Secure Firewall Management Center에서 Snort 3 권장 사항 생성

Snort 3 규칙 권장 사항

규칙 권장 사항은 호스트 환경과 관련된 규칙을 사용하여 침입 정책을 자동으로 조정합니다. 네트워크에 없는 취약성에 대한 규칙을 비활성화하여 추가 규칙을 활성화하거나 현재 규칙 집합을 조정할 수 있습니다. 자세한 내용은 Secure Firewall 권장 규칙 개요를 참고하십시오.

어떻게 프로그램을 사용할 수 있습니까?

Management Center는 IP 주소, 호스트 이름, 운영 체제, 서비스, 사용자, 클라이언트 애플리케이션과 같은 세부 정보를 사용하여 네트워크의 호스트 데이터베이스를 수동 검색을 통해 구축합니다. 시스템은 이 정보를 기반으로 검색된 각 호스트에 취약성을 매핑합니다. 권장 사항 기능은 이 호스트 데이터베이스를 사용하여 환경에 적용할 규칙을 결정합니다.

Snort 3에는 네 가지 보안 레벨이 있으며, 각 보안 레벨은 특정 Talos 정책에 해당합니다. 다음과 같습니다.

- 레벨 1 - Connectivity over Security(연결이 보안에 우선함)
- 레벨 2 - Balanced Security and Connectivity(균형 잡힌 보안 및 연결성)
- 레벨 3 - Security over Connectivity(보안이 연결에 우선함)
- 레벨 4 - Maximum Detection(최대 탐지)

Accept Recommendations to Disable Rules(규칙 비활성화를 위한 권장 사항 수락**)** 체크 박스를 선택하여 네트워크의 호스트에 없는 취약성에 대한 규칙을 비활성화합니다. 많은 알림 수로 인해 규칙 집합을 잘라내야 하거나 검사 성능을 개선하려는 경우에만 이 옵션을 선택하십시오.

이점

- 권장 사항을 구성하면 호스트 환경과 관련된 규칙을 사용하여 특정 위협 유형을 더욱 효과적으로 탐지하도록 침입 정책을 맞춤화할 수 있습니다.
- 권장 사항은 오탐 및 미탐을 줄여 인시던트 대응 프로세스의 효율성과 효과를 높입니다.

샘플 비즈니스 시나리오

대규모 기업 네트워크에서는 Snort 3를 기본 침입 탐지 및 방지 시스템으로 사용합니다. 빠르게 진화하는 위협 환경에서는 강력한 네트워크 보안 조치를 채택해야 합니다. 이 보안 팀은 사고 대응 기능을 개선하고자 합니다. 이를 수행하는 방법 중 하나는 호스트 네트워크에서 탐지된 취약성을 기반으로 권장 사항 또는 규칙 집합을 생성하는 것입니다. 이를 통해 침입 정책을 최적화하여 네트워크를 보다 효과적으로 보호할 수 있습니다.

모범 사례

- 정확한 품질의 호스트 데이터가 있어야 합니다.

  네트워크 검색의 수동 특성으로 인해 Threat Defense 디바이스는 보호되는 호스트와 최대한 가깝게 배치해야 합니다. 그러면 Threat Defense 디바이스가 이러한 호스트를 오가는 네트워크 트래픽을 감시할 수 있으며, 따라서 네트워크에 있는 애플리케이션, 서비스, 취약점에 대한 정확한 데이터를 얻을 수 있습니다.
- 디바이스는 이스트-웨스트 및 노스-사우스 트래픽 플로우에 대한 가시성이 있어야 정확한 호스트 프로파일을 구축할 수 있습니다.
- 권장 사항을 자동으로 업데이트하도록 예약된 작업을 생성할 수 있습니다.

사전 요구 사항

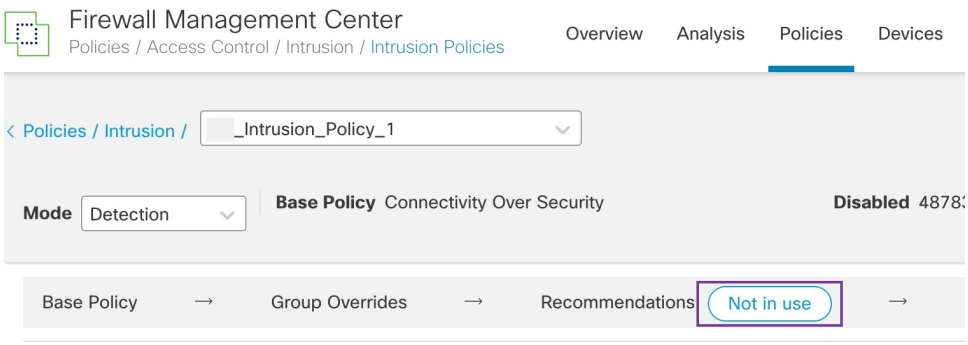
- 권장 사항을 생성하려면 시스템에 호스트가 있는지 확인합니다.
- 권장 사항에 대해 구성된 보호받는 네트워크는 시스템에 있는 호스트에 매핑되어야 합니다.

