Configuration et gestion des exclusions dans Cisco Secure Endpoint Connector

Table des matières

Introduction

Ce document décrit comment créer l'exclusion pour les différents moteurs sur la console Cisco Secure Endpoint.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Modifier et appliquer une liste d'exclusion à une stratégie dans la console Secure Endpoint
- convention CSIDL de Windows

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Console Cisco Secure Endpoint 5.4.20211013
- Révision du guide de l'utilisateur Secure Endpoint le 15 octobre 2021

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.

Workflow Secure Endpoint

Dans un haut niveau d'opérations, le point d'extrémité sécurisé Cisco traite un fichier SHA (Secure Hash Algorithm) dans cet ordre via les principaux composants du connecteur :

- Exclusions
- Moteur Tetra
- Contrôle des applications (liste verte/liste de blocage)
- Moteur SHA
- Prévention des exploits (Exprev) / Protection contre les activités malveillantes (MAP) / Protection des processus système / Moteur réseau (corrélation des flux de périphériques)

Remarque : l'exclusion ou la création d'une liste verte ou de blocage dépend du moteur qui a détecté le fichier.

Exclusions maintenues par Cisco

Les exclusions maintenues par Cisco sont créées et maintenues par Cisco afin d'assurer une meilleure compatibilité entre le connecteur Secure Endpoint et l'antivirus, les produits de sécurité ou d'autres logiciels.

Ces jeux d'exclusions contiennent différents types d'exclusions pour garantir un fonctionnement correct.

Vous pouvez suivre les modifications apportées à ces exclusions dans l'article Modifications de la liste d'exclusion de Cisco pour Cisco Secure Endpoint Console.

Exclusions personnalisées

Moteur Secure Endpoint

Analyse de fichiers (utilisation CPU / détections de fichiers) par Tetra & moteur SHA :

Utilisez ces types d'exclusions pour éviter la détection/la mise en quarantaine d'un fichier ou pour réduire le niveau élevé de CPU du point de terminaison sécurisé.

L'événement sur la console Secure Endpoint est illustré dans l'image.

Remarque : CSIDL peut être utilisé pour les exclusions. Consultez ce document Microsoft pour plus d'informations sur CSIDL.

Exclusion du chemin

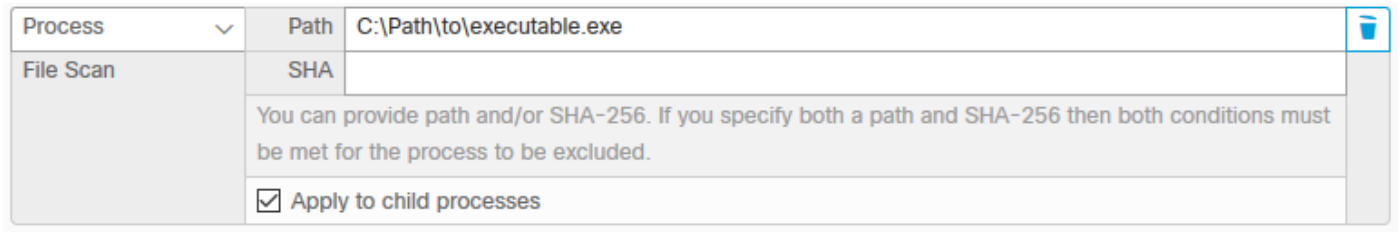
Exclusion générique

Remarque : l'option Apply to all drive letters est utilisée pour appliquer également l'exclusion aux lecteurs [A-Z] connectés au système.

Exclusion des extensions de fichier

Attention : utilisez ce type d'exclusion avec précaution car il exclut tous les fichiers portant l'extension de fichier des analyses, quel que soit l'emplacement du chemin d'accès.

Processus : Exclusion de l'analyse des fichiers

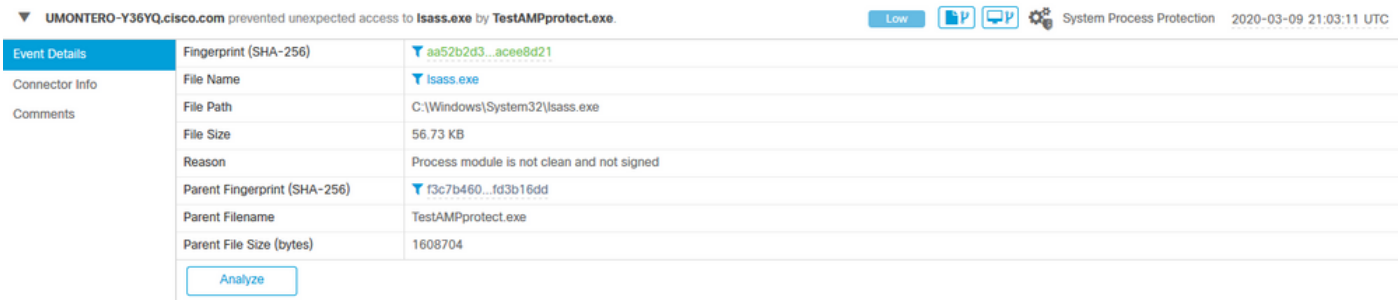


Protection des processus système (SPP)

