Cisco Secure Endpoints 커버리지 요청 모범 사례

목차

소개

이 문서에서는 이미 식별되었지만 현재 보안 엔드포인트에서 탐지되지 않은 알려진 위협에 대해 Talos 커버리지를 요청할 때 사용해야 하는 프로세스에 대해 설명합니다.

다양한 정보 소스

이러한 위협을 식별하고 게시하는 소스가 여러 개 있을 수 있으며, 일반적으로 사용되는 플랫폼 중 일부는 다음과 같습니다.

- 게시된 Cisco CVE
- 게시된 CVE(일반적인 취약성 및 노출)
- Microsoft 권고
- 3rd Party Threat Intelligence

Cisco는 Talos가 정보를 검토하고 관련 지원 범위를 확인하도록 하기 전에 데이터 소스가 합법적인지 확인하고자 합니다.

해당 위협에 대한 Cisco의 입장 및 지원 범위를 검토하기 위해 새로운 지원 범위 요청을 요청하기 전에 검토해야 하는 다양한 Cisco/Talos 소스가 있습니다.

Cisco 취약성 포털

Cisco 제품과 관련된 CVE에 대해서는 이 포털에서 자세한 내용을 검토하십시오.
https://sec.cloudapps.cisco.com/security/center/publicationListing.x

Talos 포털

Talos Intelligence Portal은 이 위협이 Talos에서 조사를 받았거나 현재 조사 중인지를 검토하기 위한 첫 번째 참조 지점이어야 합니다. https://talosintelligence.com/

Talos 블로그

Cisco Talos 블로그는 Talos가 평가하고 조사한 위협에 대한 정보도 제공합니다.
https://blog.talosintelligence.com/

대부분의 관련 정보는 게시된 모든 "Microsoft Advisories"를 포함한 "Vulnerability Information" 아래에서 찾을 수 있습니다.

Cisco 제품을 사용한 추가 조사

Cisco는 위협 벡터/해시를 검토하고 보안 엔드포인트가 위협에 대한 지원 범위를 제공하는지 확인하는 데 도움이 되는 여러 제품을 제공합니다.

Cisco SecureX Cisco CTR(Threat Response Investigation)

CTR 조사의 일환으로 위협 벡터를 조사할 수 있으며, 자세한 내용은 https://docs.securex.security.cisco.com/Threat-Response-Help/Content/investigate.html에서 확인할 수 있습니다.

Cisco XDR 조사

Cisco XDR은 위협 벡터를 조사할 수 있는 향상된 기능을 제공하며, 기능에 대한 자세한 내용은 https://docs.xdr.security.cisco.com/Content/Investigate/investigate.htm에서 확인할 수 있습니다.

유용한 Cisco 블로그

이전 섹션에서 설명한 기능 중 일부를 살펴보면서 이러한 블로그를 검토하십시오.

https://blogs.cisco.com/tag/relevant-and-extended-detection-with-securex

다음 단계

위 단계를 통해 지원되는 위협 벡터가 없는 경우, TAC 지원 요청을 제출하여 위협에 대한 Talos 지원 범위를 요청할 수 있습니다.

https://www.cisco.com/c/en/us/support/index.html

Coverage Request에 대한 평가 및 조사를 신속하게 수행하기 위해 위협에 대한 다음 정보를 요청합니다.

- 위협 인텔리전스의 소스(CVE/자문/3rd Party Investigation/기술/블로그)
- 연결된 SHA256 해시
- 파일 샘플(사용 가능한 경우)

정보가 제공되면 Talos는 평가를 수행하고 그에 따라 요청을 조사합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.