Goodwipes Uses AI to Spoof OpenAI’s Astra Ad, With a Butt-Wiping Twist

“Asstra” was developed in four days by Frank Cartagena’s OK Future.
https://www.adweek.com/creativity/goodwipes-uses-ai-spoof-openai-astra-ad/

Why the Fields Good Business Plan Is Anything But Cookie-Cutter

Co-founder Ashley Fields tapped into earned media to create a fully baked functional cookie launch.
https://www.adweek.com/brand-marketing/why-fields-good-business-plan-anything-but-cookie-cutter/

US, UK, Dutch Agencies Expose Iranian ‘Chosen Brick’

Surveillance Malware

US, UK, and Dutch government agencies published a report detailing the malware, and the FBI described the abuse of Telegram for C&C.

The post US, UK, Dutch Agencies Expose Iranian ‘Chosen Brick’ Surveillance Malware appeared first on SecurityWeek.

https://www.securityweek.com/us-uk-dutch-agencies-expose-iranian-chosen-brick-surveillance-malware/

Reese Witherspoon’s Draper James and Levain Cookies on Building Beyond Their Founders

The two CEOs discuss how to keep innovating without losing what made them famous. https://www.adweek.com/brand-marketing/reese-witherspoons-draper-james-and-levain-cookies-on-building-beyond-their-founders/

Unauthenticated RCE Flaws

Could Expose 200,000+ WordPress Sites to Takeover

Vulnerabilities in The Events Calendar can provide attackers with remote code execution capabilities.

The post Unauthenticated RCE Flaws Could Expose 200,000+ WordPress Sites to Takeover appeared first on SecurityWeek.

https://www.securityweek.com/unauthenticated-rce-flaws-could-expose-200000-wordpress-sites-to-takeover/

AI-R Studio Wins Higgsfield’s AI Adathon Competition

The winner was presented on stage at Brandweek 2026 https://www.adweek.com/creativity/ai-r-studio-wins-higgsfields-ai-adathon-competition/

Bravo Fan Fest Is Turning Brands Into Bravolebrities

Brand partners are set to be stars at Bravo Fan Fest 2026. https://www.adweek.com/convergent-tv/bravo-fan-fest-is-turning-brands-into-bravolebrities/

How Crocs Became One of TikTok Shop’s Top Sellers

Crocs chief brand officer Terence Reilly demonstrated the brand’s ‘audacious’ social strategy live at Brandweek. https://www.adweek.com/brand-marketing/how-crocs-became-one-of-tiktok-shops-top-sellers/

SBOM e supply chain: il CRA lo renderà obbligatorio, ma lo scambio tra fornitori e clienti resta raro

SBOM e supply chain sono legati da un obbligo asimmetrico. La distinta base del software è l’elenco dei componenti software di un prodotto digitale. Il Cyber Resilience Act ne renderà obbligatoria la redazione per i fabbricanti. Una rilevazione europea su 334 organizzazioni mostra però che il documento quasi non circola: il 39% non lo riceve mai dai fornitori di software commerciale e un altro 39% lo riceve raramente.

Nello stesso periodo, in Italia, il 56% delle segnalazioni di incidente grave trasmesse alla Banca d’Italia ha coinvolto un fornitore. Le due rilevazioni misurano popolazioni diverse e non si verificano a vicenda, come si dirà più avanti. Accostate, però, descrivono una tensione precisa: lo strumento

di trasparenza progettato per governare la catena di fornitura è quello che meno passa di mano.

Che cosa chiede il CRA su SBOM e supply chain

Dipendenze di primo livello, non tutta la catena

Il regolamento definisce la distinta base all'articolo 3, punto 39: "un registro formale contenente i dettagli e le relazioni della catena di approvvigionamento dei componenti inclusi negli elementi software di un prodotto con elementi digitali".

L'obbligo sta invece nell'allegato I, parte II, punto 1 del regolamento (UE) 2024/2847. Impone ai fabbricanti di identificare e documentare le vulnerabilità e i componenti del prodotto. Devono farlo redigendo "una distinta base del software in un formato di uso comune e leggibile da un dispositivo automatico, che includa almeno le dipendenze di primo livello del prodotto".

L'avverbio conta. La formula "almeno le dipendenze di primo livello" fissa un pavimento, non un tetto. Il fabbricante deve dichiarare le componenti che ha incluso direttamente, mentre le dipendenze delle dipendenze, cioè il grosso di una catena moderna, restano fuori dall'obbligo minimo.

Il considerando 77 spiega la finalità: aiutare fabbricanti e utilizzatori a tenere traccia delle vulnerabilità e dei rischi di cibersicurezza. La distanza fra quella finalità e il pavimento normativo è il primo nodo aperto.

Le tre date che contano

L'articolo 71 scagliona l'applicazione su tre momenti. Il capo

IV, articoli da 35 a 51, si applica dall’11 giugno 2026. L’articolo 14, quello sugli obblighi di segnalazione, si applica dall’11 settembre 2026. Il resto del regolamento, compresi i requisiti dell’allegato I, si applica dall’11 dicembre 2027.

