Red Hat

Report sullo stato della sicurezza di Kubernetes

Edizione 2024

Report di Red Hat

Riepilogo

Le tecnologie cloud native stanno cambiando il modo in cui le organizzazioni svolgono le attività di sviluppo, deployment e scalabilità delle applicazioni. L'agilità, la flessibilità e la scalabilità intrinseche dell'infrastruttura cloud consentono alle aziende di accelerare i tempi di rilascio, aumentare l'efficienza e migliorare l'innovazione. Tuttavia, poiché gli attacchi informatici diventano sempre più sofisticati, disporre di misure di sicurezza robuste è fondamentale per proteggere i dati sensibili, tutelarsi dalle violazioni e rispettare gli standard normativi negli ambienti di cloud ibrido. Di conseguenza, molte organizzazioni IT stanno investendo in piattaforme di sicurezza avanzate e implementando processi collaborativi incentrati sulla sicurezza per proteggere sistemi, carichi di lavoro e dati strategici. In effetti, la sicurezza IT è una priorità di finanziamento per quasi il 50% delle aziende.[1]

Prestando particolare attenzione ai carichi di lavoro dei container e a Kubernetes, Red Hat e Illuminas hanno condotto un sondaggio tra professionisti DevOps, ingegneri ed esperti di sicurezza di tutto il mondo che operano in aziende di piccole e grandi dimensioni. Sulla base di questi dati, l'edizione 2024 del report "The State of Kubernetes Security" esamina alcune delle sfide e degli impatti aziendali più comuni che le aziende devono affrontare al giorno d'oggi per la sicurezza cloud native. Analizziamo rischi specifici per la sicurezza che destano maggiori preoccupazioni per le organizzazioni, incluse le vulnerabilità legate alla catena di distribuzione del software e al runtime delle applicazioni, nonché le misure adottate per ridimensionarli. Identifichiamo i tipi e la frequenza degli incidenti di sicurezza che le imprese subiscono negli ambienti Kubernetes. Esaminiamo la distribuzione delle responsabilità legate alla sicurezza di Kubernetes tra i team che si occupano di sviluppo, sicurezza e operazioni per rivelare le ultime tendenze nell'adozione di DevSecOps. Infine, forniamo indicazioni per ridurre i rischi durante l'intero ciclo di vita delle applicazioni.

Anche se proteggere i container e Kubernetes in modo completo può rappresentare una sfida, farlo può aiutare a velocizzare l'innovazione e a offrire maggiore valore alla propria organizzazione. Utilizzando i risultati del nostro sondaggio, si potrà valutare la sicurezza di Kubernetes nel proprio caso per individuare aree di miglioramento e ottenere informazioni utili per colmare le lacune nella sicurezza. Perfezionando continuamente le misure di sicurezza, è possibile proteggere le risorse aziendali fondamentali e creare una cultura di sicurezza proattiva, garantendo l'integrità e la resilienza dell'infrastruttura e delle applicazioni.

Leggi il report per scoprire le 13 conclusioni chiave del nostro sondaggio.

*1 Report Red Hat. "**Global Tech Trends 2024**", febbraio 2024.*

Informazioni sul report

Per l'edizione 2024 di questo report, Red Hat ha sponsorizzato un sondaggio tra 600 professionisti DevOps, ingegneri ed esperti di sicurezza negli Stati Uniti (USA), nel Regno Unito (UK) e nella regione Asia Pacifico (APAC) di lingua inglese per comprendere le tendenze emergenti nell'ambito dei container, di Kubernetes e della sicurezza cloud native. I dati sono stati raccolti tramite interviste telefoniche e online della durata di 21 minuti e gli intervistati sono stati selezionati da gruppi online e database di terze parti. Il sondaggio è stato condotto nel dicembre 2023 e nel gennaio 2024.

Profilo degli intervistati:

- Professionisti del settore IT che si occupano di applicazioni, piattaforme, infrastrutture, operazioni, sicurezza, architettura del software o sviluppo
- Fanno parte di aziende con più di 100 dipendenti
- Operano in organizzazioni che dispongono di un team interno di sviluppo delle applicazioni
- Lavorano in aziende che utilizzano i container

Dati demografici degli intervistati

600
risposte totali raccolte

Professionisti DevOps

Professionisti della progettazione

Professionisti della sicurezza

25% 100-499 dipendenti
24% 500-999 dipendenti
52% Oltre 1000 dipendenti

26% Tecnologie
25% Servizi finanziari
24% Telecomunicazioni, media e intrattenimento
26% Altri settori

Conclusioni principali

Ancora una volta, il nostro sondaggio ha fornito molte informazioni sul modo in cui le organizzazioni affrontano la sicurezza di Kubernetes. Ecco alcuni punti chiave:

67% delle organizzazioni afferma di aver ritardato o rallentato il deployment a causa di problemi legati alla sicurezza di Kubernetes.

46% delle organizzazioni ha riscontrato perdite di fatturato o clienti dovute a un incidente legato alla sicurezza dei container o di Kubernetes.

42% degli intervistati ha citato la sicurezza come una delle principali preoccupazioni quando si tratta di strategie di containerizzazione e Kubernetes.

42% degli intervistati riferisce di avere iniziative DevSecOps in fase avanzata all'interno della propria organizzazione.

48% delle organizzazioni ha avviato iniziative DevSecOps nelle fasi iniziali, con team che collaborano su criteri e flussi di lavoro congiunti.

33% degli intervistati ritiene che la soluzione di sicurezza per container e Kubernetes attualmente in uso rallenti lo sviluppo.

30% degli intervistati ha indicato le vulnerabilità come la preoccupazione principale quando si parla di ambienti containerizzati e Kubernetes.

Per saperne di più sulle conclusioni del sondaggio, continua a leggere il report.

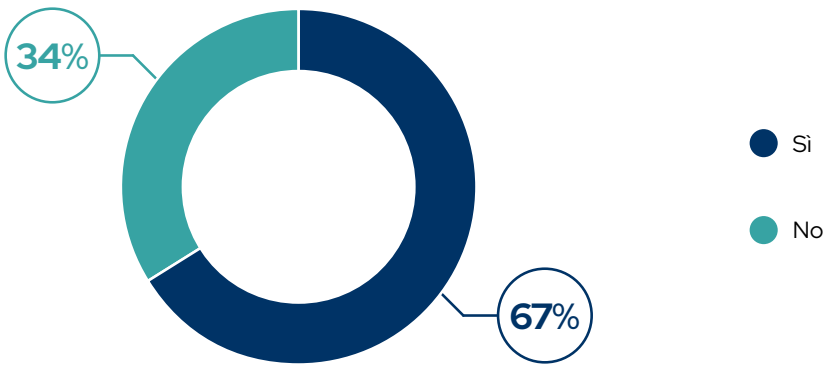
Conclusione 1

I problemi di sicurezza continuano a influire sui risultati aziendali

I problemi di sicurezza hanno costretto il 67% delle aziende a ritardare o rallentare il deployment delle applicazioni.

In tutto il mondo, le organizzazioni adottano tecnologie cloud native come Kubernetes e architetture basate su microservizi per trasformare le loro modalità di compilazione, esecuzione e scalabilità delle applicazioni. Mentre alcune organizzazioni sviluppano tutti i nuovi software come microservizi, molte eseguono il refactoring delle applicazioni esistenti utilizzando tecnologie containerizzate. In entrambi i casi, i container possono velocizzare i cicli di sviluppo e rilascio, aumentando al contempo la flessibilità di esecuzione e gestione delle applicazioni in ambienti ibridi. Tuttavia, la sicurezza incompleta durante tutto il ciclo di vita delle applicazioni, dallo sviluppo al deployment e alla manutenzione, può ridurre questi preziosi vantaggi. In effetti, dal nostro sondaggio è emerso che il 67% degli intervistati ha ritardato o rallentato il deployment di applicazioni containerizzate a causa di problemi di sicurezza.

Ha mai ritardato o rallentato il deployment di un'applicazione in produzione a causa di problemi legati alla sicurezza dei container o di Kubernetes?



D27. Ha mai ritardato o rallentato il deployment di un'applicazione in produzione a causa di problemi legati alla sicurezza dei container o di Kubernetes? Base di intervistati: totale = 600

A causa dell'arrotondamento, il totale delle percentuali potrebbe non corrispondere al 100%.

Conclusione 2

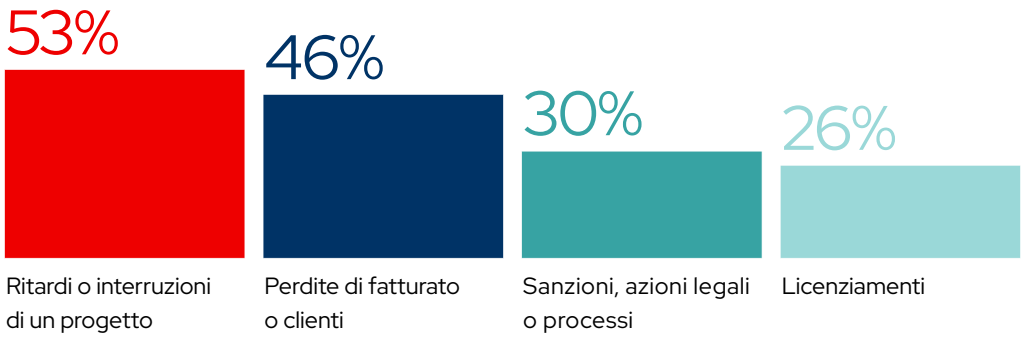
Le violazioni della sicurezza riguardano tutti

Gli incidenti legati alla sicurezza comportano conseguenze di ampio respiro, tra cui licenziamenti e perdite di fatturato.

