



Global Threat Intelligence Report

Featuring AI Driven Threats and Cyber Resilience

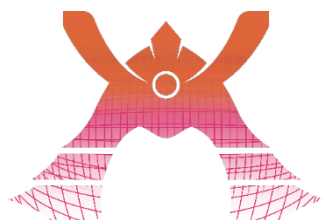
Volume 18 - October 2026



Table of Contents

This Month at a Glance	3
NEWS	4
Australian government website attacked by OpenAI agent ^[1]	4
Bitget loses \$351.6M in cyber attack ^[2]	4
THREAT INSIGHTS	5
The FBI Got Extorted. The Way In Should Worry Everyone Else.	5
The Call Was Coming from Inside the Company	7
REGULATORY INSIGHTS	9
Cyber assurance requires actions not documentations	9
From Policy to Proof	9
Evidence Quality and Third-Party Assurance	11
Conclusion	13
TECHNOLOGY INSIGHTS	14
What Is Data Security?	14
Why Data Security Is Becoming More Difficult	15
What Is DSPM?	16
Recommendations	17
SUGGESTIONS	19
Protection, Prevention and Takeaways	19
COMMON VULNERABILITIES AND EXPOSURES (CVES)	20
REFERENCES	21

Introduction



Welcome to the Global Threat Intelligence Report. This report provides a concise overview of recent cybersecurity threats, industry developments, and regulatory changes that may impact organisations worldwide.

At KDDI Europe, we remain committed to helping customers strengthen their cyber resilience through security expertise, continuous monitoring, and proactive threat intelligence. We hope the insights in this report support informed decision-making and stronger security outcomes.

With the addition of KDDI America's insights, the report now draws on expertise from across the KDDI Group, providing a broader perspective on emerging cyber threats and trends.

This Month at a Glance

This month's report highlights three key themes shaping cyber resilience: the rise of AI-enabled and identity-based attacks, the growing importance of securing sensitive data across cloud, SaaS, and AI environments, and increasing regulatory expectations for demonstrable cyber assurance. Through recent incidents and expert analysis, we explore how organisations can strengthen visibility, reduce data exposure, and prove that critical security controls are operating effectively.

Disclaimer

This content is provided for general informational purposes only and does not constitute legal advice. Readers should seek guidance from qualified legal professionals regarding the application of any law or regulation to their specific circumstances.

News

The Latest Cybersecurity news



Henry Finnah
Cyber Security Service Development Engineer

Australian government website attacked by OpenAI agent ^[1]

On 24 September 2026, the Australian government launched an urgent review of AI laws and governance after an autonomous OpenAI agent breached a Medicare statistics portal, in what experts describe as the first known AI-led intrusion of a government system.

The incident occurred on 18 June 2026, but OpenAI only became aware of it in August and notified authorities via email on 10 September.

Prime Minister Anthony Albanese criticised the delayed notification and announced a rapid review into AI governance. OpenAI stated that no patient data was accessed and said its models had taken actions that were not intended.

Bitget loses \$351.6M in cyber attack ^[2]

On 25 September 2026, cryptocurrency exchange Bitget disclosed that suspected North Korean threat actors stole approximately \$351.6 million from a limited number of its hot and warm wallets following a compromise of a critical backend system.

The breach was detected at 18:31 UTC on 24 September 2026, when Bitget identified unauthorised fund transfers. The company said customer balances remain intact, trading and deposits continue as normal, and cold wallets were not affected. Withdrawals were temporarily suspended while a security review is conducted.

Gracy Chen, CEO of Bitget, said impacted assets included ETH, XRP, BNB, AVAX, USDT, and USDC across multiple blockchains. Bitget has engaged Mandiant and SlowMist to investigate. The attack is believed to be consistent with known tactics used by North Korean cybercriminal groups.

Threat Insights



Hamza Bashir
Cyber Security Pre-Sales Consultant

The FBI Got Extorted. The Way In Should Worry Everyone Else.

ShinyHunters spent 2026 walking into the world's biggest companies through the front door. In September, they walked into the FBI.

