Condivisione delle attività necessarie per garantire la sicurezza dei carichi di lavoro

Come semplificare e rendere operative le attività dei team di sicurezza e degli amministratori IT

vmware®

Sommario

Introduzione

I team di sicurezza necessitano dell'aiuto dei team delle operation IT per proteggere i carichi di lavoro

Sia amministratori IT che team di sicurezza svolgono il proprio ruolo nel garantire la sicurezza dei sistemi, ma in modo relativamente isolato gli uni dagli altri. Tuttavia, la transizione agli ambienti cloud di applicazioni e carichi di lavoro impone un cambiamento nello svolgimento di tali ruoli.

I team di sicurezza di un'azienda sono generalmente costituiti da gruppi responsabili di policy e audit, nonché da team che si occupano di ricerca delle minacce e risposta agli incidenti. Il carico giornaliero di sicurezza e compliance ricade sul personale e sulle risorse delle operation IT, che non sono necessariamente orientati alla sicurezza. Infatti, secondo quanto risulta da un report di analisi di Forrester Consulting, solo il 33% delle aziende dispone attualmente di un team unificato per IT e sicurezza, mentre il 47% prevede che l'unificazione sarà la norma entro un periodo dai tre ai cinque anni.[1] È il momento ottimale per adottare un nuovo approccio che faciliti la coesione tra questi team.

Questo white paper illustra i costrutti chiave da adottare per consentire ai team di sicurezza e IT di ridurre in modo proattivo la superficie di attacco e di rafforzare le risorse. L'adozione di questi costrutti permetterà di ridurre la separazione tra questi team, di semplificare le operation e di condividere le attività necessarie per garantire la sicurezza dei carichi di lavoro.

COSTRUTTO CHIAVE	DESCRIZIONE
Ridurre al minimo il carico degli agenti	L'eliminazione dell'esigenza di installare agenti sui carichi di lavoro riduce la proliferazione degli agenti di sicurezza, minimizza le installazioni e i riavvi e riduce le spese operative generali. Ciò semplifica la distribuzione della sicurezza come servizio da parte del personale IT.
Condividere la visibilità sulle vulnerabilità	Una visione unificata dei dati sulla sicurezza assicura la chiarezza della comunicazione e della comprensione non appena le vulnerabilità vengono rilevate.
Automatizzare la definizione delle priorità dei rischi	Per ridurre il lavoro di avviso ed evitare di sovraccaricare le risorse, entrambi i team devono sapere su cosa concentrarsi per avare il massimo impatto sulle difese. È essenziale disporre di un sistema incentrato sul contesto che consenta di definire in modo automatico e imparziale le priorità delle vulnerabilità.
Semplificare i processi dei carichi di lavoro	Condividendo la visibilità e la definizione delle priorità dei rischi, i team di sicurezza e IT possono godere di un'esperienza senza intoppi tramite l'automazione e il miglioramento dell'operatività della sicurezza nell'ambito dell'IT hygiene.

TABELLA 1: i quattro costrutti chiave per ridurre la superficie di attacco e rafforzare le risorse.

1. Forrester Consulting, commissionato da VMware. "Security As A Team Sport: A Spotlight On The Growing Role Of IT In Security Tasks". Maggio 2020.

La sfida

I carichi di lavoro sono diventati una vulnerabilità che presenta problemi di individuazione delle responsabilità

Con la crescita e l'aumento della complessità dei nostri ambienti, i carichi di lavoro stanno diventando sempre più distribuiti. Molte applicazioni basate sul cloud sono business critical ma vulnerabili ai danneggiamenti in caso di malfunzionamento di qualsiasi parte del carico di lavoro (app, dati o sistema operativo). Ovviamente la soluzione non è spegnere un server aziendale quando si verifica un incidente. Sicurezza e operation IT sono secondarie alla produttività aziendale. Ciò significa che la protezione e il monitoraggio di ciascuna parte del carico di lavoro rappresentano ora un elemento aggiuntivo, ed essenziale, della protezione dell'azienda.

