침입 이벤트

다음 주제에서는 침입 이벤트 작업 방법을 설명합니다.

침입 이벤트 정보

Firepower System을 사용하면 네트워크에서 호스트와 호스트 데이터의 가용성, 무결성 및 신뢰성에 영향을 줄 수 있는 트래픽을 모니터링할 수 있습니다. 주요 네트워크 세그먼트에 매니지드 디바이스를 배치하면 악의적인 활동을 위해 네트워크에서 이동하는 패킷을 검토할 수 있습니다. 시스템에는 공격자들이 개발한 광범위한 익스플로잇을 찾는 데 사용하는 몇 가지 메커니즘에 있습니다.

시스템은 침입 가능성을 식별하는 경우 익스플로잇의 날짜, 시간, 익스플로잇 유형, 그리고 공격 소스와 대상에 관한 상황 정보의 레코드인 침입 이벤트(이전 용어인 'IPS 이벤트'라고 부르기도 함)를 생성합니다. 패킷 기반 이벤트의 경우 이벤트를 트리거한 패킷의 사본도 기록됩니다. 매니지드 디바이스는 Secure Firewall Management Center에 자체 이벤트를 전송합니다. 여기서는 집계된 데이터를 보고 네트워크 자산에 대한 공격을 더 잘 이해할 수 있습니다.

또한 매니지드 디바이스를 인라인, 스위치드 또는 라우티드 침입 시스템으로 구축할 수 있으며, 이를 통해 해로운 것으로 알려진 패킷을 삭제 또는 교체하도록 디바이스를 구성할 수도 있습니다.

침입 이벤트 검토 및 평가용 도구

다음 도구를 사용하여 침입 이벤트를 검토하고 네트워크 환경 및 보안 정책의 컨텍스트에서 중요성을 평가하는 데 필요한 도구를 제공합니다.

- 매니지드 디바이스에서 현재 활동을 검토할 수 있는 이벤트 요약 페이지
- 선택한 기간에 대해 생성할 수 있는 텍스트 기반 보고서와 그래프 보고서. 사용자는 자신만의 보고서를 계획하고 정해진 간격으로 실행되도록 구성할 수 있습니다.
- 공격과 관련된 이벤트 데이터를 수집하기 위해 사용할 수 있는 인시던트 처리 툴. 조사와 응답을 추적하는 데 도움이 되도록 메모를 추가할 수도 있습니다.
- SNMP, 이메일 및 시스템 로그를 위해 구성할 수 있는 자동화된 알림
- 특정 침입 이벤트에 대한 응답과 교정에 사용할 수 있는 자동화된 상관관계 정책
- 더 자세히 조사할 이벤트를 식별하기 위해 데이터에서 드릴다운할 수 있는 사전 정의 및 사용자 지정 워크플로
- 데이터 관리 및 분석을 위한 외부 툴. 시스템 로그 또는 eStreamer를 사용할 수 있습니다. 자세한 내용은 다음을 참조하십시오. 외부 툴을 사용하여 이벤트 분석

또한 **Analysis(분석) > Advanced(고급) > Contextual Cross-Launch(상황별 크로스 실행)** 페이지에서 사전 정의된 리소스 등 공개적으로 이용 가능한 정보를 사용하여 악의적인 엔터티에 대해 자세히 알아볼 수 있습니다.

특정 메시지 문자열을 검색하고 이벤트를 생성한 규칙에 대한 설명서를 검색하려면 https://www.snort.org/rule_docs/을 참조하십시오.

침입 이벤트 라이선스 요구 사항

Threat Defense 라이선스

IPS

기본 라이선스

보호

침입 이벤트 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모두

사용자 역할

- 관리자
- 침입 관리자

침입 이벤트 보기

침입 이벤트를 보고 네트워크 보안에 위협이 있는지 판단할 수 있습니다.

초기 침입 이벤트 보기는 페이지에 액세스하는 데 사용하는 워크플로에 따라 다릅니다. 하나 이상의 드릴다운 페이지, 침입 이벤트의 테이블 보기, 종료 패킷 보기 등 사전 정의 워크플로 중 하나를 사용할 수도 있고 자체 워크플로를 생성할 수도 있습니다. 침입 이벤트가 포함되어 있을 수 있는 맞춤형 테이블을 기반으로 하는 워크플로를 볼 수도 있습니다.

포함된 IP 주소가 많고 **Resolve IP Addresses(IP** 주소 확인**)** 이벤트 보기 설정을 활성화한 경우, 이벤트 보기가 표시되는 속도가 느려질 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Intrusions(**침입**)** > **Events(**이벤트**)**을(를) 선택합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- 시간 범위 조정 - 타임 윈도우 변경의 설명에 따라 이벤트 보기의 시간 범위를 조정합니다.
- 워크플로 변경 - 침입 이벤트 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용하는 경우, 워크플로 제목 옆에 있는 **(**워크플로 전환**)**를 클릭하여 시스템 제공 워크플로 중에서 선택합니다.
- 제한 - 분석에 중요한 침입 이벤트로 보기 범위를 좁히려면 침입 이벤트 워크플로 사용, 23 페이지를 참조하십시오.
- 이벤트 삭제 - 데이터베이스에서 이벤트를 삭제하려면 **Delete(**삭제**)**를 클릭하여 패킷을 보고 있는 이벤트를 삭제하거나 **Delete All(**모두 삭제**)**을 클릭하여 이전에 패킷을 선택한 모든 이벤트를 삭제합니다.
- 검토 표시 - 검토한 침입 이벤트에 표시하려면 검토된 침입 이벤트 표시, 18 페이지를 참조하십시오.
- 연결 데이터 보기 - 침입 이벤트에 연결된 연결 데이터를 보려면 침입 이벤트 관련 연결 데이터 보기, 18 페이지를 참조하십시오.
- 콘텐츠 보기 - 테이블에서 열의 콘텐츠를 보려면 침입 이벤트 필드, 4 페이지의 설명에 따릅니다.

관련 항목

침입 이벤트 패킷 보기 사용, 27 페이지

침입 이벤트 필드 정보

시스템은 침입 가능성을 식별하는 경우 익스플로잇의 날짜, 시간, 익스플로잇 유형, 그리고 공격 소스와 대상에 관한 상황 정보의 레코드인 침입 이벤트를 생성합니다. 패킷 기반 이벤트의 경우 이벤트를 트리거한 패킷의 사본도 기록됩니다.

Secure Firewall Management Center 웹 인터페이스 **Analysis(**분석**) > Intrusions(**침입**) > Events(**이벤트**)**에서 침입 이벤트 데이터를 보거나 외부 도구에서 사용할 수 있도록 일부 필드에서 데이터를 syslog 메시지로 내보낼 수 있습니다. Syslog 필드는 아래 목록에 표시됩니다. 나열된 동등한 syslog가 없는 필드는 syslog 메시지에서 사용할 수 없습니다.

침입 이벤트를 검색할 때 개별 이벤트에 사용 가능한 정보는 시스템에서 연결을 로깅한 방법, 이유 및 시기에 따라 달라질 수 있습니다. 예를 들면 해독된 트래픽에 대해 트리거된 침입 이벤트에만 TLS/SSL 정보가 포함됩니다.

참고 Secure Firewall Management Center 웹 인터페이스에서 침입 이벤트 테이블 보기의 일부 필드는 기본적으로 비활성화되어 있습니다. 세션 기간 동안 필드를 활성화하려면 검색 제약 조건을 확장한 다음 **Disabled Columns(**비활성화된 열**)** 아래에서 열 이름을 클릭합니다.

침입 이벤트 필드

액세스 제어 정책**(**시스템 로그**: ACPolicy)**

이벤트를 생성한 침입, 프리프로세서 또는 디코더 규칙이 활성화된 침입 정책과 관련된 액세스 제어 정책.

액세스 제어 규칙**(**시스템 로그**: AccessControlRuleName)**

이벤트를 생성한 침입 정책을 호출한 액세스 제어 규칙. `Default Action(기본 작업)`은 규칙이 활성화된 침입 정책이 특정 액세스 제어 규칙과 연결되지 않았지만, 대신 액세스 제어 정책의 기본 작업으로 구성되었음을 나타냅니다.

다음의 경우 (또는 시스템 로그 메시지의 경우 생략됨) 이 필드는 비어 있습니다.

- 관련 규칙/기본 작업 없음: 침입 검사가 액세스 제어 규칙 및 기본 작업과 모두 연결되지 않은 경우(예: 시스템이 어떤 규칙을 적용할지를 결정하기 전에 반드시 통과해야 하는 것으로서 패킷 처리를 위해 지정된 침입 정책에 의해 검토된 경우) (이 정책은 액세스 제어 정책의 Advanced (고급) 탭에서 지정됩니다.)
- 관련 연결 이벤트 없음: 세션에 로깅된 연결 이벤트가 데이터베이스에서 삭제된 경우(예: 연결 이벤트가 침입 이벤트보다 턴오버가 높은 경우)

애플리케이션 프로토콜(시스템 로그: **ApplicationProtocol**)

침입 이벤트를 트리거한 트래픽에서 탐지된 호스트 간 통신을 나타내는 애플리케이션 프로토콜(사용 가능한 경우).

애플리케이션 프로토콜 카테고리 및 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준

애플리케이션 위험성

침입 이벤트를 트리거한 트래픽에서 탐지된 애플리케이션과 관련된 위험성: Very High(매우 높음), High(높음), Medium(중간), Low(낮음) 또는 Very Low(매우 낮음). 연결에서 탐지된 애플리케이션의 각 유형에는 관련된 위험이 있습니다. 이 필드에는 그 중 가장 높은 위험이 표시됩니다.

사업 타당성

침입 이벤트를 트리거한 트래픽에서 탐지된 애플리케이션과 관련된 비즈니스 연관성: Very High(매우 높음), High(높음), Medium(중간), Low(낮음) 또는 Very Low(매우 낮음). 연결에서 탐지된 각 애플리케이션 유형에는 관련된 비즈니스 연관성이 있습니다. 이 필드에는 그 중 가장 낮은(가장 연관성이 적은) 값이 표시됩니다.

분류(시스템 로그: **Classification**)

이벤트를 생성한 규칙이 속하는 분류

침입 이벤트 세부 정보에서 가능한 분류 값 목록을 참조하십시오.

이 필드를 검색하는 경우, 확인하려는 이벤트를 생성한 규칙의 분류 번호 또는 분류 이름이나 설명의 전체 또는 일부를 입력합니다. 쉼표로 구분된 숫자, 이름 또는 설명의 목록을 입력할 수도 있습니다. 마지막으로, 사용자 지정 분류를 추가하는 경우 이름이나 설명의 전체 또는 일부를 사용하여 검색할 수도 있습니다.

클라이언트(시스템 로그: **Client**)

침입 이벤트를 트리거한 트래픽에서 탐지된 모니터링되는 호스트에서 실행 중인 소프트웨어를 나타내는 클라이언트 애플리케이션(사용 가능한 경우).

클라이언트 카테고리 및 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준

Connection Counter (시스템 로그만 해당)

다른 동시 연결에서 하나의 연결을 구분하는 카운터입니다. 이 필드 자체에는 중요한 의미가 없습니다.

다음 필드 전부는 특정 침입 이벤트와 관련된 연결 이벤트(디바이스 UUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 개별적으로 식별합니다.

Connection Instance ID (시스템 로그만 해당)

연결 이벤트를 처리한 Snort 인스턴스입니다. 이 필드 자체에는 중요한 의미가 없습니다.

다음 필드 전부는 특정 침입 이벤트와 관련된 연결 이벤트(디바이스 UUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 개별적으로 식별합니다.

개수

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다. 이 필드는 검색할 수 없습니다.

CVE ID

이 필드는 검색 전용입니다.

MITRE CVE(Common Vulnerabilities and Exposures) 데이터베이스(https://cve.mitre.org/)에서 취약성과 관련된 식별 번호에 의한 검색.

Destination Continent(대상 대륙)

침입 이벤트와 관련된 수신 호스트의 대륙.

Destination Country(대상 국가)

침입 이벤트와 관련된 수신 호스트의 국가.

Destination Host Criticality(대상 호스트 심각도)

이벤트가 생성될 때의 대상 호스트 심각도(해당 호스트에 대한 호스트 심각도 속성 값).

호스트의 심각도가 변경되어도 이 필드는 업데이트되지 않습니다. 그러나 새 이벤트에는 새로운 심각도 값이 적용됩니다.

대상 **IP**(시스템 로그: **DstIP**)

침입 이벤트와 관련된 수신 호스트가 사용하는 IP 주소.

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침도 참조하십시오.

대상 포트/**ICMP** 코드(시스템 로그: **DstPort, ICMPCode**)

트래픽을 수신하는 호스트의 포트 번호입니다. ICMP 트래픽에서 포트 번호가 없는 경우 이 필드에 ICMP 코드가 표시됩니다.

대상 사용자

연결 이벤트의 응답자 IP와 연결된 사용자 이름입니다. 이 호스트는 익스플로잇을 수신하는 호스트일 수도 있고 아닐 수도 있습니다. 이 값은 일반적으로 네트워크의 사용자에게만 알려져 있습니다.

선택합니다.

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침도 참조하십시오.

디바이스

액세스 제어 정책이 구축된 매니지드 디바이스입니다.

DeviceUUID (시스템 로그만 해당**)**

이벤트를 생성한 Firepower 디바이스의 고유 식별자입니다.

다음 필드 전부는 특정 침입 이벤트와 관련된 연결 이벤트(디바이스 UUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 개별적으로 식별합니다.

도메인

침입을 탐지한 디바이스의 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

이그레스 인터페이스**(**시스템 로그**: EgressInterface)**

이벤트를 트리거한 패킷의 이그레스 인터페이스. 패시브 인터페이스에 대해서는 이 인터페이스 열이 채워지지 않습니다.

이그레스 보안 영역**(**시스템 로그**: EgressZone)**

이벤트를 트리거한 패킷의 이그레스 보안 영역입니다. 패시브 구축에서는 이 보안 영역 필드가 채워지지 않습니다.

이그레스 가상 라우터

가상 라우팅을 사용하는 네트워크에서 트래픽이 네트워크에서 벗어날 때 사용하는 가상 라우터의 이름입니다.

이메일 첨부 파일

MIME Content-Disposition 헤더에서 추출된 MIME 첨부 파일 이름. 첨부 파일 이름을 표시하려면 SMTP 프리프로세서 **Log MIME Attachment Names** 옵션을 활성화해야 합니다. 여러 첨부 파일 이름이 지원됩니다.

Email Headers(이메일 헤더**)**

이 필드는 검색 전용입니다.

이메일 헤더에서 추출된 데이터입니다.

이메일 헤더를 SMTP 트래픽의 침입 이벤트와 연결하려면 SMTP 프리프로세서 **Log Headers(**헤더 로깅**)** 옵션을 활성화해야 합니다.

Email Recipient(이메일 수신자**)**

SMTP RCPT TO 명령에서 추출된 이메일 수신자의 주소. 이 필드의 값을 표시하려면 SMTP 프리프로세서 **Log To Addresses(**주소로 로깅**)** 옵션을 활성화해야 합니다. 여러 수신자 주소가 지원됩니다.

