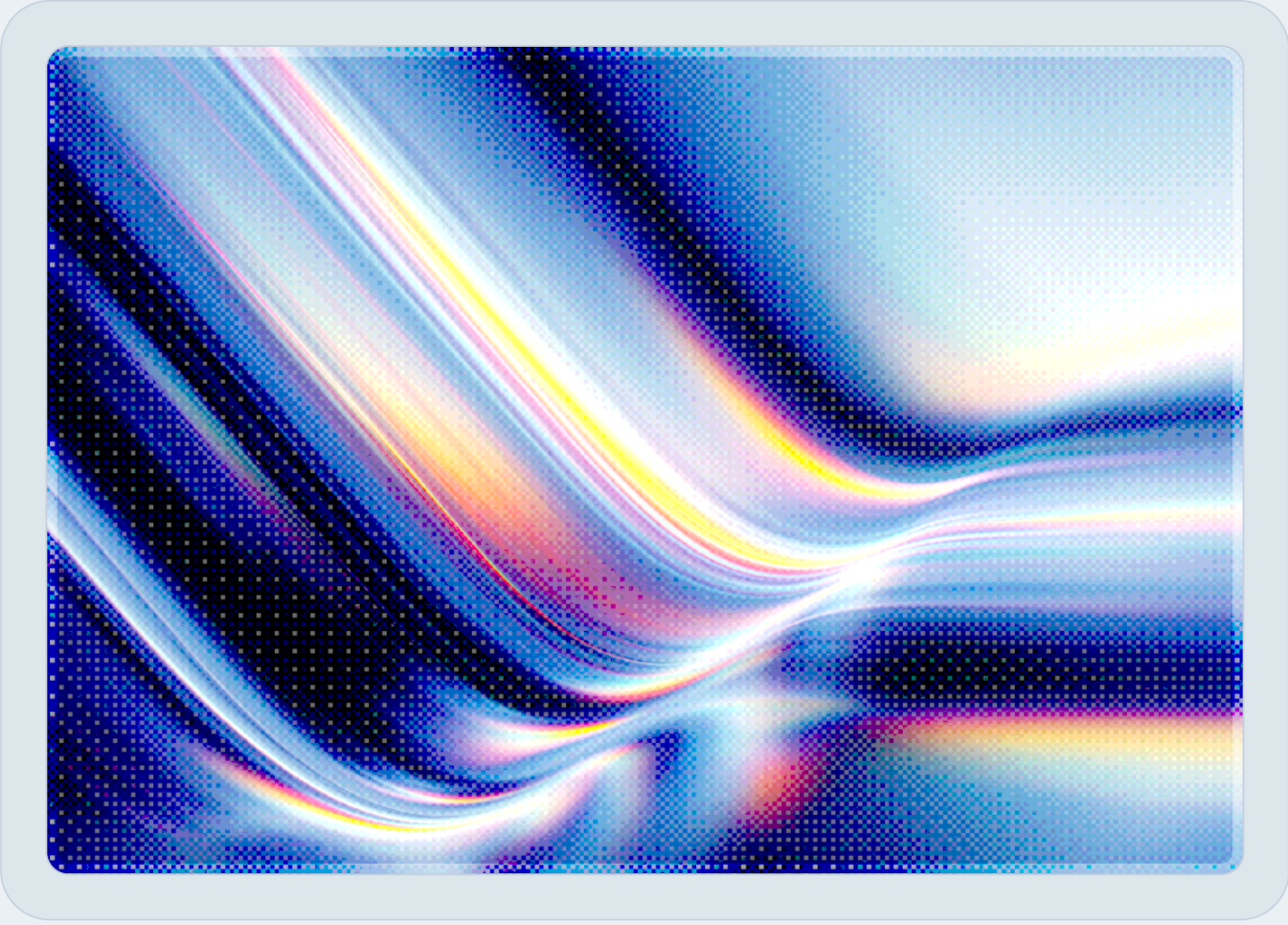
CSAI Foundation | Cloud Security Alliance