Chi è responsabile della protezione dei carichi di lavoro?
Quando i carichi di lavoro risiedevano nei server rack dei data center on-premise, era semplice assegnare le responsabilità della loro sicurezza. Attualmente, i carichi di lavoro possono risiedere in server fisici, in server virtuali, nel public cloud o essere serverless. Inoltre possono spostarsi tra questi ambienti ed è pertanto difficile monitorarli e gestirli. Responsabili della sicurezza, amministratori IT, amministratori cloud, amministratori VMware vCenter®, SRE (Site Reliability Engineer), DevOps e sviluppatori possono tutti svolgere un ruolo nel ciclo di vita dei carichi di lavoro. Talvolta possono influenzare i carichi di lavoro in modo da raggiungere un obiettivo comune, ma altre volte i loro obiettivi possono essere contrastanti.

Gli amministratori IT possono proteggere i carichi di lavoro in modo efficiente. Tuttavia, non hanno visibilità sulla maggior parte delle loro vulnerabilità e di sicuro non dispongono del contesto per definirne le priorità. Poiché gli amministratori IT spesso non hanno il controllo dell'ambiente cloud, i ruoli e le responsabilità risultano confusi. I team di sicurezza possono avere alcune delle informazioni necessarie per identificare le vulnerabilità, ma non conoscere con chiarezza le loro priorità né il contesto per poter gestire in modo efficace le correzioni.

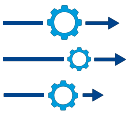
In altre parole, la sicurezza dei carichi di lavoro non viene gestita in modo adeguato da nessuno.

La responsabilità può essere condivisa?
Il punto è che sia i team di sicurezza che gli amministratori IT devono svolgere un ruolo nella sicurezza dei carichi di lavoro. Per evitare i problemi di individuazione delle responsabilità, questi team devono operare in modo unificato per quanto riguarda i processi, le informazioni e gli strumenti specifici dei carichi di lavoro.

Con una comprensione e una metodologia condivise per automatizzare l'individuazione delle vulnerabilità e la definizione delle priorità delle correzioni, diventa molto più semplice per gli amministratori IT condividere la responsabilità del rafforzamento e della riduzione delle superfici di attacco. Infatti, la sicurezza dei carichi di lavoro può essere resa operativa per eliminare la tensione e i problemi di definizione delle responsabilità tra questi due team essenziali. Per attuare tutto ciò sono necessari quattro passaggi.

DATI CHIAVE CHE DEVONO ESSERE CONDIVISI TRA TEAM DI SICUREZZA E AMMINISTRATORI IT

- Indicatori di compromissione (IOC)
- Tattiche, tecniche e procedure (TTP)
- Visibilità sugli attacchi bloccati e individuati
- Eventi ordinari che si verificano nel sistema
- Valutazione di oltre 2.000 stati di configurazione dei carichi di lavoro
- Inventario dei carichi di lavoro e relativo stato di protezione
- Contesto delle vulnerabilità senza scansione con valutazioni dei rischi e dei link al National Vulnerability Database
- Monitoraggio e tendenze dell'IT hygiene nel tempo



Quattro passaggi per semplificare e rendere operativa la sicurezza dei carichi di lavoro

Passaggio 1: ridurre al minimo il carico degli agenti

La proliferazione di agenti di sicurezza aggiunti causa molti problemi sia agli amministratori IT che ai team di sicurezza. Le sfide più comuni sono:

- Fonti separate di informazioni sulla sicurezza che portano a una scarsa comunicazione
- Maggiore carico di manutenzione e maggiori possibilità di errori
- Costi di storage aggiuntivi per i dati raccolti

Per eliminare questi problemi, occorre consolidare gli stack di sicurezza e IT, sostituendo le molteplici soluzioni mirate con un approccio olistico alla sicurezza che consenta di raccogliere i dati sia negli ambienti on-premise che negli ambienti cloud.

Scelta di un unico agente integrato
La soluzione ottimale è utilizzare nel layer di virtualizzazione un unico agente, integrato nell'infrastruttura esistente. Ciò consente la registrazione degli eventi necessari per una visibilità completa sui diversi ambienti. La presenza di un unico agente riduce al minimo possibile il footprint del monitoraggio della sicurezza.

