MITRE 프레임워크를 사용하여 Secure FMC에서 잠재적 위협을 확인하고 조치를 취합니다.

목차

소개

이 문서에서는 MITRE 프레임워크를 사용하여 안전한 FMC(Firepower 관리 센터)에서 잠재적 위협을 보고 이에 대한 조치를 취하는 방법에 대해 설명합니다.

배경 정보

MITER ATT&CK(Adversarial Tactics, Techniques, and Common Knowledge) 프레임워크는 시스템을 손상시키는 것을 목표로 하는 위협 행위자가 배포한 전술, 기술 및 절차(TTP)에 대한 통찰력을 제공하는 방대한 지식 기반 및 방법론입니다. ATT&CK는 각각 운영 체제 또는 특정 플랫폼을 나타내는 행렬로 컴파일됩니다. "전술"이라고 하는 공격의 각 단계는 이러한 단계를 달성하는 데 사용되는 특정 방법, 즉 "기술"에 매핑됩니다.

ATT&CK 프레임워크의 각 기술에는 기술, 관련 절차, 가능한 방어 및 탐지, 실제 예에 대한 정보가 수반됩니다. MITER ATT&CK 프레임워크는 또한 그룹이 사용하는 전술 및 기법 세트에 따라 위협 그룹, 활동 그룹 또는 위협 행위자를 지칭하도록 그룹을 통합합니다. Groups(그룹)를 사용하면 프레임워크를 통해 동작을 분류하고 문서화할 수 있습니다.

MITRE에 대한 자세한 내용은 https://attack.mitre.org을 참조하십시오.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Snort에 대한 지식
- 보안 FMC

- FTD(Secure Firepower Threat Defense)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 이 문서는 모든 Firepower 플랫폼에 적용됩니다
- 소프트웨어 버전 7.3.0을 실행하는 보안 FTD
- 소프트웨어 버전 7.3.0을 실행하는 FMC(Secure Firepower Management Center Virtual)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

MITRE Framework의 이점

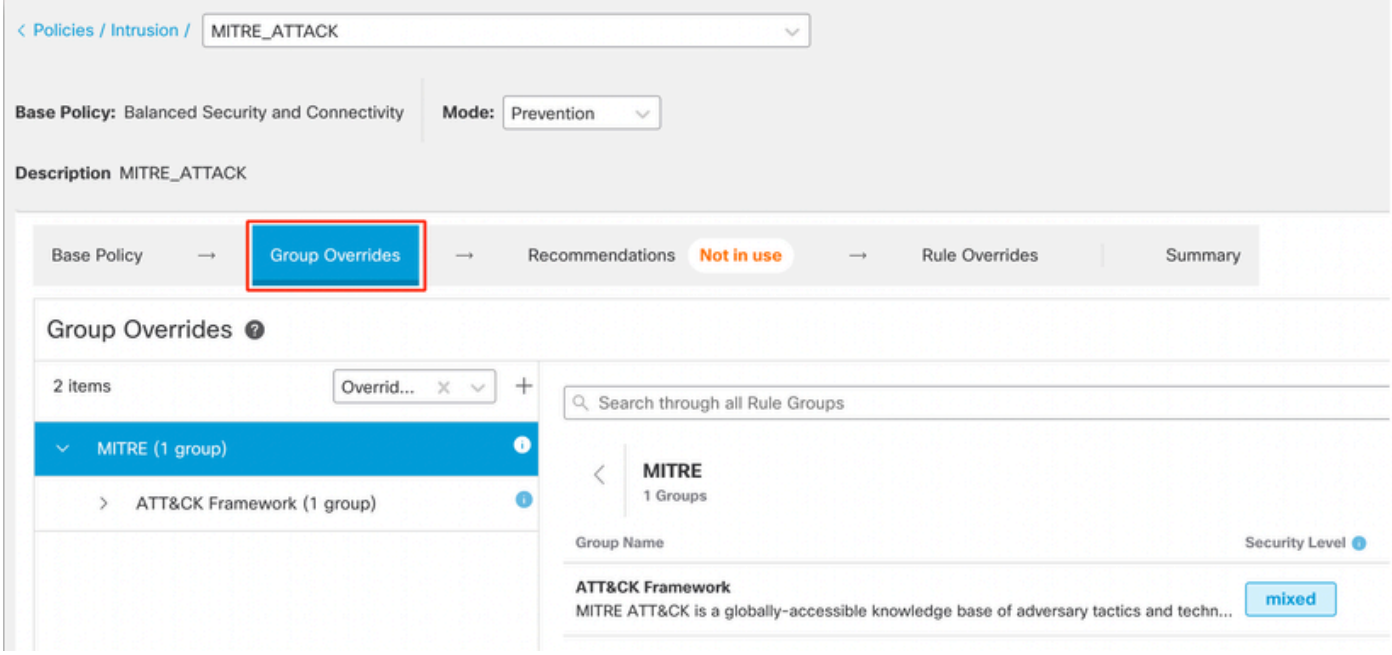
- 관리자가 MITER ATT&CK(Against Tactics Techniques and Common Knowledge) 프레임워크를 기반으로 트래픽에 대한 조치를 취할 수 있도록 하는 침입 이벤트에 MITER TTP(Tactics, Techniques, and Procedures)가 추가됩니다. 이를 통해 관리자는 더욱 세분화된 방식으로 트래픽을 보고 처리할 수 있으며, 취약성 유형, 대상 시스템 또는 위협 카테고리별로 규칙을 그룹화할 수 있습니다.
- MITER ATT&CK 프레임워크에 따라 침입 규칙을 구성할 수 있습니다. 이를 통해 특정 공격자 전술 및 기법에 따라 정책을 사용자 지정할 수 있습니다.

