규칙을 사용하여 침입 정책 조정

이 장에서는 Snort 3의 사용자 지정 규칙, 침입 규칙 작업, 침입 정책의 침입 이벤트 알림 필터, Snort 2 사용자 지정 규칙을 Snort 3로 변환, 침입 정책에 사용자 지정 규칙이 있는 규칙 그룹 추가에 대한 정보를 제공합니다.

침입 규칙 조정 개요

공유 개체 규칙, 표준 텍스트 규칙, 검사기 규칙의 규칙 상태 및 기타 설정을 구성할 수 있습니다.

규칙 상태를 Alert(알림) 또는 Block(차단)으로 설정하여 규칙을 활성화할 수 있습니다. 규칙을 활성화하면 시스템은 규칙과 일치하는 트래픽에 대해 이벤트를 생성합니다. 규칙을 비활성화하면 규칙 처리가 중지됩니다. Block(차단)으로 설정된 규칙이 일치하는 트래픽에 대해 이벤트를 생성하거나 해당 트래픽을 삭제하도록 침입 정책을 설정할 수도 있습니다.

하위 집합을 표시하도록 규칙을 필터링하면 규칙 상태 또는 규칙 설정을 변경하고자 하는 정확한 규칙 집합을 선택할 수 있습니다.

침입 규칙 또는 규칙 인수를 사용하려면 비활성화된 검사기가 필요한 경우 네트워크 분석 정책 웹 인터페이스에서 비활성화 상태로 남아 있다고 해도 시스템은 자동으로 검사기를 현재 구성으로 사용한다는 점에 유의하십시오.

침입 규칙 유형

침입 규칙은 시스템이 네트워크에서 취약점을 익스플로잇하려는 시도를 탐지하는 데 사용하는 키워드와 인수의 지정된 집합입니다. 시스템에서 네트워크 트래픽을 분석하면서 각 규칙에 지정된 조건과 패킷을 비교하고 데이터 패킷이 규칙에 지정된 모든 조건을 충족하는 경우 규칙을 트리거합니다.

칩입 정책에는 다음이 포함됩니다.

- 침입 규칙(공유 개체 규칙 및 표준 텍스트 규칙으로 세분화됨)
- 패킷 디코더의 탐지 옵션 또는 시스템에 포함된 검사기 중 하나와 연결된 검사기 규칙

다음 표에는 이러한 규칙 유형의 속성이 요약되어 있습니다.

표 *1:* 침입 규칙 유형

유형	**GID(generator ID)**	**SID(Snort ID)**	소스	복사 가능 여부	편집 가능 여부
공유 객체 규칙	3	1000000 미만	Cisco Talos(Talos Intelligence Group)	예	제한적
표준 텍스트 규칙	1 (전역 도메인 또는 레거시 GID)	1000000 미만	Talos	예	제한적
	1000 - 2000 (하위 도메인)	1000000 이상	사용자가 생성하거나 가져옴	예	예
전처리기 규칙	디코더 또는 전처리기별	1000000 미만	Talos	아니요	아니요
		1000000 이상	옵션 구성 중 시스템에서 생성	아니요	아니요

Talos에서 생성한 규칙의 변경 사항은 저장할 수 없지만 사용자 지정 규칙으로 수정된 규칙의 복사본은 저장할 수 있습니다. 규칙 또는 규칙 헤더 정보(예: 소스 및 대상 포트와 IP 주소)에 사용되는 변수 중 하나를 수정할 수 있습니다. 다중 도메인 구축에서 Talos에 의해 생성된 규칙은 전역 도메인에 속합니다. 하위 도메인의 관리자는 규칙의 로컬 복사본을 저장한 다음 편집할 수 있습니다.

Talos는 생성하는 규칙마다 각 기본 침입 정책에서 기본 규칙 상태를 할당합니다. 대부분의 전처리기 규칙은 기본적으로 비활성화되어 있으며, 시스템에서 전처리기 규칙을 위한 이벤트를 생성하고 인라인 구축에서 문제가 되는 패킷을 삭제하도록 하려면 활성화해야 합니다.

네트워크 분석 및 침입 정책 사전 요건

Snort 검사기 엔진이 침입 및 악성코드 분석을 위해 트래픽을 처리하도록 허용하려면 Threat Defense 디바이스에 대해 활성화된 IPS 라이선스가 있어야 합니다.

네트워크 분석, 침입 정책을 관리하고 마이그레이션 작업을 수행하려면 관리자 사용자여야 합니다.

Snort 3의 사용자 지정 규칙

로컬 규칙 파일을 가져와서 사용자 지정 침입 규칙을 생성할 수 있습니다. 규칙 파일은 확장자가 `.txt` 또는 `.rules`일 수 있습니다. 시스템은 규칙 생성에 사용된 방법에 상관없이 맞춤형 규칙을 로컬 규칙 카테고리에 저장합니다. 사용자 지정 규칙은 규칙 그룹에 속해야 합니다. 그런데 한 사용자 지정 규칙이 둘 이상의 그룹에 속할 수도 있습니다.

맞춤형 침입 규칙을 만들 때 시스템은 `GID: SID: Rev`형식의 고유한 규칙 번호를 규칙에 할당합니다. 이 번호의 요소는 다음과 같습니다.

