Configurazione del flusso di lavoro automatico di Isolamento endpoint con Cisco XDR

Sommario

Introduzione

In questo documento viene descritto come creare un flusso di lavoro di automazione per isolare un endpoint per un nuovo incidente.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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

In questa guida vengono illustrati in dettaglio i passaggi necessari per configurare e attivare un flusso di lavoro in modo da isolare automaticamente un endpoint quando si verifica un evento imprevisto. L'integrazione viene eseguita con Cisco Secure Endpoint e la funzionalità di automazione del flusso di lavoro. Le fasi sono descritte come segue.

Configurazione iniziale in Cisco Secure Endpoint

Passaggio 1.1: Abilitare la funzionalità di isolamento nel criterio

1. Accedere al portale Cisco Secure Endpoint.
2. Passare alla sezione Gestione > Criteri.
3. Selezionare il criterio applicabile all'endpoint che si desidera isolare.
4. Verificare che l'opzione Isolamento dispositivi sia attivata nelle impostazioni dei criteri. 

   Consenti isolamento endpoint da criteri endpoint protetti

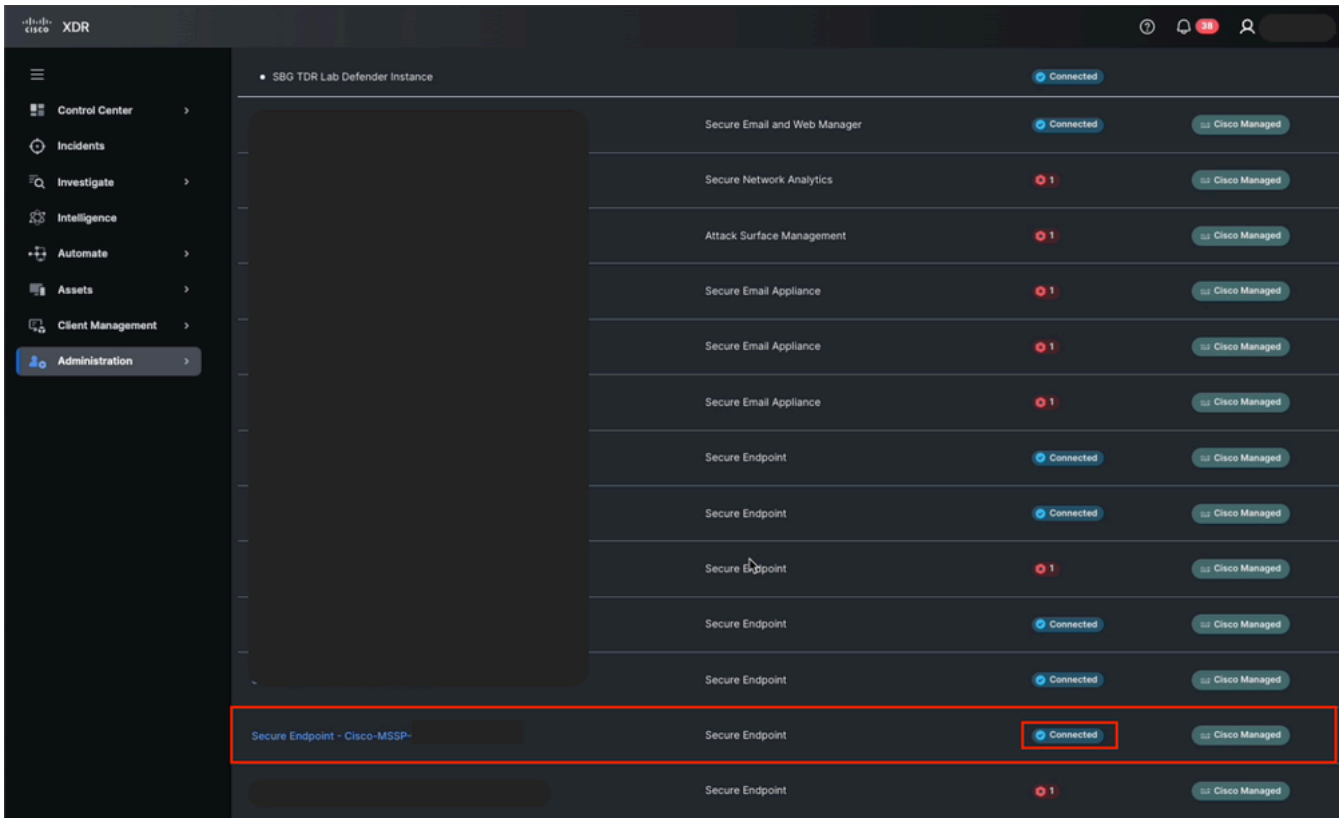
5. Salvare le modifiche e distribuire il criterio, se necessario.

