH?

Organizations operating in Europe face heightened cyber risk due to dense cross-border supply chains, widespread reliance on shared Software-as-a-Service (SaaS) and cloud platforms, and evolving regulatory requirements. Credential-based attacks impacting a single organization frequently have cascading effects across multiple countries and organizations, increasing both operational disruption and regulatory exposure. Between February and April 2026, cyber activity affecting Europe-based organizations was characterized less by technical intrusion and more by the abuse of valid credentials and trusted access paths.



Across public-sector, telecommunications, SaaS, and manufacturing incidents, adversaries repeatedly gained entry by authenticating successfully — using stolen logins, OAuth tokens, API keys, or third-party access — rather than exploiting software vulnerabilities. This shift enabled attackers to blend into normal business activity, delay detection, and extend impact across interconnected environments.

Ransomware operations during this period reinforced this pattern, often prioritizing data theft and extortion over encryption, which can trigger regulatory, legal, and reputational consequences under GDPR, NIS2, DORA, and sector-specific regulations, even when operational disruption is limited. Operational technology environments remain particularly exposed, not because of increased OT-specific exploitation, but due to legacy systems, limited visibility, and shared identity pathways between IT and OT that attackers can leverage once credentials are compromised.



At the same time, AI-enabled vulnerability discovery is accelerating disclosure rates and compressing remediation timelines, further straining organizations with technical debt and constrained patching windows.

TRIVY SUPPLY CHAIN COMPROMISE WAS THE ROOT CAUSE OF CISCO AND EUROPEAN COMMISSION BREACHES.

Cybercriminal group TeamPCP abused stolen CI/CD secrets and AWS API keys harvested via a compromised open-source security tool (Trivy) to access Cisco's internal systems and customer-linked assets and European Commission cloud environments, which ShinyHunters later leaked.

KEY TAKEAWAYS:

- In March 2026, cybercriminal group TeamPCP executed a large-scale supply-chain intrusion by compromising Aqua Security's Trivy open-source vulnerability scanner after stealing CI/CD credentials from GitHub Actions workflows tied to multiple developer environments. Using these stolen secrets, the actors force-pushed malicious updates to Trivy and reused access to compromise additional developer tools and packages. Each malicious update to Trivy acted as a credential harvesting event, collecting cloud API keys, tokens, and secrets from victim build environments and enabling lateral expansion across technology ecosystems.
- This cascading credential theft directly enabled high-impact secondary breaches, including:
  - At Cisco, where stolen CI/CD and cloud credentials were used to access internal systems, repositories, and customer-linked assets.
  - At the European Commission, where harvested AWS API keys were abused to compromise cloud accounts, resulting in the theft of over 350GB of data, including personal data, email content, and sensitive documents from the Europa.eu platform. At least 29 additional EU institutions were potentially impacted via shared infrastructure. the AWS account, and they were able to access other data.

WHY IT MATTERS:

This incident underscores Europe's growing exposure to credential theft via CI/CD tooling, rather than classic perimeter exploits. Neither incident required exploitation of a zero-day or perimeter vulnerability. Instead, valid credentials obtained upstream through the Trivy supply-chain compromise were sufficient, reinforcing threats posed by identity-driven supply-chain attacks with downstream impact.

SOURCE | SOURCE

SHINYHUNTERS SOCIALLY ENGINEERED ACCESS TO CRM CREDENTIALS TO BREACH MAJOR NETHERLANDS TELECOM.

A breach at a Dutch phone company in early February potentially compromised the personal data of 6.2 million customers, or about a third of the country's population.

KEY TAKEAWAYS:

- *ShinyHunters gained access to the company's customer contact system by posing as IT workers and contacting the customer service desk to acquire legitimate credentials, then exfiltrated and leaked customer information.*
- *The stolen data includes customer names, phone numbers, postal and email addresses, dates of birth, bank account numbers (IBAN), and details of customers' government-issued IDs.*
- *Passwords, call logs, billing information, and scans of identification documents were reportedly not affected. s.*

SOURCE

WHY IT MATTERS:

ShinyHunters recently compromised several entities using similar social engineering tactics by exploiting a combination of human error and overly permissive access settings for employees. This allows an attacker who successfully tricks an employee to gain access to a large amount of data for extortion.

RUSSIAN HACKERS EXPOSED, REVEALING STOLEN CREDENTIALS AND 2FA SECRETS FROM EUROPEAN GOVERNMENTS.

