

Dateien wiederherstellen, die von Secure Endpoint in Quarantäne gestellt wurden

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Problem](#)

[Lösung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Dateien, die über den Secure Endpoint Connector in Quarantäne verschoben wurden, über die Secure Endpoint-Konsole wiederhergestellt werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure Endpoint-Konsole

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Secure Endpoint Console v5.4.2025030619

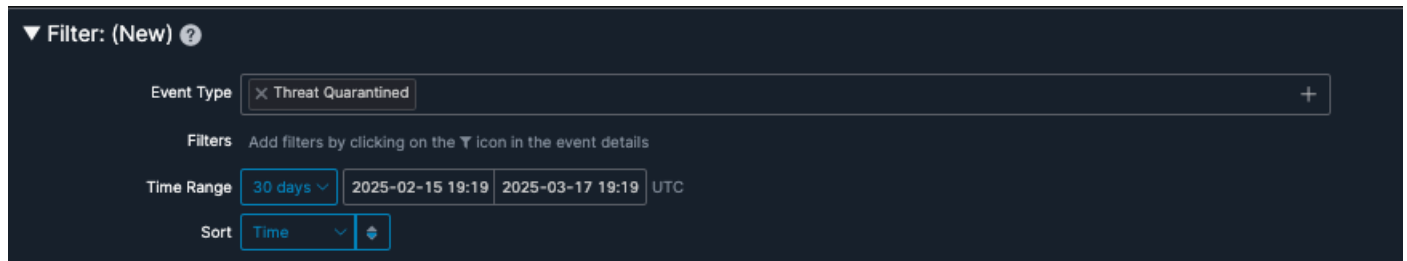
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Problem

Dateien, die über den Secure Endpoint (SE) Connector in Quarantäne gestellt wurden, können zur Dateianalyse, für falsch positive Meldungen oder zur Wiederherstellung abgerufen werden, wenn die Datei als sicher erkannt wurde. Administratoren können diese Aktion direkt über die Konsole für sichere Endgeräte ausführen.

Lösung

1. Navigieren Sie zur Seite Events auf Ihrer SE-Konsole.
2. Filtern Sie die Ereignisse, um alle erfolgreichen Quarantänen anzuzeigen, indem Sie den Filter Ereignistyp = Bedrohung in Quarantäne auswählen.



▼ Filter: (New) ?

Event Type × Threat Quarantined +

Filters Add filters by clicking on the  icon in the event details

Time Range 30 days 2025-02-15 19:19 2025-03-17 19:19 UTC

Sort Time 

Ereignistyp "Bedrohungsquarantäne"

3. Identifizieren Sie das Erkennungsereignis, das der wiederherzustellenden Datei zugeordnet ist.
4. Erweitern Sie die Ereignisdetails, um auf die Option Datei wiederherstellen zuzugreifen. Durch Auswahl von Datei wiederherstellen wird die Datei auf dem betroffenen Computer wiederhergestellt. Durch Auswahl von Alle Computer wird die Datei auf allen Computern wiederhergestellt, auf denen sie in Quarantäne verschoben wurde.

Detection	▼ Auto.16AEC5.281556.in02
Fingerprint (SHA-256)	▼ 16aec550...949beb88
File Name	▼ PEASS-ng-master.zip
File Path	/home/amir/.local/share/Trash/files/PEASS-ng-master.zip
File Size	19.55 MB
Parent	No parent SHA/Filename available.
Analyze Restore File All Computers	

