MEET IT

PROTEZIONE DEGLI AMBIENTI
CONTAINER DEV-OPS

CONTAINER SECURITY

Datasheet

Le aziende del Gruppo MEET IT

3CiME TECHNOLOGY ICT & INNOVATION

Via di Corticella, 89/2
40128 Bologna BO

+39 05 14070383
www.3cime.com | info@3cime.com

ntnuovetecnologie 25

Viale Alcide De Gasperi, 37
33100 Udine UD

+39 0432 524001
info@ntonline.it | www.ntonline.it

AUMENTA I LIVELLI DI SICUREZZA INFORMATICA

Il servizio del Gruppo MEET IT fa un altro passo avanti nel mondo della cybersecurity, offrendo un servizio per mettere in sicurezza gli ambienti Container Dev-Ops.

PREMESSA

Sebbene i Container offrano alcuni vantaggi intrinseci in termini di sicurezza, tra cui un maggiore isolamento delle applicazioni, ampliano anche il panorama delle minacce di un'organizzazione. L'incapacità di riconoscere e pianificare misure di sicurezza specifiche, relative ai Container, può aumentare i rischi per la sicurezza delle organizzazioni.

Con "Sicurezza dei Container" si intende la **protezione dell'integrità dei Container**, dalle applicazioni che contengono all'infrastruttura su cui si basano. Quella dei Container deve essere una **sicurezza integrata e continua**. In generale, questo significa che l'azienda deve proteggere:

- **Il flusso dei container e l'applicazione**
- **L'ambiente di deployment e l'infrastruttura dei Container**

Gli ambienti Container Dev-Ops stanno crescendo a vista d'occhio. Secondo questo schema di sviluppo applicativo, ogni progetto viene suddiviso in micro-servizi che sono amministrati da un orchestratore. Nei Container finiscono quindi **applicazioni e dati**. Quello che accade è che, spesso, gli sviluppatori dimenticano la security-by-design e ormai anche questi ambienti sono diventati soggetto di attacco.

Se poi consideriamo che queste applicazioni sono quelle più esposte in Internet, ecco che solo un **servizio erogato 24 ore su 24, 7 giorni su 7**, può salvare il lavoro delle organizzazioni dalle potenziali minacce.

SERVIZIO

La sicurezza dei Container è la procedura dell'utilizzo di strumenti e policy di sicurezza per proteggere tutti gli aspetti delle applicazioni containerizzate da potenziali rischi.

Il servizio gestisce i rischi dell'intero ambiente, inclusi tutti gli aspetti della supply chain del software o della pipeline CI/CD, dell'infrastruttura, del runtime dei container e delle applicazioni di gestione del ciclo di vita in esecuzione sui Container. Quando si implementano soluzioni per la sicurezza della rete dei Container, bisogna assicurarsi che queste siano integrate con l'orchestrazione sottostante per avere consapevolezza del contesto dell'applicazione.

VISITA IL SITO *MEETIT.CLOUD*

FOCUS ON: COME SI PROTEGGE UN CONTAINER DEV-OPS

Il NIST (National Institute of Standards and Technology) ha pubblicato una Guida alla Sicurezza dei Container delle applicazioni che riassume diversi approcci fondamentali per raggiungere questo obiettivo. Ecco tre considerazioni chiave tratte dal report:

- **Utilizzo di sistemi operativi host specifici per i Container.** Il NIST consiglia di utilizzare sistemi operativi host specifici per i Container, che sono creati con un numero inferiore di funzionalità per ridurre le superfici di attacco.

- **Segmentazione dei Container in base allo scopo e al profilo di rischio**. Sebbene le piattaforme di Container generalmente riescano a isolare i Container (tra di loro e dal sistema operativo sottostante), il NIST osserva che è possibile ottenere una maggiore "profondità di difesa" raggruppando i Container in base "allo scopo, alla sensibilità e allo stato delle minacce" ed eseguirli su sistemi operativi host separati. Questo approccio segue un principio di sicurezza IT generale per limitare il raggio d'azione di un incidente o di un attacco, in modo da confinare le conseguenze di una violazione a un'area quanto più ristretta possibile.

- **Utilizzo di strumenti di gestione delle vulnerabilità e di sicurezza in fase di runtime specifici per i Container.** Gli strumenti tradizionali di scansione e gestione delle vulnerabilità spesso hanno punti ciechi quando si tratta di Container e questo può portare alla creazione di report imprecisi che non rilevano eventuali problemi con le immagini dei Container, le impostazioni di configurazione ed elementi simili. Allo stesso modo, garantire la sicurezza in fase di runtime è un aspetto fondamentale dei deployment e delle operation dei Container. Gli strumenti tradizionali orientati al perimetro, come i sistemi di prevenzione delle intrusioni, spesso non vengono creati pensando ai Container e quindi non sono in grado di proteggerli adeguatamente.

Il NIST consiglia inoltre di utilizzare una **radice di attendibilità** basata su hardware, come *Trusted Platform Module (TPM)*, per avere un altro layer di affidabilità della sicurezza, oltre che per creare cultura e processi (come DevOps o DevSecOps) adatti per Container e sviluppo nativo per il cloud.

CARATTERISTICHE

Gestione continua del profilo cloud

Valuta continuamente il profilo di sicurezza cloud segnalando gli **errori di configurazione e attività sospette**, con possibilità di **blocco automatico** in caso di attacco.

Image Scanning

Automatizza la scansione (anche per AWS Fardate) nei tuoi strumenti di CI/CD senza che le immagini abbandonino il tuo ambiente, e blocca le vulnerabilità prima del deployment.

Compliance continua

Valida la compliance di Container, Kubernetes e cloud rispetto a standard quali PCI, NIST e SOC2.

Zero Trust Network Security – Sicurezza della rete

Visualizza tutte le comunicazioni di rete tra app e servizi. Applica la micro-segmentazione, automatizzando le policy di rete native di Kubernetes.

Runtime Security

Unifica l'individuazione delle minacce nei Container e nei carichi di lavoro di AWS Fargate, Kubernets e cloud con regole Falco preconfigurate che utilizzano le chiamate a sistema, audit log di k8s e log cloud.

Risposta a incidenti e dati forensi

Risponde agli incidenti e conduce indagini in maniera unificata su Container, CaaS (per es. AWS Fargate) e cloud con informazioni dettagliate.

OUTPUT

Il servizio prevede un **monitoraggio SAS** degli ambienti, con definizione congiunta delle policy di sicurezza da applicare.

Il collegamento con il **SOC** del nostro Gruppo permette di integrare **allarmistica, difesa e reportistica** a quanto sopra descritto.

VISITA IL SITO *MEETIT.CLOUD*