Cisco Secure Endpoint에서 고급 맞춤형 탐지 목록 생성

목차

소개

이 문서에서는 Cisco Secure Endpoint에서 ACD(Advanced Custom Detection)를 생성하는 단계에 대해 설명합니다.

배경 정보

TALOS Intelligence는 Microsoft 패치 Tuesday Vulnerability Closure에 대한 응답으로 2020년 1월 14일 BLOG를 게시했습니다.

업데이트 날짜: Microsoft ECC Code Signing Certificate Authority로 가장하는 인증서를 스푸핑하여 CVE-2020-0601의 익스플로잇을 탐지하는 데 사용할 수 있는 AMP용 ACD 시그니처를 추가했습니다. https://blog.talosintelligence.com/2020/01/microsoft-patch-tuesday-jan-2020.html

ACD에서 사용할 TALOS 블로그에 있는 파일의 서명:

- Win.Exploit.CVE_2020_0601:1:*:06072A8648CE3D020106*06072A8648CE3D02020130
- https://alln-extcloud-storage.cisco.com/blogs/1/2020/01/CVE-2020-0601.txt

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure Endpoint Cloud Portal
- ACD

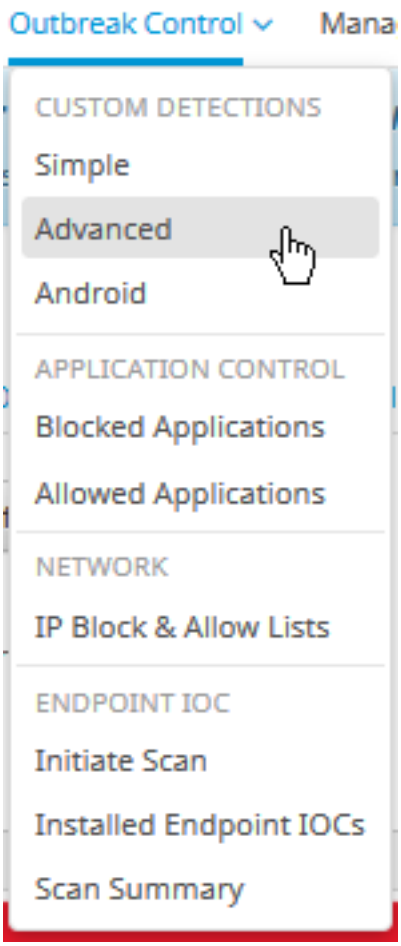
- TALOS 블로그

이 문서의 정보는 특정 랩 환경의 디바이스에서 생성되었습니다. 사용된 모든 장치는 지워진(기본) 구성으로 시작되었습니다. 네트워크가 활성화되어 있는 경우 명령의 잠재적인 영향을 이해해야 합니다.

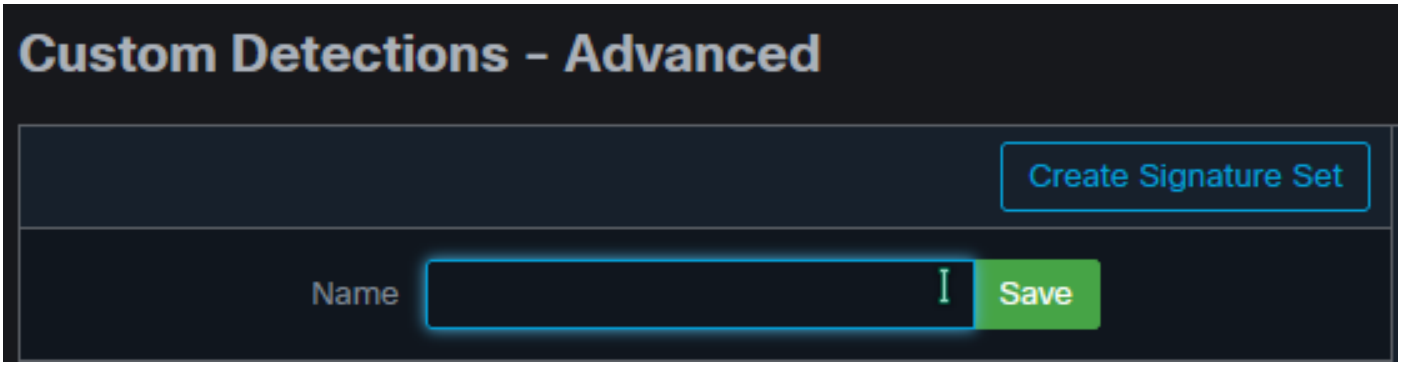
고급 맞춤형 탐지 목록 생성

이제 일치시킬 ACD를 생성하겠습니다.