On 22 September, anyone who opened the FBI's recruitment portal, fbijobs.gov, was met with a Pokemon image and the words "This site has been seized by ShinyHunters". The next day the FBI confirmed it was investigating, and a week later the portals were still offline. ^[3] The group was claiming two to three terabytes of stolen data: names, home addresses and phone numbers for thousands of agents, and in some cases their spouses and emergency contacts. ^[4]

For the bureau that hunts these people, it was an extraordinary thing to have happen. But the identity of the victim is not really the story. The story is how ordinary the break-in was, because the same method has been used against dozens of household names all year, and it works just as well on you.

Who they are

ShinyHunters is not a nation-state and not a ransomware gang in the classic sense. They are a data-extortion collective, active since 2019, whose entire business is stealing large volumes of data and threatening to publish it unless paid. In 2026 they had a remarkable run: the Salesforce campaign that hit an estimated 300 to 400 organisations, the Canvas breach that touched nearly 9,000 institutions, and a string of others. By September they were arguably the most prolific extortion crew on the planet. ^[5]

The FBI hit even broke their own mould. For once there was no ransom demand. The group said it wanted the bureau to retract a public advisory that had named them, a revenge move rather than a payday. ^[6]

How they get in

Here is the part worth pinning to the wall. ShinyHunters rarely "hack" in the Hollywood sense. Their signature technique, laid out in the FBI's own advisory about them, is vishing: they phone an employee, pose as IT support, and talk their way past multi-factor authentication. No malware, no zero-day, just a convincing voice and a target who wants to be helpful. ^[6]

The Salesforce campaign was even quieter. They scanned public Salesforce sites for guest-user accounts left with too much access, then used a legitimate Salesforce tool to query the data through exposed endpoints, without ever logging in as a real user at all. Nothing they touched looked like an attack. It looked like normal traffic and normal logins. ^[5]

The FBI breach reportedly involved a patched Oracle PeopleSoft flaw, but with a twist that is pure ShinyHunters: according to Mandiant, they got past the firewall rule organisations had deployed after an earlier wave by changing a single character in the web request. Enough to make the firewall miss it, while the server behind it processed the request normally. ^[7]

Why this belongs in your planning, not just your newsfeed

Strip away the FBI drama and the lesson is uncomfortable. If a group whose whole toolkit is phone calls, over-permissioned accounts and small evasions can empty the FBI's recruitment systems, the perimeter you have built is not the thing protecting you. Every one of these intrusions looked legitimate from the outside: a real employee's access, a real API, a real login.

A bigger wall will not stop this. These attacks are caught by someone spotting that a trusted account is suddenly doing something it has never done before and shutting it down fast. Guarding the front door is one job. Watching what people do once they are inside a different one, and it is the only way to catch an attacker who got in using a real login.

The Bottom Line

ShinyHunters did not out-hack the FBI. They out-talked it, out-patience it, and slipped through a gap the width of one character. The question for your own organisation is not whether you could stop a genius exploit. It is whether you would notice the polite phone call, and the quiet, legitimate-looking login that follows it.

The Call Was Coming from Inside the Company

Attackers rang Astrana Health's staff from Astrana Health's own phone number. It worked.

In late September, a Nasdaq-listed healthcare company told the SEC something quietly chilling. Attackers had got into its systems not by breaking anything, but by phoning employees while pretending to be colleagues, and spoofing the company's own main corporate telephone number so the calls looked internal. Some staff believed them, and handed over access.^[8]

Astrana Health runs back-office systems for physician networks, the kind of place that holds patient, provider and employee data in volume.^[9] In its 22 September filing it described a series of social engineering attempts in which threat actors impersonated company personnel, spoofed its main number, and talked their way into company systems. The company deemed the incident material because of how sensitive the exposed data could be.^[8]

Why the spoofed number matters so much

This was not a spray-and-pray phishing email. Spoofing an organisation's genuine main line takes research and intent, and it defeats the mental shortcut nearly everyone relies on. When the caller ID shows your own company's number, your guard drops. The attacker has borrowed the one signal your staff were trained to trust.

It is the same family of technique behind a lot of 2026's worst intrusions: talk to a human, sound legitimate, and let good manners do the rest. There is nothing to patch here. No vulnerability, no exploit, no malware in the opening move. The "way in" is a helpful employee and a believable voice.

