Criterio di correlazione FMC: consenti eventi elenco richiede l'attivazione dei criteri di individuazione della rete

Sommario

Problema

Quando si configurano i criteri di correlazione con gli elenchi Consenti in Cisco Secure Firewall Management Center (FMC), è importante notare che gli eventi Consenti elenco e Consenti violazioni elenco non vengono generati a meno che i criteri di individuazione della rete non siano configurati per l'IP della rete di destinazione. Senza questa configurazione, in Analisi > Correlazione > Consenti eventi elenco e Analisi > Correlazione > Consenti violazioni elenco non vengono visualizzati eventi.

Durante gli esami di laboratorio sono stati osservati i seguenti comportamenti:

- Gli eventi di correlazione vengono generati correttamente per la rete di destinazione configurata.
- Quando l'host della rete di destinazione diventa non conforme, non vengono generati eventi o violazioni elenco consentiti.

Ambiente

- Cisco Firepower Threat Defense (FTD) gestito da Secure Firewall Management Center (FMC)
- Criteri di correlazione configurati con l'elenco Consenti indirizzi IP specifici
- Elenco Consenti configurato per consentire un'applicazione Web, un'applicazione o un protocollo specifico

Risoluzione

Dopo approfonditi test di laboratorio e consultazioni con il team di sviluppo, è stato confermato che i criteri di individuazione della rete devono essere abilitati come prerequisito per la generazione di eventi elenco consentiti e violazioni elenco consentite.

La risoluzione prevede le seguenti fasi:

Passaggio 1: Abilita criteri di individuazione della rete

Passare a Criteri > Individuazione rete nell'interfaccia di FMC e creare una regola se non ne esiste alcuna.

Passaggio 2: Configura regola di individuazione della rete

Configurare la regola di individuazione della rete con le impostazioni di rete di origine appropriate:

- Specificare la rete di origine come intervallo di rete interno.
- In alternativa, usare tutte le reti (0.0.0.0/0) per monitorare tutte le origini del traffico.
- Verificare che la regola copra le reti da cui si prevede di generare gli eventi dell'elenco Consenti.

Passaggio 3: Attiva regole dei criteri di correlazione

Verificare che le regole dei criteri di correlazione siano attive e non disattivate.

Passaggio 4: Verifica generazione eventi elenco Consenti

Dopo l'attivazione dell'individuazione della rete e l'attivazione delle regole dei criteri di

correlazione:

1.- Accedere ai siti Web dalla rete di destinazione configurata utilizzando un browser (rendendo l'host non conforme).

2.- Controlla analisi > Correlazione > Consenti eventi elenco e analisi > Correlazione > Consenti violazioni elenco per generazione eventi.

3.- Verificare che gli eventi vengano popolati quando l'host diventa non conforme.

I test di laboratorio hanno confermato che dopo l'abilitazione di Individuazione rete, gli eventi elenco consentiti e le violazioni elenco consentite vengono generati correttamente per un host non conforme.

Causa

La causa principale è che Criteri individuazione rete è un prerequisito obbligatorio per la generazione di eventi elenco consentiti nei criteri di correlazione FMC. Senza un criterio di individuazione della rete attivo, il sistema non è in grado di valutare correttamente la conformità dell'host rispetto all'elenco degli indirizzi consentiti configurato. Di conseguenza, non è possibile generare eventi dell'elenco degli indirizzi consentiti quando l'host della rete di destinazione diventa non conforme.

Contenuto correlato

- Documentazione sugli elenchi di conformità Cisco FMC Correlation
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).