위협 조사

위협 연구는 위협 및 악성 활동을 탐지하기 위해 검사 엔진에 적용되는 규칙 집합에서 생성됩니다. 이 페이지에서 이러한 규칙을 볼 수 있습니다. 하루에 한 번 멀티 클라우드 방어는 네트워크 침입에 대해 새롭거나 수정된 규칙을 검색하고, 내부 라이브러리에 규칙 및 알려진 악성 소스를 포함하거나 제거합니다. 이 작업은 자동화되어 있습니다. 이 기능에는 새 IP 주소 목록을 소스로 다운로드 및 검증하여 이를 새 규칙 집합에서 구현하는 작업이 포함됩니다. 그런 다음 이러한 규칙 집합이 구축됩니다.

규칙은 정책, 클래스, 애플리케이션, 규칙 집합 라이브러리 날짜 및 기타 매개변수 등 다양한 방식으로 구성됩니다. 트립된 규칙(예: 위협 또는 악성 활동 감지)에 대해 자세히 알고 싶은 경우 **Threat Research(**위협 조사**)** 페이지에서 규칙에 대한 자세한 내용을 확인하십시오. 각 페이지의 다음 부분을 사용할 수 있습니다.

검색 창

창 상단의 검색 창을 사용하면 위협 조사에서 각 페이지에서 알려진 IP 주소, 동작, 규칙 이름, 게이트웨이 이름, 공격 유형 또는 프로파일 이름과 같은 특정 식별 요소를 검색할 수 있습니다. 스크롤하여 특정 필드 값을 찾는 경우 **Add to Search(**검색에 추가**)**를 사용하여 더 쉽게 검색할 수 있습니다.

검색은 각 페이지로 분리되어 있으며, 서로 다른 유형의 위협 조사를 교차 검색할 수 없습니다. 자세한 내용은 아래 참조하십시오.

세부사항 보기

위협 조사 중인 각 측면은 단일 인시던트 또는 공격의 세부 정보 보기 기능을 제공합니다. 이러한 세부 사항에서 제공되는 값은 위협 조사 유형에 따라 다르지만 정책, 보안 프로파일, 규칙 또는 규칙 집합을 세부적으로 조정하려는 경우 유용할 수 있습니다.

검색에 추가

여기에서 사용 가능한 모든 조사 유형의 경우, 행 내의 값 하나를 클릭하면 **Add to Search(**검색에 추가) 옵션을 자동으로 포함할 수 있습니다. 이렇게 하면 선택한 값이 창 상단의 검색창에 자동으로 적용되고 검색창의 콘텐츠에 맞게 보기 창이 필터링됩니다. 이 작업은 여러 번 수행할 수 있으며 선택한 값이 복잡한 검색 요청과 결합합니다.

- 네트워크 침입, 2 페이지
- 웹 보호, 2 페이지

• 악성 소스, 3 페이지

네트워크 침입

네트워크 침입은 네트워크에서의 무단 활동을 의미합니다. 이 표에는 IDS/IPS 엔진에 기본 제공되는 규칙 또는 이러한 규칙의 계열사 정보는 포함되지 않습니다. 이러한 규칙은 탐지 전용으로 지정됩니다. IDS/IPS 규칙의 나머지 부분은 다양한 침입 또는 공격 레벨에 따라 보호하고 작업을 수행하도록 설정됩니다.

Network Intrusion(네트워크 침입) 페이지에 다음 정보가 표시됩니다.

- **Gateway Names(**게이트웨이 이름**)** - 악성 소스를 처리한 영향을 받은 게이트웨이의 이름.
- **Profile Names(**프로파일 이름**)**- 악의적인 소스에 의해 트리거된 보안 프로파일의 이름.
- **IPS** 정책 - 이벤트 또는 공격에 의해 트리거된 멀티 클라우드 방어 내의 정책.
- **IPS** 클래스 - 공격 신호의 데이터베이스에 의해 결정된 공격 유형을 비교.
- **IPS** 범주 - 이벤트 또는 공격에 의해 트리거된 IPS 서명 범주.
- 규칙 **ID** - 멀티 클라우드 방어 내에 내부적으로 문서화된 이벤트 또는 공격에 의해 트리거된 규칙 ID.
- 영향을 받은 서비스 - 이벤트 또는 공격의 영향을 받는 웹 서비스의 유형.
- 영향 - 이벤트 또는 공격에 의한 영향의 심각도 수준(알려졌거나 가정).
- 메시지 - 공격으로 식별된 이벤트의 내용.
- 규칙 콘텐츠 - 이벤트 또는 공격에 의해 트리거된 규칙의 콘텐츠.
- **CVSS** 점수 - CVSS(Common Vulnerability Scoring System)는 정보 보안 취약점의 심각도에 숫자 점수를 할당하는 체계. CVSS 점수의 범위는 0~10이며, 10이 가장 심각합니다.
- **CVE** - CVE(Common Vulnerabilities and Exposures)는 취약점을 분류하는 용어집. 공격 또는 이벤트의 유형과 관련된 CVE가 있으면 내부 라이브러리가 자동으로 여기에서 값을 생성합니다.
- 참조 - 공개적으로 사용할 수 있는 경우 이 링크는 CVE의 원래 공지 사항 및 분류로 이동합니다.

웹 보호

WAF(Web Application Firewall) 연구는 "Web Protection(웹 보호)"으로 표시됩니다. 이를 통해 웹 위협으로부터 디바이스를 보호하고 원치 않는 콘텐츠를 규제할 수 있습니다. Web Protection(웹 보호) 페이지에 다음 정보가 표시됩니다.

- **Gateway Names(**게이트웨이 이름**)** - 악성 소스를 처리한 영향을 받은 게이트웨이의 이름.
- **Profile Names(**프로파일 이름**)**- 악의적인 소스에 의해 트리거된 보안 프로파일의 이름.
- **CRS Category(CRS** 범주**)** - 일반 공격 탐지 규칙 집합당 식별된 CRS(Core Rule Set) 범주.

- **Inspection Type(**검사 유형**)** - 공격 또는 이벤트를 캡슐화한 트래픽에서 수행한 검사 멀티 클라우드 방어.
- **Attack Type(**공격 유형**)** - 네트워크를 통해 이루어지는 무단 공격의 유형입니다.
- **Platform(**플랫폼**)** - 공격 또는 이벤트에서 식별된 플랫폼 유형.
- **Lanuage(**언어**)** - 이벤트에서 탐지된 명시된 웹 개발 언어.

악성 소스

악성 소스는 네트워크에 피해를 주는 모든 유형의 코드 또는 패킷입니다. Malicious Sources(악성 소스) 페이지에는 다음 정보가 표시됩니다.

- **Gateway Names(**게이트웨이 이름**)** - 악성 소스를 처리한 영향을 받은 게이트웨이의 이름.
- **Profile Names(**프로파일 이름**)** - 악의적인 소스에 의해 트리거된 보안 프로파일의 이름.
- **Malicious Sources Action(**악성 소스 작업**)** - 악성 소스가 식별되었을 때 수행된 작업.
- **Impact(**영향**)** - 라이브러리 내에서 순위가 매겨진 방식에 따라 결정된 악성 자료의 영향.
- **Malicious Source IP(**악성 소스 **IP)** - 악성 소스가 시작된 IP 주소.