KUDO-33 - KUBERNETES SECURITY

Categoria: **Kubernetes & Docker**

INFORMAZIONI SUL CORSO

Durata:	Categoria:	Qualifica Istruttore:	Dedicato a:	Produttore:
2 Giorni	Kubernetes & Docker	Docente Senior (min. 5 anni)	Professionista IT	PCSNET

OBIETTIVI

Al termine del corso i partecipanti saranno in grado di:

- Comprendere i principali concetti di sicurezza e conformità in un ambiente Kubernetes.
- Configurare l'auditing nel cluster Kubernetes per monitorare le attività e gli eventi di sicurezza.
- Gestire l'autenticazione e l'autorizzazione nel cluster utilizzando diverse strategie e tecnologie.
- Utilizzare Open Policy Agent (OPA) per definire e applicare politiche di sicurezza personalizzate nel cluster.
- Applicare le Security Context di Kubernetes per definire restrizioni di sicurezza sui pod e i container.
- Abilitare l'encryption at rest sul cluster Kubernetes.
- Implementare tecniche di hardening del sistema utilizzando strumenti come AppArmor per ridurre le superfici di attacco.
- Utilizzare RuntimeClass con gVisor per fornire un'isolamento avanzato della runtime dei container.
- Utilizzare Kube Bench per valutare la sicurezza del cluster rispetto alle linee guida CIS (Center for Internet Security).
- Valutare la conformità del cluster rispetto alle linee guida CIS utilizzando lo strumento CIS Assessment Tool.
- Analizzare le immagini dei container per identificare e mitigare le vulnerabilità di sicurezza.
- Firmare digitalmente le immagini dei container utilizzando Notary per garantire l'autenticità e l'integrità delle stesse.
- Monitorare le attività sospette nel cluster utilizzando Falco, uno strumento di rilevamento delle minacce basato su regole.

PREREQUISITI

- Conoscenza discreta di Kubernetes: è fondamentale avere una buona comprensione dei concetti fondamentali di Kubernetes, come la creazione e la gestione di pod, servizi e risorse di rete.
- Familiarità con la sicurezza informatica: è consigliabile avere una conoscenza di base dei principi di sicurezza informatica, come autenticazione, autorizzazione, crittografia.
- Esperienza con l'amministrazione di sistemi e reti: è utile avere competenze di base in amministrazione di sistemi, compresi concetti come file system, permessi di accesso, gestione dei processi e configurazione di reti.
- Conoscenza buona dei container: è fondamentale avere familiarità con i concetti di base di container, come la creazione e l'esecuzione di container, la gestione delle immagini e la configurazione delle reti dei container.
- Familiarità con le best practice di sicurezza di Kubernetes: è utile avere una conoscenza delle best practice di sicurezza specifiche di Kubernetes, come la configurazione dei ruoli e delle autorizzazioni, la gestione delle

immagini dei container e le politiche di rete.

-Aver frequentato i corsi ContainerD Introduction, Kubernetes Introduction, Kubernetes Resource Management, Kubernetes Install, Configure & Manage o aver acquisito conoscenze equivalenti.

CONTENUTI

-Auditing
-Authentication
-OIDC Authentication with LDAP
-OPA – Part 1
-OPA – Part 2
-Pod Service Account
-Security Context
-Encryption at Rest
-System Hardening with AppArmor
-Kube Bench
-Image Analysis
-Sign image with Notary
-CIS Assesment Tool
-RuntimeClass with gVisor
-Falco

INFO

Esame: CKS - Certified Kubernetes Security Specialist
Materiale didattico: Materiale didattico in formato digitale
Costo materiale didattico: incluso nel prezzo del corso a Calendario
Natura del corso: Operativo (previsti lab su PC)