SCADA 프리프로세서

다음 주제에서는 SCADA(감독 제어 및 데이터 획득) 프로토콜용 전처리기와 이를 구성하는 방법을 설명합니다.

- SCADA 전처리기 소개, 1 페이지
- SCADA 전처리기 라이선스 요구 사항, 2 페이지
- SCADA 전처리기 요구 사항 및 사전 요건, 2 페이지
- Modbus 전처리기, 2 페이지
- DNP3 전처리기, 5 페이지
- CIP 전처리기, 7 페이지
- S7Commplus 전처리기, 11 페이지

SCADA 전처리기 소개

참고 이 섹션은 Snort 2 전처리기에 적용됩니다. Snort 3 관리자에 대한 자세한 내용은 https://www.cisco.com/go/snort3-inspectors를 참조하십시오.

Supervisory Control(감시 제어) 및 Data Acquisition(데이터 획득. SCADA) 프로토콜은 제조, 생산, 정수처리, 배전, 공항 및 배송 시스템 등과 같은 산업, 인프라 및 설비의 데이터를 모니터링하고, 제어하며, 획득합니다. Firepower System은 전처리기에 Modbus, DNP3(Distributed Network Protocol), CIP(Common Industrial Protocol), S7Commplus SCADA 프로토콜을 제공하며, 이러한 프로토콜은 네트워크 분석 정책의 일부로 설정할 수 있습니다.

Modbus, DNP3, CIP 또는 S7Commplus 전처리기가 비활성화되고, 이러한 전처리기가 필요한 침입 규칙을 사용자가 활성화 및 구축하면 시스템은 해당 전처리기를 현재 설정을 바탕으로 자동으로 사용합니다. 단, 대응하는 네트워크 분석 정책에 대한 웹 인터페이스에서는 전처리기가 계속 비활성화됩니다.

SCADA 전처리기 라이선스 요구 사항

Threat Defense 라이선스

IPS

기본 라이선스

보호

SCADA 전처리기 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모두

사용자 역할

- 관리자
- 침입 관리자

Modbus 전처리기

참고 이 섹션은 Snort 2 전처리기에 적용됩니다. Snort 3 관리자에 대한 자세한 내용은 https://www.cisco.com/go/snort3-inspectors를 참조하십시오.

Modbus 프로토콜은 1979년 Modicon에 의해 처음 게시되어 널리 사용되는 SCADA 프로토콜입니다. Modbus 전처리기는 Modbus 트래픽 내 이상 징후를 탐지하고 규칙 엔진에 의한 처리를 위해 Modbus 프로토콜을 디코딩하는데, 특정 프로토콜 필드에 액세스하기 위해 Modbus 키워드를 사용합니다.

단일 구성 옵션을 사용하면 전처리기가 Modbus 트래픽을 검사할 포트에 대한 기본 설정을 변경할 수 있습니다.

관련 항목

SCADA 키워드

Modbus 전처리기 포트 옵션

포트

전처리기가 Modbus 트래픽을 검사하는 포트를 지정합니다. 포트가 여러 개인 경우 쉼표로 구분하십시오.

Modbus 전처리기 구성

참고 이 섹션은 Snort 2 전처리기에 적용됩니다. Snort 3 관리자에 대한 자세한 내용은 https://www.cisco.com/go/snort3-inspectors를 참조하십시오.

네트워크가 Modbus가 활성화된 디바이스를 포함하지 않는 경우, 트래픽에 적용한 네트워크 분석 정책에서 이 전처리기를 활성화해선 안 됩니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 편집하려는 정책 옆의 **Snort 2 Version(Snort 2** 버전**)**을 클릭합니다.

단계 **3** 수정하려는 정책 옆에 있는 **Edit(**수정**)** ( )를 클릭합니다.

View(보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 **5** **SCADA Preprocessors(SCADA** 전처리기**)**의 **Modbus Configuration(Modbus** 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **6** **Modbus Configuration(Modbus** 설정**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **7** **Ports(**포트**)** 필드에 값을 입력합니다.

쉼표로 여러 개의 값을 구분합니다.

단계 **8** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

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

다음에 수행할 작업

- 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하고 싶다면 Modbus 전처리기 규칙(GID 144)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정 및 Modbus 전처리기 규칙, 4 페이지의 내용을 참조하십시오.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

레이어 관리

충돌 및 변경: 네트워크 분석 및 침입 정책

Modbus 전처리기 규칙

이러한 규칙에서 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하려면 다음 표에서 Modbus 전처리기 규칙을 활성화해야 합니다.

