Umbrella 대시보드의 새로운 기능 이해

목차

소개

이 문서에서는 Umbrella Dashboard의 대상 목록을 통한 파일 검사 및 사용자 지정 URL 차단에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Umbrella 대시보드를 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.

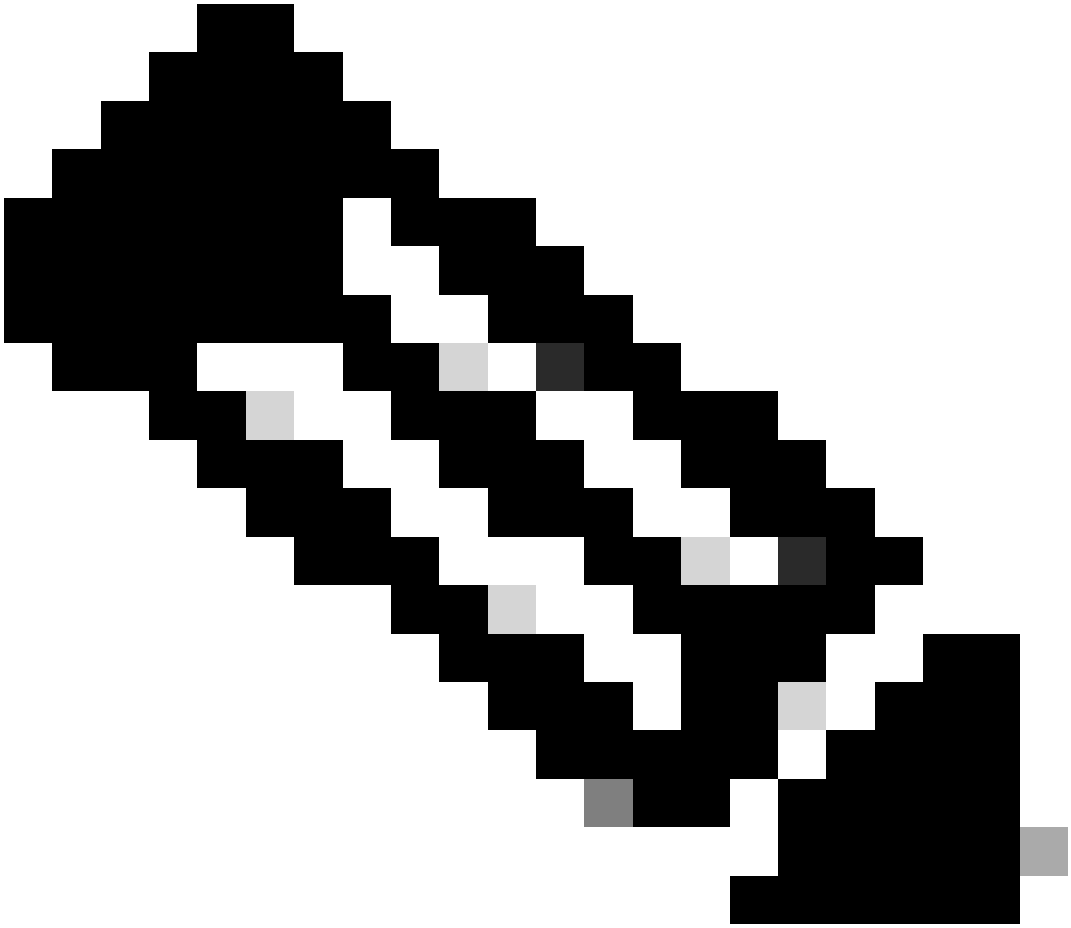
새로운 기능

Umbrella는 기능을 개선하는 새로운 기능 집합을 선보이고 있습니다. 이 변경으로 대시보드에서 두 가지 새로운 기능을 지금 확인할 수 있습니다.

- 파일 검사는 ID가 다운로드한 파일을 검사하여 악성 코드가 포함되어 있는지 확인하고 악성 코드가 포함되어 있으면 차단합니다.
- 사용자 지정 차단 URL을 사용하면 대상 목록에서 고유한 URL 집합을 차단할 수 있습니다. 이

제 전체 도메인을 차단하지 않고 특정 페이지를 차단할 수 있는 유연성을 제공합니다.