L'impatto dei problemi di sicurezza di container e Kubernetes può andare ben oltre il ritardo nel deployment delle applicazioni. Il 26% degli intervistati ha dichiarato che un incidente di sicurezza ha avuto come conseguenza un licenziamento, mentre il 30% ha riferito che la propria organizzazione è stata multata a causa di un incidente. In queste situazioni, la perdita di talenti, conoscenze ed esperienza di valore può avere un impatto significativo sulle operazioni, mentre sanzioni e pubblicità negativa possono comportare notevoli oneri finanziari per le aziende.

Il 46% degli intervistati ha anche rivelato che la propria organizzazione ha subito perdite di fatturato o clienti a seguito di un incidente legato alla sicurezza. Le violazioni della sicurezza possono rallentare la crescita aziendale quando i team rimandano progetti o nuove versioni dei prodotti per risolvere i problemi. E se i clienti perdono fiducia nelle capacità di protezione dei dati di un'azienda, potrebbero rivolgersi a concorrenti che adottano pratiche più sicure.

Negli ultimi 12 mesi, la sua azienda ha riscontrato uno o più dei seguenti effetti in seguito a problemi o incidenti legati alla sicurezza o alla conformità di container/Kubernetes?



D29. Negli ultimi 12 mesi, la sua azienda ha riscontrato uno o più dei seguenti effetti in seguito a problemi o incidenti legati alla sicurezza o alla conformità di container/Kubernetes? Base di intervistati: totale = 600

Conclusione 3

Gli incidenti di sicurezza si verificano in tutte le fasi del ciclo di vita di un'applicazione

Quasi 9 organizzazioni su 10 hanno avuto almeno un incidente di sicurezza legato ai container o a Kubernetes negli ultimi 12 mesi.

Gli incidenti di sicurezza correlati a container e Kubernetes non si verificano solo durante l'esecuzione delle applicazioni, anzi, possono influire su tutte le fasi del loro ciclo di vita. Il 45% degli intervistati ha riferito che la propria organizzazione è stata coinvolta in incidenti di runtime negli ultimi 12 mesi, mentre un numero quasi uguale (44%) ha dichiarato di aver riscontrato problemi nelle fasi di creazione e deployment, menzionando gravi vulnerabilità da correggere. Allo stesso tempo, il 40% ha affermato che la propria organizzazione ha rilevato errori di configurazione nei propri ambienti containerizzati o Kubernetes e il 26% ha riferito che la propria organizzazione non ha superato un audit.

Le tecnologie dei container e Kubernetes possono aumentare la produttività grazie a funzionalità trasversali e operazioni semplificate. Sebbene Kubernetes fornisca meccanismi come criteri di rete e il controllo degli accessi basato sui ruoli per migliorare la sicurezza all'interno del cluster, alcune funzioni sono eccessivamente permissive o disabilitate per impostazione predefinita e richiedono una configurazione aggiuntiva per garantire una protezione sufficiente. Inoltre, nonostante i controlli di sicurezza come **SELinux** possano aumentare significativamente la sicurezza delle applicazioni, possono risultare difficili da personalizzare e integrare in un ambiente operativo. Queste difficoltà spesso si manifestano come incidenti di sicurezza, vulnerabilità e configurazioni errate in diverse fasi del ciclo di vita delle applicazioni. I risultati del sondaggio dimostrano che molte organizzazioni hanno ancora difficoltà ad affrontare la complessità di proteggere gli ambienti Kubernetes containerizzati, poiché l'89% ha segnalato almeno un incidente legato alla sicurezza negli ultimi 12 mesi.

Negli ultimi 12 mesi, quali incidenti o problemi di sicurezza correlati ai container e/o a Kubernetes ha riscontrato?

D28. Negli ultimi 12 mesi, quali incidenti o problemi di sicurezza correlati ai container e/o a Kubernetes ha riscontrato? Base di intervistati: totale = 600

Conclusione 4

Le attuali strategie di sicurezza dei container destano preoccupazioni

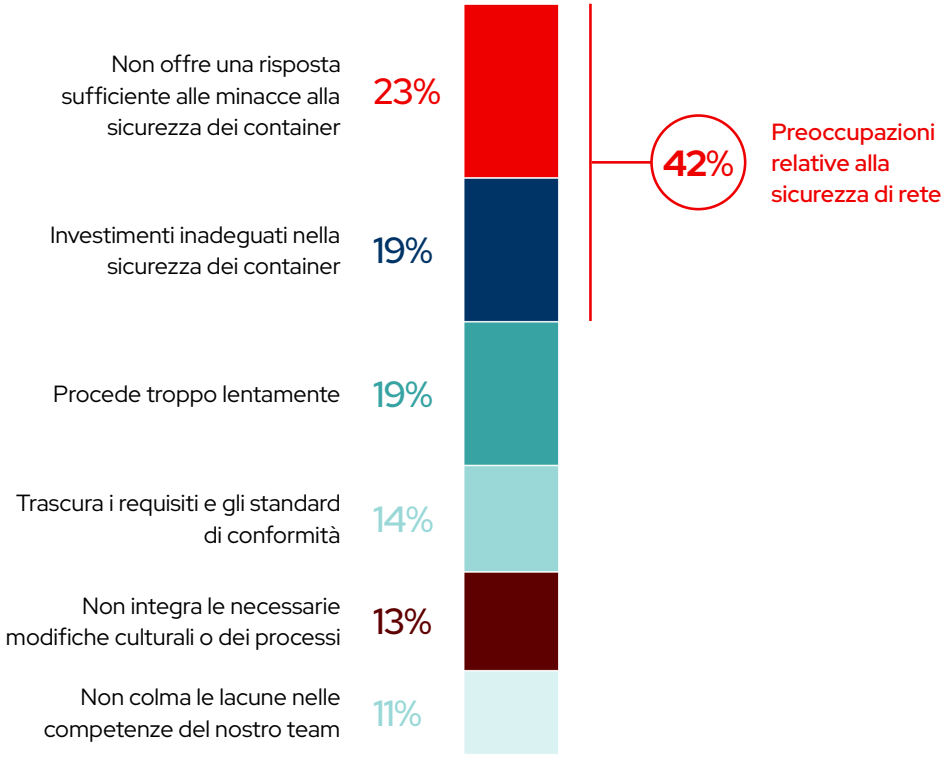
Il 42% degli intervistati ritiene che la propria azienda non investa nella sicurezza dei container o affronti le minacce correlate in modo sufficiente.

Man mano che le organizzazioni adottano ambienti containerizzati per semplificare il deployment e la scalabilità delle applicazioni, devono anche adattare i propri processi di sicurezza a questi sistemi dinamici e distribuiti. Kubernetes e i container integrano nuovi livelli software che possono aumentare la complessità e introdurre ulteriori rischi per la sicurezza dell'infrastruttura chiave. Con l'aggiunta di potenziali punti di

accesso per le minacce informatiche, sono necessarie misure di sicurezza robuste per proteggersi da vulnerabilità, accessi non autorizzati e violazioni dei dati. Tuttavia, alcuni intervistati sono scettici sulla strategia di containerizzazione della loro azienda. Il 23% ritiene che la strategia della propria organizzazione non risponda in modo sufficiente alle minacce alla sicurezza dei container, mentre il 19% crede che gli investimenti nella sicurezza dei container siano inadeguati.

Una protezione completa di container e Kubernetes inizia con la comprensione della complessità e dei potenziali rischi per la sicurezza degli ambienti moderni. Implementando controlli che coprono tutti i livelli dello stack software, tra cui l'infrastruttura alla base, il piano di controllo Kubernetes, la rete, le immagini e i registri dei container, si può iniziare a ridurre i rischi per le applicazioni cloud native.

Qual è la sua più grande preoccupazione riguardo alla strategia di containerizzazione dell'azienda?



D7. Qual è la sua più grande preoccupazione riguardo alla strategia di containerizzazione dell'azienda? Base di intervistati: totale = 600

A causa dell'arrotondamento, il totale delle percentuali potrebbe non corrispondere al 100%.

