네트워크 자산에 대한 침입 방지 맞춤화

다음 주제에서는 Cisco 권장 규칙을 사용하는 방법을 설명합니다.

Cisco 권장 규칙 정보

침입 규칙 권장사항을 사용하여 네트워크에서 탐지된 운영 체제, 서버 및 클라이언트 애플리케이션 프로토콜을 자산을 보호하기 위해 특별히 작성된 규칙과 연결할 수 있습니다. 침입 정책을모니터링되는 네트워크의 특정 요구를 조정할 수 있게 합니다.

시스템에서 각 IPS 정책 대 한 권장 사항 개별 집합을 만듭니다. 일반적으로 표준 텍스트 규칙 및 공유 개체 규칙에 대 한 규칙 상태 변경을 권장합니다. 그러나, 전처리기 및 디코더 규칙에 대 한 변경 사항을 추천해 합니다.

규칙 상태 권장 사항을 생성할 때에 기본 설정을 사용 하 여 수도 있고 고급 설정을 구성할 수 있습니다. 고급 설정을 수행할 수 있습니다.

- 취약성에 대 한 네트워크에 있는 호스트 시스템 모니터링 재정의
- 규칙 오버 헤드에 따라 시스템이 권장 규칙에 영향을
- 규칙을 비활성화 하기 위한 권장 생성을 활성화할지 지정

권장 되는 즉시 사용 또는 권장 사항 (및 영향을 받는 규칙)을 수락 하기 전에 검토 선택할 수도 있습니다.

권장 규칙 상태를 사용하도록 선택하면 읽기 전용 Cisco 권장 사항 계층이 침입 정책에 추가되고 이후 권장 규칙 상태를 사용하지 않기로 선택하면 계층이 제거됩니다.

침입 정책에서 가장 최근에 저장된 구성 설정에 따라 자동으로 권장 사항을 생성하도록 태스크를 예약할 수 있습니다.

시스템은 수동으로 설정한 규칙 상태를 변경하지 않습니다.

- 권장 사항을 생성하기 전에 지정된 규칙의 상태를 수동으로 설정하면 시스템이 향후 해당 규칙의 상태를 수정할 수 없게 됩니다.
- 권장 사항을 생성한 후 수동으로 지정된 규칙의 상태를 설정하면 해당 규칙의 권장 상태가 재정의됩니다.

팁 침입 정책 리포트는 권장 상태와 다른 규칙 상태를 가진 규칙 목록을 포함할 수 있습니다.

권장 필터링된 규칙 페이지를 표시하는 동안 또는 탐색 패널 또는 정책 정보 페이지에서 직접 규칙 페이지에 액세스한 후 규칙 상태를 수동으로 설정하고 규칙을 정렬하고 규칙 페이지에서 사용할 수 있는 다른 작업(예: 규칙 억제, 규칙 임계값 설정 등)을 수행할 수 있습니다.

참고 Talos 인텔리전스 그룹 시스템 제공 정책에서 각 규칙의 적절한 상태를 결정합니다. 시스템 제공 정책을 기본 정책으로 사용하는 경우 시스템에서 Cisco 권장 규칙 상태에 규칙을 설정하도록 허용하면 침입 정책의 규칙은 네트워크 자산에 대해 Cisco에서 권장하는 설정과 일치합니다.

권장된 규칙 및 멀티 테 넌 시

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축의 경우 상위 도메인의 침입 정책에서 이 기능을 활성화하면 모든 하위 리프 도메인의 데이터를 사용하여 권장 사항이 생성됩니다. 이로 인해 일부 리프 도메인에는 없는 자산에 맞게 조정된 침입 규칙이 활성화되어 성능에 영향을 줄 수 있습니다.

Cisco 추천 기본 설정

Cisco 추천을 생성하면 시스템은 네트워크 자산과 연결된 취약성으로부터 보호하는 규칙의 기본 정책을 검색하고 기본 정책에서 규칙의 현재 상태를 식별합니다. 그런 다음 시스템은 규칙 상태를 추천하며, 사용자가 선택하면 규칙을 권장 상태로 설정합니다.

시스템은 다음과 같은 기본 분석을 수행하여 권장 사항을 생성합니다.

표 *1:* 취약성을 기준으로 한 규칙 상태 권장 사항

규칙이 검색된 자산을 보호합니까?	기본 정책 규칙 상태	권장 규칙 상태
예	비활성화	이벤트 생성
	이벤트 생성	이벤트 생성
	이벤트 삭제 및 생성	이벤트 삭제 및 생성

규칙이 검색된 자산을 보호합니까?	기본 정책 규칙 상태	권장 규칙 상태
아니요	모두	비활성화

테이블에서 다음에 유의하십시오.

