애플리케이션 레이어 프리프로세서

다음 주제에서는 애플리케이션 계층 전처리기와 전처리기 구성 방법을 설명합니다.

- 애플리케이션 계층 전처리기 소개, 1 페이지
- 애플리케이션 계층 전처리기 라이선스 요구 사항, 2 페이지
- 애플리케이션 계층 전처리기 요구 사항 및 사전 요건, 2 페이지
- DCE/RPC 전처리기, 2 페이지
- DNS 전처리기, 14 페이지
- FTP/텔넷 디코더, 19 페이지
- HTTP 검사 전처리기, 27 페이지
- Sun RPC 전처리기, 44 페이지
- SIP 전처리기, 46 페이지
- GTP 전처리기, 51 페이지
- IMAP 전처리기, 53 페이지
- POP 전처리기, 57 페이지
- SMTP 전처리기, 60 페이지
- SSH 전처리기, 66 페이지
- SSL 전처리기, 71 페이지

애플리케이션 계층 전처리기 소개

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

애플리케이션 계층 프로토콜은 다양한 방법으로 동일한 데이터를 나타낼 수 있습니다. Firepower System은 특정 패킷 데이터 유형을 침입 규칙 엔진이 분석할 수 있는 형식으로 표준화하는 애플리케이션 계층 프로토콜 디코더를 제공합니다. 애플리케이션 계층 프로토콜 인코딩을 표준화하면 규칙 엔진이 동일한 콘텐츠 관련 규칙을 해당 데이터가 다르게 표시되는 패킷에 보다 효율적으로 적용할 수 있으며, 유익한 결과를 얻을 수 있습니다.

침입 규칙 또는 규칙 인수를 사용하려면 비활성화된 전처리기가 필요한 경우 네트워크 분석 정책 웹 인터페이스에서 비활성화 상태로 남아 있다고 해도, 시스템은 자동으로 전처리기를 현재 구성으로 사용한다는 점에 유의하십시오.

침입 정책에서 동반되는 전처리기 규칙을 활성화하지 않는 경우 대부분의 경우 전처리기는 이벤트를 생성하지 않는다는 점에 유의하십시오.

애플리케이션 계층 전처리기 라이선스 요구 사항

Threat Defense 라이선스

IPS

기본 라이선스

보호

애플리케이션 계층 전처리기 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모두

사용자 역할

- 관리자
- 침입 관리자

DCE/RPC 전처리기

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

DCE/RPC 프로토콜을 사용하면 개별 네트워크 호스트에 있는 프로세스가 동일한 호스트에 있는 것처럼 통신할 수 있습니다. 이 프로세스 간 통신은 일반적으로 TCP 및 UDP를 통해 호스트 간에 전송됩니다. TCP 전송 내에서 DCE/RPC가 Windows SMB(Server Message Block) 프로토콜 또는 Samba로 더 캡슐화될 수 있습니다. Samba는 Windows와 UNIX 또는 Linux와 유사한 운영 체제로 구성된 혼합

환경에서 프로세스 간 통신에 사용되는 오픈 소스 SMB 구현입니다. 또한 네트워크의 Windows IIS 웹 서버는 방화벽을 통해 프록시 TCP 전송 DCE/RPC 트래픽에 분산 통신을 제공하는 IIS RPC over HTTP를 사용할 수도 있습니다.

DCE/RPC 전처리기 옵션 및 기능의 설명에는 MSRPC로 알려진 DCE/RPC의 Microsoft 구현이 포함됩니다. SMB 옵션 및 기능에 대한 설명은 SMB 및 Samba를 모두 나타냅니다.

대부분의 DCE/RPC 익스플로잇이 실제로 Windows 또는 Samba를 실행하는 네트워크의 모든 호스트가 될 수 있는 DCE/RPC 서버를 대상으로 하는 DCE/RPC 클라이언트 요청에서 발생하더라도, 익스플로잇은 서버 응답에서도 발생할 수 있습니다. DCE/RPC 전처리기는 RPC over HTTP 버전 1을 사용하는 TCP에서 전송되는 DCE/RPC를 포함하여 TCP, UDP 및 SMB 전송에서 캡슐화된 DCE/RPC 요청 및 응답을 탐지합니다. 전처리기는 DCE/RPC 데이터 스트림을 분석하고 이상 징후를 보이는 작업과 DCE/RPC 트래픽 내 회피 기술을 탐지합니다. 또한 SMB 데이터 스트림을 분석하고 SMB 이상 작업 및 회피 기술을 탐지합니다.

DCE/RPC 전처리기는 또한 IP 조각 모음 전처리기가 제공하는 IP 조각 모음 및 TCP 스트림 전처리기가 제공하는 TCP 스트림 리어셈블리에 더해 SMB의 분할을 해제하고 DCE/RPC 조각을 모읍니다.

마지막으로, DCE/RPC 전처리기는 규칙 엔진에 의한 처리를 위해 DCE/RPC 트래픽을 표준화합니다.

연결 없는 **DCE/RPC** 트래픽 및 연결 지향 **DCE/RPC** 트래픽

DCE/RPC 메시지는 DCE/RPC Protocol Data Units(프로토콜 데이터 단위, PDU)의 두 가지 명시적인 프로토콜 중 하나를 준수합니다.

연결 지향 **DCE/RPC PDU** 프로토콜

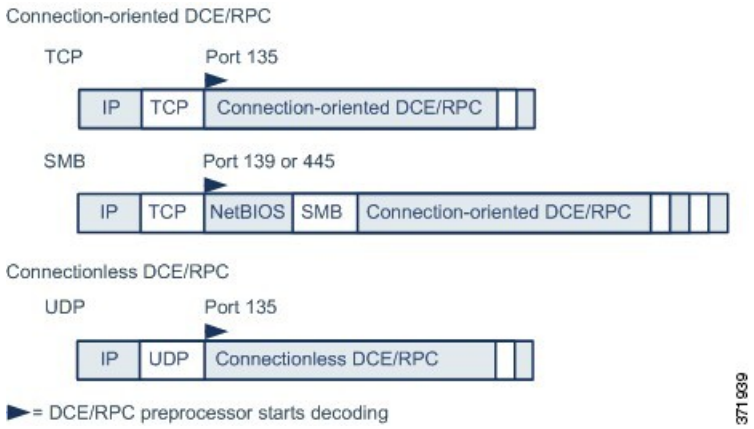
DCE/RPC 전처리기는 TCP, SMB 및 RPC over HTTP 전송에서 연결 지향 DCE/RPC를 탐지합니다.

연결 없는 **DCE/RPC PDU** 프로토콜

DCE/RPC 전처리기는 UDP 전송에서 연결 없는 DCE/RPC를 탐지합니다.

2개의 DCE/RPC PDU 프로토콜은 자체 고유한 헤더와 데이터 특성이 있습니다. 예를 들어 연결 지향 DCE/RPC 헤더 길이는 일반적으로 24바이트이며 연결 없는 DCE/RPC 헤더 길이는 80바이트로 고정됩니다. 또한 조각화된 연결 없는 DCE/RPC의 정확한 조각 순서는 연결 없는 전송으로 처리할 수 없으며, 연결 없는 DCE/RPC 헤더 값이어야 합니다. 반면 전송 프로토콜은 연결 지향 DCE/RPC의 정확한 조각 순서를 보장합니다. DCE/RPC 전처리기는 이와 그 외 기타 프로토콜 특정 특성을 이용하여 이상 징후 및 다른 회피 기술에 대한 프로토콜 모두를 모니터링하고, 트래픽을 규칙 엔진에 전달하기 전에 디코딩하고 조각 모음합니다.

다음 다이어그램은 DCE/RPC 전처리기가 여러 전송을 위해 DCE/RPC 트래픽을 처리하기 시작하는 시점에 대해 설명합니다.



그림에서 다음에 유의하십시오.

- 잘 알려진 TCP 또는 UDP 포트 135는 TCP와 UDP 전송에서 DCE/RPC 트래픽을 식별합니다.
- 그림은 RPC over HTTP를 포함하지 않습니다.

  RPC over HTTP의 경우, 연결 지향 DCE/RPC는 그림에서처럼 HTTP를 통한 초기 구성 시퀀스 후 TCP에 직접 전송됩니다.
- DCE/RPC 전처리기는 일반적으로 NetBIOS 세션 서비스의 잘 알려진 TCP 포트 139 또는 이와 유사하게 구현된 잘 알려진 Windows 포트 445에서 SMB 트래픽을 수신합니다.

  SMB에는 DCE/RPC 전송 외에도 많은 기능이 있기 때문에 전처리기는 먼저 SMB 트래픽이 DCE/RPC 트래픽을 전달하는지 테스트한 다음, 전달하지 않는 경우 처리를 중지하고 전달하는 경우 처리를 계속 진행합니다.
- IP는 모든 DCE/RPC 전송을 캡슐화합니다.
- TCP는 모든 연결 지향 DCE/RPC를 전송합니다.
- UDP는 연결 없는 DCE/RPC를 전송합니다.

DCE/RPC 대상 기반 정책

Windows 및 Samba DCE/RPC 구현은 매우 다릅니다. 예를 들어, DCE/RPC 트래픽을 조각 모음할 때 Windows의 모든 버전은 첫 번째 조각에서 DCE/RPC 컨텍스트 ID를 사용하고, Samba의 모든 버전은 마지막 조각에서 컨텍스트 ID를 사용합니다. 다른 예로, 특정 함수 호출을 식별하기 위해 Windows Vista는 첫 번째 조각의 opnum(작업 번호) 헤더 필드를 사용하고, Samba 및 다른 모든 Windows 버전은 마지막 조각의 opnum 필드를 사용합니다.

또한 Windows 및 Samba SMB 구현에도 상당한 차이점이 있습니다. 예를 들어, 명명된 파이프로 작업할 때 Windows는 SMB OPEN 및 READ 명령을 인식하지만 Samba는 이러한 명령을 인식하지 않습니다.

DCE/RPC 전처리기를 활성화할 때는 기본 대상 기반 정책을 자동으로 활성화합니다. 필요에 따라 다른 Windows 또는 Samba 버전을 실행하는 다른 호스트를 대상으로 하는 대상 기반 정책을 추가할 수 있습니다. 기본 대상 기반 정책은 다른 대상 기반 정책에 포함되지 않는 모든 호스트에 적용됩니다.

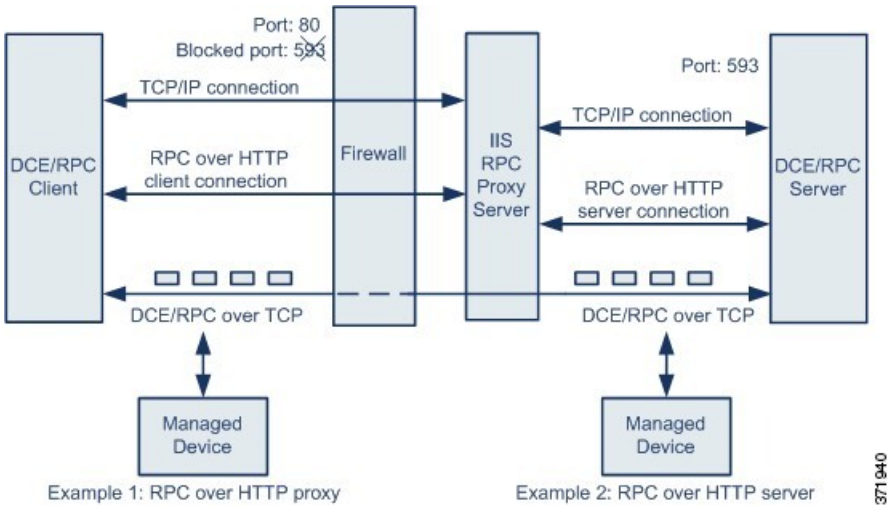
각 대상 기반 정책에서 다음과 같이 할 수 있습니다.

- 하나 이상의 전송을 활성화하고 각각에 대해 탐지 포트를 지정합니다.
- 자동 탐지 포트를 활성화하고 지정합니다.
- 사용자가 식별하는 하나 이상의 공유 SMB 리소스에 연결하려는 시도가 있는 경우 이를 탐지하도록 전처리기를 설정할 수 있습니다.
- SMB 트래픽의 파일을 탐지하고, 탐지한 파일에서 지정한 바이트 수를 검사하도록 전처리기를 구성할 수 있습니다.
- 또한 SMB 프로토콜 전문성을 가진 사용자만 변경할 수 있는 고급 옵션을 변경할 수 있습니다. 이 옵션을 통해 연속된 많은 SMB AndX 명령이 지정된 최대치를 초과하는 경우 이를 탐지하도록 전처리기를 설정할 수 있습니다.

DCE/RPC 전처리기 내 SMB 트래픽 파일 탐지를 활성화하는 것 외에도, 파일 정책을 구성하여 해당 파일을 선택적으로 수집 및 차단하거나 동적 분석을 위해 Cisco AMP 클라우드에 전송할 수 있습니다. 해당 정책 내에서 **Action(**작업**)**이 **Detect Files(**파일 탐지**)** 또는 **Block Files(**파일 차단**)**며 **Application Protocol(**애플리케이션 프로토콜**)**로 **Any(**모두**)** 또는 **NetBIOS-ssn(SMB)**을 선택한 파일 규칙을 생성해야 합니다.

RPC over HTTP 전송

HTTP 기반의 Microsoft RPC가 있으면 다음 다이어그램에서처럼 방화벽을 통해 DCE/RPC 트래픽을 터널링할 수 있습니다. DCE/RPC 전처리기는 HTTP 기반의 Microsoft RPC 버전 1을 탐지합니다.



Microsoft IIS 프록시 서버 및 DCE/RPC 서버는 동일한 호스트 또는 다른 호스트에 있을 수 있습니다. 개별 프록시와 서버 옵션은 두 경우 모두를 제공합니다. 그림에서 다음에 유의하십시오.

- DCE/RPC 서버는 DCE/RPC 클라이언트 트래픽에 대한 포트 593을 모니터링하지만, 방화벽은 포트 593을 차단합니다.

  방화벽은 일반적으로 포트 593을 기본값으로 차단합니다.

- RPC over HTTP는 방화벽이 허용할 가능성이 높은 잘 알려진 HTTP 포트 80을 사용하여 DCE/RPC over HTTP를 전송합니다.
- 예 1은 DCE/RPC 클라이언트와 Microsoft IIS RPC 프록시 서버 간 트래픽을 모니터링하기 위해 **RPC over HTTP proxy(RPC over HTTP** 프록시**)** 옵션을 선택하는 방법을 보여줍니다.
- 예 2는 Microsoft IIS RPC 프록시 서버 및 DCE/RPC 서버가 서로 다른 호스트에 있고 디바이스가 두 서버 간 트래픽을 모니터링할 때 **RPC over HTTP server(RPC over HTTP** 서버**)** 옵션을 선택하는 방법을 보여줍니다.
- 트래픽은 RPC over HTTP가 DCE/RPC 클라이언트와 서버 간의 프록시 설정을 완료한 후 연결 지향 DCE/RPC over TCP로만 구성됩니다.

DCE/RPC 전역 옵션

전역 DCE/RPC 전처리기 옵션은 전처리기가 작용하는 방법을 제어합니다. **Memory Cap Reached(**메모리 용량 도달**)** 및 **Auto-Detect Policy on SMB Session(SMB** 세션에서 자동 탐지 정책**)** 옵션을 제외한 경우, 이 옵션을 변경하면 성능 또는 탐지 기능에 부정적인 영향을 미칠 수 있다는 점에 유의하십시오. 전처리기 및 전처리기와 활성화된 DCE/RPC 규칙 간의 상호 작용을 완벽하게 파악하지 않은 경우 이들을 변경할 수 없습니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

최대 조각 크기

Enable Defragmentation(조각 모음 활성화**)**를 선택하면 허용된 최대 DCE/RPC 조각 길이를 지정합니다. 전처리기는 조각 모음 전에 처리를 위해 지정된 크기에 큰 조각을 자르지만 실제 패킷을 변경하지 않습니다. 빈 필드는 이 옵션을 비활성화합니다.

Maximum Fragment Size(최대 조각 크기**)** 옵션이 규칙이 탐지해야 하는 수준보다 크거나 동일한지 확인합니다.

리어셈블리 임계값

Enable Defragmentation(조각 모음 활성화**)**을 선택한 경우, 0은 이 옵션을 비활성화하고, 리어셈블된 패킷을 규칙 엔진으로 전송하기 전 프래그먼트된 DCE/RPC 바이트, 그리고 해당되는 경우 세그먼트된 SMB 바이트의 최소 수를 지정합니다. 낮은 값은 조기 검색 가능성을 증가시키지만 성능에 부정적인 영향을 미칠 수 있습니다. 이 옵션을 활성화하면 성능 영향을 테스트해야 합니다.

Reassembly Threshold(리어셈블리 임계값**)** 옵션이 규칙이 탐지해야 하는 수준보다 크거나 동일한지 확인합니다.

조각 모음 활성화

조각화된 DCE/RPC 트래픽을 조각 모음할지 여부를 지정합니다. 비활성화할 경우, 전처리기는 계속해서 이상 징후를 탐지하고 규칙 엔진에 DCE/RPC 데이터를 전송하지만, 조각화된 DCE/RPC 데이터에서 유실된 익스플로잇의 위험에 노출됩니다.

이 옵션을 사용하면 DCE/RPC 트래픽을 조각 모음하지 않는 유연성이 제공되지만, 대부분의 DCE/RPC 익스플로잇은 익스플로잇을 숨기기 위해 조각화를 이용하려고 시도합니다. 이 옵션을 비활성화하면 대부분의 알려진 익스플로잇을 우회하여 많은 수의 잘못된 부정이 야기됩니다.

메모리 용량 도달

전처리기에 할당된 최대 메모리 한도에 도달하거나 초과할 경우 이를 탐지합니다. 최대 메모리 용량에 도달하거나 초과할 경우, 전처리기는 메모리 용량 이벤트를 야기하고 해당 세션의 나머지 부분을 무시하는 세션과 관련된 보류 중인 모든 데이터를 비웁니다.

규칙 133:1을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

SMB 세션의 정책 자동 탐지

SMB `Session Setup AndX` 요청 및 응답에서 확인된 Windows 또는 Samba 버전을 탐지합니다. 탐지된 버전이 **Policy(**정책**)** 구성 옵션에 대해 구성된 Windows 또는 Samba 버전과 다른 경우, 탐지된 버전은 해당 세션만을 위해 구성된 버전을 대체합니다.

예를 들어 **Policy**를 Windows XP로 설정했는데 Windows Vista가 탐지된 경우, 프리프로세서는 해당 세션에 대해 Windows Vista 정책을 사용합니다. 다른 설정은 계속 적용됩니다.

DCE/RPC 전송이 SMB(즉, 전송이 TCP 또는 UDP인 경우)가 아닐 때는 버전을 탐지하고 정책을 자동으로 구성할 수 없습니다.

이 옵션을 활성화하려면 다음 드롭다운 목록 중 하나를 선택해야 합니다.

- **Client(**클라이언트**)**를 선택하여 정책 유형에 대한 서버-클라이언트 트래픽을 검사합니다.
- **Server(**서버**)**를 선택하여 정책 유형에 대한 클라이언트-서버 트래픽을 검사합니다.
- **Both(**모두**)**를 선택하여 정책 유형에 대한 서버-클라이언트 트래픽 및 클라이언트-서버 트래픽을 검사합니다.

레거시 **SMB** 검사 모드

레거시 **SMB** 검사 모드가활성화된 경우, 시스템은 SMB 버전 1 트래픽에만 SMB 침입 규칙을 적용하고, SMB 버전 1을 전송으로 사용하여 DCE/RPC 침입 규칙을 DCE/RPC 트래픽에 적용합니다. 이 옵션이 비활성화된 경우, 시스템은 SMB 버전 1, 2 및 3을 사용하는 트래픽에 SMB 침입 규칙을 적용하지만 SMB 버전 1에 대해서만 전송으로 SMB를 사용하는 DCE/RPC 트래픽에 DCE/RPC 침입 규칙을 적용합니다.

관련 항목

기본 content 또는 protected_content 키워드 인수
개요: byte_jump 및 byte_test 키워드

DCE/RPC 대상 기반 정책 옵션

각 대상 기반 정책에서 TCP, UDP, SMB 및 RPC over HTTP 전송 중 하나 이상을 활성화할 수 있습니다. 전송을 활성화할 때, 하나 이상의 탐지 포트, 즉, DCE/RPC 트래픽을 전달하는 것으로 알려진 포트를 지정해야 합니다.

Cisco는 기본 탐지 포트 사용을 권장합니다. 이는 잘 알려진 포트이거나 각 프로토콜에 일반적으로 사용하는 포트입니다. 기본이 아닌 포트에서 DCE/RPC 트래픽을 탐지한 경우에만 탐지 포트를 추가합니다.

Windows 대상 기반 정책에서는 네트워크 트래픽에 맞게 어떤 조합에서나 하나 이상의 전송에 대해 포트를 지정할 수 있지만, Samba 대상 기반 정책에서는 SMB 전송에만 포트를 지정할 수 있습니다.

