

Een eenvoudige aangepaste detectielijst instellen op het Advanced Malware Protection voor endpoints

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Werkstroom](#)

[Configuratie](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft de stappen om een Eenvoudige Aangepaste Detectielijst te maken om specifieke bestanden te detecteren, te blokkeren en in quarantaine te zetten om te voorkomen dat bestanden worden toegestaan op apparaten die de Advanced Malware Protection (AMP) voor endpoints hebben geïnstalleerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Toegang tot het AMP-portaal
- Account met administratorrechten
- Bestandsgrootte maximaal 20 MB

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Advanced Malware Protection voor endpoints, versie 5.4.2019.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Werkstroom

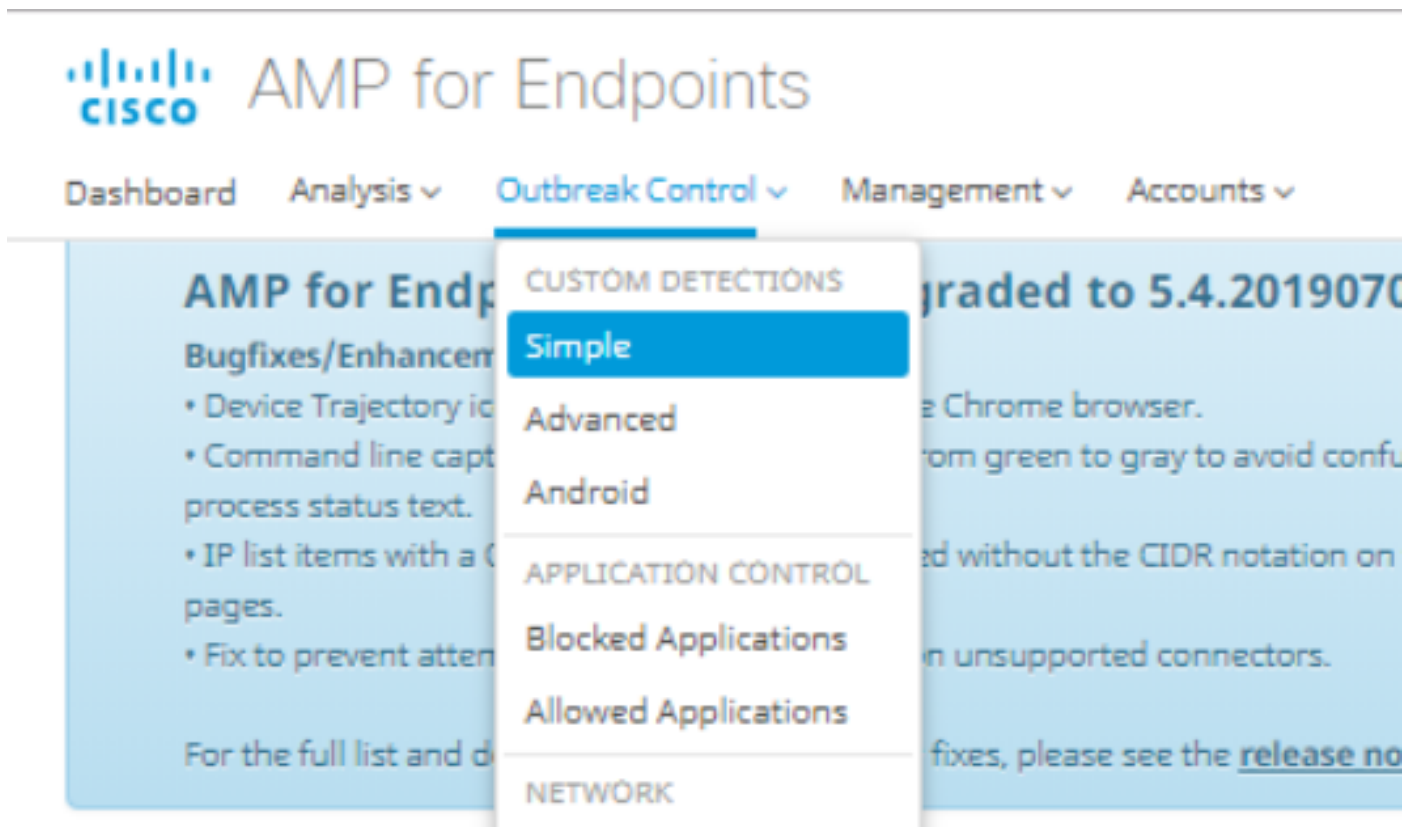
De optie Eenvoudige Aangepaste Detectie gebruikt deze werkstroom:

- De Eenvoudige Aangepaste Detectielijst die uit het AMP-portaal is gemaakt.
- Een eenvoudige lijst met aangepaste detectie die in een eerder gemaakt beleid is toegepast.
- De AMP-connector is op het apparaat geïnstalleerd en wordt in het beleid toegepast.

Configuratie

Om een eenvoudige lijst met aangepaste detectie te maken, volgt u deze stappen:

Stap 1. Ga op het AMP-portal naar **Outdoorkleding, Control > Eenvoudige** optie, zoals in de afbeelding.



Stap 2. Klik op de optie Aangepaste detectie - Eenvoudige optie, klik op knop **maken** om een nieuwe lijst toe te voegen, kies een naam om de lijst Eenvoudige aangepaste detectie te identificeren en op te slaan, zoals in de afbeelding.

