통합 이벤트

다음 항목에서는 통합 이벤트를 사용하는 방법을 설명합니다.

통합 이벤트 정보

통합 이벤트는 여러 유형의 방화벽 이벤트(연결, 침입, 파일, 악성코드 및 일부 보안 관련 연결 이벤트)를 단일 화면 보기로 제공합니다. 서로 연결된 이벤트는 테이블에 함께 누적되어 보안 이벤트에 대한 통합 보기와 추가 컨텍스트를 제공합니다. 통합 이벤트 테이블에 침입 이벤트가 있을 경우 침입 이벤트를 클릭하여 연결된 연결 이벤트를 강조 표시합니다. 연결 이벤트를 침입 이벤트와 상호 전환하면 여러 이벤트 보기 간에 전환하지 않고도 네트워크 문제를 이해하고 더 잘 해결할 수 있습니다.

통합 이벤트 테이블은 수준 높은 사용자 맞춤화가 가능합니다. 이벤트 보기에 표시되는 정보를 세부적으로 조정할 수 있도록 사용자 지정 필터를 생성하고 적용할 수 있습니다. 통합 이벤트 보기에는 특정 요구에 맞게 자주 사용하는 사용자 지정 필터를 저장한 다음, 저장된 필터를 빠르게 로드할 수 있는 옵션도 있습니다. 또한 열을 추가 또는 제거하여 사용자 지정 이벤트 보기 테이블을 만들거나, 열을 고정하거나, 열을 끌어서 순서를 변경할 수 있습니다.

통합 이벤트 테이블의 **Live View(**라이브 보기**)** 옵션을 사용하면 방화벽 이벤트를 실시간으로 확인하고 네트워크 활동을 모니터링할 수 있습니다. 예를 들어, 방화벽 관리자는 정책을 변경한 후 이벤트

업데이트를 실시간으로 확인하면 정책 변경 사항이 네트워크에 올바르게 적용되었는지 확인할 수 있습니다.

통합 이벤트 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모두

사용자 역할

- 관리자
- 보안 분석가

통합 이벤트 보기로 작업

여러 이벤트 보기 간에 전환할 필요 없이 단일 테이블에서 다양한 방화벽 이벤트 유형을 보고 작업할 수 있습니다.

이 보기를 사용하여 다음을 수행합니다.

- 통합 보기에서 서로 다른 이벤트 유형 간의 관계를 찾습니다.
- 실시간으로 정책 변경의 영향을 확인하십시오.

시작하기 전에

이 작업을 수행하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Unified Events(**통합 이벤트**)**를 선택합니다.

단계 **2** 시간 범위(고정 또는 슬라이딩)를 선택합니다. 자세한 내용은 통합 이벤트 보기에서 시간 범위 설정을 참고하십시오.

단계 **3** Secure Network Analytics 어플라이언스에 원격으로 이벤트를 저장하고 데이터 소스를 변경해야 하는 충분한 이유가 있는 경우 데이터 소스를 선택합니다. Secure Network Analytics 어플라이언스에 저장된 연결 이벤트를 사용하여 Secure Firewall Management Center에서 작업에서 자세한 정보를 참고하십시오.

단계 **4** 통합 이벤트 보기에 처음 표시되는 방대한 방화벽 이벤트 목록을 필터링할 수 있어 네트워크의 이벤트를 상황별로 더욱 상세히 파악할 수 있습니다. 자세한 내용은 통합 이벤트 보기의 필터를 참고하십시오.

단계 **5** 추가 옵션을 선택합니다.