침입 정책에서 MITRE 프레임워크 보기

MITER 프레임워크를 사용하면 침입 규칙을 탐색할 수 있습니다. MITRE는 규칙 그룹의 또 다른 카테고리일 뿐이며 Talos 규칙 그룹의 일부입니다. 여러 레벨의 규칙 그룹에 대한 규칙 탐색이 지원되므로 더 유연하고 논리적으로 규칙을 그룹화할 수 있습니다.

1. 선택합니다Policies > Intrusion.
2. 탭이Intrusion Policies선택되었는지 확인합니다.
3. 보거나 수정할 침입 정책 옆에Snort 3 Version있는 을 클릭합니다. 표시되는 Snort 헬퍼 가이드를 닫습니다.
4. 레이어를Group Overrides클릭합니다.

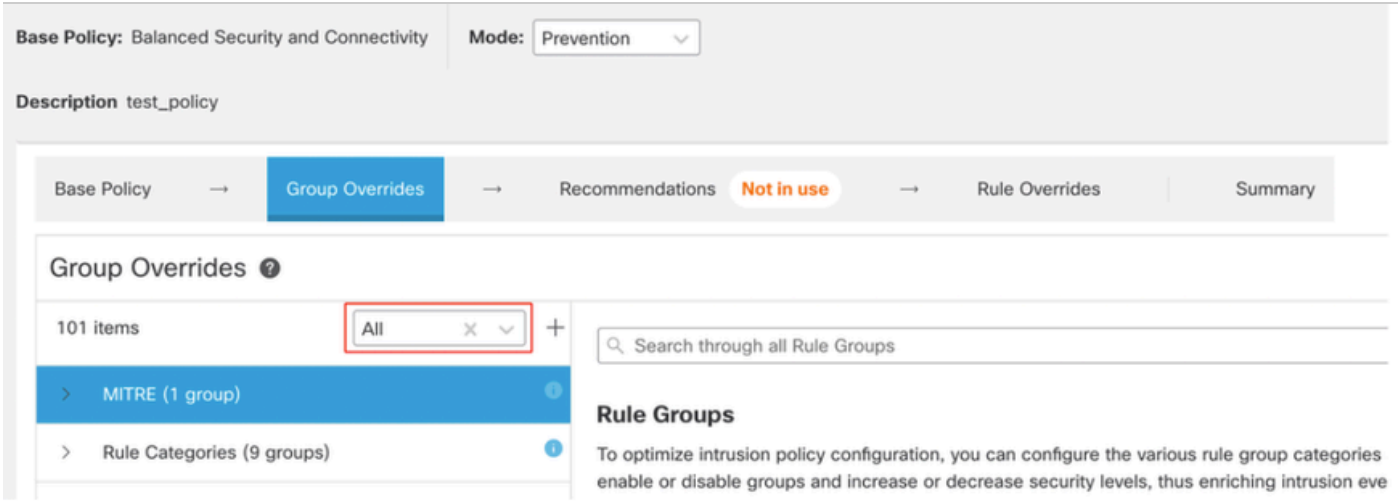
레이어Group Overrides는 규칙 그룹의 모든 범주를 계층 구조로 나열합니다. 각 규칙 그룹의 마지막 리프 규칙 그룹으로 트래버스할 수 있습니다.



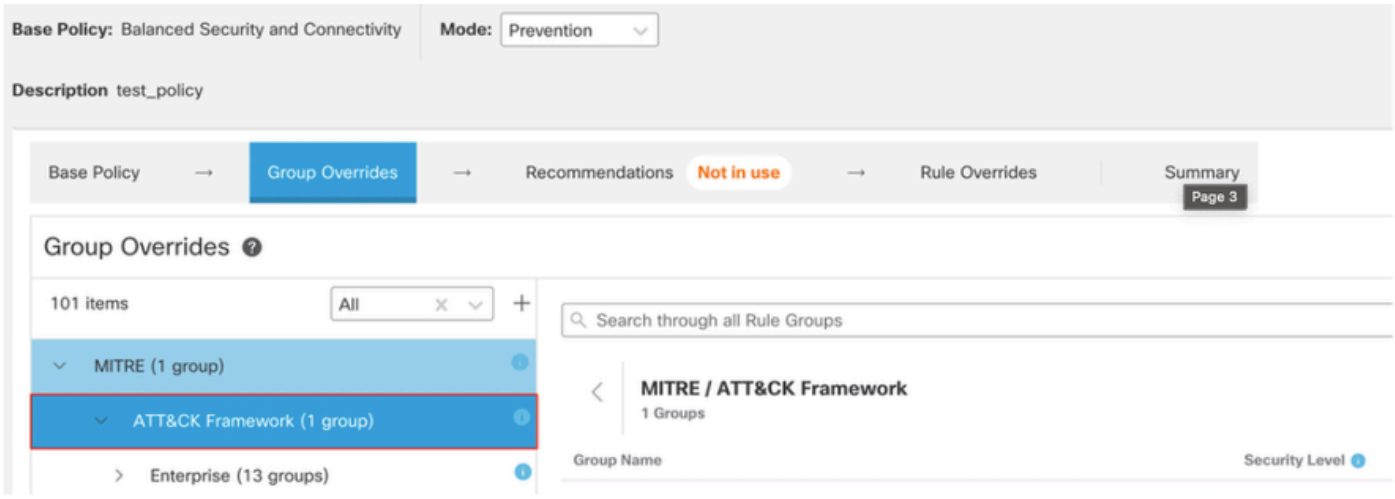
6. 아래에서Group Overrides다음을 확인합니다. All드롭다운 목록에서 선택되므로 침입 정책에 대한 모든 규칙 그룹이 왼쪽 창에 표시됩니다.

7. 클릭 MITRE왼쪽 창에 표시됩니다.

