Crear una lista de detección personalizada avanzada en Cisco Secure Endpoint

Contenido

Introducción

Este documento describe los pasos para crear una detección personalizada avanzada (ACD) en Cisco Secure Endpoint.

Antecedentes

TALOS Intelligence publicó un BLOG el 14 de enero de 2020 en respuesta a las revelaciones de vulnerabilidad del martes de parche de Microsoft.

Actualizado el 15 de enero: Se agregó una firma ACD para AMP que se puede utilizar para detectar la explotación de CVE-2020-0601 mediante la suplantación de certificados enmascarados como autoridad de firma de código ECC de Microsoft: https://blog.talosintelligence.com/2020/01/microsoft-patch-tuesday-jan-2020.html.

La firma del archivo que se encuentra en el BLOG TALOS que se utilizará en el ACD:

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

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

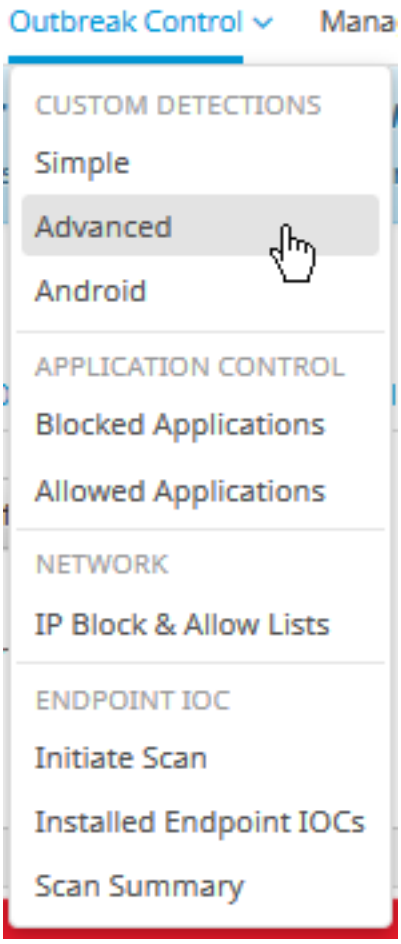
- Portal de nube de Cisco Secure Endpoint
- ACD
- Blog TALOS

La información de este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. Todos los dispositivos utilizados comenzaron con una configuración desactivada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

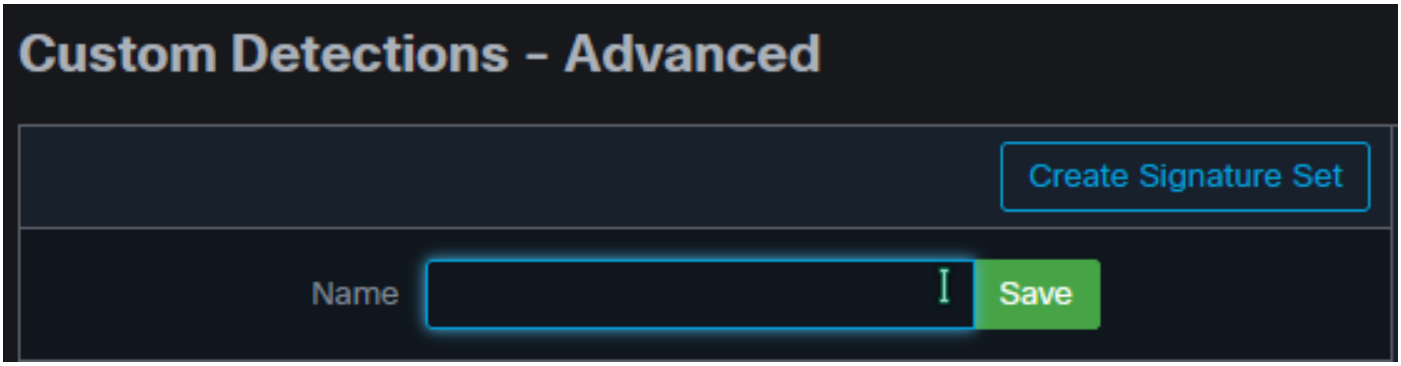
Crear lista de detección personalizada avanzada

Ahora, creemos el ACD para que coincida.

