Come adottare una soluzione DevSecOps esaustiva

Il framework Red Hat DevSecOps costituisce una base solida per realizzare una soluzione DevSecOps completa e altamente scalabile.

La sicurezza delle attività DevOps è un obiettivo complesso

Proteggere le attività DevOps è un compito difficile, soprattutto perché gli strumenti DevOps sono in rapida e costante evoluzione. I container e Kubernetes aggiungono ulteriori complessità, aprendo le porte a nuovi vettori di attacco e rischi per la sicurezza. I team operativi e di sviluppo devono integrare la sicurezza, inclusa quella di Kubernetes, nel ciclo di vita delle applicazioni, al fine di salvaguardare l'infrastruttura IT critica, proteggere i dati riservati e tenere il passo con il cambiamento.

Red Hat e i partner specializzati in soluzioni per la sicurezza hanno creato un framework che costituisce una base solida e un modello per la distribuzione di soluzioni DevSecOps caratterizzate da deployment e scalabilità efficaci. Il framework Red Hat® DevSecOps risponde ai principali requisiti di sicurezza dell'intero ciclo di vita delle attività DevOps, all'interno di una strategia di sicurezza completa incentrata sulla difesa. Insieme ai partner specializzati nel garantire la sicurezza, Red Hat aiuta a ridurre i rischi semplificando la protezione delle soluzioni DevOps e accelerando l'adozione di soluzioni DevSecOps.

I partner che operano in questo ambito, quali Anchore, Aqua, CyberArk, Lacework, NeuVector, Palo Alto Networks, Portshift, Snyk, StackRox, Synopsys, Sysdig, Thales, Tigera, Trend Micro e Tufin migliorano le funzionalità di sicurezza native di Red Hat, fornendo soluzioni DevSecOps end-to-end capaci di migliorare il tuo profilo di sicurezza, consentendoti di sfruttare al meglio i tuoi investimenti nelle soluzioni Red Hat.

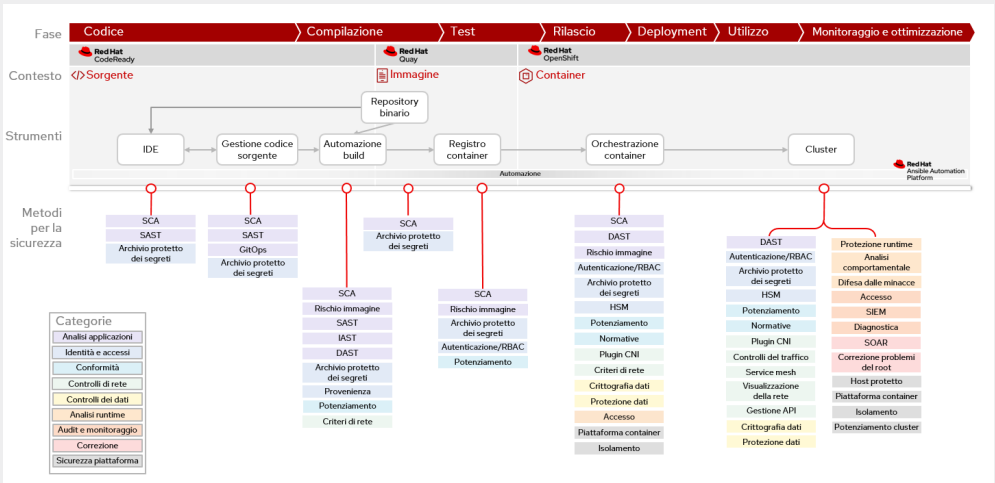

Figura 1. Il framework DevSecOps

facebook.com/RedHatItaly
twitter.com/RedHatItaly
linkedin.com/company/red-hat

Un framework completo che prevede numerosi metodi a garanzia della sicurezza

Il framework Red Hat DevSecOps identifica nove categorie di sicurezza e 32 metodi e tecnologie dedicati all'intero ciclo di vita delle applicazioni, consentendo un'integrazione strategica delle funzionalità di Red Hat, delle toolchain DevOps e delle soluzioni per la sicurezza offerte dai partner. A seconda dell'attività DevOps e dei requisiti specifici, puoi implementare alcuni o tutti i metodi e le tecnologie consigliati per ciascuna categoria.

Sicurezza della piattaforma

La sicurezza della piattaforma Kubernetes è fondamentale. Predisporre tale ambiente per renderlo capace di supportare le applicazioni business critical con modalità scalabili e sicure è tutt'altro che semplice. Di fatto, il deployment e la gestione di Kubernetes restano due sfide prioritarie per le aziende.[1] Red Hat OpenShift® è una piattaforma Kubernetes basata sui container e pensata per ambienti enterprise, che elimina le complessità, riduce gli ostacoli all'adozione e integra numerose funzionalità di sicurezza della piattaforma.

