




네트워크 자산에 대한 침입 방지 맞춤화


다음 주제에서는 Firepower 권장 규칙을 사용하는 방법을 설명합니다.

- LSP 업데이트의 Snort 3 규칙 변경, 1 페이지
- Firepower 권장 규칙 정보, 1 페이지
- Snort 2에서 생성된 Firepower 권장 사항을 Snort 3로 마이그레이션, 2 페이지

LSP 업데이트의 Snort 3 규칙 변경

정기 Snort 3 침입 규칙 LSP 업데이트 중에 기존 시스템 정의 침입 규칙이 새 침입 규칙으로 교체될 수 있습니다. 단일 규칙이 여러 규칙으로 교체되거나 여러 규칙이 단일 규칙으로 교체될 가능성이 있습니다. 이는 규칙을 결합하거나 확장하여 탐지가 개선될 수 있는 경우에 이루어집니다. 관리를 개선하기 위해 LSP 업데이트 과정에서 일부 기존 시스템 정의 규칙이 제거될 수 있습니다.

LSP 업데이트 중에 재정의된 시스템 정의 규칙의 변경 사항에 대한 알림을 받으려면 **Retain user overrides for deleted Snort 3 rules**(삭제된 Snort 3 규칙에 대한 사용자 재정의 유지) 체크 박스가 선택되어 있는지 확인합니다. 시스템 기본값으로 이 체크 박스는 선택되어 있습니다. 이 체크 박스를 선택하면 시스템은 LSP 업데이트의 일부로 추가된 새 교체 규칙에서 규칙 재정의의 유지를 유지합니다. 알림은 **Tasks**(작업) 탭의 **Cog**(톱니바퀴)() 옆에 있는 **Notifications**(알림) 아이콘 아래에 표시됩니다.

Retain user overrides for deleted Snort 3 rules(삭제된 Snort 3 규칙에 대한 사용자 재정의 유지) 체크 박스로 이동하려면 **Cog**(톱니바퀴)()를 클릭한 다음 **Configuration**(구성) > **Intrusion Policy Preferences**(침입 정책 기본 설정)를 선택합니다.

Firepower 권장 규칙 정보

Firepower 침입 규칙 권장 사항을 사용하여 네트워크에서 탐지된 호스트 에셋 관련 취약성을 대상으로 지정할 수 있습니다. 운영체제, 서버, 클라이언트 애플리케이션 프로토콜을 예로 들 수 있습니다. 침입 정책을 모니터링되는 네트워크의 특정 요구를 조정할 수 있게 합니다.

시스템에서 각 IPS 정책에 대한 권장 사항 개별 집합을 만듭니다. 일반적으로 표준 텍스트 규칙 및 공유 개체 규칙에 대한 규칙 상태 변경을 권장합니다. 그런데 검사기 및 디코더 규칙에 대한 변경 사항을 권장할 수도 있습니다.

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

- 취약성에 대한 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 Firepower 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 Cisco Talos(Talos Intelligence Group)는 시스템 제공 정책에서 각 규칙의 적절한 상태를 결정합니다. 시스템 제공 정책을 사용 하여 기본 정책으로 시스템 Firepower 권장 규칙 상태에 규칙을 설정 하도록 허용 하는 경우 네트워크 자산 대 한 Cisco에서 권장 하는 설정을 IPS 정책 규칙에 일치 합니다.

Snort 2에서 생성된 Firepower 권장 사항을 Snort 3로 마이그레이션

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

Firepower 권장 사항은 Snort 3 버전에 대해 직접 생성할 수 없습니다. Snort 2 버전의 침입 정책에 대한 Firepower 권장 사항을 생성한 다음 여기에 나와 있는 단계에 따라 Snort 3로 권장 규칙 설정을 마이그레이션합니다.

시작하기 전에

Firepower 권장 사항에는 다음 요구 사항이 있습니다.

- FTD 라이선스 - 위협
- 기본 라이선스 - 보호
- 사용자 역할 - 관리자 또는 침입 관리자

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

단계 2 침입 정책의 **Snort 2 Version(Snort 2 버전)** 버튼을 클릭합니다.

단계 3 침입 정책의 Snort 2 버전에서 권장 사항을 생성하고 적용합니다.

최신 버전의 *Firepower Management Center* 구성 가이드에서 *Firepower* 권장 사항 생성 및 적용 항목을 참조하고 해당 항목에 나온 단계를 수행하십시오.

단계 4 Snort 2 규칙 변경 사항을 Snort 3와 동기화합니다.

관련 단계는 [Snort 2 규칙](#)과 [Snort 3 동기화](#) 항목을 참조하십시오.

다음에 수행할 작업

컨피그레이션 변경사항을 구축합니다. [컨피그레이션 변경 사항 구축](#)를 참고하십시오.