수행할 작업 ...	수행해야 할 작업
열 맞춤화	• 열을 추가하거나 제거합니다. 열 선택기(▥)를 클릭하고 열을 선택합니다. 일부 필드의 값은 이벤트 유형에 따라 달라집니다. 각 필드 옆에 나타나는 다음 아이콘은 해당 이벤트 유형을 나타냅니다. • 연결 이벤트 ⇆ • 보안 관련 연결 이벤트(⇆) • 침입 이벤트 👽 • 파일 이벤트 🗋 • 악성코드 이벤트 🐞 열 세트 필터링 옵션 옆의 이벤트 아이콘을 클릭하여 선택한 이벤트 유형에 따라 이벤트 필드 목록을 필터링합니다. 참고 많은 열을 포함하면 성능이 저하될 수 있습니다. 이벤트 행을 확장하여 이벤트 세부 사항을 확인하여 숨겨진 열에 대한 데이터를 볼 수 있습니다. • 열 순서를 재지정합니다. 열 제목을 끌어다 놓습니다. • 스크롤하지 않도록 열을 테이블의 왼쪽 또는 오른쪽에 고정합니다. 열을 테이블의 왼쪽이나 오른쪽으로 끌어옵니다. 또는 열 제목을 고정된 영역으로 끌어서 놓습니다. 열 고정을 해제하려면 고정된 영역 밖으로 열을 드래그합니다. • 열 크기를 조정합니다. • 열을 기본 설정으로 되돌립니다. • 열 집합을 저장합니다. 자세한 내용은 통합 이벤트 보기에서 열 집합 저장 항목을 참고하십시오. 데이터는 항상 시간을 기준으로 정렬되며 가장 최근 이벤트가 맨 위에 옵니다.

수행할 작업 ...	수행해야 할 작업
관련 이벤트 식별	이 이벤트와 관련된 다른 이벤트를 강조 표시하려면 행을 클릭합니다. 필요한 경우 이벤트를 필터링하여 작은 이벤트 집합을 표시합니다. 참고 연결의 이니시에이터가 악성코드 파일의 발신자와 반드시 같을 필요는 없습니다. 소스 또는 대상 **IP** 필터를 통해 통합 이벤트 보기를 필터링하여 연결 이벤트에 연결된 파일 또는 악성코드 이벤트를 검색합니다.
이벤트 세부 정보 보기	행의 왼쪽 끝에서 >(확장) 아이콘을 클릭합니다. 표시할 데이터가 없는 필드는 이벤트 세부 사항에 포함되지 않습니다. 팁 또는 이벤트 행을 두 번 클릭하여 **Event Details(**이벤트 세부정보**)** 창을 볼 수 있습니다. **Event Details(**이벤트 세부 정보**)** 창이 열려 있으면 테이블에서 이벤트 행을 클릭하여 해당 이벤트의 세부 정보를 로드합니다.
패킷 트레이서를 사용하여 이벤트 문제 해결	**1.** 패킷 트레이스를 실행할 행에 인접한 줄임표 아이콘을 클릭합니다. **2.** 이벤트의 소스 및 대상 주소 지정, 프로토콜 특성을 기반으로 패킷 트레이서 툴에서 패킷을 시뮬레이션하려면 **Open in Packet Tracer(**패킷 트레이서에서 열기**)**를 선택합니다. 시뮬레이션된 패킷을 추적하고 추적 결과를 사용하여 보안 이벤트의 문제를 해결합니다. 패킷 트레이서 툴을 사용하는 방법에 대한 자세한 내용은 패킷 트레이서 사용의 내용을 참조하십시오.
실시간으로 이벤트 보기	**Go Live(**라이브 상태로 전환**)**를 클릭합니다. 자세한 내용은 통합 이벤트 보기에서 이벤트의 라이브 보기를 참고하십시오. 이벤트가 너무 빨리 스트리밍되면 필터 기준을 입력합니다.
외부 리소스에 대한 교차 실행	테이블 셀에서 줄임표를 클릭하여 해당 셀 값에 대해 사용 가능한 옵션을 확인합니다(있는 경우). 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사를 참고하십시오.
여러 통합 이벤트 뷰어 탭/창 열기	• 여러 브라우저 탭 또는 창을 사용하여 통합 이벤트 뷰어의 여러 보기를 표시할 수 있습니다. • 각 새 탭 또는 창에는 가장 최근에 수정된 탭/창의 특성이 있습니다. • 열려 있는 탭/창을 템플릿으로 만들려면 템플릿을 약간 변경합니다. • 시스템은 여러 탭의 쿼리를 순차적으로 처리합니다. • 보기(예: 수신 이벤트 비율이 높을 때의 복잡한 쿼리 또는 라이브 보기 모드에서 보기)에 따라 약 4개 이상의 탭을 동시에 열면 성능이 저하될 수 있습니다.

