검색 이벤트

다음 주제에서는 검색 이벤트를 사용하는 방법을 설명합니다.

검색 이벤트 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모두

사용자 역할

- 관리자
- 보안 분석가

검색 이벤트의 검색 및 ID 데이터

시스템은 모니터링되는 네트워크에서 탐지된 변경을 나타내는 이벤트의 테이블을 생성합니다. 이러한 테이블을 사용하여 네트워크에서의 사용자 활동을 검토하고 대응 방법을 결정할 수 있습니다. 네트워크 검색 및 *ID* 정책은 수집할 데이터 종류, 모니터링할 네트워크 세그먼트, 이를 위해 사용할 특정 하드웨어 인터페이스를 지정합니다.

검색 및 ID 이벤트 테이블을 사용하여 네트워크의 호스트, 애플리케이션, 사용자에 연결된 위협을 식별할 수 있습니다. 시스템은 시스템에서 생성되는 이벤트 분석에 사용할 수 있는 사전 정의 워크플로 집합을 제공합니다. 특정 요구와 일치하는 정보만 표시하는 맞춤형 워크플로를 생성할 수도 있습니다.

분석을 위해 네트워크 검색 및 ID 데이터를 수집하고 저장하려면 네트워크 검색 및 ID 정책을 구성해야 합니다. ID 정책을 구성한 후에는 액세스 제어 정책에서 ID 정책을 호출하여 트래픽 모니터링에 사용할 디바이스에 구축해야 합니다.

네트워크 검색 정책은 호스트, 애플리케이션, 권한 없는 사용자 데이터를 제공합니다. ID 정책은 권한 있는 사용자 데이터를 제공합니다.

다음 검색 이벤트 테이블은 Analysis(분석) > Hosts(호스트) 및 Analysis(분석) > Users(사용자) 메뉴 아래 위치합니다.

검색 이벤트 테이블	검색 데이터로 채워지는지 여부	**ID** 데이터로 채워지는지 여부
호스트	예	아니요
호스트 보안 침해 지표	예	아니요
애플리케이션	예	아니요
애플리케이션 세부사항	예	아니요
서버	예	아니요
호스트 속성	예	아니요
검색 이벤트	예	예
사용자 보안 침해 지표	예	예
활성 세션	예	예
사용자의 활동	예	예
사용자	예	예
취약성	예	아니요
서드파티 취약성	예	아니요

검색 이벤트 통계 보기

Discovery Statistics(검색 통계) 페이지에는 시스템에서 탐지한 호스트, 이벤트, 프로토콜, 애플리케이션 프로토콜 및 운영 체제의 요약이 표시됩니다.

이 페이지에는 마지막 시간에 대한 통계 및 총 누적 통계가 나열됩니다. 특정 디바이스 또는 모든 디바이스에 대한 통계를 볼 수 있습니다. 요약 내에 나열된 이벤트, 서버, 운영 체제 또는 운영 체제 공급업체를 클릭하여 페이지의 항목과 일치하는 이벤트를 볼 수도 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**)** > **Discovery Statistics(**검색 통계**)**을(를) 선택합니다.

단계 **2** 통계를 보려는 디바이스를 **Select Device(**디바이스 선택**)** 목록에서 선택합니다. 선택적으로, 모든 관리하는 모든 디바이스에 대한 통계를 보려면 management center를 선택합니다.

단계 **3** 다음과 같은 옵션이 있습니다.

- Statistics Summary(통계 요약)에서 통계 요약 섹션, 3 페이지의 설명에 따라 일반 통계를 볼 수 있습니다.
- Event Breakdown(이벤트 분류)에서 보려고 하는 이벤트 유형을 클릭합니다. 이벤트가 표시되지 않는 경우, 타임 윈도우 변경에 설명된 대로 시간 범위를 조정해야 할 수 있습니다.
- Protocol Breakdown(프로토콜 분류)에서 탐지된 이벤트가 현재 사용 중인 프로토콜을 볼 수 있습니다.
- Application Protocol Breakdown(애플리케이션 프로토콜 분류)에서 보려는 애플리케이션 프로토콜의 이름을 클릭합니다.
- OS Breakdown(OS 분류)에서 **OS Name(OS** 이름**)** 또는 **OS Vendor(OS** 공급업체**)**를 클릭합니다.

관련 항목

이벤트 분류 섹션, 4 페이지
프로토콜 분류 섹션, 5 페이지
애플리케이션 프로토콜 분류 섹션, 5 페이지
OS 분류 섹션, 5 페이지

통계 요약 섹션

다음은 Statistics Summary(통계 요약) 섹션의 행에 대한 설명입니다.

Total events

management center에 저장된 총 검색 이벤트 수.

최근 **1**시간의 전체 이벤트

마지막 시간에 생성된 총 검색 이벤트 수.

최근 **1**일의 전체 이벤트

마지막 날에 생성된 총 검색 이벤트 수

Total Application Protocols

탐지된 호스트에서 실행 중인 서버의 총 애플리케이션 프로토콜 수.

Total IP Hosts

고유한 IP 주소로 식별된 총 탐지된 호스트 수.

Total MAC Hosts

IP 주소로 식별되지 않은 총 탐지된 호스트 수.

모든 디바이스에 대한 검색 통계를 보든 특정 디바이스에 대한 검색 통계를 보든, Total MAC Hosts 통계는 동일합니다. 매니지드 디바이스는 IP 주소를 기반으로 호스트를 검색하기 때문입니다. 이 통계는 다른 수단에 의해 식별되는 총 호스트 수를 제공하며 특정 매니지드 디바이스와는 독립적입니다.

Total Routers

라우터로서 식별된 총 탐지된 노드 수.

Total Bridges

브리지로서 식별된 총 탐지된 노드 수.

Host Limit Usage

현재 사용 중인 호스트 제한의 총 비율. 호스트 제한은 management center의 모델로 정의됩니다. 모든 매니지드 디바이스에 대한 통계를 보는 경우에만 Host Limit Usage가 나타납니다.