Email Sender(이메일 발신자**)**

SMTP MAIL FROM 명령에서 추출된 이메일 발신자의 주소. 이 필드의 값을 표시하려면 SMTP 프리프로세서 **Log From Addresses(**주소에서 로깅**)** 옵션을 활성화해야 합니다. 여러 발신자 주소가 지원됩니다.

첫 번째 패킷 시간 **(**시스템 로그만 해당**)**

시스템이 첫 번째 패킷을 수신한 시간입니다.

다음 필드 전부는 특정 침입 이벤트와 관련된 연결 이벤트(디바이스 UUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 개별적으로 식별합니다.

Generator(생성기**)**

이벤트를 생성한 구성 요소.

다음에 나오는 침입 이벤트 필드인 GID, Message(메시지) 및 Snort ID에 대한 정보도 참조하십시오.

GID(시스템 로그만 있음**)**

Generator ID(생성기 ID)로, 이벤트를 생성한 구성 요소의 ID.

다음에 나오는 침입 이벤트 필드인 Generator(생성기), Message(메시지) 및 Snort ID에 대한 정보도 참조하십시오.

HTTP Hostname(HTTP 호스트네임**)**

HTTP 요청 Host 헤더에서 추출된 호스트 이름(해당되는 경우). 요청 패킷에 항상 호스트 이름이 포함되는 것은 아닙니다.

호스트 이름을 HTTP 클라이언트 트래픽에 대한 침입 이벤트와 연결하려면 HTTP Inspect 프리프로세서 **Log Hostname(**호스트네임 로깅**)** 옵션을 활성화해야 합니다.

테이블 보기에서 이 열에는 추출된 호스트 이름의 첫 50자가 표시됩니다. 약식 호스트 이름의 표시된 부분 위로 마우스 포인터를 이동하여 최대 256바이트까지 전체 이름을 표시할 수 있습니다. 패킷 보기에서 전체 호스트 이름을 최대 256바이트까지 표시할 수 있습니다.

HTTP 응답 코드**(**시스템 로그**: HTTPResponse)**

이벤트를 트리거한 연결을 통해 클라이언트의 HTTP 요청에 대한 응답으로 전송된 HTTP 상태 코드.

HTTP URI

침입 이벤트를 트리거한 HTTP 요청 패킷과 연결된 원시 URI(있는 경우). 요청 패킷에 항상 URI가 포함되는 것은 아닙니다.

URI를 HTTP 트래픽에 대한 침입 이벤트와 연결하려면 HTTP Inspect 프리프로세서 **Log URI(URI** 로깅**)** 옵션을 활성화해야 합니다.

HTTP 응답에 의해 트리거된 침입 이벤트에서 연결된 HTTP URI를 보려면 **Perform Stream Reassembly on Both Ports(**양쪽 포트에서 스트림 리어셈블리 수행**)** 옵션에서 HTTP 서버를 구성해야 합니다. 그러나 이렇게 하면 트래픽 리어셈블리를 위한 리소스 수요가 증가합니다.

이 열에는 추출된 URI의 첫 50자가 표시됩니다. 약식 URI의 표시된 부분 위로 마우스 포인터를 이동하여 최대 2048바이트까지 전체 URI를 표시할 수 있습니다. 패킷 보기에서 전체 URI를 최대 2048바이트까지 표시할 수 있습니다.

영향

이 필드의 영향 레벨은 침입 데이터, 네트워크 검색 데이터 및 취약성 정보 사이의 상관 관계를 나타냅니다.

이 필드를 검색하는 경우 영향 아이콘이 색상 또는 부분 문자열을 지정하지 않습니다. 예를 들어, 파란색, 레벨 **1**또는 **0**을 사용하지 마십시오. 대/소문자 유효한 값은 다음과 같습니다.

- 영향 0, 영향 레벨 0
- 영향 1, 영향 레벨 1
- 영향 2, 영향 레벨 2
- 영향 3, 영향 레벨 3
- 영향 4, 영향 레벨 4

NetFlow 데이터에서 네트워크 맵에 추가되는 호스트에 대해서는 운영 체제 정보가 제공되지 않으므로 시스템은 이러한 호스트와 관련된 침입 이벤트에 대해 취약함(영향 레벨 1: 빨강) 영향 레벨을 할당할 수 없습니다. 이러한 경우에는 호스트 입력 기능을 사용하여 호스트에 대한 운영 체제 ID를 수동으로 설정합니다.

인그레스 인터페이스**(**시스템 로그**: IngressInterface)**

이벤트를 트리거한 패킷의 인그레스 인터페이스입니다. 패시브 인터페이스에 대해서는 이 인터페이스 열만 채워집니다.

인그레스 보안 영역**(**시스템 로그**: IngressZone)**

이벤트를 트리거한 패킷의 인그레스 보안 영역 또는 터널 영역. 수동 배포에서는 이 보안 영역 필드만 입력됩니다.

인그레스 가상 라우터

가상 라우팅을 사용하는 네트워크에서 트래픽이 네트워크에 진입할 때 사용하는 가상 라우터의 이름입니다.

인라인 결과**(**시스템 로그**: InlineResult)**

워크플로 및 테이블 보기에서 이 필드는 다음 중 하나를 표시합니다.

표 ***1:*** 워크플로 및 테이블 보기에서 인라인 결과 필드 내용

아이콘	표시 내용
	시스템이 규칙을 트리거한 패킷을 삭제했음을 나타냅니다.

아이콘	표시 내용
	(인라인 구축에서) **Drop when Inline(**인라인 시 삭제**)** 침입 정책 옵션을 활성화하는 경우 또는 시스템 정리 중 Drop and Generate(삭제 및 생성) 규칙이 이벤트를 생성한 경우 IPS가 패킷을 삭제했음을 나타냅니다.
	IPS가 패킷을 대상에 전송했거나 전달했을 수 있지만 이 패킷을 포함했던 연결은 이제 차단됩니다.
아이콘 없음(공란)	트리거된 규칙이 Drop and Generate Events(이벤트 삭제 및 생성)로 설정되지 않았음을 나타냅니다.

다음 테이블에는 인라인 결과의 가능한 이유(Would have dropped(삭제됨) 및 Partially dropped(부분적으로 삭제됨))가 나열되어 있습니다.

인라인 결과	원인	상세 이유
Would Have Dropped(삭제됨)	패시브 또는 탭 모드의 인터페이스	인터페이스를 인라인 탭 또는 패시브 모드로 구성했습니다.
	"Detection(탐지)" 검사 모드의 침입 정책	침입 정책에서 검사 모드를 Detection(탐지)로 설정했습니다.
	Connection Timed Out(연결 시간 초과)	TCP/IP 연결이 시간 초과되어 Snort 검사 엔진이 검사를 일시 중단했습니다.
Partially Dropped(부분적으로 삭제됨)	연결 닫힘(0x01)	새 플로우를 생성하는 동안 할당된 플로우가 허용되는 플로우 수보다 많은 경우 Snort 검사 엔진이 가장 최근에 사용된 플로우를 정리합니다.
	연결 닫힘(0x02)	Snort 검사 엔진을 다시 로드하면 메모리 조정이 발생하며 가장 최근에 사용된 플로우가 제거됩니다.
	연결 닫힘(0x04)	Snort 검사 엔진이 정상적으로 종료되면 엔진은 모든 활성 플로우를 제거합니다.

수동 구축에서 인라인 인터페이스가 탭 모드에 있는 경우를 포함하여 침입 정책의 규칙 상태 또는 인라인 삭제 작업에 상관없이 시스템은 패킷을 삭제하지 않습니다.

이 필드를 검색하는 경우 다음 중 하나를 입력합니다.

- **dropped** - 패킷이 인라인 구축에서 삭제되는지 여부를 지정합니다.

- **would have dropped** - 인라인 구축에서 패킷을 삭제하도록 침입 정책을 설정했다면 패킷이 삭제되었을 것인지를 지정합니다.
- **partially dropped** - 패킷을 대상으로 전송하거나 전달할지 지정하지만, 이 패킷이 들어 있는 연결은 이제 차단됩니다.

침입 정책 **(**시스템 로그**: IntrusionPolicy)**

이벤트를 생성한 침입, 프리프로세서 또는 디코더 규칙이 활성화된 침입 정책. 액세스 제어 정책에 대한 기본 작업으로 침입 정책을 선택할 수 있습니다. 또는 침입 정책을 액세스 제어 규칙과 연결할 수 있습니다.

IOC(시스템 로그**: NumIOC)**

침입 이벤트를 트리거한 트래픽이 연결과 관련된 호스트에 대해 IOC(indication of compromise)도 트리거했는지 여부.

이 필드를 검색하는 경우 **triggered(**트리거됨**)** 또는 **n/a(**해당 없음**)**를 지정합니다.

메시지**(**시스템 로그**: Message)**

이벤트에 대한 설명 텍스트 규칙 기반 침입 이벤트의 경우, 이벤트 메시지는 규칙에서 가져옵니다. 디코더 및 프리프로세서 기반 이벤트의 경우, 이벤트 메시지는 하드 코드됩니다.

Generator ID(GID), Snort ID(SID) 및 SID 버전(Revision)이 각 메시지 끝에 콜론으로 구분되는 숫자 형식으로 괄호안에 추가됩니다(GID:SID:version). 예: **(1:36330:2)**.

MITRE

클릭하여 해당 계층 내에서 MITRE 전략 및 기술의 전체 목록을 나타내는 모달을 표시할 수 있는 기술의 수입니다.

MPLS 레이블**(**시스템 로그**: MPLS_Label)**

이 침입 이벤트를 트리거한 패킷에 연결된 Multiprotocol Label Switching(다중 프로토콜 레이블 스위칭) 레이블.

네트워크 분석 정책**(**시스템 로그**: NAPPolicy)**

이벤드 생성과 관련된 네트워크 분석(해당되는 경우).

이 필드에는 추출된 URI의 첫 50자가 표시됩니다. 약식 URI의 표시된 부분 위로 마우스 포인터를 이동하여 최대 2048바이트까지 전체 URI를 표시할 수 있습니다. 패킷 보기에서 전체 URI를 최대 2048바이트까지 표시할 수 있습니다.

원본 클라이언트 **IP**

XFF(X-Forwarded-For), True-Client-IP 또는 맞춤 정의된 HTTP 헤더에서 추출된 원래 클라이언트 IP 주소.

이 필드의 값을 표시하려면 네트워크 분석 정책에서 HTTP 프리프로세서 **Extract Original Client IP Address(**원래 클라이언트 **IP** 주소 추출**)** 옵션을 활성화해야 합니다. 또한 네트워크 분석 정책에서 최대 6개의 맞춤형 클라이언트 IP 헤더를 지정할 수 있으며 시스템이 Original Client IP 이벤트 필드에 대한 값을 선택하는 우선순위 순서를 설정할 수 있습니다.

우선순위**(**시스템 로그**: Priority)**

Talos 인텔리전스 그룹에 따라 결정된 이벤트 우선순위. 우선순위는 `priority` 키워드의 값 또는 `classtype`키워드의 값에 해당합니다. 기타 침입 이벤트의 경우, 우선순위는 디코더 또는 프리프로세서에 의해 결정됩니다. 유효한 값은 high(높음), medium(중간) 및 low(낮음)입니다.

프로토콜**(**시스템 로그**: Protocol)**

Secure Firewall Management Center 웹 인터페이스에서 이 필드는 검색 필드로만 사용됩니다.

http://www.iana.org/assignments/protocol-numbers에 열거된 대로 연결에 사용된 전송 프로토콜의 이름 또는 번호. 이것은 소스 및 대상 포트/ICMP 열과 관련된 프로토콜입니다.

검토자

이벤트를 검토한 사용자의 이름. 이 필드를 검색하는 경우, **`unreviewed(`**검토 안 함**`)`**를 입력하고 검토되지 않은 이벤트를 검색할 수 있습니다.

Revision(시스템 로그만 있음**)**

이벤트 생성에 사용된 서명의 버전.

다음에 나오는 침입 이벤트 필드인 Generator(생성기), GID, Message(메시지), SID 및 Snort ID에 대한 정보도 참조하십시오.

규칙 그룹

규칙 그룹의 전체 목록을 나타내는 모달을 표시하기 위해 클릭할 수 있는 비 MITRE 규칙 그룹의 수입니다.

보안 상황**(**시스템 로그**: Context)**

트래픽이 통과한 가상 방화벽 그룹을 식별하는 메타데이터입니다. 시스템은 다중 상황 모드의 ASA FirePOWER에 대해서만 이 필드에 내용을 입력합니다.

SID(시스템 로그만 있음**)**

이벤트를 생성하는 규칙의 서명 ID(Snort ID로도 알려짐).

다음에 나오는 침입 이벤트 필드인 Generator(생성기), GID, Message(메시지), Revision(개정) 및 Snort ID에 대한 정보도 참조하십시오.

Snort ID

이 필드는 검색 전용입니다.

(시스템 로그 필드에서 SID 참조).

검색을 수행하는 경우 이벤트를 생성한 규칙의 Snort ID(SID)를 지정합니다. 또는 선택적으로 규칙의 GID(Generator ID)와 SID 조합을 지정합니다. 여기서 GID와 SID는 GID:SID 형식으로 콜론(:)으로 구분됩니다. 다음 표에서 어떠한 값도 지정할 수 있습니다.

표 ***2: Snort ID*** 검색 값

값	예
단일 SID	10000
SID 범위	10000-11000
SID보다 큼	>10000
SID보다 크거나 같음	>=10000
SID보다 작음	<10000
SID보다 작거나 같음	<=10000
쉼표로 구분된 SID 목록	10000,11000,12000
단일 GID:SID 조합	1:10000
쉼표로 구분된 GID:SID 조합의 목록	1:10000,1:11000,1:12000
쉼표로 구분된 SID 및 GID:SID 조합의 목록	10000,1:11000,12000

보고 있는 이벤트의 SID가 Message(메시지) 열에 나열됩니다. 자세한 내용은 Message(메시지) 필드에 대한 이 섹션의 설명을 참조하십시오.

소스 대륙

침입 이벤트와 관련된 전송 호스트의 대륙.

소스 국가

침입 이벤트와 관련된 전송 호스트의 국가.

Source Criticality(소스 심각도**)**

이벤트가 생성될 때의 소스 호스트 심각도(해당 호스트에 대한 호스트 심각도 속성 값).

호스트의 심각도가 변경되어도 이 필드는 업데이트되지 않습니다. 그러나 새 이벤트에는 새로운 심각도 값이 적용됩니다.

소스 **IP(**시스템 로그**: SrcIP)**

침입 이벤트와 관련된 전송 호스트가 사용하는 IP 주소.

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침도 참조하십시오.

소스 포트/**ICMP** 유형(시스템 로그: **SrcPort, ICMPType**)

전송 호스트의 포트 번호. ICMP 트래픽에서 포트 번호가 없는 경우 이 필드에 ICMP 유형이 표시됩니다.

소스 사용자(시스템 로그: **User**)

연결을 시작한 호스트의 IP 주소와 연결된 사용자 이름으로, 익스플로잇의 소스 호스트일 수도 있고 아닐 수도 있습니다. 이 사용자 값은 일반적으로 네트워크의 사용자에게만 알려져 있습니다.

해당하는 경우 사용자 이름 앞에 `<realm>\`을 입력합니다.

SSL 실제 작업(시스템 로그: **SSLActualAction**)

Secure Firewall Management Center 웹 인터페이스에서 이 필드는 검색 필드로만 사용됩니다.