이 새로운 기능을 활용할 수 있도록 새롭게 업데이트된 보고서와 새로운 정책 생성 환경을 사용할 수 있습니다. 파일 검사 기능은 Intelligent Proxy 인프라를 발전시켜 더 많은 클라우드 기반 보안을 제공하는 데 중점을 두고 구축된 향후 릴리스에 대해 계획된 여러 가지 기능 중 하나입니다.



참고: 이러한 기능은 고객에게 소폭 증분되어 제공되고 있으며, Umbrella가 이번 릴리스를 진행함에 따라 이러한 업데이트의 가용성이 제한됩니다. 대시보드에서 이러한 기능에 대한 알림을 수신한 경우 해당 알림이 표시됩니다. 이러한 기능에 대해 자세히 알아보려면 umbrella-support@cisco.com으로 문의하십시오.

파일 검사 기능은 Umbrella Insights 또는 Umbrella Platform 패키지를 사용하는 고객에게만 제공됩니다. 패키지에 대한 자세한 내용을 확인하고 궁금한 사항은 Cisco 고객 담당자에게 문의하십시오.

이러한 기능을 활용하는 방법

다음과 같은 몇 가지 장소에서 이러한 새로운 기능에 액세스할 수 있습니다. 정책 마법사를 사용하면 요약 페이지에서 파일 검사를 활성화할 수 있으며, 대상 목록을 통해 차단된 대상 목록에 사용자

지정 URL을 추가할 수 있습니다. 또한 사용자 지정 URL 차단은 Destination Lists(대상 목록) 관리 페이지에서 특별히 관리할 수도 있습니다.

보고 측면에서는 Umbrella 대시보드의 보고서 탐색 섹션이 업데이트되어 새 보고서와 업데이트된 보고서를 쉽게 찾을 수 있습니다. 이러한 기능을 활성화하는 방법에 대한 이 문서에서 자세히 읽고 몇 가지 보고서를 확인하십시오.

파일 검사

파일 검사는 Intelligent Proxy의 기능으로, 의심스러운 도메인에 호스팅된 악성 콘텐츠를 파일을 스캔하는 기능을 추가하여 그 범위와 기능을 확장합니다. 의심스러운 도메인은 신뢰할 수 없거나 악성으로 알려져 있지 않습니다.

Umbrella 정책 마법사를 사용하면 파일 검사를 쉽게 구현할 수 있습니다. Policies(정책) > Policy List(정책 목록)로 이동하고 정책을 확장하거나 +(Add(추가)) 아이콘을 선택하여 새 정책을 생성합니다. 정책 마법사의 요약 페이지에서 파일 검사가 활성화되었는지 확인하거나, Intelligent Proxy를 활성화한 후 새 정책에서 Inspect Files(고급 설정)를 선택합니다. 이 기능에 대한 전체 설명서에서 자세한 내용을 읽어 보십시오.

파일 검사 테스트

File Inspection(파일 검사)이 활성화된 정책에 등록된 디바이스에서:

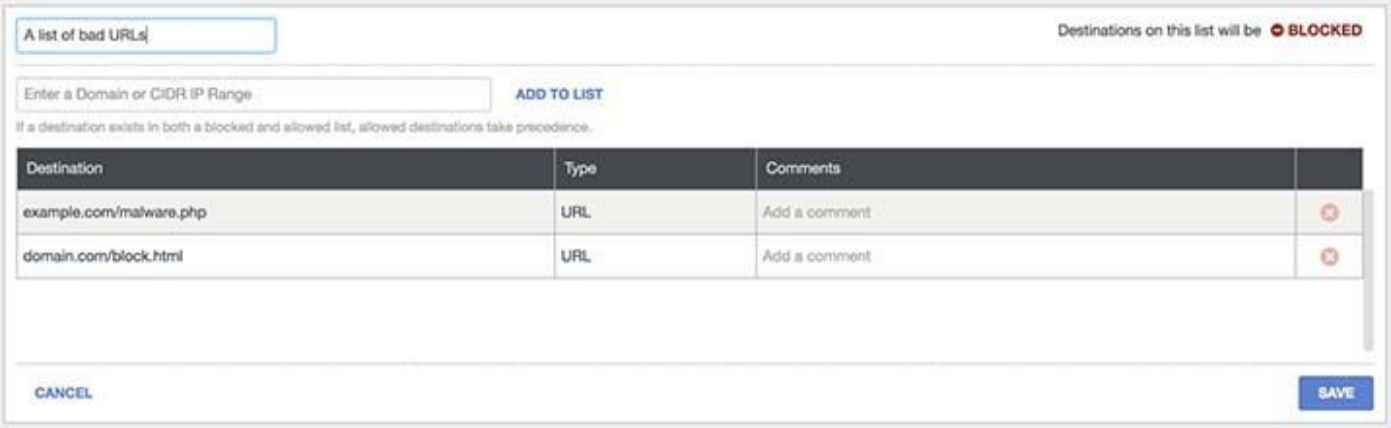
1. http://proxy.opendnstest.com/download/eicar.com으로 이동합니다.