- **GID** - Generator ID입니다. 사용자 지정 규칙의 경우 GID를 지정할 필요가 없습니다. 규칙을 업로드하는 동안 전역 도메인에 있는지 하위 도메인에 있는지에 따라 시스템이 GID를 자동으로 생성합니다. 모든 표준 텍스트 규칙의 경우, 전역 도메인에 있을 때 이 값은 2000입니다.
- **SID** - Snort ID입니다. 규칙이 시스템 규칙의 로컬 규칙인지 여부를 나타냅니다. 새 규칙을 생성할 때 고유한 SID를 규칙에 할당합니다.

  로컬 규칙의 SID 번호는 1000000에서 시작하며 각 새 로컬 규칙의 SID는 1씩 증가합니다.
- **Rev** - 수정 번호입니다. 새 규칙의 경우, 수정 번호는 1입니다. 사용자 지정 규칙을 변경할 때마다 수정 번호가 하나씩 증가합니다.

맞춤형 표준 텍스트 규칙에서 헤더 설정과 규칙 키워드 및 인수를 설정합니다. 규칙 헤더 설정을 사용하면 특정 프로토콜을 사용하며 특정 IP 주소 또는 포트를 오가는 트래픽만을 매칭하도록 규칙의 범위를 좁힐 수 있습니다.

참고

- Snort 3 사용자 지정 규칙은 수정할 수 없습니다. 사용자 지정 규칙의 규칙 텍스트 내 `classtype`에 유효한 분류 메시지가 있는지 확인하십시오. 분류를 사용하지 않거나 잘못된 분류를 사용하여 규칙을 가져온 경우 해당 규칙을 삭제하고 다시 생성합니다.
- Snort 3을 사용하여 사용자 지정 침입 규칙을 생성할 수 있습니다. 그러나 이러한 규칙 조정 및 문제 해결은 현재 제공되지 않습니다.

침입 정책의 Snort 3 침입 규칙 보기

침입 정책에서 규칙이 표시되는 방법을 조정할 수 있습니다. 또한 규칙 설정, 규칙 문서 및 기타 규칙 사양을 보려면 특정 규칙에 대한 세부 사항을 표시할 수 있습니다.

단계 1 **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

단계 2 정책 옆의 **Snort 3 Version(Snort 3** 버전**)**을 클릭합니다.

단계 3 규칙을 보면서 다음을 수행할 수 있습니다.

- 규칙 필터링
- 규칙 그룹을 선택하여 해당 그룹과 관련된 규칙 확인
- 침입 규칙의 세부 사항 보기
- 규칙 코멘트 보기
- 규칙 문서 보기

이러한 작업 수행에 대한 자세한 내용은 Snort 3 침입 정책 편집를 참조하십시오.

침입 규칙 작업

침입 규칙 작업을 통해 개별 침입 정책 내에서 규칙을 활성화하거나 비활성화할 수 있을 뿐 아니라 모니터링된 조건이 규칙을 트리거하는 경우 시스템이 수행하는 작업을 지정할 수도 있습니다.

Cisco Talos(Talos Intelligence Group)는 각 기본 정책에서 각 침입 및 검사기 규칙의 기본 작업을 설정합니다. 예를 들어, 규칙은 Security Over Connectivity(연결성에 우선하는 보안) 기본 정책에서 활성화되며 Connectivity Over Security(보안에 우선하는 연결성) 기본 정책에서는 비활성화됩니다. Talos에서는 때때로 규칙 업데이트를 사용하여 기본 정책에 있는 하나 이상의 규칙의 기본 작업을 변경합니다. 규칙 업데이트가 기반 정책을 업데이트하도록 허용하면, 정책을 생성하기 위해 사용한 기본 정책(또는 기반으로 하는 기본 정책)에서 기본 작업이 변경될 때 정책에 있는 규칙의 기본 작업을 변경하는 것도 허용됩니다. 그러나 규칙 작업을 변경한 경우 규칙 업데이트가 변경 사항을 재정의하지 않습니다.

침입 규칙을 생성하면 침입 정책은 정책 생성에 사용되는 기본 정책에 있는 규칙의 기본 작업을 상속합니다.

침입 규칙 작업 옵션

침입 정책에서 규칙의 작업을 다음 값으로 설정할 수 있습니다.

Alert(알림**)**

시스템이 일치하는 트래픽을 찾으면 특정 침입 시도를 탐지하고 침입 이벤트를 생성하도록 하려는 경우에 설정합니다. 악의적인 패킷이 네트워크를 이동하여 규칙을 트리거하면 규칙이 목

적지로 전송되고 시스템이 침입 이벤트를 생성합니다. 악의적인 패킷이 대상에 도달하지만, 이벤트 로깅을 통해 알림이 전송됩니다.

Block(차단**)**

시스템이 일치하는 트래픽을 찾으면 특정 침입 이벤트를 탐지하고, 공격을 포함하는 패킷을 삭제하고, 침입 이벤트를 생성하도록 하려는 경우에 설정합니다. 악성 패킷은 대상에 도달하지 못하며 이벤트 로깅을 통해 알림이 전송됩니다.

