

Configura elenco indirizzi IP consentiti e bloccati nella console Secure Endpoint Cloud

Sommario

Introduzione

In questo documento viene descritta la funzione IP Allow/Block (Consenti/Blocca IP) in Cisco Secure Endpoint.

Prerequisiti

Requisiti

Cisco consiglia di accedere al portale Cisco Secure Endpoints.

Componenti usati

Le informazioni discusse in questo documento si basano sulla console dell'endpoint sicuro.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione di un elenco indirizzi IP consentiti/bloccati con endpoint protetto

Che cos'è un elenco indirizzi IP consentiti/bloccati?

Gli elenchi di indirizzi IP bloccati e consentiti vengono utilizzati con la correlazione del flusso di dispositivi per definire rilevamenti di indirizzi IP personalizzati. Dopo aver creato gli elenchi, è possibile definirli nel criterio per utilizzarli in aggiunta al feed di Cisco Intelligence o singolarmente. È possibile definire gli elenchi in modo da utilizzare singoli indirizzi IP, blocchi CIDR o combinazioni di indirizzi IP e porte. Quando si invia un elenco, gli indirizzi ridondanti vengono combinati sul back-end.

Esempi di indirizzi IP

Se si aggiungono queste voci a un elenco:

- 192.0.2.0/24
- 192.0.2.15
- 192.0.2.135
- 192.0.2.200

L'elenco viene elaborato con il risultato netto di:

- 192.0.2.0/24

Tuttavia, se si includono anche le porte, il risultato è diverso:

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

L'elenco viene elaborato con il risultato netto di:

- 192.0.2.0/24
- 192.0.2.15:80

Che cos'è un elenco indirizzi IP consentiti?

Un elenco di indirizzi IP consentiti consente di specificare indirizzi IP che non si desidera rilevare. Le voci dell'elenco indirizzi IP consentiti creano una sostituzione nell'elenco indirizzi IP bloccati e nel feed di Cisco Intelligence. È possibile aggiungere singoli indirizzi IP, interi blocchi CIDR oppure specificare indirizzi IP con numeri di porta.

Che cos'è un elenco indirizzi IP bloccati?

Un elenco di indirizzi IP bloccati consente di specificare gli indirizzi IP che si desidera rilevare ogni volta che uno dei computer si connette a tali indirizzi. È possibile aggiungere singoli indirizzi IP, interi blocchi CIDR oppure specificare indirizzi IP con numeri di porta. Quando un computer effettua una connessione a un indirizzo IP dell'elenco, l'azione intrapresa dipende da quanto specificato nella sezione Rete del criterio.

Che cos'è un elenco indirizzi IP consentiti per l'isolamento?

Un elenco di indirizzi IP consentiti per l'isolamento specifica gli indirizzi IP che non vengono bloccati durante l'isolamento. Gli elenchi indirizzi IP consentiti per l'isolamento sono diversi dagli elenchi indirizzi IP consentiti in quanto gli elenchi indirizzi IP consentiti per l'isolamento non supportano i numeri di porta nella regola.

Creare un elenco indirizzi IP consentiti/bloccati

Passaggio 1. Per creare un elenco di indirizzi IP, passare al controllo delle epidemie nel portale degli endpoint sicuri e fare clic sull'opzione IP Block & Allow Lists, come mostrato nell'immagine.

Outbreak Control v



CUSTOM DETECTIONS

Simple

Advanced

Android

APPLICATION CONTROL

Blocked Applications

Allowed Applications

: gli elenchi IP caricati possono contenere fino a 10.000 righe o avere una dimensione massima di 2 MB. Al momento sono supportati solo indirizzi IPv4. Per migliorare le prestazioni e includere più indirizzi, utilizzare i blocchi CIDR.

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).