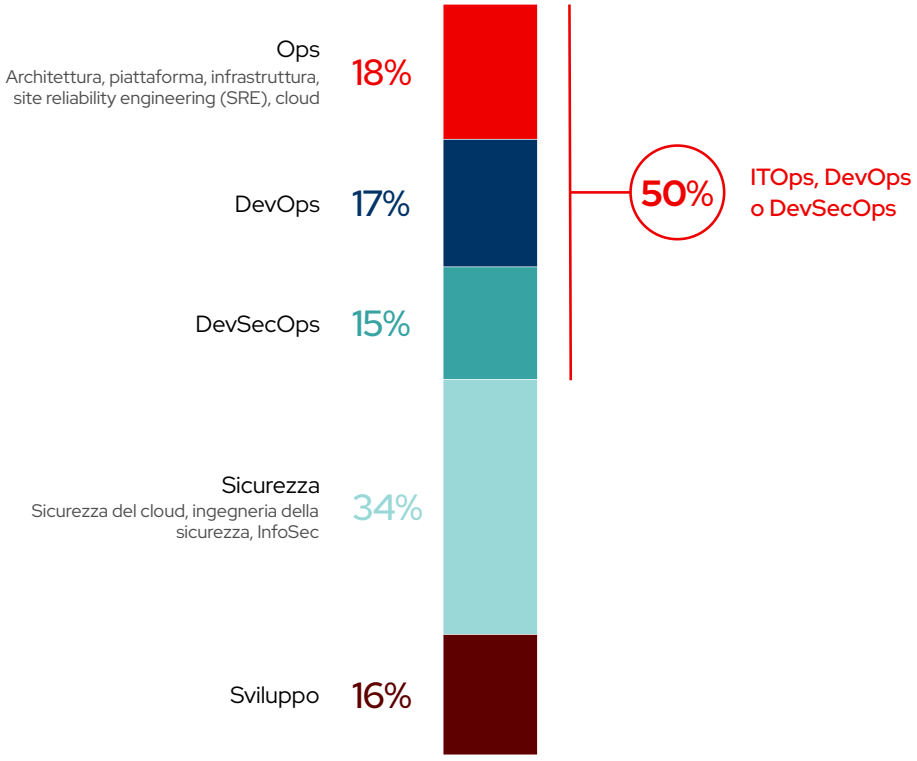
Conclusione 5

La responsabilità della sicurezza è altamente decentralizzata

Solo un terzo degli intervistati ha affermato che i propri team di sicurezza sono responsabili della sicurezza di Kubernetes.

In molte organizzazioni, ci sono più gruppi che collaborano per creare e distribuire carichi di lavoro in ambienti Kubernetes containerizzati. I risultati del sondaggio dimostrano che non esiste un'unica figura responsabile della sicurezza di Kubernetes in tutte le organizzazioni.

Nella sua azienda, quale ruolo è il principale responsabile della sicurezza dei container e di Kubernetes?



D9. Nella sua azienda, quale ruolo è il principale responsabile della sicurezza dei container e di Kubernetes? Base di intervistati: totale = 600

Solo il 34% degli intervistati complessivi ha dichiarato che i team di sicurezza sono maggiormente responsabili della sicurezza dei container e di Kubernetes all'interno della propria organizzazione. Nel 50% delle organizzazioni, sono vari ruoli operativi ad avere questa responsabilità, tra cui ITOps, DevOps e DevSecOps. È interessante notare che nelle organizzazioni dell'area APAC è più probabile che sia una figura DevSecOps ad avere maggiore responsabilità (21%).

Le tecnologie e i processi avanzati di sicurezza di Kubernetes possono promuovere una stretta collaborazione tra team diversi e rimuovere gli ostacoli che isolano gli esperti dei diversi settori. Gli sviluppatori possono creare e integrare software personalizzati, componenti open source e immagini dei container. Gli esperti di sicurezza possono definire e implementare criteri e controlli in tutte le risorse del cluster, mentre i team operativi possono gestire l'infrastruttura dei cluster, i controlli degli accessi e i meccanismi di autorizzazione utilizzando un unico set di soluzioni di sicurezza comuni.

Conclusione 6

Le pratiche DevSecOps sono comuni in tutte le organizzazioni

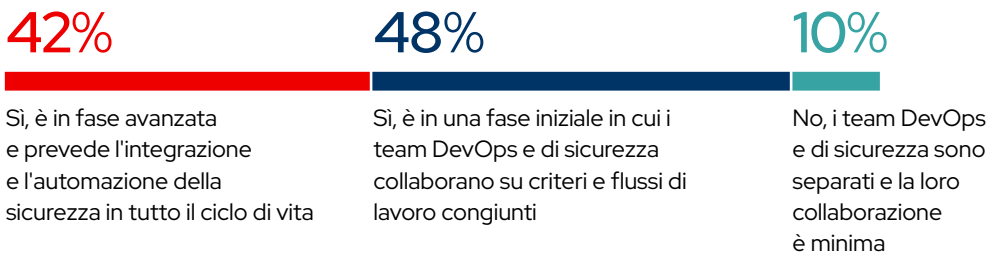
Il 42% degli intervistati ha in atto un'iniziativa DevSecOps in fase avanzata all'interno della propria organizzazione.

Le organizzazioni continuano a adottare pratiche DevSecOps per identificare e mitigare i rischi per la sicurezza nelle prime fasi dei processi di deployment di container e Kubernetes. Il 42% degli intervistati afferma che la propria organizzazione integra e automatizza la sicurezza durante l'intero ciclo di vita delle applicazioni utilizzando processi e strumenti DevSecOps come test automatizzati, monitoraggio continuo e revisioni del codice.

Allo stesso tempo, il 48% dichiara che la propria organizzazione comprende il valore di DevSecOps ed è nelle prime fasi di adozione, con team di sviluppo, operazioni e sicurezza che collaborano su criteri e flussi di lavoro congiunti. Si tratta di un aumento

significativo rispetto allo scorso anno, quando solo il 39% degli intervistati si trovava in questa fase. Per il restante 10% delle organizzazioni, team DevOps e di sicurezza separati possono portare a processi reattivi che risolvono le vulnerabilità solo durante il deployment o il runtime, con conseguente riduzione dell'efficienza, della velocità e della qualità del software, oltre a una distribuzione più lenta delle applicazioni.

La sua organizzazione ha previsto un'iniziativa DevSecOps?



D25. La sua organizzazione ha previsto un'iniziativa DevSecOps? Base di intervistati: totale = 600

Conclusione 7

Gli ambienti Kubernetes fanno emergere nuove sfide legate alla sicurezza

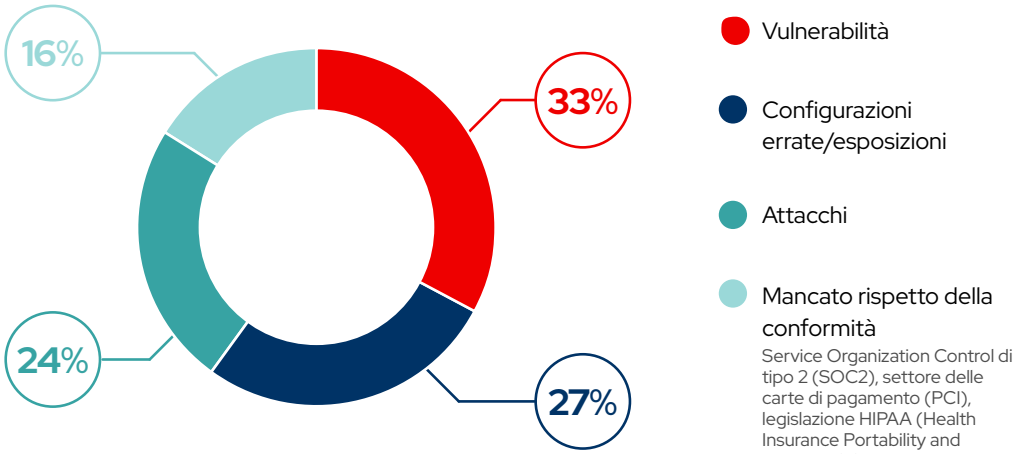
Il 60% degli intervistati si preoccupa di vulnerabilità, configurazioni errate ed esposizioni nei propri ambienti containerizzati e Kubernetes.

Mitigare le vulnerabilità in ambienti Kubernetes e containerizzati complessi e dinamici può essere difficile. Poiché i container condividono risorse host come i kernel del sistema operativo, una singola vulnerabilità in uno di essi può avere un impatto su più container. Inoltre, una vulnerabilità in un host può influire su tutti i container distribuiti nel sistema. Gli intervistati sono chiaramente consapevoli di questa difficoltà, tanto che per il 33% di loro la maggior preoccupazione è rappresentata dalle vulnerabilità nel proprio ambiente containerizzato e Kubernetes.

Il 27% degli intervistati ha come preoccupazione principale i componenti configurati in modo errato, tra cui immagini di base, librerie e dipendenze, che possono causare gravi problemi di sicurezza in interi ambienti. Se non adeguatamente convalidati e gestiti, questi componenti possono fungere da potenziali punti di attacco e compromettere l'integrità e la riservatezza di applicazioni chiave e dati sensibili.

Sebbene tali preoccupazioni siano giustificate, possono essere attenuate con processi di sicurezza completi. Ad esempio, l'implementazione di una scansione automatica e continua della sicurezza può aiutare a rilevare e correggere le vulnerabilità comuni e garantire la corretta configurazione dei componenti sensibili dal punto di vista della sicurezza.

Tra i seguenti rischi, quale rappresenta la maggiore fonte di preoccupazione rispetto agli ambienti containerizzati e Kubernetes della sua organizzazione?