참고 하나 이상의 전송이 활성화된 DCE/RPC 대상 기반 정책을 추가한 경우를 제외하고, 기본 대상 기반 정책에서는 하나 이상의 DCE/RPC 전송을 활성화해야 합니다. 예를 들어 모든 DCE/RPC 구현에 대해 호스트를 지정하고, 지정되지 않은 호스트에는 기본 대상 기반 정책을 구축하지 않을 수 있습니다. 이 경우 기본 대상 기반 정책에 대해 전송을 활성화하지 않을 수 있습니다.

또는 자동 탐지 포트, 즉 전처리기가 DCE/RPC 트래픽을 탐지하는 경우에만 포트가 DCE/RPC 트래픽을 전송하고 처리를 계속할지 결정하기 위해 전처리기가 처음 테스트하는 포트를 활성화하고 지정할 수도 있습니다.

자동 탐지 포트를 활성화할 때, 자동 탐지 포트가 전체 사용 후 삭제 포트 범위를 포함하기 위해 1024에서 65535까지의 포트 범위에 설정되어 있는지 확인합니다.

자동 탐지는 전송 탐지 포트에서 아직 식별되지 않은 포트에만 발생한다는 점에 유의하십시오.

RPC over HTTP Proxy Auto-Detect Ports(프록시 자동 탐지 포트) 옵션 또는 SMB Auto-Detect Ports(자동 탐지 포트) 옵션에 대한 자동 탐지 포트를 활성화하거나 지정할 가능성이 낮습니다. 이는 지정된 기본 탐지 포트를 제외하고는 이 둘을 위한 트래픽이 발생하거나 잠재력이 있을 가능성이 거의 없기 때문입니다.

각 대상 기반 정책을 통해 아래의 다양한 옵션을 지정할 수 있습니다. 어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

네트워크

DCE/RPC 대상 기반 서버 정책을 구축할 호스트 IP 주소입니다. 또한 대상 기반 정책을 추가할 때는 대상 추가(Add Target) 팝업 윈도우의 **Server Address(**서버 주소**)** 필드에 이름이 지정됩니다.

단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다. 기본 정책을 비롯한 255개의 총 프로파일을 설정할 수 있습니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

기본 정책의 `default` 설정은 다른 대상 기반 정책으로는 처리되지 않는 모니터링된 네트워크 세그먼트에 모든 IP 주소를 지정한다는 점에 유의하십시오. 따라서, 기본 정책에 대한 IP 주소 또는 CIDR 차단/접두사 길이를 지정할 수가 없으며, 지정할 필요도 없습니다. 그리고 다른 정책에서 이 설정을 공백으로 비워둘 수 없으며 `any`(예를 들어, 0.0.0.0/0 또는 ::/0)를 나타내는 주소 표기법을 사용할 수도 없습니다.

정책

모니터링된 네트워크 세그먼트에서 대상 호스트가 사용하는 Windows 또는 Samba DCE/RPC 구현

Auto-Detect Policy on SMB Session(SMB 세션에서 정책 자동 탐지**)** 전역 옵션을 활성화하여 SMB가 DCE/RPC 전송일 때 세션별로 이 옵션의 설정을 자동으로 대체할 수 있다는 점에 유의하십시오.

SMB 유효하지 않은 공유

하나 이상의 SMB 공유 리소스를 식별하는 전처리기는 사용자가 지정하는 공유 리소스에 연결하려는 시도가 있는 경우 이를 탐지합니다. 사용자는 쉼표로 구분된 목록에서 여러 공유를 지정할 수 있으며, 선택적으로 공유를 따옴표로 감쌀 수 있습니다. 이는 이전 소프트웨어 버전에서 필요했지만 더 이상 그럴 필요가 없습니다. 예를 들면 다음과 같습니다.

```
"C$", D$, "admin", private
```

전처리기는 **SMB Ports(SMB** 포트**)**를 활성화할 때 SMB 트래픽에서 유효하지 않은 공유를 탐지합니다.

대부분의 경우 Windows에서 명명되었고, 유효하지 않은 공유로 식별된 드라이브에 달러 표시를 추가해야 한다는 점에 유의하십시오. 예를 들어, C$ 또는 "C$"로 드라이브 C를 식별합니다.

또한 SMB 유효하지 않은 공유를 탐지하려면 **SMB Ports(SMB** 포트**)** 또는 **SMB Auto-Detect Ports(SMB** 자동 탐지 포트**)**를 활성화해야 합니다.

규칙 133:26을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

SMB 최대 **AndX** 체인

연속된 SMB AndX 명령에서 허용할 최대값입니다. 일반적으로, 연속된 여러 AndX 명령이 이상 작업을 나타내며 회피 시도를 나타낼 수 있습니다. 1을 지정하여 연속된 명령을 허용하지 않거나 0을 지정하여 연속된 명령의 수 탐지를 비활성화합니다.

동반되는 SMB 전처리기 규칙이 활성화되고 연속된 명령의 수가 구성한 값과 동일하거나 초과할 경우 전처리기는 먼저 연속된 명령의 수를 세고 이벤트를 생성한다는 점에 유의하십시오. 그런 다음 처리를 계속 진행합니다.

주의 SMB 프로토콜의 전문가만이 **SMB Maximum AndX Chains(SMB** 최대 **AndX** 체인**)** 옵션의 기본 설정을 변경해야 합니다.

규칙 133:20을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

RPC 프록시 트래픽 전용

RPC over HTTP Proxy Ports(RPC over HTTP 프록시 포트**)**를 활성화하면, 탐지된 클라이언트 측 RPC over HTTP가 프록시 트래픽 전용인지 또는 다른 웹 서버 트래픽을 포함하는지가 표시됩니다. 예를 들어, 포트 80은 프록시와 다른 웹 서버 트래픽을 모두 전달할 수 있습니다.

이 옵션을 비활성화하면, 프록시 및 다른 웹 서버 트래픽 모두 예상됩니다. 예를 들어, 서버가 전용 프록시 서버인 경우, 이 옵션을 활성화합니다. 활성화되었을 때, 전처리기는 트래픽이 DCE/RPC를 전달하고 있는지 확인하기 위해 트래픽을 테스트하고, 전달하고 있는 경우 처리를 계속 진행하고 그렇지 않은 경우 트래픽을 무시합니다. 이 옵션과 함께 **RPC over HTTP Proxy Ports(RPC over HTTP** 프록시 포트**)** 체크 박스도 활성화한 경우에만 기능이 추가됩니다.

RPC over HTTP 프록시 포트

관리되는 디바이스가 DCE/RPC 클라이언트와 Microsoft IIS RPC 프록시 서버 사이에 있는 경우 각 지정된 포트의 RPC over HTTP에서 터널링된 DCE/RPC 트래픽의 탐지를 활성화합니다.

활성화하면, 웹 서버에서 일반적으로 DCE/RPC와 기타 트래픽 모두에 기본 포트를 사용하기 때문에 트래픽이 필요한 가능성이 낮더라도, DCE/RPC 트래픽을 볼 수 있는 모든 포트를 추가할 수 있습니다. 이 탐지가 활성화되면 **RPC over HTTP Proxy Auto-Detect Ports(RPC over HTTP** 프록시 자동 탐지 포트**)**는 활성화되지 않지만, 탐지된 클라이언트 측 RPC over HTTP 트래픽이 프록시 트래픽뿐이고 다른 웹 서버 트래픽은 포함되지 않는 경우 **RPC Proxy Traffic Only(RPC** 프록시 트래픽 전용**)**는 활성화됩니다.

참고 이 옵션은 선택하는 일이 거의 없을 것입니다.

RPC over HTTP 서버 포트

Microsoft IIS RPC 프록시 서버 및 DCE/RPC 서버가 다른 호스트에 있고 디바이스가 두 서버 간 트래픽을 모니터링할 때 각 지정된 포트에서 RPC over HTTP에 의해 터널링된 DCE/RPC 트래픽의 탐지를 활성화합니다.

일반적으로 이 옵션을 활성화하는 경우 네트워크에서 프록시 웹 서버가 인식되지 않더라도 포트 범위를 1025~65535로 설정하여 **RPC over HTTP Server Auto-Detect Ports(RPC over HTTP** 서버 자동 탐지 포트**)**도 활성화해야 합니다. HTTP 서버 포트 기반의 RPC가 경우에 따라 재구성되는데, 이 경우 사용자는 이 옵션의 포트 목록에 재설정된 서버 포트를 추가해야 합니다.

TCP 포트

각 지정된 포트의 TCP에서 DCE/RPC 트래픽의 탐지를 활성화합니다.

적정 DCE/RPC 트래픽 및 익스플로잇은 다양한 포트를 사용하고, 포트 1024 이상의 다른 포트는 일반적입니다. 일반적으로 이 옵션을 활성화하면 해당 옵션에 대해 1025에서 최대 65535 포트 범위의 **TCP Auto-Detect Ports(TCP** 자동 탐지 포트**)**도 활성화해야 합니다.

UDP 포트

각 지정된 포트에서 UDP 내 DCE/RPC 트래픽의 탐지를 활성화합니다.

적정 DCE/RPC 트래픽 및 익스플로잇은 다양한 포트를 사용하고, 포트 1024 이상의 다른 포트는 일반적입니다. 일반적으로 이 옵션을 활성화하면 또한 해당 옵션에 대해 1025에서 최대 65535 포트 범위의 **UDP Auto-Detect Ports(UDP** 자동 탐지 포트**)**도 활성화해야 합니다.

SMB 포트

각 지정된 포트에서 SMB 내 DCE/RPC 트래픽의 탐지를 활성화합니다.

기본 탐지 포트를 사용하면 SMB 트래픽이 발생할 수 있습니다. 다른 포트를 사용할 경우 발생 가능성은 매우 낮습니다. 일반적으로, 기본 설정을 사용합니다.

Auto-Detect Policy on SMB Session(SMB 세션에서 정책 자동 탐지**)** 전역 옵션을 활성화하여 SMB가 DCE/RPC 전송일 때 세션별로 대상이 되는 정책에 대해 구성된 정책 유형을 자동으로 대체할 수 있다는 점에 유의하십시오.

RPC over HTTP 프록시 자동 탐지 포트

매니지드 디바이스가 DCE/RPC 클라이언트와 Microsoft IIS RPC 프록시 서버 사이에 있는 경우 지정된 포트에서 RPC over HTTP에서 터널링된 DCE/RPC 트래픽의 자동 탐지를 활성화합니다.

활성화하면, 일반적으로 1025에서 65535까지 포트 범위를 지정하여 사용 후 삭제 포트의 전체 범위를 지원할 수 있습니다.

RPC over HTTP 서버 자동 탐지 포트

Microsoft IIS RPC 프록시 서버 및 DCE/RPC 서버가 다른 호스트에 있고 디바이스가 두 서버 간 트래픽을 모니터링할 때 지정된 포트에서 RPC over HTTP에 의해 터널링된 DCE/RPC 트래픽의 자동 탐지를 활성화합니다.

TCP 자동 탐지 포트

지정된 포트의 TCP에서 DCE/RPC 트래픽의 자동 탐지를 활성화합니다.

UDP 자동 탐지 포트

각 지정된 포트에서 UDP 내 DCE/RPC 트래픽의 자동 탐지를 활성화합니다.

SMB 자동 탐지 포트

SMB 내 DCE/RPC 트래픽의 자동 탐지를 활성화합니다.

참고 이 옵션은 선택하는 일이 거의 없을 것입니다.

SMB 파일 검사

파일 검색을 위한 SMB 트래픽의 검사를 활성화합니다. 다음 옵션을 이용할 수 있습니다.

- 파일 선택을 비활성화하려면 **Off(**끄기**)**를 선택합니다.
- SMB의 DCE/RPC 트래픽 검사 없이 파일 데이터를 검사하려면 **Only(**전용**)**를 선택합니다. 이 옵션을 선택하면 파일 및 DCE/RPC 트래픽 모두의 검사 성능을 높일 수 있습니다.
- SMB에서 파일 및 DCE/RPC 트래픽을 모두 검사하려면 **On(**켜기**)**을 선택합니다. 이 옵션을 선택하면 성능에 영향을 줄 수 있습니다.

다음에 대한 SMB 트래픽의 검사는 지원되지 않습니다.

- 단일 TCP 또는 SMB 세션에서 동시에 전송된 파일
- 여러 TCP 또는 SMB 세션을 통해 전송된 파일
- 메시지 서명이 협상될 때와 같이 비인접 데이터로 전송된 파일
- 데이터를 중첩하여 동일한 오프셋에 서로 다른 데이터로 전송된 파일
- 클라이언트가 파일 서버에 저장한 수정 사항에 대해 원격 클라이언트에 열린 파일

SMB 파일 검사 수준

SMB File Inspection(SMB 파일 검사**)**이 **Only(**전용**)** 또는 **On(**켜기**)**으로 설정된 경우, 파일이 SMB 트래픽에서 탐지될 때 바이트 수를 검사합니다. 다음 중 하나를 지정하십시오.

- 양수 값
- 전체 파일을 검사하려면 `0`
- 파일 검사를 비활성화하려면 `-1`

이 필드에는 액세스 컨트롤 정책의 Advanced(고급) 탭에 있는 File and Malware Settings(파일 및 악성 코드 설정) 섹션에 정의된 것과 동일하거나 작은 값을 입력합니다. 이 옵션에 파일 유형 탐지 시 검사할 바이트 수 제한에 정의된 것보다 큰 값을 설정한 경우, 시스템은 액세스 컨트롤 정책 설정의 기능을 최대로 사용합니다.

SMB File Inspection(SMB 파일 검사**)**을 **Off(**해제**)**로 설정한 경우, 이 필드는 비활성화됩니다.

트래픽 관련 **DCE/RPC** 규칙

대부분의 DCE/RPC 전처리기 규칙은 SMB, 연결 지향 DCE/RPC 또는 연결 없는 DCE/RPC 트래픽에서 탐지된 이상 징후 및 회피 기술에 대해 트리거됩니다. 다음 표는 각 유형의 트래픽을 위해 활성화할 수 있는 규칙을 식별합니다.

표 *1:* 트래픽 관련 ***DCE/RPC*** 규칙

트래픽	전처리기 규칙 **GID:SID**
SMB	133:2~133:26 및 133:48~133:59
연결 지향 DCE/RPC	133:39를 통한 133:27
연결 없는 DCE/RPC를 탐지	133:43을 통한 133:40

DCE/RPC 전처리기 구성

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

전처리기 작동 방식을 제어하는 모든 전역 옵션을 수정함으로써, 그리고 사용자 네트워크의 DCE/RPC 서버를 그 위에서 운영되는 IP 주소 및 Windows 또는 Samba 버전 중 하나로 식별하는 하나 이상의 대상 기반 서버 정책을 지정함으로써 DCE/RPC 전처리기를 구성합니다. 또한 대상 기반 정책 설정에는 전송 프로토콜 활성화, DCE/RPC 트래픽을 해당 호스트로 전송하는 포트 지정 및 다른 서버 관련 옵션 설정이 포함되어 있습니다.

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

시작하기 전에

- 맞춤형 대상 기반 정책에서 식별하려는 네트워크가 상위 네트워크 분석 정책이 처리한 네트워크, 영역 및 VLAN 하위 집합과 일치하는지 확인합니다. 자세한 내용은 네트워크 분석 정책 고급 설정를 참조하십시오.

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** 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

단계 **5** **Application Layer Preprocessors(애플리케이션 계층 전처리기)**의 **DCE/RPC Configuration(DCE/RPC 설정)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **6** **DCE/RPC Configuration(DCE/RPC 설정)** 옆에 있는 **Edit(수정)** ()을 클릭합니다.

단계 **7** **Global Settings(전역 설정)** 섹션의 옵션을 수정합니다(DCE/RPC 전역 옵션, 6 페이지 참조).

단계 **8** 다음 옵션을 이용할 수 있습니다.

- 서버 프로파일 추가 - **Servers(서버)** 옆에 있는 **Add(추가)** ()을 클릭합니다. **Server Address(서버 주소)** 필드에 하나 이상의 IP 주소를 지정하고 **OK(확인)**를 클릭합니다.
- 서버 프로파일 삭제 - 정책 옆에 있는 **Delete(삭제)** ()을 클릭합니다.
- 서버 프로파일 편집 - **Servers(서버)**에서 프로파일에 대해 설정된 주소를 클릭하거나 **default(기본값)**를 클릭합니다. **Configuration(설정)** 섹션에서 설정을 수정할 수 있습니다(DCE/RPC 대상 기반 정책 옵션, 8 페이지 참조).

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

- 침입 이벤트를 생성하려면 DCE/RPC 전처리기 규칙(GID 132 또는 133)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정, DCE/RPC 전역 옵션, 6 페이지, DCE/RPC 대상 기반 정책 옵션, 8 페이지, 트래픽 관련 DCE/RPC 규칙, 12 페이지를 참고하십시오.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

파일 및 악성코드 탐지 성능 및 저장 옵션
DCE/RPC 키워드
레이어 관리
충돌 및 변경: 네트워크 분석 및 침입 정책

DNS 전처리기

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

DNS 전처리기는 다음 특정 익스플로잇에 대해 DNS 이름 서버 응답을 검사합니다.

- RData 텍스트 필드에서 오버플로 시도
- 사용하지 않는 DNS 리소스 레코드 유형
- 실험적 DNS 리소스 레코드 유형

DNS 이름 서버 응답의 가장 일반적인 유형은 응답을 표시한 쿼리에서 도메인 이름에 해당하는 하나 이상의 IP 주소를 제공합니다. 예를 들면, 서버 응답의 다른 유형은 원래 쿼리된 서버에서 사용 가능한 정보를 제공하는 이름 서버의 이메일 메시지 또는 위치를 위한 대상을 제공합니다.

DNS 응답은 다음으로 구성됩니다.

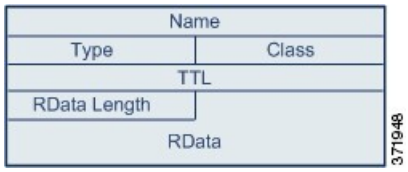
- 메시지 헤더
- 하나 이상의 요청을 포함하는 Question(질문) 섹션
- Question(질문) 섹션의 요청에 응답하는 3가지 섹션
  - 답변
  - 권한
  - 추가 정보.

이 3가지 섹션에서 응답은 이름 서버에 유지되는 리소스 레코드(RR)의 정보를 반영합니다. 다음 표는 이러한 3가지 섹션에 대해 설명합니다.

표 ***2: DNS*** 이름 서버 ***RR*** 응답

섹션	포함 내용	예시
답변	선택 사항. 쿼리에 특정 응답을 제공하는 하나 이상의 리소스 레코드	도메인 이름에 해당하는 IP 주소
권한	선택 사항. 권위 있는 이름 서버를 가리키는 하나 이상의 리소스 레코드	응답에 대한 권위 있는 이름 서버의 이름
추가 정보	선택 사항. Answer(응답) 섹션에 관련된 추가 정보를 제공한 하나 이상의 리소스 레코드	쿼리할 다른 서버의 IP 주소

많은 유형의 리소스 레코드가 있으며, 이는 모두 다음 구조를 준수합니다.



이론적으로, 모든 종류의 리소스 레코드는 이름 서버 응답 메시지의 Answer(답변), Authority(권한), 또는 Additional Information(추가 정보) 섹션에 사용될 수 있습니다. DNS 전처리기는 탐지하는 익스플로잇을 위해 3개의 응답 섹션 각각의 리소스 레코드를 검사합니다.

Type(유형) 및 RData 리소스 레코드 필드는 DNS 전처리기에 특히 중요합니다. Type(유형) 필드는 리소스 레코드 유형을 식별합니다. RData(리소스 데이터) 필드는 응답 콘텐츠를 제공합니다. RData 필드의 크기 및 내용은 리소스 레코드 유형에 따라 다릅니다.

DNS 메시지는 일반적으로 UDP 전송 프로토콜을 사용하지만 메시지 유형이 신뢰할 수 있는 전송을 요청하거나 메시지 크기가 UDP 기능을 초과할 경우 TCP도 사용합니다. DNS 전처리기는 UDP 및 TCP 트래픽 모두에서 DNS 서버 응답을 검사합니다.

세션이 삭제된 패킷 때문에 상태를 상실할 경우 DNS 전처리기는 중간에 선택된 TCP 세션을 검사하지 않으며, 검사를 중지합니다.

DNS 전처리기 옵션

포트

이 필드는 DNS 전처리기가 DNS 서버 응답에 대해 모니터링해야 하는 소스 포트 또는 포트를 지정합니다. 포트가 여러 개인 경우 쉼표로 구분하십시오.

DNS 전처리기에 대해 구성할 일반적인 포트는 잘 알려진 포트 53인데, 이는 DNS 이름 서버가 UDP 및 TCP 모두에서 DNS 메시지에 사용하는 것입니다.

