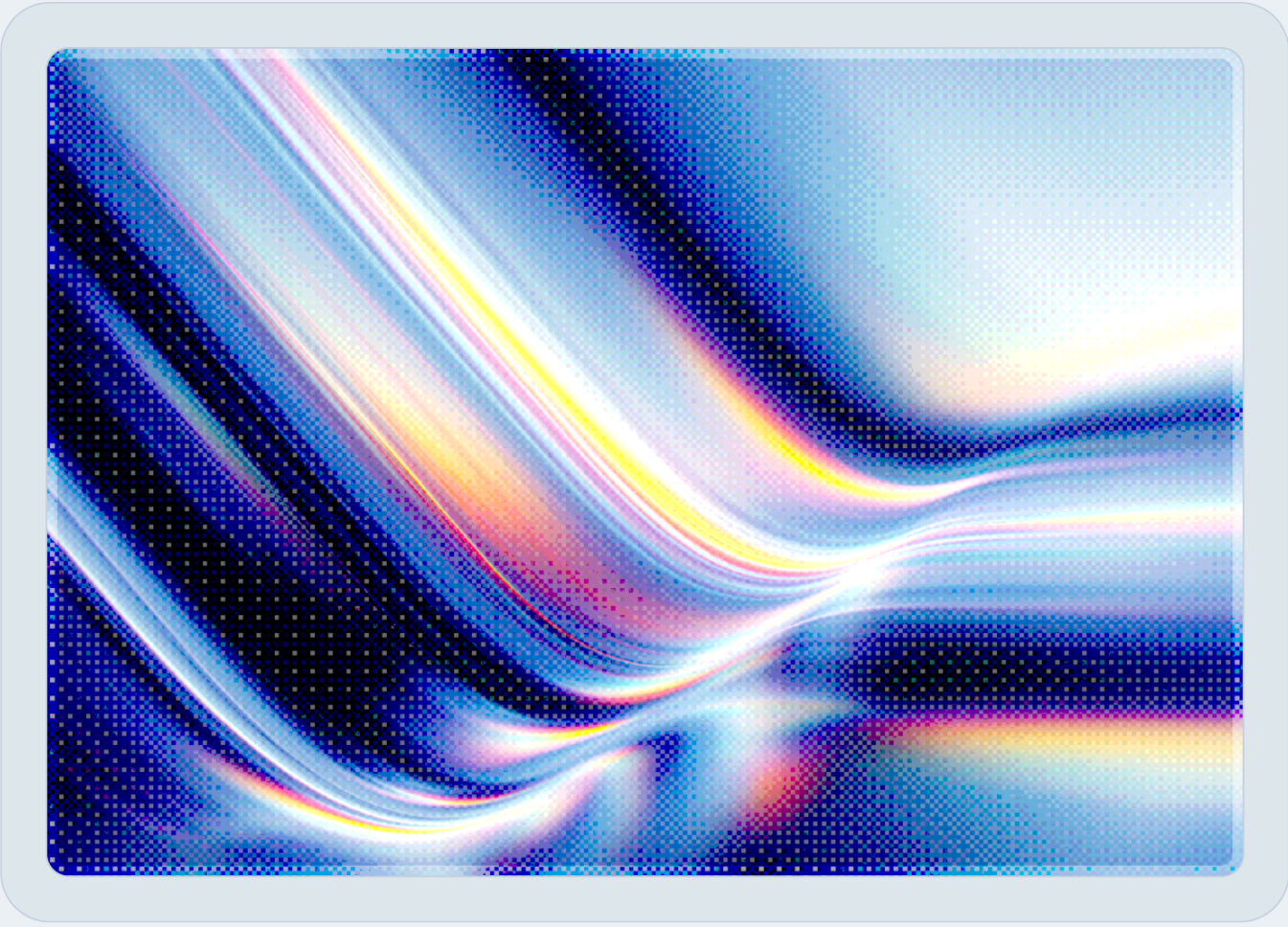
CSAI Foundation | Cloud Security Alliance

