NetEye

SECURITY INFORMATION AND EVENT MANAGEMENT

Il punto di vista dell'attaccante

MASSIMO GIAIMO, Co-Founder & Senior Security Manager at SEC4U

NetEye SIEM
il punto di vista dell'attaccante

Il punto di vista dell'attaccante

Nelle nostre attività di ethical hacking sono tre le diverse fasi nelle quali ci scontriamo con l'argomento SIEM:

- la fase precedente all'attività (quella nella quale si definisce lo Scope of Engagement, sia esso per un Vulnerability Assessment, un Penetration Test o per una simulazione di attacco vera e propria)
- la fase di VA o VAPT
- la fase successiva all'attività (che spesso coincide con la presentazione del report).

Nelle tre fasi il SIEM diventa rispettivamente: un elemento di pianificazione, un elemento di sfida, un elemento di valutazione.

Nella fase precedente all'attività, in uno scenario White Box, non di rado ci viene raccontato per quale motivo si è scelto di acquisire un determinato prodotto per gestire la sicurezza aziendale e come mai si è andati verso un certo vendor invece che verso un altro (costi, supporto localizzato nel proprio paese, abilità del pre sales...). Spesso, nel momento in cui ci viene data una descrizione di questa situazione ci viene detto "Vedrete che non sarà così facile rendere i vostri tentativi di attacco invisibili alla nostra sonda". Nel momento in cui sentiamo queste parole, abbiamo sempre una piccola speranza che effettivamente il nostro interlocutore affermi ciò per esperienza diretta e non per sentito dire o perché convinto dal vendor di cui sopra.

Fatto sta che nel momento in cui veniamo a sapere, direttamente dall'interlocutore o a fronte delle fasi di information gathering/scanning, dell'esistenza di questa tipologia di dispositivi nell'infrastruttura oggetto di test, la nostra attività di Red Team subisce qualche modifica rispetto allo standard, entrando nella modalità stealth. Dal punto di vista dell'ethical hacking significa fare meno rumore possibile all'interno dell'infrastruttura, in modo tale da ridurre ai minimi termini la possibilità di rendere evidenti i tentativi di attacco. Questo, dal punto di vista pratico, include l'utilizzo di timing piuttosto alti per svolgere le attività di scanning e l'utilizzo di payload leggeri per le attività di exploiting.

Non sempre queste attenzioni - dovute - rispecchiano una necessità reale, in quanto più di una volta ci è capitato di avere a che fare con sonde implementate in modo non opportuno oppure inserite nell'infrastruttura del cliente con una configurazione nel puro stile *copy&paste*, dove probabilmente il consulente era certo del fatto che una configurazione funzionante all'interno di un'infrastruttura gestita in precedenza lo fosse anche nella nuova. Questo è il metodo errato (e pericoloso!) di installare questi oggetti.

Massimo Giaimo
Co-founder & Senior Security Manager at SEC4U

NetEye
WÜRTHPHOENIX

Würth Phoenix S.r.l.
Via Kravogl, 4
39100 Bolzano
Italia

+39 0471 56 41 11

info@wuerth-phoenix.com
www.wuerth-phoenix.com/neteye

Pensare come un attaccante

Da tempo cerchiamo di trasmettere l'idea che ogni organizzazione, anche dal punto di vista dell'information security, ha la necessità di essere gestita in modo univoco. Il livello di sicurezza è un elemento in continua rivalutazione e dipende da molteplici aspetti: le persone, la tecnologia, le modalità operative, l'ambiente circostante. Quale organizzazione può categoricamente e ragionevolmente affermare di avere questi elementi identici ad un'altra?
Un altro elemento che stiamo provando a diffondere è l'importanza del punto di vista dell'attaccante.

Nel momento in cui un cyber criminale deve pianificare (a fronte di un ingaggio, magari da parte di un competitor) un attacco nei confronti di un target, la prima attività che porrà in essere sarà quella della ricerca di più informazioni possibili sul target stesso.
Questa attività, chiamata comunemente Information Gathering, è quella nella quale l'attaccante investirà più tempo e risorse, perché sarà proprio quella in grado di fare la differenza tra il successo o il fallimento dell'attacco.

Per quale motivo un'azienda non può anticipare questa attività, in proprio oppure delegando questa attività a terzi? Gli elementi, tra gli altri, che devono essere individuati sono: informazioni maggiormente appetibili, vettori di attacco, motivazioni dell'attaccante, ambiti di vulnerabilità.

Purtroppo questo raramente succede, in primis perché è complesso trovare al proprio interno risorse umane in grado di avere la conoscenza, il punto di vista e la sensibilità necessarie ad identificare questi elementi. Inoltre in diversi ambiti la sicurezza viene ancora vista come un costo piuttosto che come un investimento. Ed è per questo che continuano ad andare a segno attacchi piuttosto banali e subdoli, a causa della presunzione di aver già implementato un'ottima strategia di difesa o semplicemente perché manca la conoscenza di quelli che potrebbero essere i vettori di attacco.