RData 텍스트 필드의 오버플로 시도 탐지

리소스 레코드 유형이 TXT(텍스트)이면 RData 필드는 변수 길이의 ASCII 텍스트 필드입니다.

선택 시 이 옵션은 MITRE's Current Vulnerabilities and Exposures(MITRE의 현재 취약성 및 노출) 데이터베이스의 CVE-2006-3441 항속에서 식별된 특정 취약성을 탐지합니다. 이는 Microsoft Windows 2000 서비스 팩 4, Windows XP 서비스 팩 1 및 서비스 팩 2, 그리고 Windows Server 2003 서비스 팩 1에서 잘 알려진 취약성입니다. 공격자는 이러한 취약성을 악용하고 호스트를 전송하거나 호스트가 RData 텍스트 필드의 길이에서 계산 착오를 일으키도록 하는 악의적으로 조작된 이름 서버 응답을 수신하도록 하여 버퍼 오버플로를 일으킴으로써 호스트를 완전히 제어할 수 있습니다.

네트워크가 이 취약성을 해결하기 위해 업그레이드된 적이 없는 운영체제를 실행하는 호스트를 포함하는 경우 사용자는 이 옵션을 활성화해야 합니다.

규칙 131:3을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

사용하지 않는 **DNS RR** 유형 탐지

RFC 1035는 여러 리소스 레코드 유형을 사용하지 않는 것으로 식별합니다. 이는 사용하지 않는 레코드 유형이기 때문에, 일부 시스템은 이를 처리하지 않고 익스플로잇에 노출될 수 있습니다. 네트워크에 이들을 포함하도록 의도적으로 구성하지 않는 이상 일반 DNS 응답에서 이러한 레코드 유형이 발생하지 않습니다.

시스템을 구성하여 사용하지 않는 알려진 리소스 레코드 유형을 검색할 수 있습니다. 다음 표는 이러한 레코드 유형에 대해 나열하고 설명합니다.

표 *3:* 사용하지 않는 ***DNS*** 리소스 레코드 유형

RR 유형	코드	설명
3	MD	메일 대상
4	MF	메일 발송자

규칙 131:1을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

실험적 **DNS RR** 유형 탐지

RFC 1035는 여러 리소스 레코드 유형을 실험적인 것으로 식별합니다. 다음은 실험적 레코드 유형이기 때문에, 일부 시스템은 이를 처리하지 않고 익스플로잇에 노출될 수 있습니다. 네트워크에 이들을 포함하도록 의도적으로 구성하지 않는 이상 일반 DNS 응답에서 이러한 레코드 유형이 발생하지 않습니다.

시스템을 구성하여 알려진 실험적 리소스 레코드 유형을 검색할 수 있습니다. 다음 표는 이러한 레코드 유형에 대해 나열하고 설명합니다.

표 *4:* 실험적 ***DNS*** 리소스 레코드 유형

RR 유형	코드	설명
7	MB	메일함 도메인 이름
8	MG	메일 그룹 멤버
9	MR	메일 이름 변경 도메인 이름
10	NUL	null 리소스 레코드

규칙 131:2를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

DNS 전처리기 구성

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

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** **Application Layer Preprocessors(**애플리케이션 계층 전처리기**)**의 **DCE Configuration(DCE** 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **6** **DCE Configuration(DCE** 구성**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **7** DNS 전처리기 옵션, 16 페이지에서 설명하는 설정을 수정합니다.

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

- 침입 이벤트를 생성하려면 DNS 전처리기 규칙(GID 131)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정 및 DNS 전처리기 옵션, 16 페이지의 내용을 참조하십시오.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

침입 및 네트워크 분석 정책의 레이어
충돌 및 변경: 네트워크 분석 및 침입 정책

FTP/텔넷 디코더

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

FTP/텔넷 디코더는 FTP 및 텔넷 데이터 스트림을 분석하고, 규칙 엔진으로 처리하기 전에 FTP 및 텔넷 명령을 표준화합니다.

전역 FTP 및 텔넷 옵션

전역 옵션을 설정하여 FTP/텔넷 디코더가 패킷의 상태 저장 또는 상태 비저장 검사를 수행할지 여부, 디코더가 암호화된 FTP 또는 텔넷 세션을 탐지할지 여부, 그리고 암호화된 데이터가 발생한 후 디코더가 데이터 스트림 확인을 계속할지 여부를 결정할 수 있습니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

상태 저장 검사

선택하면 FTP/텔넷 디코더가 상태를 저장하고 개별 패킷을 위한 세션 콘텍스트를 제공하며, 리어셈블한 세션만 검사할 수 있습니다. 이를 취소하면, 세션 컨텍스트 없이 각 개별 패킷을 분석합니다.

FTP 데이터 전송을 확인하려면, 이 옵션을 선택해야 합니다.

암호화된 트래픽 탐지

암호화된 텔넷 및 FTP 세션을 탐지합니다.

규칙 125:7 및 126:2를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

암호화된 데이터 검사 계속 진행

데이터 스트림이 암호화된 후에도 계속 검사하여 처리 가능한. 해독된 최종 데이터를 찾도록 전처리기에 지시합니다.

텔넷 옵션

FTP/텔넷 디코더에 의한 텔넷 명령의 표준화를 활성화 또는 비활성화할 수 있으며, 특정 이상 징후의 경우를 활성화 또는 비활성화할 수 있고 허용할 AYT(Are You There) 공격의 임계값 수를 설정할 수 있습니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

포트

텔넷 트래픽을 표준화할 포트를 나타냅니다. 텔넷은 일반적으로 TCP 포트 23에 연결됩니다. 인터페이스에서, 쉼표로 구분하여 여러 개의 포트를 나열합니다.

⚠

주의 암호화된 트래픽(SSL)은 디코딩될 수 없으므로, 포트 22(SSH)를 추가하면 예측되지 않은 결과를 얻을 수 있습니다.

표준화

지정된 포트로 향하는 텔넷 트래픽을 표준화합니다.

이상 징후 탐지

해당 SE(subnegotiation 종료) 없이 텔넷 SB(subnegotiation 시작)의 탐지를 활성화합니다.

텔넷은 SB(subnegotiation 시작)로 시작하고 SE(subnegotiation 종료)로 끝나는 subnegotiation을 지원합니다. 그러나, 텔넷 서버의 특정 구현은 해당 SE가 없는 SB를 무시합니다. 이는 우회하는 경우일 수 있는 이상 작업입니다. FTP가 제어 연결에서 텔넷 프로토콜을 사용하므로, 또한 이러한 작업에 취약합니다.

규칙 126:3을 활성화하여 이벤트를 생성하고 인라인 구축에서 이 이상 징후가 텔넷 트래픽에서 탐지될 때 문제가 되는 패킷을 삭제할 수 있으며, 규칙 125:9를 활성화하여 FTP 명령 채널에서 이 이상 징후가 탐지될 때 이벤트를 생성할 수 있습니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

AYT(Are You There) 공격 임계값 수

연속적인 AYT 명령의 수가 지정된 임계값을 초과하는 경우 이를 탐지합니다. Cisco는 AYT 임계값으로 기본값을 초과하지 않는 값을 설정할 것을 권장합니다.

규칙 126:1을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

서버 레벨 **FTP** 옵션

여러 FTP 서버에서 디코딩을 위한 옵션을 설정할 수 있습니다. 생성한 각 서버 프로파일은 서버 IP 주소 및 트래픽이 모니터링되어야 할 서버의 포트를 포함합니다. 특정 서버에 대해 어느 FTP 명령을 인증할지, 그리고 어느 FTP 명령을 무시할지 지정하고 명령에 대한 최대 매개변수 길이를 설정할 수 있습니다. 또한 디코더가 특정 명령을 위해 인증해야 할 특정 명령어 구문을 설정하고, 대안이 되는 최대 명령 매개변수 길이를 지정할 수 있습니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

네트워크

FTP 서버에서 하나 이상의 IP 주소를 지정하려면 이 옵션을 사용합니다.

단일 IP 주소 또는 주소 블록을 지정하거나, 하나 또는 둘 다로 구성된 쉼표로 구분된 목록을 지정할 수 있습니다. 최대 1024개의 문자를 구성할 수 있고, 기본 프로파일을 포함하여 최대 255개 프로파일을 지정할 수 있습니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

기본 정책의 `default` 설정은 다른 대상 기반 정책으로는 처리되지 않는 모니터링된 네트워크 세그먼트에 모든 IP 주소를 지정한다는 점에 유의하십시오. 따라서, 기본 정책에 대한 IP 주소 또는 주소 블록을 지정할 수가 없으며, 지정할 필요도 없습니다. 그리고 다른 정책에서 이 설정을 공백으로 비워 둘 수 없으며 `any`(예를 들어, 0.0.0.0/0 또는 ::/0)를 나타내는 주소 표기법을 사용할 수도 없습니다.

포트

관리되는 디바이스가 트래픽을 모니터링해야 하는 FTP 서버에서 포트를 지정하려면 이 옵션을 사용합니다. 인터페이스에서, 쉼표로 구분하여 여러 개의 포트를 나열합니다. 포트 21은 잘 알려진 FTP 트래픽용 포트입니다.

File Get 명령

이 옵션을 사용하여 서버에서 클라이언트로 파일을 전송하는 데 사용되는 FTP 명령을 정의합니다. Support(지원팀)의 지시가 있는 경우가 아니면 이 값을 변경하지 마십시오.

주의 지원팀이 지시할 때만 **File Get Commands(File Get** 명령**)** 필드를 수정해야 합니다.

File Put 명령

이 옵션을 사용하여 클라이언트에서 서버로 파일을 전송하는 데 사용되는 FTP 명령을 정의합니다. Support(지원팀)의 지시가 있는 경우가 아니면 이 값을 변경하지 마십시오.

주의 지원팀이 지시할 때만 **File Put Commands(File Put** 명령**)** 필드를 수정해야 합니다.

추가 **FTP** 명령

이 문구를 사용하여 디코더가 탐지해야 하는 추가 명령을 지정합니다. 스페이스로 추가 명령을 구분합니다.

사용자가 추가할 수 있는 추가 명령에는 `XPWD`, `XCWD`, `XCUP`, `XMKD`, 그리고 `XRMD`가 포함되어 있습니다. 이 명령에 대한 자세한 내용은 네트워크 작업 그룹에 의한 디렉토리 지향 FTP 명령 사양인 RFC 775를 참고하십시오.

기본 최대 매개변수 길이

이 옵션을 사용하여 대체 매개변수 최대 길이가 설정되지 않은 명령에 대해 매개변수 최대 길이를 감지합니다. 대체 매개변수 최대 길이를 필요한 만큼 추가할 수 있습니다.

규칙 125:3을 활성화할 수 있습니다.이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

대체 매개변수 최대 길이

이 옵션을 사용하여 다른 매개변수 최대 길이를 탐지할 명령을 지정하고, 해당 명령에 대한 최대 매개변수 길이를 지정합니다. **Add(**추가**)**를 클릭하여 특정 명령을 위해 탐지할 다른 매개변수 최대 길이를 지정할 수 있는 회선을 추가합니다.

문자열 형식 공격에 대한 명령 확인

이 옵션을 사용하여 문자열 형식 공격에 대해 지정된 명령을 확인합니다.

규칙 125:5를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

명령의 유효성

이 옵션을 사용하여 특정 명령의 유효한 형식을 입력합니다. **Add(**추가**)**를 클릭하여 명령 유효성 검사 회선을 추가합니다.

규칙 125:2 및 125:4를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

FTP 전송 무시

이 옵션을 사용하여 데이터 전송 채널의 상태 확인 이외의 모든 검사를 비활성화하여 FTP 데이터 전송의 성능을 개선합니다.

참고 데이터 전송을 검사하려면 전역 FTP/Telnet **Stateful Inspection** 옵션을 선택해야 합니다.

FTP 명령 내 텔넷 이스케이프 코드 탐지

이 옵션을 사용하여 텔넷 명령이 FTP 명령 계통에서 사용되는 경우를 탐지합니다.

규칙 125:1을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

표준화 진행 중 삭제 명령 무시

Detect Telnet Escape Codes within FTP Commands(FTP 명령 내 텔넷 이스케이프 코드 탐지**)**를 선택한 경우 이 옵션을 사용하여 FTP 트래픽을 표준화할 때 텔넷 특성과 회선 삭제 명령을 무시합니다. 설정은 FTP 서버 처리가 텔넷 삭제 명령을 처리하는 방식에 일치해야 합니다. 이전 서버는 일반적으

로 이를 처리하지만 새로운 FTP 서버는 일반적으로 텔넷 삭제 명령을 무시한다는 점에 유의하십시오.

문제 해결 옵션: **FTP** 명령 유효성 검사 구성 로그

Support(지원팀)는 문제 해결 통화 중에 사용자에게 시스템을 구성하여 서버에 나열된 각 FTP 명령에 대한 구성 정보를 인쇄하도록 요청할 수 있습니다.

⚠

주의 지원팀이 지시할 때만 **Log FTP Command Validation Configuration(FTP** 명령 유효성 검사 구성 로그**)**을 활성화하십시오.

FTP 명령 검증 성명

FTP 명령을 위한 유효성 입증 명령문을 설정할 때, 스페이스로 매개변수를 분리하여 대체 매개변수 그룹을 지정할 수 있습니다. 또한 유효성 입증 명령문에서 파이프 문자(|)로 이들을 분리하여 두 매개변수 간 이진 또는 관계를 생성할 수 있습니다. 매개변수를 대괄호([])로 묶는 것은 해당 매개변수가 선택 사항임을 나타냅니다. 매개변수를 중괄호({})로 묶는 것은 해당 매개변수가 요청된 것임을 나타냅니다.

FTP 커뮤니케이션의 일부로 수신된 매개변수의 문구를 인증하는 FTP 명령 매개변수 유효성 입증 명령문을 생성할 수 있습니다.

다음 표에 나열된 모든 매개변수는 FTP 명령 매개변수 유효성 입증 명령문에 사용할 수 있습니다.

표 ***5: FTP*** 명령 매개변수

사용 대상	발생하는 유효성 검사
`int`	표시된 매개변수는 정수여야 합니다.
`number`	표시된 매개변수는 1과 255 사이의 정수여야 합니다.
`char` _chars	표시된 매개변수는 _chars 인수에 지정된 특성 중 하나인 단일 특성이거나 그 구성원이어야 합니다. 예를 들어 `MODE`의 명령 유효성을 요휴성 입증 명령문 `char`로 정의하면 SBC는 `MODE` 명령을 위한 파라미터가 (Stream(스트림) 모드를 표시하는) `S`자와 (Block(차단) 모드를 표시하는) `B`자, (Compressed(압축된) 모드를 표시하는) `C`자로 이루어짐을 확인합니다.
`date` _datefmt	_datefmt가 `#`를 포함하는 경우, 표시된 파라미터는 숫자여야 합니다. _datefmt가 `C`를 포함하는 경우, 표시된 파라미터는 문자여야 합니다. _datefmt가 리터럴 문자열을 포함하는 경우, 표시된 매개변수는 리터럴 문자열에 일치해야 합니다.
문자열	표시된 매개변수는 문자열이어야 합니다.

사용 대상	발생하는 유효성 검사
host_port	표시된 매개변수는 RFC 959에 의해 정의된 대로 유효한 호스트 포트 지정자여야 하며, File Transfer Protocol 사양은 네트워크 작업 그룹에 의해 정의된 대로 유효한 호스트 포트 지정자여야 합니다.

필요한 경우 위 표의 문구를 조합하여 트래픽의 유효성을 입증해야 할 필요가 있는 각 FTP 명령을 정확하게 입증하는 매개변수 유효성 입증 명령문을 생성할 수 있습니다.

참고 TYPE 명령에서 복잡한 표현을 포함할 때, 스페이스로 이를 묶습니다. 또한, 표현 안의 각 피연산자를 스페이스로 묶습니다. 예를 들어, `char A | B` 를 입력합니다. `char A|B`는 올바르지 않습니다.

관련 항목

서버 레벨 FTP 옵션, 20 페이지
FTP 명령 검증 성명, 23 페이지

클라이언트 레벨 FTP 옵션

이러한 옵션을 사용하여 맞춤형 FTP 클라이언트 프로파일을 구성합니다. 옵션 설명에 전처리기 규칙이 포함되어 있지 않으면 이 옵션은 전처리기 규칙과 연결되어 있지 않은 것입니다.

네트워크

FTP 클라이언트의 하나 이상의 IP 주소를 지정하려면 이 옵션을 사용합니다.

단일 IP 주소나 주소 블록 또는 둘 중 하나 또는 모두로 구성된 쉼표로 구분된 목록을 지정할 수 있습니다. 최대 1024개의 문자를 지정할 수 있고, 기본 프로파일을 포함하여 최대 255개 프로파일을 지정할 수 있습니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

기본 정책의 `default` 설정은 다른 대상 기반 정책으로는 처리되지 않는 모니터링된 네트워크 세그먼트에 모든 IP 주소를 지정한다는 점에 유의하십시오. 따라서, 기본 정책에 대한 IP 주소 또는 주소 블록을 지정할 수가 없으며, 지정할 필요도 없습니다. 그리고 다른 정책에서 이 설정을 공백으로 비워 둘 수 없으며 `any`(예를 들어, 0.0.0.0/0 또는 ::/0)를 나타내는 주소 표기법을 사용할 수도 없습니다.

최대 응답 길이

클라이언트가 수락하는 FTP 명령에 대해 허용되는 최대 응답 길이를 지정하려면 이 옵션을 사용합니다. 이는 기본 버퍼 오버플로를 탐지할 수 있습니다.

규칙 125:6을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

FTP 바운스 공격 탐지

FTP 바운스 공격을 탐지하려면 이 옵션을 사용합니다.

규칙 125:8을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

FTP 바운스 허용

FTP PORT 명령이 FTP 바운스 공격으로 처리되어서는 안 되는 호스트에서 추가 호스트 및 포트 목록을 구성하려면 이 옵션을 사용합니다.

FTP 명령 내 텔넷 이스케이프 코드 탐지

이 옵션을 사용하여 텔넷 명령이 FTP 명령 계통에서 사용되는 경우를 탐지합니다.

규칙 125:1을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

표준화 진행 중 삭제 명령 무시

Detect Telnet Escape Codes within FTP Commands를 선택한 경우 FTP 트래픽을 표준화할 때 텔넷 문자 및 줄 지우기 명령을 무시하려면 이 옵션을 사용합니다. 이 설정은 FTP 클라이언트가 텔넷 지우기 명령을 처리하는 방법과 일치해야 합니다. 이전 클라이언트는 일반적으로 이를 처리하지만 새로운 FTP 클라이언트는 일반적으로 텔넷 삭제 명령을 무시한다는 점에 유의하십시오.

FTP/텔넷 디코더 설정

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

FTP 클라이언트에 대한 클라이언트 프로파일을 구성하여 클라이언트에서 FTP 트래픽을 모니터링할 수 있습니다.

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

시작하기 전에

- 맞춤형 대상 기반 정책에서 식별하려는 네트워크가 상위 네트워크 분석 정책이 처리한 네트워크, 영역 및 VLAN 하위 집합과 일치하는지 확인합니다. 자세한 내용은 네트워크 분석 정책 고급 설정를 참조하십시오.

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 **Application Layer Preprocessors(애플리케이션 계층 전처리기)**의 **FTP and Telnet Configuration(FTP 및 텔넷 설정)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 6 **FTP and Telnet Configuration(FTP 및 텔넷 설정)** 옆에 있는 **Edit(수정)** ( )을 클릭합니다.

단계 7 **Global Settings(전역 설정)** 섹션의 옵션을 전역 FTP 및 텔넷 옵션, 19 페이지에 설명된 대로 설정합니다.

단계 8 **Telnet Settings(텔넷 설정)** 섹션의 옵션을 텔넷 옵션, 19 페이지에 설명된 대로 설정합니다.

단계 9 FTP 서버 프로파일 관리:

- 서버 프로파일 추가 - **FTP Server(FTP 서버)** 옆에 있는 **Add(추가)** ( )을 클릭합니다. **Server Address(서버 주소)** 필드에 하나 이상의 클라이언트 IP 주소를 지정하고 **OK(확인)**를 클릭합니다. 단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다. 최대 1024개의 문자를 구성할 수 있고, 기본 정책을 포함하여 최대 255개의 정책을 구성할 수 있습니다.
- 서버 프로 파일 편집 - **FTP Server(FTP 서버)**의 맞춤형 프로파일에 대해 구성된 주소를 클릭하거나 **default(기본값)**를 클릭합니다. **Configuration(설정)** 섹션에서 설정을 수정할 수 있습니다(서버 레벨 FTP 옵션, 20 페이지 참조).
- 서버 프로파일 삭제 - 프로파일 옆에 있는 **Delete(삭제)** ( )을 클릭합니다.