D10. Tra i seguenti rischi, quale rappresenta la maggiore fonte di preoccupazione rispetto agli ambienti containerizzati e Kubernetes della sua organizzazione? Base di intervistati: totale = 600

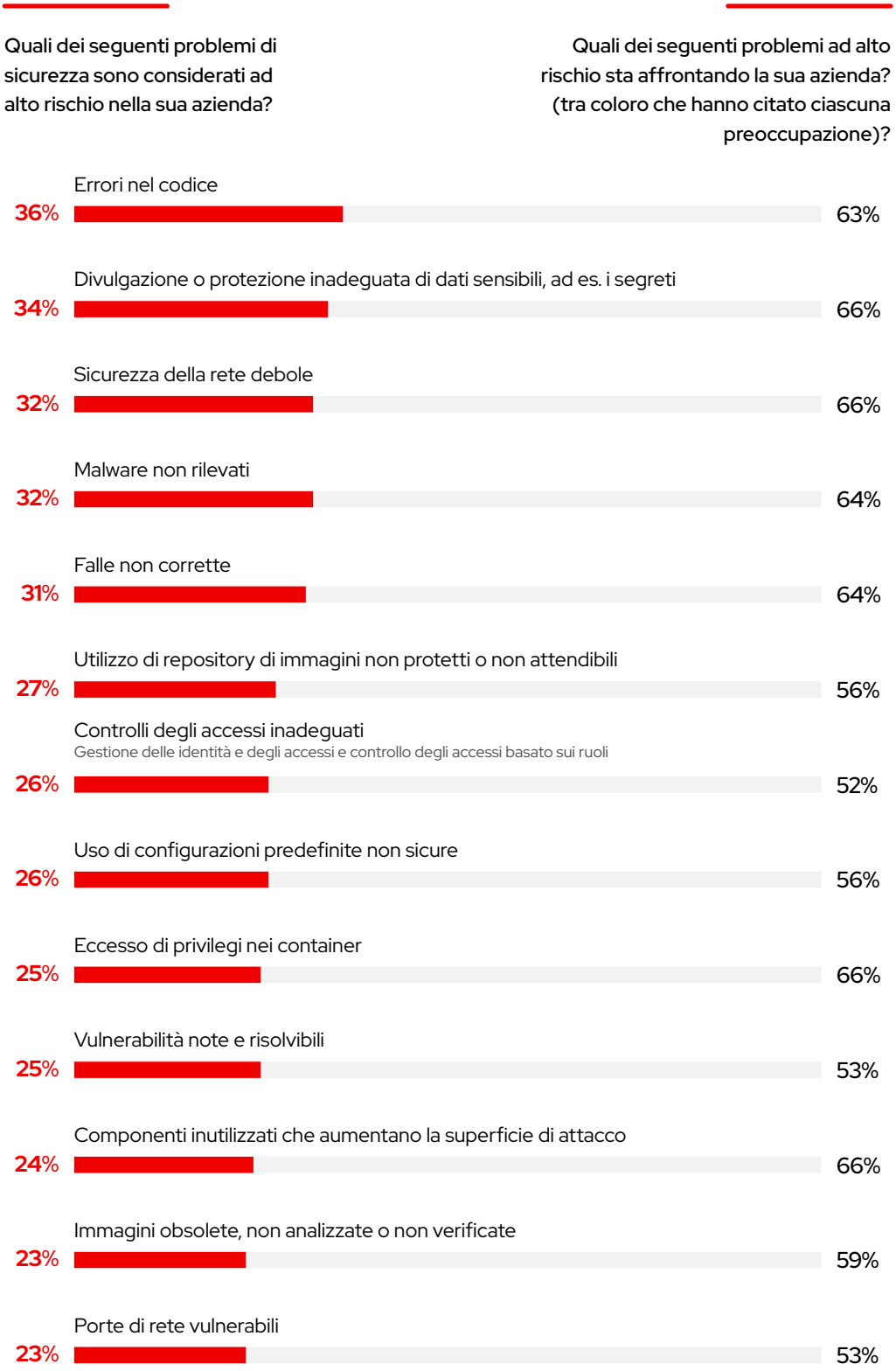
Conclusione 8

Le organizzazioni stanno lavorando attivamente sui problemi ad alto rischio

Gli errori nel codice, i dati sensibili non protetti, la scarsa sicurezza della rete e i malware non rilevati rappresentano i rischi più elevati per la sicurezza.

Nel complesso, le organizzazioni non hanno un unico rischio per la sicurezza che ritengono più grave di tutti gli altri, ma sono preoccupate quasi allo stesso modo per una serie di potenziali problemi. Dagli errori di codifica (36%) ai dati sensibili esposti (34%), dalla scarsa sicurezza della rete (32%) ai malware non rilevati (32%), questi rischi per la sicurezza mettono in luce la necessità di strategie complete per mitigare le vulnerabilità e proteggersi dalle minacce informatiche. Un'analisi completa dei componenti di Kubernetes e dei container può identificare vulnerabilità e configurazioni errate per contribuire a implementare misure di correzione mirate in tutto l'ambiente containerizzato. Robuste misure di sicurezza sviluppate su misura in base ai requisiti delle applicazioni possono ridurre efficacemente i rischi, proteggere i dati sensibili e difendere dalle minacce, mentre i controlli di sicurezza intuitivi integrati nell'intero ciclo di vita delle applicazioni possono migliorare la conformità e ridurre il rischio di errore umano.

In base ai risultati del sondaggio, le organizzazioni stanno lavorando attivamente per ridurre i problemi ad alto rischio nei loro ambienti containerizzati e Kubernetes e più della metà delle aziende intervistate si sta focalizzando su tutte le criticità. Allo stesso tempo, il 66% delle organizzazioni sta affrontando minacce relative a dati sensibili esposti, scarsa sicurezza della rete, container con eccesso di privilegi e componenti inutilizzati.



D13. Quali dei seguenti problemi di sicurezza sono considerati ad alto rischio nella sua azienda? Base di intervistati: totale = 600

D14. Quali dei seguenti problemi ad alto rischio sta affrontando la sua azienda? Base di intervistati: tra coloro che hanno citato ciascuna preoccupazione= 139 - 213

Conclusione 9

I problemi di sicurezza possono portare a gravi conseguenze

Più della metà delle organizzazioni ha riscontrato l'esecuzione non autorizzata di processi nei propri ambienti.

Molti problemi di sicurezza ad alto rischio, dall'esecuzione non autorizzata di processi (45%) all'esposizione di dati sensibili (43%) e al ransomware (41%), preoccupano gli intervistati. Questo mette in luce quanto sia importante proteggersi da una serie di minacce che possono compromettere l'integrità, la riservatezza e la disponibilità di dati e sistemi. L'esecuzione non autorizzata dei processi comporta un rischio significativo, consentendo agli utenti malintenzionati di infiltrarsi nei sistemi, interrompere le operazioni e accedere a informazioni sensibili. L'esposizione di dati sensibili solleva preoccupazioni in merito alla conformità normativa e ai danni finanziari e reputazionali derivanti da violazioni dei dati. Inoltre, gli attacchi ransomware possono causare interruzioni significative e perdite finanziarie per le organizzazioni.

Queste preoccupazioni sono giustificate: per ogni problema di sicurezza ad alto rischio identificato nel nostro sondaggio, sono più gli intervistati che lo hanno effettivamente vissuto rispetto a quelli che lo ritenevano preoccupante. Ad esempio, la preoccupazione principale è stata l'esecuzione non autorizzata dei processi, citata dal 45% degli intervistati, ma è stato il 52% a riferire che la propria organizzazione ha effettivamente sperimentato un qualche tipo di processo non autorizzato solo negli ultimi 12 mesi. Questa discrepanza è ancora maggiore per l'accesso non autorizzato alle risorse cloud interne, gli attacchi denial of service, le credenziali compromesse e i movimenti laterali non autorizzati. Ad aver vissuto direttamente uno di questi problemi senza averli precedentemente considerati una delle principali preoccupazioni è stato l'11-15% in più delle organizzazioni.

	Quali dei seguenti problemi ad alto rischio la preoccupa di più?	Negli ultimi 12 mesi, quali dei seguenti problemi ad alto rischio ha riscontrato la sua azienda? (tra coloro che hanno citato ciascuna preoccupazione)?
Esecuzione di malware, hackeraggio di risorse, mining di criptovalute o esecuzione di altri processi non autorizzati	45%	52%
Esposizione di dati sensibili come le informazioni personali	43%	44%
Ransomware	41%	47%
Accesso non autorizzato a risorse cloud interne	35%	46%
Perdita di dati	34%	37%
Attacco denial of service	33%	48%
Credenziali compromesse	32%	44%
Movimento laterale non autorizzato	32%	46%

D15. Quali dei seguenti problemi ad alto rischio la preoccupa di più? Base di intervistati: totale = 600

D16. Negli ultimi 12 mesi, quali dei seguenti problemi ad alto rischio ha riscontrato la sua azienda? Base di intervistati: tra coloro che hanno citato ciascuna preoccupazione = 189 - 270

Conclusione 10

La gestione dei rischi è fondamentale per la catena di distribuzione del software

Il 44% degli intervistati afferma che le vulnerabilità del software sono l'aspetto più ad alto rischio delle catene di distribuzione del software: un aumento del 9% rispetto allo scorso anno.