Dateioptionen wiederherstellen

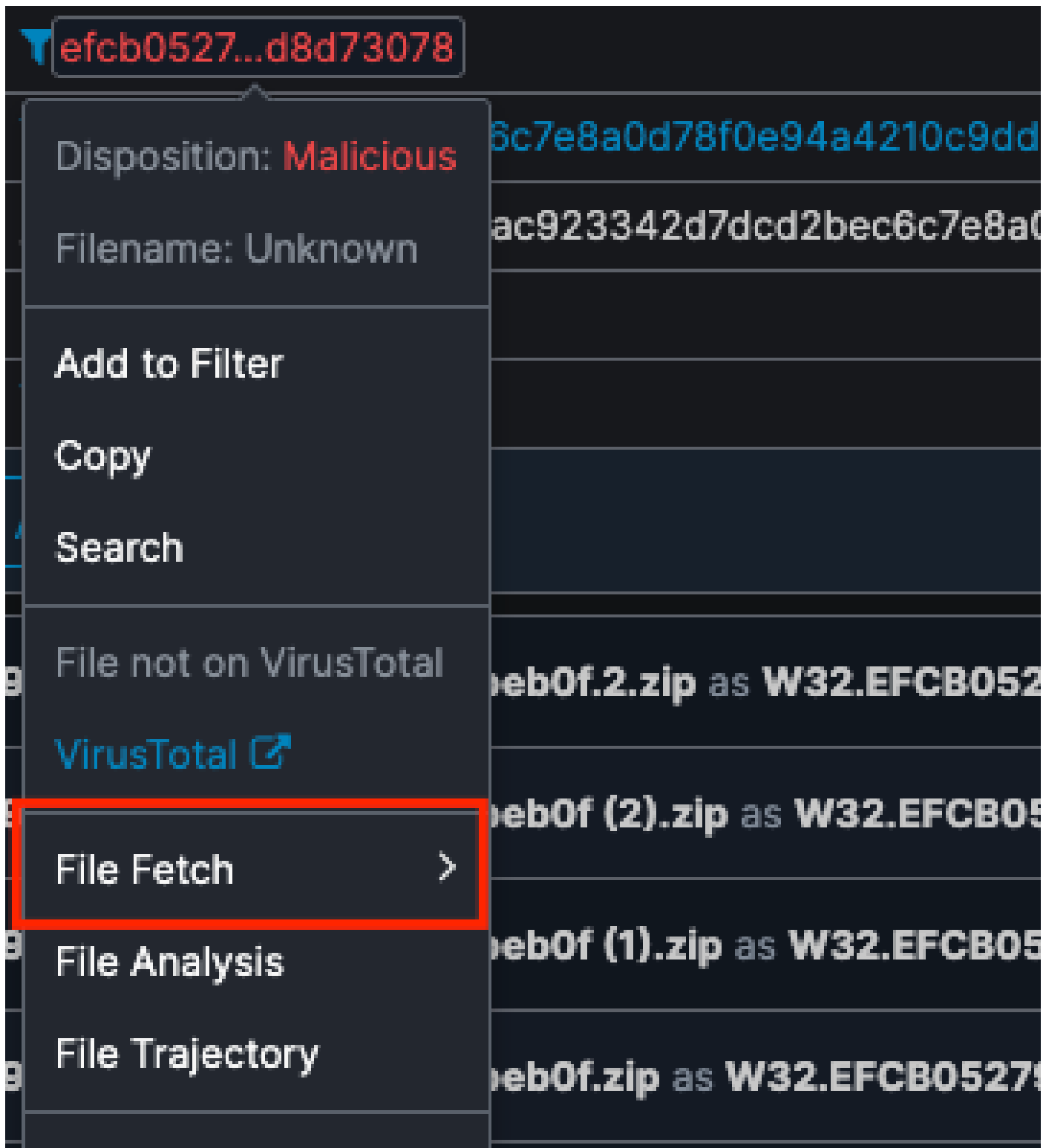
5. Das Heartbeat-Intervall gibt an, wie oft der Connector nach Hause ruft, um festzustellen, ob Dateien vorhanden sind, die vom Administrator wiederhergestellt werden müssen. Dateien werden wiederhergestellt, sobald die betroffenen Computer online sind oder das nächste Heartbeat-Intervall auftritt.
6. Wenn die Datei vertrauenswürdig ist, fügen Sie sie einer Zulassungsliste hinzu, um zu verhindern, dass sie erneut in Quarantäne verschoben wird.



Anmerkung: Dateien verbleiben 30 Tage in Quarantäne oder wenn der Quarantäne-Ordner 100 MB groß ist und die ältesten Dateien gelöscht werden. Dateien in Quarantäne können nach dem Löschen nicht mehr wiederhergestellt werden.

Wenn Sie eine Quarantäne-Datei für Bedrohungsanalysen oder falsch-positive Eingaben herunterladen müssen, ohne sie in Ihrer Umgebung wiederherzustellen, können Sie die Funktion Dateiabruf verwenden. Schritte zum Herunterladen einer Quarantäne-Datei:

1. Navigieren Sie zur Seite Events auf Ihrer SE-Konsole.
2. Filtern Sie die Ereignisse, um alle erfolgreichen Quarantänen anzuzeigen, indem Sie den Filter Ereignistyp = Bedrohung in Quarantäne auswählen.
3. Identifizieren Sie das Erkennungsereignis, das mit der herunterzuladenden Datei verbunden ist.
4. Klicken Sie auf den SHA-256-Wert der Quarantäne-Datei, um die Option Dateiabruf anzuzeigen.



Datei abrufen

Dies beinhaltet den Status des Dateiabrufs, die Option, den Abruf zu starten, und den Zugriff, um die Datei im Datei-Repository anzuzeigen.

5. Klicken Sie auf Datei abrufen, wählen Sie den Computer aus, von dem Sie die Datei abrufen möchten, und bestätigen Sie, indem Sie auf Abholen klicken.