2. 이 스크린샷과 같은 블록 페이지가 나타납니다.

Umbrella 차단 페이지

대상 목록에서 차단할 URL 활성화

URL을 차단하려면 URL을 차단된 대상 목록에 입력하거나 URL에 대해서만 새로운 차단된 대상 목록을 생성하면 됩니다. 이렇게 하려면 Policies(정책) > Destination Lists(대상 목록)로 이동하고, Destination(대상) 목록을 확장하고, URL을 추가한 다음 Save(저장)를 선택합니다.



Umbrella 차단 대상 목록

이 기능에 대한 전체 설명서에서 자세한 내용을 읽어 보십시오.

Umbrella 인프라에서 URL이 차단된 대상 목록에 정의된 것과 일치하는지 확인하기 위해 URL을 검사하려면 다음 항목이 있어야 합니다.

- 지능형 프록시 및 SSL 암호 해독은 정책의 일부로 활성화해야 합니다. 자세한 내용은 Umbrella 문서를 참조하십시오.
- Cisco Umbrella Root CA는 이 정책을 사용하여 컴퓨터에 설치해야 합니다. https 연결도 필터링됩니다. 자세한 내용은 Umbrella 문서를 참조하십시오.

정책에 있는 내용이 사용자가 액세스하려는(그리고 이후에 차단되는) 내용과 일치하도록 URL을 올바르게 지정하는 것이 중요합니다. 사용할 수 있거나 사용할 수 없는 URL에 대한 자세한 내용은 사용자 지정 URL 대상 목록 방법 을 참조하십시오.

보고

이제 Umbrella는 다음과 같은 새로운 향상된 보고서를 제공합니다.

- Security Overview Report(보안 개요 보고서): 차트 및 그래프를 통해 네트워크 활동의 스냅샷을 쉽게 읽을 수 있습니다. ID 및 해당 트래픽의 활동을 빠르게 확인할 수 있으며, 문제가 발생할 수 있는 위치를 파악할 수 있습니다. Umbrella 문서에서 자세한 내용을 알아보십시오.
- Security Activity Report(보안 활동 보고서): Umbrella 위협 인텔리전스에 의해 플래그가 지정되었지만 반드시 차단되지는 않은 보안 이벤트를 강조 표시합니다. 여기에는 인텔리전트 프록시 및 파일 검사를 통해 필터링된 보안 이벤트가 포함됩니다. Umbrella 문서에서 자세한 내용을 알아보십시오.

- 활동 검색 보고서: 다양한 ID의 모든 DNS, URL 및 IP 요청 결과를 내림차순 날짜 및 시간순으로 찾을 수 있도록 도와줍니다. 이 보고서는 선택한 기간 동안 Umbrella 내의 모든 보안 관련 활동을 나열할 수 있으며, 원하는 항목만 표시하도록 필터를 사용하여 검색을 세분화할 수 있습니다. Umbrella 문서에서 자세한 내용을 알아보십시오.

이 보고서들도 쉽게 얻을 수 있습니다.

Umbrella 피드백 보내기

Umbrella는 이러한 새로운 기능에 대한 여러분의 의견을 듣고 싶습니다. 궁금한 사항이나 의견이 있으면 Umbrella에서 귀하에게 알려주십시오! 피드백을 umbrella-support@cisco.com으로 보내 주시고 최대한 자세한 정보를 제공해 주십시오. 예를 들어, 스크린샷, 사용 중인 브라우저, OS 및 이러한 기능을 사용 중인 시나리오 등이 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.