In questo l'attività di Red Team diventa fondamentale per studiare le debolezze della propria infrastruttura, perché svolta in modalità indipendente e perché consente all'organizzazione di mettere in discussione nozioni preconcette, raggiungendo una comprensione maggiore dei problemi di sicurezza che è necessario mitigare, oltre ad evidenziare informazioni sensibili, bias e pattern potenzialmente compromettenti.

Monitoring e Security: due volti della stessa medaglia

Tornando al discorso delle sonde che alcune aziende si sono portate in casa sperando di risolvere una volta per tutte l'annoso problema della sicurezza informatica, è spiacevole constatare che durante le nostre simulazioni di attacco in più di una circostanza le stesse non sono state in grado di rilevare gli attacchi e dove si sono accorte di qualcosa di strano che stava accadendo all'interno dell'infrastruttura, hanno notificato aspetti che invece di aiutare il

NetEye
WÜRTHPHOENIX

Würth Phoenix S.r.l.
Via Kravogl, 4
39100 Bolzano
Italia

+39 0471 56 41 11

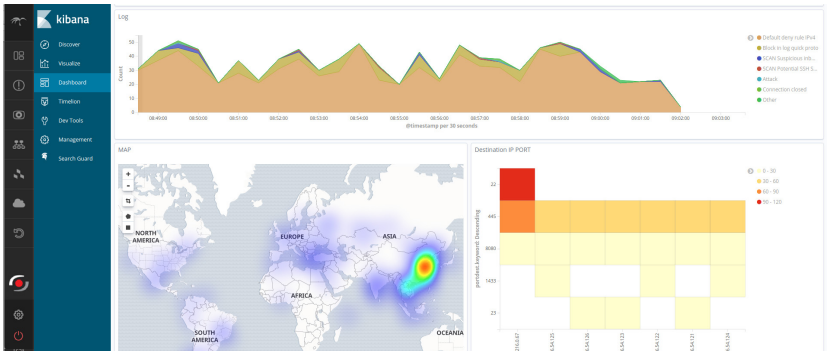
info@wuerth-phoenix.com
www.wuerth-phoenix.com/neteye

reparto IT interno ad individuare la minaccia, hanno pericolosamente confuso le idee (quale reale necessità c'è di notificare che qualcuno all'interno della rete sta visualizzando il sito di una distribuzione comunemente utilizzata per le attività di pentest mentre un attacco di tipo Cross Site Scripting, solo per fare un esempio, non viene preso minimamente in considerazione?).

Avendo a che fare quotidianamente con queste dinamiche e confrontandomi personalmente con la delusione (e con la rabbia verso il fornitore/consulente) di chi ha investito molto, sia a livello temporale che a livello economico, nella capacità di questi oggetti, ci siamo permessi di condividere alcuni concetti con Würth Phoenix, esponendo loro le nostre perplessità sulla modalità utilizzata da diversi vendor per proporre e poi implementare le soluzioni SIEM.

Da Würth Phoenix abbiamo ricevuto riscontri positivi e soprattutto volti a capire che uno strumento quale NetEye SIEM non può che trarre giovamento da questi stessi concetti.

Un elemento differenziante nella soluzione proposta da Würth Phoenix e che potenzialmente, dal punto di vista di chi scrive, può portare la soluzione ad essere uno dei punti di riferimento nel proprio ambito, è senza ombra di dubbio quella di unire, all'interno dello stesso prodotto, sia gli aspetti classici di una piattaforma di IT operations monitoring (con l'esperienza più che decennale maturata dalla soluzione in questo campo) che quelli di Security Information & Event Management. Poter osservare questi due aspetti da un unico punto di vista consente all'analista di sicurezza (o comunque a chi ha la necessità di intervenire per analizzare un determinato scenario di incidente o violazione) di veder semplificato, di molto, il proprio lavoro e di veder diminuire il tempo necessario ad individuare i diversi elementi presenti nel perimetro di osservazione dello scenario.



NetEye 4 OEM ElasticSearch Module

Di questo ci se ne rende conto appena si inizia a lavorare con NetEye SIEM, perché poter andare a generare un alert, a fronte di un evento rilevato, collegando eventualmente quell'alert ad un host già esistente e per il quale si stanno già monitorando determinate metriche (ad esempio carico della cpu, traffico di I/O, traffico delle interfacce di rete) anziché andare a generare un alert fine a se stesso (come accade invece in una piattaforma SIEM "standalone"), diventa un elemento di enorme valore. Questo per chi gestisce i sistemi è un aspetto ovvio, perché un attacco molto spesso porta ad una variazione del valore delle metriche sopra elencate.