Disable(비활성화**)**

시스템이 일치하는 트래픽을 평가하지 않도록 하려면 설정합니다.

참고 **Alert(**알림**)** 또는 **Block(**차단**)** 옵션을 선택하면 규칙이 활성화됩니다. **Disable(**비활성화**)**를 선택하면 규칙이 비활성화됩니다.

Cisco는 침입 정책 내 침입 규칙을 모두 활성화하지 않을 것을 강력히 권장합니다. 모든 규칙이 활성화될 경우 관리되는 디바이스의 성능이 저하될 수 있습니다. 대신 네트워크 환경과 가능한 한 일치하도록 규칙 설정을 조정하십시오.

침입 규칙 작업 설정

침입 규칙 작업은 정책별로 다릅니다.

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

단계 **2** 수정하려는 정책 옆의 **Snort 3 Version(Snort 3** 버전**)**을 클릭합니다.

팁 이 페이지에는 다음 항목의 총 개수가 표시됩니다.

- 비활성화된 규칙
- Alert(알림)으로 설정된 활성화된 규칙
- Block(차단)으로 설정된 활성화된 규칙
- 재정의된 규칙

단계 **3** 규칙 작업을 설정할 규칙을 하나 이상 선택합니다.

단계 **4** **Rule Action(**규칙 작업**)** 드롭다운 목록에서 규칙 작업 중 하나를 선택합니다. 다양한 규칙 작업에 대한 자세한 내용은 Snort 3 침입 정책 편집를 참조하십시오.

단계 **5** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축를 참고하십시오.

침입 정책의 침입 이벤트 알림 필터

침입 이벤트의 중요성은 발생 빈도 또는 소스/대상 IP 주소를 기준으로 결정될 수 있습니다. 어떤 경우에는 특정 횟수가 발생할 때까지 이벤트에 대해 신경 쓰지 않아도 됩니다. 예를 들어, 어떤 사용자가 서버에 로그인을 시도하는 경우 특정 횟수만큼 실패할 때까지는 염려하지 않아도 됩니다. 다른 경우에는 소수의 발생 상황만 확인해도 광범위한 문제의 존재 여부를 파악할 수 있습니다. 예를 들어 웹 서버에 대해 DoS 공격이 시작된 경우, 상황을 해결해야 하는지를 파악하려면 침입 이벤트의 발생 상황을 몇 번만 확인해보면 됩니다. 동일한 이벤트를 수백 번 확인하면 시스템에 부담을 줄 뿐입니다.

침입 이벤트 임계값

지정된 기간 내 이벤트 생성 횟수를 기반으로 시스템이 침입 이벤트를 기록 및 표시하는 횟수를 제한하도록 개별 규칙에 대한 임계값을 설정할 수 있습니다. 이를 통해 많은 수의 동일한 이벤트로 인해 마비되는 것을 방지할 수 있습니다. 공유 개체 규칙, 표준 텍스트 규칙 또는 검사기 규칙별 임계값을 설정할 수 있습니다.

침입 이벤트 임계값 구성

임계값을 설정하려면 먼저 임계값 설정 유형을 지정합니다.

표 ***2:*** 임계값 설정 옵션

옵션	설명
제한	지정된 기간 중 규칙을 트리거하는 지정된 패킷 수(count 인수로 지정)에 대한 이벤트를 로깅하고 표시합니다. 예를 들어, 유형은 **Limit(**제한**)**로, **Count(**카운트**)**는 `10`으로, 그리고 **Seconds(**초**)**는 `60`으로 설정하고 14개의 패킷이 규칙을 트리거하는 경우, 시스템은 동일한 시간(분) 내 발생한 첫 10개의 패킷을 표시한 후 규칙의 이벤트 로깅을 중단합니다.
임계값	지정된 기간 중 지정된 패킷 수(count 인수로 지정)가 규칙을 트리거하면 단일 이벤트를 로깅하고 표시합니다. 이벤트의 임계값 카운트에 도달하고 시스템이 해당 이벤트를 로깅하면 시간에 대한 카운터가 다시 시작됩니다. 예를 들어, 유형은 **Threshold(**임계값**)**로, **Count(**카운트**)**는 `10`으로, 그리고 **Seconds(**초**)**는 `60`으로 설정하면 규칙은 33초에 10번 트리거됩니다. 시스템은 하나의 이벤트를 생성한 다음, Seconds(초) Count(카운트) 카운터를 0으로 재설정합니다. 그런 다음 규칙은 다음 25초 안에 다시 10번 트리거됩니다. 카운터가 33초에 0으로 재설정되어 있기 때문에 시스템은 다른 이벤트를 로깅합니다.

옵션	설명
모두	지정된 수(카운트)의 패킷이 규칙을 트리거한 후 특정 시기 동안 한 번에 하나의 이벤트를 로깅하고 표시합니다. 예를 들어, 유형은 **Both(**모두**)**로, **Count(**카운트**)**는 2로, 그리고 **Seconds(**초**)**는 10으로 설정하면, 다음과 같이 이벤트가 계산됩니다. • 규칙이 10초 안에 한 번 트리거되는 경우, 시스템은 어떤 이벤트도 생성하지 않습니다(임계값이 충족되지 않음). • 규칙이 10초 안에 두 번 트리거되는 경우, 시스템은 하나의 이벤트를 생성합니다(규칙이 두 번째 트리거될 때 임계값이 충족됨). • 규칙이 10초에 네 번 트리거되면 시스템은 이벤트를 한 번 생성합니다(규칙이 두 번째 트리거될 때 임계값이 충족되고 이후 이벤트는 무시됨).