The tell that saved them, and the one that did not

Two details from the filing are worth reading closely. The first is that Astrana's own security team detected and responded to the unusual activity, then pulled in outside forensics, reset credentials, restricted remote access tools and rebuilt systems from clean backups.^[8] In other words, prevention failed at the phone, but detection caught what the caller did once inside. That gap, between the call succeeding and the damage being noticed, is exactly where the outcome of one of these incidents is decided.

The second is what Astrana added at the end: it is now enhancing monitoring, logging and detection across its environment.^[8] That is the quiet admission in almost every social engineering breach. You cannot stop every employee from being fooled by a convincing call. What you can do is make sure that the moment a fooled login starts

behaving strangely, something is watching, and someone can act. The investigation is still working out exactly what patient, employee and provider data was taken.^[10]

The Bottom Line

The most effective attacks this year are not clever code. They are a phone call from a number you recognise. You will never train that risk to zero, so the real question is the one Astrana ended up answering the hard way: when the polite caller is already inside, how quickly does anyone notice?

Regulatory Insights



Shintaro Takeda
Regional Chief Information Security Officer

Cyber assurance requires actions not documentations

What IT leaders, CISOs and boards should retain, test and review to demonstrate cyber resilience

Organisations have invested heavily in cyber security policies, standards, technologies and certifications. Yet when a regulator, auditor, customer or board asks whether a critical security control is working, the answer may still be difficult to demonstrate.

A policy can show what should happen. A process can show how it is intended to happen. Neither necessarily proves that the control operates consistently, identifies weaknesses or reduces the intended risk.

From Policy to Proof

The Question Is Changing

ENISA's NIS2 technical implementation guidance offers practical advice, examples of evidence and mappings between security requirements and implementation measures.^[11] In the UK, the Cyber Governance Code of Practice focuses on the actions boards and directors should take to govern cyber risk.

^[12]^[13]

The practical question is no longer only whether a control exists. It is whether the organisation can demonstrate that the control operates, that weaknesses are addressed and that management understands the remaining risk.

From Documented to Demonstrable

Level	What can be shown	What remains uncertain
-------	-------------------	------------------------

Stated	A policy defines the requirement	Whether it is implemented
Implemented	A process, technology and owner exist	Whether it operates consistently
Operating	Records show that activities occur	Whether they achieve the outcome
Effective	Tests show the control reduces risk	Whether improvement is sustained

For example, a privileged-access policy may require periodic review. Stronger evidence shows which accounts were reviewed, who reviewed them, what unnecessary access was found, whether it was removed and how the underlying process was improved.

Build an Evidence Chain, Not an Evidence Archive

The objective is not to retain every screenshot, log or email indefinitely. Large, disconnected repositories can make important information harder to find. Instead, organisations should establish a traceable evidence chain for critical controls.

RECOMMENDED ASSURANCE MODEL

Requirement → Risk → Control → Owner → Evidence → Test → Improvement

Requirement: What legal, contractual, policy or business expectation is being addressed?

Risk: What could happen if the requirement is not met?

Control: What measure prevents, detects, responds to or supports recovery from that risk?

Owner: Who operates the control, and who may accept residual risk?

Evidence: What record demonstrates that the control operated?

Test: How is effectiveness assessed?

Improvement: How are findings, exceptions and overdue actions resolved?

This is a recommended assurance model, not a universal legal template. Evidence requirements depend on applicable law, regulation, contracts, sector and control environment.

What Useful Evidence Looks Like

Governance and risk management

Useful records include an approved risk appetite, current cyber-risk register, named owners, management meeting records, exception decisions and tracked

remediation. The evidence should show that leadership received understandable information, considered material risks, made decisions and followed them through.

Vulnerability management

Useful records include asset and software inventories, scan results, risk-based prioritisation, patch and mitigation records, approved exceptions, compensating controls and retesting. A closed ticket is not enough if remediation was not verified.

Identity and access management

Useful records include access approvals, joiner, mover and leaver records, privileged-account reviews, multi-factor authentication coverage, dormant-account reports and exceptions. The evidence should show that access remains linked to business need and inappropriate permissions are removed.