시스템이 암호화된 트래픽에 적용하는 작업.

차단/차단 및 재설정

차단된 암호화된 연결을 나타냅니다.

암호 해독(재서명)

다시 서명된 서버 인증서를 사용하여 암호 해독된 발신 연결을 나타냅니다.

암호 해독(대체 키)

대체된 공개 키가 있는 자체 서명된 서버 인증서를 사용하여 암호 해독된 발신 연결을 나타냅니다.

암호 해독(알려진 키)

알려진 개인 키를 사용하여 암호 해독된 수신 연결을 나타냅니다.

기본 작업

연결이 기본 작업에 의해 처리되었음을 나타냅니다.

암호 해독 안 함

시스템이 암호 해독하지 않은 연결을 나타냅니다.

검색 워크플로 페이지의 **SSL Status**(**SSL** 상태) 필드에 필드값이 표시됩니다.

SSL 인증서 정보

이 필드는 검색 전용입니다.

트래픽 암호화에 사용하는 공개 키 인증서에 저장된 정보로 다음을 포함합니다.

- Subject/Issuer Common Name(대상자/발급자 공용 이름)
- Subject/Issuer Organization(대상자/발급자 기관)

- Subject/Issuer Organization Unit(대상자/발급자 기관 부서)
- Not Valid Before/After(유효기간)
- Serial Number(일련 번호)
- Certificate Fingerprint(인증서 지문)
- Public Key Fingerprint(공개 키 지문)

SSL Failure Reason(SSL 실패 이유)

이 필드는 검색 전용입니다.

시스템이 암호화된 트래픽의 암호 해독에 실패한 이유:

- Unknown(알 수 없음)
- No Match(일치하지 않음)
- Success(TLS 필수 성공)
- Uncached Session(캐시되지 않은 세션)
- Unknown Cipher Suite(알 수 없는 암호 그룹)
- Unsupported Cipher Suite(지원되지 않는 암호 그룹)
- Unsupported SSL Version(지원되지 않는 SSL 버전)
- SSL Compression Used(SSL 압축 사용됨)
- Session Undecryptable in Passive Mode(패시브 모드에서 세션 암호 해독 불가)
- Handshake Error(핸드셰이크 오류)
- Decryption Error(암호 해독 오류)
- Pending Server Name Category Lookup(서버 이름 카테고리 조회 보류 중)
- Pending Common Name Category Lookup(공용 이름 카테고리 조회 보류 중)
- Internal Error
- Network Parameters Unavailable(네트워크 파라미터 사용 불가)
- Invalid Server Certificate Handle(유효하지 않은 서버 인증서 처리)
- Server Certificate Fingerprint Unavailable(서버 인증서 지문 사용 불가)
- Cannot Cache Subject DN(대상자 DN 캐시 불가)
- Cannot Cache Issuer DN(발급자 DN 캐시 발가)
- Unknown SSL Version(알 수 없는 SSL 버전)
- External Certificate List Unavailable(외부 인증서 목록 사용 불가)

- External Certificate Fingerprint Unavailable(외부 인증서 지문 사용 불가)
- Internal Certificate List Invalid(내부 인증서 목록이 유효하지 않음)
- Internal Certificate List Unavailable(내부 인증서 목록 사용 불가)
- Internal Certificate Unavailable(내부 인증서 사용 불가)
- Internal Certificate Fingerprint Unavailable(내부 인증서 지문 사용 불가)
- Server Certificate Validation Unavailable(서버 인증서 검증 사용 불가)
- Server Certificate Validation Failure(서버 인증서 검증 장애)
- Invalid Action(유효하지 않은 작업)

검색 워크플로 페이지의 **SSL Status(SSL** 상태**)** 필드에 필드값이 표시됩니다.

SSL 상태

암호화된 연결을 로깅한 **SSL Actual Action(SSL** 실제 작업**)**(해독 규칙, 기본 작업 또는 암호 해독이 불가능한 트래픽 작업)과 관련된 작업.

시스템이 암호화된 연결을 해독하지 못할 경우, 실행된 **SSL Actual Action(SSL** 실제 작업**)** (해독 불가능한 트래픽 작업)과 **SSL Failure Reason(SSL** 실패 이유**)**가 표시됩니다. 예를 들어, 시스템이 알 수 없는 암호 그룹으로 암호화된 트래픽을 탐지하고 추가 검사 없이 이를 허용할 경우 이 필드는 `Do Not Decrypt (Unknown Cipher Suite)`(암호 해독 하지 않음(알려지지 않은 암호화 그룹))로 표시됩니다.

인증서 세부사항을 보려면 잠금 아이콘을 클릭합니다.

이 필드를 검색할 때 **SSL Actual Action(SSL** 실제 작업**)** 중 하나 이상과 **SSL Failure Reason(SSL** 실패 이유**)**를 입력하고 시스템이 처리했거나 암호 해독에 실패한 암호화된 트래픽을 확인합니다.

SSL Subject/Issuer Country(SSL 대상자**/**발급자 국가**)**

이 필드는 검색 전용입니다.

암호화 인증서와 관련된 대상자 또는 발급자 국가의 2자 ISO 3166-1 alpha-2 국가 코드.

시간

이벤트의 날짜 및 시간. 이 필드는 검색할 수 없습니다.

VLAN ID (시스템 로그**: VLAN_ID)**

침입 이벤트를 트리거한 패킷에 관련된 가장 안쪽의 VLAN ID

웹 애플리케이션**(**시스템 로그**: WebApplication)**

침입 이벤트를 트리거한 트래픽에서 탐지된 HTTP 트래픽의 내용 또는 요청된 URL을 나타내는 웹 애플리케이션.

HTTP의 애플리케이션 프로토콜은 탐지하지만 특정 웹 애플리케이션은 탐지하지 못하는 경우 시스템은 그 대신 일반 웹 브라우징 지정을 제공합니다.

웹 애플리케이션 카테고리 및 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준

관련 항목

이벤트 검색

침입 이벤트 영향 레벨

이벤트가 네트워크에 미치는 영향을 평가할 수 있도록 Secure Firewall Management Center는 침입 이벤트의 테이블 보기에 영향 레벨을 표시합니다. 각 이벤트에 대해 시스템은 침입 데이터, 네트워크 검색 데이터 및 취약성 정보 사이의 상관관계를 색으로 나타내는 영향 레벨 아이콘을 추가합니다.

참고 NetFlow 데이터에서 네트워크 맵에 추가되는 호스트에 대해서는 운영 체제 정보가 제공되지 않으므로 시스템은 이러한 호스트와 관련된 침입 이벤트에 대해 취약함(영향 레벨 1: 빨강) 영향 레벨을 할당할 수 없습니다. 이러한 경우에는 호스트 입력 기능을 사용하여 호스트에 대한 운영 체제 ID를 수동으로 설정합니다.

다음 표에서는 영향 레벨의 가능한 값에 대해 설명합니다.

표 *3:* 영향 레벨

영향 레벨	취약성	색상	설명
Unknown(알 수 없음)(0)	알 수 없음	그레이	소스 호스트나 대상 호스트 모두 네트워크 검색에 의해 모니터링되는 네트워크에 없습니다.
Vulnerable(취약)(1)	취약함	빨간색	다음 중 하나에 해당합니다. • 소스 또는 대상 호스트가 네트워크 맵에 있으며, 취약성이 호스트에 매핑됨 • 소스 또는 대상 호스트가 바이러스, 트로이 목마 또는 기타 악성 소프트웨어에 감염되었을 가능성이 있음
Potentially Vulnerable(잠재적으로 취약)(2)	잠재적으로 취약함	오렌지	소스 또는 대상 호스트가 네트워크 맵에 있으며, 다음 중 하나가 참임: • 포트로 향하는 트래픽의 경우 포트가 서버 애플리케이션 프로토콜을 실행함 • 포트로 향하는 트래픽이 아닌 경우 호스트가 프로토콜을 사용함

영향 레벨	취약성	색상	설명
Currently Not Vulnerable(현재 취약하지 않음**)**(3)	현재 취약하지 않음	노란색	소스 또는 대상 호스트가 네트워크 맵에 있으며, 다음 중 하나가 참임: • 포트로 향하는 트래픽의 경우(예: TCP 또는 UDP), 포트가 열려 있지 않음 • 포트로 향하는 트래픽이 아닌 경우(예: ICMP), 호스트가 프로토콜을 사용하지 않음
Unknown Target(알 수 없는 대상**)**(4)	알 수 없는 대상	블루	소스 호스트 또는 대상 호스트가 모니터링되는 호스트에 있지만 네트워크 맵에는 호스트에 대한 항목이 없음.

침입 이벤트 관련 연결 데이터 보기

시스템은 침입 이벤트가 탐지된 연결을 로깅할 수 있습니다. 이 로깅은 액세스 제어 규칙과 연결된 침입 정책에 대해 자동으로 수행되지만, 기본 작업에 대한 관련 연결 데이터를 보려면 연결 로깅을 수동으로 활성화해야 합니다.

이벤트의 테이블 보기 간에 탐색할 때에는 관련된 데이터를 보는 것이 가장 유용합니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Intrusions(**침입**)** > **Events(**이벤트**)**을(를) 선택합니다.

단계 **2** 테이블의 확인란을 사용하여 침입 이벤트를 선택한 다음 **Jump to(**이동**)** 드롭다운 목록에서 **Connections(**연결**)**를 선택합니다.

팁 특정 연결에 연결된 침입 이벤트도 비슷한 방법으로 볼 수 있습니다. 자세한 내용은 워크플로 간 탐색를 참고하십시오.

관련 항목

허용된 연결에 대한 로깅

침입 이벤트 워크플로 사용, 23 페이지

연결 및 보안 관련 연결 이벤트 테이블 사용

검토된 침입 이벤트 표시

침입 이벤트가 악의적이지 않다고 확신하면 이벤트를 검토한 것으로 표시할 수 있습니다.

침입 이벤트를 검토한 결과 네트워크 보안에 위협이 되지 않을 것으로 확신하는 경우(예: 네트워크의 호스트 중 어떤 것도 탐지된 익스플로잇에 취약하지 않음을 알고 있음) 해당 이벤트를 검토한 것으로 표시할 수 있습니다. 검토된 이벤트는 이벤트 데이터베이스에 저장되며 이벤트 요약 통계에 포함되지만, 기본 침입 이벤트 페이지에는 더 이상 나타나지 않습니다. 사용자 이름이 검토자로 표시됩니다.

다중 도메인 구축에서 이벤트를 검토된 것으로 표시하는 경우, 시스템은 해당 이벤트를 볼 수 있는 모든 도메인에서 이를 검토된 것으로 표시합니다.

백업을 수행한 후 검토한 침입 이벤트를 삭제하면, 백업의 복원은 삭제된 침입 이벤트를 복원하지만 검토된 상태는 복원하지 않습니다. 복원된 침입 이벤트는 **Reviewed Events(**검토된 이벤트**)**가 아니라 **Intrusion Events(**침입 이벤트**)**에서 볼 수 있습니다.

프로시저

침입 이벤트를 보여주는 페이지에는 두 가지 옵션이 있습니다.

- 이벤트 목록에서 하나 이상의 침입 이벤트를 표시하려면, 이벤트 옆의 확인란을 선택하고 **Review(**검토**)**를 클릭합니다.
- 이벤트 목록에서 모든 침입 이벤트를 표시하려 **Review All(**모두 검토**)**을 클릭합니다.

관련 항목

침입 이벤트 워크플로 사용, 23 페이지

이전에 검토된 침입 이벤트 보기

다중 도메인 구축에서 이벤트를 검토된 것으로 표시하는 경우, 시스템은 해당 이벤트를 볼 수 있는 모든 도메인에서 이를 검토된 것으로 표시합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Intrusions(**침입**)** > **Reviewed Events(**검토한 이벤트**)**을(를) 선택합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- 타임 윈도우 변경에 설명된 대로 시간 범위를 조정합니다.
- 침입 이벤트 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용하는 경우, 워크플로 제목 옆에 있는 **(**워크플로 전환**)**를 클릭하여 시스템 제공 워크플로 중에서 선택합니다.
- 표시되는 이벤트에 대한 자세한 내용은 침입 이벤트 필드, 4 페이지를 참조하십시오.

관련 항목

침입 이벤트 워크플로 사용, 23 페이지

검토된 침입 이벤트를 검토되지 않은 것으로 표시

이벤트를 검토하지 않은 것으로 표시함으로써 검토된 이벤트를 기본 침입 이벤트 보기로 되돌릴 수 있습니다.

다중 도메인 구축에서 이벤트를 검토된 것으로 표시하는 경우, 시스템은 해당 이벤트를 볼 수 있는 모든 도메인에서 이를 검토된 것으로 표시합니다.

프로시저

검토된 이벤트를 표시하는 페이지에는 두 가지 옵션이 있습니다.

- 검토된 이벤트 목록에서 개별 침입 이벤트를 제거하려면 특정 이벤트 옆의 확인란을 선택하고 **Unreview(**검토 취소**)**를 클릭합니다.
- 검토된 이벤트의 목록에서 모든 침입 이벤트를 제거하려면 **Unreview All(**모두 검토 취소**)**을 클릭합니다.

전처리기 이벤트

전처리기는 다음 두 가지 기능을 제공합니다. 패킷에서 지정된 작업을 수행하고(예를 들어 HTTP 트래픽 디코딩 및 표준화) 패킷이 전처리기 옵션을 트리거하고 연결된 전처리기 규칙이 활성화될 때마다 이벤트를 생성하여 지정된 전처리기 옵션의 실행을 보고하는 것입니다. 예를 들어 `Double Encoding(이중 인코딩)` HTTP 검사 옵션과 HTTP 검사 생성기(GID)가 119이고 Snort ID(SID)가 2인 연결된 전처리기 규칙을 활성화하여 전처리기에 IIS 이중 인코딩된 트래픽이 발생할 때 이벤트를 생성할 수 있습니다.

전처리기의 실행을 보고하는 이벤트를 생성하면 비정상적인 프로토콜 익스플로잇을 탐지하는 데 도움이 됩니다. 예를 들어 공격자는 중복 IP 프래그먼트를 조작하여 호스트에서 DoS 공격을 일으킬 수 있습니다. IP 조각 모음 전처리기는 이 유형의 공격을 탐지하고 이에 대한 침입 이벤트를 생성할 수 있습니다.

패킷 표시에 이벤트에 대한 자세한 규칙 설명이 포함되지 않는다는 점에서 전처리기 이벤트는 규칙 이벤트와 다릅니다. 대신 패킷 표시에는 이벤트 메시지, GID, SID, 패킷 헤더 데이터 및 패킷 페이로드가 나타납니다. 이를 통해 패킷의 헤더 정보를 분석하고, 헤더 옵션이 사용 중인지와 시스템을 악용할 수 있는지를 파악하고, 패킷 페이로드를 검사할 수 있습니다. 전처리기가 각 패킷을 분석한 후 규칙 엔진은 잠재적인 콘텐츠 수준 위협을 추가 분석하고 보고할 수 있도록 이에 대해 적절한 규칙을 실행합니다(전처리기가 이를 조각 모음하고 유효한 세션의 일부로 설정할 수 있는 경우).