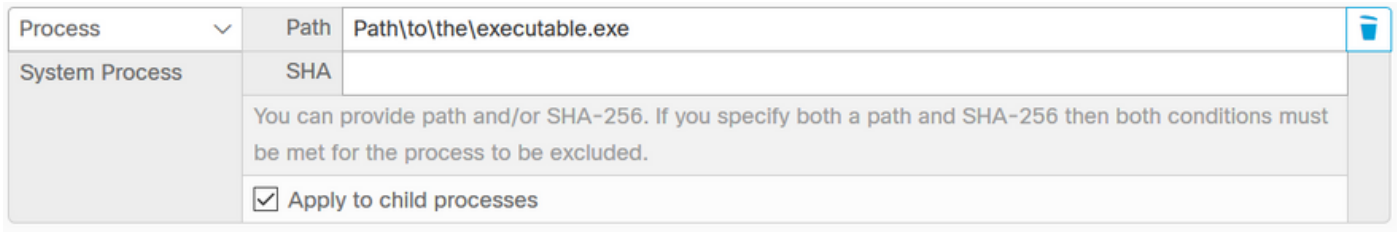
Le moteur System Process Protection est disponible à partir de la version 6.0.5 du connecteur et protège les processus Windows suivants :

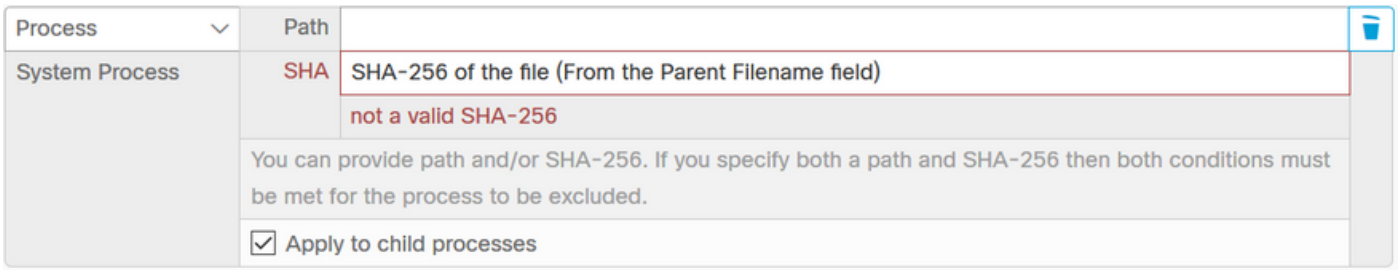
- Sous-système Gestionnaire de session (smss.exe)
- Sous-système d'exécution client/serveur (csrss.exe)
- Sous-système de l'autorité de sécurité locale (lsass.exe)
- Application de connexion Windows (winlogon.exe)
- Application de démarrage Windows (wininit.exe)

Cette image présente un événement SPP.