수행할 작업 ...	수행해야 할 작업
검색 저장	사용자 지정 검색을 즐겨찾기로 저장하고 나중에 빠르게 로드할 수 있습니다. 자세한 내용은 통합 이벤트 보기에서 검색 저장을 참고하십시오.
쿼리 결과 즐겨찾기 추가 또는 공유	브라우저 창에서 URL을 즐겨찾기에 추가하거나 복사하여 붙여 넣습니다. • URL은 슬라이딩 시간 범위를 사용하는 경우 나중에 다른 이벤트를 검색합니다. • URL은 열 가시성, 크기 및 순서, 실시간 스트리밍 설정을 캡처하지 않습니다.

통합 이벤트 보기에서 시간 범위 설정

특정 기간의 방화벽 이벤트를 보려면 통합 이벤트 보기에서 시간 범위를 구성합니다. 시간 범위를 변경하면 통합 이벤트 보기가 자동으로 새로 고침되어 변경 사항을 반영합니다.

선택하는 시간 범위는 이벤트 보기의 다른 테이블에 적용되지 않습니다. 예를 들어, 연결 이벤트를 볼 때 선택하는 시간 범위는 통합 이벤트 보기에 적용되지 않으며 그 반대의 경우도 마찬가지입니다.

중요 기간이 연결 이벤트의 보존 기간을 초과하여 다시 연장되는 경우 **Analysis(분석)** > **Connections(연결)** > **Security-Related Connection Events(보안 관련 연결 이벤트)** 아래의 테이블에서 Security-Related Connection(보안 관련 연결) 이벤트를 찾습니다.

시작하기 전에

이 작업을 수행하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

프로시저

단계 **1** **Analysis(분석)** > **Unified Events(통합 이벤트)**를 선택합니다.

기본적으로, 통합 이벤트 보기에서는 지난 1시간의 이벤트가 표시됩니다.

단계 **2** 현재 시간 범위를 클릭합니다.

단계 **3** 다음 중 하나를 선택합니다.

- 고정 시간 범위에 대한 이벤트를 확인하려면 **Fixed Time Range(고정 시간 범위)**를 클릭하고 **Start time(시작 시간)** 및 **End time(종료 시간)**을 선택합니다.

  팁 **Now(지금)**를 클릭하여 현재 시간을 **End time(종료 시간)**으로 빠르게 설정합니다.

- 지정한 길이의 슬라이딩 기본 시간대를 구성하려면 **Sliding Time Range(**슬라이딩 시간 범위**)**를 클릭합니다.

  어플라이언스는 특정 시작 시간(예: 1시간 전)부터 현재까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 새로고침하면 시간대가 슬라이딩하므로 항상 지난 1시간의 이벤트가 표시됩니다.

단계 **4** **Apply(**적용**)**를 클릭합니다.

통합 이벤트 보기에서 이벤트의 라이브 보기

수동으로 이벤트 보기를 새로 고치지 않고 방화벽 이벤트를 실시간으로 표시하도록 통합 이벤트 보기를 구성합니다. 라이브 보기 모드에서는 네트워크에서 보안 이벤트가 발생할 때 이벤트 로그가 실시간으로 표시되므로, 문제를 보다 쉽게 해결할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Unified Events(**통합 이벤트**)**를 선택합니다.

기본적으로, 통합 이벤트 보기에서는 지난 1시간의 이벤트가 표시됩니다.

단계 **2** 라이브 이벤트 업데이트를 보려면 **Go Live(**라이브 상태로 전환**)**를 클릭합니다.

새 이벤트가 이벤트 테이블 상단에 채워집니다. 시간 범위 섹션에는 통합 이벤트 보기가 라이브 상태로 유지되는 기간을 알리는 타이머가 표시됩니다.

다음에 수행할 작업

라이브 보기 모드를 종료하려면 **Live(**라이브**)**를 클릭합니다.

통합 이벤트 보기의 필터

통합 이벤트 보기에는 지난 1시간 동안의 여러 방화벽 이벤트 유형이 표시됩니다. 통합 이벤트의 기본 보기를 필터링하여 네트워크의 활동에 대한 보다 세분화된 상황별 정보를 확인할 수 있습니다. 필터는 포함 필터 기준뿐 아니라 예외도 지원합니다.

필터를 사용하면 중요한 정보에 빠르게 액세스할 수 있습니다. 예를 들어, 방화벽 관리자가 일부 사용자에게 특정 애플리케이션 액세스를 허용하거나 거부하려면 방화벽 로그를 스캔하도록 사용자 검색 기준을 설정할 수 있습니다. 이벤트 보기에는 검색 기준과 일치하는 이벤트 로그가 표시됩니다.