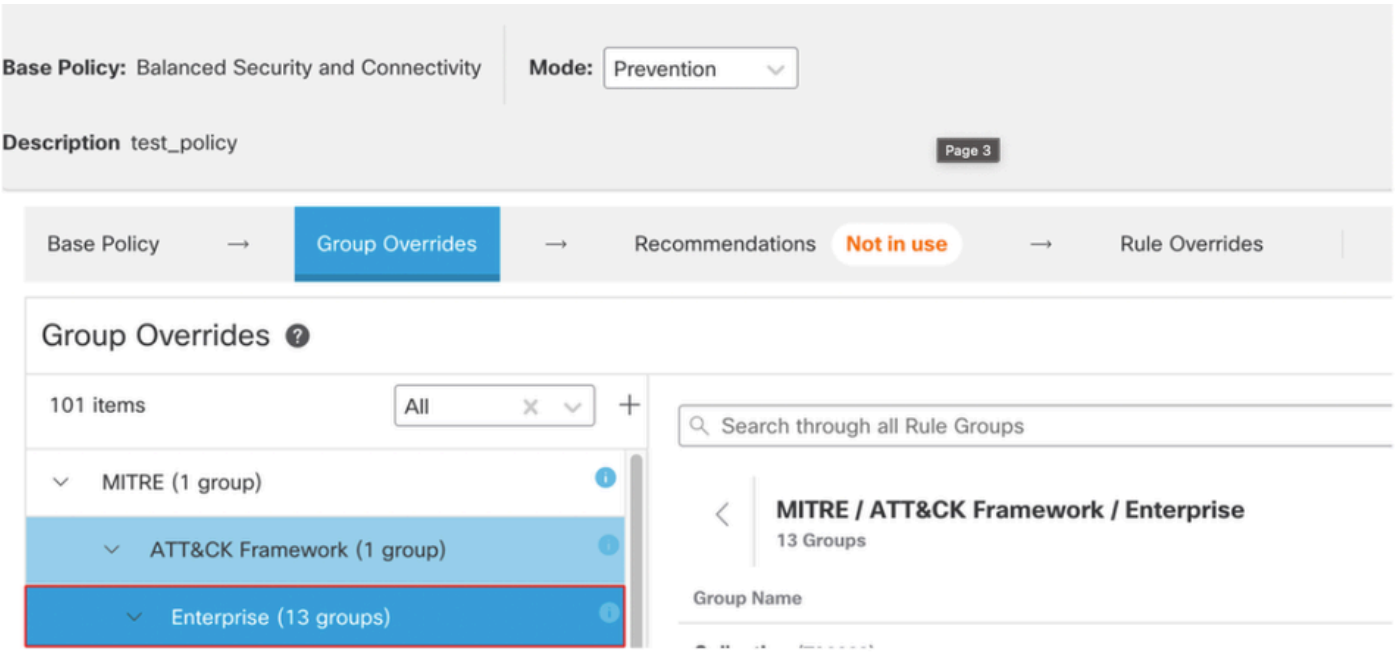
참고: 이 예에서는 MITRE가 선택되지만 특정 요구 사항에 따라 Rule Categories(규칙 카테고리) 규칙 그룹 또는 그 아래에 있는 다른 규칙 그룹 및 후속 규칙 그룹을 선택할 수 있습니다. 모든 규칙 그룹은 MITRE 프레임워크를 사용합니다.



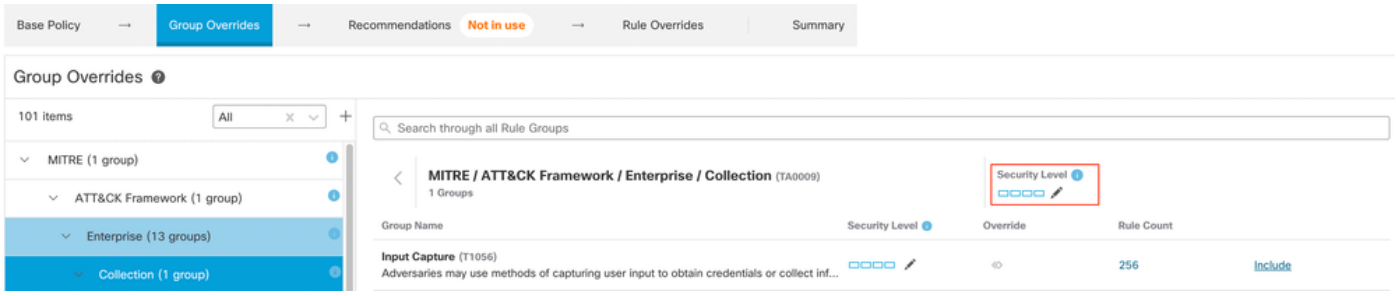
8. 아래에서MITRE프레임워크를 클릭하여ATT&CK확장합니다.



9. 아래에서ATT&CK FrameworkEnterprise를 클릭하여 확장합니다.