참고 호스트 제한에 도달하고 호스트가 삭제되는 경우, 검색 데이터를 비운 네트워크 맵에 호스트가 다시 나타나지 않습니다.

Last Event Received

가장 최근 검색 이벤트가 발생한 날짜 및 시간.

Last Connection Received

가장 최근 연결이 완료된 날짜 및 시간.

이벤트 분류 섹션

Event Breakdown(이벤트 분류) 섹션에는 마지막 시간 내에 발생한 검색 및 호스트 입력 이벤트의 각 유형별 카운트는 물론 데이터베이스에 저장된 각 이벤트 유형의 총 카운트도 나열됩니다.

검색 및 호스트 입력 이벤트에 대한 세부사항을 보는 데에도 Event Breakdown(이벤트 분류) 섹션을 사용할 수 있습니다.

관련 항목

검색 및 호스트 입력 이벤트, 9 페이지

프로토콜 분류 섹션

Protocol Breakdown(프로토콜 분류) 섹션에는 탐지된 호스트에서 현재 사용 중인 프로토콜이 나열됩니다. 탐지된 각 프로토콜 이름, 프로토콜 스택에서의 "레이어", 프로토콜을 사용하여 통신하는 총 호스트 수가 표시됩니다.

애플리케이션 프로토콜 분류 섹션

Application Protocol Breakdown(애플리케이션 프로토콜 분류) 섹션에는 탐지된 호스트에서 현재 사용 중인 애플리케이션 프로토콜이 나열됩니다. 프로토콜 이름, 지난 시간 동안 애플리케이션 프로토콜을 실행하던 총 호스트 수, 특정 시점에 프로토콜을 실행하던 것으로 탐지된 총 호스트 수가 나열됩니다.

탐지된 프로토콜을 사용하는 서버에 대한 세부사항을 보는 데에도 Application Protocol Breakdown(애플리케이션 프로토콜 분류) 섹션을 사용할 수 있습니다.

관련 항목

서버 데이터, 30 페이지

OS 분류 섹션

OS Breakdown(OS 분류) 섹션에는 모니터링되는 네트워크에서 현재 실행 중인 운영 체제와 더불어 해당 공급업체 및 각 운영 체제를 실행 중인 총 호스트 수가 나열됩니다.

운영 체제 이름 및 버전에 사용되는 `unknown` 값은 해당 운영 체제 및 버전이 시스템의 핑거프린트와 일치하지 않음을 의미합니다. `pending` 값은 시스템이 운영 체제 및 버전을 식별하는 데 필요한 정보를 아직 충분히 수집하지 못했음을 의미합니다.

탐지된 운영 체제에 대한 세부사항을 보는 데에도 OS Breakdown(OS 분류) 섹션을 사용할 수 있습니다.

관련 항목

호스트 데이터, 17 페이지

검색 성능 그래프 보기

검색 이벤트와 함께 매니지드 디바이스에 대한 성능 통계를 표시하는 그래프를 생성할 수 있습니다.

새 데이터는 통계 그래프를 위해 5분마다 누적됩니다. 따라서 그래프를 빠르게 다시 로드하는 경우 다음 5분 증가분이 발생할 때까지 데이터가 변경되지 않을 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.

시작하기 전에

애플리케이션 네트워크 검색 정책이 애플리케이션, 호스트, 사용자를 포함하도록 편집합니다. (이는 시스템 성능에 영향을 줄 수 있습니다.) 네트워크 검색 규칙 구성 및 작업 및 검색된 자산를 참조하십시오.

이 작업을 수행하려면 관리자 또는 유지보수 사용자여야 합니다.

프로시저

단계 **1** **Overview(**개요**)** > **Summary(**요약**)** > **Discovery Performance(**검색 성능**)**을(를) 선택합니다.

단계 **2** 포함할 management center 또는 매니지드 디바이스를 **Select Device(**디바이스 선택**)** 목록에서 선택합니다.

단계 **3** 검색 성능 그래프 유형, 6 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** 선택한 통계를 그래프로 표시하려면 **Graph(**그래프**)**를 클릭합니다.

검색 성능 그래프 유형

다음은 사용 가능한 그래프 유형에 대한 설명입니다.

Processed Events/Sec

Data Correlator가 초당 처리하는 이벤트 수를 나타내는 그래프를 표시합니다.

Processed Connections/Sec

Data Correlator가 초당 처리하는 연결 수를 나타내는 그래프를 표시합니다.

Generated Events/Sec

시스템이 초당 생성하는 이벤트 수를 나타내는 그래프를 표시합니다.

Mbits/Sec

초당 검색 프로세스에 의해 분석되는 트래픽의 메가비트 수를 나타내는 그래프를 표시합니다.

평균 바이트/패킷

검색 프로세스에 의해 분석되는 각 패킷에 포함된 평균 바이트 수를 나타내는 그래프를 표시합니다.

K Packets/Sec

초당 검색 프로세스에 의해 분석되는 패킷 수를 나타내는 그래프를 표시합니다(1,000 단위).

검색 및 ID 워크플로 사용

management center에서는 네트워크에 대해 생성되는 검색 및 ID 데이터 분석에 사용할 수 있는 이벤트 워크플로 집합을 제공합니다. 워크플로는 네트워크 맵과 더불어 네트워크 자산에 대한 핵심 정보 소스입니다.

management center에서는 검색 및 ID 데이터에 대한 사전 정의된 워크플로는 물론 탐지된 호스트와 호스트 속성, 서버, 애플리케이션, 애플리케이션 세부사항, 취약성, 사용자 활동, 사용자 등에 대한 사전 정의된 워크플로도 제공합니다. 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** 사전 정의된 워크플로에 액세스하려면 다음을 수행합니다.