- 규칙이 기본 정책에서 비활성화되어 있거나 Generate Events(이벤트 생성)로 설정된 경우, 권장 상태는 항상 Generate Events(이벤트 생성)입니다.

  예를 들어 기본 정책이 모든 규칙이 비활성화되는 No Rules Active(활성 규칙 없음)인 경우, Drop and Generate Events(이벤트 삭제 및 생성) 권장 사항은 없습니다.

- Drop and Generate Events(이벤트 삭제 및 생성)은 기본 정책에서 이미 Drop and Generate Events(이벤트 삭제 및 생성)로 설정된 규칙의 경우에만 권장됩니다.

  규칙을 Drop and Generate events(이벤트 삭제 및 생성)으로 설정하려 하고 해당 규칙이 기본 정책에서 비활성화되어 있거나 Generate Events(이벤트 생성)로 설정된 경우, 규칙 상태를 수동으로 재설정해야 합니다.

Cisco 권장 규칙의 고급 설정을 변경하지 않고 권장 사항을 생성하면 시스템은 검색된 전체 네트워크의 모든 호스트에 대해 규칙 상태를 변경하도록 권장합니다.

시스템은 기본적으로 오버헤드가 낮거나 중간인 규칙에 대해서만 권장 사항을 생성하며, 규칙을 비활성화하라는 권장 사항을 생성합니다.

시스템은 Impact Qualification 기능을 사용하여 비활성화하는 취약성에 기반한 침입 규칙에 대해 규칙 상태를 권장하지 않습니다.

시스템은 항상 호스트에 매핑된 서드파티 취약성에 연결된 로컬 규칙을 활성화하도록 권장합니다.

시스템은 매핑되지 않은 로컬 규칙에 대해서는 상태 권장 사항을 만들지 않습니다.

관련 항목

서드파티 제품 매핑

Cisco 추천 고급 설정

정책 보고서에 권장 사항과 규칙 상태의 모든 차이를 포함합니다

기본적으로 침입 정책 보고서는 정책의 활성화된 규칙, 즉 Generate Events(이벤트 생성) 또는 Drop and Generate Events(이벤트 삭제 및 생성)로 설정된 규칙을 나열합니다. **Include all differences(**모든 차이점 포함**)** 옵션을 활성화하면 권장 상태가 저장된 상태와 다른 규칙도 나열됩니다. 정책 보고서에 대해서는 구성 구축 정보를 참조하십시오.

검사할 네트워크

권장 사항을 위해 검사할 모니터링되는 네트워크 또는 개별 호스트를 지정합니다. 단일 IP 주소 또는 주소 블록을 지정하거나, 하나 또는 둘 다로 구성된 쉼표로 구분된 목록을 지정할 수 있습니다.

지정하는 호스트 내 주소의 목록은 부정을 제외하고 OR 연산으로 연결되며, 모든 OR 연산이 계산되면 AND 연산으로 연결됩니다.

호스트 정보를 기반으로 특정 패킷에 대해 활성 규칙 프로세싱을 동적으로 수정하려면 적응형 프로파일 업데이트을 활성화할 수도 있습니다.

권장 사항 임계값(규칙 오버 헤드별)

사용자가 선택하는 임계값보다 오버헤드가 높은 침입 규칙을 시스템이 권장하거나 자동으로 활성화하는 것을 방지합니다.

오버헤드는 규칙이 시스템 성능에 미칠 수 있는 영향과 규칙이 오탐을 생성할 가능성에 기반합니다. 오버헤드가 더 높은 규칙을 허용하면 일반적으로 권장 사항은 늘어나지만 시스템 성능에 영향이 있을 수 있습니다. 침입 Rules(규칙) 페이지의 규칙 세부 사항 보기에서 규칙의 오버헤드 등급을 볼 수 있습니다.

시스템은 규칙을 비활성화하라는 권장 사항에 대해서는 규칙 오버헤드를 고려하지 않습니다. 또한 서드파티 취약성에 매핑되지 않는 한 로컬 규칙은 오버 헤드가 없는 것으로 간주됩니다.

특정 설정의 오버헤드 등급이 있는 규칙에 대한 권장 사항을 생성할 경우, 오버헤드가 다른 권장 사항을 생성한 다음 원래 오버헤드 설정에 대해 권장 사항을 다시 생성하는 것이 차단되지 않습니다. 권장 사항의 생성 횟수 또는 생성에 사용하는 오버헤드 설정의 수와 상관없이 동일한 규칙 집합에 대해 권장 사항을 생성할 때마다 각 오버헤드 설정에 대해 동일한 규칙 상태 권장 사항을 얻게 됩니다. 예를 들면 오버헤드를 medium으로, 그 다음에는 high로, 그런 다음 마지막으로 다시 medium으로 설정하여 권장 사항을 생성할 수 있습니다. 네트워크의 호스트와 애플리케이션이 변경되지 않은 경우, 오버헤드가 medium으로 설정된 권장 사항의 두 집합은 해당 규칙 집합에 대해 동일합니다.