단계 10 FTP 클라이언트 프로파일 관리:

- 클라이언트 프로파일 추가 - **FTP Client(FTP 클라이언트)** 옆에 있는 **Add(추가)** ( )을 클릭합니다. **Client Address** 필드에서 클라이언트에 대한 하나 이상의 IP 주소를 지정하고 **OK**를 클릭합니다. 단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다. 최대 1024개의 문자를 구성할 수 있고, 기본 정책을 포함하여 최대 255개의 정책을 구성할 수 있습니다.
- 클라이언트 프로파일 편집 - **FTP Client(FTP 클라이언트)**에 추가한 프로파일에 대해 구성된 주소를 클릭하거나 **default(기본값)**를 클릭합니다. Configuration(설정) 페이지 영역에서 설정을 수정할 수 있습니다(클라이언트 레벨 FTP 옵션, 24 페이지 참조).

- 클라이언트 프로파일 삭제 - 맞춤형 프로파일 옆에 있는 **Delete(**삭제**)** ( )을 클릭합니다.

단계 **11** 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 FTP 및 텔넷 전처리기 규칙(GID 125 및 126)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정를 참고하십시오.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

레이어 관리
충돌 및 변경: 네트워크 분석 및 침입 정책

HTTP 검사 전처리기

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

HTTP Inspect(HTTP 검사) 전처리기는 다음 작업을 담당합니다.

- 사용자 네트워크 웹 서버로 전송된 HTTP 요청 및 사용자 네트워크 웹 서버에서 수신된 HTTP 응답 디코딩 및 표준화
- HTTP 관련 침입 규칙의 성능을 개선하기 위해 웹 서버로 전송된 메시지를 URI, 비 쿠키 헤더, 쿠키 헤더, 메서드 및 메시지 본문 구성 요소로 분리
- HTTP 관련 침입 규칙의 성능을 개선하기 위해 웹 서버에서 수신된 메시지를 상태 코드, 상태 메시지, 비 집합 쿠키 헤더, 쿠키 헤더 및 응답 본문 구성 요소로 분리
- 가능한 URI 인코딩 공격 탐지
- 추가 규칙을 처리하는 데 표준화된 데이터를 사용 가능하도록 하기
- JavaScript와 같은 악성 스크립트를 통한 공격 탐지 및 방지

HTTP 트래픽은 여러 형식으로 인코딩될 수 있기 때문에 규칙의 적절한 검사를 어렵게 합니다. HTTP Inspect(HTTP 검사)는 14가지 유형의 인코딩을 디코딩하여 사용자의 HTTP 트래픽이 가능한 최상의 검사를 받을 수 있도록 합니다.

HTTP Inspect(HTTP 검사) 옵션을 전역으로, 단일 서버에서 또는 서버 목록에 대해 구성할 수 있습니다.

전처리기 엔진은 HTTP 표준화를 상태 비저장으로 수행합니다. 즉, HTTP 문자열을 패킷 단위로 표준화하며, TCP 스트림 전처리기에 의해 리어셈블된 HTTP 문자열만 처리할 수 있습니다.

fast_blocking

HTTP 검사 전처리기의 전역 구성 옵션 중에서 fast_blocking 옵션이 Snort 버전 2.9.16.0부터 도입되었습니다. 이 옵션은 데이터를 지우기 전에 HTTP 데이터 검사를 활성화합니다. 이를 통해 조기 IPS 규칙 평가를 활성화할 수 있으므로, 데이터를 지운 후 차단하는 대신 차단 규칙을 적용하고 연결을 빨리 차단할 수 있습니다. 이 구성은 인라인 표준화가 활성화된 경우에만 적용됩니다.

fast_blocking 옵션을 활성화하려면 Maximum Detection(최대 탐지)을 기본 정책으로 하는 네트워크 분석 정책을 사용해야 합니다.

전역 **HTTP** 정상화 옵션

HTTP Inspect(HTTP 검사) 전처리기에 제공되는 전역 HTTP 옵션은 전처리기가 작동하는 방식을 제어합니다. 이 옵션을 사용하여 웹 서버 포트로 지정되지 않은 포트가 HTTP 트래픽을 수신할 때 HTTP 표준화를 활성화하거나 비활성화합니다.

다음 사항을 참고하십시오.

- **Unlimited Decompression(**무제한 압축 해제**)**을 활성화하는 경우, 변경 사항을 커밋하면 **Maximum Compressed Data Depth(**압축 데이터 최대 수준**)** 및 **Maximum Decompressed Data Depth(**압축 해제된 데이터 최대 수준**)** 옵션이 자동으로 65535로 설정됩니다.
- **Maximum Compressed Data Depth(**압축 데이터 최대 깊이**)** 또는 **Maximum Decompressed Data Depth(**압축 해제 데이터 최대 깊이**)**의 값이 다음에서 다른 경우 가장 높은 값을 사용합니다.
  - 기본 네트워크 분석 정책
  - 동일한 액세스 제어 정책의 네트워크 분석 규칙에서 호출된 기타 사용자 지정 네트워크 분석 정책

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

이상 **HTTP** 서버 탐지

웹 서버 포트로 지정되지 않은 포트로 전송되거나 해당 포트에서 수신되는 HTTP 트래픽을 탐지합니다.

참고 이 옵션을 설정하는 경우, HTTP 설정 페이지의 서버 프로파일에서 HTTP 트래픽을 수신하는 모든 포트를 나열해야 합니다. 이 옵션을 설정하지 않는 경우, 그리고 이 옵션 및 관련 전처리기 규칙을 활성화하는 경우, 서버를 오가는 일반 트래픽이 이벤트를 생성합니다. 기본 서버 프로파일은 보통 HTTP 트래픽에 사용되는 모든 포트를 포함하지만, 해당 프로파일을 수정한 경우, 이벤트가 생성되는 것을 방지하기 위해 다른 프로파일에 포트를 추가해야 할 수 있습니다.

규칙 120:1을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

HTTP 프록시 서버 탐지

Allow HTTP Proxy Use(HTTP 프록시 사용 허용**)** 옵션으로 정의되지 않은 프록시 서버를 사용하여 HTTP 트래픽을 탐지합니다.

규칙 119:17을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

압축 데이터 최대 수준

Inspect Compressed Data(압축 데이터 검사**)**(및 선택적으로, **Decompress SWF File(SWF** 파일 압축 해제**, LZMA)**, **Decompress SWF File(SWF** 파일 압축 해제**, Deflate)** 또는 **Decompress PDF File(PDF** 파일 압축 해제**, Deflate)**)가 활성화되어 있는 경우 압축 해제할 압축 데이터의 최대 크기를 설정합니다.

압축 해제된 데이터 최대 수준

Inspect Compressed Data(그리고 선택적으로 **Decompress SWF File(LZMA)**, **Decompress SWF File(Deflate)** 또는 **Decompress PDF File(Deflate)**) 옵션이 활성화된 경우 표준화된 압축 해제 데이터의 최대 크기를 설정합니다.

서버 레벨 **HTTP** 정상화 옵션

모니터링하는 각 서버에 대한 서버 수준 옵션을 모든 서버 또는 서버 목록에 대해 전역으로 설정할 수 있습니다. 또한, 미리 정의된 서버 프로파일을 사용하여 이 옵션을 설정하거나, 사용자 환경의 요구를 충족하도록 이들을 개별적으로 설정할 수 있습니다. 이 옵션 또는 이 옵션을 설정하는 기본 프로파일 중 하나를 사용하여 트래픽을 표준화할 HTTP 서버 포트와 표준화할 서버 응답 페이로드의 양, 그리고 표준화할 인코딩 유형을 지정합니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

네트워크

하나 이상 서버의 IP 주소를 지정하려면 이 옵션을 사용합니다. 단일 IP 주소나 주소 블록 또는 둘 중 하나 또는 모두로 구성된 쉼표로 구분된 목록을 지정할 수 있습니다.

최대 255개의 총 프로파일의 제한 외에도, 기본 프로파일을 포함하여 최대 496개의 문자 또는 약 26개의 항목을 하나의 HTTP 서버 목록에 포함할 수 있으며 모든 서버 프로파일에 대해 총 256개의 주소 항목을 지정할 수 있습니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

기본 정책의 `default` 설정은 다른 대상 기반 정책으로는 처리되지 않는 모니터링된 네트워크 세그먼트에 모든 IP 주소를 지정한다는 점에 유의하십시오. 따라서, 기본 정책에 대한 IP 주소 또는 CIDR 차단/접두사 길이를 지정할 수가 없으며, 지정할 필요도 없습니다. 그리고 다른 정책에서 이 설정을 공백으로 비워둘 수 없으며 `any`(예를 들어, 0.0.0.0/0 또는 ::/0)를 나타내는 주소 표기법을 사용할 수도 없습니다.

포트

HTTP 트래픽을 전처리기 엔진이 표준화하는 포트. 포트 번호가 여러 개인 경우 쉼표로 구분하십시오.

오버사이즈 디렉토리 길이

지정한 값보다 긴 URL 디렉토리를 탐지합니다.

지정된 길이보다 긴 URL 요청을 전처리기가 감지하면 규칙 119:15를 활성화하여 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

클라이언트 흐름 수준

Ports(포트**)**에 정의된 클라이언트 측 HTTP 트래픽의 헤더 및 페이로드 데이터를 포함하여 원시 HTTP 패킷에서 규칙이 검사하는 바이트 수를 지정합니다. 규칙 내 HTTP 콘텐츠 규칙 옵션이 요청 메시지의 특정 부분을 검사할 때 클라이언트 흐름 수준은 적용되지 않습니다.

다음 중 하나를 지정합니다.

- 양수 값은 첫 번째 패킷에서 지정된 바이트 수를 검사합니다. 첫 번째 패킷이 지정된 것보다 작은 바이트를 포함하는 경우, 전체 패킷을 검사합니다. 지정된 값이 세그먼트 및 리어셈블된 패킷 모두에 적용된다는 점에 유의하십시오.

  또한 300 값은 여러 클라이언트 요청 헤더의 끝에 나타나는 큰 HTTP 쿠키의 검사를 일반적으로 수행하지 않는다는 점에 유의하십시오.

- 0은 한 세션의 여러 패킷을 포함하여 모든 클라이언트 측 트래픽을 검사하며, 필요 시 바이트 상한을 초과합니다. 이 값이 성능에 영향을 줄 수 있다는 점에 유의하십시오.

- -1은 클라이언트 측 트래픽을 모두 무시합니다.

서버 흐름 수준

Ports(포트**)**에 지정된 서버 측 HTTP 트래픽의 원시 HTTP 패킷에서 규칙이 검사하는 바이트 수를 지정합니다. **Inspect HTTP Responses**가 비활성화된 경우 원시 헤더와 페이로드가 검사에 포함되고, **Inspect HTTP Response**가 활성화된 경우 원시 응답 본문만 검사에 포함됩니다.

서버 흐름 수준은 **Ports(**포트**)**에 정의된 서버 측 HTTP 트래픽에서 규칙이 검사하는 세션의 원시 서버 응답 데이터의 바이트 수를 지정합니다. 이 옵션을 사용하여 HTTP 서버 응답 데이터의 조사 수준 및 성능의 균형을 맞출 수 있습니다. 규칙 내 HTTP 콘텐츠 규칙 옵션이 응답 메시지의 특정 부분을 검사할 때 서버 흐름 수준은 적용되지 않습니다.

클라이언트 흐름 수준과 달리, 서버 흐름 수준은 검사하는 규칙에 대해 HTTP 요청 패킷이 아닌 HTTP 응답별로 바이트 수를 지정합니다.

다음 값 중 하나를 지정할 수 있습니다.

- 양수 값:

  Inspect HTTP Responses가 활성화된 경우 원시 HTTP 응답 본문만 검사하고 원시 HTTP 헤더는 검사하지 않습니다. **Inspect Compressed Data**가 활성화된 경우 압축 해제 데이터도 검사합니다.

  Inspect HTTP Responses가 비활성화된 경우 원시 패킷 헤더 및 페이로드를 검사합니다.

  세션이 지정된 것보다 작은 응답 바이트를 포함하는 경우, 규칙은 주어진 세션의 모든 응답 패킷을 완전히 검사하며, 필요에 따라 여러 패킷에 걸쳐 검사합니다. 세션이 지정된 것보다 많은 응답 바이트를 포함하는 경우, 규칙은 해당 세션에 대해 지정된 수의 바이트만 검사하며, 필요에 따라 여러 패킷에 걸쳐 검사합니다.

  흐름 수준 값이 작으면 **Ports(**포트**)**에 정의된 서버 측 트래픽을 대상으로 하는 규칙에서 오탐이 발생할 수 있습니다. 이러한 규칙의 대부분은 비 헤더 데이터의 처음 100바이트 정도에 있을 수 있는 HTTP 헤더 또는 콘텐츠를 대상으로 합니다. 헤더 길이는 일반적으로 300바이트보다 작지만, 헤더 크기는 다양할 수 있습니다.

  또한 지정된 값이 세그먼트 및 리어셈블된 패킷 모두에 적용된다는 점에 유의하십시오.

- 0은 65535바이트가 넘는 세션의 응답 데이터를 포함하여 **Ports(**포트**)**에 정의된 모든 HTTP 서버 측 트래픽의 전체 패킷을 검사합니다.

  이 값이 성능에 영향을 줄 수 있다는 점에 유의하십시오.

- -1:

  Inspect HTTP Responses가 활성화된 경우 원시 HTTP 헤더만 검사하고 원시 HTTP 응답 본문은 검사하지 않습니다.

  Inspect HTTP Response(HTTP 응답 검사**)**가 비활성화된 경우 **Ports(**포트**)**에 정의된 모든 서버 측 트래픽을 무시합니다.

최대 헤더 길이

HTTP 요청에서(그리고 **Inspect HTTP Responses**가 활성화된 경우 HTTP 응답에서) 지정된 최대 바이트 수보다 긴 헤더 필드를 탐지합니다. 0 값은 이 옵션을 비활성화합니다. 활성화하려면 양수 값을 지정합니다.

규칙 119:19 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.를 활성화할 수 있습니다.

최대 헤더 수

HTTP 요청에서 헤더 수가 이 설정을 초과하는 경우 이를 탐지합니다. 0 값은 이 옵션을 비활성화합니다. 활성화하려면 양수 값을 지정합니다.

규칙 119:20 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.를 활성화할 수 있습니다.

최대 스페이스 수

접혀진 회선에서 공백의 수가 HTTP 요청에서 이 설정과 동일하거나 초과하는 경우 이를 탐지합니다. 0 값은 이 옵션을 비활성화합니다. 활성화하려면 양수 값을 지정합니다.

규칙 119:26 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.를 활성화할 수 있습니다.

HTTP 클라이언트 본문 추출 수준

HTTP 클라이언트 요청의 메시지 본문에서 추출할 바이트 수를 지정합니다. 침입 규칙을 사용하여 `content` 또는 `protected_content` 키워드 **HTTP Client Body(HTTP** 클라이언트 본문**)** 옵션을 선택하여 추출된 데이터를 검사할 수 있습니다.

클라이언트 본문을 무시하려면 -1을 지정합니다. 전체 클라이언트 본문을 추출하려면 0을 지정합니다. 추출할 특정 바이트를 확인하면 시스템 성능을 개선할 수 있다는 점에 유의하십시오. **HTTP Client Body(HTTP** 클라이언트 본문**)** 옵션이 침입 규칙에서 작동하려면 0보다 크거나 같은 값을 지정해야 합니다.

소규모 청크 크기

하나의 청크가 작은 것으로 고려되는 최대 바이트 수를 지정합니다. 양수 값을 지정합니다. 0 값은 이상 징후를 보이는 연속된 소규모 세그먼트의 탐지를 비활성화합니다. 자세한 내용은 **Consecutive Small Chunks(**연속된 소규모 청크**)** 옵션을 참고하십시오.

연속된 소규모 청크

얼마나 많은 연속된 작은 청크가 청크화된 이동 인코딩을 사용하는 클라이언트 또는 서버 트래픽에서 비정상적으로 큰 수를 나타내는지 지정합니다. **Small Chunk Size(**소규모 청크 크기**)** 옵션은 작은 청크의 최대 크기를 지정합니다.

예를 들어, **Small Chunk Size(**소규모 청크 크기**)**를 10으로 설정하고 **Consecutive Small Chunks(**연속된 소규모 청크**)**를 5로 설정하여 10바이트 이하의 연속된 5개의 청크를 탐지합니다.

전처리기 규칙 119:27을 활성화하여 클라이언트 트래픽의 과도한 소규모 청크에서 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있고, 전처리기 규칙 120:7을 활성화하여 서버 트래픽의 과도한 소규모 청크에서 이벤트를 트리거할 수 있습니다. **Small Chunk Size(**소규모 청크 크기**)**가 활성화되고 이 옵션이 0 또는 1에 설정될 때, 이 규칙을 활성화하면 지정된 크기 또는 그보다 작은 모든 청크에서 이벤트가 트리거됩니다.

HTTP 메서드

시스템의 트래픽에 발생할 것으로 예상되는 GET 및 POST 외에 HTTP 요청 메서드를 지정합니다. 여러 개의 값을 구분하려면 쉼표를 사용하십시오.

침입 규칙은 HTTP 메서드에서 내용을 검색하기 위해 `content` 또는 `protected_content` 키워드와 **HTTP Method** 인수를 사용합니다. 규칙 119:31을 활성화하여 GET 및 POST 이외의 메서드 또는 이 옵션에 구성된 메서드가 트래픽에 발생할 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

경고 없음

동반되는 전처리기 규칙이 활성화된 경우 침입 이벤트를 비활성화합니다.

참고 이 옵션은 HTTP 표준 텍스트 규칙 및 공유 개체 규칙을 비활성화하지 않습니다.

HTTP 헤더 표준화

Inspect HTTP Responses(HTTP 응답 검사**)**가 활성화된 경우 요청 및 응답 헤더에서 비쿠키 데이터의 표준화를 활성화합니다. **Inspect HTTP Responses**가 활성화되지 않은 경우 요청 및 응답 헤더에서 쿠키를 비롯한 전체 HTTP 헤더의 표준화를 활성화합니다.

HTTP 쿠키 검사

HTTP 요청 헤더에서 쿠키 추출을 활성화합니다. 또한 **Inspect HTTP Responses(HTTP** 응답 검사**)**가 활성화된 경우 응답 헤더에서 set-cookie 데이터 추출을 활성화합니다. 쿠키 추출이 필요하지 않은 경우 이 옵션을 비활성화하면 성능을 높일 수 있습니다.

`Cookie:` 및 `Set-Cookie:` 헤더 이름, 헤더 행의 주요 스페이스, 그리고 헤더 행을 종료하는 `CRLF`는 헤더의 일부로 검사되지만 쿠키의 일부로는 검사되지 않는다는 점에 유의하십시오.

HTTP 헤더 내 쿠키 표준화

HTTP 요청 헤더에서 쿠키의 표준화를 활성화합니다. **Inspect HTTP Responses(HTTP** 응답 검사**)**가 활성화된 경우 응답 헤더에서 set-cookie 데이터의 표준화도 활성화합니다. 이 옵션을 선택하기 전에 **Inspect HTTP Cookies(HTTP** 쿠키 검사**)**를 선택해야 합니다.

HTTP 프록시 사용 허용

모니터링된 웹 서버가 HTTP 프록시로 사용되는 것을 허용합니다. 이 옵션은 HTTP 요청 검사에서만 사용됩니다.

URI만 검사

표준화된 HTTP 요청 패킷의 URI 부분만 검사합니다.

HTTP 응답 검사

HTTP 요청 메시지를 디코딩하고 표준화하는 것 외에도 HTTP 응답의 확장된 검사를 활성화하여 전처리기가 규칙 엔진에 의한 검사를 위해 응답 필드를 추출하도록 합니다. 이 옵션을 활성화하면 시스템이 응답 헤더, 본문, 상태 코드 등을 추출하며 **Inspect HTTP Cookies(HTTP** 쿠키 검사**)**가 활성화된 경우 set-cookie 데이터도 추출합니다.

다음과 같이 규칙 120:2 및 120:3을 활성화하여 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

표 ***6: HTTP*** 응답 규칙 검사

규칙	다음 상황에서 트리거됩니다**.**
120:2	잘못된 HTTP 응답 상태 코드가 발생합니다.
120:3	HTTP 응답에 콘텐츠 길이 또는 전송 인코딩이 포함되지 않습니다.

UTF 인코딩을 **UTF-8**로 표준화

Inspect HTTP Responses(HTTP 응답 검사**)**가 활성화된 경우 HTTP 응답에서 UTF-16LE, UTF-16BE, UTF-32LE 및 UTF32-BE 인코딩을 탐지하여 UTF-8로 표준화합니다.