Un unico agente offre grandi vantaggi
Il consolidamento delle soluzioni di sicurezza in un unico agente (una singola fonte di dati completa) offre grandi vantaggi in termini di miglioramento della sicurezza dei carichi di lavoro:

- Consente di rendere operativa più agevolmente la gestione degli agenti da parte del personale IT
- Permette l'integrazione dei workflow e la condivisione dei dati tra i team
- Offre informazioni incentrate sul contesto, con risultati utilizzabili più efficientemente nel processo decisionale
- Evita le scansioni delle vulnerabilità relative a un punto temporale specifico, con conseguente miglioramento delle prestazioni e accelerazione del tempo di risposta agli attacchi
- Riduce i costi di storage e le attività di manutenzione

Passaggio 2: condividere la visibilità sulle vulnerabilità

Il gruppo responsabile dell'installazione di patch raramente è lo stesso gruppo che monitora l'impatto sulla sicurezza delle vulnerabilità. I sistemi classici di scansione dei dati perdono rapidamente la sincronizzazione e i sistemi di richiesta di assistenza sono lenti: questo porta a differenze di interpretazione delle correzioni necessarie.

Gli amministratori IT utilizzano fonti di dati separate da quelle utilizzate dai team di sicurezza, ma sono comunque tenuti a partecipare ai processi di sicurezza su larga scala. Di conseguenza non vengano soddisfatte le aspettative e si ottengono risultati deludenti in termini di cyber hygiene.

Una visione unificata sui dati di sicurezza assicura la chiarezza nella comunicazione e nella comprensione delle vulnerabilità rilevate e del livello di rischio a loro associato.

Una visione unificata riduce in modo efficace i rischi
Il consolidamento in un unico agente del passaggio 1 agevola la condivisione dei dati sulla sicurezza tra i gli amministratori IT e i team di sicurezza. Idealmente, tali informazioni dovrebbero essere presentate all'interno degli strumenti che questi team utilizzano abitualmente, come gli strumenti di virtualizzazione (ad esempio, VMware vSphere® e vCenter).

La disponibilità degli stessi dati e degli stessi risultati di valutazione tra i team migliora la comunicazione e la collaborazione. L'aspetto più importante è la disponibilità costante dei dati sulle vulnerabilità aggiornati anziché una scansione relativa a un punto temporale specifico. Ciò assicura che i team siano sempre sincronizzati tra loro. Un inventario condiviso delle vulnerabilità dei carichi di lavoro, ordinate in base alla priorità del rischio che comportano, assicura che alle risorse venga richiesto di risolvere i problemi più critici.

Passaggio 3: automatizzare la definizione delle priorità dei rischi

L'utilizzo di un unico agente e la disponibilità di visibilità condivisa sui dati di sicurezza rappresentano grandi passi verso la gestione della sicurezza dei carichi di lavoro. Tuttavia, l'accesso alle vulnerabilità note non significa di per sé che vi sia una comprensione condivisa in merito a dove concentrare le risorse.

Il successivo passaggio logico è la presenza di un metodo standardizzato per valutare il rischio. Occorre considerare una soluzione di sicurezza che gestisca automaticamente la valutazione del rischio e la definizione delle priorità.

Dati con priorità definite in base ai rischi all'interno degli strumenti correnti per risultati utilizzabili nel processo decisionale

Una valutazione del rischio basata esclusivamente sul sistema CVSS (Common Vulnerability Scoring System) non è sufficiente. La disponibilità di dati contestuali selezionati da set di dati sulle minacce personalizzati, che includono feed dell'intelligence su exploit e minacce e oltre sette miliardi di vulnerabilità, consentirà alle aziende di impiegare modelli predittivi per prevedere le nuove vulnerabilità e definire le priorità delle attività di correzione in base al livello di criticità.

Idealmente, gli amministratori IT dovrebbero disporre di una visualizzazione degli exploit più comuni e delle vulnerabilità ad alto rischio all'interno della loro console vCenter. Ciò consentirà di incorporare agevolmente il rafforzamento dei carichi di lavoro nelle attività quotidiane di cyber hygiene.

Inoltre, gli amministratori IT hanno bisogno di informazioni di audit sullo stato corrente del sistema per poter collaborare con i team di sicurezza e adottare correzioni per le minacce. La disponibilità di una visualizzazione condivisa di tali informazioni consente a questi team di collaborare per applicare le patch in ordine di priorità o per adottare misure alternative, quali l'arresto dei sistemi vulnerabili.