다음으로 이벤트 임계값이 소스 IP 주소별로 계산되는지 대상 IP 주소별로 계산되는지 결정하는 추적을 지정합니다.

표 ***3:*** 임계값 설정 ***IP*** 옵션

옵션	설명
소스	소스 IP 주소당 이벤트 인스턴스 수를 계산합니다.
대상	대상 IP 주소당 인스턴스 이벤트 수를 계산합니다.

마지막으로, 임계값을 정의하는 기간 및 인스턴스 수를 지정합니다.

표 ***4:*** 임계값 설정 인스턴스**/**시간 옵션

옵션	설명
개수	임계값 충족에 필요한 추적 IP 주소당 지정된 기간의 이벤트 인스턴스 수.
시간(초)	카운트가 재설정되기 전에 경과된 시간(초). 임계값 유형을 **limit(**제한**)**로, 추적을 **Source IP(**소스 **IP)**로, **count(**카운트**)**를 10으로, 그리고 **seconds(**초**)**를 10으로 설정한 경우, 시스템은 주어진 소스 포트에서 10초 안에 발생한 첫 10개의 이벤트를 로깅하고 표시합니다. 첫 10초 안에 7개의 이벤트만 발생한 경우, 시스템은 이를 모두 로깅하고 표시하며, 첫 10초 안에 40개의 이벤트가 발생한 경우, 시스템은 10개를 로깅하고 표시한 후 10초의 시간이 경과한 시점에서 다시 카운팅을 시작합니다.

침입 이벤트 임계값 설정을 단독으로 사용할 수도 있고, 속도 기반 공격 방지, `detection_filter` 키워드 및 침입 이벤트 삭제와 조합하여 사용할 수도 있습니다.

팁 침입 이벤트의 패킷 보기 내에서 임계값을 추가할 수도 있습니다.

Snort 3의 침입 규칙에 대한 임계값 설정

Rule Detail(규칙 세부 사항) 페이지에서 규칙에 대한 단일 임계값을 설정할 수 있습니다. 임계값을 추가하여 규칙에 대한 기존 임계값을 덮어씁니다.

단계 1 **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**를 선택합니다.

단계 2 **Snort 3 All Rules(Snort 3** 모든 규칙**)** 탭을 클릭합니다.

단계 3 침입 규칙의 Alert Configuration(알림 구성) 열에서 **None(**없음**)** 링크를 클릭합니다.

단계 4 **Edit(**편집**)**( )을 클릭합니다.

단계 5 Alert Configuration(알림 구성) 창에서 **Threshold(**임계값**)** 탭을 클릭합니다.

단계 6 **Type(**유형**)** 드롭다운 목록에서 설정하려는 임계값 유형을 선택합니다.

- **Limit(**제한**)**를 선택하여 기간당 지정된 이벤트 인스턴스 수로 알림을 제한합니다.
- 기간당 지정된 각 이벤트 인스턴스의 수에 대해 알림을 제공하려면 **Threshold(**임계값**)**를 선택합니다.
- 지정된 이벤트 인스턴스의 수 이후 기간당 한 번 알림을 제공하려면 **Both(**모두**)**를 선택합니다.

단계 7 **Track By(**추적 기준**)** 필드에서 **Source(**소스**)** 또는 **Destination(**대상**)**을 선택하여 이벤트 인스턴스를 소스 IP 주소로 추적할지 대상 IP 주소로 추적할지 나타냅니다.

단계 8 임계값으로 사용할 이벤트 인스턴스의 수를 **Count(**카운트**)** 필드에 입력합니다.

단계 9 이벤트 인스턴스를 추적할 기간(초 단위)을 지정하는 숫자를 **Seconds(**초**)** 필드에 입력합니다.

단계 10 **Save(**저장**)**를 클릭합니다.

추가 지원 및 정보는 Snort 3 억제 및 임계값 비디오를 참조하십시오.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축를 참고하십시오.

침입 이벤트 임계값 보기 및 삭제

규칙에 대한 기존 임계값 설정을 보거나 삭제하려면 Rules Details(규칙 세부 정보) 보기를 사용하여 임계값에 대해 구성된 설정을 표시하고 해당 설정이 시스템에 적합한지 확인합니다. 적절하지 않은 경우 새 임계값을 추가하여 기존 값을 덮어쓸 수 있습니다.

단계 1 **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**를 선택합니다.

단계 2 **Snort 3 All Rules(Snort 3** 모든 규칙**)** 탭을 클릭합니다.

단계 3 **Alert Configuration(**알림 구성**)** 열에 표시된 것과 같이 구성된 임계값이 있는 규칙을 선택합니다. **Alert Configuration(**알림 구성**)** 열은 규칙에 대한 링크로 **Threshold(**임계값**)**를 표시합니다.

