FMC-correlatiebeleid Lijstgebeurtenissen toestaan vereisen dat het beleid voor netwerkdetectie is ingeschakeld

Inhoud

uitgifte

Bij het configureren van correlatiebeleid met lijsten met toegangsrechten in Cisco Secure Firewall Management Center (FMC), is het belangrijk op te merken dat Lijstgebeurtenissen toestaan en Lijstovertredingen toestaan niet worden gegenereerd, tenzij het Netwerkdetectiebeleid is geconfigureerd voor het doelnetwerk IP. Zonder deze configuratie worden geen gebeurtenissen weergegeven onder Analyse > Correlatie > Lijstgebeurtenissen en -analyse toestaan > Correlatie > Lijstovertredingen toestaan.

Tijdens laboratoriumtests werden deze gedragingen waargenomen:

- Correlatiegebeurtenissen worden correct gegenereerd voor het geconfigureerde doelnetwerk.
- Er worden geen lijstgebeurtenissen toestaan of overtredingen van lijst toestaan gegenereerd wanneer de doelnetwerkhost niet-conform wordt.

milieu

- Cisco Firepower Threat Defense (FTD) wordt beheerd door het Secure Firewall Management Center (FMC)
- Correlatiebeleid geconfigureerd met lijst met specifieke IP-adressen toestaan
- Lijst toestaan die is geconfigureerd om een specifieke webtoepassing, toepassing of protocol toe te staan

resolutie

Na uitgebreide laboratoriumtests en overleg met het ontwikkelingsteam werd bevestigd dat Network Discovery-beleid moet worden ingeschakeld als een voorwaarde voor het genereren van Allow List Events en Allow List Violations.

De resolutie omvat de volgende stappen:

Stap 1: Netwerkdetectiebeleid inschakelen

Navigeer naar Beleid > Netwerkdetectie in de FMC-interface en maak een regel als deze niet bestaat.

Stap 2: Netwerkdetectieregel configureren

Configureer de regel voor netwerkdetectie met de juiste netwerkinstellingen voor de bron:

- Geef het bronnetwerk op als uw interne netwerkbereik.
- U kunt ook alle netwerken (0.0.0.0/0) gebruiken als u alle verkeersbronnen controleert.
- Zorg ervoor dat de regel betrekking heeft op de netwerken waarvan u verwacht Allow List Events te genereren.

Stap 3: Correlatiebeleidsregels activeren

Controleer of de regels voor het correlatiebeleid actief zijn en niet in een uitgeschakelde staat.

Stap 4: Verifieer het genereren van een lijstgebeurtenis toestaan

Nadat u de netwerkdetectie hebt ingeschakeld en de regels voor het correlatiebeleid hebt

geactiveerd:

1.- Toegang tot websites van het geconfigureerde doelnetwerk met behulp van een browser (waardoor de host niet-conform is).

2.- Monitor Analyse > Correlatie > Lijstgebeurtenissen en -analyse toestaan > Correlatie > Lijstoverschrijdingen toestaan voor het genereren van gebeurtenissen.

3.- Controleer of de gebeurtenissen worden ingevuld wanneer de host niet-conform is.

Laboratoriumtests hebben bevestigd dat zodra Network Discovery is ingeschakeld, Allow List Events en de Allow List Violations succesvol zijn gegenereerd voor een host die niet aan de eisen voldoet.

Oorzaak

De hoofdoorzaak is dat Network Discovery Policy een verplichte voorwaarde is voor het genereren van Allow List Events in FMC Correlation Policies. Zonder een actief beleid voor het opsporen van netwerken kan het systeem de naleving van de hostvereisten niet goed beoordelen aan de hand van de geconfigureerde lijst met toegestane gebeurtenissen, waardoor er geen gebeurtenissen in de lijst met toegestane gebeurtenissen worden gegenereerd wanneer de host van het doelnetwerk niet-conform wordt.

Gerelateerde inhoud

- Cisco FMC Correlation Compliance Lists-documentatie
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.