ENISA 2026: Digital Dependencies Widen Europe's Attack Surface

Security Implications of the EU Threat Landscape Report's Supply-Chain Findings

2026-09-24

AI-assisted Rapid Research



CSAI | CSA cloud security alliance®

Key Takeaways

On September 22, 2026, the European Union Agency for Cybersecurity (ENISA) published its annual Threat Landscape report, analyzing 8,257 curated cyber incidents affecting EU Member States and EU-based organizations between January 1 and December 31, 2025 [1][2][3]. The report's central argument is that the security of any single organization's systems is now only part of the equation, because cyber dependencies, supply-chain relationships, and third-party service providers have become the mechanism through which a localized compromise spreads into a systemic, multi-organization incident [1][2]. Distributed denial-of-service attacks accounted for 51.3 percent of recorded incidents and unauthorized access for 39.5 percent, with vulnerability exploitation driving 60.4 percent of those unauthorized-access cases, underscoring that well-understood attack techniques are still the primary vector even as the report's headline concern shifts toward interconnection risk [3]. A ransomware attack on a single Swedish IT supplier disrupted human-resources and sick-leave reporting systems for roughly 200 municipalities and regional authorities, a case ENISA cites as emblematic of how compromising one widely used vendor can cascade into hundreds of downstream victims simultaneously [3][4]. ENISA also assesses that artificial intelligence will increasingly support malicious operations, from phishing and reconnaissance to malicious code development and post-exploitation activity, compounding the dependency problem by making it cheaper for attackers to identify and exploit the weakest link in a digital supply chain [1][3]. For CSA members, the report is consistent with a pattern CSA has tracked across cloud, SaaS, and agentic AI incidents in 2026: several of the largest breaches this year originated in a trusted third party rather than the victim's own perimeter.

Background

ENISA's Threat Landscape series is the agency's annual assessment of the cyber threat environment facing the European Union, produced to inform national authorities, EU institutions, and private-sector risk owners under the mandate created by the NIS2 Directive. The 2026 edition draws on a curated dataset of 8,257 incidents affecting EU Member States and organizations operating within the EU during calendar year 2025, combining ENISA's own monitoring with input from national Computer Security Incident Response Teams and open-source reporting [1][3]. Executive Director Juhan Lepassaar framed the report's core finding directly, stating that "the analysis highlights how threats become more interconnected and how threat groups spread their impact across the larger map of digital

services" [1]. In CSA's reading, that framing marks a shift in emphasis from prior editions, which tended to catalogue threat categories separately, toward an explicit argument that the attack surface facing any single EU organization now extends through every software vendor, cloud provider, and managed service it relies upon.

Public administration remained the most heavily targeted sector, accounting for 31.8 percent of all recorded incidents, of which 81.8 percent were distributed denial-of-service attacks tied to ideologically motivated hacktivist campaigns rather than financially motivated intrusions [1][3]. Business services, transport, manufacturing, and finance followed as the next most affected sectors, at 8.5, 8, 6.9, and 5.6 percent of incidents respectively [3]. Cybercrime accounted for 36 percent of total recorded events, with ransomware representing 40 percent of financially motivated activity and data breaches another 31 percent, while state-nexus threat actors were responsible for intrusion operations in 87 percent of their observed activity and phishing in the remaining 12 percent [1]. Hacktivist collectives filed 4,709 claimed attacks against EU Member States over the reporting period, 89 percent of which involved distributed denial-of-service techniques, continuing a trend of loosely organized, ideologically motivated groups using low-cost disruption tools to generate outsized public attention [1]. Beyond the EU-specific dataset, ENISA notes that 48,000 new CVEs were published globally in 2025, a 22 percent increase over the prior year, and that online investment fraud alone cost victims across the European Economic Area an estimated EUR 4 billion in 2024, figures the report uses to illustrate that both the technical vulnerability surface and the financially motivated threat ecosystem continued to expand independent of the dependency risks that are the report's central theme [1].

