# Umbrella를 사용하여 IPS 오탐 검토 또는 이의 제기

## 목차



## 소개

이 문서에서는 Cisco Umbrella를 사용하여 IPS(Intrusion Prevention Service) 오탐을 검토하거나 이의 제기를 하는 방법에 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

Cisco Umbrella의 Intrusion Prevention System은 알려진 위협, 취약성과 관련된 것으로 간주되는 패킷을 탐지(및 선택적으로 차단)하며, 패킷의 형식이 특이한 경우에도 마찬가지입니다.

관리자는 다음 기본 목록을 기반으로 위협을 탐지하는 데 사용할 IPS 서명 목록을 선택합니다.

- 보안을 통한 연결
- 균형 잡힌 보안 및 연결
- 연결에 대한 보안
- 최대 탐지

선택한 시그니처 목록이 발생한 IPS 오탐의 수에 큰 영향을 미칠 수 있다는 점을 기억해야 합니다. 가장 안전한 모드(예: Maximum Detection 및 Security Over Connectivity)는 보안에 중점을 두기 때문에 원치 않는 IPS 탐지를 생성할 것으로 예상됩니다. 가장 안전한 모드는 전체 보안이 필요한 경우에만 권장되며 관리자는 많은 수의 IPS 이벤트를 모니터링하고 검토할 필요성을 예상해야 합니다.

다른 모드에 대한 자세한 내용은 IPS 설명서를 참조하십시오.

## IPS 탐지 검토

Umbrella Dashboard(Umbrella 대시보드)의 Activity Search(활동 검색)를 사용하여 IPS 이벤트를 볼 수 있습니다. 각 이벤트에는 두 가지 중요한 정보가 있습니다.

- IPS 서명 ID/범주/이름 https://snort.org에서 검색 가능
- CVE 번호(해당되는 경우). https://www.cve.org/에서 검색 가능

모든 IPS 탐지가 알려진 익스플로잇/공격을 나타내는 것은 아닙니다. 대부분의 시그니처(특히 Max Detection(최대 탐지) 모드)는 특정 유형의 트래픽 또는 프로토콜 위반이 있음을 나타냅니다. 이벤트에 대한 다른 세부 정보(예: 소스/대상)와 함께 앞서 언급한 정보의 소스를 검토하여 보안 팀의 추가 조사가 필요한지 여부를 확인하는 것이 중요합니다.

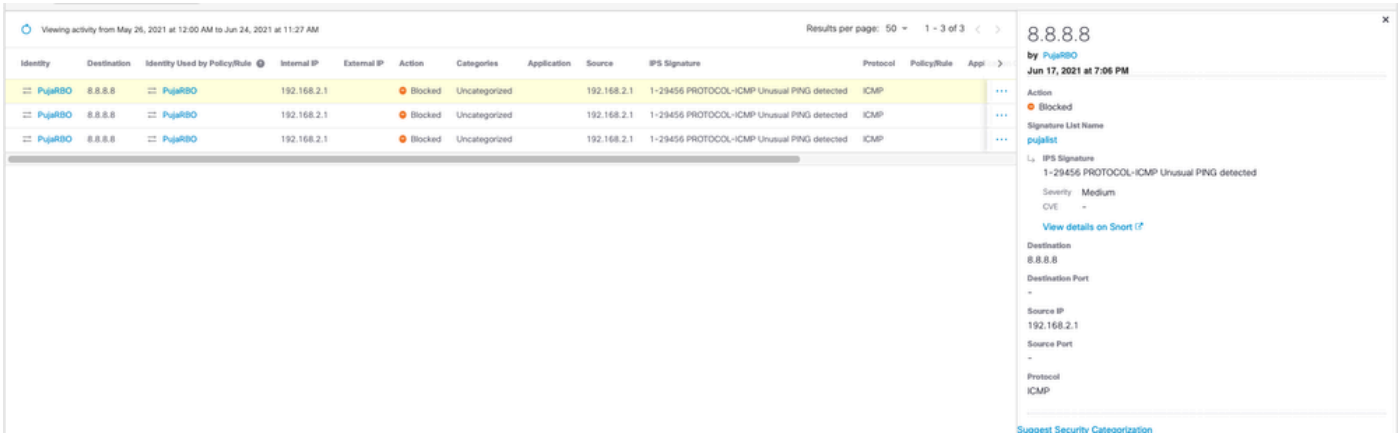
시그니처 카테고리는 IPS 탐지 유형에 대한 추가 컨텍스트를 제공하는 데 유용할 수 있습니다. snort.org에서 사용 가능한 카테고리를 검토합니다.