단계 4 규칙의 임계값을 제거하려면 **Alert Configuration(**알림 구성**)** 열에서 **Threshold(**임계값**)** 링크를 클릭합니다.

단계 5 편집 ( )을 클릭합니다.

단계 **6** **Threshold(**임계값**)** 탭을 클릭합니다.

단계 **7** **Reset(**재설정**)**을 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축를 참고하십시오.

침입 정책 삭제 구성

특정 IP 주소 또는 특정 범위의 IP 주소가 특정 규칙 또는 검사기를 트리거하면 침입 이벤트 알림을 삭제할 수 있습니다. 이렇게 하면 오탐을 없애는 데 도움이 됩니다. 예를 들어 특정 익스플로잇처럼 보이는 패킷을 전송하는 메일 서버가 있는 경우, 메일 서버에 의해 이벤트가 트리거될 때 해당 이벤트에 대한 이벤트 알림을 억제할 수 있습니다. 규칙은 모든 패킷에 대해 트리거되지만, 기준에 맞는 공격에 대한 이벤트만 표시됩니다.

침입 정책 삭제 유형

침입 이벤트 억제를 단독으로 사용할 수도 있고, 속도 기반 공격 방지, `detection_filter` 키워드 및 침입 이벤트 임계값 설정과 조합하여 사용할 수도 있습니다.

팁 침입 이벤트의 패킷 보기 내에서 억제를 추가할 수도 있습니다. 침입 규칙 편집기 페이지(**Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)** > **Snort 3 All Rules(Snort 3** 모든 규칙**)**)에서 **Alert Configuration(**알림 구성**)** 열을 사용하여 억제 설정에 액세스할 수도 있습니다.

Snort 3의 침입 규칙에 대한 억제 설정

침입 규칙에서 규칙에 하나 이상의 억제를 설정할 수 있습니다.

시작하기 전에

소스 또는 대상 억제를 위해 추가할 네트워크 개체를 생성해야 합니다.

단계 **1** **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**를 선택합니다.

단계 **2** **Snort 3 All Rules(Snort 3** 모든 규칙**)** 탭을 클릭합니다.

단계 **3** 침입 규칙의 Alert Configuration(알림 구성) 열에서 **None(**없음**)** 링크를 클릭합니다.

단계 **4** **Edit(**편집**)**( )을 클릭합니다.

단계 **5** **Suppressions(**억제**)** 탭에서 다음 옵션 옆의 추가 아이콘(+)을 클릭합니다.

- 지정된 소스 IP 주소에서 시작되는 패킷에 의해 생성된 이벤트를 억제하려면 **Source Networks(**소스 네트워크**)**를 선택합니다.

- 지정된 대상 IP 주소로 이동하는 패킷에 의해 생성된 이벤트를 억제하려면 **Destination Networks(**대상 네트워크**)**를 선택합니다.

단계 **6** **Network(**네트워크**)** 드롭다운 목록에서 사전 설정 네트워크 중 하나를 선택합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

단계 **8** (선택 사항) 필요한 경우 마지막 세 단계를 반복합니다.

단계 **9** Alert Configuration(알림 구성) 창에서 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축를 참고하십시오.

억제 조건 보기 및 삭제

기존 삭제 조건을 보거나 삭제하려고 할 수 있습니다. 예를 들어, 메일 서버는 일반적으로 익스플로잇처럼 보이는 패킷을 전송하므로 메일 서버 IP 주소에서 시작되는 패킷에 대한 이벤트 알림을 억제할 수 있습니다. 그리고 해당 메일 서버를 폐쇄하고 다른 호스트에 IP 주소를 다시 할당할 경우, 해당 소스 IP 주소에 대한 삭제 조건을 삭제해야 합니다.

단계 **1** **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**를 선택합니다.

단계 **2** **Snort 3 All Rules(Snort 3** 모든 규칙**)** 탭을 클릭합니다.

단계 **3** 억제를 보거나 삭제할 규칙을 선택합니다.

단계 **4** **Alert Configuration(**알림 구성**)** 열에서 **Suppression(**억제**)**을 클릭합니다.

단계 **5** 편집 (✎) 버튼을 클릭합니다.

단계 **6** **Suppressions(**억제**)** 탭을 클릭합니다.

단계 **7** 해당 억제 옆의 **Clear(**지우기**)**(✕)를 클릭하여 억제를 제거합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축를 참고하십시오.

침입 규칙 설명 추가

침입 정책에서 규칙에 코멘트를 추가할 수 있습니다. 이렇게 추가되는 코멘트는 해당 정책에 한정됩니다. 즉, 한 침입 정책에서 규칙에 추가하는 코멘트는 다른 침입 정책에서는 표시되지 않습니다.

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

단계 2 수정하려는 정책 옆의 **Snort 3 Version(Snort 3 버전)**을 클릭합니다.
단계 3 모든 규칙이 나열된 페이지의 오른쪽에서 코멘트를 추가하려는 규칙을 선택합니다.
단계 4 **Comments(코멘트)** 열 아래의 코멘트( )를 클릭합니다.
단계 5 **Comments(코멘트)** 필드에 규칙 코멘트를 입력합니다.
단계 6 **Add Comment(코멘트 추가)**를 클릭합니다.
단계 7 **Save(저장)**를 클릭합니다.