표 ***1: Modbus*** 전처리기 규칙

전처리기 규칙 **GID:SID**	설명
144:1	Modbus 헤더 내 길이가 Modbus 기능 코드가 요청하는 길이에 일치하지 않을 경우 이벤트를 생성합니다. 각 Modbus 기능에는 요청과 응답에 대한 예상된 형식이 있습니다. 메시지 길이가 예상된 형식과 일치하지 않는 경우 이 이벤트가 생성됩니다.
144:2	Modbus 프로토콜 ID가 0이 아닐 때 이벤트를 생성합니다. 프로토콜 ID 필드는 Modbus로 다른 프로토콜을 다중화하는 데 사용됩니다. 전처리기가 다른 프로토콜을 처리하지 않으므로, 이 이벤트가 대신 생성됩니다.
144:3	전처리기가 예약된 Modbus 기능 코드를 탐지하면 이벤트를 생성합니다.

DNP3 전처리기

참고 이 섹션은 Snort 2 전처리기에 적용됩니다. Snort 3 관리자에 대한 자세한 내용은 https://www.cisco.com/go/snort3-inspectors를 참조하십시오.

Distributed Network Protocol(DNP3)은 원래 전력발전소 간 일관된 커뮤니케이션을 제공하기 위해 개발된 SCADA 프로토콜입니다. DNP3은 또한 상수도산업, 산업 폐기물 처리업, 운송 산업 및 많은 기타 업계에서 널리 사용되고 있습니다.

DNP3 전처리기는 DNP3 트래픽 내 이상 징후를 탐지하고 규칙 엔진에 의한 처리를 위해 DNP3 프로토콜을 디코딩하는데, 특정 프로토콜 필드에 액세스하기 위해 DNP3 키워드를 사용합니다.

관련 항목

DNP3 키워드

DNP3 전처리기 옵션

포트

각 지정된 포트의 DNP3 트래픽 검사를 활성화합니다. 단일 포트 또는 쉼표로 구분된 포트 목록을 지정할 수 있습니다.

잘못된 **CRC** 로깅

DNP3 링크 레이어 프레임에 포함된 체크섬을 검증합니다. 유효하지 않은 체크섬을 가진 프레임은 무시됩니다.

규칙 145:1을 활성화하여 잘못된 체크섬이 탐지된 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

DNP3 전처리기 구성

참고 이 섹션은 Snort 2 전처리기에 적용됩니다. Snort 3 관리자에 대한 자세한 내용은 https://www.cisco.com/go/snort3-inspectors를 참조하십시오.

네트워크가 DNP3가 활성화된 디바이스를 포함하지 않는 경우, 트래픽에 적용한 네트워크 분석 정책에서 이 전처리기를 활성화해선 안 됩니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 1 **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 2 편집하려는 정책 옆의 **Snort 2 Version(Snort 2** 버전**)**을 클릭합니다.

단계 3 수정하려는 정책 옆에 있는 **Edit(**수정**)** ( )를 클릭합니다.

View(보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 4 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 5 **SCADA Preprocessors(SCADA** 전처리기**)**의 **DNP3 Configuration(DNP3** 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 6 **DNP3 Configuration(DNP3** 설정**)** 옆에 있는 **Edit(**수정**)** ( )을(를) 클릭합니다.

단계 7 **Ports(**포트**)**에 대한 값을 입력합니다.

쉼표로 여러 개의 값을 구분합니다.

단계 8 **Log bad CRCs(**배드 **CRC** 로그**)** 확인란을 선택하거나 선택 취소합니다.

단계 9 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

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

다음에 수행할 작업

- 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하고 싶다면 DNP3 전처리기 규칙(GID 145)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정, DNP3 전처리기 옵션, 5 페이지 및 DNP3 전처리기 규칙, 7 페이지를 참고하십시오.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

레이어 관리
충돌 및 변경: 네트워크 분석 및 침입 정책

DNP3 전처리기 규칙

이러한 규칙에서 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하려면 다음 표에서 DNP3 전처리기 규칙을 활성화해야 합니다.