Una visualizzazione condivisa delle minacce e delle vulnerabilità correnti, nonché dei rischi associati, consente di assegnare in modo chiaro le priorità e concentrare gli sforzi, con una conseguente risoluzione più rapida delle minacce esistenti e una migliore protezione dagli attacchi futuri.

Passaggio 4: semplificare i processi dei carichi di lavoro

Le scansioni delle vulnerabilità storicamente erano attività mensili o trimestrali. Tuttavia, tali scansioni relative a un punto temporale specifico non sono sufficienti. Data l'espansione continua dei carichi di lavoro negli ambienti multi-cloud, queste scansioni non forniscono informazioni sufficientemente ampie né sufficientemente tempestive rispetto a quanto necessario per ridurre i rischi di sicurezza critici.

Dopo la condivisione della visibilità e della definizione delle priorità dei rischi, il passaggio successivo per i team di sicurezza e IT è rendere la sicurezza dei carichi di lavoro una parte regolare dell'IT hygiene.

Rendere operativa la sicurezza dei carichi di lavoro

Per rendere operativa la sicurezza dei carichi di lavoro, gli amministratori IT devono ridurre costantemente le superfici di attacco come parte delle procedure standard di IT hygiene. Gli amministratori IT devono accedere alle valutazioni di migliaia di stati di configurazione nei loro carichi di lavoro, nonché alle informazioni e alle indicazioni per correggere le vulnerabilità individuate.

La gestione IT deve avere accesso a una visualizzazione condivisa dell'IT hygiene nel tempo. Ciò stimola le discussioni nei team in merito alla gestione delle vulnerabilità e la misurazione delle prestazioni. I responsabili IT devono utilizzare queste informazioni per assicurare che vengano seguite le priorità e che le risorse vengano allocate in modo appropriato per rafforzare costantemente i carichi di lavoro.

E ora?

L'allineamento dell'IT alla sicurezza dei carichi di lavoro riduce gli attacchi

I team di sicurezza e gli amministratori IT possono collaborare per migliorare la sicurezza dei carichi di lavoro. Se dispongono delle funzionalità di sicurezza adeguate, tale collaborazione non presenta problemi e può agevolmente essere resa operativa nelle attività di ogni giorno. Per sfruttare queste opportunità, occorre assicurarsi che questi team:

- Utilizzino una soluzione integrata con un unico agente
- Dispongano di una visualizzazione unificata sui dati di sicurezza, integrata nei lori strumenti di lavoro correnti
- Dispongano del contesto necessario e del monitoraggio continuo delle vulnerabilità con definizione automatica delle priorità dei rischi
- Abbiano il sostegno dei dirigenti per assicurarsi di rendere operativo il rafforzamento dei carichi di lavoro

Tre punti chiave per migliorare la sicurezza dei carichi di lavoro

1. Riunire gli amministratori IT e i responsabili della sicurezza affinché discutano dell'opportunità di collaborare per ridurre gli attacchi.
2. Identificare le attuali differenze in merito alla raccolta dei dati e alla visibilità per poter definire meglio le priorità delle vulnerabilità e rafforzare i carichi di lavoro.
3. Valutare soluzioni che offrano agli amministratori IT e ai team di sicurezza la visibilità e il contesto condivisi necessari per avere successo.

La gestione della sicurezza dei carichi di lavoro porta a maggiori profitti

- Copertura e visibilità su tutti i carichi di lavoro
- Semplificazione dello stack di sicurezza IT
- Possibilità di rispondere più rapidamente ai problemi grazie all'individuazione anticipata
- Migliore rafforzamento delle risorse
- Migliore prevenzione del malware e dei software e processi indesiderati
- Eliminazione completa delle minacce diverse dal malware
- Attivazione della sicurezza per il futuro: ambienti e carichi di lavoro moderni

Scopri di più

Leggi questa scheda tecnica per scoprire come VMware Carbon Black Cloud™ consente ai team IT e di sicurezza di migliorare congiuntamente la sicurezza dei carichi di lavoro.

VMware, inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel . 877-486-9273 Fax 650-427-5001 www.vmware.com
VMware, Inc . - Via Spadolini 5 - Edificio A - 20141 Milano - Tel .: (+39) 02 3041 2700 Fax: (+39) 02 3041 2701 www.vmware.com/it