팁 시스템은 Comments(코멘트) 열의 규칙 옆에 코멘트( )를 표시합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축를 참고하십시오.

Snort 2 사용자 지정 규칙을 Snort 3로 변환

사용자 지정 규칙을 사용하는 경우 Snort 2에서 Snort 3로 변환하기 전에 Snort 3용 규칙 세트를 관리할 준비가 되었는지 확인합니다. 서드파티 벤더의 규칙 세트를 사용하는 경우 해당 벤더에 연락하여 규칙이 Snort 3로 성공적으로 변환되는지 확인하거나 기본적으로 Snort 3용으로 작성된 대체 규칙 세트를 얻으십시오. 직접 작성한 사용자 지정 규칙이 있는 경우 변환 전에 Snort 3 규칙을 작성하는 방법을 숙지하여 변환 후 Snort 3 탐지를 최적화하도록 규칙을 업데이트할 수 있습니다. Snort 3의 규칙 작성에 대해 자세히 알아보려면 아래 링크를 참조하십시오.

- https://blog.snort.org/2020/08/how-rules-are-improving-in-snort-3.html
- https://blog.snort.org/2020/10/talos-transition-to-snort-3.html

Snort 3 규칙에 대해 자세히 알아보려는 경우 https://blog.snort.org/에서 다른 블로그를 참조할 수 있습니다.

시스템 제공 툴을 사용하여 Snort 2 규칙을 Snort 3 규칙으로 변환하려면 Snort 2 사용자 지정 규칙을 Snort 3로 변환, 11 페이지 항목을 참조하십시오.

중요 Snort 2 NAP(Network Analysis Policy, 네트워크 분석 정책) 설정은 Snort3에 자동으로 복사될 수 없습니다. NAP 설정은 Snort 3에서 수동으로 복제해야 합니다.

모든 침입 정책의 모든 Snort 2 사용자 지정 규칙을 Snort 3로 변환

단계 1 **Objects(개체)** > **Intrusion Rules(침입 규칙)**를 선택합니다.
단계 2 **Snort 3 All Rules(Snort 3 모든 규칙)** 탭을 클릭합니다.

단계 **3** 왼쪽 창에 **All Rules(**모든 규칙**)**가 선택되어 있는지 확인합니다.

단계 **4** **Tasks(**작업**)** 드롭다운 목록을 클릭하고 다음을 선택합니다.

- **Convert Snort 2 rules and import(Snort 2** 규칙 변환 및 가져오기**)** - 모든 침입 정책의 모든 Snort 2 사용자 지정 규칙을 Snort 3로 자동 변환하고 Management Center에 Snort 3 사용자 지정 규칙으로 가져옵니다.
- **Convert Snort 2 rules and download(Snort 2** 규칙 변환 및 다운로드**)** - 모든 침입 정책의 모든 Snort 2 사용자 지정 규칙을 Snort 3로 자동 변환하고 로컬 시스템에 다운로드합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

참고
- 앞 단계에서 **Convert and import(**변환 및 가져오기**)**를 선택한 경우 변환된 모든 규칙은 **Local Rules(**로컬 규칙**)** 아래 새로 생성된 규칙 그룹 **All Snort 2 Converted Global(**모든 **Snort 2** 변환 전역**)**에 저장됩니다.
- 앞 단계에서 **Convert and download(**변환 및 다운로드**)**를 선택한 경우 규칙 파일을 로컬에 저장합니다. 다운로드한 파일에서 변환된 규칙을 검토하고 나중에 규칙 그룹에 사용자 지정 규칙 추가, 13 페이지의 단계에 따라 업로드할 수 있습니다.

추가 지원 및 정보는 Snort 2 규칙을 Snort 3로 변환 비디오를 참조하십시오.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축를 참고하십시오.

단일 침입 정책의 **Snort 2** 사용자 지정 규칙을 **Snort 3**로 변환

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

단계 **2** **Intrusion Policies(**침입 정책**)** 탭에서 **Show Snort 3 Sync status(Snort 3** 동기화 상태 표시**)**를 클릭합니다.

단계 **3** 침입 정책의 **Sync(**동기화**)** 아이콘( )을 클릭합니다.

참고 Snort 2 버전과 Snort 3 버전의 침입 정책이 동기화된 경우 **Sync(**동기화**)** 아이콘이 녹색( )으로 표시됩니다. 이는 변환할 사용자 지정 규칙이 없음을 나타냅니다.

단계 **4** 요약을 읽고 **Custom Rules(**사용자 지정 규칙**)** 탭을 클릭합니다.

단계 **5** 다음을 선택합니다.

- **Import converted rules to this policy(**변환된 규칙을 이 정책으로 가져오기**)** - 침입 정책의 Snort 2 사용자 지정 규칙을 Snort 3로 변환하고 Management Center에 Snort 3 사용자 지정 규칙으로 가져옵니다.
- **Download converted rules(**변환된 규칙 다운로드**)** - 침입 정책의 Snort 2 사용자 지정 규칙을 Snort 3로 변환하고 로컬 시스템에 다운로드합니다. 다운로드한 파일에서 변환된 규칙을 검토하고 나중에 업로드 아이콘을 클릭하여 파일을 업로드할 수 있습니다.