- 검색 및 호스트 입력 데이터 — 검색 및 호스트 입력 이벤트 보기, 15 페이지를 참조하십시오.
- 호스트 데이터 — 호스트 데이터 보기, 17 페이지를 참조하십시오.
- 호스트 속성 데이터 — 호스트 속성 보기, 24 페이지를 참조하십시오.
- 호스트 또는 사용자 보안 침해 지표 데이터 — 보안 침해 지표 데이터 보기 및 작업, 26 페이지를 참조하십시오.
- 서버 데이터 — 서버 데이터 보기, 31 페이지를 참조하십시오.
- 애플리케이션 데이터 — 애플리케이션 데이터 보기, 34 페이지를 참조하십시오.
- 애플리케이션 세부사항 데이터 — 애플리케이션 세부사항 데이터 보기, 37 페이지를 참조하십시오.
- 활성 세션 데이터 — 활성 세션 데이터 보기, 54 페이지를 참조하십시오.
- 사용자 데이터 — 사용자 데이터 보기, 57 페이지를 참조하십시오.
- 사용자 활동 데이터 — 사용자 활동 데이터 보기, 60 페이지를 참조하십시오.
- 네트워크 맵 — 네트워크 맵 보기를 참조하십시오.

단계 **2** 맞춤형 워크플로에 액세스하려면 **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Workflows(**사용자 지정 워크플로**)**를 선택합니다.

단계 **3** 맞춤형 테이블에 기반한 워크플로에 액세스하려면 **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Tables(**사용자 지정 표**)**를 선택합니다.

단계 **4** 네트워크 검색 워크플로에서 액세스하는 모든 페이지에서 일반적으로 이루어지는 다음 작업을 수행합니다.

- 열 제한 — 표시되는 열을 제한하려면 숨기려는 열 머리글의 **Close(**닫기**)** (✕)을 클릭합니다. 표시되는 팝업 창에서 **Apply(**적용**)**를 클릭합니다.

  팁 다른 열을 숨기거나 표시하려면 **Apply(**적용**)**를 클릭하기 전에 해당 확인란을 선택하거나 확인 취소합니다. 비활성화된 열을 보기에 다시 추가하려면 확장 화살표를 클릭하여 검색 제약 조건을 확장한 다음, Disabled Columns(비활성화된 열) 아래에서 열 이름을 클릭합니다.

- 삭제 — 현재 제한된 보기에서 일부 또는 모든 항목을 삭제하려면 삭제할 항목 옆의 확인란을 선택한 후 **Delete(**삭제**)**를 클릭하거나 **Delete All(**모두 삭제**)**을 클릭합니다. 이러한 항목은 시스템의 검색 기능이 다시 시작될 때까지(이 경우 다시 탐지될 수도 있음) 삭제된 상태로 유지됩니다.

  주의 **Analysis(**분석**)** > **Users(**사용자**)** > **Active Sessions(**활동 세션**)** 페이지에서 non-VPN(비 VPN) 세션을 삭제하기 전에 해당 세션을 닫았는지 확인하십시오. 활성 세션을 삭제하면 해당 정책이 디바이스의 세션을 탐지할 수 없으므로, 이러한 작업을 수행하도록 정책을 구성한 경우에도 세션을 모니터링하거나 차단할 수 없습니다.

  참고 Analysis > Users > Active Sessions(분석 > 사용자 > 활성 세션) 페이지의 VPN 세션에 대한 자세한 내용은 원격 액세스 VPN 현재 사용자 보기를 참조하십시오.

  참고 Cisco(서드파티와 반대) 취약성은 삭제할 수 없습니다. 그러나 검토한 것으로 표시할 수는 있습니다.

- 드릴다운 — 워크플로에서 다음 페이지로 드릴다운하려면 드릴다운 페이지 사용을 참조하십시오.
- 현재 페이지 이동 — 현재 워크플로 페이지 내에서 이동하려면 워크플로 페이지 탐색 툴을 참조하십시오.
- 워크플로 내에서 이동 — 현재 제약 조건을 유지한 상태로 현재 워크플로의 페이지 간에 이동하려면, 워크플로 페이지의 왼쪽 상단에서 해당하는 페이지 링크를 클릭합니다.
- 다른 워크플로로 이동 — 다른 이벤트 보기로 이동하여 관련 이벤트를 검토하려면 워크플로 간 탐색을 참조하십시오.
- 데이터 정렬 — 워크플로의 데이터를 정렬하려면 열 제목을 클릭합니다. 정렬 순서를 반대로 하려면 열 제목을 다시 클릭합니다.
- 호스트 프로파일 보기 - IP 주소의 호스트 프로파일을 보려면 **Host Profile(**호스트 프로파일**)**을 클릭하거나 활성 IOC(Indication of Compromise) 태그가 있는 호스트의 경우에는 IP 주소 옆에 표시되는 **Compromised Host(**보안 침해된 호스트**)**를 클릭합니다.
- 사용자 프로파일 - 사용자 ID 정보를 보려면 **User Identity(**사용자 **ID)** 옆에 표시되는 사용자 아이콘 또는 IOC와 연결된 사용자라면 **Red User(**빨간색 사용자**)**를 클릭합니다. 보기

관련 항목

워크플로 사용

Management Center 데이터베이스에서 데이터 제거

검색 및 호스트 입력 이벤트

시스템에서는 모니터링되는 네트워크 세그먼트의 변경 세부사항을 전달하는 검색 이벤트를 생성합니다. 새로 검색된 네트워크 기능에 대해서는 새 이벤트가 생성되고, 이전에 식별된 네트워크 자산의 변경 사항에 대해서는 변경 이벤트가 생성됩니다.

초기 네트워크 검색 단계에서 시스템은 각 호스트에 대해, 그리고 각 호스트에서 실행 중인 것으로 검색된 TCP 또는 UDP 서버에 대해 새 이벤트를 생성합니다. 원하는 경우, 내보낸 NetFlow 레코드를 사용하여 이러한 새 호스트 및 서버 이벤트를 생성하도록 시스템을 구성할 수 있습니다.