Convalida l'integrazione con Cisco Secure Endpoint

Passaggio 2.1: Verifica dell'integrazione

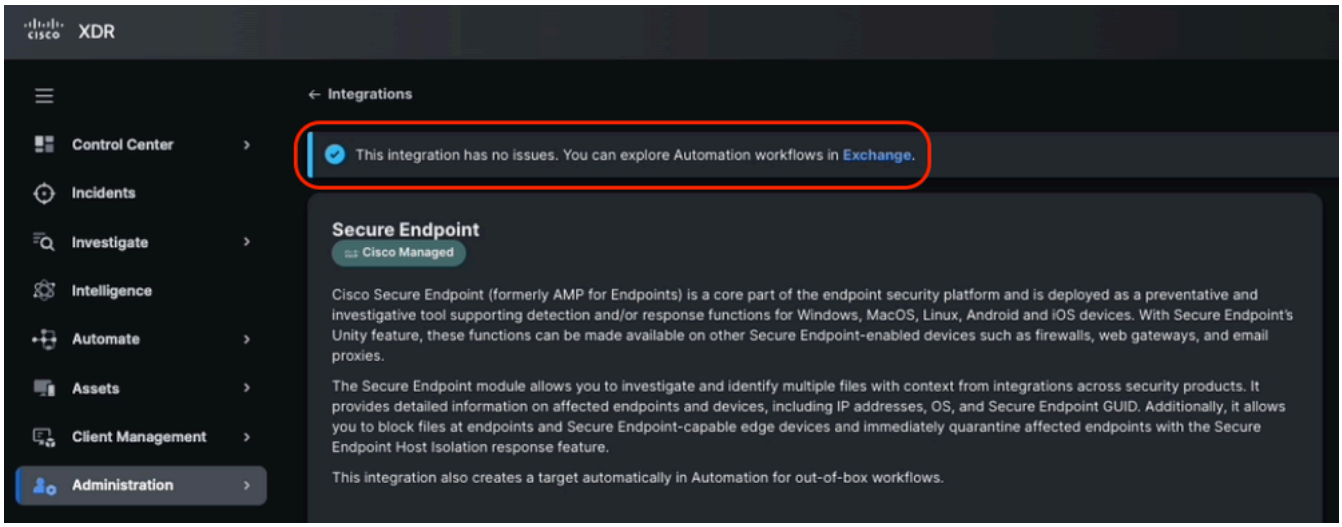
1. Accedere a Cisco XDR
2. Passare alla sezione Amministrazione > Integrazioni > Integrazioni personali.
3. Verificare che l'integrazione con Cisco Secure Endpoint sia configurata correttamente:

   Verificare lo stato di integrazione in Connesso.



Stato integrazione endpoint sicuro da Cisco XDR

Verificare che non vi siano errori nella configurazione API.



Controllo dello stato di integrazione degli endpoint sicuri

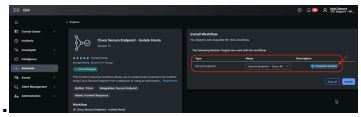
Installare il flusso di lavoro da Cisco XDR Exchange

Passaggio 3.1: Installare il flusso di lavoro Isolamento endpoint

1. Accedere a Cisco XDR e selezionare Automate > Exchange.
2. Cercare il flusso di lavoro Cisco Secure Endpoint - Isolare gli host e fare clic su Installa. 