표 *2: DNP3* 전처리기 규칙

전처리기 규칙 **GID:SID**	설명
145:1	**Log bad CRC(**잘못된 **CRC** 로깅**)**를 활성화한 경우 전처리기가 유효하지 않은 체크섬을 통해 연결 레이어 프레임을 탐지하면 이벤트를 생성합니다.
145:2	전처리기가 유효하지 않은 길이로 DNP3 연결 레이어 프레임을 탐지하면 이벤트를 생성하고 패킷을 차단합니다.
145:3	전처리기가 유효하지 않은 시퀀스 번호로 전송 레이어 세그먼트를 탐지하면 이벤트를 생성하고 리어셈블리 중에 패킷을 차단합니다.
145:4	완전한 조각이 리어셈블되기 전에 DNP3 리어셈블리 버퍼가 지워지면 이벤트를 생성합니다. 이는 다른 세그먼트가 대기된 후 FIR 플래그를 전송하는 세그먼트가 나타날 때 발생합니다.
145:5	전처리기가 예약된 주소를 사용하는 DNP3 연결 레이어 프레임을 탐지하면 이벤트를 생성합니다.
145:6	전처리기가 예약된 기능 코드를 사용하는 DNP3 요청 또는 응답을 탐지하면 이벤트를 생성합니다.

CIP 전처리기

참고 이 섹션은 Snort 2 전처리기에 적용됩니다. Snort 3 관리자에 대한 자세한 내용은 https://www.cisco.com/go/snort3-inspectors를 참조하십시오.

CIP(Common Industrial Protocol)는 산업 자동화 애플리케이션을 지원하는, 다양한 분야에서 사용하는 애플리케이션 프로토콜입니다. ENIP(EtherNet/IP)는 이더넷 기반 네트워크에서 사용하는 CIP를 구현한 결과물입니다.

CIP 전처리기는 TCP 또는 UDP에서 실행하는 CIP와 ENIP를 탐지하고 침입 규칙 엔진에 전송합니다. 맞춤형 침입 규칙에서 CIP 및 ENIP 키워드를 이용하면 CIP와 ENIP 트래픽에서의 공격을 탐지할 수 있습니다. CIP and ENIP Keywords(CIP 및 ENIP 키워드)의 내용을 참조하십시오. 또한 액세스 컨트롤 규칙에서 CIP 및 ENIP 애플리케이션 조건을 지정하여 트래픽을 제어할 수도 있습니다. 애플리케이션 조건 및 필터 구성의 내용을 참조하십시오.

CIP 전처리기 옵션

포트

CIP 및 ENIP 트래픽을 검사할 포트를 지정합니다. 0부터 65535까지의 정수를 지정할 수 있습니다. 포트 번호가 여러 개인 경우 쉼표로 구분하십시오.

참고 기본 CIP 탐지 포트 44818과 TCP 스트림 **Perform Stream Reassembly on Both Ports(**두 포트 모두에서 스트림 리어셈블리 수행**)** 목록에 나열한 다른 모든 포트를 추가해야 합니다. TCP 스트림 전처리 옵션 및 사용자 지정 네트워크 분석 정책 만들기의 내용을 참조하십시오.

기본 연결되지 않음 시간 초과**(**초**)**

CIP 요청 메시지에 프로토콜별 시간 초과 값이 없으며 **TCP** 연결당 동시 연결되지 않은 요청의 최대 수에 도달하는 경우, 시스템은 이 옵션이 지정한 초 수를 메시지에 지정합니다. 타이머가 만료되면 향후 요청을 위한 공간 확보를 위해 메시지가 제거됩니다. 0부터 360까지의 정수를 지정할 수 있습니다. 0을 지정하면 프로토콜별 시간 초과 값이 없는 모든 트래픽이 먼저 만료됩니다.

TCP 연결당 최대 동시 연결되지 않은 요청 수

시스템 연결을 닫기 전에 응답하지 않을 수 있는 동시 요청 수입니다. 1에서 1만까지의 정수를 지정할 수 있습니다.

TCP 연결당 최대 **CIP** 연결 수

시스템이 허용하는 TCP 연결당 최대 동시 CIP 연결 수입니다. 1에서 1만 까지의 정수를 지정할 수 있습니다.

CIP 이벤트

기본적으로 애플리케이션 탐지기와 이벤트 뷰어는 세션당 같은 애플리케이션을 각각 한 번만 탐지하고 표시합니다. CIP 세션이 서로 다른 패킷에 있는 여러 애플리케이션을 포함할 수 있으며, 단일 CIP 패킷이 여러 애플리케이션을 포함할 수 있습니다. CIP 전처리기는 대응하는 침입 규칙에 따라 모든 CIP 및 ENIP 트래픽을 처리합니다.

