FTD 대시보드

FTD 대시보드 정보

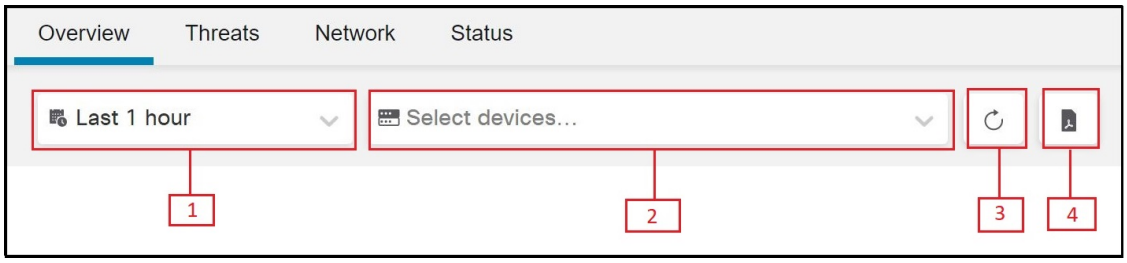
FTD 대시보드에서는 모든 CDO 관리 위협 방어 장치에서 수집 및 생성된 이벤트 데이터를 비롯하여 상태를 한눈에 볼 수 있습니다.

이 대시보드를 사용하여 디바이스 상태 및 구축에 있는 디바이스의 전반적인 상태와 관련된 종합적인 정보를 볼 수 있습니다. FTD 대시보드가 제공하는 정보는 시스템에서 디바이스의 라이선스, 구성 및 구축 방법에 따라 달라집니다. FTD 대시보드에는 모든 CDO 매니지드 위협 방어 디바이스에 대한 데이터가 표시되지만 디바이스 기반 데이터를 필터링하도록 선택할 수 있습니다. 특정 시간 범위에 대해 표시할 시간 범위를 선택할 수도 있습니다.

이 대시보드는 탭을 사용하여 사전 정의된 위젯을 표시합니다. 위젯은 시스템의 여러 측면을 파악할 수 있는 자체 포함형 소형 구성 요소입니다. 예를 들어 Network Activity(네트워크 활동) 위젯은 모든 연결, 악성코드 및 침입 이벤트에 대한 정보를 표시하는 이벤트 그래프를 표시합니다. 대시보드의 위젯은 미리 정의되어 있으며 사용자 지정할 수 없습니다. 이 대시보드는 CDO 테넌트에 액세스할 수 있는 모든 CDO 사용자에게 표시됩니다.

- 대시보드에는 기록 이벤트에 대한 이벤트 통계가 표시되지 않습니다.
- 집계 서비스는 5분마다 집계하는 이벤트를 일괄 처리하므로, 이벤트가 집계된 시간과 통계가 표시되는 시간 사이에 5분의 레이턴시를 예상할 수 있습니다.

그림 *1: FTD* 대시보드



숫자	설명
1	시간 범위를 마지막 시간 단위로 짧게, 또는 마지막 연도 단위로 길게 반영하도록 구성할 수 있습니다. 시간 범위를 변경하면 위젯은 새 시간 범위를 반영하도록 이벤트 데이터를 자동으로 업데이트합니다.
2	선택한 디바이스를 기준으로 이벤트 데이터를 필터링할 수 있습니다. 디바이스를 선택하지 않으면 사용 가능한 모든 이벤트 데이터가 위젯에 표시됩니다.
3	이벤트 데이터 쿼리 다시 시작
4	이벤트 데이터를 PDF 출력 형식으로 표시합니다. 이 PDF의 복사본을 로컬 컴퓨터에 다운로드하거나 저장할 수 있습니다.

FTD 대시보드 보기

CDO 메뉴에서 분석 > **FTD** 대시보드를 선택하여 **FTD Dashboard(FTD** 대시보드**)**를 확인합니다.

기본적으로 테넌트의 홈 페이지에서 **Overview(**개요**)** 탭이 표시됩니다.

대시보드에는 각 탭(Threat(위협), Network(네트워크), Application and Users(애플리케이션 및 사용자), Status(상태) 탭) 아래에 위젯이 나열되어 있습니다.

다음 표에는 각 탭에서 사용 가능한 위젯이 나열되어 있습니다.

탭의 이름	사용 가능한 위젯
개요	사용 가능한 모든 위젯

탭의 이름	사용 가능한 위젯
위협	• 상위 침입 규칙 • 상위 침입 공격자 • 상위 침입 대상 • 상위 악성코드 시그니처 • 상위 악성코드 발신자 • 상위 악성코드 수신자 • 속성별 악성코드 이벤트
네트워크	• 네트워크 활동 • 이벤트 활동 • 액세스 제어 작업 • 상위 액세스 제어 정책 • 상위 액세스 제어 규칙 • 상위 디바이스 • 최상위 사용자
상태	• 비정상 디바이스 • 상위 로드된 디바이스

FTD 대시보드 위젯

FTD 대시보드는 현재 시스템 상태를 한눈에 볼 수 있는 미리 정의된 위젯을 표시합니다. 볼 수 있는 항목은 다음과 같습니다.

- threat defense 디바이스에서 관리하는 FMC에서 수집하고 생성한 이벤트에 대한 데이터입니다.
- 구축에 있는 디바이스의 상태 및 전체 상태에 대한 정보입니다.