Isolamento del flusso di lavoro host da Exchange

3. Verificare che la destinazione sia disponibile prima dell'installazione.



Destinazione modulo abilitata dal flusso di lavoro

4. Installare il flusso di lavoro nel sistema di automazione.

Creare una regola di automazione

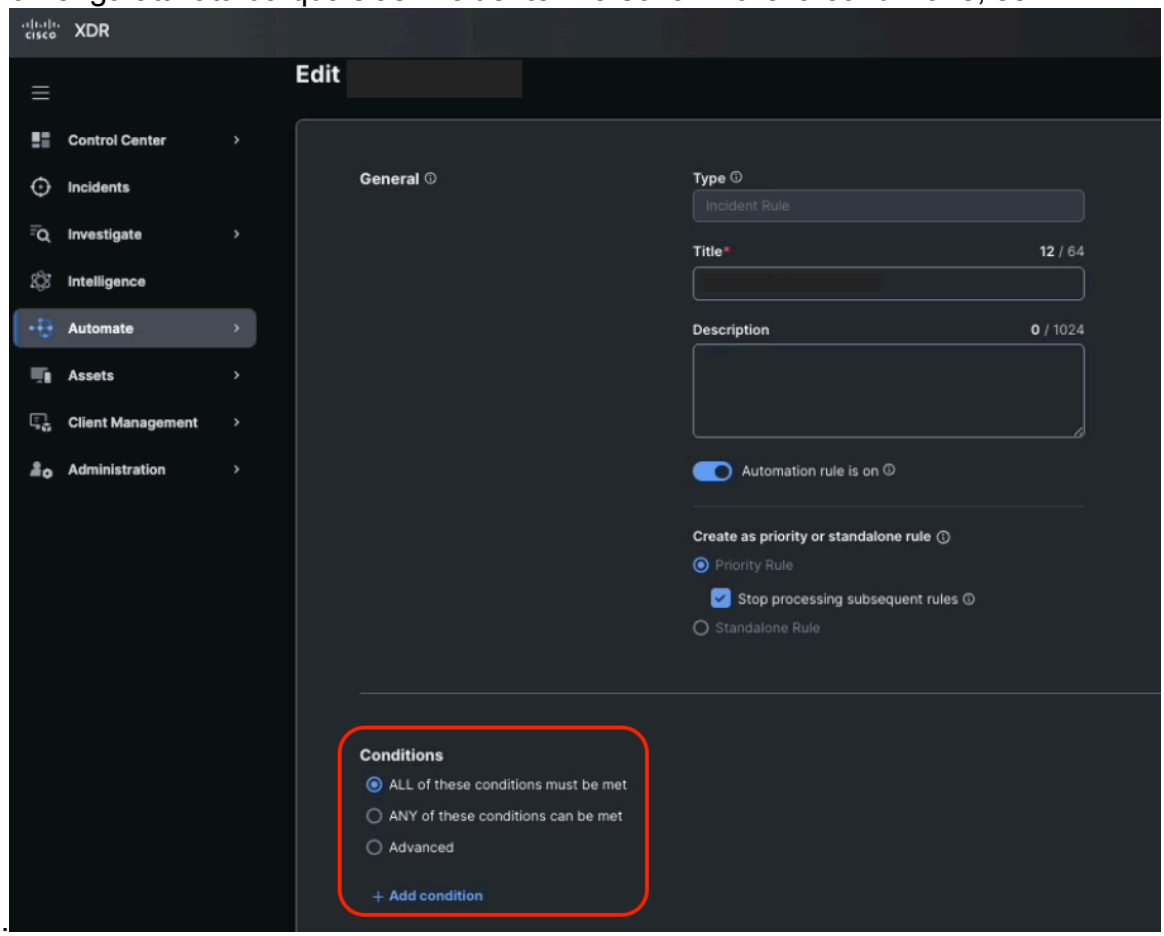
Una regola di automazione è una configurazione che definisce quando un flusso di lavoro deve essere eseguito, in base a eventi specifici o a una pianificazione predefinita. Queste regole possono includere condizioni facoltative e, se tali condizioni vengono soddisfatte, i flussi di lavoro associati vengono attivati automaticamente.