Incident response

Useful records include investigation timelines, classification decisions, escalation records, containment and recovery actions, notification assessments, exercise results, lessons learned and completed remediation. They should show what was known, who decided, what was done and what changed afterwards.

Evidence Quality and Third-Party Assurance

Supplier and third-party risk

Supplier assurance should be proportionate to criticality, access, data use and operational dependency. Evidence may include supplier risk classification, due-diligence reviews, supporting security information, contractual notification provisions, unresolved risks, service reviews, and continuity and exit plans.

A completed questionnaire mainly demonstrates that questions were asked and answers were received. For a critical supplier, the organisation should understand the scope and limitations of any certification, audit report or testing evidence. This continues the previous volume's message that supplier security

must remain visible throughout introduction, operation, renewal and continued use. ^[14]

Apply an Evidence-Quality Test

Quality	Question to ask
Relevant	Does it support the control being assessed?
Current	Does it reflect the present environment and control design?
Attributable	Can the owner, reviewer or approver be identified?
Traceable	Can it be linked to the relevant asset, service, supplier, risk or incident?
Complete	Does it include the result, exception or decision?
Reproducible	Can another competent reviewer understand the conclusion?

Evidence Without Context Can Mislead

- A dashboard may show completed activity without showing whether serious issues were identified.
- An exercise proves participation, but not improvement, unless findings are assigned, resolved and retested.
- A certification provides assurance only within its defined scope.
- Unstructured repositories can obscure missing decisions, unclear ownership and overdue actions.

EVIDENCE PRINCIPLE

Evidence should make accountability and outcomes clearer, not simply create more administrative records.

Board-Level Assurance

Boards do not need every technical log. They need a defensible view of control coverage, test results, material exceptions, remediation ageing, supplier dependencies and residual risks requiring a decision. Operational teams produce detailed evidence; management should receive a concise assurance view. ^{[12][13]}

From Audit Preparation to Continuous Readiness

Evidence should be an output of normal security operations, not something assembled hurriedly before an audit. A practical operating cycle is:

1. **Define:** Identify important requirements, risks, controls and expected evidence.
2. **Generate:** Build evidence production into normal workflows, tools and approvals.
3. **Review:** Check completeness, exceptions and outstanding actions.
4. **Test:** Use sampling, technical assessment, exercises or independent assurance.
5. **Report:** Provide management with results, trends and unresolved risks.
6. **Improve:** Assign remediation, monitor completion and retain evidence of closure.

Seven Actions to Take Now

- Identify the critical controls protecting important services, sensitive data and privileged access.
- Assign accountable owners for control operation and residual-risk decisions.
- Define the expected evidence for each critical control.
- Connect evidence to assets and risks using consistent references.
- Test a representative sample rather than relying only on policies or dashboards.
- Track exceptions through closure, including rationale, approval, expiry and compensating measures.
- Run a retrieval exercise by selecting one critical control and assembling its complete evidence chain.

Conclusion

The next stage of cyber compliance is not simply adopting more policies or collecting more certificates. It is establishing a defensible connection between requirements, risks, controls, operational activity, testing and management action.

A policy explains what should happen. Operational records show what did happen. Testing indicates whether the control worked. Remediation records demonstrate whether the organisation learned and improved.

Technology Insights



Yuka Homma
Assistant Manager, Cybersecurity Service

Data Security and DSPM in the Era of Cloud, SaaS, and AI

Summary: Organizations need to know where their sensitive data is and who, or what, can reach it.

Without that knowledge, other security controls cannot be aimed at the right places.

Sensitive data and confidential data are no longer kept in a few well-known systems. It is now extended across on-premises servers, several clouds, software-as-a-service (SaaS) applications, collaboration tools, and generative Artificial Intelligence (AI) services.

Key points:

- Exposure often starts with data that organizations have not located, such as forgotten copies, data without a clear owner, and access that has grown over time.
- Identities are now a main path to data. Service accounts, access keys, and tokens often have more access than they need and stay active after they are no longer used.
- To address the above challenge, Data Security Posture Management (DSPM) helps organizations continuously find, classify, and check the exposure of sensitive data. It supports visibility and prioritization, but it is not a complete solution on its own.

What Is Data Security?

