Metriche utilizzate per determinare il set di regole predefinito per ogni criterio di base per le intrusioni di Firepower

Sommario

Introduzione

Cisco Talos rilascia Snort Rule Updates (SRU) per affrontare le minacce e le vulnerabilità più recenti. Una nuova release SRU può contenere set di regole aggiornati per ogni policy di base. In questo documento viene illustrato il processo utilizzato da Talos per decidere come assegnare le regole a ciascuna policy di base Intrusion per i dispositivi Firepower.

Intento criterio di base Talos definito nei metadati della regola

Le regole di base vengono gestite dai metadati all'interno degli SRU stessi. Lo stato di una determinata regola in uno dei criteri predefiniti viene definito nella parte metadati del corpo della regola. Ad esempio:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"MALWARE-CNC 1.php outbound connection
attempt"; sid:38753; gid:3; rev:1; classtype:trojan-activity; metadata:engine shared, soid
3|38753, policy balanced-ips drop, policy security-ips drop, impact_flag red; )
```

Si noti che nella regola di esempio mostrata in precedenza, la sezione dei metadati contiene policy balance-ips drop, policy security-ips drop. **Ciò indica che questa regola 1:38753 è abilitata e impostata per essere eliminata nel *criterio Balanced Security and Connectivity* e nel *criterio Security over Connectivity*.**

Metriche utilizzate per determinare il set di regole predefinito

- La metrica principale utilizzata è il punteggio CVSS (Common Vulnerability Scoring System) assegnato a ciascuna vulnerabilità che potrebbe essere coperta da una regola.
- La seconda metrica è basata sul tempo e riguarda l'età di una particolare vulnerabilità.
- La metrica finale è l'area di copertura specifica per la regola. Le regole SQL Injection, ad esempio, sono considerate abbastanza importanti da influenzare l'inclusione delle regole.

Nota: Le vulnerabilità coperte dalle norme in queste categorie sono considerate importanti, indipendentemente dall'età.

Criteri di base connettività su sicurezza

Nota: Il criterio di **connettività** è progettato specificamente per favorire le prestazioni del dispositivo rispetto ai controlli di sicurezza nel criterio. Dovrebbe consentire a un cliente di installare uno dei nostri dispositivi con il minimo di falsi positivi e prestazioni complete della scatola nella maggior parte delle installazioni di rete. Inoltre, questa policy dovrebbe rilevare le minacce più comuni e più diffuse che i nostri clienti possono sperimentare.

1. Il punteggio CVSS deve essere 10

2. La vulnerabilità riguarda gli ultimi due anni (compresi). Ad esempio:

   - Anno corrente (ad esempio, 2019)
   - Ultimo anno (2018 in questo esempio)
   - Anno prima dell'ultimo anno (in questo esempio, il 2017)

3. Categoria regola

   - Non utilizzato per questo criterio

Criterio di base bilanciato

Nota: Il criterio **Bilanciato** è il criterio predefinito consigliato per le distribuzioni iniziali. Questa politica cerca di bilanciare le esigenze di sicurezza e le caratteristiche prestazionali dei nostri sistemi. I clienti dovrebbero essere in grado di iniziare con questa politica e ottenere un ottimo tasso di blocco con strumenti di valutazione pubblici e un tasso di prestazioni relativamente elevato con strumenti di valutazione e test. Inoltre, questa regola deve garantire una prestazione pari all'80% della capacità nominale del dispositivo in condizioni normali di rete selvatica. La cosa principale da tenere sempre a mente con la regola Bilanciato è che questo è il punto di partenza del cliente, se ha una cattiva esperienza con falsi positivi, rilevamento limitato, o scarse prestazioni la maggior parte dei clienti indagherà altri dispositivi per la distribuzione nella loro infrastruttura. Si tratta dello stato di spedizione predefinito del set di regole per abbonati Snort per Snort open-source venduto su Snort.org.