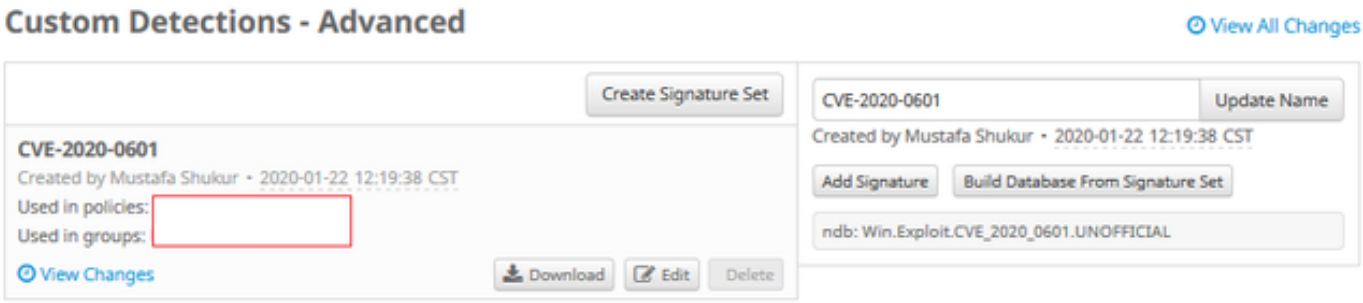
Paso 1. Vaya a **Secure Endpoint Portal > Outbreak Control > Advanced Custom Detection** como se muestra en la imagen.



Paso 2. Comience con un nombre para el conjunto de firmas **CVE-2020-0601** como se muestra en la imagen.

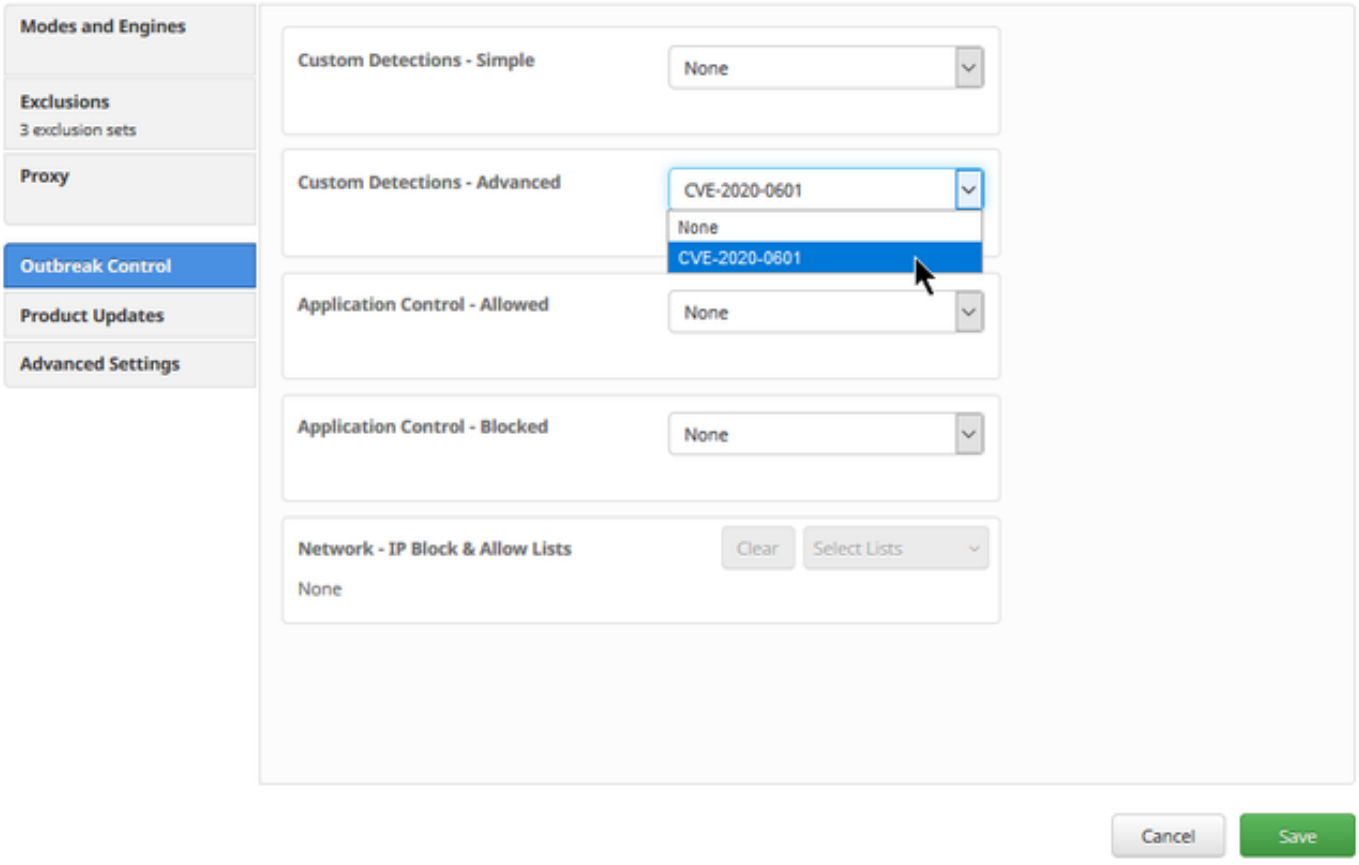


Paso 3. A continuación, **edite** ese nuevo conjunto de firmas y **agregue firma**. **Win.Exploit.CVE_2020_0601:1:*:06072A8648CE3D020106*06072A8648CE3D020130**.