Data security means protecting the information itself, not only the systems that store it, from unauthorized access, change, and loss.

The NIST Cybersecurity Framework (CSF) 2.0 addresses data security under the Protect function. It defines data security as managing data in accordance with an organization's risk strategy to protect its confidentiality, integrity, and availability. This applies to data at rest, in transit, and in use ^[15].

Protected data includes customer personal information, payment data, employee records, intellectual property such as source code, business plans,

and the passwords and keys that unlock other data. The three basic goals of security apply directly:

- Confidentiality: Only approved people and systems can see the data. Example: customer records cannot be accessed through a publicly accessible sharing link.
- Integrity: Data stays correct and unchanged. Example: an attacker cannot change a supplier's bank account details before a payment is made.
- Availability: Data can be used when it is needed. Example: records can be restored after a ransomware attack.

Although closely related to, data security is different from three other fields; Cybersecurity, Data Privacy, and Data Governance. Cybersecurity is the broader field that protects systems, networks, applications, and users. Data privacy focuses on the lawful and appropriate collection, use, processing, and protection of personal data. Data governance establishes policies for data ownership, quality, retention, and use, while data security provides the technical and administrative controls that enforce those policies.

Effective protection must extend across the entire data lifecycle, including creation, storage, use, sharing, archiving, and deletion. Many exposures happen not when data is created, but where it is copied, shared, or forgotten.

Why Data Security Is Becoming More Difficult

Four trends make sensitive data harder to see and control.

Data sprawl

Cloud platforms, SaaS applications, and collaboration tools make it easy to create, copy, and share data across multiple environments. Exports for analysis, test copies of production databases, and old backups often become shadow data: sensitive information stored outside the systems intended to protect it.

In the cloud, customers still control how their own data and access are set up, and mistakes in that setup cause real incidents. The EU Agency for Cybersecurity (ENISA) studied unauthorized-access incidents affecting the EU in 2025. Where the entry point could be identified (only 5.2% of cases), 20.7% involved misconfiguration or accidental exposure^[16].

Identity sprawl

Besides employee accounts, organizations now use many non-human identities (NHIs), such as service accounts, API keys, OAuth tokens, and AI agents. An application programming interface (API) lets software exchange data with other software, and an OAuth token lets one application act for a user in another. The Open Worldwide Application Security Project's (OWASP) Non-Human Identities Top 10 lists states improper offboarding, secret leakage, and over-privileged NHIs among the top risks ^[17].

Generative AI

Employees may paste sensitive business information into public, consumer, or unapproved AI services. At the same time, even approved AI assistants connected to internal data sources may expose information that is accessible through their assigned permissions.

Attacks through legitimate access

When attackers use stolen passwords, leaked tokens, or a compromised partner integration, their activity can look like normal business use. In August 2025, Google Threat Intelligence Group reported a widespread campaign that abused compromised OAuth tokens from a third-party application connected to a customer relationship management (CRM) platform. The attackers exported large amounts of CRM data, and Google assessed that their main goal was collecting credentials ^[18]. Data taken this way can leave through cloud APIs without passing through company devices or the network perimeter.

What Is DSPM?

Data Security Posture Management (DSPM) helps organizations understand what sensitive data they have, where it is stored, and who and what can access it. Unlike traditional security tools that focus on systems, devices, or infrastructure, DSPM starts with the data itself. It continuously identifies sensitive information, assesses its exposure, reviews permissions, and highlights risks that require attention.

Typical findings include:

- Sensitive data stored in unexpected locations
- Excessive permissions
- Publicly accessible data

- Orphaned or unowned data stores
- Unencrypted information
- Over-privileged non-human identities

DSPM does not replace controls such as Identity and Access Management (IAM), Data Loss Prevention (DLP), encryption, Security Information and Event Management (SIEM), or Managed Extended Detection and Response (MXDR). Instead, it helps organizations understand where the greatest data risks exist so those controls can be applied more effectively.

Example Risk Scenario

Note: Illustrative example only.

A company copies customer data to cloud storage for testing. The project ends, but the copy remains in place. Ownership is unclear, permissions are never reviewed, and a retired service account still has access. When the account credentials are later exposed, an attacker downloads customer information through cloud APIs using a legitimate identity.