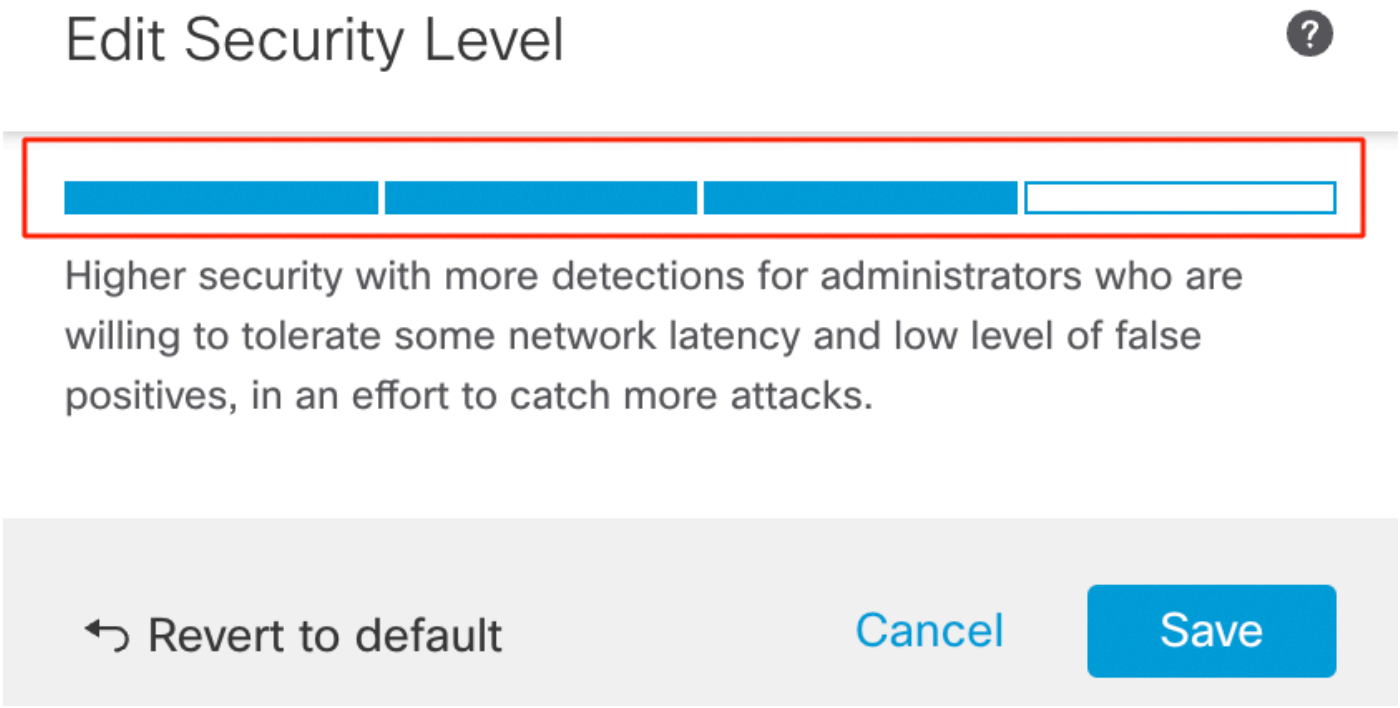


10.Edit ( ) 규칙 그룹의 보안 수준 옆에 있는 을 눌러 모든 연결된 규칙 그룹에 대한 보안 수준을 일괄 변경합니다. Enterprise규칙 그룹 범주.



보안 규칙 그룹 편집

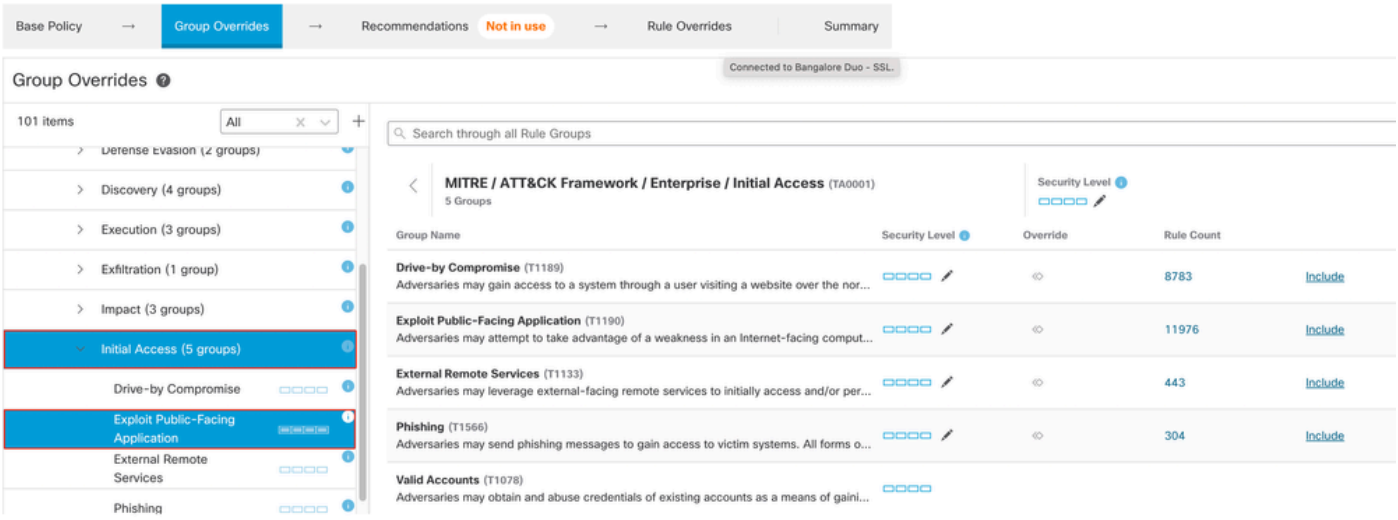
11. 예를 들어, 창에서 보안 레벨 3을 선택하고Edit Security Level을 **Save**클릭합니다.