시작하기 전에

다음 작업을 수행하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Unified Events(**통합 이벤트**)**를 선택합니다.

단계 **2** 필터 기준 입력:

- 필터 기준을 수동으로 입력하려면 검색 텍스트 필드에 정확한 기준을 입력하거나 드롭다운 목록에서 기준을 선택합니다. 그런 다음 필터 기준 값을 제공합니다. 값을 입력하는 동안 가능할 때마다 드롭다운 목록에 제안 메시지가 나타납니다.
- 테이블의 이벤트에 대한 셀의 점을 클릭하고 필터 기준에서 해당 값을 포함하거나 제외할 옵션을 선택합니다.

  팁
  - 포함 필터 기준을 빠르게 추가하려면 **Ctrl+click**(Windows) 또는 **Command-click**(Mac) 키를 사용합니다.
  - 예외 필터 기준을 빠르게 추가하려면 **Ctrl+click**(Windows) 또는 **Command-click**(Mac) 키를 사용합니다.

- 필터 조건을 구체화하십시오. 와일드 카드 및 검색 동작에 대한 중요한 정보는 이벤트 검색의 내용을 참조하십시오.
- 값 앞의 값 필드에 연산자(예: <, >, ! 등)를 포함합니다. 예를 들어, **Action(**작업**)** 필드에 `!Allow(허용)`를 입력하여 Allow(허용) 이외의 작업이 있는 모든 이벤트를 찾습니다.

단계 **3** 검색을 수행합니다.

팁 **Ctrl+Enter**(Windows) 또는 **Command-Enter**(Mac) 키 명령을 사용하여 검색을 시작할 수 있습니다.

통합된 이벤트 보기의 이벤트는 표시된 열이 모두 동일한 값을 가질 때 집계되지 않습니다. 필터 기준과 일치하는 모든 이벤트가 개별적으로 나열됩니다.

다음에 수행할 작업

사용자 지정 필터를 저장하려면 통합 이벤트 보기에서 검색 저장 항목을 참고하십시오.

통합 이벤트 보기에서 검색 저장

시작하기 전에

검색을 저장하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Unified Events(**통합 이벤트**)**를 선택합니다.

단계 **2** 통합 이벤트 보기의 필터 항목에 설명된 대로 검색 기준을 설정합니다.

단계 **3** 검색 텍스트 상자에서 즐겨찾기 검색(☆) 아이콘을 클릭합니다.

단계 **4** 다음 중 하나를 수행합니다.

- 새 검색을 저장하려면 검색 이름을 지정하고 **Save as new(**새 검색으로 저장**)**를 클릭합니다.
- 저장된 검색을 덮어쓰려면 덮어쓸 저장된 검색에서 **Edit(**수정**)**를 클릭하고 **Overwrite(**덮어쓰기**)**를 클릭합니다.

다음에 수행할 작업

저장된 검색을 로드하려면 통합 이벤트 보기에 저장된 검색 로드 항목을 참고하십시오.

통합 이벤트 보기에 저장된 검색 로드

시작하기 전에

- 이 작업을 수행하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.
- 통합 이벤트 보기에서 검색 저장 항목에 설명된 대로 저장된 검색을 설정합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Unified Events(**통합 이벤트**)**를 선택합니다.

단계 **2** 검색 텍스트 상자에서 즐겨찾기 검색(☆) 아이콘을 클릭합니다.

단계 **3** 로드하려는 저장된 검색을 클릭합니다.

통합 이벤트 보기에서 열 집합 저장

시작하기 전에

열 집합을 저장하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Unified Events(**통합 이벤트**)**를 선택합니다.

단계 **2** 열 선택기 아이콘(▥)을 클릭하고 저장할 열 집합을 선택합니다.

단계 **3** **Favorite column sets(**즐겨찾기 열 집합**)**(☆) 아이콘을 클릭합니다.

단계 **4** 다음 중 하나를 수행합니다.