Il framework Red Hat DevSecOps offre funzionalità di base per proteggere il container host (Red Hat Enterprise Linux® e Red Hat CoreOS) e la piattaforma di container. La maggior parte delle funzionalità di sicurezza di Red Hat sono attivate per impostazione predefinita, per semplificare il deployment e ridurre al minimo il rischio. Consentono inoltre di proteggere i container ai confini e l'host da un'eventuale perdita di dati.

Metodi per garantire la sicurezza della piattaforma

- Sicurezza dell'host: fornisce controlli d'accesso vincolato con SELinux, strutture kernel per il controllo delle chiamate al sistema con modalità di elaborazione sicura (seccomp) e funzionalità kernel per isolare CPU, memoria e altre risorse con CGroups.
- Sicurezza della piattaforma container: fornisce un ambiente runtime per container leggero con CRI-O e un registro sicuro per le immagini dei container con Quay.
- Spazio dei nomi Linux: per l'isolamento delle applicazioni a livello di team, gruppi e reparti.
- Consolidamento di Kubernetes e container: per l'applicazione di standard come NIST 800-190 e CIS Benchmarks.

Analisi delle applicazioni

Le funzioni di analisi delle applicazioni aiutano a identificare le vulnerabilità e altri problemi di sicurezza nelle fasi iniziali del ciclo di vita dell'applicazione. Svolgendo le attività di prevenzione nelle fasi iniziali del ciclo di vita DevOps è possibile identificare e risolvere le vulnerabilità tempestivamente, ed evitare di ripetere il lavoro in un secondo momento.

Metodi per l'analisi delle applicazioni

- Test SAST (Static Application Security Testing): analizza il codice nella fase di sviluppo, allo scopo di individuare vulnerabilità e problemi di qualità.
- Analisi SCA (Software Composition Analysis: esamina i pacchetti con dipendenze inclusi nelle applicazioni, alla ricerca di vulnerabilità note e di problemi legati alle licenze.
- Strumenti IAST (Interactive Application Security Testing) e DAST (Dynamic Application Security Testing): analizza le applicazioni in esecuzione per individuare vulnerabilità nei processi operativi.

---

1 *Vizard, Mike. "Survey Sees Kubernetes Enterprise Adoption Gains." Container Journal, marzo 2020.*

L'analisi delle applicazioni include approcci alla sicurezza come la gestione della configurazione GitOps e funzionalità di gestione dei rischi per le immagini dei container, come l'identificazione di malware, segreti inclusi nel codice e difetti di configurazione.

Gestione di identità e accessi

I metodi di gestione di identità e accessi (IAM) controllano l'accesso ai dati, alle applicazioni e alle risorse in ambienti cloud e on premise, basandosi sull'identità dell'utente o dell'applicazione e su criteri definiti a livello amministrativo. Sono presenti in ogni fase del ciclo di vita DevOps e proteggono contro gli accessi al sistema e i movimenti laterali non autorizzati.

Metodi IAM

- Controlli di autenticazione e autorizzazione: verificano l'identità di utenti e applicazioni e concedono l'accesso a risorse e funzioni specifiche.
- Controlli RBAC (Role-based Access Controls): garantiscono a gruppi di utenti l'accesso a risorse o funzioni in base al rispettivo ruolo o responsabilità di mansione, semplificando l'amministrazione e l'onboarding, e limitando l'estensione dei privilegi.
- Provider di identità, archivi protetti di segreti e moduli HSM (Hardware Security Modules): gestiscono e proteggono le credenziali, le chiavi, i certificati e i segreti, garantendo la sicurezza dei dati a riposo e durante il trasferimento.

Altri metodi IAM includono funzioni per l'identificazione della provenienza delle immagini dei container e per la firma delle immagini, al fine di convalidarne l'autenticità e stabilirne l'attendibilità.

Conformità

I metodi e le tecnologie finalizzate a garantire la conformità aiutano a rispettare le normative governative e di settore, e le policy aziendali. Automatizzando la convalida della conformità e la generazione di report lungo l'intero processo DevOps, si semplificano gli audit e si evitano sanzioni e processi costosi.

L'applicazione di questi metodi migliora la conformità ai principali obblighi sulla privacy dei dati e la sicurezza delle informazioni, tra cui:

- Standard PCI-DSS (Payment Card Industry Data Security Standard).
- Standard ISO 27001 per la gestione della sicurezza delle informazioni.
- Legislazione HIPAA (Health Insurance Portability and Accountability Act), vigente negli Stati Uniti.
- Regolamento generale sulla protezione dei dati dell'Unione Europea (GDPR).

Controlli e segmentazione della rete

I metodi per il controllo e la segmentazione della rete consentono di controllare, isolare e visualizzare il traffico Kubernetes. Aiutano a isolare i tenant e a proteggere i flussi di comunicazione tra le applicazioni containerizzate e i microservizi.