Snort 3 권장 사항 생성

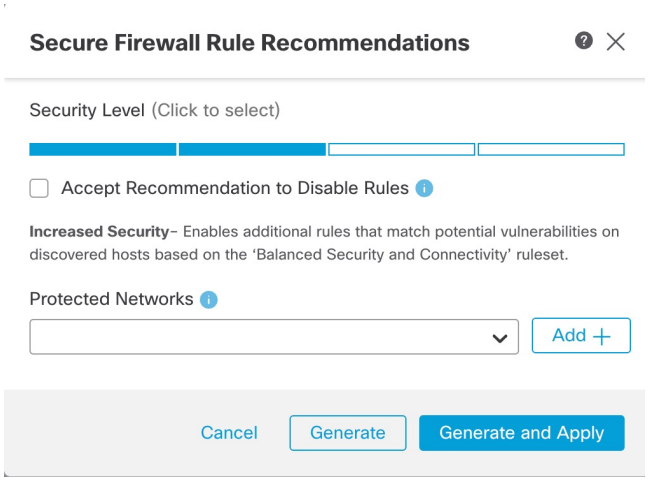
단계 1 **Policies(정책)** > **Intrusion(침입)**을 선택합니다.

단계 2 해당하는 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.



Cisco Recommended Rules(Cisco 권장 규칙) 창에서 보안 레벨을 설정할 수 있습니다.



단계 4 클릭하여 보안 레벨을 선택합니다.

단계 5 (선택 사항) 네트워크의 호스트에 없는 취약성에 대해 작성된 규칙을 비활성화하려면 **Accept Recommendation to Disable Rules(규칙 비활성화를 위한 권장 사항 수락)** 체크 박스를 선택합니다.

많은 알림 수로 인해 규칙 집합을 잘라내야 하거나 검사 성능을 개선하려는 경우에만 이 옵션을 사용하십시오.

단계 6 **Protected Networks(보호되는 네트워크)** 드롭다운 목록에서 권장 사항에서 검사해야 하는 네트워크 개체를 선택합니다. 따로 선택하지 않은 경우 기본적으로 IPv4 또는 IPv6 네트워크가 선택됩니다.

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

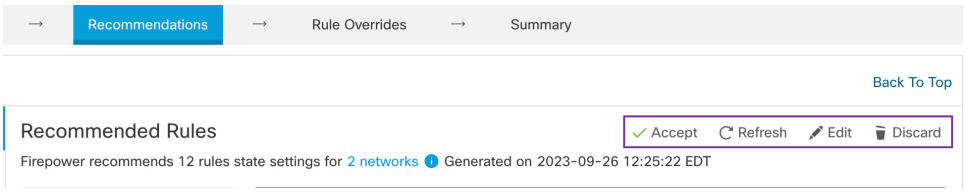
단계 7 권장 사항을 생성하고 적용합니다.

- **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 (Not in use)(**권장 규칙**(**사용되지 않음**))** 아래에 규칙을 나열합니다.