전처리기 생성기 **ID**

각 전처리기에는 어떤 전처리기가 패킷에 의해 트리거되었는지를 나타내는 자체 GID(Generator ID)가 있습니다. 일부 전처리기에는 잠재적 공격을 분류하는 ID 번호인 관련 SID도 있습니다. 이를 통해 규칙의 Snort ID(SID)가 규칙을 트리거하는 패킷의 컨텍스트를 제공하는 것과 유사한 방식으로 이벤트의 유형을 카테고리화하여 이벤트를 더 효과적으로 분석할 수 있습니다. 침입 정책 Rules(규칙) 페이지의 Preprocessors(전처리기) 필터 그룹에서 전처리기별로 전처리기 규칙을 나열할 수 있습니다.

또한 Category(카테고리) 필터 그룹의 전처리기 및 패킷 디코더 하위 그룹에 전처리기 규칙을 나열할 수도 있습니다.

참고 표준 텍스트 규칙에 의해 생성된 이벤트는 생성기 ID 1(전역 도메인 또는 레거시 GID) 또는 1000 - 2000(하위 도메인)을 갖습니다. 공유 개체 규칙의 경우, 이벤트에 생성기 ID는 3입니다. 두 규칙 모두 이벤트의 SID는 트리거된 특정 규칙을 나타냅니다.

다음 표에서는 각 GID를 생성하는 이벤트 유형에 대해 설명합니다.

표 *4:* 생성기 *ID*

ID	구성 요소	설명
1	표준 텍스트 규칙	패킷이 표준 텍스트 규칙(전역 도메인 또는 레거시 GID)을 트리거할 때 이벤트가 생성되었습니다.
2	태그가 지정된 패킷	태그 지정된 세션에서 패킷을 생성하는 Tag 생성기에 의해 이벤트가 생성되었습니다. 이는 `tag` 규칙 옵션이 사용될 때 발생합니다.
3	공유 개체 규칙	패킷이 공유 개체 규칙을 트리거할 때 이벤트가 생성되었습니다.
102	HTTP 디코더	디코더 엔진이 패킷 내에서 HTTP 데이터를 디코딩했습니다.
105	Back Orifice 탐지기	Back Orifice 탐지기가 패킷에 연결된 Back Orifice 공격을 식별했습니다.
106	RPC 디코더	RPC 디코더가 패킷을 디코딩했습니다.
116	패킷 디코더	패킷 디코더에 의해 이벤트가 생성되었습니다.
119, 120	HTTP 검사 전처리기	HTTP 검사 전처리기에 의해 이벤트가 생성되었습니다. GID 120 규칙은 서버별 HTTP 트래픽과 관련이 있습니다.
122	포트스캔 탐지기	포트스캔 플로우 디코더에 의해 이벤트가 생성되었습니다.
123	IP 조각 모음기	조각난 IP 데이터그램을 제대로 리어셈블할 수 없을 때 이벤트가 생성되었습니다.
124	SMTP 디코더	SMTP 전처리기가 SMTP 동사에서 익스플로잇을 탐지하여 이벤트가 생성되었습니다.
125	FTP 디코더	FTP/텔넷 디코더가 FTP 트래픽 내에서 익스플로잇을 탐지하여 이벤트가 생성되었습니다.
126	텔넷 디코더	FTP/텔넷 디코더가 텔넷 트래픽 내에서 익스플로잇을 탐지하여 이벤트가 생성되었습니다.
128	SSH 전처리기	SSH 전처리기가 SSH 트래픽 내에서 익스플로잇을 탐지하여 이벤트가 생성되었습니다.

ID	구성 요소	설명
129	스트림 전처리기	스트림 전처리기에 의한 스트림 전처리 중에 이벤트가 생성되었습니다.
131	DNS 전처리기	DNS 전처리기에 의해 이벤트가 생성되었습니다.
133	DCE/RPC 전처리기	DCE/RPC 전처리기에 의해 이벤트가 생성되었습니다.
134	규칙 레이턴시 패킷 레이턴시	규칙 레이턴시가 침입 규칙의 그룹을 일시 중지(134:1) 또는 다시 활성화(134:2)하거나 패킷 레이턴시 임계값이 초과되었기 때문에 시스템이 패킷 검사를 중지하여(134:3) 이벤트가 생성되었습니다.
135	속도 기반 공격 탐지기	속도 기반 공격 탐지기가 네트워크의 호스트에 대한 과도한 연결을 식별하여 이벤트가 생성되었습니다.
137	SSL 전처리기	TLS/SSL 전처리기에 의해 이벤트가 생성되었습니다.
138, 139	민감한 데이터 전처리기	민감한 데이터 전처리기에 의해 이벤트가 생성되었습니다.
140	SIP 전처리기	SIP 전처리기에 의해 이벤트가 생성되었습니다.
141	IMAP 전처리기	IMAP 전처리기에 의해 이벤트가 생성되었습니다.
142	POP 전처리기	POP 전처리기에 의해 이벤트가 생성되었습니다.
143	GTP 전처리기	GTP 전처리기에 의해 이벤트가 생성되었습니다.
144	Modbus 전처리기	Modbus SCADA 전처리기에 의해 이벤트가 생성되었습니다.
145	DNP3 전처리기	DNP3 SCADA 전처리기에 의해 이벤트가 생성되었습니다.
148	CIP 전처리기	CIP SCADA 전처리기에 의해 이벤트가 생성되었습니다.
149	S7Commplus 전처리기	Modbus SCADA 전처리기에 의해 이벤트가 생성되었습니다.
1000 - 2000	표준 텍스트 규칙	패킷이 표준 텍스트 규칙(하위 도메인)을 트리거할 때 이벤트가 생성되었습니다.

침입 이벤트 워크플로 페이지

현재 침입 정책에서 활성화된 전처리기, 디코더 및 침입 규칙은 모니터링하는 트래픽이 정책을 위반할 때마다 침입 이벤트를 생성합니다.

Firepower System은 이벤트 데이터로 채워치고 침입 이벤트를 보고 분석할 수 있는 사전 정의된 워크플로 집합을 제공합니다. 이러한 각 워크플로는 평가할 침입 이벤트를 정확히 찾아낼 수 있도록 일련의 페이지를 통해 사용자를 안내합니다.

사전 정의된 침입 이벤트 워크플로에는 세 가지 페이지 유형 또는 이벤트 보기가 포함되어 있습니다.

- 하나 이상의 드릴다운 페이지

- 침입 이벤트의 테이블 보기
- 패킷 보기

*Drill-down(*드릴다운*)* 페이지에는 일반적으로 한 테이블(일부 드릴다운 보기의 경우 둘 이상의 테이블)에 하나의 특정 정보 유형을 볼 수 있는 둘 이상의 열이 포함되어 있습니다.

하나 이상의 대상 포트에 대한 추가 정보를 찾기 위해 "드릴다운"할 때 자동으로 이러한 이벤트를 선택하게 되며, 워크플로의 다음 페이지가 나타납니다. 이런 식으로 드릴다운 테이블은 한 번에 분석하는 이벤트 수를 줄입니다.

침입 이벤트의 초기 테이블 보기에서는 각 침입 이벤트가 고유한 행에 나열됩니다. 테이블의 열에는 시간, 소스 IP 주소와 포트, 대상 IP 주소와 포트, 이벤트 우선순위, 이벤트 메시지 등의 정보가 나열됩니다.

워크플로에서 이벤트를 선택하고 다음 페이지를 표시하는 대신, 테이블 보기에서 이벤트를 선택하면 제약 조건이라는 것이 추가됩니다. 제약 조건이란 분석할 이벤트 유형에 적용하는 제한입니다.

예를 들어 임의의 열에서 **Close(**닫기**)** (✕)을 클릭하고 드롭다운 목록에서 **Time(**시간**)**을 지우면 열 중 하나로 Time(시간)을 제거할 수 있습니다. 분석에서 이벤트 목록을 좁히려면 테이블 보기의 행 중 하나에서 값의 링크를 클릭할 수 있습니다. 예를 들어 소스 IP 주소 중 하나(잠재적인 공격자)에서 생성되는 이벤트로 분석을 제한하려면 **Source IP Address(**소스 **IP** 주소**)** 열에서 해당 IP 주소를 클릭합니다.

테이블 보기에서 하나 이상의 행을 선택한 다음 **View(**보기**)**를 클릭하면 패킷 보기가 나타납니다. 패킷 보기는 규칙을 트리거한 패킷 또는 이벤트를 생성한 전처리기에 대한 정보를 제공합니다. 패킷 보기의 각 섹션에는 패킷의 특정 레이어에 대한 정보가 포함되어 있습니다. 더 많은 정보를 보려면 축소된 섹션을 확장할 수 있습니다.

참고 각 포트스캔 이벤트는 여러 패킷에 의해 트리거되므로, 포트스캔 이벤트는 패킷 보기의 특수 버전을 사용합니다.

미리 정의된 워크플로가 특정 요구 사항을 충족하지 않는 경우, 관심 있는 정보만 표시되는 맞춤형 워크플로를 만들 수 있습니다. 맞춤형 침입 이벤트 워크플로에는 드릴 다운 페이지나 이벤트의 테이블 보기 또는 둘 다가 포함될 수 있습니다. 시스템은 자동으로 패킷 페이지를 마지막 페이지로 포함합니다. 이벤트를 조사하려는 방법에 따라 사전 정의 워크플로와 맞춤형 워크플로 간에 손쉽게 전환할 수 있습니다.

침입 이벤트 워크플로 사용

이벤트의 드릴다운 보기 및 테이블 보기에는 몇 가지 공통된 기능이 있습니다. 이러한 기능을 사용하면 이벤트 목록의 범위를 좁히고 관련 이벤트의 그룹으로 분석을 집중할 수 있습니다.

서로 다른 워크플로 페이지에 동일한 침입 이벤트가 표시되지 않도록, 시간 범위는 다른 이벤트 페이지를 표시하기 위해 페이지 아래쪽에서 링크를 클릭할 때 일시 중지되고, 후속 페이지에서 다른 작업을 수행하기 위해 클릭할 때 다시 시작됩니다.

팁 프로세스의 어떤 지점에서든 제약 조건을 검색 기준 집합으로 저장할 수 있습니다. 예를 들어 지난 며칠 동안 네트워크가 단일 IP 주소의 공격자에 의해 프로브된 것을 발견한 경우, 조사 중에 제약 조건을 저장한 다음 나중에 다시 사용할 수 있습니다. 그러나 복합 제약 조건을 검색 기준 집합으로 저장할 수는 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Intrusions(**침입**)** > **Events(**이벤트**)**를 사용하여 침입 이벤트 워크플로에 액세스합니다.

단계 **2** 원하는 경우, 침입 이벤트 드릴다운 페이지 제약 조건, 25 페이지 또는 침입 이벤트 테이블 보기 제약 조건, 26 페이지에 설명된 대로 이벤트 보기에 나타나는 침입 이벤트 수를 제한합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- 표시되는 열에 대한 자세한 내용은 침입 이벤트 필드, 4 페이지를 참조하십시오.
- 호스트의 프로파일을 보려면 호스트 IP 주소 옆에 표시되는 **Host Profile(**호스트 프로파일**)**을 클릭합니다.
- 지리위치 세부 사항을 보려면 Source Country(소스 국가) 또는 Destination Country(대상 국가) 열에 표시되는 플래그를 클릭합니다.
- Firepower 시스템 외부에서 이용할 수 있는 소스의 데이터를 보려면 이벤트 값에서 마우스 오른쪽 버튼으로 클릭합니다. 표시되는 옵션은 데이터 유형에 따라 다르며 공개 소스를 포함합니다. 다른 소스는 구성한 리소스에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사 섹션을 참조해 주십시오.
- 이벤트에 대한 일반 정보를 수집하려면 테이블에서 이벤트 값을 마우스 오른쪽 버튼으로 클릭하고 Cisco 또는 서드파티 인텔리전스 소스에서 선택합니다. 예를 들어 Cisco Talos에서 의심스러운 IP 주소에 대한 상세정보를 얻을 수 있습니다. 표시되는 옵션은 데이터 유형 및 시스템에서 구성된 통합에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사를 참고하십시오.
- 표시된 이벤트의 시간 및 날짜 범위를 수정하려면 타임 윈도우 변경를 참조하십시오.

  팁 이벤트 보기에 침입 이벤트가 나타나지 않는 경우 지정된 기간을 조정하면 결과가 반환될 수 있습니다. 더 오래된 시간 범위를 지정한 경우, 해당 시간 범위의 이벤트가 삭제되었을 수 있습니다. 규칙 임계값 지정 구성을 조정하면 이벤트가 생성될 수 있습니다.

  참고 어플라이언스의 구성된 기간(전역 또는 이벤트 전용 모두 해당)을 벗어나 생성된 이벤트는 시간 기준으로 이벤트 보기를 제한할 경우 이벤트 보기에 나타날 수 있습니다. 이는 어플라이언스에 대한 슬라이딩 시간 창을 구성한 경우에도 발생할 수 있습니다.

- 현재 워크플로 페이지에서 이벤트를 정렬하거나 현재 워크플로 페이지 내에서 이동하려면 워크플로 사용을 참조하십시오.
- 현재 제약 조건을 유지하면서 현재 워크플로의 페이지 사이를 이동하려면 워크플로 페이지의 왼쪽 위에서 해당 페이지 링크를 클릭합니다.
- 이벤트 데이터베이스에서 이벤트를 삭제하려면 삭제할 이벤트 옆의 확인란을 선택한 다음 **Delete(**삭제**)**를 클릭하거나 **Delete All(**모두 삭제**)**을 클릭합니다.
- 이벤트를 검토된 것으로 표시하여 침입 이벤트 페이지에서는 제거하되 이벤트 데이터베이스에서는 제거하지 않으려면 검토된 침입 이벤트 표시, 18 페이지을 참조하십시오.
- 선택된 각 이벤트를 트리거한 패킷의 로컬 사본(libpcap 형식의 패킷 캡처 파일)을 다운로드하려면 다운로드하려는 패킷이 트리거한 이벤트 옆의 확인란을 선택한 다음 **Download Packets(**패킷 다운로드**)**를 클릭하거나 **Download All Packets(**모든 패킷 다운로드**)**를 클릭합니다. 캡처된 패킷은 libpcap 형식으로 저장됩니다. 이 형식은 여러 인기 있는 프로토콜 분석기에서 사용됩니다.
- 다른 이벤트 보기로 이동해 연결된 이벤트를 보려면 워크플로 간 탐색을 참조하십시오.
- 다른 워크플로우를 임시로 사용하려면 **(**워크플로우 전환**)**를 클릭합니다.
- 빠르게 돌아올 수 있도록 현재 페이지를 즐겨찾기하려면 **Bookmark This Page(**이 페이지 즐겨찾기**)**를 클릭합니다.
- Summary Dashboard(요약 대시보드)의 Intrusion Events(침입 이벤트) 섹션을 보려면 **Dashboards(**대시보드**)**를 클릭합니다.
- 즐겨찾기 관리 페이지로 이동하려면 **View Bookmarks(**즐겨찾기 보기**)**를 클릭합니다.
- 현재 보기의 데이터를 기반으로 보고서를 생성하려면 이벤트 보기에서 보고서 템플릿 생성을 참조하십시오.

관련 항목

이벤트 검색

북마크

침입 이벤트 드릴다운 페이지 제약 조건

다음 표에서는 드릴다운 페이지를 사용하는 방법에 대해 설명합니다.