Passaggio 4.1: Configurare una regola di automazione

1. Passare alla sezione Automazione > Trigger.
2. Crea una nuova regola. Fare clic su Aggiungi regola di automazione e assegnare un nome.

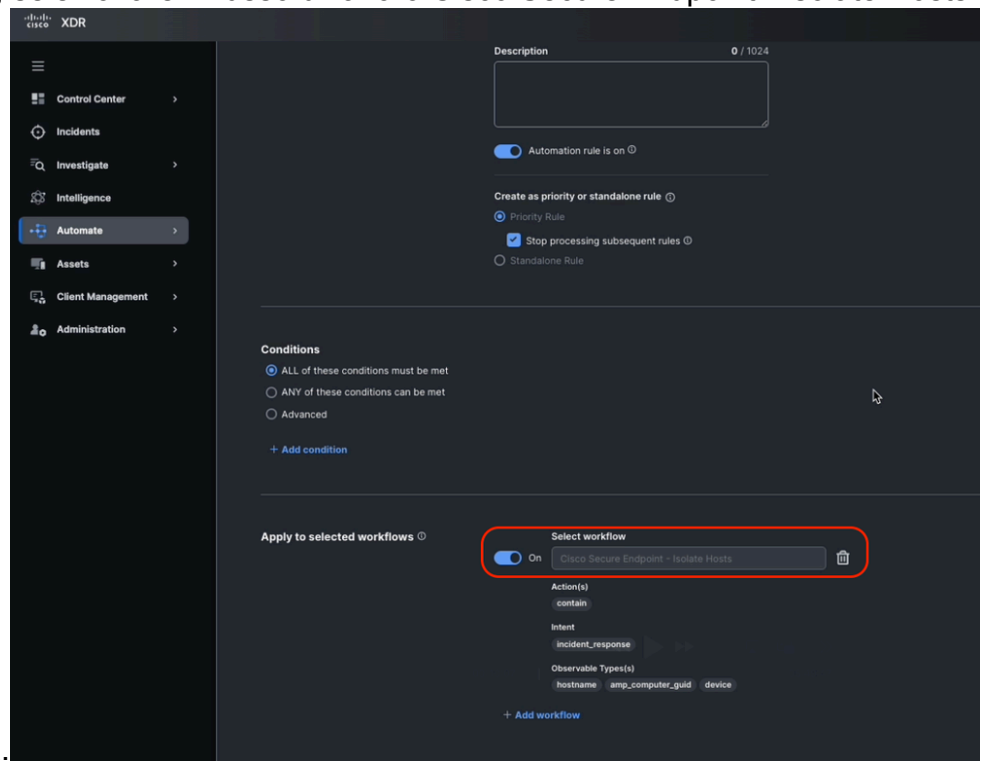
Aggiungi regola di automazione da trigger

3. Impostare le condizioni di attivazione. È possibile lasciare vuote le condizioni per garantire che la regola venga attivata da qualsiasi incidente. Personalizzare la condizione, se necessario.



Condizioni delle regole di automazione

4. Nell'azione della regola, selezionare il flusso di lavoro Cisco Secure Endpoint - Isolate Hosts installato in precedenza.