NetEye
WÜRTHPHOENIX

Würth Phoenix S.r.l.
Via Kravogl, 4
39100 Bolzano
Italia

+39 0471 56 41 11

info@wuerth-phoenix.com
www.wuerth-phoenix.com/neteye

Quali dati inviare al SIEM?

Una delle domande che sempre più spesso riceviamo è “quali fonti di dato devo integrare, con maggiore priorità, all’interno di una piattaforma SIEM?”. L’unica risposta sensata che si può dare in questi casi è “dipende dalla necessità di monitoraggio e dai casi d’uso che si pensa possano essere maggiormente utili”. La domanda successiva diventa “ok, quali sono i miei casi d’uso?”.

Ed è in questo momento che il consulente deve tirare fuori il meglio di sé, diventando il professionista in grado di studiare alla perfezione il perimetro, interno ed esterno, dell’organizzazione, individuando in modo puntuale gli elementi citati in precedenza (informazioni maggiormente appetibili, vettori di attacco, motivazioni dell’attaccante, ambiti di vulnerabilità). Questa è un’attività di elevata complessità, perché costringe il consulente a pensare fuori dagli schemi, cercando di clonare il pensiero che avrebbe il cyber criminale nel momento di pianificazione dell’attacco.

Un aiuto fondamentale, all’interno di NetEye SIEM, deriva certamente dalla possibilità di integrare il gran lavoro già svolto dagli sviluppatori del progetto Sigma, i quali hanno censito centinaia di firme di diverse tipologie di attacco, mettendo le stesse a disposizione dell’intera community. Ci siamo così appassionati al progetto Sigma che abbiamo deciso di dare il nostro contributo, scrivendo delle regole puntuali per il rilevamento degli attacchi che spesso conduciamo durante le nostre simulazioni.

Certamente nella fase di valutazione su quali devono essere le fonti di dato da integrare nel SIEM un aspetto rilevante lo ha la componente economica, considerato che la maggior parte dei SIEM ha una modalità di licenza per gigabyte/day o EPS (Events Per Second).

E quindi: conviene utilizzare come fonte di dato quella prodotta, ad esempio, dal DHCP o dal DNS server, che magari impegnerà il 5/10% del volume della licenza e verrà utilizzata per scrivere poche o nessuna regola di rilevamento di attacchi? Meglio concentrarsi sulla fonte di dato generata dall’Intrusion Detection/Prevention System o dal WAF (Web Application Firewall)? Anche in questo caso la risposta è: dipende dal contesto.

Fortunatamente la soluzione NetEye SIEM ci viene incontro, consentendoci di limitare (utilizzando ad esempio i filtri attivabili all’interno degli Elasticsearch Beats, i componenti di Data Shipping presenti all’interno della soluzione) allo stretto necessario i dati presi in considerazione per le singole fonti di dato. Mi spiego meglio: non è necessario inviare tutti i log generati dal DHCP o dal DNS server, ma solo i messaggi utili a rilevare un attacco.

Chiaramente questo implica una profonda conoscenza, da parte del consulente, di quali possono essere gli scenari di attacco implementabili per un particolare protocollo. Stesso discorso per quanto riguarda i log generati da eventuali sistemi di EDR (Endpoint Detection & Response) già presenti, per i quali sarà opportuno filtrare gli avvisi “critici”.

NetEye
WÜRTHPHOENIX

Würth Phoenix S.r.l.
Via Kravogl, 4
39100 Bolzano
Italia

+39 0471 56 41 11

info@wuerth-phoenix.com
www.wuerth-phoenix.com/neteye

Purtroppo (o per fortuna) non esiste al momento un SIEM in grado di auto-configurarsi. Certamente, alcuni scenari "di default" possono essere implementati out of the box su diverse organizzazioni, ma ciò non è abbastanza.

Qualche anno fa un ricercatore di sicurezza descrisse la differenza tra un tool di rilevamento automatico delle vulnerabilità e una completa attività manuale di penetration test, dicendo che "gli strumenti di test (automatici) della sicurezza delle applicazioni possono dirti qualcosa sulla sicurezza. Cioè, che sei nei guai più profondi".

Il valore aggiunto in una soluzione SIEM deve per forza di cose essere la flessibilità e la completa personalizzazione di ogni parametro. Entrambi aspetti che all'interno della soluzione di Würth Phoenix sono presenti. E che configurati con il corretto tuning possono permettere di avvisare chi di dovere prima che il guaio diventi così profondo!

NetEye
WÜRTHPHOENIX

Würth Phoenix S.r.l.
Via Kravogl, 4
39100 Bolzano
Italia

+39 0471 56 41 11

info@wuerth-phoenix.com
www.wuerth-phoenix.com/neteye