

Colmare le lacune nella sicurezza della supply chain: checklist per la valutazione del ciclo SSDLC

Gli attacchi alla supply chain sono tra le minacce informatiche più pericolose e difficili da contrastare. Gli attacchi subiti da SolarWinds, Polyfill.io, 3CX e MOVEit dimostrano come colpire i fornitori di software permette agli aggressori di compromettere interi settori su vasta scala.



30%

di tutte le violazioni del 2024 hanno coinvolto una terza parte, un aumento del 15% rispetto al 2023¹

Le tradizionali valutazioni dei fornitori si concentrano sulla situazione finanziaria e sulla sicurezza dell'infrastruttura, ma trascurano l'origine effettiva della maggior parte delle vulnerabilità: il processo di sviluppo del software.

Dove si nascondono le vulnerabilità: il processo di sviluppo del software

Attacchi alla supply chain che hanno fatto storia

| Azienda | Settore | Data | Impatto |
|-------------|---|------|---|
| Polyfill.io | Rete di distribuzione e consegna di contenuti | 2024 | Migliaia di siti web colpiti |
| 3CX | Servizi VoIP | 2023 | Migliaia di aziende colpite |
| MOVEit | Trasferimento di file | 2023 | Oltre 2.000 organizzazioni colpite |
| SolarWinds | Software IT | 2020 | Oltre 18.000 organizzazioni compromesse |

I controlli di sicurezza applicati in fase di runtime non possono correggere il codice non sicuro in modo retroattivo. Se le vulnerabilità vengono introdotte nelle fasi di progettazione o codifica, i clienti devono attendere l'applicazione delle patch da parte dai fornitori, ma nel mentre restano esposti.

Il ciclo di vita dello sviluppo sicuro del software (SSDLC) verte sull'integrazione della sicurezza in ogni fase dello sviluppo software, dalla progettazione alla manutenzione post-rilascio.

Come valutare lo sviluppo software

Una strategia basata su prove richiede la valutazione di sei aspetti:



Governance e policy

Policy documentate, ruoli di sicurezza formali e supervisione del team dirigenziale.