L’obbligo di redigere la distinta base non è quindi ancora in vigore. Chi oggi la produce lo fa per scelta, per pressione contrattuale o per anticipare la scadenza.

Prodotto sì, consegnato no

I dati che seguono vengono dal rapporto SBOM Adoption State of Play 2026 di ENISA, pubblicato nel giugno 2026 su una rilevazione condotta a fine 2025. Hanno risposto 334 organizzazioni, per l’87,72% del settore privato, per oltre il 65% grandi imprese sopra i 250 dipendenti e per il 65% operanti principalmente nell’Unione.

Chi lo riceve, e quanto spesso

Alla domanda su quanto spesso ricevano un SBOM dai fornitori di software commerciale, il **39%** delle organizzazioni risponde mai e un altro **39%** raramente. Solo il **2%** risponde sempre.

È il dato che ribalta la percezione corrente. Si discute molto di come produrre una distinta base e pochissimo del fatto che, oggi, riceverne una da un fornitore è statisticamente un’eccezione.

Dieci contratti su cento

Sul versante contrattuale la fotografia è coerente. Solo il **10%** dei rispondenti dichiara che la propria organizzazione ha stabilito requisiti SBOM obbligatori nei contratti di fornitura.

Le altre risposte descrivono intenzioni più che pratiche

consolidate: il 55% si dichiara in procinto di inserirli in modo sistematico, il 37% li inserisce già in modo occasionale, il 27% prevede di farlo. Le voci non sono mutuamente esclusive, quindi non vanno sommate né lette come una ripartizione.

Quanti fornitori soddisfano i requisiti

Dove i requisiti esistono, la conformità resta bassa. Il **45%** delle organizzazioni dichiara che solo fra lo 0 e il 25% dei propri fornitori soddisfa i requisiti richiesti. Appena il **2%** colloca i propri fornitori nella fascia fra il 75 e il 100%.

C'è anche un divario fra la profondità di analisi che serve e quella che arriva: il **24%** dichiara di avere bisogno di SBOM con analisi a profondità piena, ma solo il **14%** li riceve.

ENISA indica l'ostacolo che incide in modo estremo con maggiore frequenza: l'indisponibilità o la scarsa qualità degli SBOM di terze parti. Non è un problema di strumenti interni, è un problema di consegna.

Adozione avviata, uso ancora no

Sul grado di adozione interna, il **9%** dichiara un livello maturo e pienamente automatizzato. Il 25% afferma che gli SBOM sono ampiamente adottati nei propri prodotti, il 44% si trova in fase pilota o di adozione limitata, mentre il 22% non ha ancora iniziato.

La domanda più rivelatrice riguarda però la distanza fra produrre una distinta base e usarla davvero. Il 44% dichiara un divario moderato, il 23% un divario significativo, e solo il **7%** lo ha chiuso del tutto.

ENISA ne trae una conclusione esplicita, che vale la pena riportare: gli SBOM non sono usati appieno per la sicurezza, ma principalmente per finalità di conformità. Il documento diventa un adempimento, non un controllo.

Formati frammentati e correlazione difficile

Gli ostacoli tecnici spiegano in parte il divario. Il 62% dei rispondenti giudica la completezza dell'SBOM abbastanza o estremamente difficile da ottenere. Sulla correlazione fra componenti e vulnerabilità note, il 35% risponde abbastanza difficile e il 23% estremamente difficile. Il 37% segnala problemi di qualità dei dati e il 28% carenza di competenze.

I formati restano frammentati. CycloneDX è usato dal 44% e SPDX dal 29%, mentre il 17% adotta un formato proprietario e l'11% dichiara di non usare alcun formato standard. ENISA legge quel 28% complessivo come una possibile barriera all'interoperabilità sul mercato europeo, che è cosa diversa dalla leggibilità automatica del file.

La leva per risolverla esiste già, e non è stata usata. L'articolo 13, paragrafo 24 consente alla Commissione di specificare con atti di esecuzione il formato e gli elementi della distinta base di cui all'allegato I. Gli atti devono tenere conto delle norme e delle migliori pratiche europee o internazionali.

Il 79% che va maneggiato con cura

Il rapporto riporta anche una nota di ottimismo: secondo le stime dei rispondenti, il 79% delle organizzazioni raggiungerà il livello di maturità necessario entro la piena applicabilità del CRA, indicata nel dicembre 2027.

Tre cautele prima di citarla. È una autovalutazione, non una misura. Proviene dallo stesso campione che dichiara un tasso di adozione matura del 9%. E lo stesso rapporto registra che il 30% dei rispondenti prevede di aver bisogno di due anni o più per arrivare a quel livello.

