

Creazione di un elenco avanzato di rilevamento personalizzato in Cisco Secure Endpoint

Sommario

[Introduzione](#)

[Premesse](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Crea elenco di rilevamento personalizzato avanzato](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come creare un Advanced Custom Detection (ACD) in Cisco Secure Endpoint.

Premesse

Talos Intelligence ha pubblicato un BLOG il 14 gennaio 2020 in risposta a Microsoft Patch Tuesday Vulnerability Disclosures.

Aggiornato il 15 gennaio: È stata aggiunta una firma ACD per AMP che può essere utilizzata per rilevare lo sfruttamento di CVE-2020-0601 mediante lo spoofing dei certificati mascherati da autorità di certificazione del codice Microsoft ECC:

<https://blog.talosintelligence.com/2020/01/microsoft-patch-tuesday-jan-2020.html>.

Firma del file trovato nel BLOG TALOS da utilizzare nell'ACD:

- Win.Exploit.CVE_2020_0601:1*:06072A8648CE3D020106*06072A8648CE3D020130
- <https://alln-extcloud-storage.cisco.com/blogs/1/2020/01/CVE-2020-0601.txt>

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

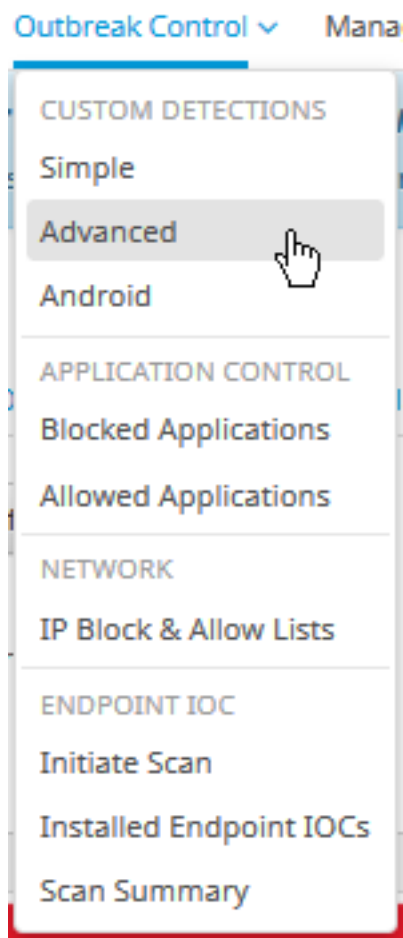
- Cisco Secure Endpoint Cloud Portal
- ACD
- Blog TALOS

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Tutti i dispositivi utilizzati sono stati avviati con una configurazione ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Crea elenco di rilevamento personalizzato avanzato

Ora, creiamo l'ACD per farla corrispondere.

Passaggio 1. Passare a **Secure Endpoint Portal > Outbreak Control > Advanced Custom Detection**, come mostrato nell'immagine.



Passaggio 2. Iniziare con un nome per il set di firme **CVE-2020-0601** come mostrato nell'immagine.

Custom Detections - Advanced

Create Signature Set

Name

Save

Passaggio 3. Quindi, **modificare** il nuovo set di firme e **aggiungere la firma**.
Win.Exploit.CVE_2020_0601:1:*:06072A8648CE3D020106*06072A8648CE3D020130.

Custom Detections - Advanced

[View All Changes](#)

Create Signature Set

CVE-2020-0601 Update Name

Created by Mustafa Shukur • 2020-01-22 12:19:38 CST

Used in policies:

Used in groups:

[View Changes](#) [Download](#) [Edit](#) [Delete](#)

Add Signature Build Database From Signature Set

ndb: Win.Exploit.CVE_2020_0601.UNOFFICIAL

Passaggio 4. Selezionare **Crea database dal set di firme** e il database è stato creato.

Passaggio 5. Applicare il nuovo set di firme a un criterio, fare clic su **Modifica** > **Controllo epidemie** > **Rilevamenti personalizzati** > Avanzate come mostrato nell'immagine.