보안 수준

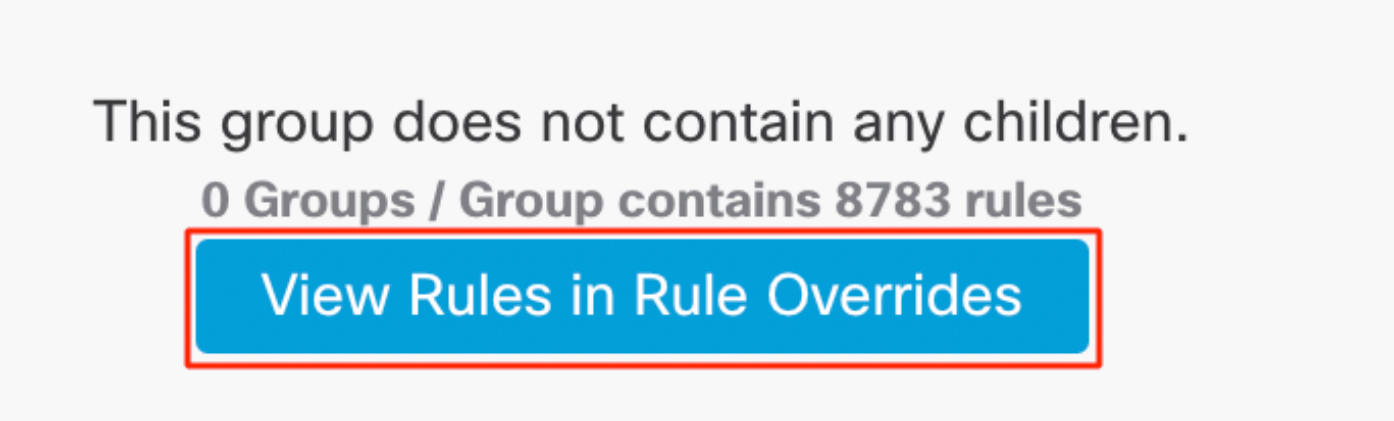
12. 아래에서Enterprise를 클릭하여 Initial Access확장합니다.

13. 아래에서Initial Access마지막 리프 그룹인 을 클릭합니다Exploit Public-Facing Application.



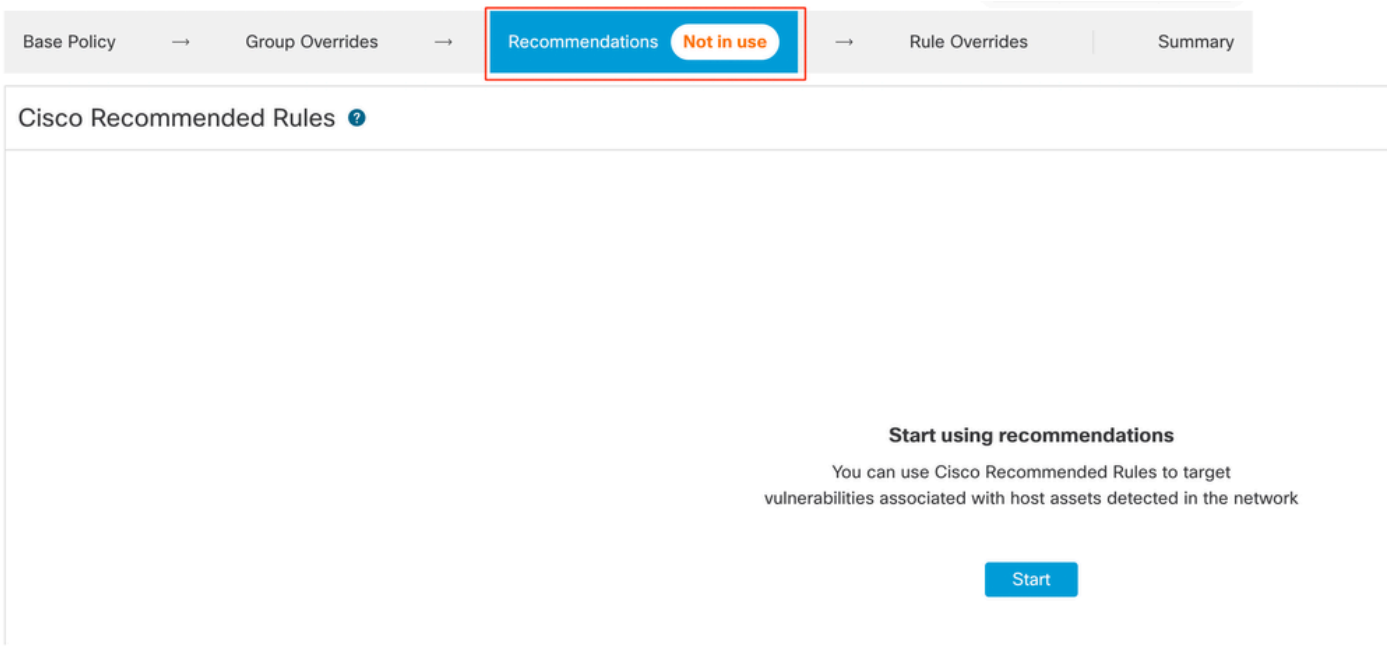
초기 액세스 그룹

14. 다음을 클릭합니다. **View Rules in Rule Overrides**단추를 클릭하면 다른 규칙에 대한 다른 규칙, 규칙 세부사항, 규칙 작업 등을 볼 수 있습니다.