Dove gli incidenti accadono davvero

Il peso dei fornitori nelle segnalazioni italiane

La Banca d’Italia ha pubblicato il 9 luglio 2026 il Quadro segnaletico di Vigilanza dei gravi incidenti ICT. L’analisi completa del primo bilancio DORA italiano è su queste pagine, e qui conta un dato solo. Nel **56% delle segnalazioni** del 2025 risulta coinvolto un fornitore di servizi. Per le banche meno significative l’Istituto scrive che il fornitore è all’origine dell’evento nella quasi totalità delle segnalazioni relative a incidenti operativi.

Il confronto con gli anni precedenti va fatto con il dato giusto. Le due edizioni non sono direttamente comparabili, perché cambiano base normativa, perimetro e soglie. L’Istituto dedica al raffronto una sezione apposita, che restringe l’analisi ai soli soggetti presenti in entrambi gli schemi.

Su quel sottoinsieme, scrive la Banca d’Italia, il coinvolgimento dei fornitori di servizi ICT negli incidenti “rimane elevato, pari a circa il 57%”. È la fonte stessa a qualificare quel livello come elevato. I valori degli anni precedenti compaiono nel grafico che accompagna la frase, quindi il confronto puntuale anno su anno non si ricostruisce dal testo.

Un accostamento, non una correlazione

I due blocchi di dati vanno letti insieme con una precisazione. ENISA interroga organizzazioni di settori diversi in tutta Europa, la Banca d’Italia conta segnalazioni di intermediari finanziari vigilati in Italia. Le popolazioni non coincidono e nessuna delle due fonti misura l’altra.

L’accostamento regge come argomento, non come nesso

statistico. Dice che la dipendenza da terzi è il punto dove gli incidenti si realizzano, e che lo strumento pensato per renderla trasparente è anche quello che meno passa di mano.

Il meccanismo è visibile negli attacchi alla supply chain, dove la compromissione di un pacchetto si propaga attraverso dipendenze che nessun inventario di primo livello avrebbe intercettato. Sul versante degli standard SBOM il lavoro di normalizzazione procede, ma riguarda il formato del documento, non la sua circolazione.

Perché un documento riservato non produce trasparenza

La tensione non nasce dalla prassi, sta dentro il regolamento. Il considerando 77 include fra i destinatari del beneficio anche chi acquista il software: la distinta base "può fornire a coloro che realizzano, acquistano e utilizzano il software informazioni che migliorano la loro comprensione della catena di approvvigionamento". Lo stesso considerando si chiude però con una frase netta: "I fabbricanti non dovrebbero essere obbligati a rendere pubblica la distinta base del software".

La parte dispositiva conferma. L'allegato VII colloca la distinta base fra le informazioni sui processi di gestione delle vulnerabilità che compongono la documentazione tecnica del prodotto, cioè il fascicolo che il fabbricante tiene a disposizione delle autorità.

Verso il cliente, invece, la consegna resta facoltativa. L'allegato II elenca le informazioni e le istruzioni per l'utente. Al punto 9 chiede di indicare dove reperire il documento solo "se il fabbricante decide di mettere a disposizione dell'utilizzatore la distinta base del software". È il regolamento stesso a contemplare la scelta di non consegnarla.

Anche il potere delle autorità è circoscritto. L’articolo 13, paragrafo 25 consente alle autorità di vigilanza del mercato di chiedere le distinte base ai soli fabbricanti delle categorie di prodotti individuate dal gruppo di cooperazione amministrativa. Il contesto è la valutazione della dipendenza degli Stati membri e dell’Unione nel suo complesso dai componenti software, in particolare quelli liberi e open source. Le informazioni sulle dipendenze arrivano poi al gruppo in forma anonimizzata e aggregata, “al fine di tutelare la riservatezza delle distinte base del software”.

L’obbligo di redazione nasce quindi orientato al controllo regolamentare, non allo scambio commerciale. Il dato misurato da ENISA è la conseguenza prevedibile di quella scelta: un documento che si genera e non si consegna.

Le leve disponibili sono contrattuali prima che tecniche. Un requisito vincolante nel contratto di fornitura, oggi presente in un caso su dieci, è la variabile su cui un’organizzazione può agire senza attendere il dicembre 2027. Chi si occupa di gestione del rischio dei fornitori trova qui la richiesta più concreta da mettere a contratto.

Tre grandezze diranno se qualcosa si muove: la quota di organizzazioni che riceve una distinta base dai propri fornitori, la quota che la rende obbligo contrattuale, e la percentuale di fornitori che effettivamente la consegna. Finché resteranno dove sono, il legame fra SBOM e supply chain resterà sulla carta: il documento certificherà la conformità di chi lo redige, senza migliorare la sicurezza di chi dovrebbe riceverlo.

https://www.ictsecuritymagazine.com/articoli/sbom-fornitori-cra/

After 15 Years of Pro, Politico Finally Launches a Second Subscription

Priced at roughly $1,000 a year, Decoded is a fraction of the cost but has a similar strategy. https://www.adweek.com/media/politico-launches-decoder-subscription/