네트워크 자산에 대한 침입 방지 맞춤화

이 장에서는 Secure Firewall 권장 규칙과 Secure Firewall 권장 규칙을 생성 및 적용하는 방법에 대한 인사이트를 제공합니다.

LSP 업데이트의 Snort 3 규칙 변경

정기 Snort 3 LSP(Lightweight Security Package) 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.

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.

기본적으로 이 체크 박스는 선택되어 있습니다. 이 체크 박스를 선택하면 시스템은 LSP 업데이트의 일부로 추가된 새 교체 규칙에서 규칙 재정의를 유지합니다. 알림은 **Tasks(**작업**)** 탭의 **Cog(**톱니바퀴**)(**⚙**)** 옆에 있는 Notifications(알림) 아이콘 아래에 표시됩니다.

Secure Firewall 권장 규칙 개요

침입 규칙 권장 사항을 사용하여 네트워크에서 탐지된 호스트 자산 관련 취약성을 대상으로 지정할 수 있습니다. 운영 체제, 서버, 클라이언트 애플리케이션 프로토콜을 예로 들 수 있습니다. 이를 통해 모니터링되는 네트워크의 특정 요구에 맞게 침입 정책을 조정할 수 있습니다.

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 때 기본 설정을 사용하거나 고급 설정을 구성할 수 있습니다. 고급 설정을 수행할 수 있습니다.

- 취약성에 대한 네트워크에 있는 호스트 시스템 모니터링 재정의
- 규칙 오버헤드에 따라 시스템이 권장하는 규칙 영향
- 규칙을 비활성화하기 위한 권장 생성을 활성화할지 지정

또한 권장 사항을 즉시 사용하거나 권장 사항(및 영향을 받는 규칙)을 검토한 후 수락하도록 선택할 수 있습니다.

권장 규칙 상태를 사용하도록 선택하면 읽기 전용 Secure Firewall 권장 사항 레이어가 침입 정책에 추가되고 이후 권장 규칙 상태를 사용하지 않기로 선택하면 레이어가 제거됩니다.

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

시스템은 다음과 같이 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 보고서는 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 기본 정책으로 사용하여 시스템에서 Secure Firewall 권장 규칙 상태에 규칙을 설정하도록 허용하는 경우 네트워크 자산에 대해 권장하는 설정을 침입 정책 규칙에 일치시킵니다.

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 3에서 새로운 Secure Firewall 권장 사항 생성

침입 정책에 대한 Secure Firewall 권장 사항을 생성한 다음 여기에 나열된 단계에 따라 Snort 3에서 새 권장 규칙 설정을 만듭니다. 규칙 오버헤드는 Snort 3에서 사용자가 선택한 임계값 정책을 기반으로 하는 보안 레벨로 해석됩니다. 권장 작업은 선택한 보안 레벨을 기반으로 하며, 기본 정책보다 높은 경우 권장 사항은 이벤트 생성에만 국한되지 않습니다.

Secure Firewall 권장 사항을 설정하기 전에 아래에 나열된 세 가지 사항 중 목표에 가장 일치하는 것이 무엇인지 자문해야 합니다.

- Increased Protection(보호 강화) - 호스트 데이터베이스에서 발견된 취약성을 기반으로 추가 규칙을 활성화하고 규칙을 자동으로 비활성화하지 않습니다. 이로 인해 규칙 집합이 커질 수 있습니다.
- Focused Protection(보호 우선) - 호스트 데이터베이스에서 발견된 취약성에 따라 추가 규칙을 활성화하며 기존 규칙을 비활성화합니다. 이렇게 하면 검색된 취약성에 따라 규칙 수를 늘리거나 줄일 수 있습니다.
- Higher Efficency(고효율) - 현재 활성화된 규칙 집합을 사용하고 호스트 데이터베이스에 없는 취약성에 대한 규칙은 모두 비활성화합니다. 이로 인해 활성화된 규칙 집합의 크기가 작아질 수 있습니다.

응답을 기반으로 하는 권장 작업은 다음과 같습니다.