다음 표에서는 이벤트 보기에 표시되는 CIP 값을 확인할 수 있습니다.

표 ***3: CIP*** 이벤트 필드 값

이벤트 필드	표시되는 값
애플리케이션 프로토콜	CIP 또는 ENIP
클라이언트	CIP 클라이언트 또는 ENIP 클라이언트

이벤트 필드	표시되는 값
웹 애플리케이션	특정 애플리케이션이 다음과 같은 요소를 탐지합니다. • 트랙픽을 허용하거나 모니터링하는 액세스 컨트롤의 경우, 세션에서 탐 이션 프로토콜. 연결을 로깅하도록 설정한 액세스 컨트롤 규칙은 지정된 CIP 애플리케이 생성하지 않을 수 있으며, 연결을 로깅하도록 설정하지 않은 액세스 컨트 케이션에 대한 이벤트를 생성할 수 있습니다. • 트래픽을 차단하는 액세스 컨트롤 규칙의 경우, 차단을 트리거한 애플리 액세스 컨트롤 규칙이 CIP 애플리케이션 목록을 차단하는 경우, 이벤트 뷰 한 애플리케이션을 표시합니다.

CIP 전처리기 규칙

다음 표에 있는 CIP 전처리기 규칙이 이벤트를 생성하게 하려면, 해당 규칙을 활성화해야 합니다. 규칙 활성화에 대한 자세한 내용은 침입 규칙 상태 설정를 참고하십시오

표 *4: CIP* 전처리기 규칙

GID: SID	규칙 메시지
148:1	CIP_MALFORMED
148:2	CIP_NON_CONFORMING
148:3	CIP_CONNECTION_LIMIT
148:4	CIP_REQUEST_LIMIT

CIP 전처리기 설정 지침

CIP 전처리기를 설정하는 경우 다음 사항에 유의하십시오.

- 기본 CIP 탐지 포트 44818과 TCP 스트림 **Perform Stream Reassembly on Both Ports(**두 포트 모두에서 스트림 리어셈블리 수행**)** 목록에 나열한 다른 모든 CIP 포트를 추가해야 합니다. CIP 전처리기 옵션, 8 페이지, 사용자 지정 네트워크 분석 정책 만들기 및 TCP 스트림 전처리 옵션 섹션을 참고하십시오.
- 이벤트 뷰어는 CIP 애플리케이션에 특수한 처리를 제공합니다. CIP 이벤트, 8 페이지의 내용을 참조하십시오.
- Cisco는 침입 방지 작업을 액세스 컨트롤 정책의 기본 작업으로 사용할 것을 권장합니다.
- CIP 전처리기는 침입 규칙과 액세스 컨트롤 규칙에서 지정한 CIP 애플리케이션이 트리거한 트래픽을 삭제하지 않는 등의 바람직하지 않은 행동을 유발할 수 있는, **Access Control: Trust All**

Traffic(액세스 컨트롤**:** 모든 트래픽 신뢰**)**을 액세스 컨트롤 정책 기본 작업으로 지원하지 않습니다.

- CIP 전처리기는 차단되선 안 되는 CIP 애플리케이션 차단 등의 바람직하지 않은 행동을 유발할 수 있는, **Access Control: Block All Traffic(**액세스 컨트롤**:** 모든 트래픽 차단**)**을 액세스 컨트롤 정책 기본 작업으로 지원하지 않습니다.
- CIP 전처리기는 네트워크 검색 같은 CIP 애플리케이션에 대한 애플리케이션 가시성을 지원하지 않습니다.
- CIP 및 ENIP 애플리케이션을 탐지하고 액세스 컨트롤 규칙과 침입 규칙 등에서 이를 사용하려면, 해당하는 맞춤형 네트워크 분석 정책에서 CIP 전처리기를 수동으로 활성화해야 합니다. 사용자 지정 네트워크 분석 정책 만들기, Setting the Default Network Analysis Policy(기본 네트워크 분석 정책 설정), 네트워크 분석 규칙 설정 섹션의 내용을 참조하십시오.
- CIP 전처리기 규칙과 CIP 침입 규칙을 트리거하는 트래픽을 삭제하려면, 해당하는 침입 정책에서 **Drop when Inline(**인라인시 삭제**)**가 활성화되어 있는지 확인합니다. Setting Drop Behavior in an Inline Deployment(인라인 구축에서 삭제 동작 설정)의 내용을 참조하십시오.
- 액세스 컨트롤 규칙을 이용해 CIP 또는 ENIP 애플리케이션 트래픽을 차단하려면, 해당하는 네트워크 분석 정책에서 인라인 표준화 전처리기와 전처리기의 **Inline Mode(**인라인 모드**)** 옵션이 활성화(기본 설정)되어 있는지 확인합니다. 사용자 지정 네트워크 분석 정책 만들기, Setting the Default Network Analysis Policy(기본 네트워크 분석 정책 설정), 인라인 구축의 전처리기 트래픽 수정의 내용을 참조하십시오.