또한 시스템은 검색된 각 호스트에서 실행 중인 각 애플리케이션 프로토콜, 네트워크 및 전송에 대해 새 이벤트를 생성합니다. NetFlow 엑스포터를 모니터링하도록 구성된 검색 규칙에서는 애플리케이션 프로토콜 탐지를 비활성화할 수 있지만, 매니지드 디바이스를 모니터링하도록 구성된 검색 규칙에서는 비활성화할 수 없습니다. 비 NetFlow 검색 규칙에서 호스트 또는 사용자 검색을 비활성화하면 애플리케이션이 자동으로 검색됩니다.

초기 네트워크 매핑이 완료되면 시스템은 변경 이벤트를 생성하여 네트워크 변경 사항을 계속해서 기록합니다. 전에 검색된 자산의 구성이 변경될 때마다 변경 이벤트가 생성됩니다.

생성된 검색 이벤트는 데이터베이스에 로깅됩니다. management center 웹 인터페이스를 사용하여 검색 이벤트를 보고, 검색하고, 삭제할 수 있습니다. 상관관계 규칙에서도 검색 이벤트를 사용할 수 있습니다. 생성된 검색 이벤트 유형 및 지정한 다른 기준을 기반으로 상관관계 규칙을 작성할 수 있습니다. 상관관계 정책에서 사용할 경우 이러한 규칙은 네트워크 트래픽이 기준을 충족하면 교정과 syslog, SNMP, 이메일 알림 응답을 실행합니다.

호스트 입력 기능을 사용하여 네트워크 맵에 데이터를 추가할 수 있습니다. 운영 체제 정보를 추가, 수정 또는 삭제할 수 있으며, 이 경우 시스템은 해당 호스트에 대한 해당 정보의 업데이트를 중지합니다. 또한 애플리케이션 프로토콜, 클라이언트, 서버 및 호스트 속성을 수동으로 추가, 수정 또는 삭제하거나 취약성 정보를 수정할 수도 있습니다. 이렇게 하면 시스템은 호스트 입력 이벤트를 생성합니다.

검색 이벤트 유형

네트워크 검색 정책에서 시스템이 기록하는 검색 이벤트의 유형을 설정할 수 있습니다. 검색 이벤트 테이블을 볼 경우 **Event** 열에 이벤트 유형이 나열됩니다. 다음은 검색 이벤트 유형에 대한 설명입니다.

호스트에 대해 추가 **MAC** 탐지됨

시스템이 전에 검색된 호스트에 대해 새 MAC 주소를 탐지할 경우 이 이벤트가 생성됩니다.

시스템이 라우터를 통해 트래픽을 전달하는 호스트를 탐지할 경우 이 이벤트가 종종 생성됩니다. 각 호스트에는 서로 다른 IP 주소가 있지만, 모든 호스트는 라우터와 연결된 MAC 주소가 있는 것으로 표시됩니다. IP 주소와 연결된 실제 MAC 주소를 탐지할 경우 시스템은 호스트 프로파일 내에 MAC 주소를 굵은 텍스트로 표시하며, 이벤트 보기의 이벤트 설명 내에 "ARP/DHCP detected" 메시지를 표시합니다.

클라이언트 시간 초과

시스템이 비활성 상태를 이유로 클라이언트를 데이터베이스에서 삭제하면 이 이벤트가 생성됩니다.

클라이언트 업데이트

시스템이 HTTP 트래픽에서 페이로드(즉, 오디오, 비디오, 웹메일 등 특정 유형의 콘텐츠)를 탐지할 경우 이 이벤트가 생성됩니다.

DHCP: IP 주소 변경됨

DHCP 주소 할당 때문에 호스트 IP 주소가 변경된 것을 시스템이 탐지할 경우 이 이벤트가 생성됩니다.

DHCP: IP 주소 재할당

호스트가 IP 주소를 재사용할 경우, 즉 DHCP IP 주소 할당 때문에 호스트가 전에 다른 물리적 호스트에 사용되던 IP 주소를 얻는 경우 이 이벤트가 생성됩니다.

홉 변경

호스트 및 해당 호스트를 탐지하는 디바이스 간 다수의 네트워크 홉에서 시스템이 변경 사항을 탐지할 경우 이 이벤트가 생성됩니다. 발생 조건은 다음과 같습니다.

- 디바이스가 여러 라우터를 통과하는 호스트 트래픽을 확인하고 호스트 위치에 대한 더 나은 결정을 내릴 수 있는 경우
- 디바이스가 호스트로부터 ARP 전송을 탐지하고 로컬 세그먼트에 호스트가 있음을 나타내는 경우

호스트 삭제됨**:** 호스트 한도 도달함

management center에서 호스트 제한이 초과되어 네트워크 맵에서 모니터링되는 호스트가 삭제될 경우 이 이벤트가 생성됩니다.

호스트 삭제됨**:** 호스트 한도 도달함

management center에서 호스트 제한에 도달하여 새 호스트가 삭제될 경우 이 이벤트가 생성됩니다. 이 이벤트를 호스트 제한에 도달할 경우 오래된 호스트가 네트워크 맵에서 삭제되는 이전 이벤트와 비교해보십시오.

호스트 제한에 도달할 경우 새 호스트를 삭제하려면 **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)** > **Advanced(**고급**)**로 이동하여 **When Host Limit Reached(**호스트 제한 도달 시**)**를 **Drop hosts(**호스트 삭제**)**로 설정합니다.

호스트 **IOC** 설정

호스트에 대해 IOC(indication of compromise)가 설정되고 알림이 생성될 경우 이 이벤트가 발생합니다.

호스트 시간 초과

호스트가 네트워크 검색 정책에 정의된 간격 내에 트래픽을 생성하지 못했기 때문에 네트워크 맵에서 삭제될 경우 이 이벤트가 생성됩니다. 개별 호스트 IP 주소 및 MAC 주소는 개별적으로 시간 초과됩니다. 관련된 모든 주소가 시간 초과되기 전에는 호스트가 네트워크 맵에서 사라지지 않습니다.