ENISA 2026: Dependencies Turn EU Cyber Risk Systemic

2026-09-26

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

- ENISA's Threat Landscape 2026, published 22 September 2026 and covering 8,257 incidents recorded between January and December 2025, concludes that the defining feature of the EU threat environment is not a new attack type but the growing interconnectedness of digital ecosystems, where a single compromise of a shared dependency now routinely cascades into large-scale, multi-organization impact [1].
- Vulnerability exploitation enabled 60.4% of unauthorized-access incidents where an intrusion vector could be identified, against a backdrop of more than 48,000 newly published CVEs in 2025, a 22% year-over-year increase, suggesting defenders face a widening and faster-moving exposure surface even before dependency effects are considered [1].
- Software supply-chain compromises, illustrated by the Shai-Hulud npm worm and a ransomware attack on a single French wealth-management software provider that disrupted banks and advisers for days, illustrate that targeting one upstream provider can be an efficient way for cybercriminals to reach many downstream victims at once [1].
- Financially motivated cybercrime (29.3% of all recorded incidents) and ideology-driven hacktivism (57.3%) remain the largest categories by volume, while ENISA assesses that AI is highly likely to directly enable an increasing number of attack kill-chain phases during 2026, including early experimentation with human-out-of-the-loop operations [1].
- Public administration remained the most targeted EU sector (31.8% of events), and ENISA's companion NIS360 assessment flags railway and maritime transport as sitting in a "risk zone" where cybersecurity maturity lags the criticality of the services these sectors provide, reinforcing that dependency exposure is unevenly distributed across the economy [1] [5].

Background

The European Union Agency for Cybersecurity (ENISA) released the ninth edition of its annual Threat Landscape report on 22 September 2026, shifting the reporting period to the full calendar year and analyzing 8,257 incidents drawn from open-source reporting, EU Member State input, and the ENISA Cyber Partnership Programme [1]. The report itself cautions that it should be read as a snapshot of prevailing trends rather than a complete census of EU cyber activity, since open-source reporting is uneven across sectors, geographies, and threat types, and because slower-moving campaigns such as

cyberespionage are often documented years after the fact [1]. Within those limits, the 2026 edition arrives at a conclusion with implications well beyond any single incident type: the EU's cyber threat environment is best understood as systemic, shaped less by the emergence of novel attack techniques than by the convergence of established ones across an increasingly interconnected set of digital dependencies [1].

That framing was reinforced directly by ENISA leadership at publication. Executive Director Juhan Lepassaar described the central dynamic as one in which threats "become more interconnected and spread impact across the larger map of digital services and infrastructures," a formulation that echoes throughout the report's sectoral, cybercrime, and vulnerability chapters [2]. The statistics that follow are consistent with that framing: DDoS attacks accounted for 51.3% of all recorded incidents and unauthorized access for a further 39.5%, with phishing remaining the dominant social-engineering technique at 77.8% of cases (these figures are measured by incident type, a separate, non-additive breakdown from the motivation-based figures discussed later in this note), increasingly delivered through commoditized phishing kits, Phishing-as-a-Service platforms, and the ClickFix technique that tricks victims into executing malicious code while ostensibly "fixing" a displayed error [1]. Layered on top of these familiar intrusion patterns, ENISA documents a persistent and growing pattern of attacks against supply chains, third-party providers, and cloud environments that "continued to be observed, with several examples of large-scale and/or impactful incidents throughout the reporting period" [1].