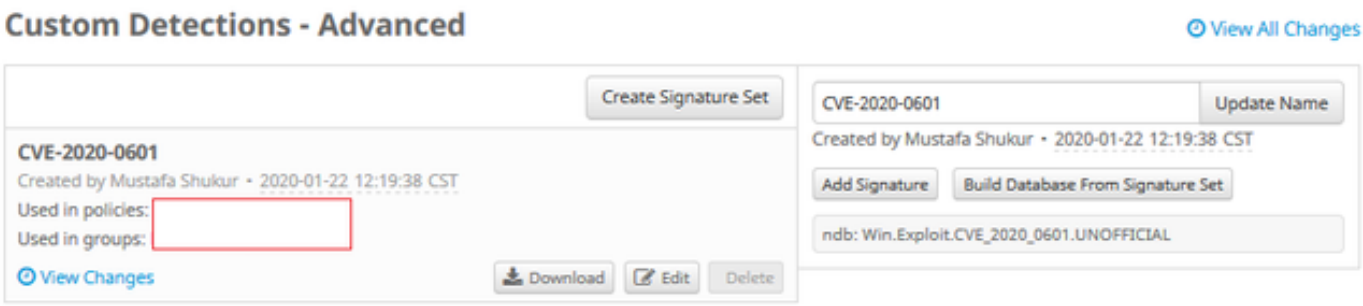
1단계. 이미지에 표시된 대로 **Secure Endpoint Portal > Outbreak Control > Advanced Custom Detection**으로 이동합니다.



2단계. 이미지에 표시된 대로 시그니처 세트 **CVE-2020-0601의 이름**으로 시작합니다.

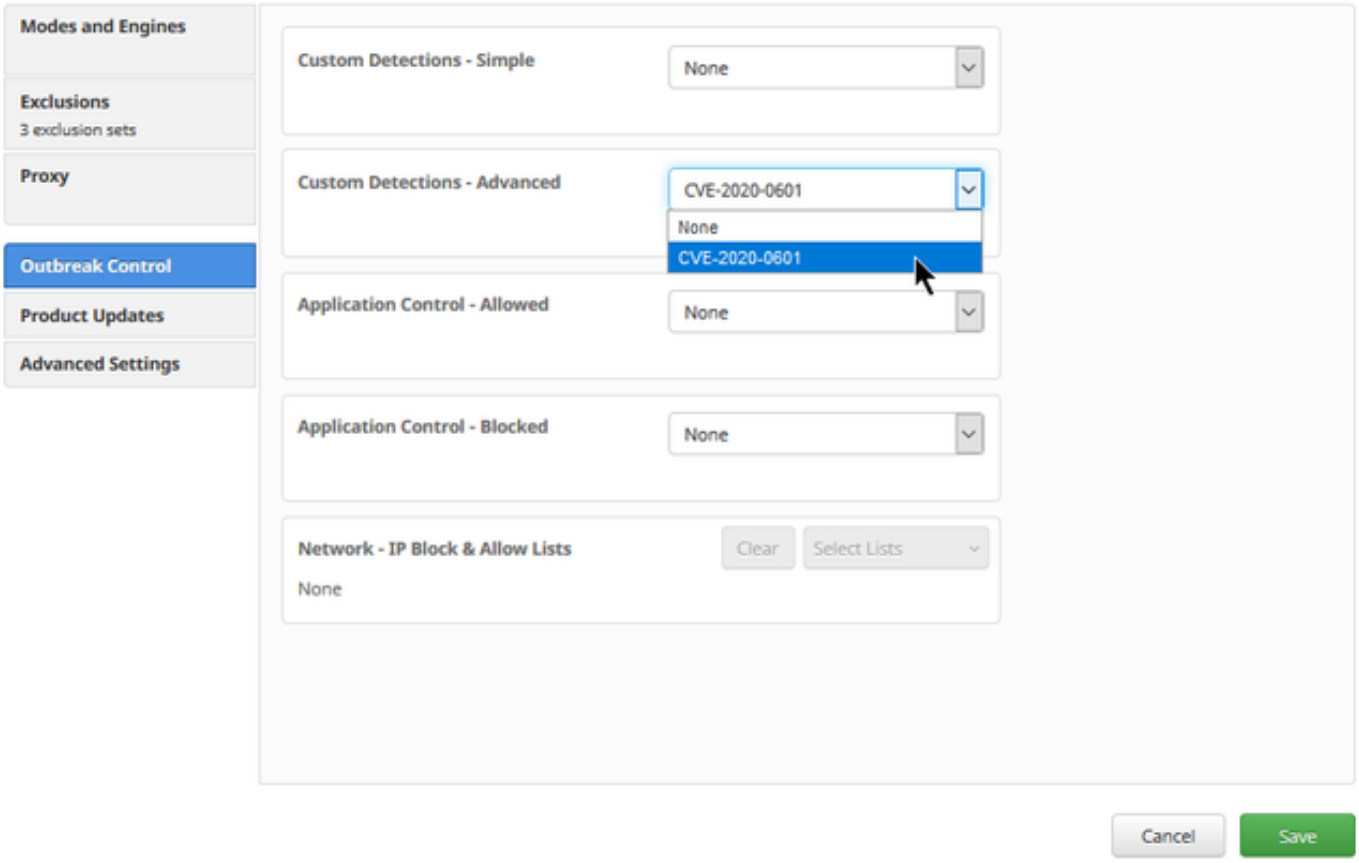


3단계. 그 다음, 새 서명 세트를 편집하고 **서명 추가**.
Win.Exploit.CVE_2020_0601:1:*:06072A8648CE3D020106*06072A8648CE3D02020130.