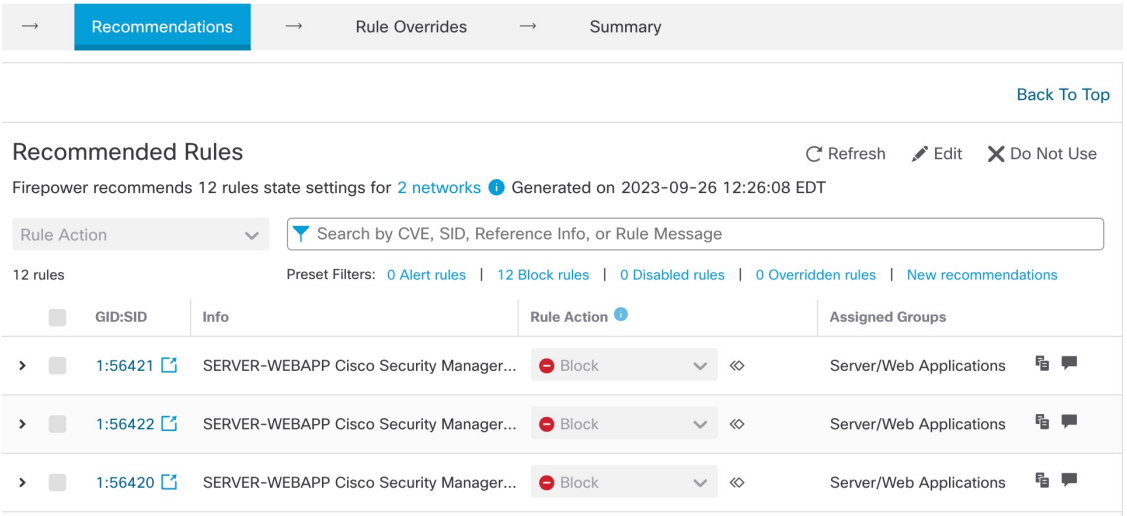
권장 사항이 생성되었습니다. 모든 권장 규칙 및 해당 권장 작업이 포함된 새 권장 사항 탭이 나타납니다. 이 탭에서 새로운 권장 사항 외에도 규칙 작업 프리셋 필터를 사용할 수 있습니다.

단계 **8** 권장 사항을 확인한 다음 적절하게 적용합니다.

- **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.
- **Discard(**폐기**)** - 적용된 권장 규칙을 되돌리거나 정책에서 제거합니다. **Recommendations(**권장 사항**)** 탭도 제거합니다.



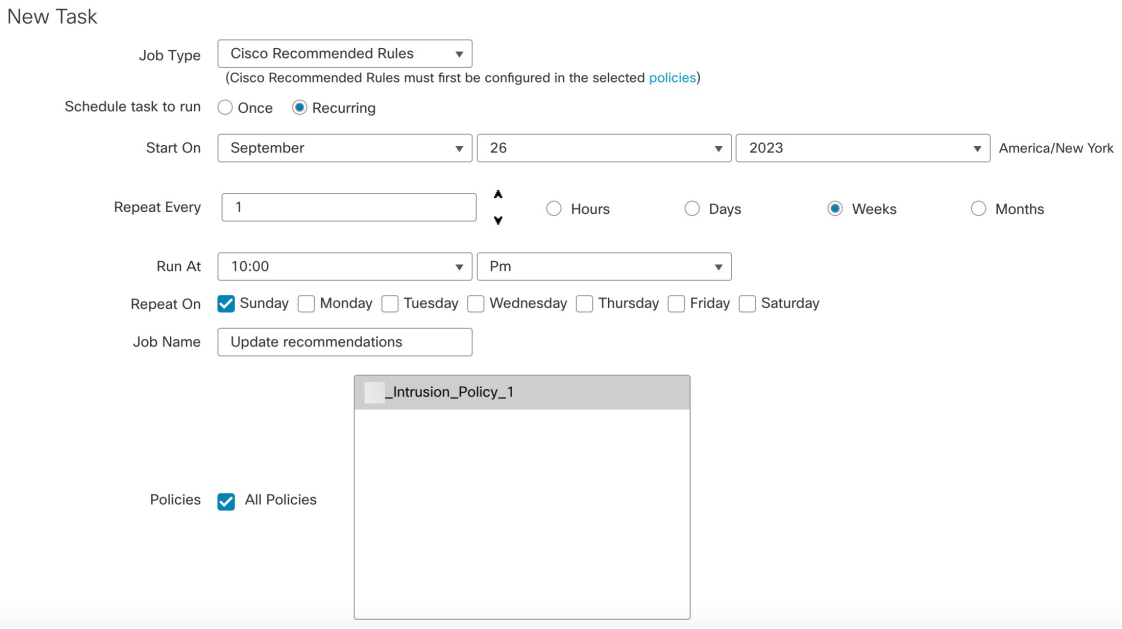
All Rules(모든 규칙**)** 아래의 Recommended Rules(권장 규칙) 섹션에 권장 규칙이 나와 있습니다.



단계 **9** 권장 사항을 효과적으로 사용하려면 주기적으로 업데이트해야 합니다. 다음 단계를 수행합니다.

1. **System(**시스템**) >Tools(**툴**) > Scheduling(**예약**)**을 선택합니다.
2. **Add Task(**작업 추가**)**를 클릭합니다.

3. **Job Type(**작업 유형**)** 드롭다운 목록에서 **Cisco Recommended Rules(Cisco** 권장 규칙**)**를 선택합니다.
4. 필요에 따라 필수 필드를 업데이트합니다.



5. **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참조하십시오.

구성 변경 사항 구축

구성을 변경한 후 해당하는 디바이스에 구축합니다.