Metodi per il controllo e la segmentazione della rete

- Policy di sicurezza della rete Kubernetes: controllano i flussi di traffico al livello dell'indirizzo IP o della porta e possono essere migliorati con controlli del traffico in ingresso e in uscita dal cluster, accesso e visualizzazione della rete.
- Software defined networking (SDN): offre un'infrastruttura di rete programmabile e adattabile con provisioning in tempo reale a supporto dei requisiti di sicurezza dinamici e delle esigenze di business in continua evoluzione.
- Service mesh: fornisce segmentazione e visualizzazione della rete, autenticazione e autorizzazioni per applicazioni containerizzate e microservizi.

Controlli dei dati

I metodi e le tecnologie per il controllo dei dati aiutano a proteggerne l'integrità e a prevenirne la divulgazione non autorizzata. Proteggono i dati a riposo e durante il trasferimento, aiutando a difendere la proprietà intellettuale e le informazioni riservate dei clienti.

Metodi per il controllo dei dati

- Crittografia dei dati: fornisce funzionalità di crittografia dei dati, creazione di token, data masking e gestione delle chiavi che contribuiscono a prevenire la diffusione non autorizzata dei dati contenuti in database, file e container.
- Protezione dei dati: individua e classifica i dati, con attività di audit e monitoraggio per proteggere i dati sensibili e migliorare la conformità.

Analisi e protezione del runtime

I metodi di protezione del runtime aiutano a conservare l'integrità del cluster identificando e mitigando le attività sospette e dannose in tempo reale.

Metodi di analisi e protezione del runtime

- Controller di ammissione: svolge la funzione di controllo in Kubernetes, verificando ed eseguendo nel cluster solo le attività consentite.
- Analisi comportamentale del runtime delle applicazioni: esamina l'attività del sistema e rileva azioni sospette o dannose in modo intelligente e in tempo reale.
- Metodo RASP (Runtime Application Self Protection): individua e arresta gli attacchi informatici in tempo reale.
- Gestione delle API: controlla l'accesso alle API e ne protegge il traffico.

Audit e monitoraggio

I metodi di audit e monitoraggio forniscono informazioni sugli incidenti di sicurezza che si verificano nell'ambiente di produzione. Indicano quando si è verificato l'evento, la probabile causa e forniscono informazioni sul potenziale impatto, aiutando a migliorare la visibilità e ad accelerare la risposta all'incidente.

I metodi di audit e monitoraggio includono:

- SIEM (Security Information and Event Management): centralizza i report degli eventi consolidando registri e flussi di dati della rete generati da dispositivi, endpoint e applicazioni distribuite.
- Diagnostica: fornisce informazioni sulle violazioni della sicurezza e prove a supporto degli audit di conformità, accelerando le attività di ripristino.

Correzione

I metodi di correzione avviano automaticamente azioni correttive quando si verificano incidenti di sicurezza negli ambienti di produzione. Contribuiscono a incrementare i tempi di attività e a evitare perdite di dati.

Metodi di correzione

- Piattaforme SOAR (Security Orchestration, Automation, and Response): reagiscono agli incidenti di sicurezza con azioni automatiche e integrandosi con altri strumenti di sicurezza.
- Correzione di problemi del root: risolve automaticamente i problemi legati agli errori di configurazione Kubernetes e alle violazioni delle policy.

Conclusioni

Il framework Red Hat® DevSecOps costituisce una base affidabile e scalabile per aumentare la sicurezza delle attività DevOps e ridurre i rischi. Red Hat e i partner specializzati in soluzioni per la sicurezza mettono a tua disposizione le tecnologie indispensabili per semplificare e accelerare l'adozione di procedure DevSecOps. Contattaci per saperne di più

INFORMAZIONI SU RED HAT

Red Hat è leader mondiale nella fornitura di soluzioni software open source. Con un approccio basato sul concetto di community, distribuisce tecnologie come Kubernetes, container, Linux e hybrid cloud caratterizzate da affidabilità e prestazioni elevate. Red Hat favorisce l'integrazione di applicazioni nuove ed esistenti, lo sviluppo di applicazioni cloud-native, la standardizzazione su uno tra i principali sistemi operativi enterprise, e consente di automatizzare e gestire ambienti complessi in modo sicuro. I pluripremiati servizi di consulenza, formazione e assistenza hanno reso Red Hat un partner affidabile per le aziende della classifica Fortune 500. Lavorando al fianco di provider di servizi cloud e applicazioni, system integrator, clienti e community open source, Red Hat prepara le organizzazioni ad affrontare un futuro digitale.

facebook.com/RedHatItaly
twitter.com/RedHatItaly
linkedin.com/company/red-hat

ITALIA
it.redhat.com
italy@redhat.com

EUROPA, MEDIO ORIENTE, E AFRICA (EMEA)
00800 7334 2835
it.redhat.com
europe@redhat.com

it.redhat.com
#F26043_1220