FMC-Korrelationsrichtlinie Listenereignisse zulassen erfordert Aktivierung der Netzwerkerkennungsrichtlinie

Inhalt

Problem

Beim Konfigurieren von Korrelationsrichtlinien mit Zulassungslisten im Cisco Secure Firewall Management Center (FMC) ist zu beachten, dass Zulassungslistenereignisse und Zulassungslistenverletzungen nur dann generiert werden, wenn die Netzwerkerkennungsrichtlinie für die Zielnetzwerk-IP konfiguriert ist. Ohne diese Konfiguration werden unter Analyse > Korrelation > Listenereignisse zulassen und Analyse > Korrelation > Listenverletzungen zulassen keine Ereignisse angezeigt.

Während der Labortests wurden folgende Verhaltensweisen beobachtet:

- Korrelationsereignisse werden für das konfigurierte Zielnetzwerk richtig generiert.
- Es werden keine Zulassungslistenereignisse oder Zulassungslistenverletzungen generiert, wenn der Zielnetzwerk-Host nicht mehr konform ist.

Umwelt

- Cisco FirePOWER Threat Defense (FTD), verwaltet vom Secure Firewall Management Center (FMC)
- Korrelationsrichtlinie konfiguriert mit Zulassungsliste für spezifische IP-Adressen
- Zulassungsliste, die so konfiguriert ist, dass sie eine bestimmte Webanwendung, Anwendung oder ein bestimmtes Protokoll zulässt

Auflösung

Nach ausführlichen Labortests und Konsultationen mit dem Entwicklungsteam wurde bestätigt, dass die Netzwerkerkennungsrichtlinie aktiviert sein muss, damit Ereignisse in der Zulassungsliste und Verstöße gegen die Zulassungsliste generiert werden können.

Die Entschließung umfasst folgende Schritte:

Schritt 1: Netzwerkerkennungsrichtlinie aktivieren

Navigieren Sie in der FMC-Schnittstelle zu Policies > Network Discovery, und erstellen Sie eine Regel, wenn keine vorhanden ist.

Phase 2: Netzwerkerkennungsregel konfigurieren

Konfigurieren Sie die Netzwerkanalyseregel mit den entsprechenden Quellnetzwerkeinstellungen:

- Geben Sie das Quellnetzwerk als internen Netzwerkbereich an.
- Alternativ können Sie alle Netzwerke (0.0.0.0/0) verwenden, um alle Datenverkehrsquellen zu überwachen.
- Stellen Sie sicher, dass die Regel die Netzwerke abdeckt, von denen Sie erwarten, dass sie Zulassungslistenereignisse generieren.

Schritt 3: Korrelationsrichtlinien-Regeln aktivieren

Überprüfen Sie, ob die Korrelationsrichtlinienregeln aktiv sind und sich nicht im deaktivierten Zustand befinden.

Schritt 4: Überprüfung der Generierung von Zulassungslistenereignissen

Nach der Aktivierung der Netzwerkerkennung und der Aktivierung der Korrelationsrichtlinienregeln:

1.- Zugriff auf Websites aus dem konfigurierten Zielnetzwerk über einen Browser (dadurch wird der Host als nicht konform eingestuft)

2.- Analyse überwachen > Korrelation > Listenereignisse und Analyse zulassen > Korrelation > Listenverletzungen für Ereignisgenerierung zulassen.

3.- Überprüfen Sie, ob Ereignisse ausgefüllt werden, wenn der Host nicht konform ist.

Labortests haben bestätigt, dass nach Aktivierung der Netzwerkerkennung die Generierung von Zulassungslistenereignissen und Zulassungslistenverletzungen für einen nicht konformen Host erfolgreich abgeschlossen wurde.

Ursache

Die Ursache liegt darin, dass die Netzwerkerkennungsrichtlinie eine obligatorische Voraussetzung für das Generieren von Zulassungslistenereignissen in FMC-Korrelationsrichtlinien ist. Ohne eine aktive Netzwerkerkennungsrichtlinie kann das System die Host-Konformität nicht ordnungsgemäß mit der konfigurierten Zulassungsliste vergleichen, was dazu führt, dass keine Zulassungslistenereignisse generiert werden, wenn der Zielnetzwerk-Host nicht mehr konform ist.

Verwandte Inhalte

- Dokumentation zu Cisco FMC Correlation-Compliance-Listen
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.