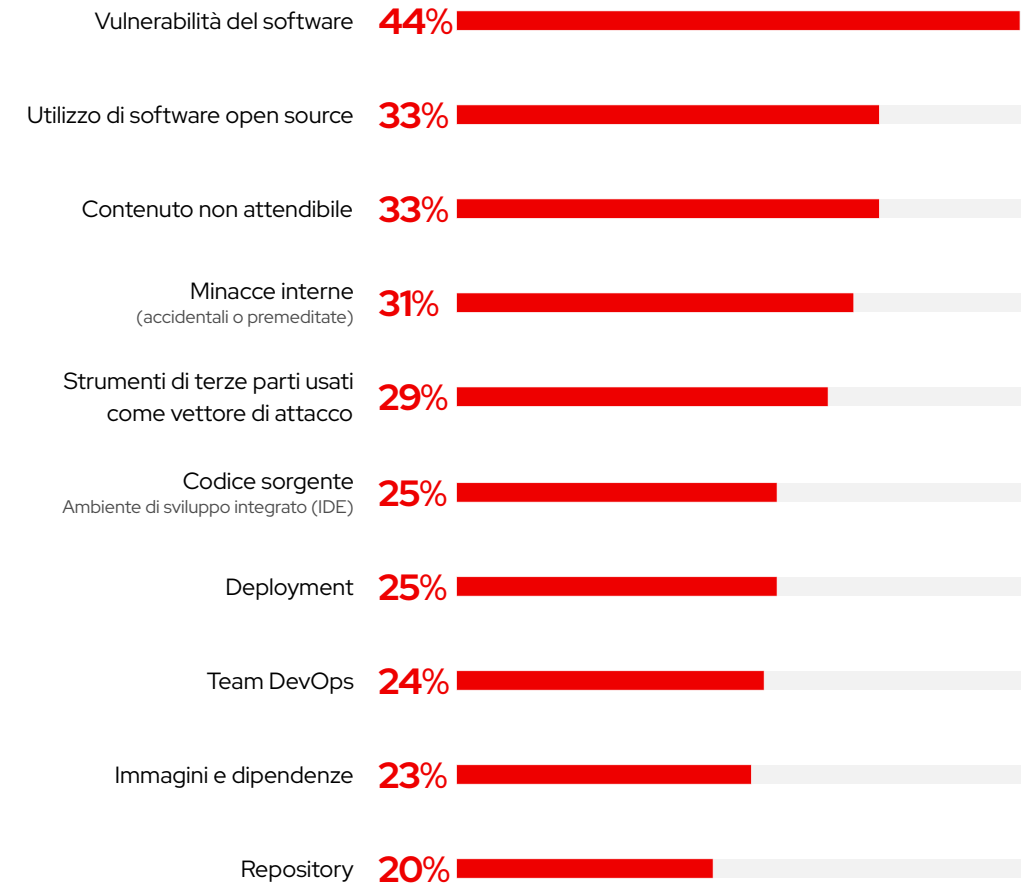
Proteggere le catene di distribuzione del software può essere difficile a causa della loro complessità intrinseca e della portata globale. Le catene di distribuzione spesso integrano software di diversi fornitori commerciali e progetti open source, pertanto è fondamentale garantire l'integrità, l'autenticità e la sicurezza di ogni componente.

Abbiamo chiesto agli intervistati di identificare gli aspetti più a rischio delle catene di distribuzione del software. Le vulnerabilità del software (44%), il software open source (33%) e i contenuti non attendibili (33%) si sono classificati ai primi posti. Questo risultato non sorprende, dato che ciascuno di questi aspetti può comportare gravi conseguenze. Le vulnerabilità del software possono causare incidenti di sicurezza come violazioni dei dati e l'esecuzione di malware. Il software open source deve essere adeguatamente esaminato, scansionato e gestito per ridurre il rischio di introdurre nuove vulnerabilità. Inoltre, i contenuti non attendibili possono compromettere l'integrità del sistema e consentire l'accesso non autorizzato.

In particolare, le preoccupazioni relative alle vulnerabilità del software sono aumentate del 9%: dal 35% del 2023 al 44% di quest'anno. E gli intervistati che operano del settore tecnologico hanno dato un peso ancora più rilevante a questa voce, raggiungendo il 51%. Abbiamo anche riscontrato che gli intervistati di piccole aziende hanno classificato le minacce interne più in alto della media, raggiungendo il 36% rispetto al 31% complessivo.

Le organizzazioni possono affrontare queste sfide con un approccio completo alla sicurezza della catena di distribuzione del software che include valutazioni rigorose dei fornitori, procedure di programmazione incentrate sulla sicurezza e il monitoraggio continuo delle dipendenze del software. Dando la priorità alla sicurezza in ogni fase della catena di distribuzione del software, è possibile ridurre al minimo i rischi, proteggersi dalle minacce informatiche e garantire l'integrità del software distribuito a utenti e stakeholder.

Quali aspetti della sicurezza della catena di distribuzione del software rappresentano il rischio più elevato?



D30. Quali aspetti della sicurezza della catena di distribuzione del software rappresentano il rischio più elevato? Base di intervistati: totale = 600

Conclusione 11

Le preoccupazioni per la sicurezza della catena di distribuzione del software sono giustificate

Il 57% delle organizzazioni ha rilevato componenti di applicazioni vulnerabili nella catena di distribuzione del software negli ultimi 12 mesi.

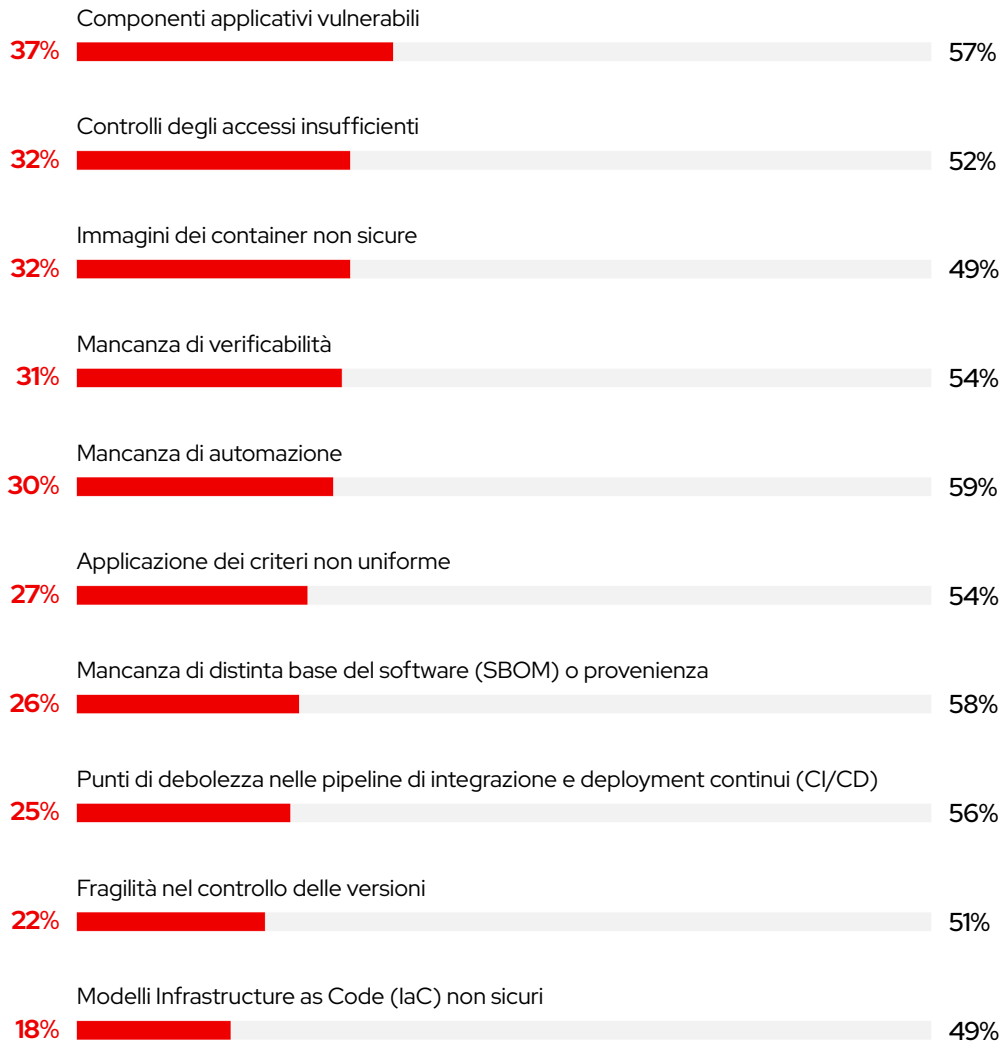
La sicurezza della catena di distribuzione del software contribuisce a garantire integrità, riservatezza e disponibilità per l'intero ciclo di vita delle applicazioni. Adottando robuste misure di sicurezza, le organizzazioni possono ridurre il rischio di attacchi alla catena di distribuzione, accessi non autorizzati e violazioni dei dati per salvaguardare le risorse digitali e mantenere la fiducia di clienti e stakeholder.

