ServiceNow Security Operations

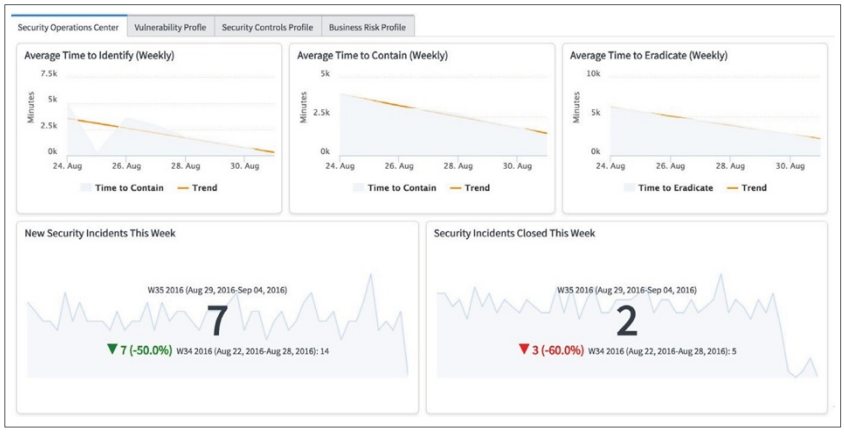
La sfida legata alla sicurezza
Al giorno d'oggi, i team responsabili della sicurezza sono inondati da avvisi e informazioni provenienti da un numero sempre crescente di soluzioni diverse e non comunicanti. Nel contempo, i servizi aziendali d'importanza critica, le infrastrutture IT e gli utenti sono oggetto di costanti attacchi che sfruttano le vulnerabilità note e sconosciute. Tali incidenti e vulnerabilità non sono contestualizzati nell'ambito dell'azienda e, pertanto, è difficile capire da dove provengano le principali minacce per la sicurezza dell'organizzazione. Inoltre, i processi manuali e i vari passaggi di consegne tra i diversi team impediscono al team responsabile della sicurezza di rispondere in maniera efficace agli attacchi o di valutare e correggere le eventuali vulnerabilità.

Una domanda ancora più importante in termini di sicurezza è la seguente: la nostra organizzazione è sicura e la situazione sta migliorando o peggiorando? Sebbene non sia facile dare una risposta a questo interrogativo, gran parte delle organizzazioni cerca di definire dei parametri baseline, tracciabili nel tempo, per valutare il livello generale di sicurezza delle proprie infrastrutture. Senza questo tipo di conoscenza, non è possibile rafforzare l'infrastruttura e migliorare l'efficacia degli interventi.

Da ciò ne conseguono tempi di rilevamento e risposta quantificabili in mesi e attacchi mancati che potrebbero comportare eventuali violazioni o compromissioni della sicurezza.

La soluzione ServiceNow
ServiceNow® Security Operations aiuta le organizzazioni a mettere in collegamento i team responsabili dell'IT e della sicurezza, fornire una risposta più rapida ed efficiente alle minacce e acquisire un quadro più completo del livello generale di sicurezza delle loro infrastrutture. Assicura il collegamento dei flussi di lavoro e delle funzionalità di gestione dei sistemi della Now Platform™ con i dati relativi alla sicurezza dei principali fornitori, in modo da offrire un'unica piattaforma di intervento che può essere condivisa dai team responsabili della sicurezza e dell'IT. Grazie all'orchestrazione, all'automazione e a una migliore visibilità, i team sono in grado di rispondere con maggiore efficienza, riducendo così i rischi per l'azienda.

La soluzione utilizza il ServiceNow® Configuration Management Database (CMDB) per mappare le minacce, gli incidenti di sicurezza e le vulnerabilità in base ai servizi aziendali e all'infrastruttura IT. Tale mappatura consente di definire le priorità e i punteggi di rischio sulla base dell'impatto aziendale, affinché i team responsabili della sicurezza possano concentrarsi sugli aspetti più critici per l'azienda. Inoltre, le mappe visive dei servizi aziendali mostrano le dipendenze dei sistemi interessati al fine di ridurre al minimo le richieste di cambiamento e i tempi di indisponibilità dei servizi. Poiché la soluzione Security Operations è parte integrante della Now Platform, il relativo CMDB è gestito da tutta l'organizzazione e non soltanto dal team responsabile della sicurezza.



Le dashboard personalizzabili forniscono, in tempo reale, un quadro generale del livello di sicurezza dell'azienda.