Assegna la regola di automazione al flusso di lavoro

5. Fare clic su Save (Salva).

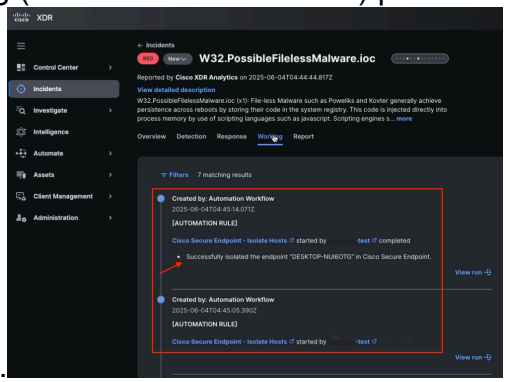
Convalida funzionalità flusso di lavoro

Passaggio 5.1: Verifica esecuzione flusso di lavoro

1. Generare o attendere un evento imprevisto che soddisfi le condizioni della regola. 

Rilevato nuovo incidente in Cisco XDR

2. Una volta creato l'incidente, controllare la scheda Worklog (all'interno dell'incidente) per verificare che il workflow sia stato eseguito correttamente.

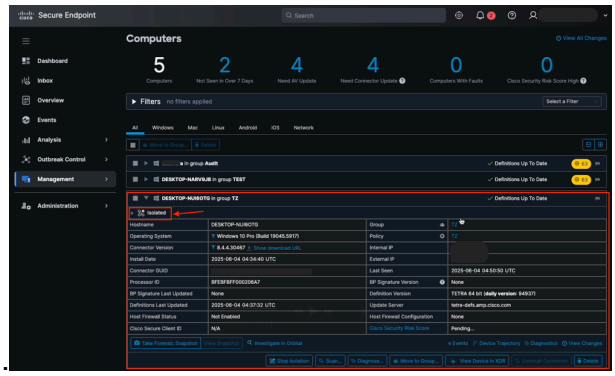


Informazioni sulla scheda Registro di lavoro incidenti

Passaggio 5.2: Conferma isolamento endpoint

1. Accedere al portale Cisco Secure Endpoint.
2. Passare alla sezione Gestione > Computer e individuare l'endpoint di destinazione.

3. Confermare che lo stato del dispositivo sia Isolato.



Stato di isolamento dai computer endpoint protetti

4. Se l'endpoint non è isolato, esaminare i registri e la configurazione del flusso di lavoro per identificare i possibili problemi.

Problema comune

La funzione di isolamento non è abilitata da Cisco Secure Endpoint

1. Da Cisco XDR, passare a Incidenti, individuare l'ultimo incidente e passare a Worklog.

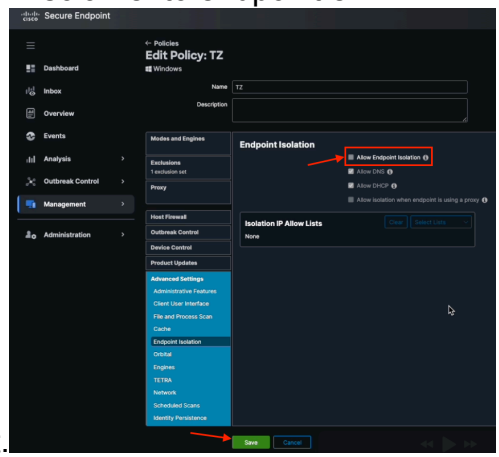
2. Verificare la presenza di eventuali errori correlati dopo l'esecuzione del flusso di lavoro di automazione.

L'isolamento degli endpoint, ad esempio, non ha consentito di isolare l'host perché l'isolamento degli endpoint non è stato abilitato nei criteri per gli endpoint sicuri.

