



La sicurezza è nulla senza controllo

“Le aziende hanno investito nel rafforzare le proprie infrastrutture di sicurezza puntando su diverse tecnologie, dai Firewall ai meccanismi di autenticazione, dalle sonde intrusion detection e prevention ai sistemi di encryption. Purtroppo però da quando è nato il software ha visto la luce anche il concetto di vulnerabilità. Oggi ne contiamo più di 2000 per semestre (dati ISTR Vol XIII); 46 sono invece i giorni medi che gli 8 top Software vendor impiegano per rilasciare le relative patch. Diventa quindi evidente come gli investimenti fatti dalle aziende in strumenti di protezione quali Firewall e Intrusion Detection e Prevention possano essere messi in discussione se non vengono affiancati da una attività costante di monitoraggio in tempo reale dei dati che essi producono al fine di innescare nel minor tempo possibile il processo di gestione degli incidenti che porta al contenimento del rischio a cui ci si espone.”

A cura di Alberto Meneghini, Business Development Manager, Mediterranean Region & SMED, Managed Security Services, Symantec Corporation

Adottare un modello efficace di governo della sicurezza aiuta non soltanto a mantenere l'integrità degli asset aziendali, ma soprattutto permette di rispettare le normative vigenti aiutando così a rafforzare la fiducia nel proprio marchio.

Tale modello richiede una combinazione di tecnologia, personale con elevate competenze, processi e soprattutto fonti di *Security Intelligence* che poche aziende possono oggi vantare.

Diverse organizzazioni hanno scelto di adottare un modello cosiddetto “In-House”, scontrandosi però con innumerevoli problemi soprattutto nell'identificare gli eventi di sicurezza.

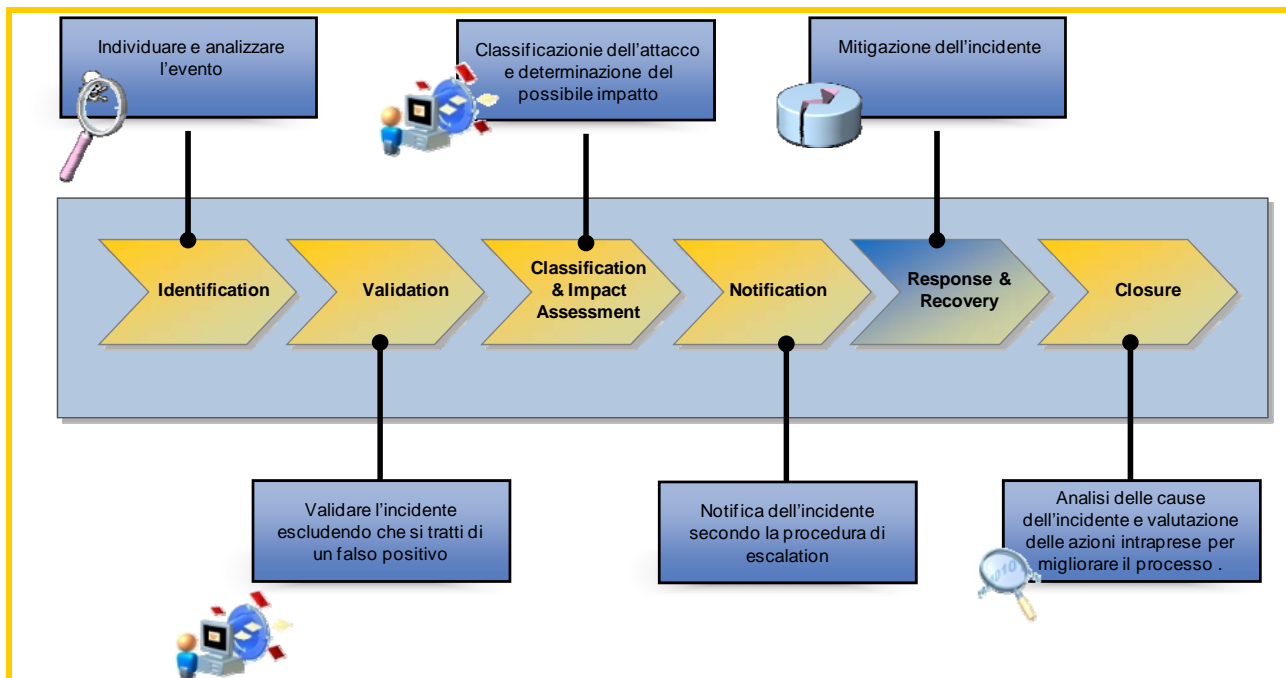
Nello specifico la sfida risiede nell'abbattere il lasso di tempo necessario per identificare gli asset a rischio, il conseguente impatto, e quale priorità attribuire all'incidente nelle procedure di *incident management*.