Independent coverage of the release corroborates ENISA's framing of convergence over novelty. Industrial Cyber's analysis of the report emphasized that "the central message is less about the emergence of entirely new threats than about the convergence and scaling of existing ones," noting that cybercrime, state-linked activity, hacktivism, and vulnerability exploitation increasingly rely on overlapping tools, techniques, and dependencies [3]. Help Net Security's coverage similarly characterized the report's core warning as one about Europe's technology backbone becoming a cyber target in its own right, rather than any single actor or campaign [4]. That convergence arguably elevates dependency risk to a systemic concern: as cybercriminal, hacktivist, and state-nexus operators increasingly rely on the same access vectors and shared tooling, defensive postures built around attributing and countering one threat actor type at a time may become correspondingly less effective.

Security Analysis

Cyber dependencies as an amplifying layer

ENISA's report is explicit that the targeting of cyber dependencies, including supply-chain and third-party attacks, "continued to be observed, with several examples of large-scale and/or impactful incidents throughout the reporting period," and that cybercriminals increasingly target third-party providers such as digital services specifically to optimize the efficiency of their attacks [1]. The report's clearest illustration of this dynamic involves the compromise of a single French wealth-management software provider, whose disruption reportedly cascaded into banks and wealth advisers being unable to operate normally for several days, a case ENISA cites explicitly for showing "the cascading effects of attacks against specialised services providers" [1]. A comparable pattern appeared in the software supply chain itself: the Shai-Hulud campaign compromised popular npm packages and browser extensions, prompting ENISA to publish a dedicated technical advisory on the secure use of package managers in March 2026 [1]. Both cases share a structural feature that ENISA highlights in its outlook: as organizations continue integrating third-party services into their operations, "opportunities for threat groups to achieve broader impact through a single compromise are likely to increase" [1], which this analysis treats as the operational hallmark of systemic risk, as distinct from isolated incident risk.

The vulnerability landscape compounds this dependency exposure. ENISA recorded more than 48,000 newly published CVEs in 2025, a 22% increase over the prior year, and among unauthorized-access incidents where an intrusion vector could be identified, 60.4% involved exploitation of an N-day or 0-day vulnerability, with misconfiguration and accidental exposure accounting for a further 20.7% [1]. Since November 2025 ENISA has also served as a Root CVE Numbering Authority, giving it a more direct operational role in vulnerability disclosure across EU CSIRTs and national authorities, which the agency frames as a response to the scale of the exposure it is tracking [1]; CSA's own analysis of this designation examines its implications for NIS2 compliance and cross-border vulnerability disclosure [10]. Insider-driven unauthorized access also grew as a share of incidents, which ENISA attributes in part to Famous Chollima, a DPRK-nexus intrusion set that has sought IT-worker positions inside EU companies, including in the defense and government sectors, which, in effect, turns the hiring pipeline itself into a dependency adversaries can exploit.

Sectoral concentration and financially motivated activity

Public administration remained the most heavily targeted EU sector, accounting for 31.8% of all recorded events, followed by business services (8.5%), transport (8%), manufacturing (6.9%), and finance and banking (5.6%) [1]. ENISA's companion NIS360 assessment, referenced throughout the 2026 Threat

Landscape, identifies railway and maritime transport as sectors sitting in a defined "risk zone," a designation driven by their reliance on heterogeneous legacy systems and their outsized strategic importance to EU supply chains [1] [5]. Within transport, railway-related incidents rose sharply, from roughly 2% of transport-sector events in the prior reporting period to 31.9% in 2025, driven largely by a wave of DDoS claims against railway, metro, and tram operators during the second half of the year [1].