Custom Detections - Simple

	<input type="button" value="Create"/>
Name <input type="text" value="Custom_list_1"/>	<input type="button" value="Save"/>
<input type="button" value="«"/> <input type="button" value="<"/> <input type="button" value="1"/> <input type="button" value="2"/> <input type="button" value="3"/> <input type="button" value="4"/> <input type="button" value="5"/> ... <input type="button" value=">"/> <input type="button" value="»"/>	

Stap 3. Klik op de knop **Bewerken** om de lijst met bestanden toe te voegen die u wilt blokkeren, zoals in de afbeelding.

Custom_list_1
0 files Created by Yeraldin Sanchez Mendoza • 2019-07-14 18:33:13 UTC
Not associated with any policy or group
[View Changes](#) Edit Delete

Stap 4. Voor de optie SHA-256 toevoegen, plakt u de SHA-256-code die eerder is verzameld uit het specifieke bestand dat u wilt blokkeren, zoals in de afbeelding.

Custom_list_1 Update Name

Add SHA-256 Upload File Upload Set of SHA-256s

Add a file by entering the SHA-256 of that file

SHA-256

Note

Add

Files included
You have not added any files to this list

Stap 5. Blader in de optie Upload File voor het specifieke bestand dat u wilt blokkeren wanneer het bestand is geüpload, de SHA-256 van dit bestand wordt toegevoegd aan de lijst, zoals in de afbeelding.

Add SHA-256 Upload File Upload Set of SHA-256s

Upload a file to be added to your list (20 MB limit)

File Browse

Note

Upload

Files included

Stap 6. Met de optie Upload Set van SHA-256s kunt u een bestand toevoegen met een lijst met meerdere SHA-256-codes die u eerder hebt aangeschaft, zoals in de afbeeldingen.

SHA256_list.txt - Notepad

File Edit Format View Help

```
85B5F70F84A10FC22271D32B82393EF28CAA55A534F8C08EE3A7DC76139A4DE2  
CEAFF4CD2FDE8B313C52479984E95C0E66A7727313B27516D8F3C70E9F74D71D  
89D599BB4BB64AF353329C1A7D32F1E3FF8C5E0B22D27A4AFEE6A1C3697A0D2A
```

Custom_list_1 Update Name

Add SHA-256 Upload File Upload Set of SHA-256s

Upload a file containing a set of SHA-256s

File SHA256_list.txt Browse

Note This is the SHA256 list to block

Upload

Files included

Stap 7. Zodra de lijst Eenvoudige Eigen detectie is gegenereerd, navigeer dan naar **Beheer > Beleid** en kies het beleid waar u de eerder gemaakte lijst wilt toepassen, zoals in de afbeeldingen.

Dashboard Analysis Outbreak Control Management Accounts

AMP for Endpoints Console

Bugfixes/Enhancement

- Device Trajectory icons now show properly
- Command line capture text has been changed to show process status text.
- IP list items with a CIDR block of /32 are displayed on separate pages.
- Fix to prevent attempting to create a snapshot

For the full list and details of new features and bugfixes, see the release notes.

Quick Start

Computers

Groups

Policies

Exclusions

Download Connector

Deploy Clarity for iOS

Deployment Summary

WIN POLICY LEISANCH			
Modes and Engines		Exclusions	Proxy
Files	Quarantine	leisanch2Excl	Not Configured
Network	Disabled	Microsoft Windows Default	
Malicious Activity Prot...	Disabled	Windows leisanch Policy	
System Process Protec...	Disabled		
Outbreak Control			
Custom Detections - Simple		Custom Detections - Advanced	Application Control
Not Configured		Not Configured	leisanch_blocking2 Blocked
			Network
			Not Configured
View Changes Modified 2019-07-15 20:04:21 UTC Serial Number 12625 Download XML Duplicate Edit Delete			

Stap 8. Klik op de knop **Bewerken** en navigeer naar **Outdoorkleding > Aangepaste Detectie - Eenvoudig**, selecteer de lijst die eerder gegenereerd is in het vervolgkeuzemenu en bewaar de wijzigingen, zoals in de afbeelding.

< Edit Policy

Windows

Name WIN POLICY LEISANCH

Description

Modes and Engines	Custom Detections - Simple	Custom_list_1
Exclusions 3 exclusion sets	Custom Detections - Advanced	None
Proxy	Application Control - Allowed	None
Outbreak Control	Application Control - Blocked	leisanch_blocking2
Product Updates	Network - IP Block & Allow Lists	Clear Select Lists
Advanced Settings	None	

Zodra alle stappen zijn uitgevoerd en de connectors zijn gesynchroniseerd voor de laatste beleidswijzigingen, wordt de Eenvoudige Aangepaste Detectie van kracht.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Waarschuwing: Als een bestand wordt toegevoegd aan een Eenvoudige Eigen Detectielijst, moet de cache tijd verlopen voordat de detectie effect heeft.

Opmerking: Wanneer u een eenvoudige aangepaste detectie toevoegt, is deze onderworpen aan cached. Hoe lang een bestand gecached is, is mede afhankelijk van de beschikbaarheid, zoals in deze lijst wordt weergegeven:

- Bestanden reinigen: 7 dagen
- Onbekende bestanden: 1 uur
- Kwaadaardige bestanden: 1 uur