Tuttavia, gli intervistati hanno espresso molti dubbi legati alla sicurezza delle catene di distribuzione del software delle proprie organizzazioni, inclusi componenti applicativi vulnerabili (37%), controlli degli accessi insufficienti (32%) e immagini dei container non sicure (32%). Come per i problemi generali di sicurezza (**Conclusione 9**), queste preoccupazioni sono giustificate. Quasi tutte le problematiche individuate nel sondaggio sono state realmente affrontate da oltre la metà delle organizzazioni partecipanti. I componenti applicativi vulnerabili, la scarsa automazione e la mancanza di distinte base del software (SBOM) hanno avuto un impatto quasi sul 60% delle aziende.

Inoltre, le organizzazioni che hanno affrontato un problema per cui non erano inizialmente preoccupate sono almeno 1,5 in più per ogni categoria. Le quattro problematiche che destavano meno preoccupazioni (mancanza di SBOM, punti di debolezza nelle pipeline di integrazione e deployment continui, fragilità nel controllo delle versioni e modelli Infrastructure as Code non sicuri) sono state affrontate da più del doppio delle organizzazioni che ne erano preoccupate.

Quali dei seguenti problemi di sicurezza relativi alla catena di distribuzione del software preoccupano maggiormente la sua azienda?

Negli ultimi 12 mesi, quali dei seguenti problemi di sicurezza relativi alla catena di distribuzione del software ha riscontrato la sua azienda? (tra coloro che hanno citato ciascuna preoccupazione)?



D32. Quali dei seguenti problemi di sicurezza relativi alla catena di distribuzione del software preoccupano maggiormente la sua azienda? Base di intervistati: totale = 600

D33. Negli ultimi 12 mesi, quali dei seguenti problemi di sicurezza relativi alla catena di distribuzione del software ha riscontrato la sua azienda? Base di intervistati: tra coloro che hanno citato ciascuna preoccupazione = 107 - 223

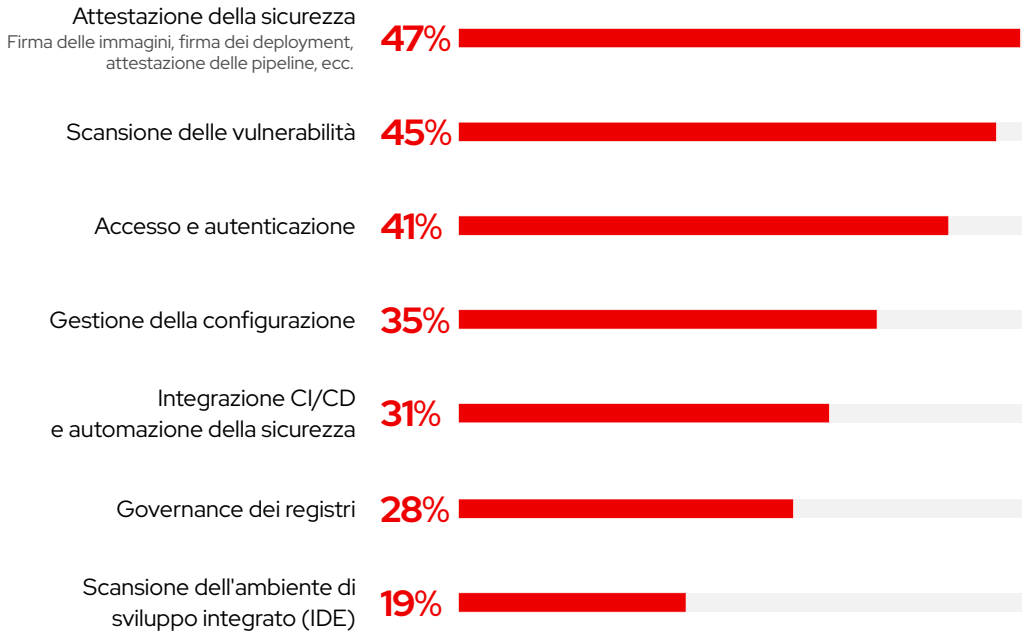
Conclusione 12

Strumenti e processi supportano la sicurezza della catena di distribuzione del software

Quasi la metà degli intervistati considera l'attestazione di sicurezza come un controllo di sicurezza chiave della catena di distribuzione del software.

Le organizzazioni mitigano le vulnerabilità e proteggono le catene di distribuzione del software essenziali con un assortimento di strumenti e tecnologie di sicurezza avanzati, tra cui attestazione della sicurezza (47%), scansione delle vulnerabilità (45%) e meccanismi di accesso e autenticazione (41%). Verificando l'origine, l'autenticità e la

Quali dei seguenti aspetti ritiene più importanti quando si parla della sicurezza della catena di distribuzione del software?



D31. Quali dei seguenti aspetti ritiene più importanti quando si parla della sicurezza della catena di distribuzione del software? Selezionare fino a 3 opzioni. Base di intervistati: totale = 600

conformità di ciascun componente software agli standard di sicurezza, l'attestazione della sicurezza aiuta a garantire l'integrità e l'affidabilità delle applicazioni. La scansione delle vulnerabilità consente di affrontare in modo proattivo i rischi per la sicurezza, prima che possano essere sfruttati, identificando e risolvendo potenziali punti deboli e vulnerabilità nella catena di distribuzione del software. Grazie a meccanismi come l'autenticazione a più fattori (MFA) e il controllo degli accessi basato sui ruoli, è possibile ridurre il rischio di accesso non autorizzato a componenti software e dati sensibili.

Conclusione 13

Le organizzazioni utilizzano strumenti open source per la sicurezza di Kubernetes

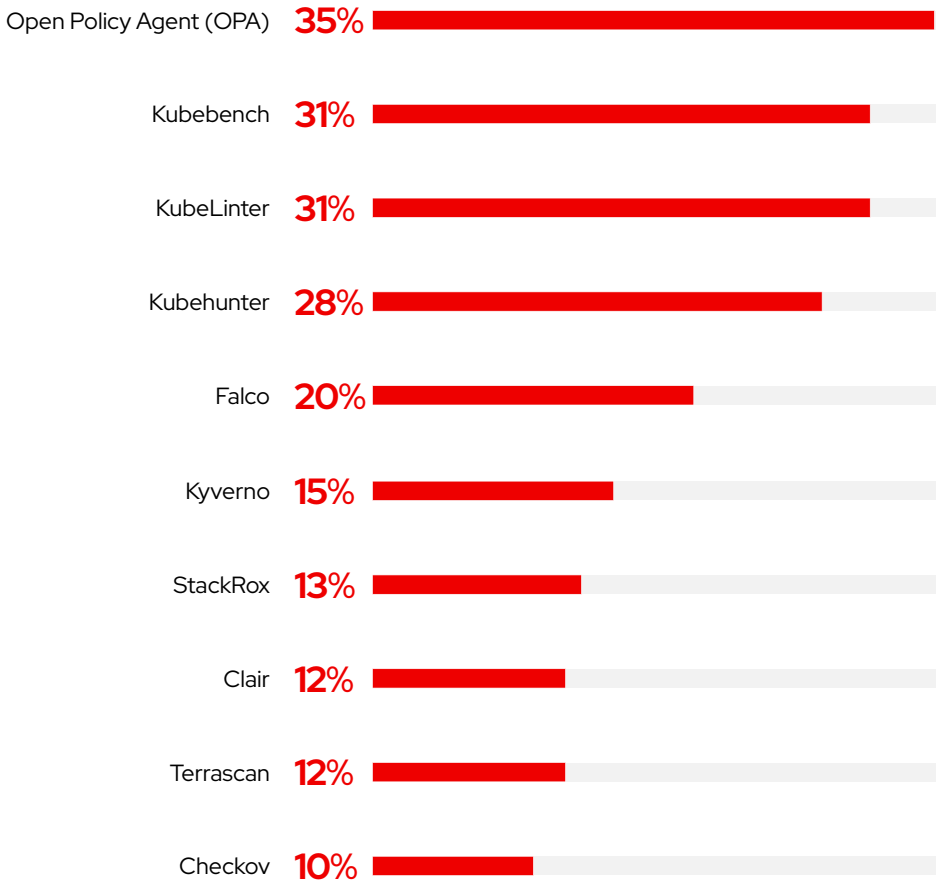
Open Policy Agent, Kube-bench e KubeLinter sono gli strumenti di sicurezza di Kubernetes open source più diffusi.

Un ecosistema completo di strumenti open source, con tecnologie avanzate sviluppate da collaboratori dedicati, fornisce una gamma di soluzioni di sicurezza per ambienti containerizzati e Kubernetes. Le organizzazioni partecipanti si affidano a molti di questi strumenti di sicurezza open source per proteggere le loro applicazioni cloud native:

- Il 35% semplifica la gestione delle policy con **Open Policy Agent**, un set di strumenti e un framework per policy unificate in stack cloud native.
- Il 31% confronta la sicurezza del deployment di Kubernetes rispetto al **CIS Kubernetes Benchmark** utilizzando **Kube-bench**.
- Il 31% garantisce che le applicazioni aderiscano alle procedure consigliate con **KubeLinter**, uno strumento di analisi statica per i file YAML Kubernetes e i grafici Helm.
- Il 28% identifica i problemi di sicurezza nei cluster Kubernetes e negli ambienti cloud native utilizzando **Kube-hunter**, uno strumento di analisi e scansione di sicurezza.

Nel complesso, le organizzazioni utilizzano in media 2,1 strumenti open source correlati alla sicurezza all'interno dei loro ambienti Kubernetes.