네트워크 검색 정책에서 모니터링할 네트워크를 변경하는 경우, 호스트 제한에서 계산되지 않도록 네트워크 맵에서 오래된 호스트를 수동으로 삭제하고자 할 수 있습니다.

네트워크 디바이스로 호스트 유형 변경됨

탐지된 호스트가 실제로 네트워크 디바이스임을 시스템에서 확인할 경우 이 이벤트가 생성됩니다.

ID 충돌

서버 또는 운영체제에 대한 현재의 능동 ID와 충돌하는 새 서버 또는 운영체제 ID를 시스템이 탐지할 경우 이 이벤트가 생성됩니다.

새로운 능동 ID 데이터를 얻기 위해 호스트를 다시 스캔하여 ID 충돌을 해결하려면 Nmap 교정을 트리거하는 Identity Conflict(ID 충돌) 이벤트를 사용할 수 있습니다.

ID 시간 초과

활성 소스의 서버 또는 운영체제 ID 데이터가 시간을 초과하면 이 이벤트가 생성됩니다.

새로운 능동 ID 데이터를 얻기 위해 호스트를 다시 스캔하여 ID 데이터를 새로 고치려면 Nmap 교정을 트리거하는 Identity Conflict(ID 충돌) 이벤트를 사용할 수 있습니다.

MAC 정보 변경

특정 MAC 주소 또는 TTL 값과 연결된 정보에서 시스템이 변경 사항을 탐지할 경우 이 이벤트가 생성됩니다.

시스템이 라우터를 통해 트래픽을 전달하는 호스트를 탐지할 경우 이 이벤트가 종종 발생합니다. 각 호스트에는 서로 다른 IP 주소가 있지만, 모든 호스트는 라우터와 연결된 MAC 주소가 있는 것으로 표시됩니다. IP 주소와 연결된 실제 MAC 주소를 탐지할 경우 시스템은 호스트 프로파일 내에 MAC 주소를 굵은 텍스트로 표시하며, 이벤트 보기의 이벤트 설명 내에 "ARP/DHCP detected" 메시지를 표시합니다. 트래픽이 여러 라우터를 통과할 수 있으므로 TTL이 변경될 수 있습니다. 또는 시스템이 호스트의 실제 MAC 주소를 탐지하는 경우에도 TTL이 변경될 수 있습니다.

NETBIOS 이름 변경

시스템이 호스트 NetBIOS 이름의 변경을 탐지할 경우 이 이벤트가 생성됩니다. 이 이벤트는 NetBIOS 프로토콜을 사용하는 호스트에 대해서만 생성됩니다.

새 클라이언트

시스템이 새 클라이언트를 탐지할 경우 이 이벤트가 생성됩니다.

참고 분석용 클라이언트 데이터를 수집 및 저장하려면 네트워크 검색 정책의 검색 규칙에서 애플리케이션 탐지를 활성화하십시오.

새 호스트

시스템이 네트워크에서 실행 중인 새 호스트를 탐지할 경우 이 이벤트가 생성됩니다.

이 이벤트는 디바이스가 새 호스트와 관련된 NetFlow 데이터를 처리하는 경우에도 생성될 수 있습니다. 이 경우 이벤트를 생성하려면, NetFlow 데이터를 관리해 호스트를 검색하는 네트워크 검색 규칙을 설정해야 합니다.

새 네트워크 프로토콜

호스트가 새 네트워크 프로토콜(IP, ARP 등)과 통신 중임을 시스템이 탐지할 경우 이 이벤트가 생성됩니다.

새 **OS**

시스템이 호스트에 대한 새 운영체제를 탐지하거나 호스트 운영체제에서 변경 사항을 탐지할 경우 이 이벤트가 생성됩니다.

새 **TCP** 포트

호스트에서 활성화된 새 TCP 서버 포트(예: SMTP 또는 웹 서비스에서 사용하는 포트)를 시스템이 탐지할 경우 이 이벤트가 생성됩니다. 이 이벤트는 애플리케이션 프로토콜 또는 이와 연결된 서버를 식별하는 데 사용되지 않습니다. 그러한 정보는 TCP Server Information Update(TCP 서버 정보 업데이트) 이벤트에서 전송됩니다.

또한 이 이벤트는 네트워크 맵에 존재하지 않는 모니터링되는 네트워크 상의 서버와 관련된 NetFlow 데이터를 디바이스가 처리할 때도 생성됩니다. 이 경우 이벤트를 생성하려면, NetFlow 데이터를 관리해 애플리케이션을 검색하는 네트워크 검색 규칙을 설정해야 합니다.

새 전송 프로토콜

호스트가 TCP, UDP 등의 새 네트워크 프로토콜과 통신 중임을 시스템이 탐지할 경우 이 이벤트가 생성됩니다.

새 **UDP** 포트

시스템이 호스트에서 실행 중인 새 UDP 서버 포트를 탐지할 경우 이 이벤트가 생성됩니다.

또한 이 이벤트는 네트워크 맵에 존재하지 않는 모니터링되는 네트워크 상의 서버와 관련된 NetFlow 데이터를 디바이스가 처리할 때도 생성됩니다. 이 경우 이벤트를 생성하려면, NetFlow 데이터를 관리해 애플리케이션을 검색하는 네트워크 검색 규칙을 설정해야 합니다.

TCP 포트 닫힘

시스템이 호스트에서 닫힌 TCP 포트를 탐지할 경우 이 이벤트가 생성됩니다.

TCP 포트 시간 초과

시스템이 네트워크 검색 정책에 정의된 간격 내에 TCP 포트로부터의 활동을 탐지하지 못한 경우 이 이벤트가 생성됩니다.

TCP 서버 정보 업데이트

시스템이 호스트에서 실행 중인 검색된 TCP 서버에서 변경 사항을 탐지할 경우 이 이벤트가 생성됩니다.

TCP 서버가 업그레이드되는 경우에도 이 이벤트가 생성될 수 있습니다.