- 새 열 집합을 저장하려면 열 집합 이름을 지정하고 **Save as new(**새 이름으로 저장**)**를 클릭합니다.
- 즐겨찾는 열 집합을 덮어쓰려면 덮어쓸 열 집합에서 **Edit(**수정**)**⋮를 클릭하고 **Overwrite(**덮어쓰기**)**를 클릭합니다.

다음에 수행할 작업

저장된 열 집합을 로드하려면 통합 이벤트 보기에서 저장된 열 집합 로드 항목을 참고하십시오.

통합 이벤트 보기에서 저장된 열 집합 로드

시작하기 전에

- 이 작업을 수행하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.
- 통합 이벤트 보기에서 열 집합 저장 항목에 설명된 대로 즐겨찾기 열 집합을 저장합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Unified Events(**통합 이벤트**)**를 선택합니다.

단계 **2** 열 선택기 아이콘(▥)을 클릭합니다.

단계 **3** **Favorite column sets(**즐겨찾기 열 집합**)** 아이콘(☆)을 클릭합니다.

단계 **4** 로드할 열 집합을 클릭합니다.

통합 이벤트 보기 열 설명

일부 필드의 값은 이벤트 유형에 따라 달라집니다. 기본 필드의 필드 통신은 다음과 같습니다.

통합 이벤트 뷰어 필드 이름	연결 또는 보안 인텔리전스 이벤트 필드 이름	침입 이벤트 필드 이름	파일 이벤트 필드 이름	악성코드 이벤트 필드 이름
시간	첫 번째 패킷 아래 참고를 참조하십시오.	시간	시간	시간
이벤트 유형	--	--	--	--
조치	작업	인라인 결과	작업	작업
이유	이유	이유	(해당 없음)	(해당 없음)
소스 **IP**	초기자 IP	소스 IP	송신 IP	송신 IP
목적지 **IP**	응답기 IP	목적지 IP	수신 IP	수신 IP
소스 포트/**ICMP** 유형	소스 포트	소스 포트	송신 포트	송신 포트
대상 포트/**ICMP** 유형	목적지 포트	목적지 포트	수신 포트	수신 포트
웹 애플리케이션	웹 애플리케이션	웹 애플리케이션	웹 애플리케이션	웹 애플리케이션
규칙	액세스 제어 규칙	액세스 제어 규칙	(해당 없음)	(해당 없음)
정책	액세스 제어 정책	침입 정책	파일 정책	파일 정책
디바이스	디바이스	디바이스	디바이스	디바이스

모든 이벤트 필드와 해당 필드를 보려면 열 선택기(▮▮) 아이콘을 클릭합니다.

필드 설명은 다음 항목을 참조하십시오.

- 연결 및 보안 관련 연결 이벤트 필드
- 침입 이벤트 필드
- 파일 및 악성코드 이벤트 필드

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

참고 연결 시작시 로깅을 활성화하지 않은 경우에도 시스템은 이 값을 통합 이벤트 뷰어의 시간 필드로 사용합니다. 연결 시작 및 종료시 연결 이벤트가 기록되었는지 확인하려면 이벤트의 행을 확장하여 세부 정보를 확인합니다. 연결의 양쪽 끝에 기록된 경우 **Last Packet(**마지막 패킷**)** 필드가 표시됩니다.

통합 이벤트 기록

기능	버전	세부 사항
통합 이벤트 보기용 패킷 트레이서	7.4.1	새로 Unified Event Viewer(통합 이벤트 보기) 페이지에서 패킷 트레이서를 열어 보안 이벤트의 문제를 해결할 수 있습니다. 패킷 추적을 실행할 이벤트 옆에 있는 생략부호 아이콘(확장)을 클릭하고 **Open in Packet Tracer(**패킷 트레이서에서 열기**)**를 클릭합니다.
통합 이벤트 보기 개선 사항	7.4.1	필터 창과 열 집합 및 검색 저장 기능이 개선되었습니다.
즐겨찾기 검색 저장	7.4.1	열 집합 및 검색을 즐겨찾기로 저장하고 나중에 빠르게 실행할 수 있습니다.
통합 이벤트 뷰어	7.4.1	연결, 보안 인텔리전스 포함), 침입, 파일 및 악성 코드 등 여러 이벤트 유형이 포함된 단일 테이블을 보고 작업합니다. 새 페이지/수정 페이지: 분석 > 통합 이벤트 아래 새 페이지 지원되는 플랫폼: management center