An exposed Russian-backed APT28 (aka Fancy Bear) server revealed thousands of stolen government emails, passwords, and Time-based One-Time Password (TOTP) secrets from NATO-linked European targets.

KEY TAKEAWAYS:

- Security researchers discovered two open server doors previously attributed to Russian-backed APT28 (aka Fancy Bear) to gain insight into the group's long-running credential harvesting campaign via webmail access.
- The campaign aimed to collect intelligence on NATO-aligned countries involved in Russia's war in Ukraine. It targeted Ukraine, Romania, Greece, Bulgaria, Serbia, and North Macedonia.
- Within the open-directory, researchers found exfiltrated government and military emails, 240 sets of stolen credentials including passwords and TOTP 2FA secrets, silent email-forwarding rules, and thousands of contact addresses harvested from victims' address books across multiple targeted countries.
- Separately, other analysts discovered a second exposed open-directory that stored APT28's full command-and-control (C2) source code, additional JavaScript payloads, campaign telemetry logs, and exfiltrated data that provided researchers with a clearer picture of the broader operation.

SOURCE

WHY IT MATTERS:

Nation-state actors continue to capture credentials at scale and reuse them in other cyber operations. One of the most concerning discoveries was APT28's method for silently stealing TOTP-based 2FA secrets from victims who believed their accounts were fully protected. With both the victim's password and TOTP secret secured, APT28 could generate valid authentication codes at any future point, bypassing two-factor protection entirely without ever needing physical access to the victim's device.

VERCEL OAUTH TOKEN ABUSE VIA COMPROMISED AI TOOL CASCADES INTO SAAS RISK.

Vercel, the cloud platform behind Next.js and its millions of weekly npm downloads, was compromised in April by an employee using an unsanctioned AI tool that was hit with Lumma infostealer malware. In April 2026, Vercel — the cloud platform supporting Next.js and widely used across the JavaScript ecosystem — disclosed unauthorized access stemming from abused identity trust within a SaaS environment.

KEY TAKEAWAYS:

- The incident began when an employee used an approved third-party AI tool (Context.ai) that was compromised with Lumma infostealer malware, allowing attackers to exploit delegated SaaS access rather than breach Vercel's infrastructure directly.
- The third-party AI service introduced a malicious OAuth integration that leveraged delegated access to the employee's enterprise Google Workspace account. In other words, attackers piggybacked on the employee's work account through a hidden sign-in connection.
- Once granted, the OAuth authorization provided attackers with ongoing access independent of passwords or multifactor authentication, enabling them to operate using the employee's cloud identity.
- Using this access, the attackers interacted with internal Vercel systems through existing SaaS trust relationships rather than exploiting vulnerabilities or bypassing security controls.
- Although protected secrets were not directly exposed, the attackers accessed lower-classification tokens, keys, and configuration data, prompting precautionary credential rotation.

SOURCE

WHY IT MATTERS:

Hackers exploited exiting SaaS trust relationships without passwords or MFA rather than breaching Vercel's infrastructure directly. This incident shows how attackers can gain access without stealing passwords or breaking in, by abusing trusted app connections that already exist in SaaS environments. Because the access comes from approved applications, suspicious activity can look normal and avoid common security alerts. The key takeaway is that apps and the permissions they receive need the same oversight as user accounts, since they can quietly provide long-lasting access if misused.

FAKE VPN CLIENTS HARVESTING ENTERPRISE CREDENTIALS.

Cybercriminal group Storm-2561 used SEO poisoning to distribute fake VPN installers that silently stole enterprise VPN credentials.

KEY TAKEAWAYS:

- Victims were redirected from search engines to malicious “look-alike” VPN downloads hosted on attacker-controlled websites.
- When users click to download the software, they were redirected to a malicious GitHub repository that’s no longer available that hosted the fake VPN client for direct download.
- The fake VPN software enables credential collection and exfiltration while appearing like a benign VPN client application. The malware harvested credentials and VPN configuration data.

SOURCE

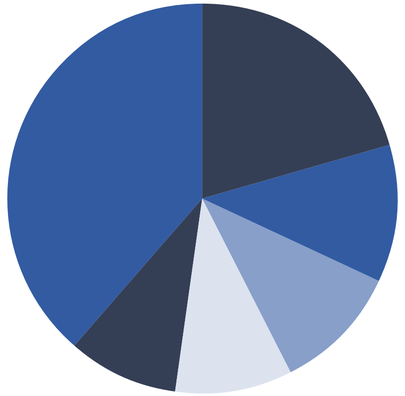
WHY IT MATTERS:

This activity shows how user-initiated trust (search behavior) is now a primary credential-theft vector. Organizations relying heavily on VPN access should prioritize certificate-based authentication, device binding, and conditional access, as stolen passwords alone still unlock networks.