UTF 표준화가 실패할 경우, 규칙 120:4를 활성화하여 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

압축 데이터 검사

Inspect HTTP Responses(HTTP 응답 검사**)**가 활성화된 경우 HTTP 응답 본문에 있는 gzip 및 deflate 호환 압축 데이터의 압축 해제 및 표준화된 압축 해제 데이터의 검사를 활성화합니다. 시스템은 청크 및 비 청크 HTTP 응답 데이터를 검사합니다. 시스템은 필요에 따라 여러 패킷에 걸쳐 패킷 별로 압축 해제된 데이터 패킷을 검사합니다. 즉 시스템이 검사를 위해 서로 다른 패킷의 압축 해제된 데이터를 결합하지 않습니다. **Maximum Compressed Data Depth(**압축 데이터 최대 수준**)**, **Maximum Decompressed Data Depth(**압축 해제된 데이터 최대 수준**)** 또는 압축 해제된 데이터의 끝부분에 도달하면 압축 해제가 종료됩니다. **Unlimited Decompression(**무제한 압축 해제**)**을 선택하지 않은 경우 **Server Flow Depth(**서버 흐름 수준**)**에 도달하면 압축 해제된 데이터의 검사가 종료됩니다. `file_data` 규칙 키워드를 사용하여 압축 해제된 데이터를 검사할 수 있습니다.

다음과 같이 규칙 120:6 및 120:24를 활성화하여 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

표 ***7:*** 압축된 ***HTTP*** 응답 규칙 검사

규칙	다음 상황에서 트리거됩니다**.**
120:6	압축된 HTTP 응답의 압축 해제에 실패합니다.
120:24	압축된 HTTP 응답의 부분적 압축 해제에 실패합니다.

무제한 압축 해제

Inspect Compressed Data(그리고 선택적으로 **Decompress SWF File(LZMA)**, **Decompress SWF File(Deflate)** 또는 **Decompress PDF File(Deflate)**)가 활성화된 경우 여러 패킷에서 **Maximum Decompressed Data Depth**를 재정의합니다. 즉, 이 옵션은 여러 패킷에서 무제한 압축 해제를 활성화합니다. 이 옵션을 활성화해도 단일 패킷 내 **Maximum Compressed Data Depth(**압축 데이터 최대 수준**)** 또는 **Maximum Decompressed Data Depth(**압축 해제된 데이터 최대 수준**)**에 영향을 주지 않는다는 점에 유의하십시오. 또한 이 옵션을 활성화하는 경우 변경을 커밋하면 **Maximum Compressed Data Depth(**압축 데이터 최대 수준**)** 및 **Maximum Decompressed Data Depth(**압축 해제된 데이터 최대 수준**)**를 65535로 설정한다는 점에 유의하십시오.

JavaScript 표준화

Inspect HTTP Responses가 활성화된 경우 HTTP 응답 본문 내에서 Javascript의 탐지 및 표준화를 활성화합니다. 전처리기는 unescape 및 decodeURI 함수 및 String.fromCharCode 메서드와 같이 난독 처리된 JavaScript 데이터를 표준화합니다. 전처리기는 unescape, decodeURI 및 decodeURIComponent 함수에서 다음 인코딩을 표준화합니다.

- %XX
- %uXXXX
- 0xXX
- \xXX
- \uXXXX

전처리기는 연속적인 여백을 탐지하고 이를 단일 스페이스로 표준화합니다. 이 옵션을 활성화할 경우, 구성 필드를 사용하여 사용자가 난독 처리된 JavaScript 데이터에서 허용할 연속적인 여백의 최대 수를 지정할 수 있습니다. 1에서 65535까지의 값을 입력할 수 있습니다. 이 필드와 연결된 전처리기 규칙(120:10)이 활성화되는지 여부에 관계없이 0 값은 이벤트 생성을 비활성화합니다.

전처리기는 또한 JavaScript의 더하기(+) 연산자를 표준화하고 연산자를 사용하여 문자열을 연결합니다.

`file_data` 침입 규칙 키워드를 사용하여 침입 규칙이 표준화된 JavaScript 데이터를 가리키도록 할 수 있습니다.

다음과 같이 규칙 120:9, 120:10, 120:11을 활성화하여 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

표 ***8: JavaScript*** 옵션 규칙 표준화

규칙	다음 상황에서 트리거됩니다**.**
120:9	전처리기 내 난독 처리 수준은 2와 같거나 큽니다.
120:10	JavaScript 난독 처리된 데이터에서 연속적인 여백의 수는 허용된 연속적인 여백의 최대 수에 구성된 값과 같거나 큽니다.
120:11	이스케이프 또는 인코딩된 데이터는 하나 이상의 인코딩 유형을 포함합니다.

SWF 파일 압축 해제**(LZMA)** 및 **SWF** 파일 압축 해제**(Deflate)**

HTTP Inspect Responses(HTTP 응답 검사**)**가 활성화된 경우 이러한 옵션은 HTTP 요청의 HTTP 응답 본문 내에 있는 파일의 압축된 부분을 압축 해제합니다.

참고 HTTP GET 응답에서 찾은 파일의 압축된 부분만 압축 해제할 수 있습니다.

- **Decompress SWF File(LZMA)(SWF** 파일 압축 해제**, LZMA)**은 Adobe ShockWave Flash(`.swf`) 파일의 LZMA 호환 가능 압축된 부분을 압축 해제합니다.
- **Decompress SWF File(SWF** 파일 압축 해제**, Deflate)**은 Adobe ShockWave Flash(`.swf`) 파일의 deflate 호환 가능 압축된 부분을 압축 해제합니다.

Maximum Compressed Data Depth(압축 데이터 최대 수준**)**, **Maximum Decompressed Data Depth(**압축 해제된 데이터 최대 수준**)** 또는 압축 해제된 데이터의 끝부분에 도달하면 압축 해제가 종료됩니다. **Unlimited Decompression(**무제한 압축 해제**)**을 선택하지 않은 경우 **Server Flow Depth(**서버 흐름 수준**)**에 도달하면 압축 해제된 데이터의 검사가 종료됩니다. `file_data` 침입 규칙 키워드를 사용하여 압축 해제된 데이터를 검사할 수 있습니다.

다음과 같이 규칙 120:12 및 120:13을 활성화하여 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

표 ***9: SWF*** 파일 압축 해제 옵션 규칙

규칙	다음 상황에서 트리거됩니다**.**
120:12	deflate 파일 압축 풀기에 실패합니다.
120:13	LZMA 파일 압축 풀기에 실패합니다.

PDF 파일 압축 해제**(Deflate)**

HTTP Inspect Responses(HTTP 응답 검사**)**가 활성화된 경우, **Decompress PDF File(Deflate)(PDF** 파일 압축 해제**, Deflate)**은HTTP 요청의 HTTP 응답 본문 내에 있는 Portable Document Format(`.pdf`) 파일의 deflate 호환 가능 압축된 부분을 압축 해제합니다. 시스템은 `/FlateDecode` 스트림 필터를 사용하는 PDF 파일의 압축만 해제할 수 있습니다. 다른 스트림 필터(`/FlateDecode /FlateDecode` 포함)는 지원되지 않습니다.

참고 HTTP GET 응답에서 찾은 파일의 압축된 부분만 압축 해제할 수 있습니다.

Maximum Compressed Data Depth(압축 데이터 최대 수준**)**, **Maximum Decompressed Data Depth(**압축 해제된 데이터 최대 수준**)** 또는 압축 해제된 데이터의 끝부분에 도달하면 압축 해제가 종료됩니다. **Unlimited Decompression(**무제한 압축 해제**)**을 선택하지 않은 경우 **Server Flow Depth(**서버 흐름 수준**)**에 도달하면 압축 해제된 데이터의 검사가 종료됩니다. `file_data` 침입 규칙 키워드를 사용하여 압축 해제된 데이터를 검사할 수 있습니다.

다음과 같이 규칙 120:14, 120:15, 120:16, 120:17을 활성화하여 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

표 ***10: PDF*** 파일 압축 해제***(Deflate)*** 옵션 규칙

규칙	다음 상황에서 트리거됩니다**.**
120:14	파일 압축 풀기에 실패합니다.
120:15	지원되지 않는 압축 유형 때문에 파일 압축 풀기에 실패합니다.
120:16	지원되지 않는 PDF 스트림 필터로 인해 파일 압축 풀기에 실패합니다.
120:17	파일 구문 분석에 실패합니다.

원래 클라이언트 **IP** 주소 추출

침입 검사 중에 원래 클라이언트 IP 주소 검사를 활성화합니다. 시스템은 XFF(X-Forwarded-For), True-Client-IP 또는 **XFF Header Priority(XFF** 헤더 우선 순위**)** 옵션에 정의하는 맞춤형 HTTP 헤더에서 원래 클라이언트 IP 주소를 추출합니다. 추출된 원래 클라이언트 IP 주소를 침입 이벤트 테이블에서 확인할 수 있습니다.

규칙 119:23, 119:29, 119:30 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.을 활성화할 수 있습니다.

XFF 헤더 우선 순위

HTTP 요청에 헤더가 여러 개 있을 때 시스템이 원래 클라이언트 IP HTTP 헤더를 처리할 순서를 지정합니다. 시스템은 기본적으로 XFF(X-Forwarded-For) 헤더를 검사한 다음 True-Client-IP 헤더를 검사합니다. 각 헤더 유형 옆에 있는 위쪽 및 아래쪽 화살표 아이콘을 사용하여 해당 우선 순위를 조정합니다.

또한 이 옵션을 통해 추출 및 평가용으로 XFF 또는 True-Client-IP 이외의 원래 클라이언트 IP 헤더를 지정할 수 있습니다. **Add(**추가**)**를 클릭하여 우선 순위 목록에 맞춤형 헤더 이름을 추가합니다. 시스템은 XFF 또는 True-Client-IP 헤더와 같은 구문을 사용하는 맞춤형 헤더만 지원합니다.

이 옵션을 구성할 때는 다음을 유의하시기 바랍니다.

- 시스템은 액세스 제어 및 침입 검사 둘 다를 위해 원래 클라이언트 IP 주소 헤더를 평가할 때 이 우선 순위 순서를 사용합니다.
- 원래 클라이언트 IP 헤더가 여러 개 있으면 시스템은 우선 순위가 가장 높은 헤더만 처리합니다.
- XFF 헤더는 요청이 통과한 프록시 서버를 나타내는 IP 주소 목록을 포함합니다. 스푸핑을 방지하기 위해 시스템은 목록의 마지막 IP 주소(신뢰할 수 있는 프록시가 추가된 주소)를 원래 클라이언트 IP 주소로 사용합니다.

URI 로그

HTTP 요청 패킷의 원시 URI 추출(있는 경우)을 활성화하고 세션에 대해 생성된 모든 침입 이벤트와 해당 URI를 연결합니다.

이 옵션을 활성화할 경우, 침입 이벤트 표 보기의 HTTP URI 열에서 추출한 URI의 첫 50자를 표시할 수 있습니다. 패킷 보기에서 전체 URI를 최대 2048바이트까지 표시할 수 있습니다.

호스트 이름 로그

HTTP 요청 호스트 헤더의 호스트 이름 추출(있는 경우)을 활성화하고 세션에 대해 생성된 모든 침입 이벤트와 해당 호스트 이름을 연결합니다. 여러 호스트 헤더가 있을 경우, 첫 번째 헤더에서 호스트 이름을 추출합니다.

이 옵션을 활성화할 경우, 침입 이벤트 표 보기의 HTTP Hostname(호스트 이름) 열에서 추출한 호스트 이름의 첫 50자를 표시할 수 있습니다. 패킷 보기에서 전체 호스트 이름을 최대 2048바이트까지 표시할 수 있습니다.

규칙 119:25를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

활성화된 119:24는 이 옵션의 설정에 상관없이 HTTP 요청에서 여러 호스트 헤더를 탐지하는 경우, 트리거됩니다.

프로파일

HTTP 트래픽에 표준화된 인코딩 유형을 지정합니다. 시스템은 대부분의 서버에 적절한 기본 프로파일, Apache 서버 및 IIS 서버의 기본 프로파일, 모니터링되는 트래픽의 요구 사항에 맞게 조정할 수 있는 맞춤형 기본 설정을 제공합니다.

- 모든 서버에 대해 적절한 표준 기본 프로파일을 사용하려면 **All(**모두**)**을 선택합니다.
- 시스템 제공 IIS 프로파일을 사용하려면 **IIS**를 선택합니다.
- 시스템 제공 Apache 프로파일을 사용하려면 **Apache**를 선택합니다.
- 자체 서버 프로파일을 생성하려면 **Custom(**맞춤형**)**을 선택합니다.

서버 레벨 **HTTP** 정상화 인코딩 옵션

HTTP 서버 수준 **Profile(**프로파일**)** 옵션을 `Custom(맞춤형)`으로 설정하면 HTTP 트래픽에 대해 표준화된 인코딩 유형을 지정하고, 다양한 인코딩 유형을 포함하는 트래픽에 대한 이벤트를 생성하도록 HTTP 전처리기 규칙을 활성화할 수 있습니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

ASCII 인코딩

인코딩된 ASCII 문자를 디코딩하고 규칙 엔진이 ASCII 인코딩된 URI에서 이벤트를 생성할지 여부를 지정합니다.

규칙 119:1을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

UTF-8 인코딩

URI에서 표준 UTF-8 유니코드 시퀀스를 디코딩합니다.

규칙 119:6을 활성화할 수 있습니다.이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

Microsoft %U 인코딩

4개 문자가 IIS 유니코드 코드 포인트와 관련이 있는 16진수로 인코딩된 값인 4개 문자가 뒤에 오는 %u를 사용하는 IIS %u 인코딩 체계를 디코딩합니다.

팁 적법한 클라이언트는 %u 인코딩을 거의 사용하지 않으며, 따라서 Cisco는 %u 인코딩으로 인코딩된 HTTP 트래픽을 디코딩할 것을 권장합니다.

규칙 119:3을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

베어 바이트 **UTF-8** 인코딩

UTF-8 값 디코딩 시 비ASCII 문자를 유효한 값으로 사용하는 베어 바이트 인코딩을 디코딩합니다.

팁 베어 바이트 인코딩을 사용하면 사용자는 IIS 서버를 에뮬레이트하고 비표준 인코딩을 정확하게 해석할 수 있습니다. 합법적인 클라이언트는 이런 방식으로 UTF-8을 인코딩하지 않으므로 Cisco는 이 옵션 활성화를 권장합니다.

규칙 119:4를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

Microsoft IIS 인코딩

유니코드 코드 포인트 매핑을 사용하여 디코딩합니다.

팁 이는 주로 공격 및 우회 시도에서 발견되므로 Cisco는 이 옵션 활성화를 권장합니다.

규칙 119:7을 활성화할 수 있습니다.이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

이중 인코딩

각각에서 디코딩을 수행하는 요청 URI를 통해 두 개 회선을 만들어 IIS 이중 인코딩된 트래픽을 디코딩합니다. 이는 주로 공격 시나리오에서 발견되므로 Cisco는 이 옵션 활성화를 권장합니다.

규칙 119:2를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

다중 슬래시 난독 처리

연속된 다중 슬래시를 단일 슬래시로 표준화합니다.

규칙 119:8을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

IIS 백슬래시 난독 처리

백슬래시를 사선으로 표준화합니다.

규칙 119:9를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

디렉토리 접근 공격

디렉토리 접근 공격 및 자기 참조 디렉토리를 표준화합니다. 이 트래픽 유형에 대한 이벤트를 생성하기 위해 해당 전처리기 규칙을 활성화하는 경우, 일부 웹사이트에서 디렉터리 접근 공격을 사용하는 파일을 참조하므로 잘못된 긍정이 생성될 수 있습니다.

규칙 119:10 및 119:11을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

탭 난독 처리

공백 구분 기호에 탭을 사용하는 비 RFC 표준을 표준화합니다. Apache 및 기타 비 IIS 웹 서버는 URL의 구분 기호로 탭 문자(0x09)를 사용합니다.

참고 이 옵션의 구성에 관계없이, 공백 문자(0x20)가 이 앞에 오는 경우 HTTP Inspect(HTTP 검사) 전처리기는 탭을 공백으로 처리합니다.

규칙 119:12를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

유효하지 않은 **RFC** 구분 기호

URI 데이터 내 행 바꿈(\n)을 표준화합니다.

규칙 119:13을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

Webroot 디렉토리 접근 공격

URL에서 초기 디렉토리를 가로질러 통과하는 디렉토리 접근 공격을 탐지합니다.

규칙 119:18을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

탭 **URI** 구분 기호

URI의 구분 기호로 탭 문자(0x09) 사용을 설정합니다. IIS의 Apache, 새 버전, 다른 웹 서버는 URL의 탭으로 구분 문자를 사용합니다.

참고 이 옵션의 구성에 관계없이, 공백 문자(0x20)가 이 앞에 오는 경우 HTTP Inspect(HTTP 검사) 전처리기는 탭을 공백으로 처리합니다.

비 **RFC** 문자

사용자가 추가한 비 RFC 문자 목록이 수신 및 발신 URI 데이터에 나타날 때 해당 필드에서 이를 탐지합니다. 이 필드를 수정할 경우, 바이트 문자를 나타내는 16진수 형식을 사용합니다. 이 옵션을 구성할 경우 값을 신중하게 설정합니다. 매우 일반적인 문자를 사용하면 이벤트가 과하게 생성될 수 있습니다.

규칙 119:14를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

최대 청크 인코딩 크기

URI 데이터에서 비정상적으로 큰 청크 크기를 탐지합니다.

규칙 119:16 및 119:22를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

파이프라인 디코딩 비활성화

파이프라인 요청에 대한 HTTP 디코딩을 비활성화합니다. 이 옵션을 비활성화하면, 파이프라인에 대기 중인 HTTP 요청이 디코딩되거나 분석되지 않고, 일반 패턴 일치만 사용하여 검사되기 때문에 성능이 향상됩니다.

엄격하지 않은 **URI** 구문 분석

엄격하지 않은 URI 구문 분석을 활성화합니다. "GET /index.html abc xo qr \n" 형식에서 비표준 URI를 수용하는 서버에서만 이 옵션을 사용합니다. 이 옵션을 사용하면, 두 번째 스페이스 뒤에 유효한 HTTP 식별자가 없는 경우에도 디코더는 URI가 첫 번째와 두 번째 스페이스 사이에 있다고 가정합니다.

확장된 **ASCII** 인코딩

HTTP 요청 URI 내 확장된 ASCII 문자의 구문 분석을 활성화합니다. 이 옵션은 사용자 지정 서버 프로파일에서만 사용 가능하며, Apache, IIS 또는 모든 서버에 제공된 기본 프로파일에서는 그렇지 않다는 점에 유의하십시오.

관련 항목

개요: HTTP content 및 protected_content 키워드 인수

HTTP 검사 전처리기 설정

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

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

시작하기 전에

- 맞춤형 대상 기반 정책에서 식별하려는 네트워크가 상위 네트워크 분석 정책이 처리한 네트워크, 영역 및 VLAN 하위 집합과 일치하는지 확인합니다. 자세한 내용은 네트워크 분석 정책 고급 설정를 참조하십시오.

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** **Application Layer Preprocessors(**애플리케이션 계층 전처리기**)**의 **HTTP Configuration(HTTP** 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

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

단계 **7** Global Settings(전역 설정) 페이지 영역의 옵션을 수정합니다(전역 HTTP 정상화 옵션, 28 페이지 참조).

단계 **8** 다음 3가지 옵션을 사용할 수 있습니다.

- 서버 프로파일 추가 - **Servers(**서버**)** 섹션 옆에 있는 **Add(**추가**)** ( )을 클릭합니다. **Server Address(**서버 주소**)** 필드에 하나 이상의 클라이언트 IP 주소를 지정하고 **OK(**확인**)**를 클릭합니다. 단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다. 목록에 최대 496개의 문자를 포함할 수 있고, 모든 서버 프로파일에 대해 총 256개

의 주소 항목을 지정할 수 있으며, 기본 프로파일을 포함하여 총 255개의 프로파일을 생성할 수 있습니다.

- 서버 프로파일 편집 - **Servers(**서버**)**에 추가한 프로파일에 대해 설정된 주소를 클릭하거나 **default(**기본값**)**를 클릭합니다. **Configuration(**설정**)** 섹션에서 설정을 수정할 수 있습니다(서버 레벨 HTTP 정상화 옵션, 29 페이지 참조). 또한 **Custom(**맞춤형**)**를 **Profile(**프로파일**)** 값으로 선택하면 서버 레벨 HTTP 정상화 인코딩 옵션, 38 페이지에서 설명하는 인코딩 옵션을 수정할 수 있습니다.
- 서버 프로파일 삭제 - 맞춤형 프로파일 옆에 있는 **Delete(**삭제**)** ( )을 클릭합니다.

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 HTTP 전처리기 규칙(GID 119)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정를 참고하십시오.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

레이어 관리
충돌 및 변경: 네트워크 분석 및 침입 정책

추가 HTTP 검사 전처리기 규칙

다음 표의 **Preprocessor Rule GID:SID(**전처리기 규칙 **GID:SID)** 열에서 규칙을 활성화하여 특정 구성 옵션과 관련이 없는 HTTP Inspect(HTTP 검사) 전처리기 규칙에 대한 이벤트를 생성할 수 있습니다.