Lo smisurato volume di informazioni prodotte dalle diverse tecnologie di sicurezza quali Firewall, Intrusion Detection/Prevention rende tale sfida ancor più complessa.

Come risultato, molte organizzazioni che attualmente gestiscono la sicurezza “In-House” sono alla ricerca di alternative per superare tali ostacoli.

Si trovano quindi spesso a dover valutare l'opzione di collaborare con un *Managed Security Service Provider* (MSSP) che fa del monitoraggio in tempo reale della sicurezza il proprio *core business*.

I Managed Security Service Provider erogano servizi di Montoraggio ed eventualmente Gestione dei Dispositivi di Sicurezza basandosi su Security Operation Centre (SOC) ad elevata disponibilità riducendo così il numero di specialisti di sicurezza che un'azienda deve assumere, formare e trattenere.



In un processo strutturato per la gestione degli incidenti, come mostrato in fig. 1., la cosiddetta fase di identificazione è considerata una delle più critiche, ed è proprio in tale fase che il monitoraggio in tempo reale dei dispositivi di sicurezza è in grado di fare la differenza.

Partendo dall'assunto che a protezione dei propri dati siano stati introdotti i corretti sistemi di protezione come Firewall e Intrusion detection/prevention, il problema che ci si pone è come correlare e analizzare le smisurate quantità di dati da loro provenienti per identificare nel minor tempo possibile le attività illecite. Assegnare tale compito ad un MSSP (Managed Security Service Provider) si è rivelata ad oggi una delle scelte con il miglior rapporto costo/beneficio.

Gli MSSP basano la propria attività su una piattaforma di correlazione degli eventi di sicurezza che consente non soltanto di centralizzare i file di Log provenienti dai più diversi dispositivi di classe enterprise, quali Firewall e Intrusion Detection/Prevention, ma di potersi avvalere di un team di analisti in grado di configurare le regole di correlazione per individuare anche le più recenti tipologie di attacco.

Quando i file di log raggiungono il SOC, dovrebbero essere soggetti alle seguenti attività:

- **Normalizzazione:** provenendo da diverse tipologie di device di sicurezza i dati contenuti nei file di log devono essere ricondotti ad una forma standard che sia indipendente dalla sorgente per poter essere caricati nella piattaforma di correlazione.
- **Correlazione:** utilizzando le appropriate regole che l'MSSP crea per la propria piattaforma vengono eliminati i falsi positivi più evidenti e si vengono a creare gli eventi di sicurezza.
- **Contestualizzazione:** correlando l'evento di sicurezza con i dati provenienti da sorgenti di Vulnerability Assessment e RiskAssessment si può attribuire la corretta gravità e validare quindi l'incidente.

A questo punto il Security Analyst completa la procedura di Contestualizzazione con le proprie valutazioni e innesca la procedura di escalation. Il team che si occupa delle attività di remediation riceve la notifica ed inizia le attività di necessarie per mitigare l'impatto dell'incidente.

Appare quindi evidente come la tempestività e l'accuratezza della notifica unite alla tipologia di informazioni fornite al team che occupa delle attività di remediation siano in grado di discriminare la qualità del Managed Security Service Provider.