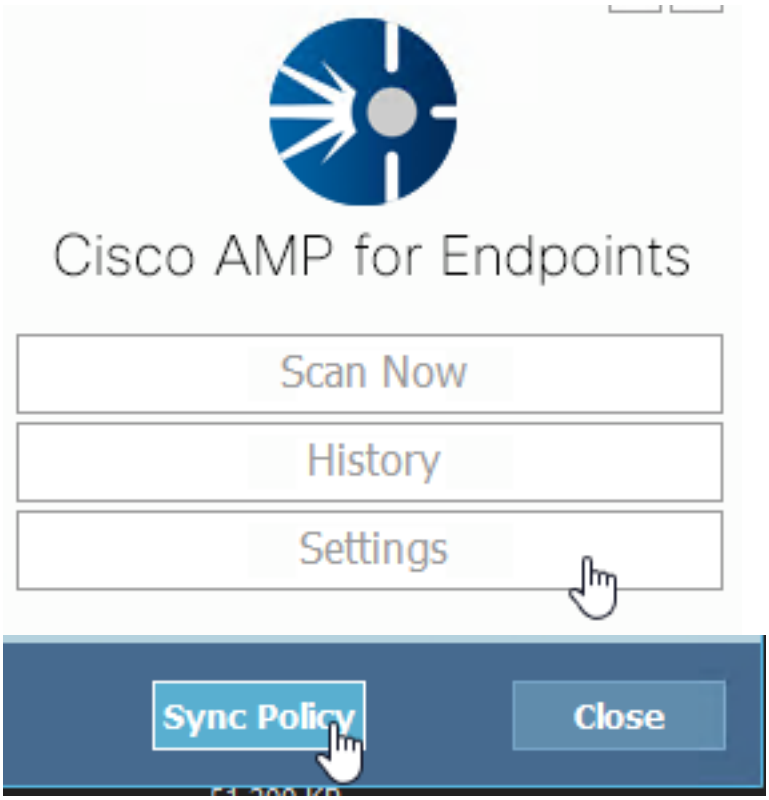


Paso 4. Seleccione **Generar base de datos desde conjunto de firmas** y la base de datos se ha generado.

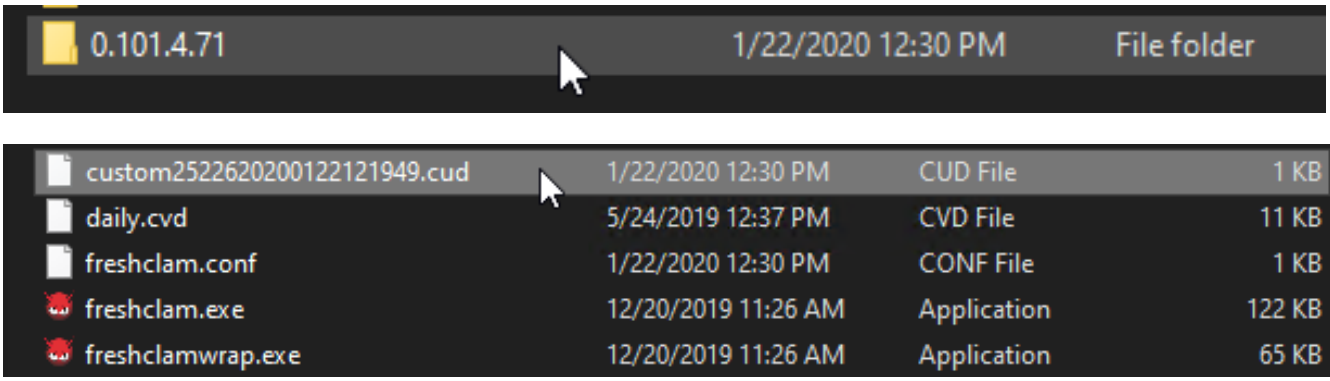
Paso 5. Aplique el nuevo conjunto de firmas a una política, haga clic en **Editar > Control de brotes > Detecciones Personalizadas** > Avanzadas como se muestra en la imagen.



Paso 6. Guarde la política y la sincronización en la interfaz de usuario del conector como se muestra en la imagen.



Paso 7. Busque en el directorio **C:\Program Files\Cisco\AMP\ClamAV** una nueva carpeta Signature creada ese día, como se muestra en la imagen.



Información Relacionada

- La generación utilizada para la prueba es Windows 10 1909, que no se ve afectada por la vulnerabilidad por el 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
- Se aplica a: Windows 10, versión 1809, Windows Server versión 1809, Windows Server 2019, todas las versiones
- **Soporte Técnico y Documentación - Cisco Systems**