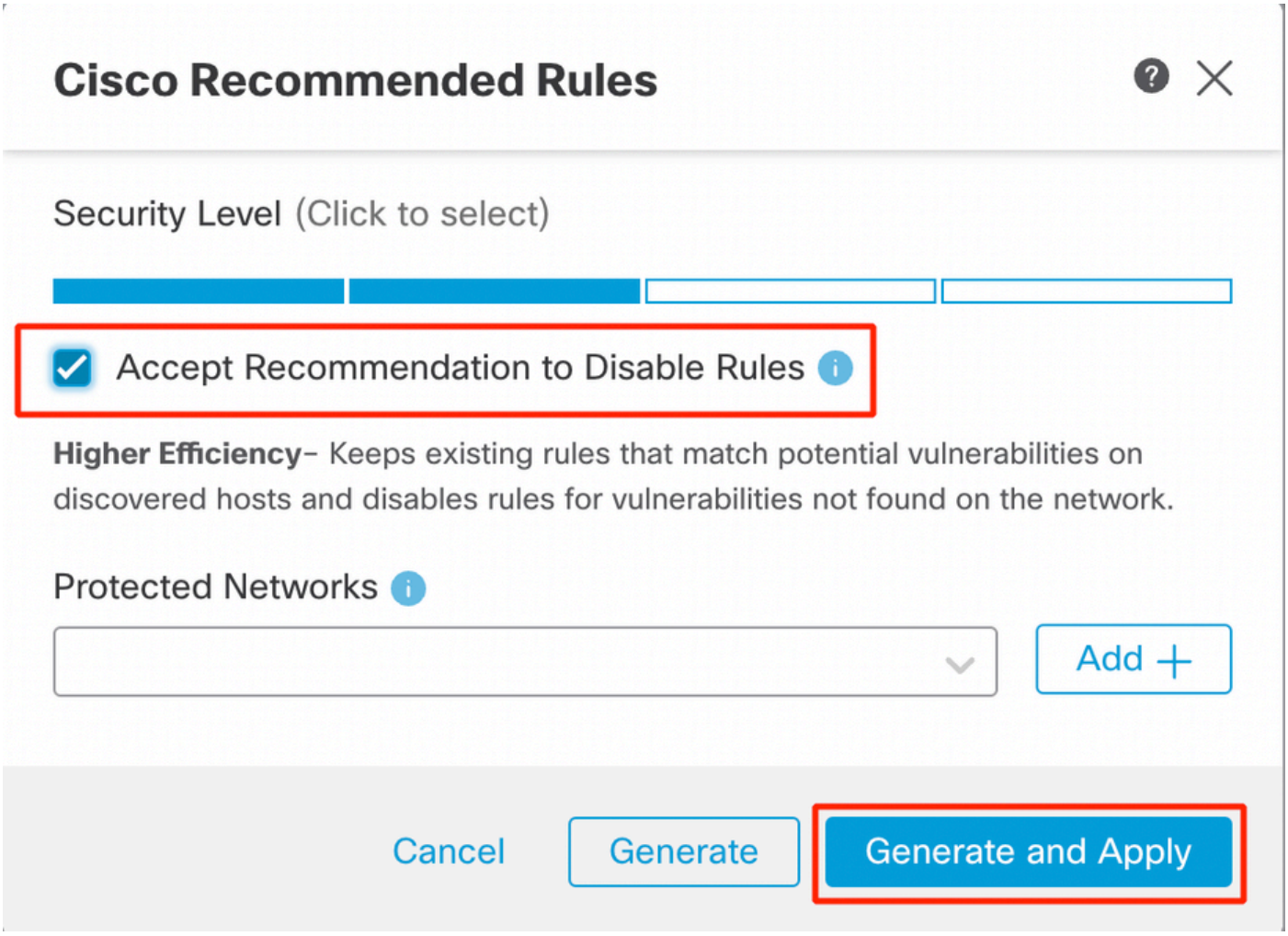


규칙 재정의의 규칙

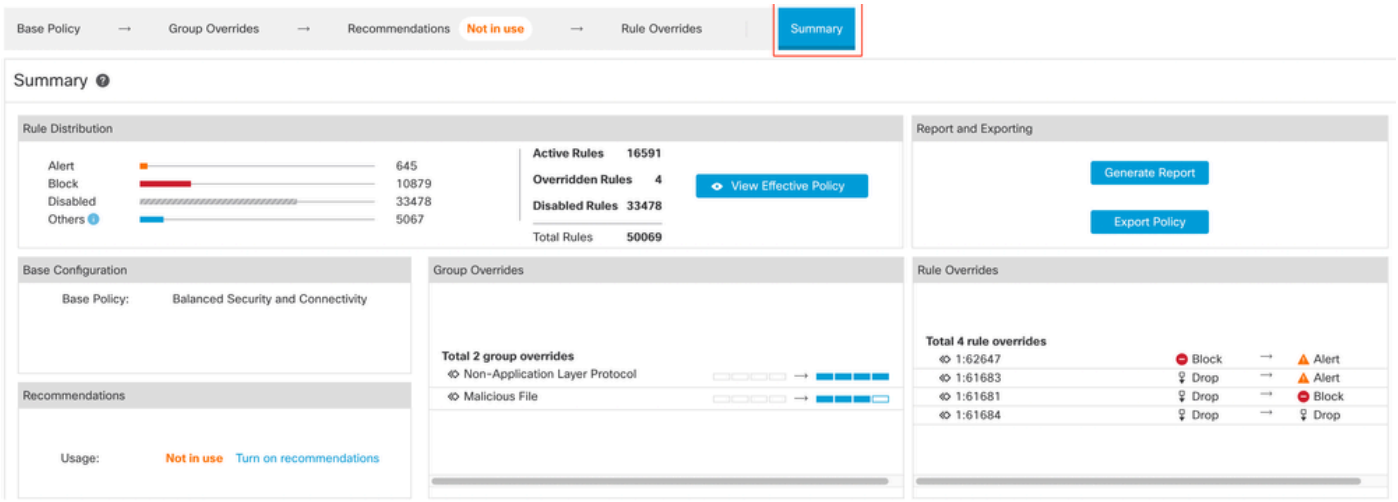
15. RecommendationsCisco 권장 규칙을 사용하려면 레이어를 클릭한 다음Start클릭합니다. 침입 규칙 권장 사항을 사용하여 네트워크에서 탐지된 호스트 자산과 관련된 취약성을 대상으로 지정할 수 있습니다. 추가 정보.



권장 사항



16. 다음을 클릭합니다. Summary레이어 - 정책에 대한 현재 변경 사항을 종합적으로 볼 수 있습니다. 정책의 규칙 배포, 그룹 재정의, 규칙 재정의 등을 볼 수 있습니다.



