Configurer la liste verte et la liste noire IP dans la console Secure Endpoint Cloud

Table des matières

Introduction

Ce document décrit la fonctionnalité IP Allow/Block au sein de Cisco Secure Endpoint.

Conditions préalables

Exigences

Cisco vous recommande d'accéder au portail Cisco Secure Endpoints.

Composants utilisés

Les informations contenues dans ce document sont basées sur la console Secure Endpoint.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configuration d'une liste d'autorisation/de blocage IP avec un terminal sécurisé

Qu'est-ce qu'une liste d'adresses IP autorisées/bloquées ?

Les listes de blocage et d'autorisation IP sont utilisées avec la corrélation de flux de périphérique pour définir des détections d'adresses IP personnalisées. Une fois que vous avez créé vos listes, vous pouvez définir dans la stratégie de les utiliser en plus de Cisco Intelligence Feed ou seuls. Les listes peuvent être définies pour utiliser des adresses IP individuelles, des blocs CIDR ou des combinaisons d'adresses IP et de ports. Lorsque vous soumettez une liste, les adresses redondantes sont combinées sur le serveur principal.

Exemples d'adresses IP

Si vous ajoutez ces entrées à une liste :

- 192.0.2.0/24
- 192.0.2.15

- 192.0.2.135
- 192.0.2.200

La liste est traitée avec un résultat net de :

- 192.0.2.0/24

Cependant, si vous incluez également des ports, le résultat est différent :

- 192.0.2.0/24
- 192.0.2.15:80
- 192.0.2.135
- 192.0.2.200

La liste est traitée avec un résultat net de :

- 192.0.2.0/24
- 192.0.2.15:80

Qu'est-ce qu'une liste verte IP ?

Une liste d'adresses IP autorisées vous permet de spécifier des adresses IP que vous ne souhaitez jamais détecter. Les entrées de votre liste IP autorisée créent un remplacement dans votre liste IP bloquée ainsi que dans le flux Cisco Intelligence. Vous pouvez ajouter des adresses IP uniques, des blocs CIDR entiers ou spécifier des adresses IP avec des numéros de port.

Qu'est-ce qu'une liste de blocage IP ?

Une liste de blocage IP vous permet de spécifier les adresses IP que vous souhaitez détecter chaque fois qu'un de vos ordinateurs s'y connecte. Vous pouvez ajouter des adresses IP uniques, des blocs CIDR entiers ou spécifier des adresses IP avec des numéros de port. Lorsqu'un ordinateur établit une connexion à une adresse IP de votre liste, l'action entreprise dépend de ce que vous avez spécifié dans la section Réseau de votre stratégie.

Qu'est-ce qu'une liste d'adresses IP autorisées ?

Une liste d'autorisation IP d'isolement spécifie les adresses IP qui ne sont pas bloquées pendant l'isolement. Les listes d'autorisation IP d'isolation sont différentes des listes d'autorisation IP car les listes d'autorisation IP d'isolation ne prennent pas en charge les numéros de port dans la règle.

Créer une liste d'autorisation/de blocage IP

Étape 1. Afin de créer une liste IP, naviguez jusqu'à Outbreak Control dans le portail Secure Endpoint et cliquez sur IP Block & Allow Lists option, comme indiqué dans l'image.

Outbreak Control

CUSTOM DETECTIONS

Simple

Advanced

Android

APPLICATION CONTROL

Blocked Applications

: les listes d'adresses IP téléchargées peuvent contenir jusqu'à 10 000 lignes ou avoir une taille maximale de 2 Mo. Seules les adresses IPv4 sont actuellement prises en charge. Pour améliorer les performances et inclure davantage d'adresses, utilisez des blocs CIDR.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.