Modes and Engines

Exclusions
3 exclusion sets

Proxy

Outbreak Control

Product Updates

Advanced Settings

Custom Detections - Simple None

Custom Detections - Advanced CVE-2020-0601
None
CVE-2020-0601

Application Control - Allowed None

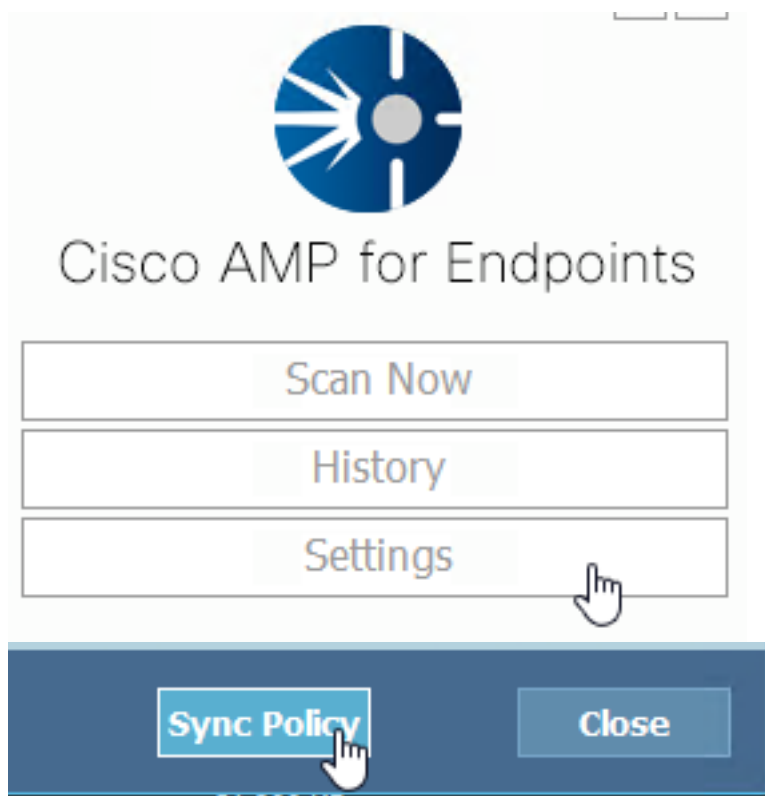
Application Control - Blocked None

Network - IP Block & Allow Lists Clear Select Lists

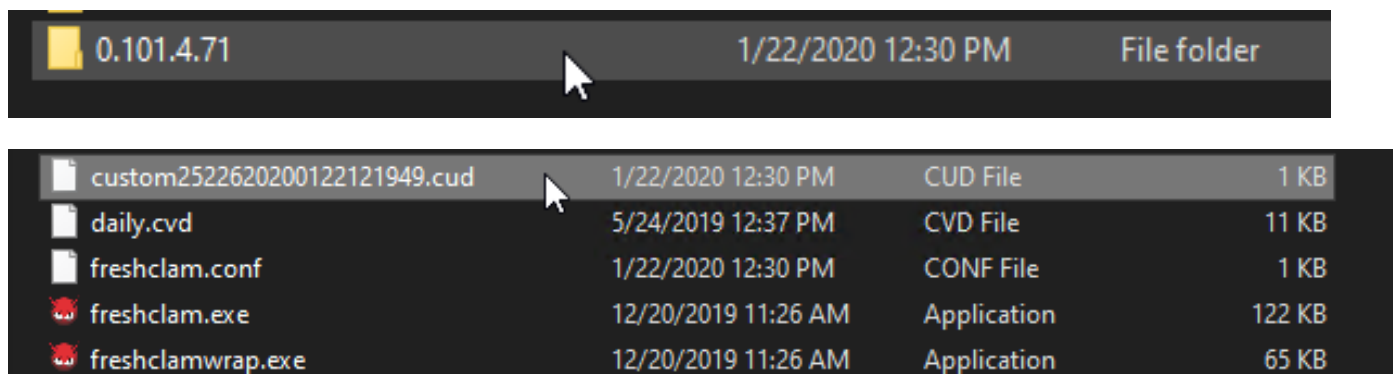
None

Cancel Save

Passaggio 6. Salvare il criterio e sincronizzarlo nell'interfaccia utente del connettore come mostrato nell'immagine.



Passaggio 7. Cercare nella directory **C:\Program Files\Cisco\AMP\ClamAV** una nuova cartella Signature creata quel giorno, come mostrato nell'immagine.



Informazioni correlate

- La build utilizzata per il test è Windows 10 1909, che non è influenzato dalla vulnerabilità secondo MSKB; <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601>
- <https://support.microsoft.com/en-us/help/4534273/windows-10-update-kb4534273>
- Si applica a: Windows 10, versione 1809, Windows Server versione 1809, Windows Server 2019, tutte le versioni
- [Documentazione e supporto tecnico – Cisco Systems](#)