Across incidents in this reporting period—supply-chain compromise, SaaS abuse, telecom breaches, and ransomware—attackers consistently leveraged valid credentials, OAuth tokens, API keys, and CI/CD secrets rather than exploiting vulnerabilities directly. This reflects a broader shift in European threat activity toward identity-first intrusion strategies that blend into normal business operations and delay detection.

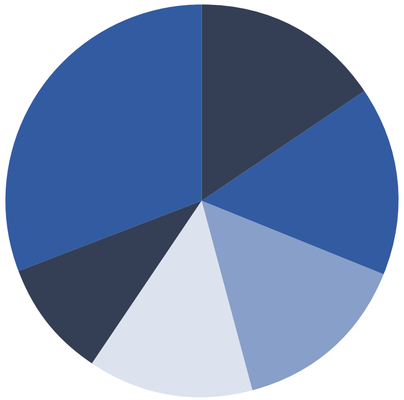
EU-based organizations, incidents involving credential abuse, SaaS data exfiltration, or third-party compromise may trigger reporting and enforcement obligations under GDPR, NIS2, and sector-specific regulations, even if systems remain operational and no ransomware is deployed.

EUROPE RANSOMWARE TRENDS



Most targeted industries:

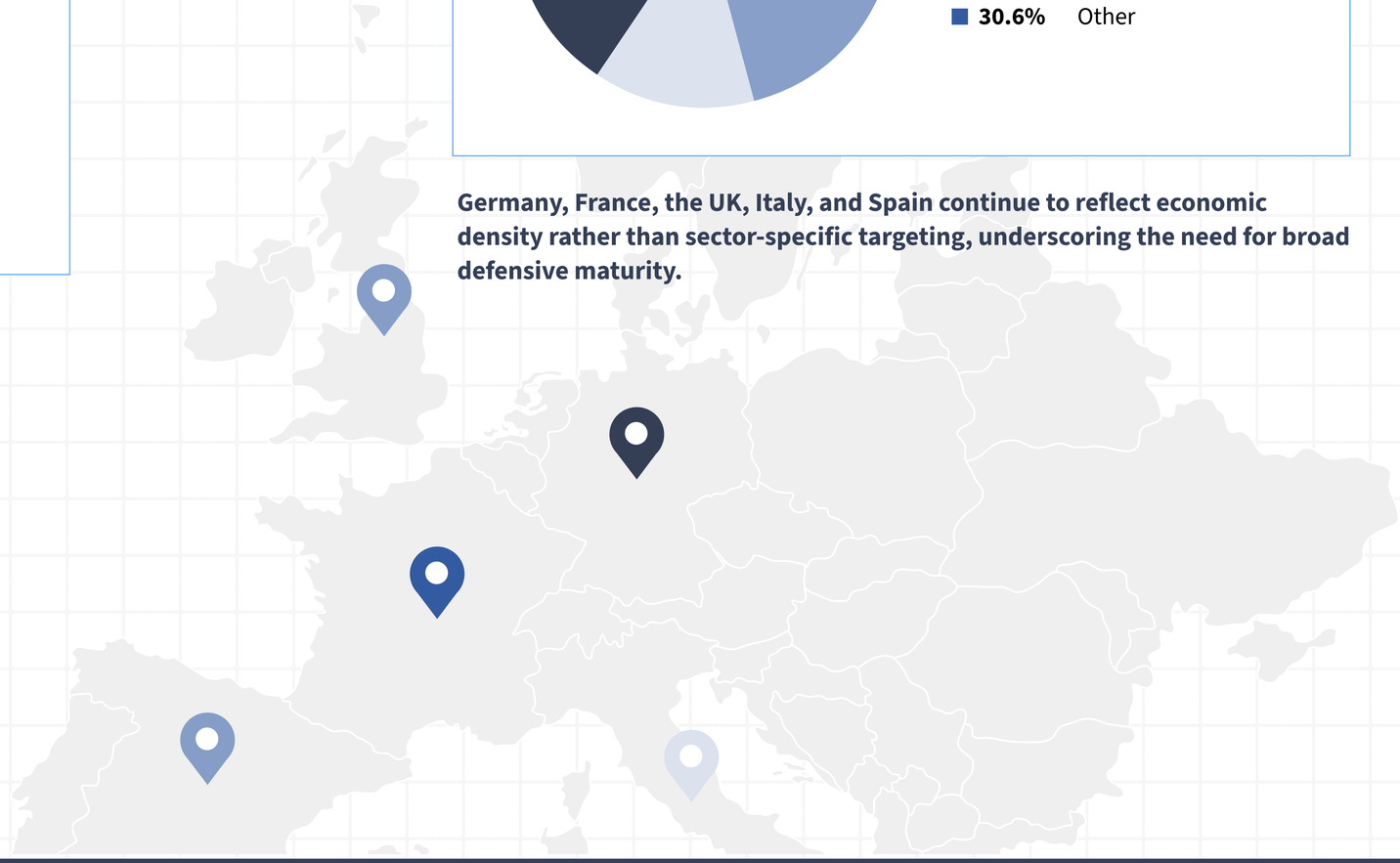
- **20.7%** Manufacturing
- **11.5%** Construction & Engineering
- **10.5%** Technology
- **9.6%** Legal & Professional Services
- **9.2%** Retail
- **38.8%** Other