UDP 포트 닫힘

시스템이 호스트에서 닫힌 UDP 포트를 탐지할 경우 이 이벤트가 생성됩니다.

UDP 포트 시간 초과

시스템이 네트워크 검색 정책에 정의된 간격 내에 UDP 포트로부터의 활동을 탐지하지 못한 경우 이 이벤트가 생성됩니다.

UDP 서버 정보 업데이트

시스템이 호스트에서 실행 중인 검색된 UDP 서버에서 변경 사항을 탐지할 경우 이 이벤트가 생성됩니다.

UDP 서버가 업그레이드되는 경우에도 이 이벤트가 생성될 수 있습니다.

VLAN 태그 정보 업데이트

시스템이 호스트에 속하는 VLAN 태그에서 변경 사항을 탐지할 경우 이 이벤트가 생성됩니다.

관련 항목

호스트 입력 이벤트 유형, 13 페이지

호스트 입력 이벤트 유형

검색 이벤트의 테이블을 볼 경우 **Event** 열에 이벤트 유형이 나열됩니다.

사용자가 특정 작업(예: 수동으로 호스트 추가)을 수행할 때 생성되는 호스트 입력 이벤트를 시스템이 모니터링되는 네트워크에서 직접 변경 사항을 탐지(예: 전에 탐지되지 않던 호스트에서 트래픽 탐지)할 때 생성되는 검색 이벤트와 비교해보십시오.

네트워크 검색 정책을 수정하여, 시스템이 기록하는 호스트 입력 이벤트의 유형을 설정할 수 있습니다.

서로 다른 유형의 호스트 입력 이벤트가 제공하는 정보를 이해하면 어떤 이벤트를 기록하고 알림을 전송할지, 상관관계 정책에서 이러한 알림을 어떻게 사용할지를 좀 더 효과적으로 결정할 수 있습니다. 또한 이벤트 유형의 이름을 알면 좀 더 효과적으로 이벤트를 검색할 수 있습니다. 다음은 서로 다른 유형의 호스트 입력 이벤트에 대한 설명입니다.

클라이언트 추가

사용자가 클라이언트를 추가할 경우 이 이벤트가 생성됩니다.

호스트 추가

사용자가 호스트를 추가할 경우 이 이벤트가 생성됩니다.

프로토콜 추가

사용자가 프로토콜을 추가할 경우 이 이벤트가 생성됩니다.

스캔 결과 추가

시스템이 Nmap 스캔의 결과를 호스트에 추가할 경우 이 이벤트가 생성됩니다.

포트 추가

사용자가 서버 포트를 추가할 경우 이 이벤트가 생성됩니다.

클라이언트 삭제

사용자가 시스템에서 클라이언트를 삭제할 경우 이 이벤트가 생성됩니다.

호스트/네트워크 삭제

사용자가 시스템에서 IP 주소 또는 서브넷을 삭제할 경우 이 이벤트가 생성됩니다.

프로토콜 삭제

사용자가 시스템에서 프로토콜을 삭제할 경우 이 이벤트가 생성됩니다.

포트 삭제

사용자가 시스템에서 서버 포트 또는 서버 포트 그룹을 삭제할 경우 이 이벤트가 생성됩니다.

호스트 특성 추가

사용자가 새 호스트 속성을 생성할 경우 이 이벤트가 생성됩니다.

호스트 특성 삭제

사용자가 사용자 정의 호스트 속성을 삭제할 경우 이 이벤트가 생성됩니다.

호스트 특성 삭제 값

사용자가 호스트 속성에 할당된 값을 삭제할 경우 이 이벤트가 생성됩니다.

호스트 특성 설정 값

사용자가 호스트에 대한 호스트 속성 값을 설정할 경우 이 이벤트가 생성됩니다.

호스트 특성 업데이트

사용자가 사용자 정의 호스트 속성의 정의를 변경할 경우 이 이벤트가 생성됩니다.

호스트 중요도 설정

사용자가 호스트에 대한 호스트 중요도 값을 설정 또는 수정할 경우 이 이벤트가 생성됩니다.

운영 시스템 정의 설정

사용자가 호스트에 대한 운영체제를 설정할 경우 이 이벤트가 생성됩니다.

서버 정의 설정

사용자가 서버에 대한 벤더 및 버전 정의를 설정할 경우 이 이벤트가 생성됩니다.

취약성 영향 자격 설정

취약성 영향 자격이 설정될 경우 이 이벤트가 생성됩니다.

영향 자격에 대해 사용 중인 취약성이 전역 레벨에서 비활성화되거나 전역 레벨에서 취약성이 활성화될 경우 이 이벤트가 생성됩니다.

취약성 설정 유효하지 않음

사용자가 취약성을 무효화 또는 검토할 경우 이 이벤트가 생성됩니다.

취약성 설정 유효함

전에 잘못된 것으로 표시되었던 취약성을 사용자가 검증할 경우 이 이벤트가 생성됩니다.

관련 항목

검색 이벤트 유형, 9 페이지

검색 및 호스트 입력 이벤트 보기

검색 이벤트 워크플로를 사용하면 검색 이벤트와 호스트 입력 이벤트에서 데이터를 볼 수 있습니다. 찾고 있는 정보에 따라 이벤트 보기를 조작할 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.

이벤트에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 검색 이벤트의 테이블 보기 및 호스트 보기 종료 페이지를 포함하는 사전 정의 워크플로를 사용할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Hosts(**호스트**)** > **Discovery Events(**검색 이벤트**)**을(를) 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 타임 윈도우 변경에 설명된 대로 시간 범위를 조정합니다.

  참고 어플라이언스의 구성된 타임 윈도우(전역 또는 이벤트 전용 모두 해당)를 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.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**(워크플로 전환)를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 7 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(검색 이벤트 필드, 16 페이지 참조).

관련 항목

검색 및 ID 워크플로 사용, 7 페이지

검색 이벤트 필드

다음은 검색 이벤트 테이블에서 보고 검색할 수 있는 필드에 대한 설명입니다.