표 ***11:*** 추가 ***HTTP*** 검사 전처리기 규칙

전처리기 규칙 **GID:SID**	다음 상황에서 트리거 됩니다.
119:21	HTTP 요청 헤더에 둘 이상의 `content-length(콘텐츠 길이)` 필드가 있음.
119:24	HTTP 요청에 둘 이상의 Host(호스트) 헤더가 있음.
119:28	HTTP POST 메서드에는 `content-length` 헤더와 청크 분할된 `transfer-encoding`이 포함되어 있지 않습니다.
119:32	HTTP 버전 0.9가 트랙픽에서 발생함. TCP 스트림 구성 역시 활성화되어야 한다는 점에 유의하십시오.

전처리기 규칙 **GID:SID**	다음 상황에서 트리거 됩니다.
119:33	HTTP URI가 이스케이프되지 않은 스페이스를 포함함.
119:34	TCP 연결이 24개 이상의 파이프라인 처리된 HTTP 요청을 포함함.
120:5	HTTP 응답 트래픽에서 UTF-7 인코딩이 발생함. UTF-7은 SMTP 트래픽에서와 같이 7비트 패리티가 필요한 경우에만 표시되어야 합니다.
120:8	`content-length` 또는 청크 크기가 유효하지 않습니다.
120:18	HTTP 서버 응답이 클라이언트가 요청하기 전에 발생함.
120:19	HTTP 응답이 여러 콘텐츠 길이를 포함함.
120:20	HTTP 응답이 여러 콘텐츠 인코딩을 포함함.
120:25	HTTP 응답이 잘못된 헤더 포딩을 포함함.
120:26	스팸 회선이 HTTP 응답 헤더 전에 발생함.
120:27	HTTP 응답이 헤더의 끝을 포함하지 않음.
120:28	잘못된 청크 크기가 발생하거나 청크 크기 뒤에 정크 문자가 있음.

Sun RPC 전처리기

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

RPC(원격 절차 호출) 표준화가 조각화된 RPC 레코드를 가져와 단일 레코드로 표준화하므로 규칙 엔진이 전체 레코드를 검사할 수 있습니다. 예를 들어, 공격자는 RPC `admind`가 실행되는 포트를 검색하려고 시도할 수 있습니다. 일부 UNIX 호스트는 RPC `admind`를 사용하여 원격 배포된 시스템 작업을 수행합니다. 호스트가 보안성이 낮은 인증을 수행할 경우, 악의적인 사용자가 원격 관리를 적용할 수 있습니다. Snort ID(SID) 575가 포함된 표준 텍스트 규칙(GID: 1)은 특정 위치의 콘텐츠를 검색해 이 공격을 탐지하여 부적절한 `portmap GETPORT` 요청을 식별합니다.

Sun RPC 전처리기 옵션

포트

트래픽을 표준화할 포트를 지정합니다. 인터페이스에서, 쉼표로 구분하여 여러 개의 포트를 나열합니다. 일반적인 RPC 포트는 111 및 32771입니다. 네트워크가 다른 포트에 RPC 트래픽을 전송할 경우 이들의 추가를 고려하십시오.

조각화된 **RPC** 레코드 탐지

조각화된 RPC 레코드를 탐지합니다.

규칙 106:1 및 106:5를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

1개의 패킷에서 여러 레코드 탐지

패킷(또는 리어셈블된 패킷)당 1개 이상의 RPC 요청을 탐지합니다.

규칙 106:2를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

단일 조각을 초과하는 조각화된 레코드 총합 탐지

현재 패킷 길이를 초과하는 리어셈블된 조각 레코드 길이를 탐지합니다.

규칙 106:3을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

1개의 패킷 크기를 초과하는 단일 조각 레코드 탐지

일부 레코드를 탐지합니다.

규칙 106:4를 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

Sun RPC 전처리기 구성

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

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** **Application Layer Preprocessors(**애플리케이션 계층 전처리기**)**의 **Sun RPC Configuration(Sun RPC** 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **6** **Sun RPC Configuration(Sun RPC** 설정**)** 옆에 있는 **Edit(**수정**)** (✎)을 클릭합니다.

단계 **7** Sun RPC 전처리기 옵션, 44 페이지에서 설명하는 설정을 수정합니다.

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 Sun RPC 전처리기 규칙(GID 106)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정를 참고하십시오.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

레이어 관리
충돌 및 변경: 네트워크 분석 및 침입 정책

SIP 전처리기

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

SIP(세션 시작 프로토콜)는 인터넷 텔레포니, 멀티미디어 컨퍼런싱, 인스턴트 메시징, 온라인 게임 및 파일 전송과 같은 클라이언트 애플리케이션의 한 명 이상의 사용자를 위한 하나 이상의 세션을 가진 통화 설정, 수정 및 세분화를 제공합니다. 각 SIP 요청의 *method(*메서드*)* 필드는 요청의 목적을 확인하고, Request-URI는 요청을 전송할 위치를 지정합니다. 각 SIP 응답의 상태 코드는 요청된 작업의 결과를 나타냅니다.

통화가 SIP를 사용하여 설치되면 RTP(실시간 전송 프로토콜)가 이후의 오디오 및 비디오 커뮤니케이션을 담당합니다. 세션의 이 부분은 경우에 따라 통화 채널, 데이터 채널 또는 오디오/비디오 데이터 채널로 지칭됩니다. RTP는 데이터 채널 파라미터 협상, 세션 공지 및 세션 초대를 위한 SIP 메시지 본문 내에서 SDP(세션 설명 프로토콜)를 사용합니다.

SIP 전처리기는 다음과 같은 작업을 담당합니다.

- SIP 2.0 트래픽 디코딩 및 분석
- SDP 데이터가 있는 경우 이를 포함하여 SIP 헤더 및 메시지 본문 추출, 추가 검사를 위해 규칙 엔진에 추출된 데이터 전달
- 다음 조건이 탐지되고 해당 전처리기 규칙이 활성화된 경우 이벤트를 생성:
  - 이상 징후 및 취약성 SIP 패킷 내의 알려진 취약성
  - 비순차 및 잘못된 통화 시퀀스
- 또는 통화 채널 무시

전처리기는 SIP 메시지 본문에 내장된 SDP 메시지에서 식별된 포트에 따라 RTP 채널을 식별하지만, 전처리기는 RTP 프로토콜 검사를 제공하지 않습니다.

SIP 전처리기를 사용하는 경우 다음 사항에 유의하십시오.

- UDP는 일반적으로 SIP에서 지원되는 미디어 세션을 전송합니다. UDP 스트림 전처리는 SIP 전처리기에 SIP 세션 추적을 제공합니다.
- SIP 규칙 키워드를 통해 SIP 패킷 헤더 또는 메시지 본문으로 이동하고 특정 SIP 메서드 또는 상태 코드의 패킷에 대한 탐지를 제한할 수 있습니다.

SIP 전처리기 옵션

다음 옵션의 경우, 1부터 65535바이트까지의 양수 값을 지정하거나 0을 지정해 연결된 규칙의 활성화 여부에 상관없이 옵션에서 이벤트 생성을 비활성화할 수 있습니다.

- 요청 **URI** 최대 길이
- 통화 **ID** 최대 길이
- 요청 이름 최대 길이
- 발신지 최대 길이
- 수신지 최대 길이
- 경유지 최대 길이
- 접촉 최대 길이
- 콘텐츠 최대 길이

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

포트

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

점검할 메서드

탐지할 SIP 메서드를 지정합니다. 다음 중 하나로 현재 정의된 SIP 메서드를 지정할 수 있습니다.

```
ack, benotify, bye, cancel, do, info, invite, join, message,
notify, options, prack, publish, quath, refer, register,
service, sprack, subscribe, unsubscribe, update
```

메서드는 대소문자를 구분하지 않습니다. 메서드 이름은 알파벳 문자, 숫자 및 밑줄 문자를 포함할 수 있습니다. 다른 특수 문자는 허용되지 않습니다. 메서드가 여러 개인 경우 쉼표로 구분하십시오.

향후 새 SIP 메서드가 정의될 수도 있기 때문에, 사용자의 구성은 현재 정의되지 않은 영문자열을 포함할 수 있습니다. 시스템은 최대 32개의 메서드까지 지원하는데, 최근 정의된 메서드 21개에 메서드 11개를 추가한 것입니다. 시스템은 사용자가 구성할 수 있는 정의되지 않은 모든 메서드를 무시합니다.

이 옵션에 지정한 메서드 외에도 총 32개의 메서드에는 침입 규칙에서 `sip_method` 키워드를 사용하여 지정된 메서드가 포함된다는 점에 유의하십시오.

세션 내 최대 대화 상자

스트림 세션 내에서 허용되는 최대 대화 상자 수를 지정합니다. 이 숫자보다 많은 대화 상자가 생성되는 경우 대화 상자 수가 지정된 최대 수를 초과하지 않을 때까지 가장 오래된 대화 상자부터 삭제됩니다. 1에서 4194303까지의 정수를 지정할 수 있습니다.

규칙 140:27을 활성화할 수 있습니다. 이벤트를 생성하고, 인라인 구축에서 이 옵션에 문제가 되는 패킷을 삭제합니다. 침입 규칙 상태 설정의 내용을 참조하십시오.

요청 **URI** 최대 길이

Request-URI 헤더 필드에서 허용할 최대 바이트 수를 지정합니다. 규칙 140:3이 활성화된 경우 더 긴 URI가 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.합니다. 요청 URI 필드는 요청에 대한 대상 경로 또는 페이지를 나타냅니다.

통화 **ID** 최대 길이

요청 또는 응답 Call-ID 헤더 필드에서 허용할 최대 바이트 수를 지정합니다. 규칙 140:5가 활성화된 경우 더 긴 Call-ID가 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.합니다. Call-ID 필드는 요청 및 응답에서 SIP 세션을 고유하게 식별합니다.

요청 이름 최대 길이

CSeq 트랜잭션 식별자에 지정된 메서드의 이름인 요청 이름에서 허용할 최대 바이트 수를 지정합니다. 규칙 140:7이 활성화된 경우 더 긴 요청 이름이 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.합니다.

발신지 최대 길이

요청 또는 응답 From 헤더 필드에서 허용할 최대 바이트 수를 지정합니다. 규칙 140:9가 활성화된 경우 더 긴 From 필드에서 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.합니다. From 필드는 메시지 초기자를 식별합니다.

수신지 최대 길이

요청 또는 응답 To 헤더 필드에서 허용할 최대 바이트 수를 지정합니다. 규칙 140:11이 활성화된 경우 더 긴 To 필드에서 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.합니다. To 필드는 메시지 수신자를 식별합니다.

경유지 최대 길이

요청 또는 응답 Via 헤더 필드에서 허용할 최대 바이트 수를 지정합니다. 규칙 140:13이 활성화된 경우 더 긴 Via 필드가 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.합니다. Via 필드는 요청이 뒤따르는 경로를 제공하며, 응답에서는 수신 정보를 제공합니다.

접촉 최대 길이

요청 또는 응답 Contact 헤더 필드에서 허용할 최대 바이트 수를 지정합니다. 규칙 140:15가 활성화된 경우 더 긴 Contact 필드에서 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.합니다. Contact 필드는 이후의 메시지와 접촉할 위치를 지정하는 URI를 제공합니다.

콘텐츠 최대 길이

요청 또는 응답 메시지 본문의 콘텐츠에서 허용할 최대 바이트 수를 지정합니다. 규칙 140:16이 활성화된 경우 더 긴 콘텐츠가 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.합니다.

오디오/비디오 데이터 채널 무시

데이터 채널 트래픽에 대한 검사를 활성화 및 비활성화합니다. 이 옵션을 활성화하면 전처리기는 비데이터 채널 SIP 트래픽에 대한 검사를 계속합니다.

관련 항목

SIP 키워드

SIP 전처리기 구성

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

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** **Application Layer Preprocessors(**애플리케이션 계층 전처리기**)**의 **SIP Configuration(SIP** 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **6** **SIP Configuration(SIP** 설정**)** 옆에 있는 편집 아이콘**(Edit(**수정**)** ( ))을 클릭합니다.

단계 **7** SIP 전처리기 옵션, 47 페이지에 설명된 대로 옵션을 수정합니다.

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 SIP 전처리기 규칙(GID 140)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정를 참고하십시오.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

레이어 관리
충돌 및 변경: 네트워크 분석 및 침입 정책

추가 SIP 전처리기 규칙

다음 표의 SIP 전처리기 규칙은 특정 구성 옵션과 관련이 없습니다. 다른 SIP 전처리기 규칙에서와 마찬가지로 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하고 싶다면 이러한 규칙을 활성화해야 합니다.

표 *12:* 추가 *SIP* 전처리기 규칙

전처리기 규칙 **GID:SID**	다음 상황에서 트리거 됩니다**.**
140:1	전처리기가 시스템에서 허용되는 SIP 세션의 최대 수를 모니터링하고 있음.
140:2	요청된 Request_URI 필드가 SIP 요청에서 비어 있음.
140:4	Call-ID 헤더 필드가 SIP 요청 또는 응답에서 비어 있음.

전처리기 규칙 **GID:SID**	다음 상황에서 트리거 됩니다.
140:6	SIP 요청 또는 응답 CSeq 필드의 시퀀스 번호 값이 231보다 작은 32비트 무부호 정수가 아님.
140:8	From 헤더 필드가 SIP 요청 또는 응답에서 비어 있음.
140:10	To 헤더 필드가 SIP 요청 또는 응답에서 비어 있음.
140:12	Via 헤더 필드가 SIP 요청 또는 응답에서 비어 있음.
140:14	요청된 Contact 헤더 필드가 SIP 요청 또는 응답에서 비어 있음.
140:17	UDP 트래픽의 단일 SIP 요청 또는 응답 패킷이 여러 메시지를 포함함. 이전 버전의 SIP는 여러 메시지를 지원했지만 SIP 2.0은 패킷당 1개의 메시지만 지원한다는 점에 유의하십시오.
140:18	UDP 트래픽의 SIP 요청 또는 응답에서 메시지 본문의 실제 길이가 SIP 요청 또는 응답 내 Content-Length 헤더 필드에 지정된 값과 다름.
140:19	전처리기가 SIP 응답의 CSeq 필드에서 메서드 이름을 인식하지 못함.
140:20	SIP 서버가 입증된 초대 메시지에 이의를 제기하지 않음. 이는 InviteReplay 청구 공격의 경우 발생한다는 점에 유의하십시오.
140:21	통화가 설정되기 전에 세션 정보가 변경됨. 이는 FakeBusy 청구 공격의 경우 발생한다는 점에 유의하십시오.
140:22	응답 상태 코드가 3자리 수가 아님.
140:23	Content-Type(콘텐츠 유형) 헤더 필드가 콘텐츠 형식을 지정하지 않고 메시지 텍스트가 데이터를 포함함.
140:24	SIP 버전이 1, 1.1, 또는 2.0가 아님.
140:25	CSeq 헤더 및 메서드 필드에 지정된 메서드가 SIP 요청과 일치하지 않음.
140:26	전처리기가 SIP 요청 방법 필드에서 명명된 메서드를 인식하지 못함.

GTP 전처리기

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

GTP(GPRS[General Service Packet Radio] 터널링 프로토콜)는 GTP 코어 네트워크를 통한 통신을 제공합니다. GTP 전처리기는 GTP 트래픽 내 이상 징후를 탐지하고 검사를 위해 규칙 엔진에 명령 채널 신호 메시지를 전달합니다. `gtp_version`, `gtp_type` 및 `gtp_info` 규칙 키워드를 사용하여 익스플로잇 탐지를 위해 GTP 명령 채널 트래픽을 검사할 수 있습니다.

단일 구성 옵션을 사용하면 전처리기가 GTP 명령 채널 메시지를 검사하는 포트의 기본 설정을 변경할 수 있습니다.

GTP 전처리기 규칙

GTP 전처리기 규칙이 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하게 하려면 다음 표에서 해당 규칙을 활성화해야 합니다.

표 ***13: GTP*** 전처리기 규칙

전처리기 규칙 **GID:SID**	설명
143:1	전처리기가 유효하지 않은 메시지 길이를 탐지하면 이벤트를 생성합니다.
143:2	전처리기가 유효하지 않은 정보 요소 길이를 탐지하면 이벤트를 생성합니다.
143:3	전처리기가 비순차적 정보 요소를 탐지하면 이벤트를 생성합니다.

GTP 전처리기 설정

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

이 절차를 수행하여 GTP 전처리기가 GTP 명령 메시지를 모니터링하는 포트를 수정할 수 있습니다.

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** 왼쪽 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.

단계 **5** **Application Layer Preprocessors(**애플리케이션 계층 전처리기**)**의 **GTP Command Channel Configuration(GTP** 명령 채널 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **6** **GTP Command Channel Configuration(GTP** 명령 채널 설정**)** 옆에 있는 **Edit(**수정**)** (✎)을 클릭합니다.

단계 **7** **Ports(**포트**)** 값을 입력합니다.

포트가 여러 개인 경우 쉼표로 구분하십시오.

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

- 침입 이벤트를 활성화하려면 GTP 전처리기 규칙(GID 143)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정를 참고하십시오.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

IMAP 전처리기

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

Internet Message Application Protocol(인터넷 메시지 애플리케이션 프로토콜, IMAP)을 사용하여 원격 IMAP 서버의 이메일을 검색합니다. IMAP 전처리기는 서버-클라이언트 IMAP4 트래픽을 검사하고 관련 전처리기 규칙이 활성화되면 변칙 트래픽에 이벤트를 생성합니다. 전처리기는 또한 클라이언트-서버 IMAP4 트래픽의 이메일 첨부 파일을 추출하여 디코딩하고 규칙 엔진에 첨부 파일 데이터를 보낼 수 있습니다. 첨부 파일 데이터를 지정할 때 침입 규칙에서 `file_data` 키워드를 사용할 수 있습니다.

여러 첨부 파일이 있는 경우 추출 및 디코딩에 포함되며, 여러 패킷을 포괄하는 큰 첨부 파일도 포함됩니다.

IMAP 전처리기 옵션

MIME 이메일 첨부 파일에 디코딩이 필요하지 않은 경우 디코딩 또는 추출에는 여러 첨부 파일(있는 경우) 및 여러 패킷을 포괄하는 큰 첨부 파일이 포함된다는 점에 유의하십시오.

또한 다음 상황에서 **Base64 Decoding Depth(Base64** 디코딩 수준**)**, **7-Bit/8-Bit/Binary Decoding Depth(7**비트**/8**비트**/**이진 디코딩 수준**)**, **Quoted-Printable Decoding Depth(**따옴표로 묶인 인쇄 가능한 디코딩 수준**)** 또는 **Unix-to-Unix Decoding Depth(Unix-to-Unix** 디코딩 수준**)** 옵션의 값이 서로 다를 때 가장 높은 값이 사용된다는 점에 유의하십시오.

- 기본 네트워크 분석 정책
- 동일한 액세스 제어 정책의 네트워크 분석 규칙에서 호출된 기타 사용자 지정 네트워크 분석 정책

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

포트

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

Base64 디코딩 수준

Base64로 인코딩된 각 MIME 이메일 첨부 파일에서 추출하고 디코딩할 최대 바이트 수를 지정합니다. 양수를 지정할 수 있으며, 0을 지정하여 모든 Base64 데이터를 디코딩할 수도 있습니다. Base64 데이터를 무시하려면 -1을 지정합니다.

4로 나누어지지 않는 양수는 다음 4의 배수로 올림 처리된다는 점에 유의하십시오. 이때 65533, 65534, 및 65535 값은 제외되는데, 이들은 65532로 내림 처리됩니다.

이 옵션이 활성화된 경우, 규칙 141:4를 활성화하여 디코딩이 실패할 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 예를 들어 유효하지 않은 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다.

7비트**/8**비트**/**이진 디코딩 수준

디코딩이 필요하지 않은 각 MIME 이메일 첨부 파일에서 추출할 데이터의 최대 바이트를 지정합니다. 이 첨부 파일 형식에는 평문, jpeg 이미지, mp3 파일 등과 같이 7비트, 8비트, 이진 및 다양한 다중 부분 콘텐츠 형식 등이 있습니다. 양수 값을 지정할 수 있으며, 0을 지정하여 패킷의 모든 데이터를 추출할 수도 있습니다. 디코딩되지 않은 데이터를 무시하려면 -1을 지정합니다.

이 옵션이 활성화된 경우, 규칙 141:6을 활성화하여 추출이 실패할 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 예를 들어 손상된 데이터로 인해 추출이 실패할 수 있습니다.

따옴표로 묶인 인쇄 가능한 디코딩 수준

QP(Quoted-Printable)로 인코딩된 각 MIME 이메일 첨부 파일에서 추출 및 디코딩할 최대 바이트 수를 지정합니다. 양수를 지정할 수 있으며, 0을 지정하여 패킷의 모든 QP 인코딩 데이터를 디코딩할 수도 있습니다. QP로 인코딩된 데이터를 무시하려면 -1을 지정합니다.

이 옵션이 활성화된 경우, 규칙 141:5를 활성화하여 디코딩이 실패할 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 예를 들어 유효하지 않은 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다.