Security Analysis

The report's supply-chain and dependency findings are best understood through the specific case ENISA highlights rather than through aggregate statistics alone. A ransomware attack against a Swedish IT supplier serving municipal governments, independently reported as affecting the company Miljödata, disrupted human-resources and sick-leave reporting systems used by roughly 200 of the country's municipalities and regional authorities after the ransomware actor was able to compromise the supplier's environment [3][4]. The incident exposed HR records including medical certificates, rehabilitation plans, and work-related injury reports for employees across the affected municipalities [4]. ENISA's inclusion of this case illustrates the report's broader thesis: none of the affected municipalities was individually breached, yet each was rendered unable to process HR and payroll functions because a single upstream dependency failed, a dynamic the report identifies as characteristic of supply-chain and third-party compromise generally rather than as an isolated incident [1][3].

That dynamic is not confined to traditional IT service providers. Open-source software ecosystems experienced comparable dependency failures throughout the same reporting period. Beginning in September 2025, a self-propagating campaign that researchers named Shai-Hulud compromised more than 500 npm packages by harvesting credentials from continuing-integration pipelines and cloud metadata endpoints, then used those credentials to republish additional infected packages under legitimate maintainer accounts, allowing the worm to spread automatically across the JavaScript package ecosystem without further attacker involvement [5]. The campaign's severity prompted the U.S. Cybersecurity and Infrastructure Security Agency to issue a direct advisory to the developer community, and a second, substantially larger wave documented by Microsoft in December 2025 ultimately backdoored hundreds of additional packages [5][6]. While this campaign centers on global open-source infrastructure rather than a single EU supplier, it demonstrates the same structural vulnerability ENISA describes at the organizational level: a compromise several layers upstream in a dependency chain can silently propagate into every organization that consumes the affected software, often before the organization is even aware the dependency exists in its environment.

The report's vulnerability-exploitation statistics reinforce why these dependency chains remain exploitable in practice. Sixty percent of unauthorized-access incidents in the EU dataset stemmed from exploitation of known or zero-day vulnerabilities rather than credential theft or social engineering, a proportion consistent with the growth in published CVEs [1], and plausibly reflecting the well-documented industry pattern of patch cadences lagging vulnerability disclosure across large vendor ecosystems. ENISA also documents the emergence of newer social-engineering techniques operating alongside this exploitation activity, including the "ClickFix" technique that tricks users into executing malicious commands through fabricated troubleshooting instructions, and a shift toward encrypted messaging platforms such as Signal and WhatsApp as delivery channels for phishing and malware, both of which complicate detection for security teams still tuned primarily to email-based threats [3]. Taken together, these findings describe an environment in which the exploitation techniques themselves are largely familiar, but the blast radius of a successful exploitation event has grown because so much of the affected infrastructure sits several organizational boundaries away from the ultimate victim.

Recommendations

Immediate Actions

Security teams should compile or refresh an inventory of critical third-party dependencies, including managed IT service providers, SaaS platforms, and any software components pulled from public package registries, prioritizing those that touch human-resources, payroll, identity, or other systems

whose disruption would halt core operations rather than merely degrade them [1][3]. Organizations using npm, PyPI, or comparable package ecosystems should confirm that dependency-scanning tooling has been updated against current indicators for the Shai-Hulud campaign and similar worm-style compromises, and should audit CI/CD pipeline credentials and cloud metadata endpoint access for any exposure consistent with the campaign's documented harvesting technique [5][6]. Because 60 percent of unauthorized-access incidents in the ENISA dataset trace back to vulnerability exploitation, organizations should also confirm that patch management service-level agreements with critical vendors specify maximum remediation windows for actively exploited vulnerabilities, not merely a general commitment to patch [1][3].