표 ***5:*** 드릴다운 페이지에서 이벤트 제한

목적	방법
다음 워크플로 페이지로 드릴다운하여 특정 값으로 제한	값을 클릭 합니다. 예를 들어 Destination Port(대상 포트) 워크플로에서 대상 포트 80으로 이벤트를 제한하려면 **DST Port/ICMP Code(DST** 포트**/ICMP** 코드**)** 열에서 **80/tcp**를 클릭합니다. 워크플로의 다음 페이지인 Events(이벤트)가 나타나고, 포트 80/tcp 이벤트만 포함됩니다.

목적	방법
다음 워크플로 페이지로 드릴다운하여 선택한 이벤트로 제한	다음 워크플로 페이지에서 보려는 이벤트 옆에 있는 확인란을 선택하고 **View(**보기**)**를 클릭합니다. 예를 들어 Destination Port(목적지 포트) 워크플로에서 목적지 포트 20/tcp 및 21/tcp로 이벤트를 제한하려면 해당 포트의 행 옆에 있는 확인란을 선택하고 **View(**보기**)**를 클릭합니다. 워크플로의 다음 페이지인 Events(이벤트)가 나타나고, 포트 20/tcp 및 21/tcp 이벤트만 포함됩니다. 여러 행으로 제한하려는 경우 테이블에 열이 두 개 이상이면(Count 열은 포함하지 않음) 복합 제약 조건을 구축해야 합니다. 복합 제약 조건은 의도한 것보다 더 많은 이벤트가 제약 조건에 포함되지 않도록 보장합니다. 예를 들어 Event and Destination(이벤트 및 목적지) 워크플로를 사용하는 경우 첫 번째 드릴다운 페이지에서 선택하는 각 행은 복합 제약 조건을 생성합니다. 목적지 IP 주소가 10.10.10.100인 이벤트 1:100을 선택하고 목적지 IP 주소가 192.168.10.100인 이벤트 1:200도 선택하는 경우, 복합 제약 조건은 1:100을 이벤트 유형으로, 192.168.10.100을 목적지 IP 주소로 포함하는 이벤트 또는 1:200을 이벤트 유형으로, 10.10.10.100을 목적지 IP 주소로 포함하는 이벤트도 선택되지 않도록 합니다.
현재의 제약 조건을 유지한 채 다음 워크플로 페이지로 드릴다운	**View All(**모두 보기**)**를 클릭합니다.

침입 이벤트 테이블 보기 제약 조건

다음 표에서는 테이블 보기를 사용하는 방법에 대해 설명합니다.

표 ***6:*** 이벤트의 테이블 보기에서 이벤트 제한

목적	방법
단일 속성이 있는 이벤트로 보기를 제한	속성을 클릭합니다. 예를 들어 목적지 포트가 80인 이벤트로 보기를 제한하려면 **DST Port/ICMP Code(DST** 포트**/ICMP** 코드**)** 열에서 **80/tcp**를 클릭합니다.
테이블에서 열 제거	숨기려는 열 머리글에서 **Close(**닫기**)** (✕)을 클릭합니다. 표시되는 팝업 창에서 **Apply(**적용**)**를 클릭합니다. 다른 열을 숨기거나 표시하려면 **Apply(**적용**)**를 클릭하기 전에 해당 확인란을 선택하거나 선택 취소합니다. 비활성화된 열을 보기에 다시 추가하려면 확장 화살표를 클릭하여 검색 제약 조건을 확장한 다음, **Disabled Columns(**비활성화된 열**)** 아래에서 열 이름을 클릭합니다.

목적	방법
하나 이상의 이벤트에 연결된 패킷 보기	다음 중 하나: • 패킷을 보려는 이벤트 옆에 있는 아래쪽 화살표를 클릭합니다. • 패킷을 보려는 하나 이상의 이벤트를 선택하고 페이지 아래쪽에서 **View(**보기**)**를 클릭합니다. • 페이지 아래쪽에서, 현재 제약 조건과 일치하는 모든 이벤트에 대한 패킷을 보려면 **View All(**모두 보기**)**을 클릭합니다.

침입 이벤트 패킷 보기 사용

패킷 보기는 침입 이벤트를 생성한 규칙을 트리거한 패킷에 대한 정보를 제공합니다.

팁 이벤트를 탐지한 디바이스에 대해 **Transfer Packet(**패킷 전송**)** 옵션이 비활성화된 경우 Secure Firewall Management Center의 패킷 보기에는 패킷 정보가 포함되지 않습니다.

패킷 보기는 패킷이 트리거한 침입 이벤트에 대한 정보를 제공함으로써 특정 패킷이 캡처된 이유를 나타냅니다. 그러한 정보에는 이벤트의 타임스탬프, 메시지, 분류, 우선순위가 포함되며, 이벤트가 표준 텍스트 규칙에 의해 생성된 경우 이벤트를 생성한 규칙도 포함됩니다. 패킷 보기는 또한 크기를 비롯한 패킷에 대한 일반 정보도 제공합니다.

패킷 보기에는 데이터 링크, 네트워크, 전송 등 패킷의 각 레이어에 대해 설명하는 섹션은 물론, 패킷을 구성하는 바이트에 대해 설명하는 섹션도 있습니다. 시스템이 패킷을 해독하면 해독된 바이트를 볼 수 있습니다. 자세한 정보를 보려면 축소된 섹션을 확장할 수 있습니다.

참고 각 포트스캔 이벤트는 여러 패킷에 의해 트리거되므로, 포트스캔 이벤트는 패킷 보기의 특수 버전을 사용합니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** 침입 이벤트의 테이블 보기에서 침입 이벤트 테이블 보기 제약 조건, 26 페이지에 설명된 대로 볼 패킷을 선택합니다.

단계 **2** 필요에 따라 하나 이상의 이벤트를 선택한 경우, 페이지 하단의 페이지 번호를 사용하여 패킷 보기에서 페이지를 전환할 수 있습니다.

단계 **3** 다음과 같은 옵션이 있습니다.

- 조정 - 패킷 보기에서 날짜 및 시간 범위를 수정하려면 타임 윈도우 변경를 참조하십시오.
- 구성 - 이벤트를 트리거한 침입 규칙을 구성하려면 Actions(작업) 옆의 화살표를 클릭하고 패킷 보기 내 침입 규칙 설정, 31 페이지에 설명된 대로 계속합니다.
- 삭제 - 데이터베이스에서 이벤트를 삭제하려면 **Delete(**삭제**)**를 클릭하여 패킷을 보고 있는 이벤트를 삭제하거나 **Delete All(**모두 삭제**)**을 클릭하여 이전에 패킷을 선택한 모든 이벤트를 삭제합니다.
- 다운로드 - 이벤트를 트리거한 패킷의 로컬 사본(libpcap 형식의 패킷 캡처 파일)을 다운로드하려면 **Download Packet(**패킷 다운로드**)**을 클릭하여 보고 있는 이벤트의 캡처된 패킷 사본을 저장하거나 **Download All Packets(**모든 패킷 다운로드**)**를 클릭하여 패킷을 이전에 선택한 모든 이벤트의 캡처된 패킷 사본을 저장합니다. 캡처된 패킷은 libpcap 형식으로 저장됩니다. 이 형식은 여러 인기 있는 프로토콜 분석기에서 사용됩니다.

  참고 단일 포트스캔 이벤트는 여러 패킷을 기반으로 하기 때문에 포트스캔 패킷을 다운로드할 수 없습니다. 그러나 포트스캔 보기는 사용할 만한 모든 패킷 정보를 제공합니다. 다운로드하려면 사용 가능한 디스크 공간이 15% 이상 남아 있어야 합니다.

- 검토 표시 - 이벤트를 검토된 것으로 표시하여 이벤트 보기에서는 제외하되 이벤트 데이터베이스에서는 제외하지 않으려면 **Review(**검토**)**를 클릭하여 패킷을 보고 있는 이벤트를 표시하거나 **Review All(**모두 검토**)**을 클릭하여 이전에 패킷을 선택한 모든 이벤트를 표시합니다. 자세한 내용은 검토된 침입 이벤트 표시, 18 페이지를 참고하십시오.
- 추가 정보 보기 - 페이지 섹션을 확장하거나 축소하려면 섹션 옆에 있는 화살표를 클릭합니다. 자세한 내용은 이벤트 정보 필드, 28 페이지, 프레임 정보 필드, 35 페이지, 데이터 링크 레이어 정보 필드, 36 페이지을 참조하십시오.
- 네트워크 레이어 정보 보기 - 네트워크 레이어 정보 보기, 37 페이지를 참조하십시오.
- 패킷 바이트 정보 보기 - 패킷 바이트 정보 보기, 42 페이지를 참조하십시오.
- 전송 레이어 정보 보기 - 다음 참조 전송 레이어 정보 보기, 39 페이지

관련 항목

포트스캔 탐지

이벤트 정보 필드

패킷 보기에서는 Event Information(이벤트 정보) 섹션에서 패킷에 대한 정보를 볼 수 있습니다.

Event(이벤트**)**

이벤트 메시지입니다. 규칙 기반 이벤트의 경우에는 규칙 메시지에 해당합니다. 다른 이벤트의 경우에는 디코더 또는 전처리기에 의해 결정됩니다.

이벤트의 ID는 (GID:SID:Rev) 형식으로 메시지에 추가됩니다. GID는 이벤트를 생성한 규칙 엔진, 디코더 또는 전처리기의 생성자 ID입니다. SID는 규칙, 디코더 메시지 또는 전처리기 메시지의 식별자입니다. Rev는 규칙의 개정 번호입니다.

타임스탬프

패킷이 캡처된 시간(UTC 시간대)입니다.

분류

이벤트 분류입니다. 규칙 기반 이벤트의 경우 규칙 분류에 해당합니다. 다른 이벤트의 경우에는 디코더 또는 전처리기에 의해 결정됩니다.

Priority(우선순위**)**

이벤트 우선순위입니다. 규칙 기반 이벤트의 경우 `priority` 키워드의 값 또는 `classtype` 키워드의 값에 해당합니다. 다른 이벤트의 경우에는 디코더 또는 전처리기에 의해 결정됩니다.

인그레스 보안 영역

이벤트를 트리거한 패킷의 인그레스 보안 영역입니다. 수동 배포에서는 이 보안 영역 필드만 입력됩니다.

이그레스 보안 영역

이벤트를 트리거한 패킷의 이그레스 보안 영역입니다. 패시브 구축에서는 이 필드가 채워지지 않습니다.

도메인

매니지드 디바이스가 속한 도메인입니다. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

디바이스

액세스 제어 정책이 구축된 매니지드 디바이스입니다.

보안 상황

트래픽이 통과한 가상 방화벽 그룹을 식별하는 메타데이터입니다. 시스템은 다중 상황 모드의 ASA FirePOWER에 대해서만 이 필드를 채웁니다.

인그레스 인터페이스

이벤트를 트리거한 패킷의 인그레스 인터페이스입니다. 패시브 인터페이스에 대해서는 이 인터페이스 열만 채워집니다.

이그레스 인터페이스

인라인 집합의 경우 이벤트를 트리거한 패킷의 이그레스 인터페이스입니다.

Source/Destination IP

이벤트(소스)를 트리거한 패킷이 시작된 호스트 IP 주소 또는 도메인 이름 또는 이벤트를 트리거한 트래픽의 대상(목적지) 호스트입니다.

소스 포트**/ICMP** 유형

이벤트를 트리거한 패킷의 소스 포트입니다. ICMP 트래픽의 경우 포트 번호가 없으면 시스템은 ICMP 유형을 표시합니다.

대상 포트**/ICMP** 코드

트래픽을 수신하는 호스트의 포트 번호입니다. ICMP 트래픽의 경우 포트 번호가 없으면 시스템은 ICMP 코드를 표시합니다.

Email Headers(이메일 헤더**)**

이메일 헤더에서 추출된 데이터입니다. 이메일 헤더는 침입 이벤트의 테이블 보기에 나타나지 않지만 이메일 헤더를 검색 기준으로 사용할 수 있습니다.

이메일 헤더를 SMTP 트래픽의 침입 이벤트와 연결하려면 SMTP 프리프로세서 **Log Headers(**헤더 로깅**)** 옵션을 활성화해야 합니다. 규칙 기반 이벤트의 경우 이메일 데이터가 추출될 때 이 행이 나타납니다.

HTTP Hostname(HTTP 호스트네임**)**

HTTP 요청 Host 헤더에서 추출된 호스트 이름(있는 경우). 이 행은 최대 256바이트까지 전체 호스트 이름을 표시합니다. 단일 행보다 길 경우 전체 호스트 이름을 확장할 수 있습니다.

호스트 이름을 표시하려면 HTTP Inspect 전처리기 **Log Hostname(**호스트 이름 로깅**)** 옵션을 활성화해야 합니다.

HTTP 요청 패킷에 항상 호스트 이름이 포함되는 것은 아닙니다. 규칙 기반 이벤트의 경우 이 행은 패킷에 HTTP 호스트 이름 또는 HTTP URI가 포함된 경우 나타납니다.

HTTP URI

침입 이벤트를 트리거한 HTTP 요청 패킷과 연결된 원시 URI(있는 경우). 이 행은 최대 2048바이트까지 전체 URI를 표시합니다. 단일 행보다 길 경우 전체 URI를 확장할 수 있습니다.

URI를 표시하려면 HTTP Inspect 전처리기 **Log URI(URI** 로깅**)** 옵션을 활성화해야 합니다.

HTTP 요청 패킷에 항상 URI가 포함되는 것은 아닙니다. 규칙 기반 이벤트의 경우 이 행은 패킷에 HTTP 호스트 이름 또는 HTTP URI가 포함된 경우 나타납니다.

HTTP 응답에 의해 트리거된 침입 이벤트에서 연결된 HTTP URI를 보려면 **Perform Stream Reassembly on Both Ports(**양쪽 포트에서 스트림 리어셈블리 수행**)** 옵션에서 HTTP 서버를 구성해야 합니다. 그러나 이렇게 하면 트래픽 리어셈블리를 위한 리소스 수요가 증가합니다.

침입 정책

침입 이벤트를 생성한 침입, 전처리기 또는 디코더 규칙이 활성화된 침입 정책(있는 경우). 액세스 제어 정책의 기본 작업으로 침입 정책을 선택하거나 침입 정책을 액세스 제어 규칙과 연결할 수 있습니다.

액세스 제어 정책

이벤트를 생성한 침입, 전처리기 또는 디코더 규칙이 활성화된 침입 정책을 포함하는 액세스 제어 정책.

액세스 제어 규칙

이벤트를 생성한 침입 규칙에 연결된 액세스 제어 규칙입니다. Default Action(기본 작업)은 규칙이 활성화된 침입 정책이 액세스 제어 규칙과 연결되지 않은 대신 액세스 제어 정책의 기본 작업으로 구성되었음을 나타냅니다.

규칙

표준 텍스트 규칙 이벤트의 경우, 이벤트를 생성한 규칙입니다.

이벤트가 공유 개체 규칙, 디코더 또는 전처리기를 기반으로 하는 경우에는 규칙을 사용할 수 없습니다.