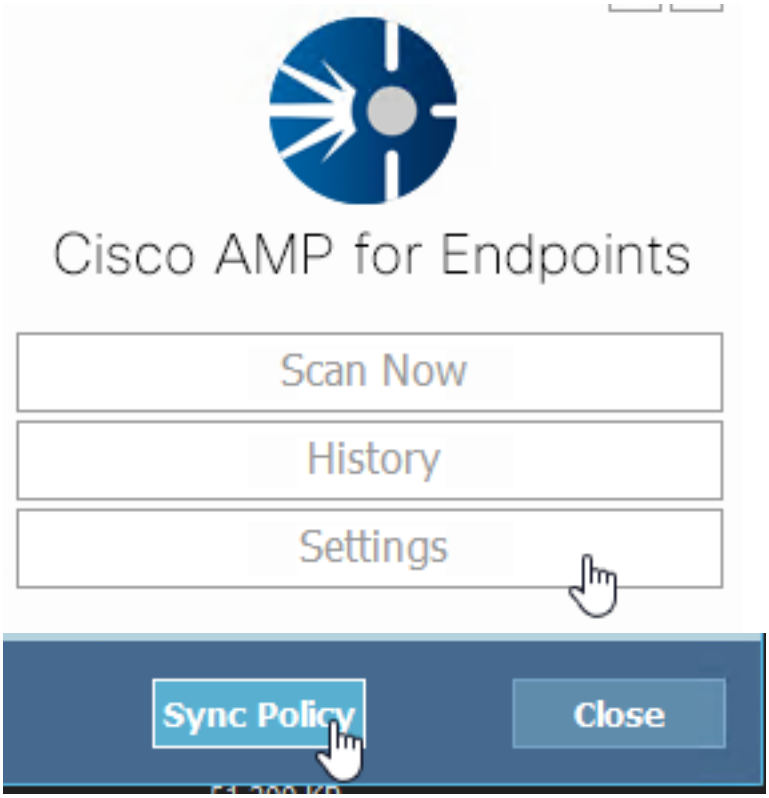


4단계. **시그니처 세트에서 데이터베이스** 빌드를 **선택하고** 데이터베이스가 빌드되었습니다.

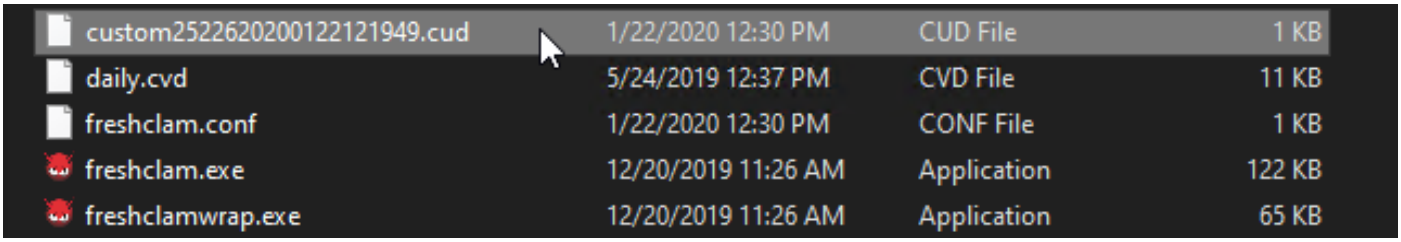
5단계. 새 서명 세트를 정책에 적용하고 이미지에 표시된 대로 **Edit> Outbreak Control > Custom Detections > Advanced**를 클릭합니다.



6단계. 이미지에 표시된 대로 커넥터 UI에 정책 및 동기화를 저장합니다.



7단계. 이미지에 표시된 대로 해당 날짜에 생성된 새 Signature 폴더를 디렉토리에서 검색합니다. C:\Program Files\Cisco\AMP\ClamAV



관련 정보

- 테스트에 사용되는 빌드는 MSKB당 취약성의 영향을 받지 않는 Windows 10 1909입니다. 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
- 적용 대상: Windows 10, 버전 1809, Windows Server 버전 1809, Windows Server 2019, 모든 버전
- **기술 지원 및 문서 – Cisco Systems**