Short-Term Mitigations

Given the prevalence of both ClickFix-style social engineering and phishing delivered through encrypted messaging platforms, security awareness programs should be updated to cover these specific delivery mechanisms rather than relying on email-focused training alone, since 77.8 percent of social-engineering incidents in the ENISA dataset involved phishing broadly defined [3]. Organizations should extend contractual and monitoring requirements for critical suppliers to include prompt breach notification and evidence of their own dependency management practices, following the pattern exposed by the Swedish municipal incident, in which the affected organizations had no independent visibility into the security posture of the software vendor on which they depended [3][4]. Incident response plans should be tested against a scenario in which the initiating compromise occurs entirely outside the organization's own network, at a shared IT provider or software supplier, since this class of incident requires coordination with the vendor and often with other affected customers rather than a purely internal response.

Strategic Considerations

The report's core argument, that interconnection itself is now a primary driver of cyber risk, implies that organizations cannot fully manage their exposure through internal controls alone; third-party and supply-chain risk management must be resourced and governed as a first-class security function rather than a compliance checkbox satisfied by periodic vendor questionnaires [1][2]. Given ENISA's assessment that AI will increasingly support reconnaissance, phishing, and exploit development, organizations should expect the economics of identifying and targeting the weakest link in a dependency chain to continue improving in the attacker's favor, which argues for investing in dependency mapping and concentration-risk analysis now rather than after a downstream vendor is compromised [1][3]. For organizations operating within scope of the NIS2 Directive, the report's finding that 73 percent of

targeted organizations are NIS2 essential or important entities [1] should inform how supply-chain risk management obligations under that framework are prioritized and resourced relative to other compliance activities.

CSA Resource Alignment

CSA's own recent research reinforces several of the same structural findings the ENISA report describes at the EU-wide level, and provides more granular, actionable controls guidance for the specific dependency categories involved. CSA's own threat intelligence tracking of SaaS supply-chain incidents has documented a comparable pattern of single-vendor compromises cascading into large numbers of downstream customer organizations without any vulnerability in the customers' own environments being exploited, a dynamic directly analogous to the single-supplier cascade ENISA highlights in the Swedish municipal case; both demonstrate that a customer's security posture can be entirely sound while remaining exposed through a trusted third party's compromised credentials. CSA's presentation, Software Transparency: Securing the Digital Supply Chain, addresses the open-source and software-composition risks underlying incidents like the Shai-Hulud npm campaign directly, covering software bill of materials adoption, dependency scanning, and CI/CD pipeline security practices that map to the immediate actions recommended above [7]. CSA's broader research agenda has also begun extending this same dependency-risk pattern into the agentic AI marketplace context, relevant given ENISA's assessment that AI tooling will increasingly be woven into both attacker and defender workflows going forward. Finally, the supply chain, vendor risk, and identity and access management domains of the AI Controls Matrix (AICM) v1.1 provide the underlying control objectives organizations can use to formalize third-party dependency governance into an auditable program rather than the ad hoc vendor review processes the ENISA report suggests are currently insufficient across much of the EU digital ecosystem [8].

References

[1] ENISA. "Exploring the evolution of the cyber threat landscape: How dependencies weaken our digital resilience." European Union Agency for Cybersecurity, September 2026.

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

[3] Help Net Security. "Europe's technology backbone is becoming a cyber target." Help Net Security, September 24, 2026.

[4] The Record. "Hundreds of Swedish municipalities impacted by suspected ransomware attack on IT supplier." Recorded Future News, August 27, 2025.

[5] Cybersecurity and Infrastructure Security Agency. "Widespread Supply Chain Compromise Impacting npm Ecosystem." CISA, September 23, 2025.

[6] Microsoft Security. "Shai-Hulud 2.0: Guidance for detecting, investigating, and defending against the supply chain attack." Microsoft Security Blog, December 9, 2025.

[7] Cloud Security Alliance. "Software Transparency: Securing the Digital Supply Chain." Cloud Security Alliance.

[8] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." Cloud Security Alliance, 2026.