Exclusion SPP

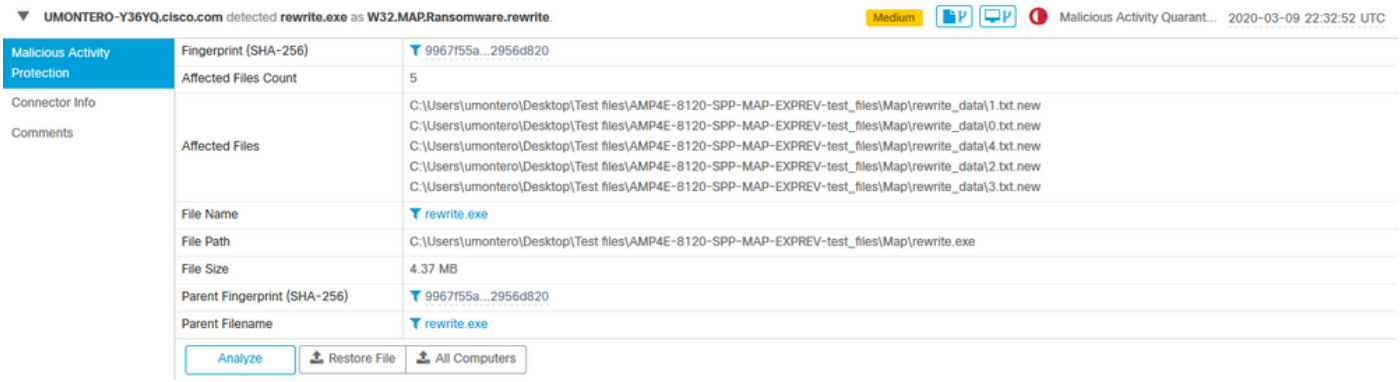




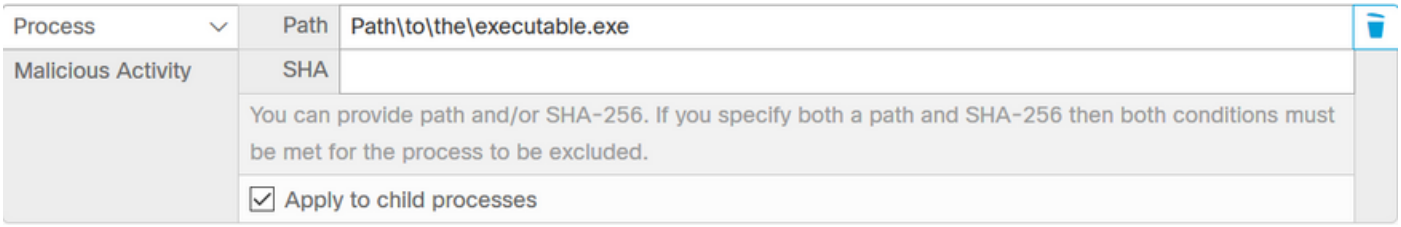
Protection contre les activités malveillantes (MAP)

Le moteur de protection contre les activités malveillantes (MAP) protège votre terminal d'une attaque par ransomware. Il identifie les actions ou les processus malveillants lors de leur exécution et protège vos données contre le chiffrement.

Un événement MAP est illustré dans cette image.



Exclusion MAP

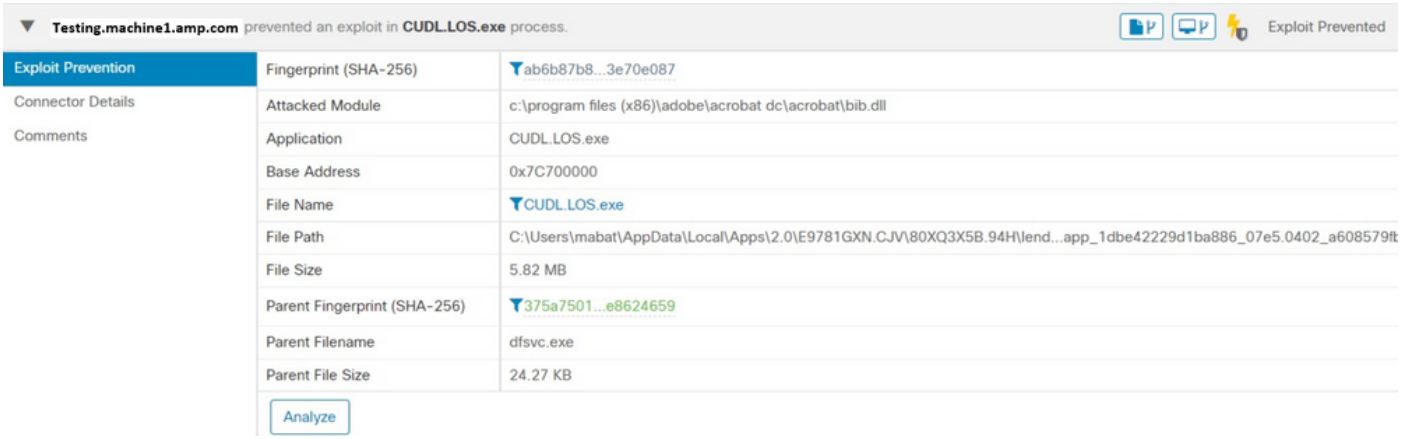


⚠ Attention : utilisez ce type d'exclusion avec précaution et après avoir confirmé que la détection n'est pas malveillante.

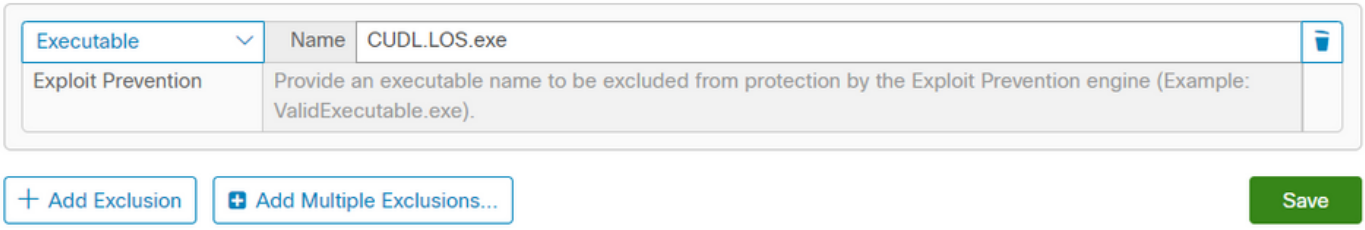
Prévention des exploits (Exprev)

Le moteur de prévention des exploits protège vos terminaux des attaques par injection de mémoire couramment utilisées par les programmes malveillants et d'autres attaques de type « zero-day » sur des logiciels non corrigés
vulnérabilités. Lorsqu'il détecte une attaque contre un processus protégé, il est bloqué et génère un événement, mais il n'y a pas de quarantaine.

