Umbrella의 잠재적으로 유해한 보안 카테고리 이해

목차

소개

이 문서에서는 Cisco Umbrella의 Potentially Hazard 보안 카테고리에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

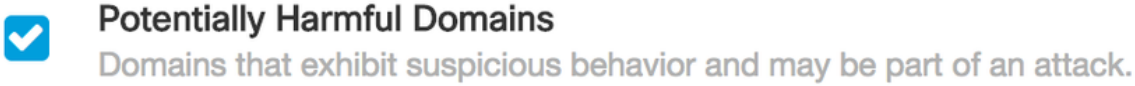
사용되는 구성 요소

이 문서의 정보는 Cisco Umbrella를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

Umbrella 고객은 보안과 관련하여 각기 다른 수준의 위험 허용 수준을 가집니다. 업종과 업무 유형에 따라 잠재적으로 해로운 활동을 사전 예방적으로 모니터링하고 차단하는 것이 유익할 수 있습니다. 새로운 "잠재적으로 유해한" 보안 설정은 다른 보안 설정 옆의 방지에서 찾을 수 있으며 기본적으로 허용으로 설정됩니다.



115011476788

세부사항

Potentially Affect는 악의적일 가능성이 있는 도메인을 포함하는 보안 범주입니다. Umbrella는 악성 코드가 실제로 악성인지 여부에 대해 낮은 신뢰도로 순위를 매겼기 때문에 Umbrella의 "악성코드" 범주와 다릅니다. 이를 표현하는 또 다른 방법은 연구 분석가 및 전반적인 사항을 파악하는 데 사용하는 알고리즘에 따라 이러한 도메인이 의심스러운 것으로 간주되지만 악성으로 확인되지는 않는다는 것입니다.

이 범주의 사용은 잠재적으로 좋은 도메인을 차단하기 위한 위험을 허용하는 데 따라 달라집니다. 고도로 안전한 환경의 경우, 차단하기에 좋은 범주이며, 환경이 더 허술하다면 간단하게 허용하고 모니터링할 수 있습니다.

이러한 항목 중 어느 항목에 해당하는지 확실하지 않은 경우 보고서에서 "Potentially Hazardous"로 확인된 작업을 모니터링할 수 있습니다. 이 카테고리를 사용할 수 있게 되면 트래픽 분류가 한층 세분화되어 가시성이 향상되고 더 강력한 보호 기능을 제공하며 사고 대응을 개선할 수 있습니다. 예를 들어, 어떤 시스템이 악성코드에 감염되었다고 판단되면 해당 시스템이 방문한 잠재적 위험 도메인을 확인하여 보안 침해 수준을 평가하는 데 도움이 될 수 있습니다.

Umbrella는 도메인이 분명히 악의적이지 않지만 위협이 될 수 있음을 나타내는 여러 요소를 따져 "잠재적으로 해로운" 항목을 결정합니다. 예를 들어 다양한 유형의 DNS 터널링 서비스가 있습니다. 이러한 서비스 중 일부는 양성, 악성, DNS 터널링 VPN의 범주에 속하지만 일부는 더 불분명하며 이러한 범주에 속하지 않습니다. 터널링에 대한 활용 사례를 알 수 없고 의심스러운 경우 대상이 Potentially Hazard 범주에 포함될 수 있습니다.

또 다른 예는 Umbrella의 Spike 순위 모델에서 비롯됩니다. Umbrella의 Spike 순위 모델은 방대한 양의 DNS 요청 데이터를 활용하고 음파 그래프를 사용하여 DNS 요청 패턴이 급증하는 도메인을 탐지합니다. Spike 순위 도메인에서 높은 레벨에 도달한 트래픽은 자동으로 악성으로 분류되고 임계값에서 낮은 트래픽은 Potentially Hazard 범주에 속할 수 있습니다.

다음 범주 중 하나에서 원치 않는 탐지를 보고하려면

- 모든 데이터 분류 요청을 Talos 지원을 통해 Cisco Talos에 제출하십시오.
- Cisco Talos에 요청을 제출하는 일반적인 단계는 방법: 분류 요청을 제출합니다.

Potentially Affective 범주의 경우 Umbrella는 도메인이 완전히 합법적임을 보증하지 않고 이 범주를 안전한 것으로 다시 분류하지 않습니다.

두 범주 모두 다른 보안 범주와 마찬가지로 보고서에서 기준으로 필터링할 수 있습니다.

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.