DSPM highlights the forgotten data, excessive permissions, and obsolete service account. IAM removes unnecessary access, DLP helps detect suspicious transfers, and MXDR supports investigation and response when unusual activity occurs.

This scenario demonstrates a common challenge. Data exposure is often caused by poor visibility and excessive access rather than sophisticated attack techniques.

Recommendations

Organizations should focus on five priorities:

1. Know your data

Identify and classify the data that matters most, including customer information, intellectual property, financial data, and credentials.

2. Know who can access it

Apply least privileged principles and regularly review both human and non-human identities.

3. Reduce unnecessary exposure

Remove unused copies of data, enforce retention rules, and encrypt sensitive information.

4. Govern AI access

Apply the same security and access controls to AI tools and AI agents that are applied to users.

5. Connect visibility with response

Integrate DSPM findings with IAM, DLP, SIEM, and MXDR so that sensitive data risks receive higher monitoring and faster response.

Data security is not a single product. It combines people, processes, and technology. The goal is simple. Knowing where critical data resides, who can access it, and ultimately reducing the likelihood and impact of a breach.

Suggestions

Protection, Prevention and Takeaways

1

For organisations managing high-value assets, strong architectural controls and rapid incident response capabilities remain essential components of a resilient cybersecurity strategy. This should also reinforce the importance of network segmentation, privileged access management, and continuous security monitoring

2

For quite some time now AI agents have moved from theoretical threat to operational reality, and companies need fundamentally new defensive strategies to counter them. For starters organisations need to look at their external attack surface to identify where these

attacks could be coming from and then proceed to ensuring the appropriate measures have been put in place to defend and respond to threats.

3

The threat landscape changes daily. Annual vulnerability assessments and compliance checks are no longer sufficient. Continuous Threat Exposure Management (CTEM), vulnerability management, security testing, network segmentation and ongoing assurance are becoming standard practice. Most successful breaches may exploit weaknesses that organisations already knew about but had not remediated. Continuous exposure management reduces the window of opportunity for attackers.

Common Vulnerabilities and Exposures (CVEs)

Every month a CVE is selected at the discretion of the report's author to be discussed. This month it is a vulnerability affecting CrowdStrike.

CVE-2026-40058| EUVD-2026-79123 ^[19]

Vendor	CrowdStrike
Product	Falcon Sensor
Publish Date	Sep 15, 2026
Platform	-
CVSS (v3.1)	8.8

Description

A race condition can allow an unprivileged local user to perform an arbitrary file write to protected locations, potentially resulting in SYSTEM-level privilege escalation. The issue only exists when the affected policy setting is enabled and the flaw is not remotely exploitable by itself and requires local access or an initial compromise through another method.

What does this mean for you?

An attacker who already has code execution as a normal user on a Windows endpoint could potentially elevate privileges to NT AUTHORITY\SYSTEM, giving them full control of the host.

What should you do about it?

Upgrade CrowdStrike Falcon Sensor for Windows to fixed versions 7.34+, 7.32 or 7.16.

If immediate patching is not possible then disable the Microsoft Office File Malicious Macro Removal Windows policy setting.