상위 침입 규칙 위젯

상위 침입 규칙 위젯은 지정된 시간 범위에 발생한 침입 이벤트의 카운트를 우선순위별로 표시합니다. 이러한 카운트에는 삭제된 패킷 및 서로 다른 영향과 함께 침입 이벤트에 대한 통계도 포함됩니다. 생성된 목록은 스크롤할 수 있습니다.

상위 침입 공격자 위젯

상위 침입 공격자 위젯은 모니터링되는 네트워크에서 상위 공격 호스트 IP 주소(이벤트를 일으키는)에 대한 침입 이벤트의 카운트를 보여줍니다.

상위 침입 대상 위젯

상위 침입 대상 위젯은 모니터링되는 네트워크에서 상위 대상 호스트 IP 주소(이벤트를 일으키는 연결의 대상)에 대한 침입 이벤트의 카운트를 보여줍니다.

상위 악성코드 시그니처 위젯

Top Malware Signatures(상위 악성코드 서명**)** 위젯은 상위 파일 전송 호스트 IP 주소에 대한 네트워크 트래픽에서 탐지된 상위 악성코드 서명의 카운트를 표시합니다.

상위 악성코드 발신자 위젯

Top Malware Senders(상위 악성코드 발신자**)** 위젯은 상위 파일 전송 호스트 IP 주소에 대한 네트워크 트래픽에서 탐지된 상위 악성코드 위협의 카운트를 표시합니다.

상위 악성코드 수신자 위젯

Top Malware Signatures(상위 악성코드 서명**)** 위젯은 모든 상위 파일을 수신하는 호스트 IP 주소에 대해 네트워크 트래픽에서 탐지된 상위 악성코드 위협의 수를 표시합니다.

배치 위젯별 악성코드 이벤트

Malware Events by Disposition 위젯은 매니지드 디바이스가 악성코드가 포함된 파일을 탐지할 때 생성되는 모든 악성코드 이벤트 속성의 카운트를 표시합니다.

네트워크 활동 위젯

네트워크 활동 위젯은 연결 이벤트의 정보를 기반으로 하는 모든 인그레스 및 이그레스 데이터 속도를 표시합니다.

이벤트 활동 위젯

이벤트 활동 위젯은 지난 1시간 동안 발생한 이벤트의 수와 데이터베이스에서 사용 가능한 각 이벤트 유형의 총 수를 표시합니다.

액세스 제어 작업 위젯

Access Control Actions(액세스 제어 작업**)** 위젯은 각 이벤트에 대해 허용되거나 차단된 액세스 제어 작업을 기준으로 로깅된 이벤트의 카운트를 표시합니다. 원도표 위에 마우스를 올려놓으면 허용된 작업과 차단된 작업의 백분율을 볼 수 있습니다.

상위 액세스 제어 정책 위젯

상위 액세스 제어 정책 위젯은 이벤트를 생성하는 상위 액세스 제어 정책의 카운트를 표시합니다.

상위 액세스 제어 규칙 위젯

상위 액세스 제어 규칙 위젯은 각 이벤트에 사용되는 액세스 제어 규칙의 상위 5개 카운트를 표시합니다. 이러한 카운트는 바이트 또는 이벤트를 기준으로 정렬할 수 있습니다.

상위 디바이스 위젯

Top Devices(상위 디바이스**)** 위젯은 디바이스별 이벤트 수를 표시합니다. 이러한 개수는 바이트 또는 이벤트를 기준으로 정렬할 수 있습니다.

상위 사용자 위젯

상위 사용자 위젯은 가장 많은 침입 이벤트 수와 관련된 모니터링 네트워크의 사용자 목록을 표시합니다. 이는 침입 탐지(IDS) 사용자 통계 및 Intrusion Events(침입 이벤트) 테이블의 데이터를 주로 보여줍니다. 신뢰할 수 있는 사용자 데이터를 표시합니다.

비정상 디바이스 위젯

비정상 디바이스 위젯은 CDO에서 관리하는 위협 방어 디바이스의 현재 컴파일된 상태를 표시합니다.

상위 로드된 디바이스 위젯

Top Loaded Devices(상위 로드된 디바이스**)** 위젯은 CPU 사용량 정보와 함께 위협 방어 디바이스 목록을 표시합니다.

FTD 대시보드에 대한 시간 설정 수정

시간 범위를 변경하여 지난 시간처럼 짧은 기간(기본값) 또는 지난해처럼 긴 기간을 반영할 수 있습니다. 시간 범위를 변경할 때, 시간을 통해 자동 제한될 수 있는 위젯은 새로운 시간 범위를 반영하도록 업데이트합니다.

그래프의 최대 데이터 포인트 수는 300이며, 시간 설정은 각 데이터 포인트 내에 요약되는 시간을 결정합니다. 다음은 각 시간 범위에 대한 FTD 대시보드에서 다루는 데이터 포인트 수 및 시간 범위입니다.

- 1시간 = 12개의 데이터 포인트, 각 5분
- 6시간 = 72개 데이터 포인트, 각 5분
- 1일 = 288개의 데이터 포인트, 각 5분
- 1주 = 300개의 데이터 포인트, 각 33.6분
- 2주 = 300개의 데이터 포인트, 각 67.2분
- 30일 = 300개 데이터 포인트, 각 144분
- 90일 = 300개의 데이터 포인트, 각 432분
- 180일 = 300개 데이터 포인트, 각 864분
- 1년 = 300개의 데이터 포인트, 각 1752분