단계 **6** **Re-Sync(**재동기화**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축를 참고하십시오.

규칙 그룹에 사용자 지정 규칙 추가

Management Center에서 사용자 지정 규칙을 업로드하면 로컬로 생성한 사용자 지정 규칙이 모든 Snort 3 규칙 목록에 추가됩니다.

단계 **1** **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**를 선택합니다.

단계 **2** **Snort 3 All Rules(Snort 3** 모든 규칙**)** 탭을 클릭합니다.

단계 **3** **Tasks(**작업**)** 드롭다운 목록을 클릭합니다.

단계 **4** **Upload Snort 3 Rules(Snort 3** 규칙 업로드**)**를 클릭합니다.

단계 **5** 생성한 Snort 3 사용자 지정 규칙이 포함된 `.txt` 또는 `.rules` 파일을 끌어다 놓습니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

참고 선택한 파일에 오류가 있으면 더 이상 진행할 수 없습니다. 오류 파일을 다운로드하고 **Replace File(**파일 교체**)** 링크를 클릭하여 오류를 수정한 후에 파일의 버전 2를 업로드할 수 있습니다.

단계 **7** 규칙 그룹에 규칙을 연결하여 새 규칙을 그룹에 추가합니다.

Create New Custom Rule Group(새 사용자 지정 규칙 그룹 생성**)** 링크를 클릭하여 새 사용자 지정 규칙 그룹을 생성한 다음 새 그룹에 규칙을 추가할 수도 있습니다.

참고 기존 로컬 규칙 그룹이 없는 경우 **Create New Custom Rule Group to proceed(**계속하려면 새 사용자 지정 규칙 그룹 생성**)**를 클릭하여 계속 진행합니다. 새 규칙 그룹의 **Name(**이름**)**을 입력하고 **Save(**저장**)**를 클릭합니다.

단계 **8** 다음 중 하나를 선택합니다.

- **Merge Rules(**규칙 병합**)** - 규칙 그룹의 기존 규칙과 추가하는 새 규칙을 병합합니다.
- **Replace all rules in the group with file contents(**그룹의 모든 규칙을 파일 콘텐츠로 교체**)** - 모든 기존 규칙을 추가하는 새 규칙으로 교체합니다.

참고 앞 단계에서 둘 이상의 규칙 그룹을 선택한 경우 **Merge Rules(**규칙 병합**)** 옵션만 사용할 수 있습니다.

단계 **9** **Next(**다음**)**를 클릭합니다.

요약을 검토하여 추가되는 새 규칙 ID를 확인하고 필요한 경우 요약을 다운로드합니다.

단계 **10** **Finish(**마침**)**를 클릭합니다.

중요 업로드된 모든 규칙의 규칙 작업은 비활성화된 상태입니다. 규칙을 활성화하려면 필요한 상태로 변경해야 합니다.

다음에 수행할 작업

- Management Center에서 사용자 지정 규칙을 업로드하면 생성한 사용자 지정 규칙이 모든 Snort 3 규칙 목록에 추가됩니다. 이러한 사용자 지정 규칙을 트래픽에 적용하려면 필요한 침입 정책에서 이러한 규칙을 추가하고 활성화합니다. 침입 정책에 사용자 지정 규칙이 포함된 규칙 그룹 추가에 대한 자세한 내용은 침입 정책에 사용자 지정 규칙이 포함된 규칙 그룹 추가, 14 페이지 항목을 참조하십시오. 사용자 지정 규칙 활성화에 대한 자세한 내용은 Snort 3의 사용자 지정 규칙 관리, 14 페이지 항목을 참조하십시오.
- 구성 변경사항을 구축합니다. 구성 변경 사항 구축를 참고하십시오.

침입 정책에 사용자 지정 규칙이 포함된 규칙 그룹 추가

시스템에서 업로드된 사용자 지정 규칙을 침입 정책에서 활성화해야만 트래픽에 이러한 규칙이 적용됩니다. Management Center에서 사용자 지정 규칙을 업로드한 후 새 사용자 지정 규칙이 포함된 규칙 그룹을 침입 정책에 추가합니다.

단계 1 **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.
단계 2 **Intrusion Policies(**침입 정책**)** 탭에서 침입 정책의 **Snort 3 Version(Snort 3** 버전**)**을 클릭합니다.
단계 3 Rule Groups(규칙 그룹) 검색 창 옆에 있는 **Add(**추가**)**(+)를 클릭합니다.
단계 4 **Add Rule Groups(**규칙 그룹 추가**)** 창에서 규칙 그룹 옆에 있는 > 아이콘을 클릭하여 로컬 규칙 그룹을 확장합니다.
단계 5 업로드된 사용자 지정 규칙 그룹 옆의 체크 박스를 선택합니다.
단계 6 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축를 참고하십시오.

Snort 3의 사용자 지정 규칙 관리

시스템에서 업로드된 사용자 지정 규칙을 침입 정책에 추가하고 활성화해야만 트래픽에 이러한 규칙이 적용됩니다. 업로드된 사용자 지정 규칙을 모든 정책에서 활성화하거나 개별 정책에서 선택적으로 활성화할 수 있습니다.