- 권장 사항을 다음으로 가장 높은 보안 레벨로 설정하고 규칙 비활성화의 선택을 취소합니다.
- 권장 사항을 다음으로 가장 높은 보안 레벨로 설정하고 규칙 비활성화를 확인합니다.
- 권장 사항을 현재 보안 레벨로 설정하고 규칙 비활성화를 확인합니다.

시작하기 전에

Secure Firewall 권장 사항에는 다음 요구 사항이 있습니다.

- 권장 사항을 생성하려면 시스템에 호스트가 있는지 확인합니다.
- 권장 사항에 대해 구성된 보호받는 네트워크는 시스템에 있는 호스트에 매핑되어야 합니다.

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

단계 **2** 침입 정책의 **Snort 3 Version(Snort 3 버전)** 버튼을 클릭합니다.

단계 **3** **Recommendations (Not in Use)(**권장 사항**(**사용되지 않음**))** 레이어를 클릭하여 규칙 권장 사항을 구성합니다. **Start(**시작**)**를 클릭합니다.

Secure Firewall Rule Recommendations(Secure Firewall Firepower 규칙 권장 사항) 창에서 다음을 설정할 수 있습니다.

- **Security Level(**보안 레벨**)**: 보안 레벨을 선택하려면 클릭합니다. 필요에 따라, 입력 보안 레벨 및 보호된 네트워크에서 활성화되지 않은 규칙을 비활성화하려면 **Accept Recommendation to Disable Rules(**규칙을 비활성화하라는 권장 사항 수락**)** 체크 박스를 선택할 수 있습니다. 많은 알림 수로 인해 규칙 집합을 잘라내거나 검사 성능을 개선해야 하는 경우에만 이 옵션을 활성화하십시오. 보안 레벨은 다음과 같습니다.
  - 보안 레벨 1: Connectivity over Security(연결이 보안에 우선함)

    No Impact(영향 없음**)** - 새 규칙이 활성화되지 않으며 기존 규칙이 비활성화되지 않습니다. 보호를 강화하려면 더 높은 보안 레벨을 선택하십시오.

    Low Security(낮은 보안 수준**)**(체크 박스 선택됨) - 검색된 호스트의 잠재적 취약성과 일치하는 Connectivity Over Security(연결이 보안에 우선함) 규칙 집합의 규칙을 제외하고 모든 규칙이 비활성화됩니다. 대신 기본 정책을 조정하는 것이 좋습니다.
  - 보안 레벨 2: Balanced Security Over Connectivity(균형 잡힌 보안이 연결에 우선함)

    No Impact(영향 없음**)** - 새 규칙이 활성화되지 않으며 기존 규칙이 비활성화되지 않습니다. 보호를 강화하려면 더 높은 보안 레벨을 선택하십시오.

    Higher Efficiency(효율성 향상**)**(체크 박스 선택됨) - 검색된 호스트에서 잠재적인 취약점과 일치하는 기존 규칙을 유지하고 네트워크에서 찾을 수 없는 취약점에 대한 규칙을 비활성화합니다.
  - 보안 레벨 3: Security Over Connectivity(보안이 연결에 우선함)

    Increased Security(보안 강화**)** - Maximum Detection(최대 탐지) 규칙 집합을 기반으로 검색된 호스트에서 잠재적인 취약점과 일치하는 추가 규칙을 활성화합니다.

    Focused Security(보안 우선**)**(체크 박스 선택됨) - Security over Connectivity(보안이 연결에 우선함) 규칙 집합을 기반으로 검색된 호스트의 취약점과 일치하는 추가 규칙을 활성화하면서 검색된 호스트의 잠재적인 취약점과 일치하지 않는 기존 규칙은 비활성화합니다.
  - 보안 레벨 4: Maximum Detection(최대 탐지)

    Increased Security(보안 강화**)** - Security over Connectivity(보안이 연결에 우선함) 규칙 집합을 기반으로 검색된 호스트에서 잠재적인 취약점과 일치하는 추가 규칙을 활성화합니다.