규칙 데이터에는 네트워크에 대한 민감한 정보가 포함될 수 있으므로 관리자는 사용자 역할 편집기의 View Local Rules(로컬 규칙 보기) 권한을 사용하여 패킷 보기에서 규칙 정보를 보는 사용자의 기능을 전환할 수 있습니다.

작업

표준 텍스트 및 맞춤형 규칙 이벤트의 경우, 이벤트를 트리거한 규칙에 대해 다음 작업을 수행하려면 **Actions(**작업**)**를 확장합니다.

- 규칙 수정
- 규칙의 개정 설명서를 봅니다. 표준 텍스트 규칙에 한해 Actions(작업)에서 **View Documentation(**설명서 보기**)**을 클릭한 후 설명서 팝업창에 있는 **Rule Documentation(**규칙 설명서**)**을 클릭하면 더 구체적인 규칙 세부 정보를 볼 수 있습니다.
- 규칙에 코멘트 추가
- 규칙의 상태 변경
- 규칙에 대한 임계값 설정
- 규칙 억제

이벤트가 공유 개체 규칙, 디코더 또는 전처리기를 기반으로 하는 경우에는 규칙을 사용할 수 없습니다.

패킷 보기 내 침입 규칙 설정

침입 이벤트 패킷 보기 내에서 이벤트를 트리거한 규칙에 여러 작업을 수행할 수 있습니다. 이벤트가 공유 개체 규칙, 디코더 또는 전처리기를 기반으로 하는 경우에는 규칙을 사용할 수 없습니다.

프로시저

단계 **1** 침입 규칙에 의해 생성된 침입 이벤트의 패킷 보기 내에서 Event Information(이벤트 정보) 섹션의 **Actions(**작업**)**를 확장합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- 코멘트 - 표준 텍스트 규칙 이벤트의 경우, **Rule Comment(**규칙 코멘트**)**를 클릭하여 이벤트를 생성한 규칙에 텍스트 코멘트를 추가합니다. 그러면 식별된 정책 위반 또는 공격 및 규칙에 대한 자세한 컨텍스트 및 정보를 제공할 수 있습니다. 침입 규칙 편집기에서도 규칙 코멘트를 추가하고 볼 수 있습니다.
- Disable(비활성화) - 이 규칙을 비활성화하려면 다음 옵션 중 하나를 클릭합니다.
  - 현재 **Snort 2** 정책**(<policy_name>)**에서 이 규칙 비활성화
  - 로컬로 작성된 모든 **Snort 2** 정책에서 이 규칙 비활성화

  이 이벤트가 표준 텍스트 규칙에 의해 생성된 경우, 필요 시 규칙을 비활성화할 수 있습니다. 로컬로 수정할 수 있는 모든 정책에서 규칙을 설정할 수 있습니다. 또는 현재 정책을 로컬로 수정할 수 있는 경우 현재 정책(즉, 이벤트를 생성한 정책)에서만 규칙을 설정할 수 있습니다.

  현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어 맞춤형 정책은 수정할 수 있지만 시스템에서 제공한 기본 정책은 수정할 수 없습니다.

  참고 패킷 보기에서 공유 개체 규칙을 비활성화할 수 없으며, 기본 정책에서도 규칙을 비활성화할 수 없습니다.

- 패킷 삭제 및 이벤트 생성 - 패킷을 트리거하고 이벤트를 생성하는 패킷을 삭제하도록 규칙을 설정하려면 다음 옵션 중 하나를 클릭합니다.
  - 현재 **Snort 2** 정책**(<policy_name>)**에서 트리거 패킷을 삭제하고 이벤트를 생성하도록 이 규칙 설정
  - 로컬로 작성된 모든 **Snort 2** 인라인 정책에서 트리거 패킷을 삭제하고 이벤트를 생성하도록 이 규칙 설정

  매니지드 디바이스가 네트워크에서 인라인으로 구축된 경우, 이벤트를 트리거한 규칙이 로컬로 수정할 수 있는 모든 정책에서 규칙을 트리거하는 패킷을 삭제하도록 설정할 수 있습니다. 또는 현재 정책을 로컬로 수정할 수 있는 경우 현재 정책(즉, 이벤트를 생성한 정책)에서만 규칙을 설정할 수 있습니다.

  현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어 맞춤형 정책은 수정할 수 있지만 시스템에서 제공한 기본 정책은 수정할 수 없습니다. 또한 이 옵션은 **Drop when Inline(**인라인 시 삭제**)**이 현재 정책에서 활성화된 경우에만 나타납니다.

- 편집 - 표준 텍스트 규칙 이벤트의 경우 **Edit(**편집**)**를 클릭하여 Snort 2 규칙을 편집하거나 **Edit Snort 3 Rule(Snort 3** 규칙 편집**)**을 클릭하여 이벤트를 생성한 규칙을 수정합니다. 이벤트가 공유 개체 규칙, 디코더 또는 전처리기를 기반으로 하는 경우에는 규칙을 사용할 수 없습니다.

참고 (맞춤형 표준 텍스트 규칙과 달리) 시스템 제공 규칙을 수정하는 경우, 실제로는 새 로컬 규칙을 생성하는 것입니다. 이벤트를 생성하도록 로컬 규칙을 설정하고, 현재 침입 정책에서 원래 규칙을 비활성화해야 합니다. 그러나 기본 정책의 로컬 규칙은 활성화할 수 없습니다.

- 이벤트 생성 - 이벤트를 생성하도록 규칙을 설정하려면 **Set this rule to generate events in all locally created Snort 2 policies(**로컬로 작성된 모든 **Snort 2** 정책에서 이벤트를 생성하도록 이 규칙 설정**)**를 클릭합니다.

  이 이벤트가 표준 텍스트 규칙에 의해 생성된 경우, 로컬에서 수정할 수 있는 모든 정책에서 이벤트를 생성하도록 규칙을 설정할 수 있습니다.

  현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어 맞춤형 정책은 수정할 수 있지만 시스템에서 제공한 기본 정책은 수정할 수 없습니다.

  참고 패킷 보기에서 공유 개체 규칙을 비활성화할 수 없으며, 기본 정책에서도 규칙을 비활성화할 수 없습니다.

- 억제 옵션 설정 - **Set Suppression Options(**억제 옵션 설정**)**를 확장하고 패킷 보기 내 삭제 옵션 설정, 34 페이지에 설명된 대로 계속합니다.

  이 옵션을 사용하면 로컬로 수정할 수 있는 모든 정책에서 이 이벤트를 트리거한 규칙을 억제할 수 있습니다. 또는 현재 정책을 로컬로 수정할 수 있는 경우 현재 정책(즉, 이벤트를 생성한 정책)에서만 규칙을 억제할 수 있습니다.

  현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어 맞춤형 정책은 수정할 수 있지만 Cisco에서 제공한 기본 정책은 수정할 수 없습니다.

- 임계값 옵션 설정 - **Set Thresholding Options(**임계값 옵션 설정**)**를 확장하고 패킷 보기 내 임계값 옵션 설정, 33 페이지의 설명에 따라 계속합니다.

  이 옵션을 사용하면 로컬로 수정할 수 있는 모든 정책에서 이 이벤트를 트리거한 규칙에 대해 임계값을 생성할 수 있습니다. 또는 현재 정책을 로컬로 수정할 수 있는 경우 현재 정책(즉, 이벤트를 생성한 정책)에 대해서만 임계값을 생성할 수 있습니다.

  현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어 맞춤형 정책은 수정할 수 있지만 시스템에서 제공한 기본 침입 정책은 수정할 수 없습니다.

- 설명서 보기 - 이벤트를 생성한 규칙에 대해 자세히 알아보려면 **View Documentation(**설명서 보기**)**을 클릭합니다.원하는 경우, 더 구체적인 규칙 세부 사항을 보려면 **Rule Documentation(**규칙 설명서**)**을 클릭합니다.

패킷 보기 내 임계값 옵션 설정

침입 이벤트의 패킷 보기에서 임계값 옵션을 설정하여 시간이 지남에 따라 규칙당 생성되는 이벤트의 수를 제어할 수 있습니다. 로컬로 수정할 수 있는 모든 정책에서 임계값 옵션을 설정하거나 로컬로 수정할 수 있는 경우, 현재 정책(즉, 이벤트 생성을 트리거한 정책)에서만 임계값 옵션을 설정할 수 있습니다.

프로시저

단계 **1** 침입 규칙에 의해 생성된 침입 이벤트의 패킷 보기 내에서 Event Information(이벤트 정보) 섹션의 **Actions(**작업**)**를 확장합니다.

단계 **2** **Set Thresholding Options(**임계값 설정 옵션 설정**)**를 확장하고 가능한 다음 두 가지 옵션 중 하나를 선택합니다.

- 현재 **Snort 2** 정책**(<policy_name>)**에서
- 로컬로 작성된 모든 **Snort 2** 정책에서

단계 **3** 설정하려는 임계값 유형을 선택합니다.

- **Limit(**제한**)**를 클릭하여 기간당 지정된 이벤트 인스턴스 수로 알림을 제한합니다.
- 기간당 지정된 각 이벤트 인스턴스의 수에 대해 알림을 제공하려면 **Threshold(**임계값**)**를 클릭합니다.
- 지정된 이벤트 인스턴스의 수 이후 기간당 한 번 알림을 제공하려면 **Both(**모두**)**를 클릭합니다.

단계 **4** 이벤트 인스턴스를 소스 IP 주소로 추적할지 대상 IP 주소로 추적할지 나타내려면 해당 임계값을 클릭합니다.

단계 **5** 임계값으로 사용할 이벤트 인스턴스의 수를 **Count(**카운트**)** 필드에 입력합니다.

단계 **6** 이벤트 인스턴스를 추적할 기간을 지정하는 1~86400의 숫자를 **Seconds(**초**)** 필드에 입력합니다.

단계 **7** 기존 침입 정책에서 이 규칙에 대한 현재 임계값을 재정의하려면 **Override any existing settings for this rule(**이 규칙의 모든 기본 설정 재정의**)** 확인란을 선택합니다.

단계 **8** **Save Thresholding(**임계값 설정 저장**)**을 클릭합니다.

패킷 보기 내 삭제 옵션 설정

억제 옵션을 사용하여 침입 이벤트를 완전히 억제하거나 소스 또는 목적지 IP 주소를 기반으로 억제할 수 있습니다. 로컬로 수정할 수 있는 모든 정책에서 억제 옵션을 설정할 수 있습니다. 또는 현재 정책을 로컬로 수정할 수 있는 경우 현재 정책(즉, 이벤트를 생성한 정책)에서만 억제 옵션을 설정할 수 있습니다.

프로시저

단계 **1** 침입 규칙에 의해 생성된 침입 이벤트의 패킷 보기 내에서 Event Information(이벤트 정보) 섹션의 **Actions(**작업**)**를 확장합니다.

단계 **2** **Set Suppression Options(**억제 옵션 설정**)**를 확장하고 가능한 다음 두 가지 옵션 중 하나를 선택합니다.

- 현재 **Snort 2** 정책**(<policy_name>)**에서
- 로컬로 작성된 모든 **Snort 2** 정책에서

참고 현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어 맞춤형 정책은 수정할 수 있지만 Cisco에서 제공한 기본 정책은 수정할 수 없습니다.

단계 **3** 다음 **Track By(**추적 기준**)** 옵션 중 하나를 선택합니다.

- 지정된 소스 IP 주소에서 시작되는 패킷에 의해 생성된 이벤트를 억제하려면 **Source(**소스**)**를 클릭합니다.
- 지정된 대상 IP 주소로 가는 패킷에 의해 생성된 이벤트를 억제하려면 **Destination(**대상**)**을 클릭합니다.
- 이 이벤트를 트리거한 규칙의 이벤트를 완전히 억제하려면 **Rule(**규칙**)**을 클릭합니다.

단계 **4** 소스 또는 대상 IP 주소로 지정하려는 IP 주소 또는 CIDR 블록/접두사 길이를 **IP address or CIDR block(IP** 주소 또는 **CIDR** 블록**)** 필드에 입력합니다.

단계 **5** **Save Suppression(**억제 저장**)**을 클릭합니다.

관련 항목

Firepower System IP 주소 규칙

프레임 정보 필드

패킷 보기에서 캡처된 프레임에 대한 정보를 볼 **Frame(**프레임**)** 옆에 있는 화살표를 클릭합니다. 패킷 보기에 단일 프레임 또는 다중 프레임이 표시될 수 있습니다. 각 프레임은 개별 네트워크 패킷에 대한 정보를 제공합니다. 예를 들면 태그가 지정된 패킷에서 또는 리어셈블된 TCP 스트림의 패킷에서 여러 프레임을 보게 될 수 있습니다.

Frame n

캡처된 프레임. 여기서 *n*은 단일 프레임 패킷의 경우 1이고 다중 프레임 패킷의 경우 증분 프레임 수입니다. 프레임에서 캡처된 바이트의 수가 프레임 수에 추가됩니다.

Arrival Time

프레임이 캡처된 날짜와 시간.

Time delta from previous captured frame

다중 프레임 패킷의 경우 이전 프레임이 캡처된 이후 경과한 시간.

Time delta from previous displayed frame

다중 프레임 패킷의 경우 이전 프레임이 표시된 이후 경과한 시간.

Time since reference or first frame

다중 프레임 패킷의 경우 첫 번째 프레임이 캡처된 이후 경과한 시간.

Frame Number

증분 프레임 수.

Frame Length

바이트 단위의 프레임 길이.

Capture Length

바이트 단위의 캡처된 프레임 길이.

Frame is marked

프레임이 표시되었는지 여부(true 또는 false).

Protocols in frame

프레임에 포함된 프로토콜.

관련 항목

tag 키워드
TCP 스트림 리어셈블리

데이터 링크 레이어 정보 필드

패킷 보기에서 데이터 링크 레이어 프로토콜(예: **Ethernet II**) 옆에 있는 화살표를 클릭하여 소스 및 대상 호스트의 48비트 MAC(media access control) 주소가 포함된 패킷에 대한 데이터 링크 레이어 정보를 봅니다. 하드웨어 프로토콜에 따라 패킷에 대한 기타 정보도 표시될 수 있습니다.

참고 이 예에서는 이더넷 링크 레이어 정보에 대해 설명합니다. 다른 프로토콜도 나타날 수 있습니다.

패킷 보기는 데이터 링크 레이어에 사용된 프로토콜을 반영합니다. 다음 목록에서는 패킷 보기에 표시될 수 있는 Ethernet II 또는 IEEE 802.3 Ethernet 패킷 정보에 대해 설명합니다.

대상

대상 호스트의 MAC 주소.

참고 이더넷은 멀티캐스트 및 브로드캐스트 주소를 대상 주소로 사용할 수도 있습니다.

소스

소스 호스트의 MAC 주소.

유형

Ethernet II 패킷의 경우 이더넷 프레임으로 캡슐화된 패킷의 유형(예: IPv6 또는 ARP 데이터그램). 이 항목은 Ethernet II 패킷에 대해서만 나타납니다.

길이

IEEE 802.3 Ethernet 패킷의 경우 체크섬을 제외한 패킷의 전체 길이(바이트 단위). 이 항목은 IEEE 802.3 Ethernet 패킷에 대해서만 나타납니다.

네트워크 레이어 정보 보기

프로시저

패킷과 관련된 네트워크 레이어 정보에 대해 자세히 알아보려면 패킷 보기에서 네트워크 레이어 프로토콜(예: **Internet Protocol**) 옆에 있는 화살표를 클릭합니다.