1. Punteggio CVSS 9 o superiore

2. La vulnerabilità riguarda gli ultimi due anni (compresi). Ad esempio:

   - Anno corrente (ad esempio, 2019)
   - Ultimo anno (2018 in questo esempio)
   - Anno prima dell'ultimo anno (in questo esempio, il 2017)

3. Categoria regola

- Malware-CnC
- Blacklist
- SQL Injection
- Exploit-kit

4. Se la regola è inclusa nel criterio **di connettività**

Criterio di base sicurezza su connettività

> **Nota:** La politica di **sicurezza** è stata concepita per il segmento più piccolo della nostra base clienti, che si occupa in modo eccezionale della sicurezza dell'organizzazione. I clienti implementano questo criterio in reti protette, che hanno requisiti di larghezza di banda inferiori, ma requisiti di sicurezza molto più elevati. Inoltre, i clienti si preoccupano meno dei falsi positivi e delle firme rumorose. Anche il controllo delle applicazioni e l'utilizzo della rete bloccato rappresentano problemi per i clienti che implementano questo criterio. Dovrebbe fornire la massima protezione e il massimo controllo delle applicazioni, ma non dovrebbe far crollare la rete.

1. Punteggio CVSS 8 o superiore

2. La vulnerabilità riguarda gli ultimi tre anni (compresi). Ad esempio:

   - Anno corrente (ad esempio, 2019)
   - Ultimo anno (2018 in questo esempio)
   - Anno prima dell'ultimo anno (in questo esempio, il 2017)
   - Anno precedente (2016 in questo esempio)

3. Categoria regola

   - Malware-CnC
   - Blacklist
   - SQL Injection
   - Exploit-kit

4. Se la regola è nella politica **Bilanciamento** e **connettività**

Criterio di base Max-Detect (rilevamento massimo):

> **Nota:** Il set di regole **Rilevamento massimo** deve essere utilizzato negli ambienti di test e pertanto non è ottimizzato per le prestazioni. I falsi positivi per molte delle norme di questa politica sono tollerati e/o attesi e le indagini del PQ di norma non saranno intraprese.

1. La copertura è necessaria per le prove sul campo.

2. Include le regole nei set di regole **Sicurezza**, **Bilanciato** e **Connettività**.

3. Include tutte le regole attive sopra il SID: 10000, salvo diversa indicazione.

Frequenza degli aggiornamenti dei criteri

Tutte le nuove regole vengono inserite nelle politiche basate su questi criteri. Ogni anno le politiche saranno riesaminate e le regole degli anni precedenti, come l'età delle vulnerabilità, saranno rimosse dalla politica per mantenere la politica conforme ai nostri criteri di selezione temporale.

Se il punteggio CVSS cambia per una particolare vulnerabilità coperta da una regola, la sua presenza in una politica basata sulla metrica CVSS viene rivalutata.

Le politiche sono in continua crescita. A parte un forte ribilanciamento per allinearli a un obiettivo specifico, le principali perdite di regole dalle politiche non sempre si verificano se siamo soddisfatti del numero di regole e delle prestazioni della politica sul prodotto

> Nota: Le politiche di base possono crescere oltre il riequilibrio annuale principale per allinearle a un obiettivo specifico. Le eliminazioni di regole dai criteri non sempre si verificano se Talos è soddisfatto del numero di regole e delle prestazioni dei criteri sul prodotto in condizioni di rete normali. Le regole nei criteri elencati vengono valutate in base a una regola per regola. Alcune regole sono meno recenti e non sono incluse nei criteri indicati in precedenza, ma saranno incluse nei criteri predefiniti. Quanto sopra è il criterio di selezione per le regole predefinite ed è sempre soggetto a modifiche in base al panorama delle minacce.

> Nota: le regole nei criteri elencati vengono valutate in base a una regola. Alcune regole sono meno recenti e non sono incluse nei criteri indicati in precedenza, ma saranno incluse nei criteri predefiniti. Quanto sopra rappresenta il criterio di selezione per le regole predefinite ed è sempre soggetto a modifiche in base allo scenario di minaccia