Risultati del flusso di lavoro di automazione dal registro eventi imprevisti

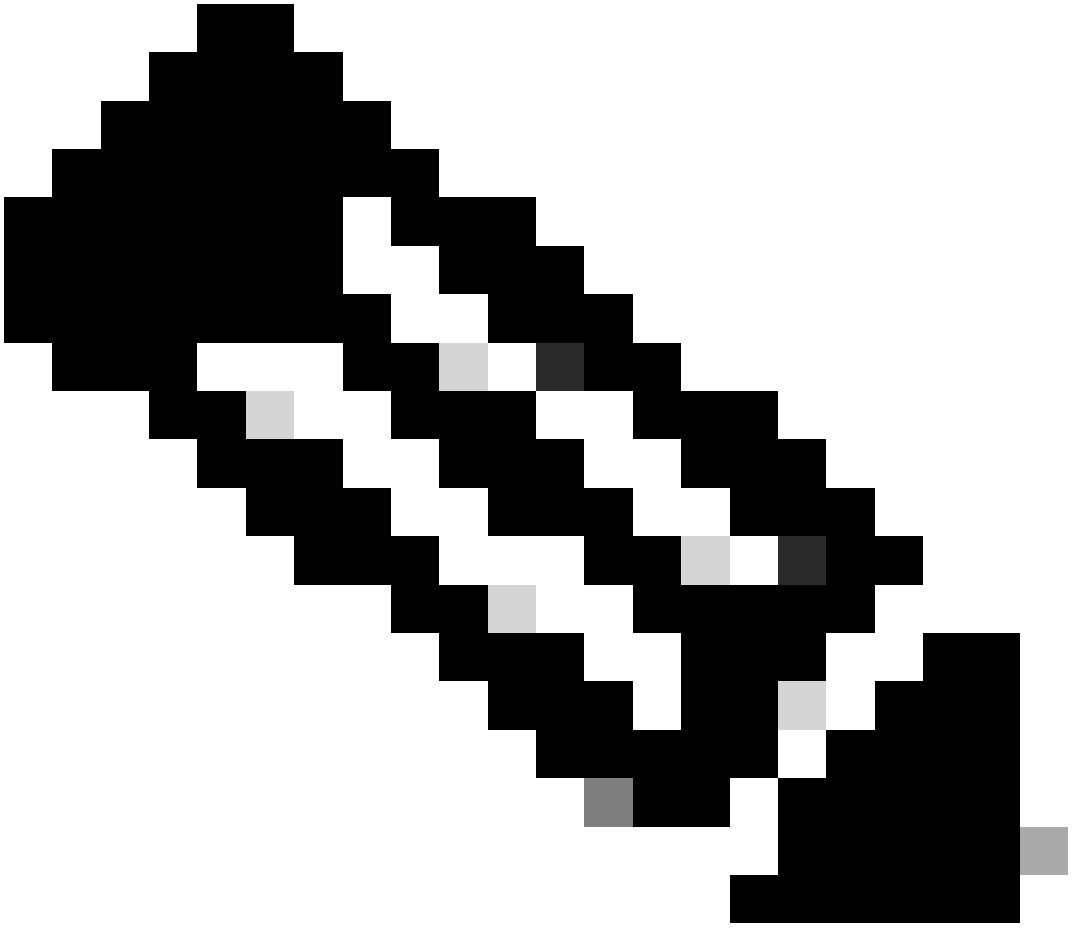
3. Da Secure Endpoint, passare a Gestione > Criteri e selezionare il criterio in questione.

4. Una volta inserito il criterio, passare a Impostazioni avanzate > Isolamento endpoint e selezionare la casella di controllo Consenti isolamento endpoint.