## 프로토콜 위반

이 예에서는 IPS 이벤트가 이 서명에 연결됩니다.
https://www.snort.org/rule_docs/1-29456

서명의 설명은 다음과 같습니다.

"규칙은 네트워크에 들어오는 PING 트래픽이 일반적인 PING 형식을 따르지 않는 경우를 찾습니다."




4403885889428

이 경우 Snort 규칙은 반드시 특정 익스플로잇을 탐지하는 것이 아니라, 대신 차단된 잘못된 형식의 ICMP 패킷을 탐지합니다. 관리자는 snort.org에서 제공되는 정보 및 이벤트에 대한 기타 세부사항(예: 소스/대상)을 기반으로 이 이벤트에 대해 추가 조사가 필요하지 않음을 결정할 수 있습니다

## 애플리케이션 호환성

일부 합법적인 애플리케이션은 IPS 시그니처와 호환되지 않습니다. 특히 좀 더 적극적인(최대 탐지) 모드가 구성된 경우 더욱 그렇습니다. 이러한 시나리오에서는 프로토콜 위반 섹션에서 설명한 이유로 애플리케이션을 차단할 수 있습니다. 애플리케이션은 예기치 않은 방식으로 프로토콜을 사용하거나 일반적으로 다른 트래픽용으로 예약된 포트를 통해 사용자 지정 프로토콜을 사용할 수 있습니다.

애플리케이션이 합법적이지만 이러한 탐지는 유효한 경우가 많으며 Cisco에서 항상 수정할 수는 없습니다.

합법적인 애플리케이션이 IPS에 의해 차단된 경우, Umbrella는 애플리케이션의 공급업체에 이벤트/시그니처의 세부 정보를 문의할 것을 권장합니다. 타사 애플리케이션의 IPS 시그니처와의 호환성을 snort.org에서 테스트해야 합니다.

현재 IPS 검사에서 개별 애플리케이션/대상을 제외할 수 없습니다.

## IPS 서명 비활성화

서명의 경우 서드파티 애플리케이션과의 호환성 문제가 발생하는 경우, 해당 서명은 일시적으로 또는 영구적으로 비활성화될 수 있습니다. 이는 애플리케이션을 신뢰하고 애플리케이션의 가치가 특정 서명의 보안 이점을 능가한다고 판단한 경우에만 수행해야 합니다.

사용자 지정 서명 목록 생성에 대한 자세한 내용은 Add a Custom Signature List 설명서의 단계를 완료합니다. 현재 설정을 템플릿으로 사용한 다음 Log Only 또는 Ignore로 설정하여 원하는 규칙을 비활성화할 수 있습니다.

## 지원

## 기록 이벤트

Umbrella Support에서는 내역 IPS 이벤트에 대한 추가 세부 정보를 제공할 수 없습니다. IPS Events(IPS 이벤트)는 트래픽이 IPS 시그니처와 일치하지 않음을 알려줍니다. 서명에 대한 자세한 내용은 snort.org을 참조하십시오. Umbrella는 원시 트래픽/패킷의 복사본을 저장하지 않으므로 IPS 이벤트의 특성에 대한 추가 컨텍스트 또는 확인을 제공할 수 없습니다.

## IPS 문제/오탐

현재 IPS 문제(예: False Positive)에 대해 논쟁하려면 Umbrella Support에 문의하십시오.

이러한 문제를 조사하려면 Umbrella Support에서 패킷 캡처를 수행해야 합니다. 트래픽에서 IPS 탐지를 트리거한 방법을 결정하려면 패킷의 원시 내용이 필요합니다. 패킷 캡처를 생성하려면 문제를 복제할 수 있어야 합니다.

티켓을 올리기 전에 Wireshark와 같은 툴을 사용하여 문제를 복제할 때 패킷 캡처를 생성합니다. 지침은 당사의 지식 기반에 나와 있습니다.

또는 Umbrella Support에서 패킷 캡처 생성을 지원할 수 있습니다. 영향을 받는 사용자 또는 애플리케이션에 문제가 다시 발생할 수 있는 시간을 예약해야 합니다.

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.