Connessione tra sicurezza e IT
Coordina la risposta dei team per agevolare il trasferimento dei compiti tra i gruppi e ridurre i tempi di risoluzione. Promuovi l'assunzione di responsabilità a tutti i livelli dell'organizzazione con la tranquillità di sapere che il lavoro viene svolto nel rispetto degli SLA.

Assicura una risposta più rapida ed efficiente in termini di sicurezza
Riduci la quantità di tempo spesa in attività basilari con gli strumenti di orchestrazione. Aggiungi automaticamente la funzione di threat intelligence per velocizzare i tempi di remediation in caso di incidenti di sicurezza e integra una piattaforma di intervento nel tuo portfolio di prodotti per la sicurezza già esistente.

Migliore conoscenza del livello generale di sicurezza della tua azienda
Visualizza lo stato attuale del tuo sistema di sicurezza mediante dashboard personalizzabili e report supportati da dati quantitativi. Migliora i processi e le prestazioni del team utilizzando parametri di misurazione e revisioni post incidente.

La Now Platform offre ulteriori funzionalità di livello enterprise immediatamente fruibili dai team, come i valori soglia degli SLA (service level agreement) integrati, l'instradamento basato sulle competenze, le notifiche, i flussi di lavoro avanzati e la collaborazione in tempo reale. L'applicazione Security Operations isola anche gli eventi di sicurezza dal resto del sistema, garantendo così la riservatezza dei dati di sicurezza sensibili.

Applicazione Security Incident Response
Security Incident Response semplifica l'identificazione degli incidenti critici e fornisce flussi di lavoro e strumenti di automazione che consentono di accelerare il processo di remediation. I dati acquisiti dagli strumenti di sicurezza esistenti o dal Security Information and Event Manager (SIEM) vengono importati tramite API o avvisi via e-mail per definire automaticamente la priorità da assegnare agli incidenti di sicurezza. I modelli dei flussi di lavoro per la sicurezza possono essere personalizzati per automatizzare le attività e garantire l'adozione delle best practice da parte dell'azienda.

La soluzione ti permette di visualizzare e tenere traccia facilmente degli interventi di risposta eseguiti in parallelo. Il sistema invierà un promemoria alle persone incaricate di svolgere determinate attività nel caso in cui non vengano completate entro i tempi stabiliti negli SLA o provvederà a trasferire la richiesta al livello successivo, laddove necessario. Ciò garantisce che eventuali decisioni o attività non vengano accidentalmente trascurate. Gli analisti della sicurezza possono comunicare con gli stakeholder direttamente dalla Now Platform tramite conference call o lo strumento di messaggistica Connect chat in modo da tenere costantemente aggiornate tutte le parti interessate.

Per accelerare i tempi di risposta e consentire al team responsabile della sicurezza di concentrarsi sull'individuazione delle minacce più complesse, la soluzione Security Incident Response, se utilizzata insieme all'applicazione Threat Intelligence, automatizza le attività basilari, come le richieste di approvazione, le scansioni per il rilevamento di malware o l'acquisizione di maggiori informazioni sulle minacce. I pacchetti di orchestrazione per i prodotti integrati per la sicurezza agevolano le attività più comuni, come le richieste di blocco dei firewall, direttamente dall'applicazione Security Operations. Una knowledge base (KB) sulla sicurezza fornisce ulteriori informazioni e gli articoli della KB più pertinenti vengono automaticamente associati agli incidenti per semplificarne la consultazione.

Tutte le attività svolte durante il ciclo di vita di un incidente, dall'analisi e dalle indagini fino al contenimento e alla remediation, sono registrate nella piattaforma. Quando si chiude un incidente, le relative valutazioni vengono trasmesse al team e viene automaticamente creata una revisione post-incidente, con indicazione della data e dell'ora, che fungerà da record storico dell'audit.

Applicazione Vulnerability Response
L'applicazione Vulnerability Response integrata nella soluzione Security Operations definisce la priorità degli asset vulnerabili e fornisce maggiore contesto per poter determinare se i sistemi business-critical sono a rischio. Utilizzando il CMDB, è anche in grado di identificare facilmente le interdipendenze tra i sistemi e valutare rapidamente l'impatto di eventuali cambiamenti o dell'indisponibilità dei servizi a livello aziendale. Vulnerability Response offre un quadro completo di tutte le vulnerabilità che riguardano un determinato servizio nonché una panoramica dello stato corrente delle varie vulnerabilità che interessano l'organizzazione nel suo complesso.