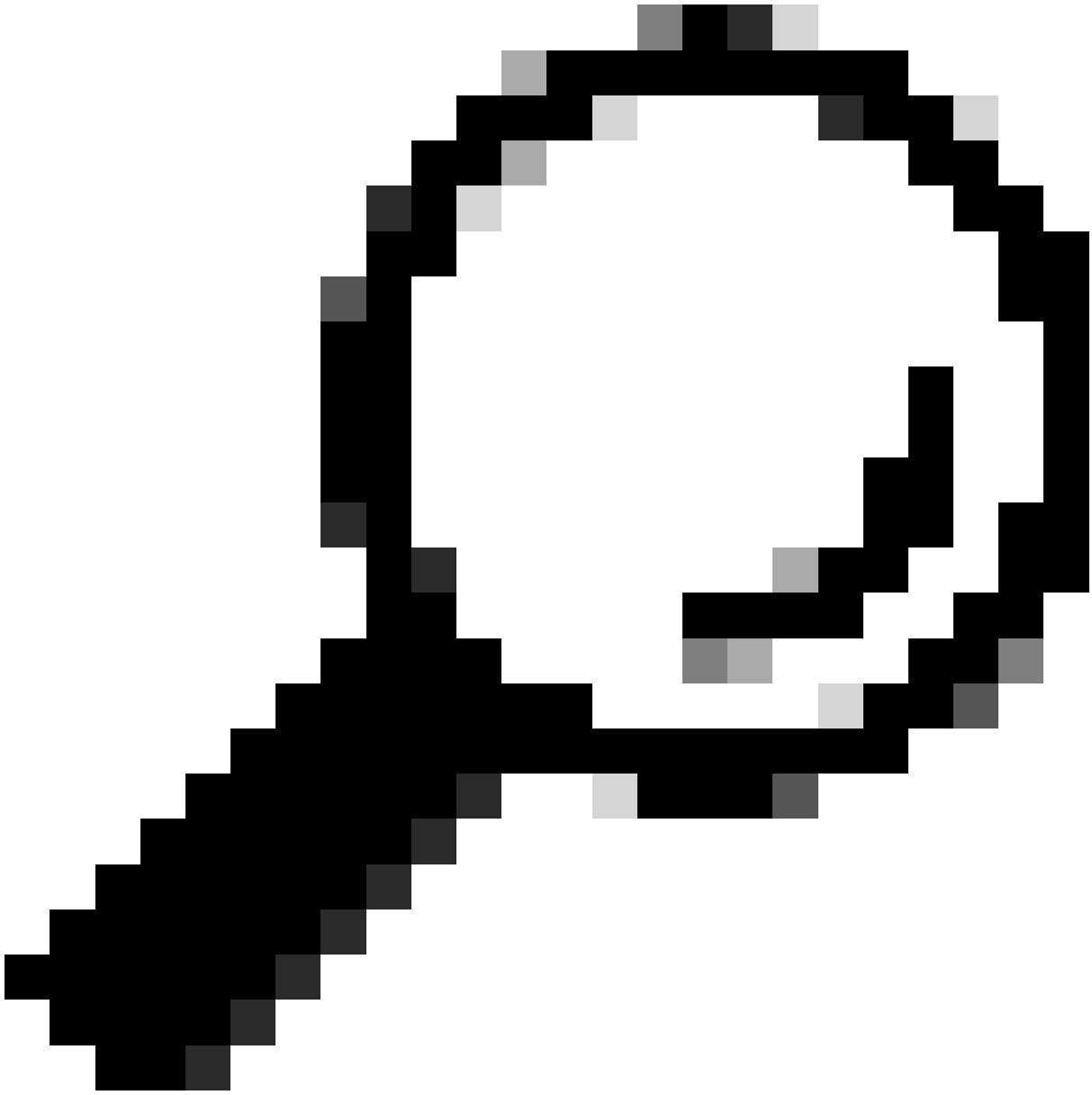


Casella di controllo Consenti isolamento endpoint nei criteri per gli endpoint protetti