Quale dei seguenti strumenti open source utilizza per la sicurezza di Kubernetes?



D20. Quale dei seguenti strumenti open source utilizza per la sicurezza di Kubernetes? Base di intervistati: totale = 600

Migliora la sicurezza dei container e di Kubernetes

I container e Kubernetes possono velocizzare lo sviluppo e il deployment delle applicazioni in ambienti di cloud ibrido. L'integrazione di tecnologie e processi incentrati sulla sicurezza durante l'intero ciclo di vita consente di: proteggere le applicazioni senza rallentare lo sviluppo o aumentare la complessità operativa; tutelare i dati sensibili, la proprietà intellettuale e le informazioni dei clienti; soddisfare i requisiti normativi aziendali, settoriali e governativi; garantire la continuità operativa; mantenere la fiducia dei clienti; ridurre i costi degli interventi di correzione tardivi.

Ecco tre suggerimenti per rendere più sicuri gli ambienti cloud native.

1 Utilizzare i controlli di sicurezza Kubernetes native

La sicurezza Kubernetes native utilizza dati dichiarativi e controlli nativi per proteggere i carichi di lavoro dei container.

- Analizza i dati dichiarativi disponibili in Kubernetes per ottenere informazioni basate sul rischio in merito alla gestione della configurazione, alla conformità, alla segmentazione e alle vulnerabilità.
- Semplifica e velocizza l'analisi e la risoluzione dei problemi utilizzando la stessa infrastruttura e i controlli per lo sviluppo e la sicurezza.
- Riduce i conflitti operativi grazie all'automazione e alla scalabilità della sicurezza.

2 Estendere la sicurezza per tutto il ciclo di vita delle applicazioni

Un'attenzione alla sicurezza durante tutte le fasi del ciclo di vita delle applicazioni può aiutare a identificare e mitigare le potenziali vulnerabilità nelle fasi iniziali, riducendo il rischio di violazioni dei dati, attacchi informatici e compromissione della fiducia degli utenti.

- Integra le procedure consigliate DevSecOps e i controlli interni con i controlli di configurazione dentro la piattaforma di sicurezza utilizzata.
- Automatizza le valutazioni della sicurezza della configurazione Kubernetes utilizzando la piattaforma per container e Kubernetes preferita.

3 Adottare strumenti che supportino le pratiche DevSecOps

Le tecnologie e le soluzioni di sicurezza giuste possono aumentare la collaborazione tra i team che si occupano di sviluppo, sicurezza e operazioni.

- Utilizza la piattaforma per container e Kubernetes per eseguire valutazioni dei rischi e fornire controlli di sicurezza per gli ambienti.
- Adotta strumenti in grado di identificare e spiegare le vulnerabilità nei deployment effettivi per comprendere e applicare pratiche incentrate sulla sicurezza.

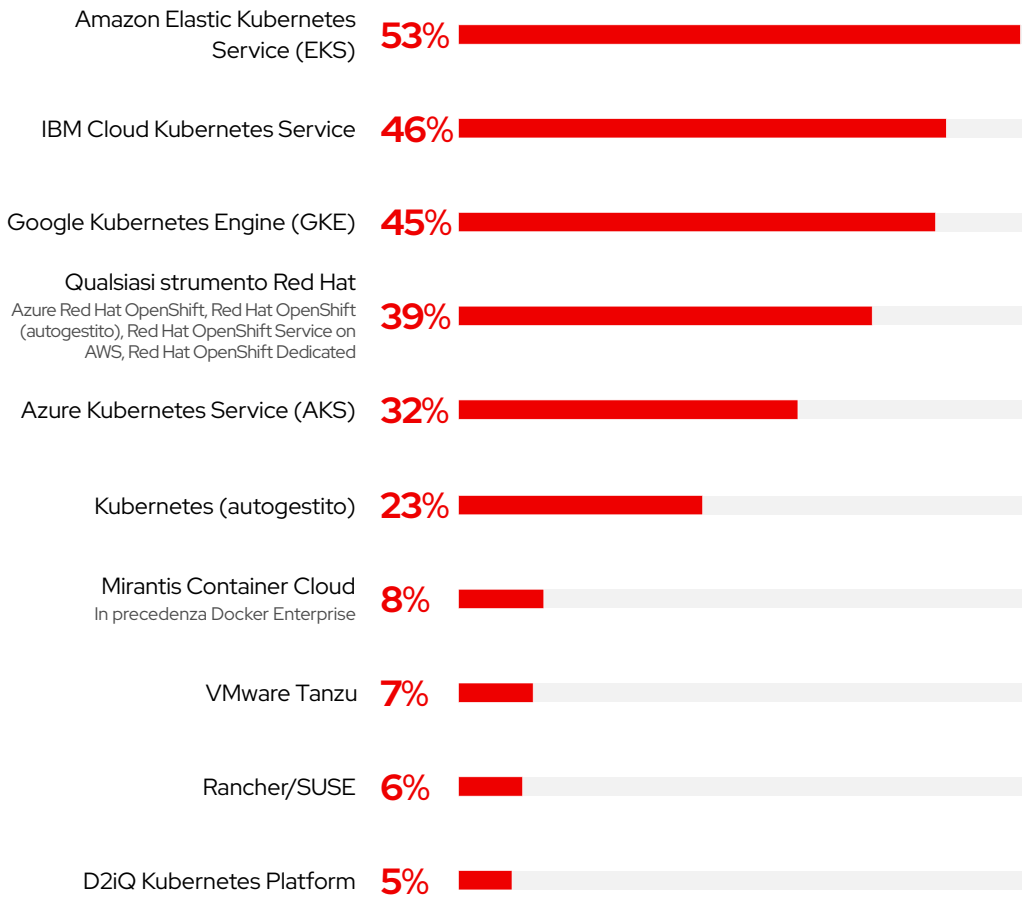
Informazioni sugli intervistati

Questa sezione fornisce ulteriori informazioni sugli intervistati e sulle loro organizzazioni.

Adozione di Kubernetes

La maggior parte degli intervistati utilizza Kubernetes nella produzione e le piattaforme più diffuse sono soluzioni Kubernetes basate su cloud.

Quale piattaforma Kubernetes utilizza per l'orchestrazione dei container?

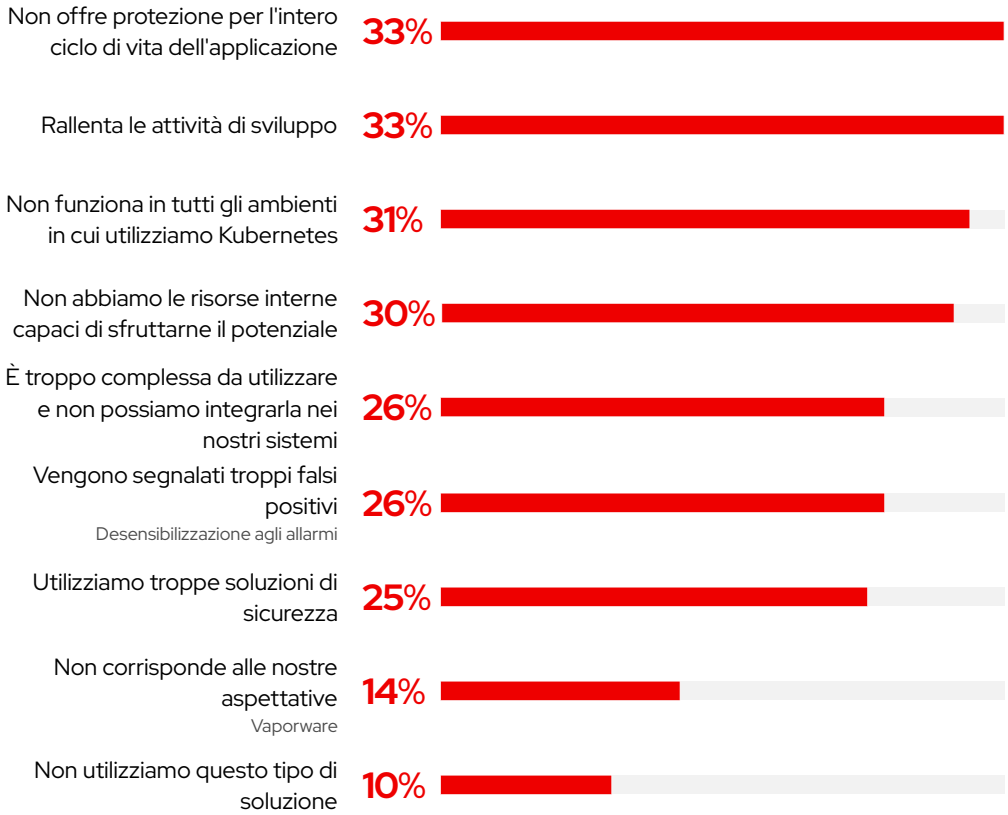


D3. Quale piattaforma Kubernetes utilizza per l'orchestrazione dei container? Base di intervistati: coloro che usano Kubernetes = 390

Problematiche comuni

La mancanza di protezione per l'intero ciclo di vita e i deployment lenti sono i due aspetti principali che vengono criticati alle soluzioni di sicurezza per Kubernetes.