시간

시스템이 이벤트를 생성한 시간

이벤트

검색 이벤트 유형 또는 호스트 입력 이벤트 유형.

IP 주소

이벤트와 관련된 호스트와 연결된 IP 주소

사용자

이벤트가 생성되기 전 이벤트와 관련된 호스트에 로그인한 마지막 사용자. 권한 있는 사용자 이후 권한 없는 사용자만 로그인한 경우, 권한 있는 사용자가 호스트에 대한 현재 사용자로 유지됩니다(또 다른 권한 있는 사용자가 로그인하지 않는 한).

MAC 주소

검색 이벤트를 트리거한 네트워크 트래픽에 의해 사용된 NIC의 MAC 주소. 이 MAC 주소는 이벤트와 관련된 호스트의 실제 MAC 주소일 수도 있고, 트래픽이 통과한 네트워크 디바이스의 MAC 주소일 수도 있습니다.

MAC Vendor(MAC 벤더)

검색 이벤트를 트리거한 네트워크 트래픽에 의해 사용된 NIC의 MAC 하드웨어 공급업체

포트

이벤트를 트리거한 트래픽에서 사용하는 포트(해당되는 경우)

설명

이벤트의 텍스트 설명

도메인

호스트를 검색한 디바이스의 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

Device(디바이스)

이벤트를 생성한 매니지드 디바이스의 이름입니다. NetFlow 데이터를 기반으로 하는 새 호스트 및 새 서버 이벤트의 경우 이것이 해당 데이터를 처리한 매니지드 디바이스입니다.

관련 항목

이벤트 검색

호스트 데이터

시스템은 호스트를 탐지하고 관련 정보를 수집하여 호스트 프로파일을 작성할 때 이벤트를 생성합니다. management center 웹 인터페이스를 사용하여 호스트를 보고, 검색하고, 삭제할 수 있습니다.

호스트를 보는 동안 선택한 호스트를 기반으로 트래픽 프로필 및 규정 준수 허용 목록을 생성할 수 있습니다. 또한 호스트 중요도 값(비즈니스 중요도를 지정)을 비롯한 호스트 속성을 호스트 그룹에 할당할 수 있습니다. 그런 다음 상관관계 규칙 및 정책 내에서 이러한 중요도 값, 허용 목록 및 트래픽 프로필을 사용할 수 있습니다.

시스템에서는 내보낸 NetFlow 기록에서 네트워크 맵에 호스트를 추가할 수 있지만, 이러한 호스트에 사용할 수 있는 정보는 제한됩니다. NetFlow와 매니지드 디바이스 데이터의 차이점의 내용을 참조하십시오.

호스트 데이터 보기

management center를 사용하면 시스템에서 탐지한 호스트의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 보기를 조작할 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.

호스트에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 미리 정의된 두 워크플로는 사용자의 제한 사항을 충족하는 모든 호스트에 대한 호스트 프로파일이 포함된 호스트 보기에서 종료됩니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** 호스트 데이터에 액세스합니다.

- 사전 정의된 워크플로를 사용 중인 경우 **Analysis(분석)** > **Hosts(호스트)** > **Hosts(호스트)**를 선택합니다.
- 호스트의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭한 다음 **Hosts(호스트)**를 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 7 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(호스트 데이터 필드, 18 페이지 참조).
- 옵션을 보려면 테이블에서 항목을 마우스 오른쪽 버튼으로 클릭합니다. (옵션을 제공하지 않는 열도 있습니다.)
- 특정 호스트에 호스트 속성을 할당합니다(선택한 호스트에 대해 호스트 속성 설정, 25 페이지 참조).
- 특정 호스트에 대한 트래픽 프로파일을 생성합니다(선택한 호스트에 대한 트래픽 프로파일 생성, 22 페이지 참조).
- 특정 호스트를 기반으로 컴플라이언스 허용 목록을 생성합니다(선택한 호스트를 기반으로 규정 준수 허용리스트 생성, 23 페이지 참조).

호스트 데이터 필드

시스템은 호스트를 검색하면 해당 호스트에 대한 데이터를 수집합니다. 여기에는 호스트의 IP 주소, 실행 중인 운영 체제 등이 포함될 수 있습니다. 그러한 정보 중 일부는 호스트의 테이블 보기에서 볼 수 있습니다.

다음은 호스트 테이블에서 보고 검색할 수 있는 필드에 대한 설명입니다.

Last Seen(최종 확인**)**

시스템에서 마지막으로 탐지한 호스트 IP 주소 중 하나의 날짜 및 시간. Last Seen(최종 확인) 값은 적어도 네트워크 검색 정책에서 구성한 업데이트 간격만큼 그리고 호스트 IP 주소 중 하나에 대해 새 호스트 이벤트를 생성할 때 업데이트됩니다.

호스트 입력 기능을 사용하여 업데이트된 운영 체제 데이터가 있는 호스트의 경우 Last Seen(최종 확인) 값은 데이터가 원래 추가된 날짜 및 시간을 나타냅니다.

IP Address(IP 주소**)**

호스트와 연결된 IP 주소

MAC Address(MAC 주소)

호스트에서 탐지한 NIC의 MAC 주소.

MAC Address 필드는 호스트 워크플로에서 찾을 수 있는 호스트의 테이블 보기에 나타납니다. MAC Address 필드를 다음에도 추가할 수 있습니다.

- 호스트 테이블의 필드를 포함하는 사용자 지정 테이블
- 호스트 테이블 기반의 사용자 지정 워크플로에 있는 드릴다운 페이지

MAC Vendor(MAC 벤더)

호스트에서 탐지한 NIC의 MAC 하드웨어 공급업체.

MAC Vendor 필드는 호스트 워크플로에서 찾을 수 있는 호스트의 테이블 보기에 나타납니다. MAC Vendor 필드를 다음에도 추가할 수 있습니다.