참고 이 예에서는 IP 패킷에 대해 설명합니다. 다른 프로토콜도 나타날 수 있습니다.

IPv4 Network Layer Information(IPv4 네트워크 레이어 정보) 필드

다음 목록에서는 IPv4 패킷에 나타날 수 있는 프로토콜 관련 정보에 대해 설명합니다.

버전

Internet Protocol version number(Internet Protocol 버전 번호).

Header Length(헤더 길이)

헤더의 바이트 수(IP 옵션 포함). 옵션이 없는 IP 헤더의 길이는 20바이트입니다.

Differentiated Services(차별화된 서비스) 필드

전송 호스트가 ECN(Explicit Congestion Notification)을 지원하는 방법을 나타내는 차별화된 서비스에 대한 값.

- `0x0` - ECT(ECN-Capable Transport)를 지원하지 않음
- `0x1` 및 `0x2` - ECT를 지원함
- `0x3` - CE(Congestion Experienced)

Total Length(총 길이)

IP 패킷에서 IP 헤더를 뺀 길이(바이트 단위).

식별

소스 호스트가 전송한 IP 데이터그램을 고유하게 식별하는 값. 이 값은 동일한 데이터그램의 프래그먼트를 추적하는 데 사용됩니다.

플래그

IP 프래그먼트화를 제어하는 값.

Last Fragment 플래그의 값은 데이터그램과 관련된 프래그먼트가 더 있는지 여부를 나타냅니다.

- 0 - 데이터그램에 연결된 프래그먼트가 더 이상 없음
- 1 - 데이터그램에 연결된 프래그먼트가 더 있음

Don't Fragment 플래그의 값은 데이터그램을 프래그먼트화할 수 있는지 여부를 나타냅니다.

- 0 - 데이터그램이 프래그먼트화될 수 있음
- 1 - 데이터그램이 프래그먼트화되어서는 안 됨

Fragment Offset(프래그먼트 오프셋**)**

데이터그램 시작에서부터 프래그먼트 오프셋의 값.

Time to Live(ttl)

데이터그램이 만료되기 전 데이터그램이 라우터 간에 만들 수 있는 나머지 홉(hop)의 수.

프로토콜

IP 데이터그램에서 캡슐화되는 전송 프로토콜(예: ICMP, IGMP, TCP 또는 UDP).

Header Checksum(헤더 체크섬**)**

IP 체크섬이 유효한지를 나타내는 지표. 체크섬이 유효하지 않으면, 데이터그램이 전송 중에 손상되었거나 침입 회피 시도에 사용 중일 수 있습니다.

소스**/**대상

소스(또는 대상) 호스트의 IP 주소나 도메인 이름.

도메인 이름을 표시하려면 IP 주소 확인을 활성화해야 합니다.

주소 또는 도메인 이름을 클릭하여 상황에 맞는 메뉴를 표시한 다음 호스트에서 whois 검색을 수행하려면 **Whois**를, 호스트 정보를 보려면 **View Host Profile(**호스트 프로파일 보기**)**을, 전역 차단 목록 또는 차단 안 함 목록에 주소를 추가하려면 옵션을 선택합니다.

IPv6 네트워크 레이어 정보 필드

다음 목록에서는 IPv6 패킷에 나타날 수 있는 프로토콜 관련 정보에 대해 설명합니다.

Traffic Class(트래픽 클래스**)**

IPv4에 대해 제공되는 차별화된 서비스 기능과 유사한 IPv6 패킷 클래스 또는 우선순위를 식별하기 위한 IPv6 헤더의 실험적인 8비트 필드. 사용되지 않는 경우 이 필드는 0으로 설정됩니다.

Flow Label

기본이 아닌 서비스 품질 또는 실시간 서비스 등의 특수 플로우를 식별하는 선택적인 20비트 IPv6 16진수 값 1~FFFFF. 사용되지 않는 경우 이 필드는 0으로 설정됩니다.

Payload Length(페이로드 길이**)**

IPv6 페이로드에서 옥텟 수를 식별하는 16비트 필드로, IPv6 헤더 뒤에 나오는 모든 패킷(확장 헤더 포함)으로 구성됨.

Next Header(다음 헤더**)**

IPv6 헤더 바로 뒤에 나오는 헤더 유형을 식별하는 8비트 필드로, IPv4 Protocol 필드와 같은 값 사용.

Hop Limit(홉 제한**)**

패킷을 전달하는 각 노드가 1씩 감소하는 8비트 10진수 정수. 감소한 값이 0에 도달하면 패킷이 취소됩니다.

소스

소스 호스트의 128비트 IPv6 주소.

대상

대상 호스트의 128비트 IPv6 주소.

전송 레이어 정보 보기

프로시저

단계 **1** 패킷 보기에서 전송 레이어 프로토콜(예: **TCP**, **UDP** 또는 **ICMP**) 옆의 화살표를 클릭합니다.

단계 **2** 원하는 경우, 패킷 보기의 Packet Information(패킷 정보) 섹션에서 바로 위에 있는 프로토콜에 대한 페이로드의 처음 24바이트를 보려면 **Data**(있는 경우)를 클릭하십시오.

단계 **3** TCP Packet View(TCP 패킷 보기) 필드, 39 페이지, UDP 패킷 보기 필드, 41 페이지 또는 ICMP 패킷 보기 필드, 41 페이지에 설명된 대로 TCP, UDP, ICMP 프로토콜 전송 계층의 콘텐츠를 확인합니다.

참고 이 예에서는 TCP, UDP 및 ICMP 패킷에 대해 설명합니다. 다른 프로토콜도 나타날 수 있습니다.

TCP Packet View(TCP 패킷 보기**)** 필드

이 절에서는 TCP 패킷의 프로토콜 관련 정보에 대해 설명합니다.

소스 포트

시작 애플리케이션 프로토콜을 식별하는 번호.

목적지 포트

수신 애플리케이션 프로토콜을 식별하는 번호.

sequence number(시퀀스 번호**)**

현재 TCP 세그먼트의 첫 번째 바이트에 대한 값으로, TCP 스트림에서 초기 시퀀스 번호로 키가 지정됨.

Next sequence number(다음 시퀀스 번호**)**

응답 패킷에서, 전송할 다음 패킷의 시퀀스 번호.

Acknowledgement number(승인 번호**)**

전에 허용된 데이터의 시퀀스 번호로 키가 지정되는 TCP 승인.

Header Length(헤더 길이**)**

헤더의 바이트 수.

플래그

TCP 세그먼트의 전송 상태를 나타내는 6개 비트.

- `U` - Urgent Pointer가 유효함
- `A` - 승인 번호가 유효함
- `P` - 수신자가 데이터를 푸시해야 함
- `R` - 연결 재설정
- `S` - 새 연결을 시작하도록 시퀀스 번호 동기화
- `F` — 보낸 사람이 데이터 전송을 완료 했습니다.

Window size(창 크기**)**

수신 호스트가 허용하는, 승인되지 않은 데이터의 양(바이트 단위)

체크섬

TCP 체크섬이 유효한지를 나타내는 지표. 체크섬이 유효하지 않으면, 데이터그램이 전송 중에 손상되었거나 회피 시도에 사용 중일 수 있습니다.

Urgent Pointer(긴급 포인터**)**

긴급 데이터가 종료되는 TCP 세그먼트의 위치(있는 경우). U 플래그와 함께 사용됨.

옵션

TCP 옵션의 값(있는 경우)

UDP 패킷 보기 필드

이 절에서는 UDP 패킷의 프로토콜 관련 정보에 대해 설명합니다.

소스 포트

시작 애플리케이션 프로토콜을 식별하는 번호.

목적지 포트

수신 애플리케이션 프로토콜을 식별하는 번호.

길이

UDP 헤더 및 데이터를 결합한 길이.

체크섬

UDP 체크섬이 유효한지를 나타내는 지표. 체크섬이 유효하지 않으면 전송 중 데이터그램이 손상되었을 수 있습니다.

ICMP 패킷 보기 필드

이 절에서는 ICMP 패킷의 프로토콜 관련 정보에 대해 설명합니다.

유형

ICMP 메시지의 유형:

- 0 - 에코 응답
- 3 - 목적지 도달 불가
- 4 - 소스 억제
- 5 - 리디렉션
- 8 - 에코 요청
- 9 - 라우터 알림
- 10 - 라우터 요청
- 11 - 시간 초과
- 12 - 파라미터 문제

- 13 - 타임스탬프 요청
- 14 - 타임스탬프 응답
- 15 - 정보 요청(사용되지 않음)
- 16 - 정보 응답(사용되지 않음)
- 17 - 주소 마스크 요청
- 18 - 주소 마스크 응답

코드

ICMP 메시지 유형에 대해 함께 제공 되는 코드입니다. ICMP 메시지 유형 3, 5, 11, 12에는 RFC 792에 설명된 대로 해당 코드가 있습니다.

체크섬

ICMP 체크섬이 유효한지를 나타내는 지표. 체크섬이 유효하지 않으면 전송 중 데이터그램이 손상되었을 수 있습니다.

패킷 바이트 정보 보기

프로시저

패킷을 구성하는 바이트의 16진수 및 ASCII 버전을 보려면 패킷 보기에서 **Packet Bytes(**패킷 바이트**)** 옆에 있는 화살표를 클릭합니다. 시스템이 트래픽을 해독하면 해독된 패킷 바이트를 볼 수 있습니다.

내부 소스 침입 이벤트

내부 소스에서 들어오는 침입 이벤트는 네트워크의 호스트가 손상되었음을 나타냅니다. 소스 IP 주소가 네트워크에 있는 경우 이 호스트를 조사해야 한다는 신호입니다.

침입 이벤트 통계 보기

Intrusion Event Statistics(침입 이벤트 통계) 페이지에서는 어플라이언스의 현재 상태 및 네트워크에 대해 생성된 침입 이벤트에 대한 빠른 요약을 제공합니다.

페이지에 표시되는 각 IP 주소, 포트, 프로토콜, 이벤트 메시지 등은 링크입니다. 연결된 이벤트 정보를 보려면 링크를 클릭하십시오. 예를 들어 상위 10개 대상 포트 중 하나가 `80 (http)/tcp`인 경우 해당 링크를 클릭하면 기본 침입 이벤트 워크플로의 첫 번째 페이지가 표시되고, 해당 포트를 대상으로 하는 이벤트가 나열됩니다. 현재 시간 범위의 이벤트(및 이벤트를 생성하는 매니지드 디바이스)만 나타납니다. 또한 검토한 것으로 표시한 침입 이벤트는 통계에 계속 나타납니다. 예를 들어 현재의 시

간 범위가 과거 시간이지만 첫 번째 이벤트가 5시간 전에 생성된 경우, **First Event(**첫 번째 이벤트**)** 링크를 클릭하면 시간 범위를 변경하기 전에는 결과 이벤트 페이지에 이벤트가 표시되지 않습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Overview(**개요**)** > **Summary(**요약**)** > **Intrusion Event Statistics(**침입 이벤트 통계**)**을(를) 선택합니다.

단계 **2** 페이지 상단에 있는 두 개의 선택 상자에서 통계를 보려는 영역 및 디바이스를 선택합니다. 침입 이벤트를 수집하는 모든 디바이스에 대한 통계를 보려면 **All Security Zones(**모든 보안 영역**)** 및 **All Devices(**모든 디바이스**)**를 선택합니다.

단계 **3** **Get Statistics(**통계 가져오기**)**를 클릭합니다.

팁 맞춤형 시간 범위의 데이터를 보려면 페이지 오른쪽 위 영역의 링크를 클릭하고 타임 윈도우 변경의 지침을 따르십시오.

호스트 통계 자료

Intrusion Event Statistics(침입 이벤트 통계) 페이지의 Host Statistics(호스트 통계) 절에서는 어플라이언스 자체에 대한 정보를 제공합니다. Secure Firewall Management Center에서 이 섹션은 매니지드 디바이스에 대한 정보도 제공합니다.

이 정보에는 다음 항목이 포함됩니다.

시간

어플라이언스의 현재 시간.

Uptime(실행 시간**)**

어플라이언스 자체를 다시 시작한 이후의 일 수, 시간, 분. Secure Firewall Management Center에서 업타임은 각 매니지드 디바이스가 마지막으로 재부팅된 시간, 로그인한 사용자 수 및 로드 평균도 보여줍니다.

디스크 사용

사용 중인 디스크의 백분율

메모리 사용

사용 중인 시스템 메모리의 백분율

로드 평균

지난 1분, 5분 15분 동안 CPU 큐 프로세스의 평균 수.

이벤트 개요

Intrusion Event Statistics(침입 이벤트 통계) 페이지의 Event Overview(이벤트 개요) 섹션에서는 침입 이벤트 데이터베이스의 정보 개요를 제공합니다.

이러한 통계에는 다음이 포함됩니다.

이벤트

침입 이벤트 데이터베이스의 이벤트 수.

시간 범위 내 이벤트

현재 선택된 시간 범위는 물론 시간 범위에 속하는 데이터베이스의 이벤트 수와 비율도 표시합니다.

첫 번째 이벤트

이벤트 데이터베이스에 있는 첫 번째 이벤트의 이벤트 메시지.

마지막 이벤트

이벤트 데이터베이스에 있는 마지막 이벤트의 이벤트 메시지.

참고 Secure Firewall Management Center에서 침입 이벤트 데이터를 보는 동안 매니지드 디바이스를 선택하면 해당 디바이스에 대 한 Event Overview(이벤트 개요) 섹션이 대신 표시됩니다.

이벤트 통계

Intrusion Event Statistics(침입 이벤트 통계) 페이지의 Event Statistics(이벤트 통계) 섹션에서는 침입 이벤트 데이터베이스의 정보에 대한 좀 더 구체적인 정보를 제공합니다.

이 정보에는 다음에 대한 세부사항이 포함됩니다.

- 상위 10개 이벤트 유형
- 상위 10개 소스 IP 주소
- 상위 10개 대상 IP 주소
- 상위 10개 대상 포트
- 이벤트 수가 가장 많은 프로토콜, 수신 및 송신 보안 영역, 디바이스

참고 다중 도메인 구축에서 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 따라서 리프 도메인은 네트워크 내에서는 고유하지만 다른 리프 도메인과 동일한 IP 주소를 포함할 수 있습니다. 상위 도메인에서 이벤트 통계를 볼 때 반복되는 IP 주소의 여러 인스턴스가 표시될 수 있습니다. 처음에는 이것이 중복된 항목으로 보일 수 있습니다. 하지만 각 IP 주소의 호스트 프로파일 정보로 드릴다운하는 경우, 시스템은 이들이 서로 다른 리프 도메인에 속한다고 표시합니다.

침입 이벤트 성능 그래프 보기

침입 이벤트 성능 페이지에서 특정 기간 동안 Secure Firewall Management Center 또는 매니지드 디바이스에 대한 침입 이벤트의 성능 통계를 보여주는 그래프를 생성할 수 있습니다. 초당 침입 이벤트의 수, 초당 메가비트의 수, 패킷당 평균 바이트 수, Snort에서 검사하지 않은 패킷의 비율, TCP 표준화로 인해 차단된 패킷의 수를 보여주는 그래프를 생성할 수 있습니다. 이러한 그래프는 운영의 마지막 시간, 마지막 날, 마지막 주 또는 마지막 달에 대한 통계를 보여줄 수 있습니다.