Quali sono le problematiche principali che ha riscontrato con la soluzione di sicurezza utilizzata per Kubernetes?

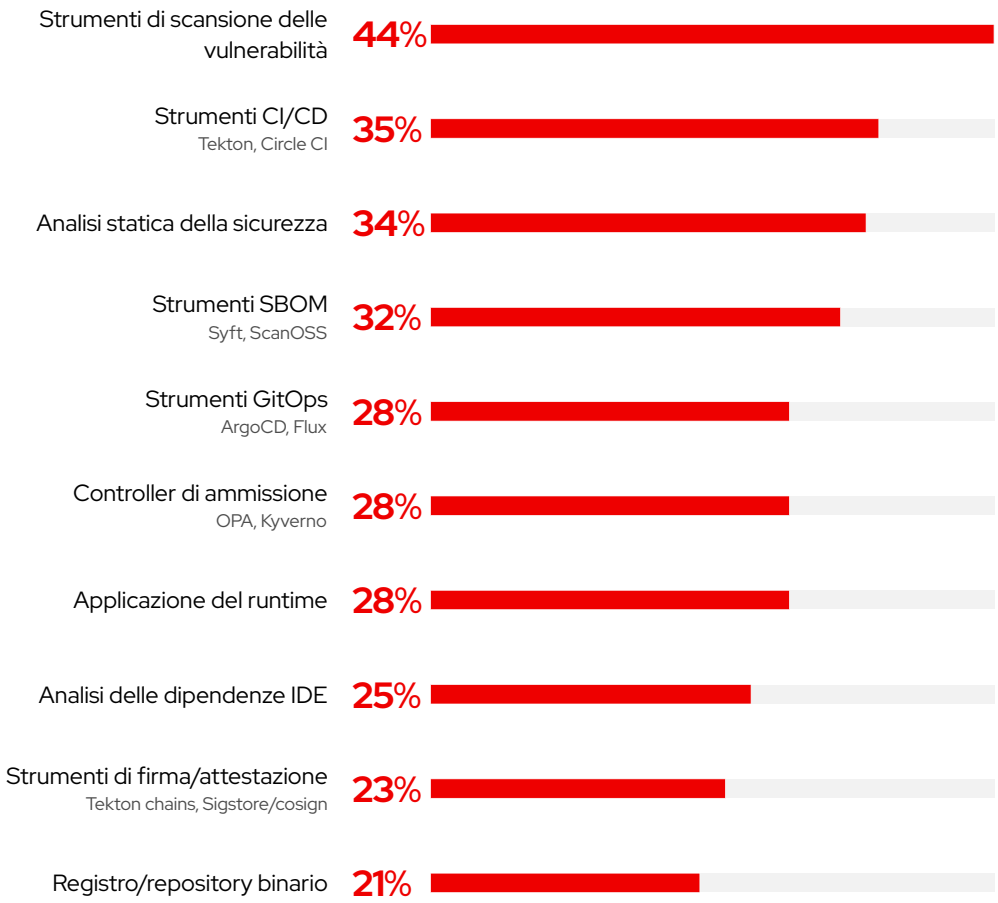


D26. Quali sono le problematiche principali che ha riscontrato con la soluzione di sicurezza utilizzata per Kubernetes? Selezionare fino a 3 problematiche. Base di intervistati: totale = 600

Strumenti di sicurezza della catena di distribuzione

Gli strumenti di scansione delle vulnerabilità sono i più utilizzati, seguiti da CI/CD, analisi statica della sicurezza e strumenti SBOM. Le organizzazioni utilizzano in media 3 strumenti di sicurezza per le loro catene di distribuzione del software.

Quali dei seguenti strumenti di sicurezza utilizza per la catena di distribuzione del software?

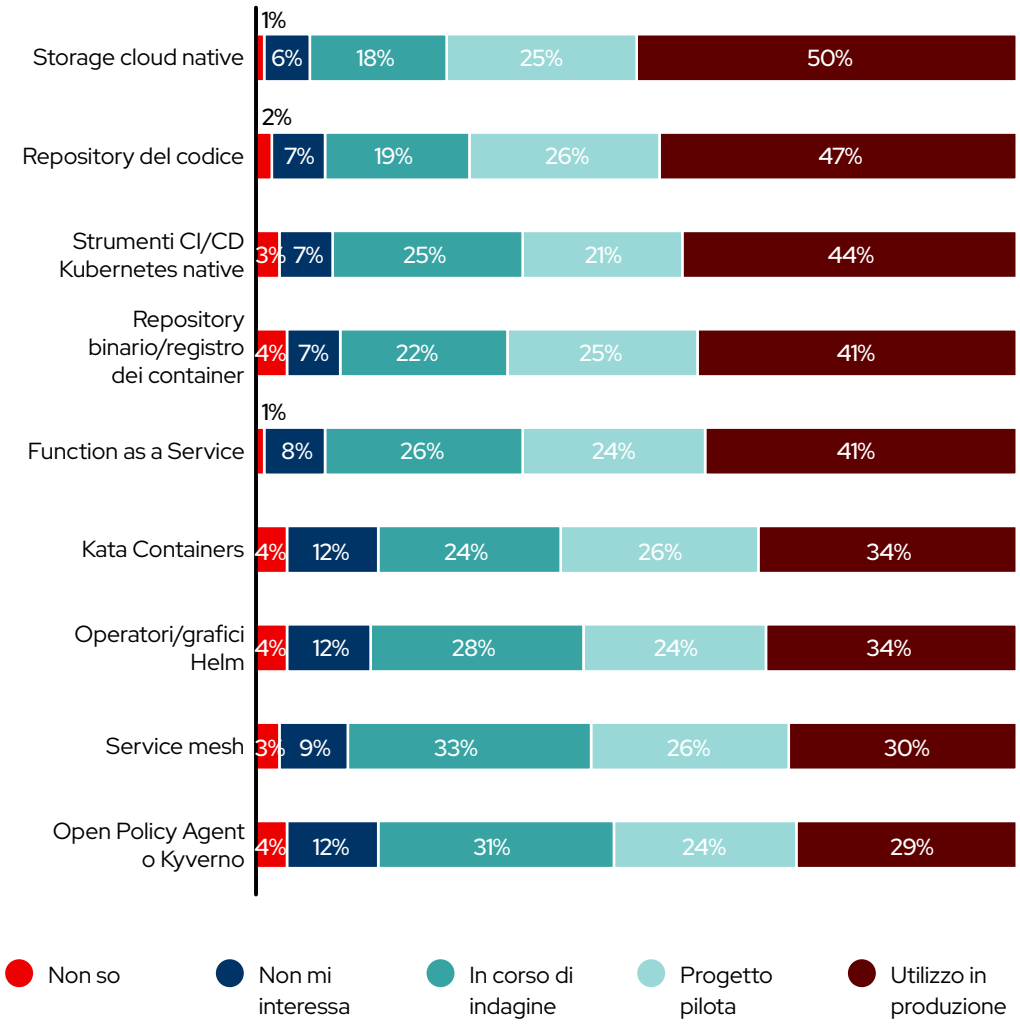


D22. Quali dei seguenti strumenti di sicurezza utilizza per la catena di distribuzione del software? Base di intervistati: totale = 600

Altre tecnologie cloud native

Fra le tecnologie cloud native più utilizzate ci sono gli strumenti CI/CD Kubernetes native.

Quali tecnologie cloud native utilizza o prevede di adottare?



D6. Quali tecnologie cloud native utilizza o prevede di adottare? Base di intervistati: totale = 600

A causa dell'arrotondamento, il totale delle percentuali potrebbe non corrispondere al 100%.

Prova subito Red Hat Advanced Cluster Security for Kubernetes

Red Hat® Advanced Cluster Security for Kubernetes è una piattaforma di sicurezza Kubernetes native che permette di creare, distribuire ed eseguire applicazioni cloud native in modo più sicuro. Con Red Hat Advanced Cluster Security si possono proteggere i carichi di lavoro Kubernetes containerizzati nei principali ambienti di cloud pubblico e piattaforme di cloud ibrido, tra cui Red Hat OpenShift, Amazon Elastic Kubernetes Service (EKS), Microsoft Azure Kubernetes Service (AKS) e Google Kubernetes Engine (GKE).

Ridurre al minimo i rischi operativi

Monitorare, raccogliere e valutare gli eventi a livello di sistema, come l'esecuzione dei processi, le connessioni e i flussi di rete e l'escalation dei privilegi, per rilevare attività dannose: da malware attivi e accessi non autorizzati a intrusioni e movimenti laterali.

Aumentare la produttività DevSecOps

Integra Red Hat Advanced Cluster Security con le pipeline CI/CD e i registri delle immagini per correggere rapidamente le immagini vulnerabili e con errori di configurazione, direttamente negli ambienti di sviluppo, con feedback e avvisi in tempo reale.

Proteggere l'infrastruttura Kubernetes

Assicurati che l'infrastruttura Kubernetes rimanga solida e protetta grazie a confronti continui con i benchmark CIS e ad altre procedure consigliate per la sicurezza.

Pianifica una demo personalizzata di Red Hat Advanced Cluster Security for Kubernetes su misura per la tua azienda e le tue esigenze.

Red Hat