정책 요약

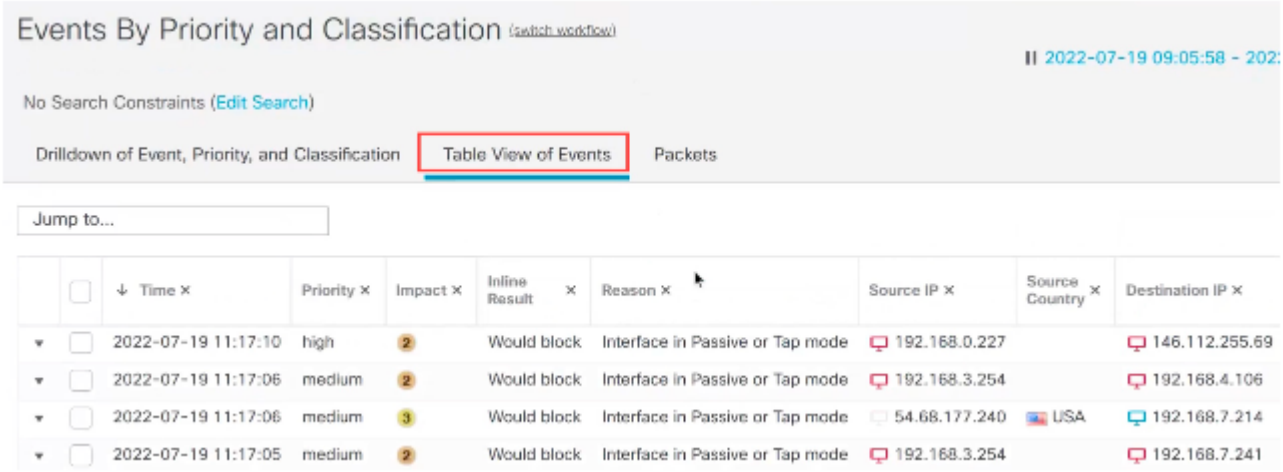
침입 이벤트 보기

Classic Event Viewer 및 Unified Event Viewer의 침입 이벤트에서 MITER ATT&CK 기술과 규칙 그룹을 볼 수 있습니다. Talos는 Snort 규칙(GID:SID)에서 MITER ATT&CK 기술 및 규칙 그룹으로의 매핑을 제공합니다. 이러한 매핑은 LSP(Lightweight Security Package)의 일부로 설치됩니다.

시작하기 전에 Snort 규칙에 의해 트리거된 이벤트를 탐지하고 기록하기 위해 침입 및 액세스 제어 정책을 구축해야 합니다.

1. 을Analysis > Intrusions > Events클릭합니다.

2. **Table View of Events**탭에 표시됩니다.



이벤트

3. MITRE ATT&CK열 머리글에서는 침입 이벤트에 대한 기술을 볼 수 있습니다.

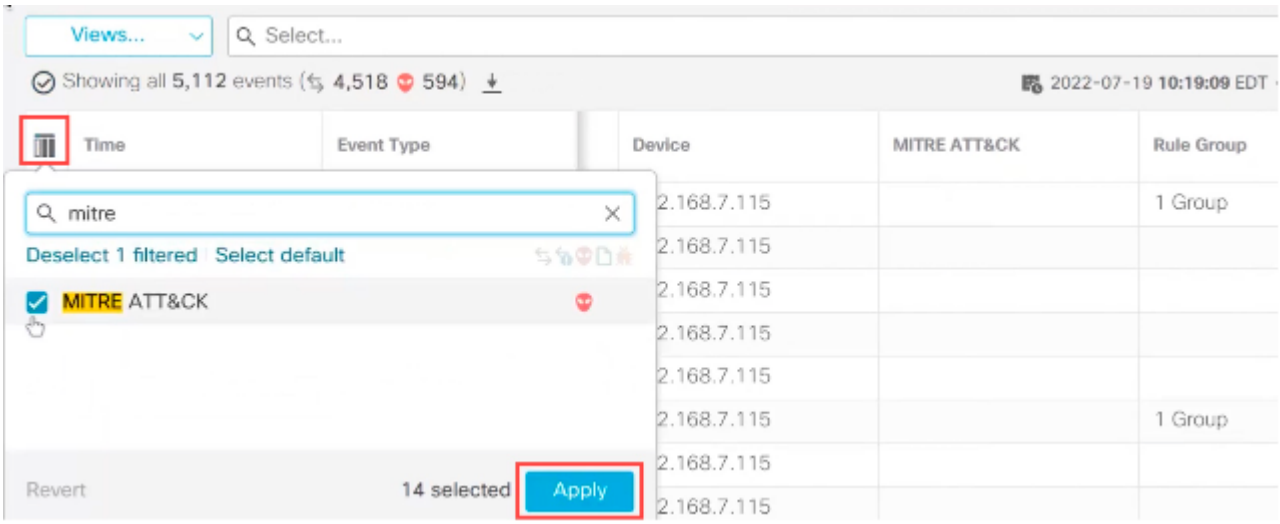
사접 열 머리글

4. 클릭 1 Technique이 그림과 같이 MITER ATT&CK 기법을 볼 수 있습니다. 이 예에서는 Exploit Public-Facing Application바로 기술입니다.

사접 ATT&CK 기법

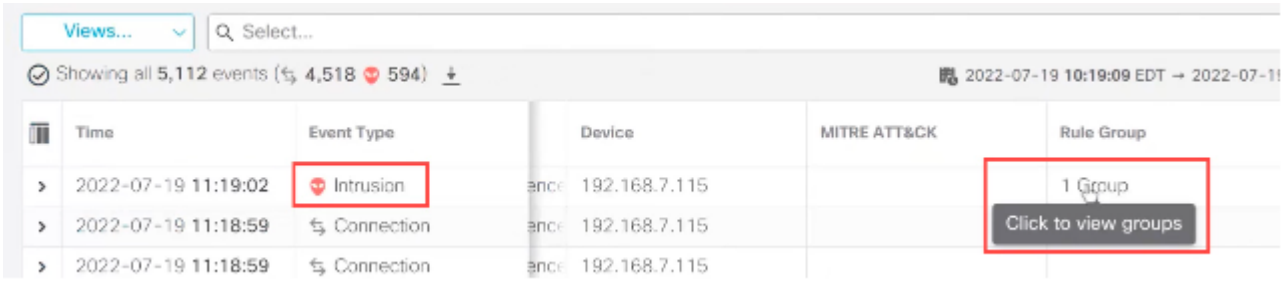
5. 을Close클릭합니다.