Un événement Exprev est affiché dans cette image.



Exclusion Exprev

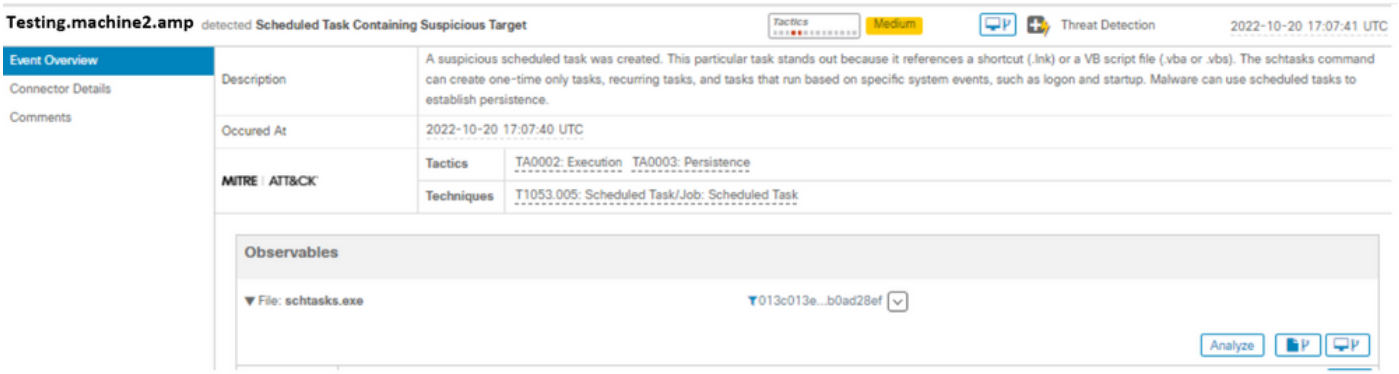


⚠ Attention : utilisez cette exclusion chaque fois que vous approuvez l'activité sur le module/l'application affecté(e).

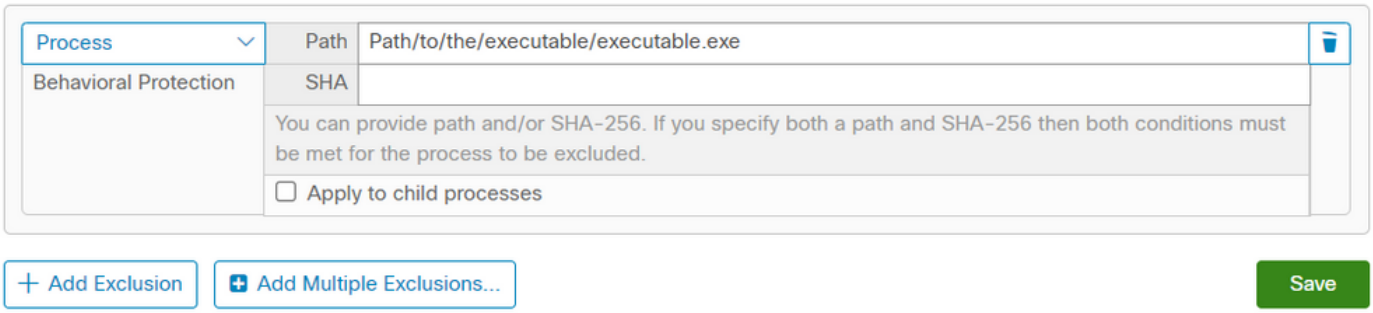
Protection du comportement (BP)

Le moteur de protection comportementale améliore la capacité de détection et d'arrêt comportemental des menaces. Il renforce la capacité à détecter les attaques « hors du pays » et fournit
une réponse plus rapide aux changements dans le paysage des menaces grâce à des mises à jour des signatures.

Un événement BP est illustré dans cette image.



exclusion des points de présence



Informations connexes

- Pour plus d'informations sur la configuration des politiques, accédez au Guide de l'utilisateur
- Créer des exclusions dans la vidéo Cisco Secure Endpoint Connector

- Assistance et documentation techniques - Cisco Systems

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.