Most targeted countries:

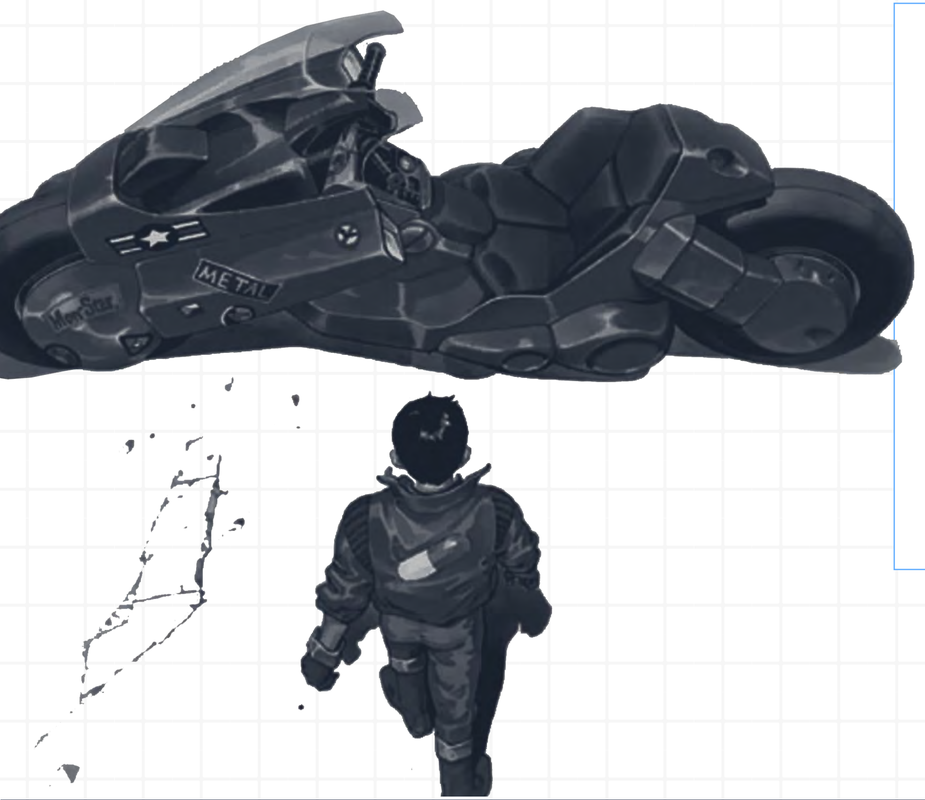
- **15.7%** Germany
- **15.5%** France
- **14.8%** United Kingdom
- **13.5%** Italy
- **9.9%** Spain
- **30.6%** Other

Germany, France, the UK, Italy, and Spain continue to reflect economic density rather than sector-specific targeting, underscoring the need for broad defensive maturity.



MOST ACTIVE GROUPS:

- Qilin
- The Gentlemen
- AKIRA
- LockBit
- Dragonforce



Akira relies on high-speed exploitation of unpatched software and vulnerabilities in public-facing applications. They often partner with Initial Access Brokers (IABs) to obtain VPN credentials, allowing them to conduct stealthy, rapid encryption of large networks within hours of initial entry. In Europe, specifically within the financial sector, Akira has shifted toward data exfiltration-first models. This is compounded by "Shadow AI," or the unauthorized use of AI tools within organizations, which often introduces new, AI-detectable misconfigurations that Akira affiliates are quick to exploit to steal sensitive customer data.