참고 새 데이터는 통계 그래프를 위해 5분마다 누적됩니다. 따라서 그래프를 빠르게 다시 로드하는 경우 다음 5분 증가분이 발생할 때까지 데이터가 변경되지 않을 수 있습니다. 각 그래프는 선택한 기간(마지막 달, 주, 날 또는 시간) 동안 표시된 간격(일, 시간 또는 5분) 내 평균 값을 표시합니다. 평균이 1보다 작으면 소수 값이 표시됩니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Overview(**개요**)** > **Summary(**요약**)** > **Intrusion Event Performance(**침입 이벤트 성능**)**을(를) 선택합니다.

단계 **2** 데이터를 보려는 디바이스를 **Select Device(**디바이스 선택**)** 목록에서 선택합니다.

단계 **3** 침입 이벤트 성능 통계 그래프 유형, 45 페이지에 설명된 대로 **Select Graph(s)(**그래프 선택**)** 목록에서 생성할 그래프 유형을 선택합니다.

단계 **4** **Select Time Range(**시간 범위 선택**)** 목록에서 그래프에 사용할 시간 범위를 선택합니다.

단계 **5** **Graph(**그래프**)**를 클릭합니다.

단계 **6** 그래프를 저장하려면 마우스 오른쪽 버튼으로 그래프를 클릭하고 브라우저의 지시에 따라 이미지를 저장합니다.

침입 이벤트 성능 통계 그래프 유형

다음 표에는 사용 가능한 그래프 유형이 나열되어 있습니다. 네트워크 분석 정책 **Inline Mode(**인라인 모드**)** 설정의 영향을 받는 데이터로 채워지는 경우 그래프 유형이 다르게 표시됩니다. **Inline Mode(**인라인 모드**)**가 비활성화되어 있으면 웹 인터페이스에서 별표(*)로 표시된 그래프 유형(아래 열에서 (yes로 표시된 행)은 **Inline Mode(**인라인 모드**)**가 활성화되었다면 시스템에서 수정 또는 삭제했을 트래픽에 대한 데이터로 채워집니다.

표 *7:* 침입 이벤트 성능 그래프 유형

데이터를 생성할 항목	수행해야 할 작업	나타내는 내용	**Inline Mode(**인라인 모드**)**의 영향 적용 여부
평균 바이트/패킷	해당 없음	각 패킷에 포함된 평균 바이트 수입니다.	아니요
TCP 트래픽/패킷에서 표준화된 ECN 플래그	**Explicit Congestion Notification(**명시적 폭주 통지**)**를 활성화하고 **Packet(**패킷**)** 선택	협상 여부와 상관없이 패킷당 기준으로 ECN 플래그가 지워진 패킷의 수입니다.	예
TCP 트래픽/세션에서 표준화된 ECN 플래그	**Explicit Congestion Notification(**명시적 폭주 통지**)**을 활성화하고 **Stream(**스트림**)** 선택	ECN 사용이 협상되지 않은 경우 스트림 단위로 ECN 플래그가 지워진 횟수입니다.	예
이벤트/초	해당 없음	디바이스에서 생성되는 초당 이벤트 수입니다.	아니요
ICMPv4 에코 표준화	**Normalize ICMPv4** 활성화	Echo(Request) 또는 Echo Reply 메시지의 8비트 Code 필드가 지워진 ICMPv4 패킷의 수	예
ICMPv6 에코 정규화	**Normalize ICMPv6** 활성화	Echo(Request) 또는 Echo Reply 메시지의 8비트 Code 필드가 지워진 ICMPv4 패킷의 수입니다.	예
IPv4 DF 플래그 표준화	**Normalize IPv4** 및 **Normalize Don't Fragment Bit** 활성화	IPv4 Flags 헤더 필드의 단일 비트 Don't Fragment 하위 필드가 지워진 IPv4 패킷의 수입니다.	예
IPv4 옵션 표준화	**Normalize IPv4** 활성화	옵션 옥텟이 1(No Operation)로 설정된 IPv4 패킷의 수입니다.	예
IPv4 예약 플래그 표준화	**Normalize IPv4** 및 **Normalize Reserved Bit** 활성화	IPv4 Flags 헤더의 단일 비트 Reserved 하위 필드가 지워진 IPv4 패킷의 수입니다.	예
IPv4 크기 조정 표준화	**Normalize IPv4** 활성화	IP 헤더에 지정된 데이터그램 길이로 잘린, 과도한 길이의 페이로드가 있는 IPv4 패킷의 수입니다.	예
IPv4 TOS 표준화	**Normalize IPv4** 및 **Normalize TOS Bit** 활성화	1바이트 Differentiated Services(DS) 필드(이전의 Type of Service(TOS) 필드)가 지워진 IPv4 패킷의 수입니다.	예
IPv4 TTL 표준화	**Normalize IPv4**, **Maximum TTL** 및 **Reset TTL** 활성화	IPv4 Time to Live 표준화의 수입니다.	예

데이터를 생성할 항목	수행해야 할 작업	나타내는 내용	**Inline Mode(**인라인 모드**)**의 영향 적용 여부
IPv6 옵션 정규화	**Normalize IPv6** 활성화	Hop-by-Hop Options(홉 바이 홉 옵션) 또는 Destination Options(대상 옵션) 확장 헤더의 Option Type(옵션 유형) 필드가 `00`(건너뛰고 계속 처리)으로 설정된 IPv6 패킷의 수입니다.	예
IPv6 TTL 정규화	**Normalize IPv6**, **Minimum TTL** 및 **Reset TTL** 활성화	IPv6 Hop Limit(TTL) 표준화의 수입니다.	예
메가비트/초	해당 없음	디바이스를 통해 전달되는 트래픽의 초당 메가비트 수입니다.	아니요
MSS 표준화에 맞게 크기 조정된 패킷	**Trim Data to MSS(MSS**로 데이터 절감**)** 활성화	페이로드가 TCP Data 필드보다 길어서 Maximum Segment Size로 잘리는 패킷의 수입니다.	예
TCP 창 표준화에 맞게 크기 조정된 패킷	**Trim Data to Window** 활성화	TCP Data 필드가 수신 호스트의 TCP 창에 맞게 잘리는 패킷의 수입니다.	예
삭제된 패킷 비율	해당 없음	선택한 모든 디바이스에서 검사하지 않은 패킷의 평균 비율입니다. 예를 들어 디바이스를 2개 선택하고 평균이 50%이면, 한 디바이스는 삭제율이 90%이고 나머지는 삭제율이 10%라는 뜻일 수 있습니다. 또는 두 디바이스 모두 삭제율이 50%임을 나타낼 수도 있습니다. 그래프는 단일 디바이스를 선택할 경우의 총 삭제 %만 나타냅니다.	아니요
데이터 스트립된 RST 패킷 표준화	**Remove Data on RST(RST** 데이터 제거**)** 활성화	TCP 재설정(RST) 패킷에서 데이터가 삭제된 패킷의 수입니다.	예
데이터 스트립된 SYN 패킷 표준화	**Remove Data on SYN(SYN** 데이터 제거**)** 활성화	TCP 운영체제가 Mac OS가 아닐 때 SYN 패킷에서 데이터가 제거된 패킷의 수입니다.	예
TCP 헤더 패딩 표준화	**Normalize/Clear Option Padding Bytes(**옵션 패딩 바이트 표준화/지우기**)** 활성화	옵션 패딩 바이트가 0으로 설정되었을 때 TCP 패킷의 수입니다.	예
TCP 옵션 없음 표준화	**Allow These TCP Options**를 활성화하고 `any` 이외의 옵션으로 설정	Time Stamp 옵션이 제거된 패킷의 수입니다.	예
TCP NS 플래그 표준화	**Explicit Congestion Notification(**명시적 폭주 통지**)**을 활성화하고 **Packet(**패킷**)** 선택	ECN Nonce Sum(NS) 옵션 표준화의 수입니다.	예

데이터를 생성할 항목	수행해야 할 작업	나타내는 내용	**Inline Mode(**인라인 모드**)**의 영향 적용 여부
TCP 옵션 표준화	**Allow These TCP Options**를 활성화하고 `any` 이외의 옵션으로 설정	옵션 필드가 No Operation(TCP Option 1)으로 설정된 옵션(MSS, Window Scale, Time Stamp 및 명시적으로 허용된 옵션 제외)의 수입니다.	예
표준화에 의해 차단된 TCP 패킷	**Normalize TCP Payload** 활성화(세그먼트 리어셈블리가 실패함)	TCP 세그먼트를 제대로 리어셈블할 수 없기 때문에 삭제된 패킷의 수입니다.	예
TCP 예약 플래그 표준화	**Normalize/Clear Reserved Bits(**예약 비트 표준화/지우기**)** 활성화	Reserved 비트가 지워진 TCP 패킷의 수입니다.	예
TCP 세그먼트 리어셈블리 표준화	**Normalize TCP Payload** 활성화(세그먼트 리어셈블리가 성공함)	재전송된 데이터의 일관성을 보장하기 위해 TCP Data 필드가 표준화된 패킷의 수(제대로 리어셈블할 수 없는 세그먼트는 삭제됨)입니다.	예
TCP SYN 옵션 표준화	**Allow These TCP Options**를 활성화하고 `any` 이외의 옵션으로 설정	SYN 제어 비트가 설정되지 않아 Maximum Segment Size or Window Scale 옵션이 No Operation(TCP Option 1)으로 설정된 옵션의 수입니다.	예
TCP 타임스탬프 ECR 표준화	**Allow These TCP Options**를 활성화하고 `any` 이외의 옵션으로 설정	Acknowledgment(수신 확인, ACK) 제어 비트가 설정되지 않아 Time Stamp Echo Reply(타임 스탬프 에코 응답, TSecr) 옵션 필드가 지워진 패킷의 수입니다.	예
TCP 긴급 포인터 표준화	**Normalize Urgent Pointer(**긴급 포인터 표준화**)** 활성화	2바이트 TCP 헤더 Urgent Pointer(긴급 포인터) 필드가 페이로드 길이보다 긴 패킷 및 페이로드 길이로 설정된 패킷의 수입니다.	예
총 차단된 패킷	**Inline Mode** 또는 **Drop when Inline** 설정	규칙, 디코더 및 전처리기 삭제를 비롯한 삭제된 패킷의 총 수입니다.	아니요
총 삽입된 패킷	**Inline Mode** 설정	재전송되기 전에 크기가 조정된 패킷의 수입니다.	아니요
총 TCP 필터링된 패킷	TCP 스트림 전처리 설정	TCP 포트 필터링 때문에 스트림에서 건너뛴 패킷의 수입니다.	아니요
총 UDP 필터링된 패킷	UDP 스트림 전처리 설정	UDP 포트 필터링 때문에 스트림에서 건너뛴 패킷의 수입니다.	아니요

데이터를 생성할 항목	수행해야 할 작업	나타내는 내용	**Inline Mode(**인라인 모드**)**의 영향 적용 여부
긴급 플래그 지워진 표준화	**Clear URG if Urgent Pointer is Not Set(**긴급 포인터가 설정되지 않은 경우 **URG** 지우기**)** 활성화	긴급 포인터가 설정되지 않아서 TCP 헤더 URG 제어 비트가 지워진 패킷의 수입니다.	예
긴급 포인터 및 긴급 플래그 지워진 표준화	**Clear Urgent Pointer/URG on Empty Payload(**빈 페이로드의 긴급 포인터**/URG** 지우기**)** 활성화	페이로드가 없어 TCP 헤더 Urgent Pointer(긴급 포인터) 필드 및 URG 제어 비트가 지워진 패킷의 수입니다.	예
긴급 포인터 지워진 표준화	**Clear Urgent Pointer if URG=0(URG=0**인 경우 긴급 포인터 지우기**)** 활성화	Urgent(URG) 제어 비트가 설정되지 않아 16비트 TCP 헤더 Urgent Pointer(긴급 포인터) 필드가 지워진 패킷의 수입니다.	예

관련 항목

- 인라인 정상화 전처리기
- 인라인 구축의 전처리기 트래픽 수정
- 인라인 구축의 삭제 작업

침입 이벤트 그래프 보기

Firepower System은 시간에 따른 침입 이벤트 추세를 보여주는 그래프를 제공합니다. 하나 또는 모든 매니지드 디바이스에 대해 지난 1시간부터 지난 달까지의 시간 동안의 침입 이벤트 그래프를 생성할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Overview(**개요**)** > **Summary(**요약**)** > **Intrusion Event Graphs(**침입 이벤트 그래프**)**을(를) 선택합니다.

단계 **2** **Select Device(**디바이스 선택**)** 아래에서 **all**을 선택하여 모든 디바이스를 포함하거나 그래프에 포함할 특정 디바이스를 선택합니다.

단계 **3** **Select Graph(s)(**그래프 선택**)**에서 생성할 그래프 유형을 선택합니다.

- 상위 10개 대상 포트
- 상위 10개 소스 IP 주소
- 상위 10개 이벤트 메시지

단계 **4** **Select Time Range(**시간 범위 선택**)**에서 그래프의 시간 범위를 선택합니다.

- 마지막 시간
- 지난 1일
- 지난주
- 지난달

단계 **5** **Graph(**그래프**)**를 클릭합니다.

침입 이벤트 기록

기능	버전	세부 사항	최소 Threat Defense
IPS 이벤트 데이터스토어 교체	7.1	침입 인시던트, 침입 이벤트 클립보드 및 기본 사용자 지정 테이블(침입 이벤트 열 - **Intrusion Events with Source Criticality(**소스 중요도가 있는 침입 이벤트**)** 및 **Intrusion Events with Destination Criticality(**대상 중요도가 있는 침입 이벤트**)** 사용)은 더 이상 사용되지 않습니다. 더 이상 **Copy(**복사**)** 및 **Copy All(**모두 복사**)** 버튼을 사용하여 클립보드에 이벤트를 추가할 수 없습니다. 사용되지 않는 페이지: • **Analysis(**분석**) > Intrusions(**침입**) > Clipboard(**클립보드**)** • **Analysis(**분석**) > Intrusions(**침입**) > Incidents(**인시던트**)** • 기본 침입 이벤트 테이블에 **Source Host Criticality(**소스 호스트 중요도**)**와 **Destination Host Criticality(**대상 호스트 중요도**)**의 두 필드가 새로 추가되었습니다. 지원되는 플랫폼: Secure Firewall Management Center	모든
시스템 로그의 연결 이벤트 통합 식별자	6.4.0.4	연결 및 시스템 로그 필드는 함께 연결 이벤트를 개별적으로 식별하며, 침입 이벤트의 경우에는 시스템 로그에 디바이스 UUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터로 표시됩니다.	모든
이제 IntrusionPolicy 필드가 시스템 로그에 포함됩니다.	6.4.0	침입 이벤트 시스템 로그는 이제 이벤트를 트리거한 침입 정책을 표시합니다.	모든
새 침입 이벤트 검색 필드: CVE ID	6.4.0	이제 MITRE의 일반 취약성 및 노출 식별 번호로 검색할 수 있습니다. 수정된 화면: **Analysis(**분석**) > Intrusions(**침입**) > Events(**이벤트**) > Edit Search(**검색 편집**)** 지원되는 플랫폼: 전체.	모든