6. 을Analysis > Unified Events클릭합니다.
7. 열 선택기 아이콘을 눌러MITRE ATT&CK및 열을 사용할 수Rule Group있습니다.



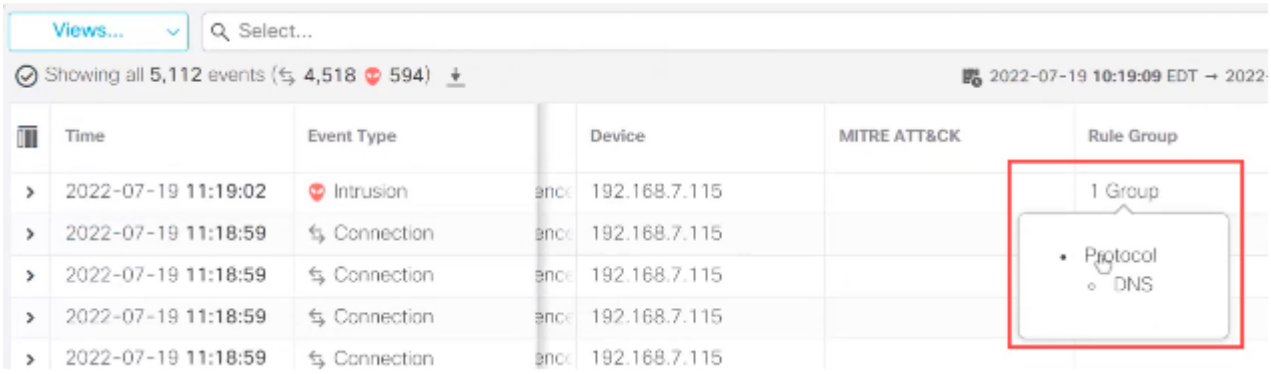
사접 공격 사용

8. 이 예에서 보여주는 것처럼, 침입 이벤트는 하나의 규칙 그룹에 매핑된 이벤트에 의해 트리거되었습니다. 다음1 Group 에서 클릭하십시오. Rule Group열.



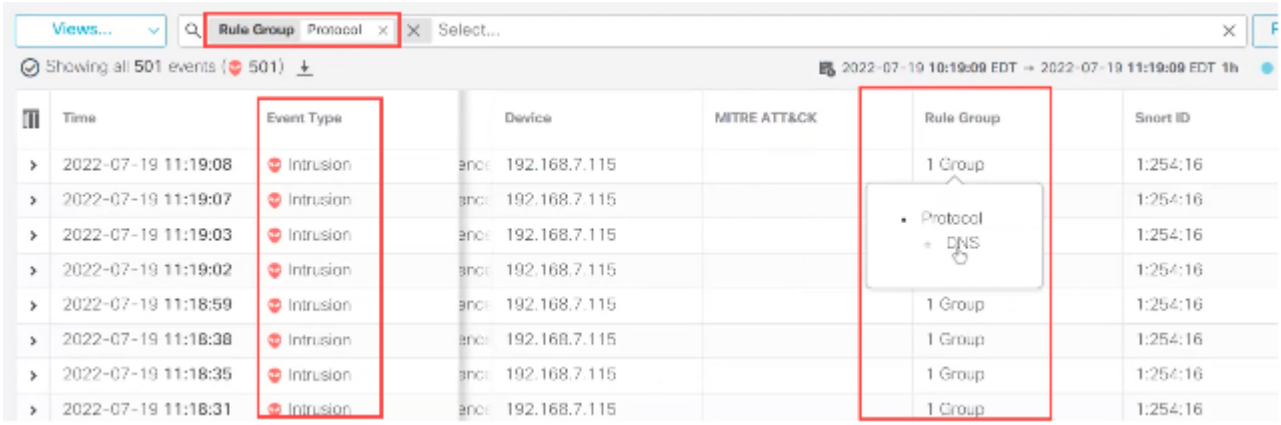
규칙 그룹

9. 예를 들어 상위 규칙 그룹인 Protocol과 그 아래의 DNS 규칙 그룹을 볼 수 있습니다.



프로토콜 보기

10. 하나 이상의 규칙 그룹이 있는 모든 침입 이벤트, 즉 를 클릭하여Protocol검색할 수 있습니다Protocol > DNS. 검색 결과가 여기에 표시된 예와 같이 표시됩니다.


Views...
Rule Group Protocol
Select...
Showing all 501 events (501)
2022-07-19 10:19:09 EDT → 2022-07-19 11:19:09 EDT 1h
Time
Event Type
Device
MITRE ATT&CK
Rule Group
Snort ID
2022-07-19 11:19:08 Intrusion 192.168.7.115 1 Group 1:254:16
2022-07-19 11:19:07 Intrusion 192.168.7.115 1:254:16
2022-07-19 11:19:03 Intrusion 192.168.7.115 1:254:16
2022-07-19 11:19:02 Intrusion 192.168.7.115 1:254:16
2022-07-19 11:18:59 Intrusion 192.168.7.115 1 Group 1:254:16
2022-07-19 11:18:38 Intrusion 192.168.7.115 1 Group 1:254:16
2022-07-19 11:18:35 Intrusion 192.168.7.115 1 Group 1:254:16
2022-07-19 11:18:31 Intrusion 192.168.7.115 1 Group 1:254:16
Protocol
DNS

규칙 그룹 프로토콜

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.