Unix-to-Unix 디코딩 수준

Unix-to-Unix로 인코딩된(uuencoded) 각 이메일 첨부 파일에서 추출 및 디코딩할 최대 바이트 수를 지정합니다. 양수를 지정할 수 있으며, 0을 지정하여 패킷의 모든 비인코딩 데이터를 디코딩할 수도 있습니다. uuencoded 데이터를 무시하려면 -1을 지정합니다.

이 옵션이 활성화된 경우, 규칙 141:7을 활성화하여 디코딩이 실패할 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 예를 들어 유효하지 않은 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다.

관련 항목

file_data 키워드

IMAP 전처리기 구성

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

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 **Application Layer Preprocessors(**애플리케이션 계층 전처리기**)**의 **IMAP Configuration(IMAP** 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

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

단계 7 IMAP 전처리기 옵션, 54 페이지에서 설명하는 설정을 수정합니다.

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

- 침입 이벤트를 활성화하려면 IMAP 전처리기 규칙(GID 141)을 활성화합니다(침입 규칙 상태 설정 참조).
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

침입 및 네트워크 분석 정책의 레이어
충돌 및 변경: 네트워크 분석 및 침입 정책

추가 IMAP 전처리기 규칙

다음 표의 IMAP 전처리기 규칙은 특정 구성 옵션과 관련이 없습니다. 다른 IMAP 전처리기 규칙에서와 마찬가지로 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하고 싶다면 이러한 규칙을 활성화해야 합니다.

표 *14:* 추가 *IMAP* 전처리기 규칙

전처리기 규칙 **GID:SID**	설명
141:1	전처리기가 RFC 3501에 정의되지 않은 클라이언트 명령을 탐지하면 이벤트를 생성합니다.
141:2	전처리기가 RFC 3501에 정의되지 않은 서버 응답을 탐지하면 이벤트를 생성합니다.
141:3	전처리기가 시스템에서 허용되는 최대 메모리 양을 사용하는 경우 이벤트를 생성합니다. 여기서, 전처리기는 메모리를 사용할 수 있을 때까지 디코딩을 중지합니다.

POP 전처리기

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

Post Office Protocol(포스트 오피스 프로토콜, POP)을 사용하여 원격 POP 서버의 이메일을 검색합니다. POP 전처리기는 서버-클라이언트 POP3 트래픽을 검사하고 관련 전처리기 규칙이 활성화되면 변칙 트래픽에 이벤트를 생성합니다. 전처리기는 또한 클라이언트-서버 POP3 트래픽의 이메일 첨부 파일을 추출 및 디코딩하고 규칙 엔진에 첨부 파일 데이터를 보낼 수 있습니다. 첨부 파일 데이터를 지정할 때 침입 규칙에서 `file_data` 키워드를 사용할 수 있습니다.

여러 첨부 파일이 있는 경우 추출 및 디코딩에 포함되며, 여러 패킷을 포괄하는 큰 첨부 파일도 포함됩니다.

POP 전처리기 옵션

MIME 이메일 첨부 파일에 디코딩이 필요하지 않은 경우 디코딩 또는 추출에는 여러 첨부 파일(있는 경우) 및 여러 패킷을 포괄하는 큰 첨부 파일이 포함된다는 점에 유의하십시오.

또한 다음 상황에서 **Base64 Decoding Depth(Base64** 디코딩 수준**)**, **7-Bit/8-Bit/Binary Decoding Depth(7**비트**/8**비트**/**이진 디코딩 수준**)**, **Quoted-Printable Decoding Depth(**따옴표로 묶인 인쇄 가능한 디코딩 수준**)** 또는 **Unix-to-Unix Decoding Depth(Unix-to-Unix** 디코딩 수준**)** 옵션의 값이 서로 다를 때 가장 높은 값이 사용된다는 점에 유의하십시오.

- 기본 네트워크 분석 정책
- 동일한 액세스 제어 정책의 네트워크 분석 규칙에서 호출된 기타 사용자 지정 네트워크 분석 정책

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

포트

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

Base64 디코딩 수준

Base64로 인코딩된 각 MIME 이메일 첨부 파일에서 추출하고 디코딩할 최대 바이트 수를 지정합니다. 양수를 지정할 수 있으며, 0을 지정하여 모든 Base64 데이터를 디코딩할 수도 있습니다. Base64 데이터를 무시하려면 -1을 지정합니다.

4로 나누어지지 않는 양수는 다음 4의 배수로 올림 처리된다는 점에 유의하십시오. 이때 65533, 65534, 및 65535 값은 제외되는데, 이들은 65532로 내림 처리됩니다.

이 옵션이 활성화된 경우, 규칙 142:4를 활성화하여 디코딩이 실패할 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 예를 들어 유효하지 않은 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다.

7비트**/8**비트**/**이진 디코딩 수준

디코딩이 필요하지 않은 각 MIME 이메일 첨부 파일에서 추출할 데이터의 최대 바이트를 지정합니다. 이 첨부 파일 형식에는 평문, jpeg 이미지, mp3 파일 등과 같이 7비트, 8비트, 이진 및 다양한 다중 부분 콘텐츠 형식 등이 있습니다. 양수 값을 지정할 수 있으며, 0을 지정하여 패킷의 모든 데이터를 추출할 수도 있습니다. 디코딩되지 않은 데이터를 무시하려면 -1을 지정합니다.

이 옵션이 활성화된 경우, 규칙 142:6을 활성화하여 추출이 실패할 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 예를 들어 손상된 데이터로 인해 추출이 실패할 수 있습니다.

따옴표로 묶인 인쇄 가능한 디코딩 수준

QP(Quoted-Printable)로 인코딩된 각 MIME 이메일 첨부 파일에서 추출 및 디코딩할 최대 바이트 수를 지정합니다. 양수를 지정할 수 있으며, 0을 지정하여 패킷의 모든 QP 인코딩 데이터를 디코딩할 수도 있습니다. QP로 인코딩된 데이터를 무시하려면 -1을 지정합니다.

이 옵션이 활성화된 경우, 규칙 142:5를 활성화하여 디코딩이 실패할 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 예를 들어 유효하지 않은 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다.

Unix-to-Unix 디코딩 수준

Unix-to-Unix로 인코딩된(uuencoded) 각 이메일 첨부 파일에서 추출 및 디코딩할 최대 바이트 수를 지정합니다. 양수를 지정할 수 있으며, 0을 지정하여 패킷의 모든 비인코딩 데이터를 디코딩할 수도 있습니다. uuencoded 데이터를 무시하려면 -1을 지정합니다.

이 옵션이 활성화된 경우, 규칙 142:7을 활성화하여 디코딩이 실패할 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 예를 들어 유효하지 않은 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다.

관련 항목

- 레이어 관리
- 충돌 및 변경: 네트워크 분석 및 침입 정책
- file_data 키워드

POP 전처리기 구성

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

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** **Application Layer Preprocessors(**애플리케이션 계층 전처리기**)**의 **POP Configuration(POP** 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

단계 **6** **POP Configuration(POP** 구성**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **7** POP 전처리기 옵션, 57 페이지에서 설명하는 설정을 수정합니다.

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

- 침입 이벤트를 활성화하려면 POP 전처리기 규칙(GID 142)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정를 참고하십시오.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

레이어 관리
충돌 및 변경: 네트워크 분석 및 침입 정책

추가 **POP** 전처리기 규칙

다음 표의 POP 전처리기 규칙은 특정 구성 옵션과 관련이 없습니다. 다른 POP 전처리기 규칙에서와 마찬가지로 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하고 싶다면 이러한 규칙을 활성화해야 합니다.

표 *15:* 추가 *POP* 전처리기 규칙

전처리기 규칙 **GID:SID**	설명
142:1	전처리기가 RFC 1939에 정의되지 않은 클라이언트 명령을 탐지하면 이벤트를 생성합니다.
142:2	전처리기가 RFC 1939에 정의되지 않은 서버 응답을 탐지하면 이벤트를 생성합니다.
142:3	전처리기가 시스템에서 허용되는 최대 메모리 양을 사용하는 경우 이벤트를 생성합니다. 여기서, 전처리기는 메모리를 사용할 수 있을 때까지 디코딩을 중지합니다.

SMTP 전처리기

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

SMTP 전처리기는 규칙 엔진이 SMTP 명령을 표준화하도록 지시합니다. 전처리기는 또한 클라이언트-서버 트래픽의 이메일 첨부 파일을 추출하고 디코딩할 수 있습니다. 그리고, SMTP 트래픽에서 트리거된 침입 이벤트를 표시할 경우 이메일 파일 이름, 주소 및 헤더 데이터를 소프트웨어 버전에 따라 추출하여 컨텍스트를 제공할 수 있습니다.

SMTP 전처리기 옵션

표준화를 활성화하거나 비활성화하고, SMTP 디코더가 탐지하는 변칙 트래픽 유형을 제어하는 옵션을 구성할 수 있습니다.

MIME 이메일 첨부 파일에 디코딩이 필요하지 않은 경우 디코딩 또는 추출에는 여러 첨부 파일(있는 경우) 및 여러 패킷을 포괄하는 큰 첨부 파일이 포함된다는 점에 유의하십시오.

또한 다음 상황에서 **Base64 Decoding Depth(Base64** 디코딩 수준**)**, **7-Bit/8-Bit/Binary Decoding Depth(7**비트**/8**비트/이진 디코딩 수준**)**, **Quoted-Printable Decoding Depth(**따옴표로 묶인 인쇄 가능한 디코딩 수준**)** 또는 **Unix-to-Unix Decoding Depth(Unix-to-Unix** 디코딩 수준**)** 옵션의 값이 서로 다를 때 가장 높은 값이 사용된다는 점에 유의하십시오.

- 기본 네트워크 분석 정책
- 동일한 액세스 제어 정책의 네트워크 분석 규칙에서 호출된 기타 사용자 지정 네트워크 분석 정책

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

포트

SMTP 트래픽을 표준화할 포트를 지정합니다. 0 이상의 값을 지정할 수 있습니다. 포트가 여러 개인 경우 쉼표로 구분하십시오.

상태 저장 검사

이를 선택하면, SMTP 디코더가 상태를 저장하고 개별 패킷을 위한 세션 컨텍스트를 제공하며, 리어셈블한 세션만 검사할 수 있습니다. 이를 취소하면, 세션 컨텍스트 없이 각 개별 패킷을 분석합니다.

표준화

`All(모두)`로 설정된 경우, 모든 명령을 표준화합니다. 명령 다음에 나오는 하나 이상의 공백 문자를 확인합니다.

`None(없음)`으로 설정된 경우, 어떤 명령도 표준화하지 않습니다.

`Cmds`로 설정된 경우, **Custom Commands(**맞춤형 명령**)**에 나열된 명령을 표준화합니다.

사용자 지정 명령

Normalize(표준화**)**가 `Cmds`로 설정된 경우, 나열된 명령을 표준화합니다.

텍스트 상자에서 표준화되어야 하는 명령을 지정합니다. 명령 다음에 나오는 하나 이상의 공백 문자를 확인합니다.

스페이스(ASCII 0x20) 및 탭(ASCII 0x09) 문자는 표준화를 위한 공백 문자로 간주됩니다.

데이터 무시

메일 데이터를 처리하지 않습니다. MIME 메일 헤더 데이터만 처리합니다.

TLS 데이터 무시

Transport Layer Security(전송 레이어 보안) 프로토콜의 암호화된 데이터를 처리하지 않습니다.

경고 없음

동반되는 전처리기 규칙이 활성화된 경우 침입 이벤트를 비활성화합니다.

알 수 없는 명령 탐지

SMTP 트래픽에서 알 수 없는 명령을 탐지합니다.

규칙 124:5를 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

명령줄 최대 길이

SMTP 명령줄이 이 값보다 길 경우 이를 탐지합니다. 명령줄 길이를 탐지하지 않으려면 `0`을 지정합니다.

간단한 메일 전송 프로토콜의 네트워크 작업 그룹 사양인 RFC 2821은 명령줄 최대 길이로 512를 권장합니다.

규칙 124:1을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

헤더 행 최대 길이

SMTP 데이터 헤더 행이 이 값보다 길 경우 이를 탐지합니다. 데이터 헤더 행 길이를 탐지하지 않으려면 0을 지정합니다.

규칙 124:2 및 124:7을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

응답 회선 최대 길이

SMTP 응답 회선이 이 값보다 길 경우 이를 탐지합니다. 응답 회선 길이를 탐지하지 않으려면 0을 지정합니다.

RFC 2821는 응답 회선 최대 길이로 512를 권장합니다.

규칙 124:3을 활성화하여 이 옵션에 대해 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있고, 해당 옵션이 활성화되면 **Alt Max Command Line Len(**대안적 명령줄 최대 길이**)**에 대해서도 가능합니다.

대안적 명령줄 최대 길이

지정된 모든 명령에 대한 SMTP 명령줄이 이 값보다 길 경우 이를 탐지합니다. 지정된 명령에 대한 명령줄 길이를 탐지하지 않으려면 0을 지정합니다. 여러 명령에 대해 다양한 기본 회선 길이가 설정됩니다.

이 설정은 지정된 명령에 대한 Max Command Line Len(명령줄 최대 길이) 설정을 무시합니다.

규칙 124:3을 활성화하여 이 옵션에 대해 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있고, 해당 옵션이 활성화되면 **Max Response Line Len(**최대 응답 줄 길이**)**에 대해서도 가능합니다.

유효하지 않은 명령

이 명령어가 클라이언트 측에서 전송되는지 여부를 탐지합니다.

규칙 124:6을 활성화하여 이 옵션 및 **Invalid Commands(**유효하지 않은 명령**)**에 대해 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

유효한 명령

이 목록에 있는 명령을 허용합니다.

이 명령이 비어 있더라도 전처리기는 다음의 유효한 명령을 허용합니다. ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SIZE SOML STARTTLS TICK TIME TURN TURNME

VERB VRFY XADR XAUTH XCIR XEXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE XSTA XTRN XUSR

참고 RCPT TO 및 MAIL FROM은 SMTP 명령입니다. 전처리기 구성은 RCPT와 MAIL의 명령 이름을 각각 사용합니다. 해당 코드 안에서, 전처리기는 RCPT와 MAIL을 정확한 명령 이름에 매핑합니다.

규칙 124:4를 활성화하여 이 옵션에 대해 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있고, 해당 옵션이 구성되면 **Invalid Command(**유효하지 않은 명령**)**에 대해서도 가능합니다.

데이터 명령

SMTP DATA 명령이 RFC 5321당 데이터를 전송하는 것과 동일한 방식으로 데이터 전송을 시작하는 명령을 나열합니다. 공백을 사용하여 여러 명령을 구분하십시오.

이진 데이터 명령

BDAT 명령이 RFC 3030당 데이터를 전송하는 것과 유사한 방식으로 데이터 전송을 시작하는 명령을 나열합니다. 공백을 사용하여 여러 명령을 구분하십시오.

인증 명령

클라이언트와 서버 간의 인증 교환을 시작하는 명령을 나열합니다. 공백을 사용하여 여러 명령을 구분하십시오.

xlink2state 탐지

X−Link2State Microsoft Exchange 버퍼 데이터 오버플로 공격의 일부인 패킷을 탐지합니다. 인라인 배포에서, 시스템은 해당 패킷을 삭제할 수 있습니다.

규칙 124:8을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

Base64 디코딩 수준

Ignore Data(데이터 무시**)**가 비활성화된 경우, Base64로 인코딩된 각 MIME 이메일 첨부 파일에서 추출 및 디코딩할 최대 바이트 수를 지정합니다. 양수 값을 지정할 수도 있고 0을 지정하여 모든 Base64 데이터를 디코딩할 수도 있습니다. Base64 데이터를 무시하려면 -1을 지정합니다. **Ignore Data(**데이터 무시**)**를 선택한 경우 전처리기는 데이터를 디코딩하지 않습니다.

4로 나누어지지 않는 양수는 다음 4의 배수로 올림 처리된다는 점에 유의하십시오. 이때 65533, 65534, 및 65535 값은 제외되는데, 이들은 65532로 내림 처리됩니다.

이 옵션이 활성화된 경우, 규칙 124:10을 활성화하여 디코딩이 실패할 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 예를 들어, 잘못된 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다.

이 옵션은 **Enable MIME Decoding(MIME** 디코딩 활성화**)** 및 **Maximum MIME Decoding Depth(MIME** 디코딩 최대 수준**)**와 같이 더 이상 사용되지 않는 옵션을 대체한다는 점에 유의하십시오. 이 옵션은 이전 버전과의 호환성을 위해 기존 침입 정책에서 계속 지원됩니다.

7비트**/8**비트**/**이진 디코딩 수준

Ignore Data가 비활성화된 경우 디코딩이 필요하지 않은 각 MIME 이메일 첨부 파일에서 추출할 최대 데이터 바이트를 수를 지정합니다. 이 첨부 파일 형식에는 평문, jpeg 이미지, mp3 파일 등과 같이 7비트, 8비트, 이진 및 다양한 다중 부분 콘텐츠 형식 등이 있습니다. 양수 값을 지정할 수 있으며, 0을 지정하여 패킷의 모든 데이터를 추출할 수도 있습니다. 디코딩되지 않은 데이터를 무시하려면 -1을 지정합니다. **Ignore Data**가 선택된 경우 프리프로세서는 데이터를 추출하지 않습니다.

따옴표로 묶인 인쇄 가능한 디코딩 수준

Ignore Data(데이터 무시**)**가 비활성화된 경우, QP(Quoted−Printable)로 인코딩된 각 MIME 이메일 첨부 파일에서 추출 및 디코딩할 최대 바이트 수를 지정합니다.

1~65535바이트를 지정할 수 있으며, 0을 지정하여 패킷의 QP로 인코딩된 모든 데이터를 디코딩할 수도 있습니다. QP로 인코딩된 데이터를 무시하려면 -1을 지정합니다. **Ignore Data(**데이터 무시**)**를 선택한 경우 전처리기는 데이터를 디코딩하지 않습니다.

이 옵션이 활성화된 경우, 규칙 124:11을 활성화하여 디코딩이 실패할 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 예를 들어 잘못된 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다.

Unix−to−Unix 디코딩 수준

Ignore Data(데이터 무시**)**가 비활성화된 경우, Unix−to−Unix로 인코딩된(uuencoded) 각 MIME 이메일 첨부 파일에서 추출 및 디코딩할 최대 바이트 수를 지정합니다. 1~65535바이트를 지정할 수 있으며, 0을 지정하여 패킷의 모든 uuencoded 데이터를 디코딩할 수도 있습니다. uuencoded 데이터를 무시하려면 -1을 지정합니다. **Ignore Data(**데이터 무시**)**를 선택한 경우 전처리기는 데이터를 디코딩하지 않습니다.

이 옵션이 활성화된 경우, 규칙 124:13을 활성화하여 디코딩이 실패할 경우 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. 예를 들어 잘못된 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다.

MIME 첨부 파일 이름 로그

MIME Content−Disposition 헤더에서 MIME 첨부 파일 이름의 추출을 활성화하고 파일 이름을 세션에 대해 생성된 모든 침입 이벤트와 연결합니다. 여러 파일 이름이 지원됩니다.

이 옵션을 사용할 경우, 침입 이벤트 표 보기의 Email Attachment(이메일 첨부 파일) 열에서 이벤트와 관련된 파일 이름을 볼 수 있습니다.

수신지 주소 로그

SMTP RCPT TO 명령에서 수신자 전자 메일 주소의 추출을 활성화하고 수신자 주소를 세션에 대해 생성된 모든 침입 이벤트와 연결합니다. 여러 수신자가 지원됩니다.

이 옵션을 사용할 경우, 침입 이벤트 표 보기의 Email Recipient(전자 메일 수신자) 열에서 이벤트와 관련된 수신자를 볼 수 있습니다.

발신지 주소 로그

SMTP MAIL FROM 명령에서 발신자 전자 메일 주소의 추출을 활성화하고 발신자 주소를 세션에 대해 생성된 모든 침입 이벤트와 연결합니다. 여러 발신자 주소가 지원됩니다.

이 옵션을 사용할 경우, 침입 이벤트 표 보기의 Email Sender(이메일 발신자) 열에서 이벤트와 관련된 발신자를 볼 수 있습니다.

헤더 로그

전자 메일 헤더의 추출을 활성화합니다. 추출할 바이트 수는 **Header Log Depth(**헤더 로그 수준**)**에 지정된 값에 따라 결정됩니다.

이메일 헤더 데이터를 패턴으로 사용하는 침입 규칙을 작성하려면 `content` 또는 `protected_content` 키워드를 사용할 수 있습니다. 또한 침입 이벤트 패킷 보기에서 추출한 전자 메일 헤더를 볼 수 있습니다.

헤더 로그 수준

Log Headers(헤더 로그**)**가 활성화된 경우 추출할 전자 메일 헤더의 바이트 수를 지정합니다. 0~20480 바이트를 지정할 수 있습니다. 값을 0으로 지정하면 **Log Headers(**헤더 로그**)**가 비활성화됩니다.

