Umbrella 대시보드: 새 기능 및 파일 검사

목차

소개

이 문서에서는 새로운 Umbrella 대시보드에 대해 설명합니다.

Umbrella 대시보드에 대해 다른 점이 있습니까? 자, 우리는 우리가 사람들을 멋진 Umbrella의 새로운 기능 세트로 옮기는 과정을 시작하고 있다는 것을 발표하게 되어 기쁩니다. 첫 번째 소개할 기능은 파일 검사입니다. 파일 검사는 ID가 다운로드한 파일을 검사하여 악성 코드가 포함되어 있는지 확인하고 악성 코드가 포함되어 있으면 차단합니다.

이 새로운 기능을 활용할 수 있도록 새롭게 업데이트된 보안 보고서와 새로운 정책 생성 환경도 공개했습니다. 이 기능은 Intelligent Proxy 인프라를 발전시켜 사용자를 위한 더욱 향상된 클라우드 기반 보안을 제공하는 데 중점을 두고 설계된 향후 릴리스에 대해 계획한 몇 가지 기능 중 하나입니다.

이러한 기능은 고객에게 소폭 확대되고 있습니다. 대시보드에서 이러한 기능에 대한 알림을 받은 경우, 이를 확인할 수 있습니다! 이러한 기능을 조기에 도입하려면 umbrella-support@cisco.com으로 문의하십시오.

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

좋습니다, 파일 검사를 어떻게 활용할 수 있나요?

정책 마법사를 사용하면 요약 페이지에서 또는 새 정책을 만들 때 파일 검사를 활성화할 수 있습니다.

보고 측면에서는 Umbrella 대시보드의 보고서 탐색 섹션이 업데이트되어 새로 업데이트된 보고서를 쉽게 찾을 수 있습니다. 기능을 활성화하고 몇 가지 보고서를 체크 아웃하는 방법을 알아보겠습니다.

파일 검사 활성화

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

성으로 알려져 있지 않으며 Cisco의 '회색 목록'에 나열됩니다.

Umbrella 정책 마법사를 사용하면 파일 검사를 쉽게 구현할 수 있습니다. Policies(정책) > Policy List(정책 목록)로 이동하고 정책을 확장하거나 +(추가) 아이콘을 클릭하여 새 정책을 생성하면 됩니다. 정책 마법사에서 요약 페이지에서 파일 검사가 활성화되었는지 확인하거나, 고급 설정에서 Intelligent Proxy를 활성화한 후 새 정책에서 Inspect Files(파일 검사)를 선택해야 합니다. 이 기능에 대한 전체 설명서는 https://docs.umbrella.com/deployment-umbrella/docs/file-inspection에서 확인할 수 있습니다.

이 기능을 최대한 활용하려면 SSL 암호 해독을 활성화하는 것이 좋습니다.

파일 검사 테스트

File Inspection이 활성화된 정책에 등록된 디바이스에서:

1. http://proxy.opendnstest.com/download/eicar.com으로 이동합니다.
2. 다음과 같은 차단 페이지가 나타납니다.

파일 검사 보고

차단된 항목(뿐만 아니라 언제, 왜, 어떻게)에 대한 더 많은 가시성을 제공하기 위한 일환으로, Umbrella에서는 수정된 보안 활동 보고서를 포함하여 일부 보고서를 업데이트했습니다.

- 보안 개요 보고서
  차트 및 그래프를 통해 네트워크 활동의 스냅샷을 쉽게 읽을 수 있습니다. ID와 해당 트래픽의 진행 상황을 빠르게 파악하여 문제가 발생할 수 있는 위치를 파악할 수 있습니다. 여기서 자세히 알아보십시오.

- 보안 활동 보고서
  Umbrella 위협 인텔리전스에 의해 플래그가 지정된(반드시 차단되어야 하는 것은 아님) 보안 이벤트를 강조 표시합니다. 여기에는 인텔리전트 프록시 및 파일 검사를 통해 필터링된 보안 이벤트가 포함됩니다. 이 보고서는 차단된 항목, 차단 이유 및 차단 방법을 표시하는 데 특히 중요합니다. 여기서 자세히 알아보십시오.

- 활동 검색 보고서
  다양한 ID에서 모든 DNS, URL 및 IP 요청의 결과를 내림차순 날짜 및 시간순으로 찾을 수 있도록 도와줍니다. 이 보고서는 선택한 기간 동안 Umbrella 내의 모든 활동을 나열하며, 필터를 사용하면 원하는 항목만 표시하도록 검색을 세분화할 수 있습니다. 여기서 자세히 알아보십시오.

또한 새로 업데이트된 탐색 기능으로 이 보고서를 쉽게 확인할 수 있습니다! 왼쪽 메뉴 창을 확장하고 대시보드의 다른 위치에서 곧바로 임의의 보고서로 이동합니다.

내 생각을 당신에게 어떻게 알려줘야 하나요?

이러한 새로운 기능에 대한 여러분의 의견을 듣고 싶습니다. 궁금한 점이나 의견이 있으시면 언제든지 문의해 주시기 바랍니다. umbrella-support@cisco.com으로 피드백을 보내 주십시오. 자세한 내용은 최대한 적어 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.