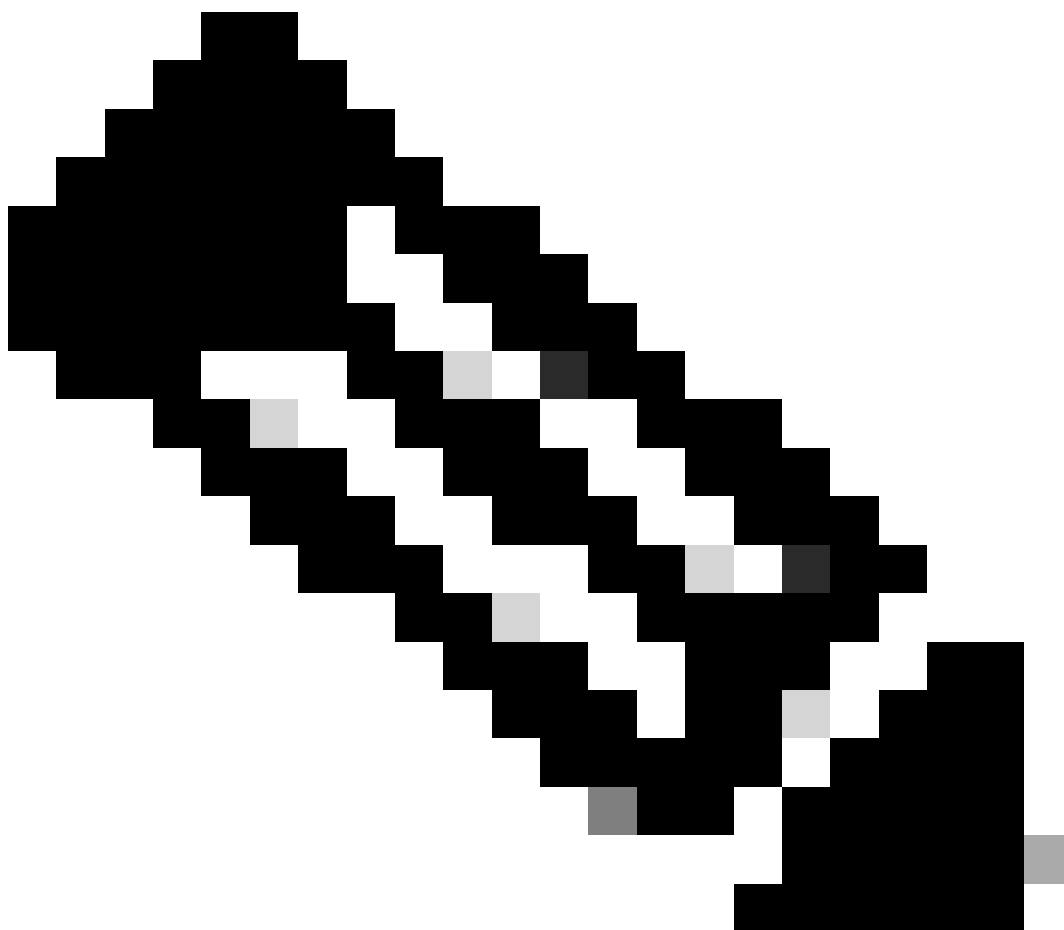
6. Eine E-Mail-Benachrichtigung wird gesendet, sobald die Datei in das Datei-Repository hochgeladen wurde.

7. Sobald die Datei verfügbar ist, können Sie die Datei und die Option zum Herunterladen in Analysis> File Repository sehen.