TARGET PROFILE:

Small and medium-sized businesses remain the most frequently targeted in Europe, but downstream impact often reaches larger enterprises through shared suppliers and service providers.

BOTTOM LINE

Ransomware operations in Europe reinforced a clear trend that identity failures, not technical exploits, are the primary enabler, and trust relationships—particularly in SaaS and supply chains—are amplifying risk. Effective prevention now depends as much on identity governance, third-party risk, and behavioral detection as on backups, patching, and endpoint controls.

DEEP DIVE: **AI-ENABLED VULNERABILITY DETECTION IS USHERING IN THE "PATCH WAVE"**

Advances in AI-driven vulnerability discovery are rapidly increasing the number, speed, and scale at which software flaws are identified. As weaknesses in widely deployed technologies are surfaced faster, organizations are facing an unprecedented surge in patches and remediation demands. This compressed discovery-to-exploitation timeline is placing significant strain on defenders, who must now respond faster than traditional patching and risk-management models were designed to support.

KEY POINTS

- The UK's National Cyber Security Centre (NCSC) has warned that AI tools used "by sufficiently skilled and knowledgeable individuals" are increasing the likelihood that vulnerabilities will be identified and weaponized at scale.
- New AI capabilities such as Anthropic's Claude Mythos are accelerating vulnerability discovery to machine speed, effectively reducing exploit development timelines from months to minutes or seconds. In parallel, major technology companies have launched the Project Glasswing initiative to improve coordinated disclosure and protection of critical software ecosystems.
- These effects are already visible in operational security data. Vendors are reporting sharp increases in disclosed vulnerabilities and patches.
  - In April 2026, Microsoft issued more than 160 security fixes during Patch Tuesday — its second-largest monthly release on record — plus an additional ~60 browser-related fixes later the same month. While multiple factors are at play, AI-assisted vulnerability discovery is increasingly cited as a contributor to this surge.
  - In April 2026, Mozilla released Firefox 150, which included fixes for 271 security-sensitive bugs.

WHY THIS MATTERS:

The acceleration of vulnerability discovery is shifting the advantage toward attackers who can automate testing, exploit development, and targeting at scale. At the same time, defenders must contend with years of accumulated technical debt, legacy systems, and uneven patch coverage. Defenders also take more time to operationalize, risk assess, test, and roll out new tech/capabilities, giving a further advantage to attackers. These conditions create a widening gap between discovery and remediation. For sectors already struggling with patch hygiene, such as critical infrastructure, healthcare, and public services, this "patch wave" threatens to overwhelm existing security and operational processes. Organizations that rely on slow, manual, or reactive patching models will struggle to keep up in an environment where weakness discovery now operates at machine speed.

- Defensive strategies must evolve from fixed, monthly patch cycles toward continuous, risk-informed remediation, supported by automation and AI-assisted prioritization.
- Vulnerabilities in old, internet-facing, or end-of-life systems will become increasingly attractive targets as AI lowers the cost of discovery and exploitation.
- The ability to decide what not to patch immediately — based on exposure, exploitability, and business impact — will be as important as patching itself.

- **FOCUS ON EXPOSURE FIRST:** Prioritize patching for internet-facing systems, identity infrastructure, SaaS platforms, VPNs, cloud control planes, and critical operational technology, where newly discovered flaws are most likely to be exploited quickly.
- **MOVE TOWARD AUTOMATION AND CONTINUOUS REMEDIATION:** Enable automatic updates, hot patching, and configuration drift detection wherever feasible to reduce reliance on manual intervention and change windows.
- **ADOPT RISK-BASED PATCH PRIORITIZATION:** Incorporate threat intelligence, exploit availability, active scanning data, and asset criticality to determine which vulnerabilities require immediate action versus monitored acceptance.
- **REDUCE LONG-TERM TECHNICAL DEBT:** Identify and accelerate replacement of legacy and end-of-life systems that cannot be patched or monitored effectively, as these will increasingly represent systemic risk.
- **STRENGTHEN IDENTITY AND SAAS HYGIENE:** Ensure patching and remediation efforts extend to SaaS configurations, identity providers, OAuth applications, and cloud management tools, which are often updated outside traditional IT processes.
- **PREPARE FOR SURGE CONDITIONS:** Update incident response and change-management plans to account for high-volume patch scenarios, including staffing, vendor coordination, and rollback procedures.