Financially motivated activity, dominated by ransomware, remained the most damaging category in the short term, representing 29.3% of all recorded incidents. Within that category, ransomware accounted for 47.3% of financially motivated claims and data breaches for 36%, with fraud and impersonation schemes making up the remaining 13.3% [1]. The European Banking Authority and European Central Bank separately reported that fraudulent payment transactions — spanning credit transfers, card payments, cash withdrawals, and e-money — totaled an estimated €4.2 billion across the European Economic Area in 2024, a 17% year-over-year increase, which ENISA cites as evidence of the direct financial stakes tied to fraud and social-engineering-driven cybercrime [1] [6]. Ideology-driven hacktivism accounted for an even larger 57.3% share of total recorded incidents, with ENISA logging 4,709 hacktivist claims against EU Member States during 2025, more than 89% of them DDoS-based and heavily concentrated among a small number of pro-Russia groups such as NoName057(16); Germany, France, Italy, Spain, and Poland were the most frequently targeted Member States [1]. State-nexus cyberespionage represented a comparatively small 5.9% share of recorded incidents but is assessed by ENISA to carry disproportionate long-term impact, since these campaigns are typically documented with a lag of six months to more than four years, suggesting today's volume figures likely understate their eventual footprint [1].

AI as a force multiplier for existing threats

ENISA's assessment of artificial intelligence in the 2026 report focuses on AI's current role: during 2025, AI was incorporated into the playbooks of cybercriminal, state-nexus, and information-manipulation actors, but largely in a supporting rather than primary capability [1]. That is expected to shift. ENISA assesses it is likely that 2026 will see AI directly enable a growing number of phases across the attack kill chain, including early experimentation with human-out-of-the-loop proof-of-concepts, a development the agency notes would complicate detection and attribution for network defenders [1]. The growing availability of frontier models and specialized dual-use tooling is described as already lowering the barrier to entry for less sophisticated actors and accelerating the speed, scale, and adaptability of both cybercriminal and state-nexus operations [1]. Industrial Cyber's coverage reached a similar conclusion independently, noting that the growing availability of frontier AI models "has already demonstrated its impact in augmenting the development of malicious capabilities" [3]. Read alongside the report's dependency findings, the implication is that AI is not introducing a distinct new risk category so much as amplifying the existing convergence between cybercrime, hacktivism, and state-nexus activity that ENISA identifies as the report's central theme.

Recommendations

Immediate Actions

Security and risk teams should treat ENISA's dependency findings as a prompt to inventory, rather than assume, their exposure to third-party and supply-chain compromise. Organizations should map which software suppliers, managed service providers, cloud platforms, and customer-service environments sit upstream of critical business functions, since ENISA's own analysis shows that a single compromise at any of these points can produce downstream disruption measured in days, not hours, as demonstrated by the French wealth-management provider incident [1]. Teams that consume open-source packages or browser extensions should specifically review their exposure to the Shai-Hulud campaign and related npm compromises, and should consult ENISA's March 2026 technical advisory on secure package-manager use as a baseline control set [1]. Given that 60.4% of identifiable unauthorized-access incidents involved vulnerability exploitation, patch and configuration management for internet-facing and N-day-affected systems should be treated as a near-term priority rather than a routine maintenance item [1].

Short-Term Mitigations

Organizations operating in or serving the sectors ENISA identifies as most exposed, including public administration, business services, transport, and finance, should reassess third-party risk management programs against the specific pattern the report describes: attackers targeting shared providers precisely because doing so multiplies their reach [1]. This means moving beyond point-in-time vendor questionnaires toward continuous visibility into supplier dependencies and toward pre-negotiated incident response coordination with critical suppliers, mirroring the kind of dependency mapping and business impact analysis called for in CSA's Zero Trust Guidance for Achieving Operational Resilience [7]. Given the sustained volume of DDoS activity tied to hacktivist campaigns, particularly against public-facing services in the sectors and Member States ENISA identifies as most targeted, organizations should also validate that DDoS mitigation and public-facing service resilience plans are tested against realistic, high-volume, ideologically triggered surge scenarios rather than generic capacity assumptions [1].