하나 이상의 침입 정책에서 사용자 지정 규칙을 활성화하려면 다음 단계를 수행합니다.

단계 **1** **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**를 선택합니다.
단계 **2** **Snort 3 All Rules(Snort 3** 모든 규칙**)** 탭을 클릭합니다.
단계 **3** **Local Rules(**로컬 규칙**)**를 확장합니다.
단계 **4** 필요한 규칙 그룹을 선택합니다.
단계 **5** 규칙 옆의 체크 박스를 선택하여 규칙을 선택합니다.
단계 **6** **Rule Actions(**규칙 작업**)** 드롭다운 목록에서 **Per Intrusion Policy(**침입 정책별**)**를 선택합니다.
단계 **7** 다음 중에서 선택합니다.

- **All Policies(**모든 정책**)** - 추가할 모든 규칙에 대해 동일한 규칙 작업을 수행합니다.
- **Per Intrusion Policy(**침입 정책별**)** - 각 침입 정책에 대해 서로 다른 규칙 작업을 수행합니다.

단계 **8** 다음과 같이 규칙 작업을 설정합니다.

- 앞 단계에서 All Policies(모든 정책)를 선택한 경우 **Select Override state(**재정의 상태 선택**)** 드롭다운 목록에서 필요한 규칙 작업을 선택합니다.
- 앞 단계에서 Per Intrusion Policy(침입 정책별)를 선택한 경우 해당 정책 이름에 대해 **Rule Action(**규칙 작업**)**을 선택합니다. 정책을 더 추가하려면 **Add Another(**다른 하나 추가**)**를 클릭합니다.

단계 **9** 선택적으로 **Comments(**코멘트**)** 텍스트 상자에 코멘트를 추가합니다.
단계 **10** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

디바이스에서 변경 사항을 구축합니다. 참고, 구성 변경 사항 구축.

맞춤형 규칙 삭제

단계 **1** **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**를 선택합니다.
단계 **2** **Snort 3 All Rules(Snort 3** 모든 규칙**)** 탭을 클릭합니다.
단계 **3** 왼쪽 창에서 **Local Rules(**로컬 규칙**)**를 확장합니다.
단계 **4** 삭제할 규칙의 체크 박스를 선택합니다.
단계 **5** 선택한 모든 규칙에 대한 규칙 작업이 **Disable(**비활성화**)**인지 확인합니다.

필요한 경우 아래 단계에 따라 선택한 여러 규칙에 대해 규칙 작업을 비활성화합니다.

a) **Rule Actions(**규칙 작업**)** 드롭다운 상자에서 **Per Intrusion Policy(**침입 정책별**)**를 선택합니다.
b) **All Policies(**모든 정책**)** 라디오 버튼을 선택합니다.
c) **Select Override state(**재정의 상태 선택**)** 드롭다운 목록에서 **Disable(**비활성화**)**을 선택합니다.
d) **Save(**저장**)**를 클릭합니다.

e) 삭제할 규칙의 체크 박스를 선택합니다.

단계 **6** **Rule Actions(**규칙 작업**)** 드롭다운 목록에서 **Delete(**삭제**)**를 선택합니다.

단계 **7** Delete Rules(규칙 삭제) 팝업 창에서 **Delete(**삭제**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축를 참고하십시오.

규칙 그룹 삭제

시작하기 전에

삭제하려는 규칙 그룹을 해당 규칙 그룹이 포함된 모든 침입 정책에서 제외합니다. 침입 정책에서 규칙 그룹을 제외하는 단계는 Snort 3 침입 정책 편집 항목을 참조하십시오.

단계 **1** **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**를 선택합니다.

단계 **2** **Snort 3 All Rules(Snort 3** 모든 규칙**)** 탭을 클릭합니다.

단계 **3** 왼쪽 창에서 **Local Rules(**로컬 규칙**)**를 확장합니다.

단계 **4** 삭제할 규칙 그룹을 선택합니다.

단계 **5** 계속하기 전에 그룹의 모든 규칙에 대한 규칙 작업이 **Disable(**비활성화**)**로 설정되어 있는지 확인합니다.

규칙에 대한 규칙 작업이 **Disable(**비활성화**)** 이외로 설정된 경우 규칙 그룹을 삭제할 수 없습니다. 필요한 경우 아래 단계에 따라 모든 규칙에 대해 규칙 작업을 비활성화합니다.

a) **Rule Actions(**규칙 작업**)** 드롭다운 목록 아래의 체크 박스를 선택하여 그룹의 모든 규칙을 선택합니다.
b) **Rule Actions(**규칙 작업**)** 드롭다운 상자에서 **Per Intrusion Policy(**침입 정책별**)**를 선택합니다.
c) **All Policies(**모든 정책**)** 라디오 버튼을 선택합니다.
d) **Select Override state(**재정의 상태 선택**)** 드롭다운 목록에서 **Disable(**비활성화**)**을 선택합니다.
e) **Save(**저장**)**를 클릭합니다.

단계 **6** 규칙 그룹 옆에 있는 **Delete(**삭제**)**( )를 클릭합니다.

단계 **7** Delete Rule Group(규칙 그룹 삭제) 팝업 창에서 **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축를 참고하십시오.