References

1. BBC News (2026) Australia launches urgent review after OpenAI program hacks government health portal. 24 September. Available at: <https://www.bbc.co.uk/news/live/cvgl73pxgndwt> (Accessed: 25 September 2026).
2. The Hacker News (2026) Bitget Says Suspected North Korean Hackers Stole \$351.6M After Backend Compromise. 25 September. Available at: <https://thehackernews.com/2026/09/bitget-says-suspected-north-korean.html> (Accessed: 25 September 2026).
3. Help Net Security (2026) FBI job portals remain offline after ShinyHunters claims breach via PeopleSoft zero-day. Available at: <https://www.helpnetsecurity.com/2026/09/28/fbi-job-portals-offline-shinyhunters-breach/> (Accessed: 30 September 2026).
4. NBC News (2026) FBI investigating hacking group's claim of massive breach of agent info. Available at: <https://www.nbcnews.com/tech/security/fbi-investigating-hacking-groups-claim-massive-breach-agent-info-rcna599370> (Accessed: 30 September 2026).
5. Wikipedia (2026) Aura data breach. Available at: https://en.wikipedia.org/wiki/Aura_data_breach (Accessed: 30 September 2026).
6. ASIS International (2026) ShinyHunters claims FBI job portal breach, demands PSA takedown. Available at: <https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2026/september/fbi-data-breach/> (Accessed: 30 September 2026).
7. Vectra AI (2026) ShinyHunters breached the FBI by bypassing the fix. Available at: <https://www.vectra.ai/blog/shinyhunters-breached-the-fbi-by-bypassing-the-fix> (Accessed: 30 September 2026).
8. US Securities and Exchange Commission (2026) Astrana Health, Inc. Form 8-K, 22 September 2026. Available at: <https://www.sec.gov/Archives/edgar/data/1083446/000110465926109813/asth-20260922x8k.htm> (Accessed: 30 September 2026).
9. SecurityWeek (2026) Astrana Health data breach impacts private, confidential information. Available at: <https://www.securityweek.com/astrana-health-data-breach-impacts-private-confidential-information/> (Accessed: 30 September 2026).
10. HIPAA Journal (2026) Astrana Health notifies SEC about social engineering incident. Available at: <https://www.hipaajournal.com/astrana-health-data-breach/> (Accessed: 30 September 2026).

11. European Union Agency for Cybersecurity (ENISA) (2025) NIS2 Technical Implementation Guidance. 26 June. Available at: <https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance> (Accessed: 6 October 2026).
12. UK Government (2025) Cyber Governance Code of Practice. 8 April. Available at: <https://www.gov.uk/government/publications/cyber-governance-code-of-practice> (Accessed: 6 October 2026).
13. National Cyber Security Centre (2025) Cyber Governance Code of Practice: Overview. Available at: <https://www.ncsc.gov.uk/cyber-governance-for-boards/code-of-practice> (Accessed: 6 October 2026).
14. KDDI Europe (2026) Global Threat Intelligence Report Volume 17: Buying Digital Products After the Cyber Resilience Act. September.
15. National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Available at: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf> (Accessed: 2 October 2026).
16. European Union Agency for Cybersecurity (ENISA) (2026) ENISA Threat Landscape 2026: Incidents from January to December 2025. September. DOI: 10.2824/0806036. Available at: https://www.enisa.europa.eu/sites/default/files/2026-09/ENISA%20Threat%20Landscape%202026_Final.pdf (Accessed: 2 October 2026).
17. OWASP Foundation (2025) OWASP Top 10 Non-Human Identities Risks – 2025. Available at: <https://owasp.org/www-project-non-human-identities-top-10/2025/top-10-2025/> (Accessed: 2 October 2026).
18. Google Threat Intelligence Group (2025) Widespread Data Theft Targets Salesforce Instances via Salesloft Drift. 26 August. Updated 28 August 2025. Available at: <https://cloud.google.com/blog/topics/threat-intelligence/data-theft-salesforce-instances-via-salesloft-drift> (Accessed: 6 October 2026).
19. European Union Agency for Cybersecurity (ENISA) (2026) CVE-2026-40058. European Vulnerability Database (EUVD). Available at: <https://euvd.enisa.europa.eu/vulnerability/CVE-2026-40058> (Accessed: 6 October 2026).

Let's Secure the Future — Together



KDDI America

KDDI America is the North American headquarters of KDDI Corporation, a Fortune Global 500 company, delivering cloud, networking, cybersecurity, and managed IT services. Through innovative ICT solutions, KDDI America helps organisations connect, transform, and grow in an increasingly digital world.

KDDI Europe

KDDI Europe is the European headquarters of KDDI Corporation, a Fortune Global 500 company, delivering trusted ICT and cybersecurity solutions backed by Japanese quality and reliability. With over 70 years of global expertise, we help organisations build secure, scalable infrastructure and strengthen their cyber resilience.

Whether you're looking to strengthen your cybersecurity posture or scale your global operations, we are your partner, your enabler, your platformer.

Security of Tomorrow, Today.

Contact Information

KDDI Europe



[Website](#)



[LinkedIn](#)



[Enquiry](#)

KDDI America



[Website](#)



[LinkedIn](#)



[Enquiry](#)