I team di intervento possono anche avvalersi dei flussi di lavoro e degli strumenti di automazione disponibili nella Now Platform per porre rimedio più rapidamente alle vulnerabilità riscontrate. Quando si rilevano vulnerabilità critiche, un flusso di lavoro può avviare automaticamente una richiesta di approvazione di una patch di emergenza. Ottenuta l'approvazione, gli strumenti di orchestrazione possono applicare la patch e attivare un'ulteriore scansione delle vulnerabilità per verificare che il problema sia stato effettivamente risolto. In caso di patch non urgenti, è sufficiente selezionare un pulsante per creare una richiesta di cambiamento e inviare le informazioni pertinenti allo staff IT. In questo modo, viene messa in atto una strategia coordinata di remediation delle vulnerabilità per i vari servizi e asset che consente di porre rapidamente rimedio alle principali criticità.

> “Security Incident Response semplifica l'identificazione degli incidenti critici e fornisce flussi di lavoro e strumenti di automazione per accelerare il processo di remediation.

Applicazione Configuration Compliance
Un'errata configurazione del software può esporre le organizzazioni al rischio di compromissioni. L'applicazione Configuration Compliance definisce le priorità e pone rimedio alle vulnerabilità degli asset non configurati correttamente in base ai dati di analisi delle configurazioni di sicurezza di terzi. Utilizza il CMDB per stabilire quali elementi presentano le maggiori criticità. I flussi di lavoro e gli strumenti di automazione consentono di intervenire rapidamente sui singoli asset o di apportare cambiamenti in blocco a gruppi di asset.

Coordina facilmente le attività con il team IT da un'unica piattaforma per gestire i necessari cambiamenti e aggiornamenti. Inoltre, i dati dell'applicazione Configuration Compliance possono essere integrati nella funzionalità di monitoraggio continuo di ServiceNow® Governance, Risk and Compliance per mitigare ulteriormente i rischi.

Applicazione Threat Intelligence
La soluzione Security Operations comprende l'applicazione Threat Intelligence, che consente al personale incaricato di rispondere agli incidenti di individuare gli indicatori di compromissione (IoC, Indicators of Compromise) e ricercare eventuali minacce e attacchi nascosti. Quando un IoC è connesso a un incidente di sicurezza, l'applicazione esegue automaticamente una ricerca nei feed di informazioni sulle minacce e può inviare gli IoC a soggetti terzi per sottoporli a un'ulteriore analisi. I risultati sono direttamente riportati nel record dell'incidente di sicurezza che verrà esaminato dall'analista, in modo da risparmiare tempo prezioso. ServiceNow supporta numerosi feed di informazioni sulle minacce, ivi inclusi gli standard STIX e TAXII, per integrare i dati di treat intelligence provenienti da diverse fonti.

Applicazione Trusted Security Circles
Utilizza Trusted Security Circles per condividere i dati di threat intelligence con i colleghi del settore, con i fornitori o con una community di clienti ServiceNow a livello globale. Invia una query in forma anonima, contenente gli observable di sicurezza, ad altri utenti e ricevi automaticamente il numero delle osservazioni effettuate. Questi dati possono essere utilizzati dagli analisti della sicurezza per stabilire se l'attività sospetta può essere parte di un attacco su più larga scala.

Gli utenti possono impostare valori limite per il numero di osservazioni al fine di creare automaticamente un incidente di sicurezza qualora la soglia degli observable venga superata. La partecipazione ai Trusted Security Circles può contribuire ad allertare tempestivamente gli utenti di eventuali attacchi sferrati a gruppi comuni.

Performance Analytics per Security Operations
Crea dashboard e report avanzati in tempo reale grazie all'applicazione Performance Analytics, che comprende indicatori chiave di prestazione (KPI) integrati e consente la creazione di ulteriori KPI personalizzati per tenere traccia dei parametri di misurazione più importanti per la tua organizzazione. Utilizza i dati storici per individuare eventuali colli di bottiglia, perfezionare i processi di intervento e identificare le attività da automatizzare. Ottieni una migliore visibilità e acquisisci maggiore fiducia nel livello generale di sicurezza della tua azienda grazie a dati affidabili.

> “La soluzione Security Operations comprende l'applicazione Threat Intelligence, che consente al personale incaricato di rispondere agli incidenti di individuare gli indicatori di compromissione e ricercare eventuali minacce e attacchi nascosti.

servicenow

SN-DS-Security-Operations-062018