참고 이 주제에서는 구성 변경 사항 구축과 관련된 기본 단계를 다룹니다. 최신 버전의 *Cisco Secure Firewall Management Center* 구성 가이드에서 구성 변경 사항 구축 주제를 참조하여 단계를 진행하기 전에 변경 사항 구축의 사전 요건과 영향을 파악할 것을 강력하게 권장합니다.

주의 구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 구성을 구축하면 Snort 프로세스가 재시작되므로 트래픽 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다.

단계 **1** Secure Firewall Management Center 메뉴 모음에서 **Deploy(**구축**)**를 클릭하고 **Deployment(**구축**)**를 선택합니다.

GUI 페이지에는 **Pending(**보류 중**)** 상태인 오래된 구성이 있는 디바이스가 나열됩니다.

- **Modified By(**수정 주체**)** 열에는 정책 또는 개체를 수정한 사용자가 나열됩니다. 디바이스 목록을 확장하여 각 정책 목록에 대한 정책을 수정한 사용자를 볼 수 있습니다.

  참고 삭제된 정책 및 개체에 대해서는 사용자 이름이 제공되지 않습니다.

- **Inspect Interruption(**검사 중단**)** 열은 구축 중에 디바이스에서 트래픽 검사 중단이 발생할 수 있는지 여부를 나타냅니다.

  디바이스에 대한 이 열이 비어 있으면 구축 중에 해당 디바이스에서 트래픽 검사가 중단되지 않음을 나타냅니다.

- **Last Modified Time(**마지막 수정 시간**)** 열은 구성 변경을 마지막으로 수행한 시간을 지정합니다.
- **Preview(**미리보기**)** 열에서는 다음 구축에 대한 변경 사항을 미리 볼 수 있습니다.
- **Status(**상태**)** 열은 각 구축의 상태를 제공합니다.

단계 **2** 구성 변경 사항을 구축할 디바이스를 식별하여 선택합니다.

- Search(검색)-검색 상자에서 디바이스 이름, 유형, 도메인, 그룹 또는 상태를 검색합니다.
- Expand(확장)-구축할 디바이스별 구성 변경 사항을 보려면 확장 화살표( )를 클릭합니다.

디바이스에 인접한 체크박스를 선택하면 디바이스에 대해 이루어지고 디바이스 아래에 나열된 모든 변경 사항이 구축을 위해 푸시됩니다. 그러나 정책 선택( )을 사용하면 구축하지 않고 나머지 변경 사항을 보류하면서 구축할 개별 정책 또는 특정 구성을 선택할 수 있습니다.

참고

- **Inspect Interruption(**검사 중단**)** 열의 상태가 **(Yes(**예**))**인 경우(구축하면 위협 방어 디바이스에서 검사가 중단되며 트래픽도 중단될 수 있음) 확장된 목록에서 검사 중단( ) 중단을 야기하는 특정 구성을 표시합니다.
- 인터페이스 그룹, 보안 영역 또는 개체가 변경되면 영향을 받는 디바이스는 management center에서 오래된 것으로 표시됩니다. 이러한 변경 사항을 적용하려면 이러한 인터페이스 그룹, 보안 영역 또는 개체가 포함된 정책도 이러한 변경 사항과 함께 구축해야 합니다. 영향을 받는 정책은 management center의 **Preview(**미리보기**)** 페이지에서 만료된 것으로 표시됩니다.

단계 **3** **Deploy(**구축**)**를 클릭합니다.

단계 **4** 구축할 변경 사항에서 오류나 경고를 식별하면 시스템은 **Validation Messages(**검증 메시지**)** 창에 이를 표시합니다. 전체 세부 사항을 보려면 경고 또는 오류 앞에 있는 화살표 아이콘을 클릭합니다.

다음 옵션을 이용할 수 있습니다.

- Deploy(구축) - 경고 조건을 해결하지 않고 구축을 계속합니다. 오류가 식별되는 경우 계속 진행할 수 없습니다.
- Close(닫기) - 구축하지 않고 종료합니다. 오류 및 경고 조건을 해결하고 구성을 재구축합니다.

다음에 수행할 작업

구축 중에 구축 장애가 발생하는 경우 해당 장애가 트래픽에 영향을 미칠 수 있습니다. 그러나 특정 조건에 따라 달라집니다. 구축의 특정 구성이 변경된 경우 구축 장애로 인해 트래픽이 중단될 수 있습니다. 자세한 내용은 최신 버전의 *Cisco Secure Firewall Management Center* 구성 가이드에 있는 구성 변경 사항 구축 주제를 참조하십시오.