    Focused Security(보안 우선**)**(체크 박스 선택됨) - Maximum Detection(최대 탐지) 규칙 집합을 기반으로 검색된 호스트의 취약점과 일치하는 추가 규칙을 활성화하면서 검색된 호스트의 잠재적인 취약점과 일치하지 않는 기존 규칙은 비활성화합니다.

    참고 Maximum Detection(최대 탐지)은 매우 많은 규칙을 활성화하며 성능에 영향을 미칠 수 있습니다. 생산 환경에 구축하기 전에 이 설정을 검토하고 테스트하는 것이 좋습니다.

- **Protected Networks(**보호되는 네트워크**)**: 권장 사항을 위해 검사할 모니터링 중인 네트워크 또는 개별 호스트를 지정합니다. 드롭다운 목록에서 하나 이상의 시스템 또는 사용자 정의한 네트워크 개체를 선택할 수 있습니다. 따로 선택하지 않은 경우 기본적으로 IPv4 또는 IPv6 네트워크가 선택됩니다.

중요 Secure Firewall 규칙 권장 사항은 네트워크 검색에 따라 다릅니다. Protected Networks(보호되는 네트워크)는 네트워크 검색 정책에 구성한 범위 내에서 검색된 모든 호스트에 적용됩니다. 자세한 내용은 *Cisco Secure Firewall Management Center* 디바이스 구성 가이드의 네트워크 검색 정책 장을 참조하십시오.

Add +(추가 **+)** 버튼을 클릭하여 호스트 또는 네트워크 유형의 새 네트워크 개체를 생성하고 **Save(**저장**)**를 클릭합니다.

단계 **4** 권장 사항을 생성하고 적용합니다.

- **Generate(**생성**)**: 침입 정책에 대한 권장 사항을 생성합니다. 이 작업은 Recommended Rules (Not in use)(권장 규칙(사용되지 않음)) 아래에 규칙을 나열합니다.
- **Generate and Apply(**생성 및 적용**)**: 침입 정책에 대한 권장 사항을 생성하고 적용합니다. 이 작업은 Recommended Rules (In use)(권장 규칙(사용 중)) 아래에 규칙을 나열합니다.

권장 사항이 생성되었습니다. 모든 권장 규칙 및 해당 권장 작업이 포함된 새 권장 사항 탭이 나타납니다. 이 탭에서 새로운 권장 사항과 함께 규칙 작업 프리셋 필터도 사용할 수 있습니다.

단계 **5** 권장 사항을 확인한 다음 적절하게 적용하도록 선택할 수 있습니다.

- **Accept(**수락**)** - 침입 정책에 대해 이전에 생성된 권장 사항을 적용합니다.
- **Refresh(**새로 고침**)** - 침입 정책에 대한 규칙 권장 사항을 다시 생성하고 업데이트합니다.
- **Edit(**편집**)** - 권장 사항 입력 값을 제공한 다음 권장 사항을 생성할 수 있는 Recommendations(권장 사항) 대화 상자를 엽니다.
- **Remove All(**모두 제거**)** - 적용된 권장 규칙을 되돌리거나 정책에서 제거하며, Recommendations(권장 사항) 탭도 제거합니다.

All Rules(모든 규칙**)** 아래의 Recommended Rules(권장 규칙) 섹션에 권장 규칙이 나와 있습니다.

참고 침입 규칙에 대한 최종 작업은 규칙 작업 우선순위에 따라 적용되며 규칙 작업 우선순위는 다음과 같습니다.

Rule Override(규칙 재정의) > Generated Recommendations(생성된 권장 사항) > Group Override(그룹 재정의) > Base Policy Default Action(기본 정책 기본 작업)

활성화된 권장 사항의 경우 management center에서는 현재 상태(그룹 재정의, 기본 정책, 권장 사항 구성)를 고려하며 작업의 우선순위는 다음과 같습니다.

pass(통과) > block(차단) > reject(거부) > drop(삭제) > rewrite(재작성) > alert(알림)

다음에 수행할 작업

구성 변경 사항을 구축합니다. 구성 변경 사항 구축를 참고하십시오.

번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.