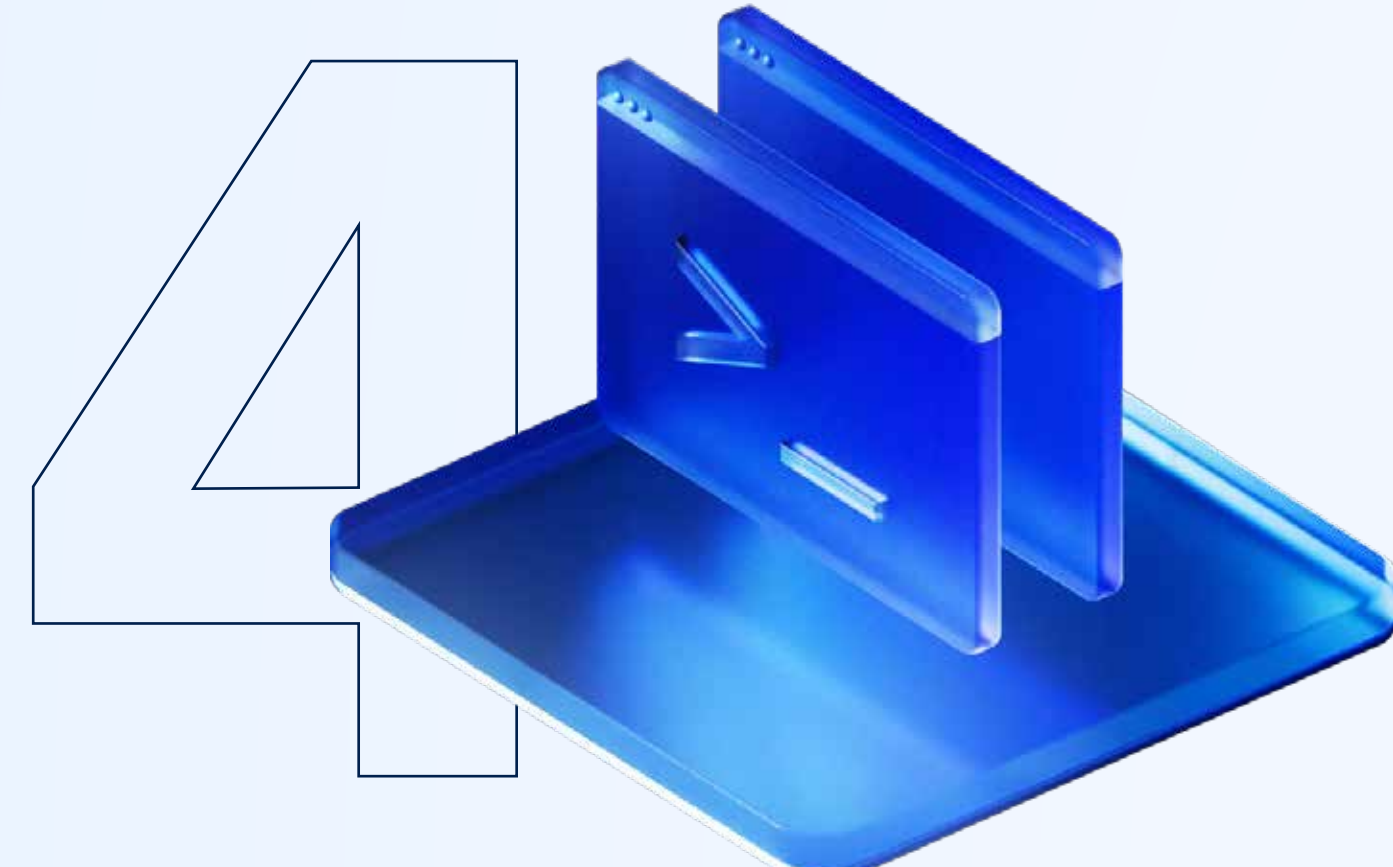
Gestione del rischio e progettazione

Modellazione delle minacce, requisiti di sicurezza e valutazioni della progettazione.