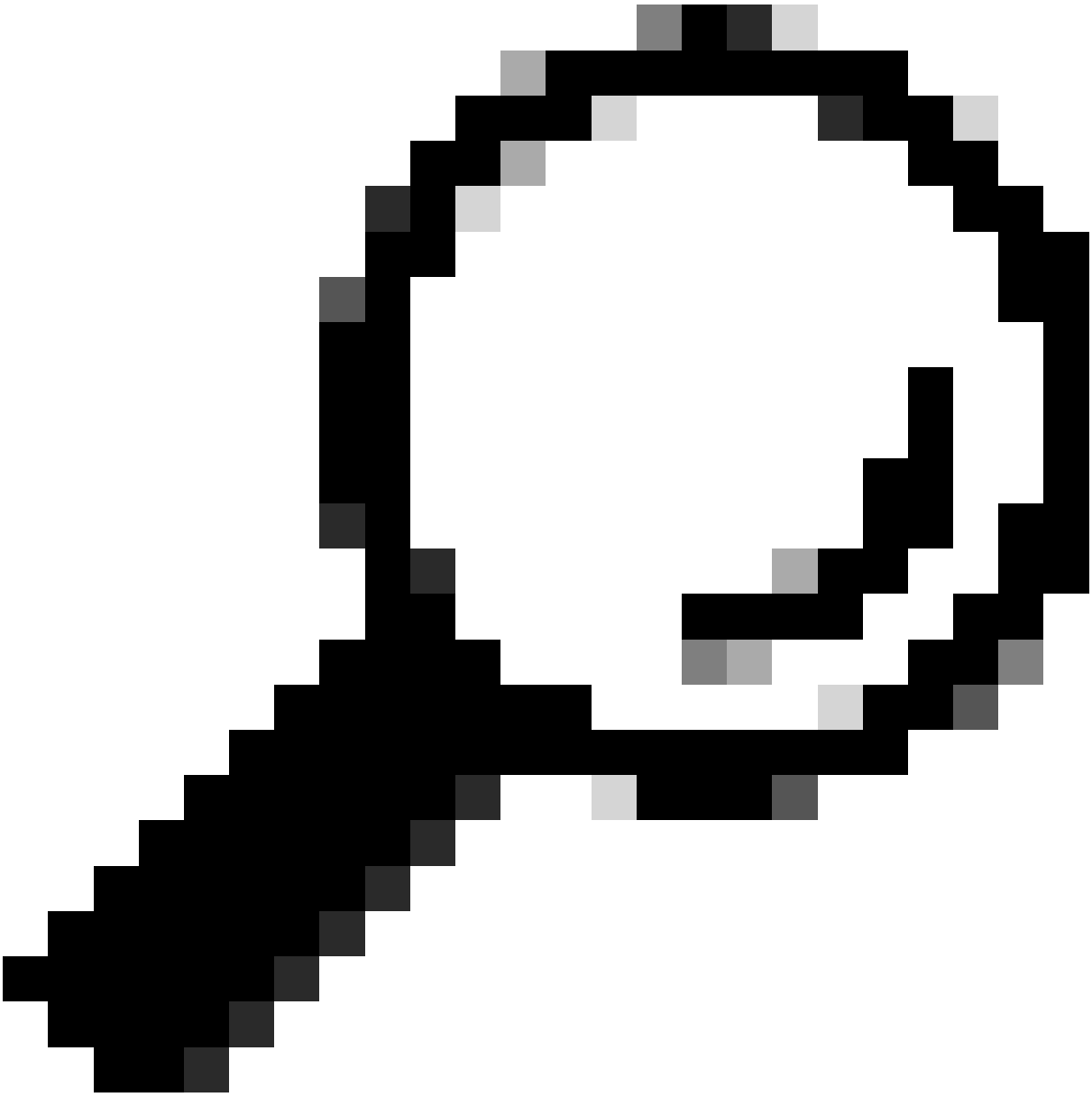
5. Fare clic su Salva.



Nota: assicurarsi di disporre delle autorizzazioni amministrative necessarie per configurare l'integrazione e il flusso di lavoro.



Suggerimento: Eseguire il test dell'installazione in un ambiente controllato prima di distribuire l'automazione in produzione.



Suggerimento: Documentare eventuali modifiche personalizzate apportate al flusso di lavoro o alla regola di automazione.

Una volta completate queste operazioni, è possibile configurare e attivare con successo un flusso di lavoro che isola automaticamente un endpoint dopo la creazione di un evento imprevisto e garantisce una risposta rapida ed efficace alle minacce alla sicurezza.

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).