규칙을 비활성화하라는 권장 사항 수락

시스템은 Cisco 권장 사항을 기반으로 하는 침입 규칙을 비활성화 여부를 지정 합니다.

규칙을 비활성화하라는 권장 사항을 수용하면 규칙 적용 범위가 제한됩니다. 규칙을 비활성화하라는 권장 사항을 생략하면 규칙 적용 범위가 증가합니다.

관련 항목

적응형 프로파일 업데이트 및 Cisco 추천 규칙

Cisco 권장 사항 생성 및 적용

Cisco 권장 사항 사용을 시작하거나 중지하려면 네트워크 및 침입 규칙 집합의 크게에 따라 몇 분 정도 걸릴 수 있습니다.

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축의 경우 상위 도메인의 침입 정책에서 이 기능을 활성화하면 모든 하위 리프 도메인의 데이터를 사용하여 권장 사항이 생성됩니다. 이로 인해 일부 리프 도메인에는 없는 자산에 맞게 조정된 침입 규칙이 활성화되어 성능에 영향을 줄 수 있습니다.

시작하기 전에

- Cisco 권장 사항에는 다음 요구 사항이 있습니다.
  - Threat Defense 라이선스—IPS
  - 기본 라이선스—보호
  - 사용자 역할—관리자 또는 침입 관리자
- 단계를 시작하기 전에 네트워크 검색 정책을 구성합니다. Cisco 권장 사항이 적합하도록 내부 호스트를 정의할 네트워크 검색 정책을 구성합니다. 참고, 네트워크 검색 맞춤 설정.

프로시저

단계 **1** Snort 2 침입 정책 편집기의 탐색창에서 **Cisco** 권장 사항을 클릭합니다.

단계 **2** (선택 사항) 고급 설정을 구성합니다(Cisco 추천 고급 설정, 3 페이지 참조).

단계 **3** 권장 사항을 생성하고 적용합니다.

- 권장 사항 생성 및 사용 - 권장 사항을 생성하고 일치하도록 규칙 상태를 변경합니다. 권장 사항을 생성한 적이 없는 경우에만 사용할 수 있습니다.
- 권장 사항 생성 - 권장 사항을 사용 중인지 여부에 상관없이 새로운 권장 사항을 생성하지만 일치하도록 규칙 상태를 변경하지는 않습니다.
- 권장 사항 업데이트 - 권장 사항을 사용 중인 경우, 권장 사항을 생성하고 일치하도록 규칙 상태를 변경합니다. 그렇지 않은 경우, 규칙 상태를 변경하지 않고 새 권장 사항을 생성합니다.
- 권장 사항 사용 - 구현되지 않은 권장 사항과 일치하도록 규칙 상태를 변경합니다.
- 권장 사항 사용 안 함 - 권장 사항 사용을 중지합니다. 권장 사항을 적용하기 전에 규칙의 상태를 수동으로 변경한 경우, 규칙 상태는 사용자가 부여한 값으로 돌아갑니다. 그렇지 않은 경우, 규칙 상태는 기본값으로 돌아갑니다.

권장 사항을 생성할 때 시스템은 권장 변경 사항의 요약을 표시합니다. 시스템이 상태 변경을 권장하는 규칙의 목록을 보려면 새로 제안된 규칙 상태 옆에 있는 **View(**보기**)**를 클릭합니다.

단계 **4** 구현한 권장 사항을 평가하고 조정합니다.

대부분의 Cisco권장 사항을 수락하는 경우에도 규칙 상태를 수동으로 설정하여 개별 권장 사항을 재정의할 수 있습니다(참조침입 규칙 상태 설정).

단계 **5** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경 사항 구축의 내용을 참고하십시오.

스크립트 탐지

스크립트 감지는 부분 검사를 통해 너무 오래 걸리는 Snort 차단 침입을 방지합니다. HTML 파일이 클라이언트와 서버간에 전송될 때 이러한 파일에는 공격을 시작하기 위한 JavaScript와 같은 악성 스크립트가 포함될 수 있습니다. 이러한 악성 스크립트가 발견되면 부분 검사를 통해 모든 IPS 규칙이 악성 스크립트에서 일치하도록 허용하고 검사기는 검사 및 감지를 통해 해당 데이터 세그먼트를 플러시합니다. 악성 파일이 대상에 도달하지 않습니다. 이 기능은 HTTP/1 및 HTTP/2 트래픽을 모두 지원합니다.

이 기능은 기본적으로 항상 활성화되어 있습니다. 해제하려면 **`http_inspect.script_detection=true`**를 false로 설정합니다.