Strategic Considerations

At a governance level, boards and risk committees should treat the convergence ENISA describes, where cybercriminal, hacktivist, and state-nexus actors increasingly share access vectors and tooling, as a reason to consolidate rather than fragment cyber risk oversight across categories that have traditionally

been managed separately. Because AI is assessed as likely to accelerate existing attack patterns rather than introduce wholly new ones in the near term, organizations should prioritize hardening the dependency and vulnerability-management foundations ENISA identifies as already exploited today, since those same weaknesses are the ones AI-enabled tooling is expected to exploit faster and at greater scale in 2026 [1]. Finally, given ENISA's explicit caution that open-source reporting undercounts slower-moving threats like cyberespionage, organizations with elevated exposure to state-nexus targeting, particularly in government, defense, and critical infrastructure, should weight long-term threat intelligence and insider-risk programs accordingly rather than relying solely on incident-volume statistics to prioritize investment [1].

CSA Resource Alignment

ENISA's finding that supply-chain and developer-toolchain compromises, including the Shai-Hulud npm campaign, are producing large-scale, cascading impact across the EU directly parallels CSA's analysis in *Developer Toolchain as Enterprise Attack Surface*, which documents how compromised package registries, IDE extensions, and CI/CD pipelines allow a single upstream compromise to propagate across thousands of downstream organizations [8]. That paper's finding that only a small fraction of organizations pin their build dependencies to immutable references, leaving the majority exposed to exactly the kind of mutable, retroactively poisoned dependency ENISA describes, gives EU-facing security teams a concrete starting point for addressing the software-supply-chain exposure this report identifies [8].

ENISA's emphasis on cyber dependencies as an amplifying layer, and its call for organizations to map critical suppliers rather than assume resilience, aligns closely with CSA's *Zero Trust Guidance for Achieving Operational Resilience*, which provides frameworks for mapping critical dependencies, conducting business impact analysis, and aligning resilience programs with regulatory requirements including NIS2 and DORA [7]. Organizations using this ENISA report to justify investment in third-party risk management can use CSA's guidance as the operational counterpart, translating ENISA's incident-level findings into the dependency-mapping and blast-radius-reduction practices the guidance recommends [7].

Finally, ENISA's assessment that AI is likely to directly enable a growing share of attack kill-chain phases during 2026 connects to CSA's AI Controls Matrix (AICM) v1.1, whose Threat and Vulnerability Management and Application and Interface Security domains provide governance controls for organizations assessing how AI-enabled tooling changes their exposure to the vulnerability-exploitation and unauthorized-access patterns ENISA documents as already accounting for the majority of

identifiable intrusions [9]. ENISA's own elevation to Root CVE Numbering Authority status is examined in detail, including its NIS2 compliance and cross-border disclosure implications, in CSA's *ENISA Designated as EU CVE Root* research note [10].

References

[1] ENISA. "ENISA Threat Landscape 2026." European Union Agency for Cybersecurity, September 2026.

[2] ENISA. "Exploring the Evolution of the Cyber Threat Landscape: How Dependencies Weaken Our Digital Resilience." ENISA News, September 2026.

[3] Industrial Cyber. "ENISA Threat Landscape 2026 Highlights Ransomware, Vulnerability Exploitation, AI-Enabled Attacks Across EU Organizations." Industrial Cyber, September 2026.

[4] Help Net Security. "Europe's Technology Backbone Is Becoming a Cyber Target." Help Net Security, September 2026.

[5] ENISA. "ENISA NIS360 2026." European Union Agency for Cybersecurity, May 2026.

[6] European Central Bank / European Banking Authority. "EBA-ECB Report on Payment Fraud." European Central Bank, December 2025.

[7] Cloud Security Alliance. "Zero Trust Guidance for Achieving Operational Resilience." Cloud Security Alliance.

[8] Cloud Security Alliance. "Developer Toolchain as Enterprise Attack Surface." Cloud Security Alliance AI Safety Initiative, 2026.

[9] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." Cloud Security Alliance.

[10] Cloud Security Alliance. "ENISA Designated as EU CVE Root: Implications for NIS2 Compliance and Cross-Border Vulnerability Disclosure." Cloud Security Alliance AI Safety Initiative, March 2026.