관련 항목

기본 content 또는 protected_content 키워드 인수

SMTP 복호화 구성

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

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** 탐색창에서 **Settings(**설정**)**를 클릭합니다.

단계 **5** **Application Layer Preprocessors(**애플리케이션 계층 전처리기**)**의 **SMTP Configuration(SMTP** 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

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

단계 **7** SMTP 전처리기 옵션, 60 페이지에 설명된 대로 옵션을 수정합니다.

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 SMTP 전처리기 규칙(GID 124)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정를 참고하십시오.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

레이어 관리
충돌 및 변경: 네트워크 분석 및 침입 정책

SSH 전처리기

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

SSH 전처리기는 다음을 탐지합니다.

- 시도-응답 버퍼 오버플로 익스플로잇
- CRC-32 익스플로잇
- SecureCRT SSH 클라이언트 버퍼 오버플로 익스플로잇
- 프로토콜 불일치

- 잘못된 SSH 메시지 방향
- 버전 1 또는 2 이외의 다른 버전 문자열

시도-응답 버퍼 오버플로 및 CRC-32 공격은 키 교환 이후에 발생하며, 따라서 암호화됩니다. 두 공격 모두 인증 시도 직후 서버에 20KB가 넘는 터무니없이 큰 페이로드를 보냅니다. CRC-32 공격은 SSH 버전 1에만 적용되고, 시도-응답 버퍼 오버플로 익스플로잇은 SSH 버전 2에만 적용됩니다. 버전 문자열은 세션 시작 시 읽혀집니다. 버전 문자열의 차이를 제외하면, 두 공격 모두 동일하게 취급됩니다.

SecureCRT SSH 익스플로잇 및 프로토콜 불일치 공격은 키 교환 전에, 보안 연결을 하려고 할 때 발생합니다. SecureCRT 익스플로잇은 버퍼 오버플로를 야기하는 클라이언트에 과도하게 긴 프로토콜 식별자 문자열을 보냅니다. 프로토콜 불일치는 비SSH 클라이언트 애플리케이션이 보안 SSH 서버에 연결을 시도하거나 서버와 클라이언트 버전 번호가 일치하지 않는 경우 발생합니다.

전처리기가 지정된 포트 또는 포트 목록의 트래픽을 검사하거나 자동으로 SSH 트래픽을 탐지하도록 설정할 수 있습니다. 전처리기는 지정된 수의 암호화된 패킷이 지정된 수의 바이트 내부를 통과할 때까지 또는 지정된 최대 수의 바이트가 지정된 수의 패킷 내부에서 초과될 때까지 계속해서 SSH 트래픽을 검사합니다. 최대 수의 바이트가 초과된 경우, CRC-32(SSH 버전 1) 또는 시도-응답 버퍼 오버플로(SSH 버전 2) 공격이 발생한 것으로 가정합니다. 전처리기는 설정하지 않아도 버전 1 또는 2 이외의 다른 모든 버전의 문자열 값을 탐지한다는 점에 유의하십시오.

또한 SSH 전처리기는 무차별 암호 대입 공격을 처리하지 않는다는 점도 주의해야 합니다.

SSH 전처리기 옵션

전처리기는 다음 사항 중 하나가 발생할 경우 세션에 대한 트래픽 검사를 중지합니다.

- 서버와 클라이언트 간 유효한 교환이 이 암호화된 패킷의 수만큼 발생하며 연결은 지속됩니다.
- **Number of Bytes Sent Without Server Response(**서버 응답 없이 전송된 바이트 수**)**에 도달한 후에 검사할 암호화된 패킷 수에 도달하며 공격이 있는 것으로 간주됩니다.

Number of Encrypted Packets to Inspect(검사할 암호화된 패킷 수**)**가 경과되는 동안 유효한 각 서버 응답은 **Number of Bytes Sent Without Server Response(**서버 응답 없이 전송된 바이트 수**)**를 재설정하며 패킷 카운트가 계속됩니다.

다음의 예시 SSH 전처리기 구성을 고려하십시오.

- **Server Ports(**서버 포트**)**: 22
- **Autodetect Ports(**자동 탐지된 포트**)**: 꺼짐
- **Maximum Length of Protocol Version String(**프로토콜 버전 문자열의 최대 길이**)**: 80
- **Number of Encrypted Packets to Inspect(**검사할 암호화된 패킷 수**)**: 25
- **Number of Bytes Sent Without Server Response(**서버 응답 없이 전송된 바이트 수**)**: 19,600
- 모든 탐지 옵션이 활성화됩니다.

예제에서, 전처리기는 포트 22에서만 트래픽을 검사합니다. 즉 연결 자동 탐지가 비활성화되므로 지정된 포트에서만 검사합니다.

또한, 다음 사항 중 하나가 발생할 경우 예제의 전처리기는 트래픽 검사를 중지합니다.

- 클라이언트는 누적해서 19,600 미만의 바이트를 포함하는 25개의 암호화된 패킷을 전송합니다. 공격이 전혀 없는 것으로 가정합니다.
- 클라이언트는 25개의 암호화된 패킷으로 19,600 이상의 바이트를 전송합니다. 이 경우, 예제의 세션이 SSH 버전 2 세션이므로 전처리기는 해당 공격이 시도-응답 버퍼 오버플로 익스플로잇이라고 간주합니다.

예제에서 전처리기는 트래픽을 처리하는 동안 발생하는 다음과 같은 모든 징후를 탐지합니다.

- 80바이트보다 큰 버전 문자열에서 트리거되었고 SecureCRT 익스플로잇을 나타내는 서버 오버플로
- 프로토콜 불일치
- 잘못된 방향으로 흐르는 패킷

마지막으로, 전처리기는 버전 1 또는 버전 2 외에도 자동으로 모든 버전 문자열을 탐지합니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

서버 포트

SSH 전처리기가 트래픽을 검사할 포트를 지정합니다.

단일 포트 또는 쉼표로 구분된 포트 목록을 설정할 수 있습니다.

자동 탐지된 포트

전처리기는 자동으로 SSH 트래픽을 탐지할 수 있습니다.

이 옵션을 선택하면, 전처리기는 SSH 버전 번호에 대한 모든 트래픽을 검사합니다. 이는 클라이언트와 서버 패킷 모두가 버전 번호를 포함하지 않을 때 처리를 중지합니다. 이를 비활성화하면, 전처리기는 **Server Ports(**서버 포트**)** 옵션에서 확인된 트래픽만 검사합니다.

검사할 암호화된 패킷 수

세션당 검토할 스트림 리어셈블 암호화된 패킷 수를 지정합니다.

이 옵션을 0으로 설정하면 모든 트래픽이 통과할 수 있습니다.

검사할 암호화된 패킷 수를 줄이면 일부 공격이 탐지를 이스케이프할 수 있습니다. 검사할 암호화된 패킷 수를 늘리면 성능에 부정적인 영향을 줄 수 있습니다.

서버 응답 없이 전송된 바이트 수

시도-응답 버퍼 오버플로 공격 또는 CRC-32 공격이 있는 것으로 가정하기 전에 SSH 클라이언트가 응답을 받지 않고 서버에 보낼 수 있는 최대 바이트 수를 지정합니다.

전처리기가 시도-응답 버퍼 오버플로 또는 CRC-32 익스플로잇에서 오탐을 생성하는 경우 이 옵션의 값을 높이십시오.

프로토콜 버전 문자열의 최대 길이

문자열을 SecureCRT 익스플로잇으로 간주하기 전에 서버의 버전 문자열에 허용할 최대 바이트 수를 지정합니다.

시도-응답 버퍼 오버플로 공격 탐지

시도-응답 버퍼 오버플로 익스플로잇에 대한 탐지를 활성화 또는 비활성화합니다.

규칙 128:1을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다. SFTP 세션이 때때로 규칙 128:1을 트리거할 수 있습니다.

SSH1 CRC-32 공격 탐지

CRC-32 익스플로잇에 대한 탐지를 활성화 또는 비활성화합니다.

규칙 128:2를 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

서버 오버플로 탐지

SecureCRT SSH 클라이언트 버퍼 오버플로 익스플로잇에 대한 탐지를 활성화 또는 비활성화합니다.

규칙 128:3을 활성화하여 이 옵션에 대해 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

프로토콜 불일치 탐지

프로토콜 불일치에 대한 탐지를 활성화 또는 비활성화합니다.

규칙 128:4를 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

오류 메시지 방향 탐지

트래픽이 잘못된 방향으로 흐르는 경우(즉, 가정한 서버가 클라이언트 트래픽을 생성하거나, 클라이언트가 서버 트래픽을 생성한 경우) 탐지를 활성화 또는 비활성화합니다.

규칙 128:5를 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

지정된 페이로드에 대해 유효하지 않은 페이로드 크기 탐지

SSH 패킷에서 지정한 길이가 IP 헤더에 지정된 총 길이와 일관되지 않고 메시지 끝이 잘렸을 때, 즉, 전체 SSH 헤더에 충분한 데이터가 있지 않은 경우에 유효하지 않은 페이로드 크기를 가진 패킷 탐지를 활성화 또는 비활성화합니다.

규칙 128:6을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

유효하지 않은 버전 문자열 탐지

이를 활성화할 경우, 전처리기가 설정 없이도 버전 1 또는 2 이외의 다른 모든 버전의 문자열을 탐지한다는 점에 유의하십시오.

규칙 128:7을 활성화하여 이 옵션에 대한 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.할 수 있습니다.

SSH 전처리기 구성

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

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** **Application Layer Preprocessors(**애플리케이션 계층 전처리기**)**의 **SSH Configuration(SSH** 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

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

단계 **7** SSH 전처리기 옵션, 67 페이지에 설명된 대로 옵션을 수정합니다.

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

- 침입 이벤트를 활성화하려면 SSH 전처리기 규칙(GID 128)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정를 참고하십시오.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

레이어 관리
충돌 및 변경: 네트워크 분석 및 침입 정책

SSL 전처리기

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

SSL 전처리기는 SSL 검사의 설정을 허용합니다. 이를 통해 암호화된 트래픽을 차단 또는 해독하거나 액세스 컨트롤로 트래픽을 검사할 수 있습니다. SSL 검사의 설정 여부와 상관없이 SSL 전처리기는 트래픽에서 탐지된 SSL 핸드셰이크 메시지를 분석하고, 세션이 암호화되는 시기를 결정합니다. 암호화된 트래픽을 식별하면 시스템은 암호화된 페이로드의 침입 및 파일 검사를 중지하는데, 이는 오탐을 줄이고 성능을 향상하는 데 도움이 됩니다.

SSL 전처리기는 또한 암호화된 트래픽에서 Heartbleed 버그를 악용하려는 시도를 탐지하고, 그러한 익스플로잇을 탐지하는 경우 이벤트를 생성합니다.

세션이 암호화되면 트래픽의 침입 및 악성코드 검사를 일시 중단할 수 있습니다. 또한 SSL 검사를 구성하는 경우 SSL 전처리기는 액세스 컨트롤로 차단, 해독 또는 검사할 수 있는 암호화된 트래픽을 식별합니다.

SSL 전처리기를 이용한 암호화된 트래픽 해독은 라이선스가 필요하지 않습니다. 악성코드 및 침입에 대한 암호화된 페이로드의 검사 정지, Heartbleed 버그 익스플로잇 탐지 등 다른 모든 SSL 전처리기 기능에는 Protection(보호) 라이선스가 필요합니다.

SSL 전처리 작동 방식

SSL 검사를 구성한 경우, SSL 전처리기는 암호화된 데이터의 침입 및 파일 검사를 중지하고 SSL 정책으로 암호화된 트래픽을 검사합니다. 이는 오탐을 줄이는 데 도움이 됩니다. SSL 전처리기는 SSL 핸드쉐이크를 검사할 때 상태 정보를 유지하며, 해당 세션에 대한 상태 및 SSL 버전을 모두 추적합니다. 세션 상태가 암호화되었음을 전처리기가 탐지하면 시스템은 해당 세션의 트래픽이 암호화되었음을 표시합니다. 암호화가 설정된 경우 암호화된 세션의 모든 패킷에 대한 처리를 중지하도록, 그리고 Heartbleed 버그를 악용하려는 시도를 탐지할 경우 이벤트를 생성하도록 시스템을 구성할 수 있습니다.

SSL 전처리기는 각 패킷에 대해 트래픽이 IP 헤더, TCP 헤더 및 TCP 페이로드를 포함하며 SSL 전처리를 위해 지정된 포트에서 발생한다는 것을 확인합니다. 다음 시나리오는 트래픽 검증을 위해 트래픽이 암호화되었는지 여부를 확인합니다.

- 시스템은 세션 내 모든 패킷을 관찰하고, **Server side data is trusted(**서버 측 데이터가 신뢰됨**)** 기능은 활성화되지 않으며, 서버와 클라이언트 모두로부터 수신된 완료됨 메시지와 애플리케이션 레코드가 있지만 경고 레코드는 없는 각 측면으로부터 수신된 최소 하나의 패킷이 세션에 포함됩니다.
- 시스템은 트래픽 일부를 유실하고, **Server side data is trusted(**서버 측 데이터가 신뢰됨**)** 기능은 활성화되지 않으며, 경고 레코드로 응답되지 않은 애플리케이션 레코드를 가진 각 측면으로부터 수신된 최소 하나의 패킷이 세션에 포함됩니다.
- 시스템은 세션 내 모든 패킷을 관찰하고, **Server side data is trusted(**서버 측 데이터가 신뢰됨**)** 기능이 활성화되며, 클라이언트로부터 수신된 완료됨 메시지 및 애플리케이션 레코드가 있지만 경고 레코드는 없는 각 클라이언트로부터 수신된 최소 하나의 패킷이 세션에 포함됩니다.
- 시스템은 트래픽 일부를 유실하고, **Server side data is trusted(**서버 측 데이터가 신뢰됨**)** 기능이 활성화되며, 경고 레코드로 응답되지 않은 애플리케이션 레코드를 가진 각 클라이언트로부터 수신된 최소 하나의 패킷이 세션에 포함됩니다.

암호화된 트래픽 처리를 중단하도록 선택할 경우, 시스템은 세션이 암호화된 것으로 표시한 후에는 세션의 이후 패킷을 무시합니다.

또한, SSL 핸드쉐이크 중, 전처리기는 하트비트 요청과 응답을 모니터링합니다. 전처리기는 다음을 탐지하는 경우 이벤트를 생성합니다.

- 페이로드 자체보다 큰 페이로드 길이 값을 포함하는 하트비트 요청
- Max Heartbeat Length(하트비트 최대 길이) 필드에 저장된 값보다 큰 하트비트 응답

참고 `ssl_state` 및 `ssl_version` 키워드를 규칙에 추가하여 SSL 상태 또는 버전 정보를 규칙과 함께 사용할 수 있습니다.

관련 항목

SSL 키워드

SSL 전처리기 옵션

참고 시스템 제공 네트워크 분석 정책은 기본적으로 SSL 전처리기를 활성화합니다. Cisco는 암호화된 트래픽이 네트워크를 통과할 것으로 예상하는 경우 맞춤형 구축에서 SSL 전처리기를 비활성화하지 않을 것을 권장합니다.

SSL 검사를 구성하지 않으면 시스템은 암호화된 트래픽에서 해독 없이 악성코드와 침입을 검사하려고 시도합니다. SSL 전처리기를 활성화하면, 세션이 암호화되는 경우를 탐지합니다. SSL 전처리기를 활성화한 후, 규칙 엔진은 전처리기를 호출하여 SSL 상태 및 버전 정보를 얻을 수 있습니다. 침입 정책에서 `ssl_state` 및 `ssl_version` 키워드를 사용하여 규칙을 활성화하는 경우 SSL 프리프로세서도 활성화해야 합니다.

포트

SSL 전처리기가 암호화된 세션의 트래픽을 모니터링할 포트를 쉼표로 구분하여 지정합니다. 이 필드에 포함된 포트만 암호화된 트래픽을 검사합니다.

참고 SSL 전처리기가 SSL 모니터링을 위해 지정된 포트를 통해 비 SSL 트래픽을 탐지하는 경우, 해당 트래픽을 SSL 트래픽으로 디코딩하려고 시도한 다음 이를 손상된 것으로 표시합니다.

암호화된 트래픽 검사 중지

세션이 암호화된 것으로 표시되면 세션의 트래픽에 대한 검사를 활성화하거나 비활성화합니다.

암호화된 세션의 검사와 리어셈블리를 비활성화하려면 이 옵션을 활성화하십시오. SSL 전처리기가 이 세션에 대한 상태를 유지하므로 세션의 모든 트래픽의 검사를 비활성화할 수 있습니다. 이 옵션을 활성화하면 세션의 일부 패킷을 검증해 플로우가 심층 검사를 우회한 후 암호화되게 합니다. 모든 우회 세션은 **show snort statistics** 명령에 대한 응답에 표시되는, 빨리 감은 플로우 숫자를 높입니다. 또한 심층 검사를 우회하기 때문에 연결 이벤트에서의 이니시에이터와 반응기 바이트가 정확하지 않습니다. Snort가 검사한 패킷만 포함하며 심층 검사 우회 후의 패킷은 포함하지 않기 때문에, 실제 세션 값 미만이 됩니다. 이 동작은 연결 요약 이벤트와 위젯에 표시되는 모든 트래픽 값에 적용됩니다.

다음 두 조건 충족 시, 시스템은 암호화된 세션의 트래픽 검사를 중지합니다.

- SSL 전처리기가 활성화됨
- 이 옵션이 선택됨

이 옵션의 선택을 취소하면 **Server side data is trusted(**서버 측 데이터가 신뢰됨**)** 옵션을 수정할 수 없습니다.

서버 측 데이터가 신뢰됨

암호화된 트래픽 검사 중지가 활성화되면, 클라이언트측 트래픽에만 기반을 두는 암호화된 트래픽 식별이 활성화됩니다.

최대 하트비트 길이

바이트 수를 지정하면 Heartbleed 버그 악용 시도에 대한 SSL 핸드셰이크 내의 하트비트 요청 및 응답 검사를 활성화할 수 있습니다. `1~65535`까지의 정수를 지정할 수 있으며, `0`을 지정하여 옵션을 비활성화할 수도 있습니다.

전처리기가 실제 페이로드 길이보다 큰 페이로드 길이를 가진 하트비트 요청을 감지하고 규칙 137:3이 활성화되거나, 규칙 137:4가 활성화되었을 때 이 옵션에 설정된 값보다 하트비트 응답이 크다면 전처리기는 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.

SSL 전처리기 구성

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

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** **Application Layer Preprocessors(**애플리케이션 계층 전처리기**)**의 **SSL Configuration(SSL** 설정**)**이 비활성화되었다면 **Enabled**를 클릭합니다.

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

단계 **7** SSL 전처리기 옵션, 72 페이지에서 설명하는 설정을 수정합니다.

- **Ports(**포트**)** 필드에 값을 입력합니다. 쉼표로 여러 개의 값을 구분합니다.
- **Stop inspecting encrypted traffic(**암호화된 트래픽 검사 중지**)** 확인란을 선택하거나 선택 취소합니다.
- **Stop inspecting encrypted traffic(**암호화된 트래픽 검사 중지**)**를 선택했다면 **Server side data is trusted(**서버 측 데이터가 신뢰됨**)**을 선택하거나 선택 취소합니다.
- **Max Heartbeat Length(**최대 하트비트 길이**)** 필드에 값을 입력합니다.

  팁 0 값은 이 옵션을 비활성화합니다.

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

- 침입 이벤트를 활성화하려면 SSL 전처리기 규칙(GID 137)을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정를 참고하십시오.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

레이어 관리
충돌 및 변경: 네트워크 분석 및 침입 정책

SSL 전처리기 규칙

이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하고 싶다면 SSL 전처리기 규칙(GID 137)을 활성화합니다.

다음 표는 사용자가 활성화할 수 있는 SSL 전처리기 규칙에 대해 설명합니다.

표 ***16: SSL*** 전처리기 규칙

전처리기 규칙 **GID:SID**	설명
137:1	ServerHello 메시지 후에 나타나는 ClientHello 메시지를 탐지합니다. 해당 메시지는 유효하지 않으며 이상 작업으로 간주됩니다.
137:2	SSL 전처리기 옵션인 **Server side data is trusted(**서버 측 데이터가 신뢰됨**)** 기능이 비활성화되면 ClientHelloo 없는 ServerHello 메시지를 탐지합니다. 해당 메시지는 유효하지 않으며 이상 작업으로 간주됩니다.
137:3	SSL 전처리기 옵션인 **Max Heartbeat Length(**최대 하트비트 길이**)**에 0이 아닌 값이 포함된 경우 페이로드 길이가 페이로드 자체보다 큰 하트비트 요청을 탐지합니다. 이는 Heartbleed 버그를 악용하려는 시도를 나타냅니다.
137:4	SSL 전처리기 옵션인 **Max Heartbeat Length(**하트비트 최대 길이**)**에 지정된 0이 아닌 값보다 큰 하트비트 응답을 탐지합니다. 이는 Heartbleed 버그를 악용하려는 시도를 나타냅니다.