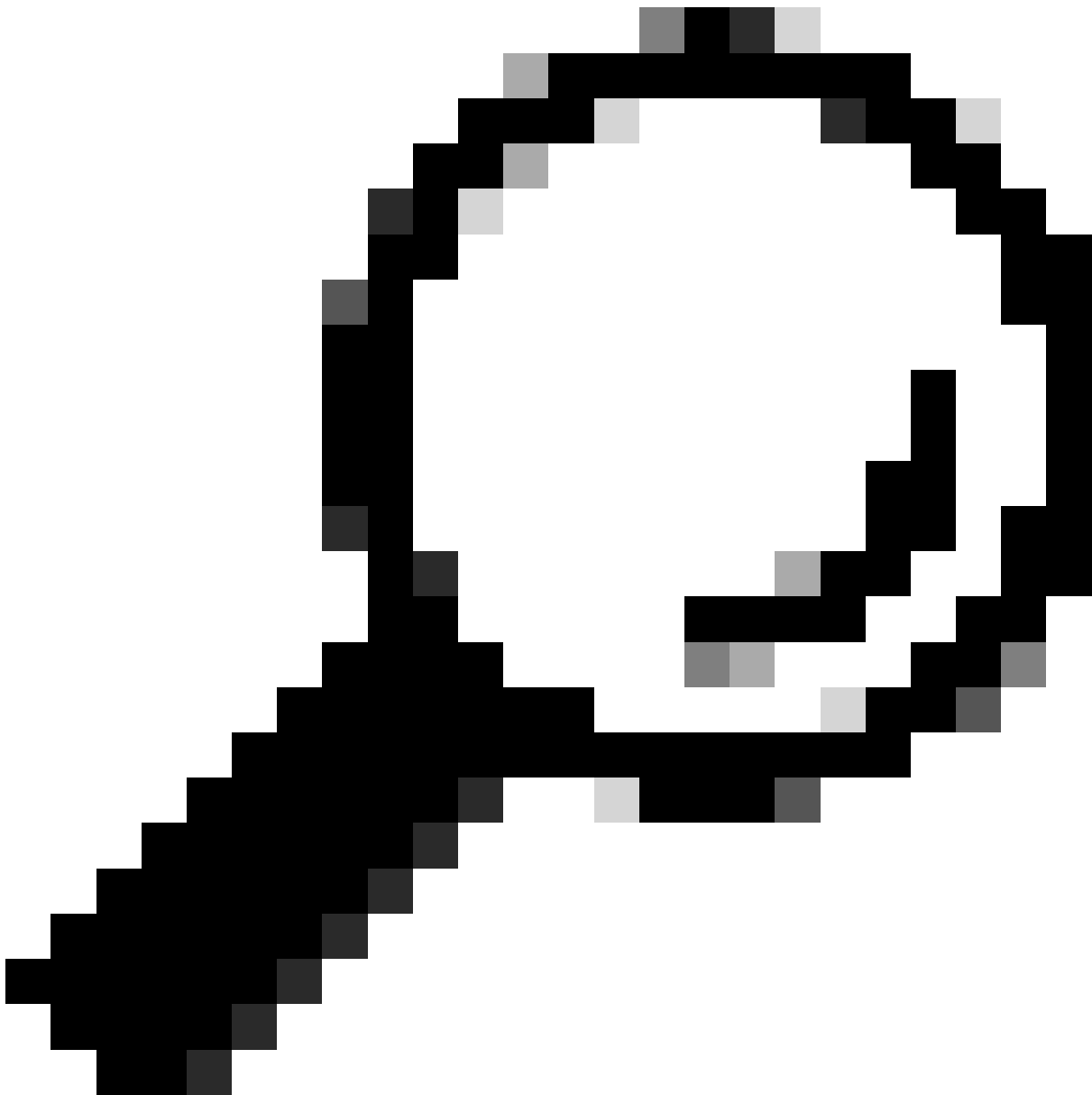
0ac923342d7dcd2bec6c7e8a0d78f0e94a4210c9dd0cbf1a750619c29c7beb0f (1).zip		Available	Aishwarya G	2025-03-17 19:34:10 UTC		
Original File Name	0ac923342d7dcd2bec6c7e8a0d78f0e94a4210c9dd0cbf1a750619c29c7beb0f (1).zip					
Fingerprint (SHA-256)	efcb0527...d8d73078					
File Size	4.99 KB					
Computer	amir					
View Changes						Analyze Download Delete

Datei herunterladen

Alle aus dem Datei-Repository heruntergeladenen Dateien sind gezippt und kennwortgeschützt.



Anmerkung: Damit der Dateiabruf ordnungsgemäß funktioniert, muss der Netzwerkverkehr zum entsprechenden Dateiabruferserver entsprechend Ihrer Cloud-Region zugelassen werden: Europa: rff.eu.amp.cisco.com Nordamerika: rff.amp.cisco.com APJC: rff.apjc.amp.cisco.com. Stellen Sie außerdem sicher, dass die Zwei-Faktor-Authentifizierung (2FA) für das Administratorkonto aktiviert ist, da dies erforderlich ist, um eine Anforderung zum Abrufen von Dateien erfolgreich zu initiieren.



Tipp: Sie können Ereignisse filtern mit Ereignistyp = Wiederherstellung in Quarantäne fehlgeschlagen und Ereignistyp = Dateiabruf fehlgeschlagen, um Fehler zu identifizieren und die entsprechenden Gründe für Wiederherstellungs- bzw. Dateiabholvorgänge zu überprüfen.

Wenn Sie die Datei nicht mithilfe der beschriebenen Schritte wiederherstellen können, wenden Sie sich an Cisco TAC, und geben Sie die .qrt-Datei im Verzeichnis C:\Program Files\Cisco\AMP\Quarantine an.

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.