CIP 전처리기 설정

참고 이 섹션은 Snort 2 전처리기에 적용됩니다. Snort 3 관리자에 대한 자세한 내용은 https://www.cisco.com/go/snort3-inspectors를 참조하십시오.

시작하기 전에

- 기본 CIP 탐지 포트 44818과 TCP 스트림 **Perform Stream Reassembly on Both Ports(**두 포트 모두에서 스트림 리어셈블리 수행**)** 목록에 CIP 포트로 나열한 다른 모든 포트를 추가해야 합니다. CIP 전처리기 옵션, 8 페이지, 사용자 지정 네트워크 분석 정책 만들기 및 TCP 스트림 전처리 옵션 섹션을 참고하십시오.
- CIP 전처리기 설정 지침, 9 페이지의 내용을 숙지하십시오.
- CIP 전처리기는 threat defense 디바이스에서 지원되지 않습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 편집하려는 정책 옆의 **Snort 2 Version(Snort 2** 버전**)**을 클릭합니다.

단계 **3** 수정하려는 정책 옆에 있는 **Edit(**수정**)** ( )를 클릭합니다.

View(보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 **5** **SCADA Preprocessors(SCADA** 전처리기**)**의 **CIP Configuration(CIP** 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **6** CIP 전처리기 옵션, 8 페이지에서 설명한 모든 옵션을 수정할 수 있습니다.

단계 **7** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

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

다음에 수행할 작업

- 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.를 원하는 경우, CIP 침입 규칙과 필요에 따라 CIP 전처리기 규칙(GID 148)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정, CIP 전처리기 규칙, 9 페이지 및 CIP 이벤트, 8 페이지를 참고하십시오.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

S7Commplus 전처리기

참고 이 섹션은 Snort 2 전처리기에 적용됩니다. Snort 3 관리자에 대한 자세한 내용은 https://www.cisco.com/go/snort3-inspectors를 참조하십시오.

S7Commplus 전처리기는 S7Commplus 트래픽을 탐지합니다. 맞춤형 침입 규칙에서 S7Commplus 키워드를 이용해서 S7Commplus 트래픽에서의 침입을 탐지할 수 있습니다. S7Commplus 키워드의 내용을 참조하십시오.

S7Commplus 전처리기 구성

참고 이 섹션은 Snort 2 전처리기에 적용됩니다. Snort 3 관리자에 대한 자세한 내용은 https://www.cisco.com/go/snort3-inspectors를 참조하십시오.

S7Commplus 전처리기는 모든 threat defense 디바이스에서 지원됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 편집하려는 정책 옆의 **Snort 2 Version(Snort 2** 버전**)**을 클릭합니다.

단계 **3** 수정하려는 정책 옆에 있는 **Edit(**수정**)** ( )를 클릭합니다.

View(보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 **5** **SCADA Preprocessors(SCADA** 전처리기**)**에서 **S7Commplus Configuration(S7Commplus** 설정**)**이 비활성화되었다면 **Enabled(**활성화됨**)**를 클릭합니다.

단계 **6** 필요에 따라 **S7Commplus Configuration(S7Commplus** 설정**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭하고 **s7commplus_ports**를 수정하여 전처리기가 S7Commplus 트래픽을 검사하는 포트를 식별합니다. 포트가 여러 개인 경우 쉼표로 구분하십시오.

단계 **7** 마지막 정책 커밋 이후 이 정책에 적용된 변경 사항을 저장하려면 **Policy Information(**정책 정보**)**을 클릭한 다음 **Commit Changes(**변경 사항 커밋**)**를 클릭합니다.

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

다음에 수행할 작업

- 침입 이벤트를 생성하려면 S7Commplus 전처리기 규칙(GID 149)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정을 참조해 주십시오.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.