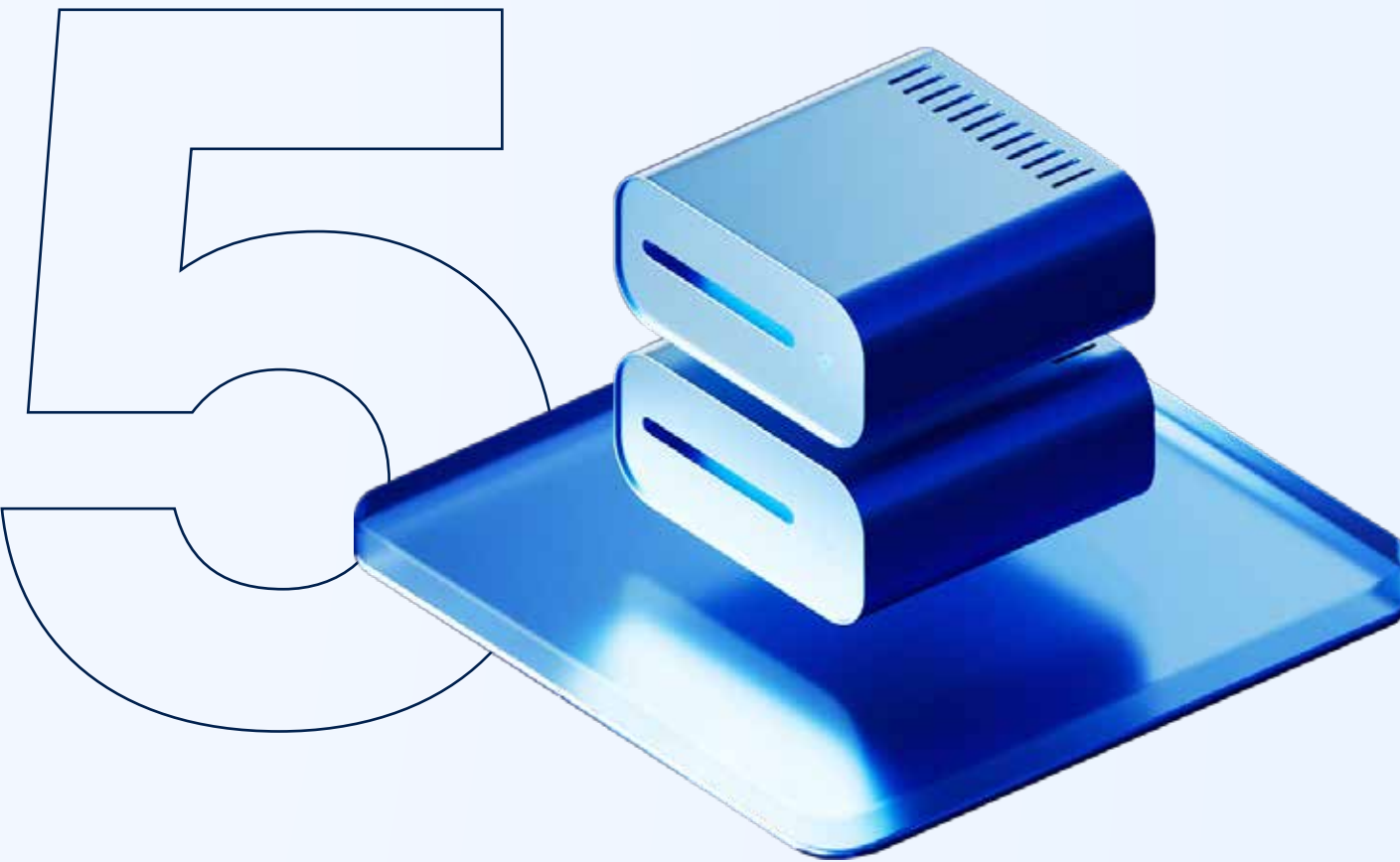
Procedure di implementazione

Formazione degli sviluppatori, standard di codifica sicura e revisione del codice.



Verifica e convalida

Test automatizzati, test di penetrazione e convalida di terzi indipendenti.



Rilascio e distribuzione

Pipeline rinforzate, firma del codice e isolamento degli ambienti.



Manutenzione e monitoraggio

Segnalazione delle vulnerabilità, tempistiche di applicazione delle patch e notifiche ai clienti.

Acronis: eccellenza SSDLC certificata

Acronis può dimostrare la propria leadership in ambito SSDLC grazie alle certificazioni verificate da organismi indipendenti:



IEC 62443-4-1
Sviluppo sicuro dei prodotti per ambienti OT



ISO/IEC 27001
Gestione della sicurezza delle informazioni

ISO/IEC 27017/27018
Sicurezza e privacy dei servizi cloud



STAR Livello 2 di CSA
Valutazione indipendente della sicurezza del cloud

Tutte queste certificazioni sono esclusive e complesse da ottenere.

IEC 62443-4-1 rappresenta lo standard di riferimento per lo sviluppo sicuro dei prodotti negli ambienti industriali, e convalida che i prodotti Acronis integrano la sicurezza sin dalla fase di progettazione. I clienti e i Partner OT possono affidarsi con fiducia alle soluzioni Acronis, in grado di ridurre i rischi della loro supply chain e di semplificare la conformità alle normative NIS 2 e DORA, tra le altre.



Scopri di più

Rafforza la sicurezza della supply chain con l'approccio certificato di Acronis:

- [Visualizza il Certificato IEC 62443-4-1 di Acronis](#)
- [Leggi il white paper su SSDLC](#)
- [Esplora le soluzioni di Cyber Protection di Acronis](#)
- [Programma una demo individuale con un Acronis Solutions Engineer](#)



Informazioni su Acronis

Acronis, leader globale nella Cyber Protection, fornisce soluzioni che integrano nativamente Cyber Security, protezione dei dati e gestione degli endpoint, progettate per i Managed Service Provider (MSP), le piccole e medie imprese (PMI) e reparti IT aziendali. Le soluzioni di Acronis sono altamente efficienti e progettate per identificare, prevenire, rilevare, rispondere e ripristinare dai moderni cyberthreats con un tempo di inattività minimo, garantendo l'integrità dei dati e la continuità aziendale. Grazie alla straordinaria capacità di soddisfare le esigenze degli attuali ambienti IT, eterogenei e distribuiti, Acronis offre agli MSP la soluzione di sicurezza più completa del mercato.

Società svizzera fondata a Singapore nel 2003, Acronis conta 15 sedi in tutto il mondo e dipendenti in oltre 45 paesi. La soluzione Acronis Cyber Protect è disponibile in 26 lingue e in 150 paesi, ed è utilizzata da oltre 20.000 Service Provider per proteggere più di 750.000 aziende. Per ulteriori informazioni, visita il sito www.acronis.com.

¹ Verizon, "2025 Data Breach Investigations Report".