- 호스트 테이블의 필드를 포함하는 사용자 지정 테이블
- 호스트 테이블 기반의 사용자 지정 워크플로에 있는 드릴다운 페이지

이 필드를 검색할 경우 `virtual_mac_vendor`를 입력하여 가상 호스트와 관련된 이벤트와 일치시킵니다.

Current User(현재 사용자)

현재 호스트에 로그인한 사용자의 사용자 ID(사용자 이름)

권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다. 또한 권한 없는 사용자가 호스트의 현재 사용자인 경우, 해당 사용자를 사용자 제어에 사용할 수 없습니다.

Host Criticality(호스트 심각도)

호스트에 할당된 사용자 지정 중요도 값.

NetBIOS Name(NetBIOS 이름)

호스트의 NetBIOS 이름. NetBIOS 프로토콜을 실행하는 호스트만이 NetBIOS 이름을 가질 수 있습니다.

VLAN ID

호스트에서 사용하는 VLAN ID.

Hops(홉)

호스트를 탐지한 디바이스에서 호스트로의 네트워크 홉 수

Host Type(호스트 유형**)**

호스트의 유형. 호스트, 모바일 디바이스, 탈옥 모바일 디바이스, 라우터, 브리지, NAT 디바이스 및 로드 밸런서 중 어떤 것이든 가능합니다.

시스템이 네트워크 디바이스를 구분하기 위해 사용하는 방법은 다음과 같습니다.

- CDP(Cisco Discovery Protocol) 메시지의 분석 - 네트워크 디바이스 및 유형을 식별할 수 있습니다(Cisco 디바이스만 해당).
- STP(Spanning Tree Protocol)의 탐지 - 디바이스를 스위치 또는 브리지로 식별합니다.
- 동일한 MAC 주소를 사용하는 여러 호스트 탐지 - MAC 주소를 라우터에 속한 것으로 식별합니다.
- 클라이언트 측에서 TTL 값 변경 탐지 또는 일반적인 부팅시간보다 더 자주 변경되는 TTL 값 - NAT 디바이스 및 로드 밸런서를 탐지합니다.

네트워크 디바이스로 식별되지 않는 디바이스는 호스트로 분류됩니다.

이 필드를 검색할 경우 `!host`를 입력하여 모든 네트워크 디바이스를 검색합니다.

Hardware(하드웨어**)**

모바일 디바이스용 하드웨어 플랫폼.

OS

다음 중 하나에 해당합니다.

- 호스트에서 탐지되거나 Nmap 또는 호스트 입력 기능을 사용하여 업데이트된 운영 체제(이름, 벤더 및 버전)
- `unknown` - 운영 체제가 알려진 핑거프린트와 일치하지 않는 경우
- `pending` - 시스템이 운영체제를 식별하는 데 필요한 정보를 아직 충분히 수집하지 못한 경우

시스템에서는 여러 ID를 탐지하면 쉼표로 구분된 목록으로 표시합니다.

대시보드의 Custom Analysis 위젯에서 호스트 이벤트 보기를 호출할 경우 이 필드가 나타납니다. 이것은 또한 호스트 테이블 기반의 사용자 지정 테이블에 있는 필드 옵션이기도 합니다.

이 필드를 검색할 경우 `n/a`를 입력하여 운영 체제가 아직 식별되지 않은 호스트를 포함합니다.

OS Conflict(OS 컨플릭트**)**

이 필드는 검색 전용입니다.

OS Vendor(OS 벤더**)**

다음 중 하나에 해당합니다.

- 호스트에서 탐지되었거나 Nmap 또는 호스트 입력 기능을 사용하여 업데이트된 운영 체제의 벤더

- `unknown` - 운영 체제가 알려진 핑거프린트와 일치하지 않는 경우
- `pending` - 시스템이 운영 체제를 식별하는 데 필요한 정보를 아직 충분히 수집하지 못한 경우

시스템에서는 여러 벤더를 탐지하면 쉼표로 구분된 목록으로 표시합니다.

이 필드를 검색할 경우 `n/a`를 입력하여 운영 체제가 아직 식별되지 않은 호스트를 포함합니다.

OS Name(OS 이름)

다음 중 하나에 해당합니다.

- 호스트에서 탐지되거나 Nmap 또는 호스트 입력 기능을 사용하여 업데이트된 운영 체제
- `unknown` - 운영 체제가 알려진 핑거프린트와 일치하지 않는 경우
- `pending` - 시스템이 운영 체제를 식별하는 데 필요한 정보를 아직 충분히 수집하지 못한 경우

시스템에서는 여러 이름을 탐지하면 쉼표로 구분된 목록으로 표시합니다.

이 필드를 검색할 경우 `n/a`를 입력하여 운영 체제가 아직 식별되지 않은 호스트를 포함합니다.

OS Version(OS 버전)

다음 중 하나에 해당합니다.

- 호스트에서 탐지되었거나 Nmap 또는 호스트 입력 기능을 사용하여 업데이트된 운영 체제
- `unknown` - 운영 체제가 알려진 핑거프린트와 일치하지 않는 경우
- `pending` - 시스템이 운영 체제를 식별하는 데 필요한 정보를 아직 충분히 수집하지 못한 경우

시스템에서는 여러 버전을 탐지하면 쉼표로 구분된 목록으로 표시합니다.

이 필드를 검색할 경우 `n/a`를 입력하여 운영 체제가 아직 식별되지 않은 호스트를 포함합니다.

Source Type(소스 유형)

호스트의 운영 체제 ID를 설정하는 데 사용되는 소스의 유형입니다.

- 사용자: user_name
- 애플리케이션: app_name
- 스캐너: scanner_type(네트워크 검색 구성을 통해 추가된 Nmap 또는 스캐너)
- 시스템에서 탐지한 운영 체제용 `Firepower`

시스템에서는 운영 체제의 ID를 확인하기 위해 여러 소스의 데이터를 조정할 수 있습니다.

신뢰

다음 중 하나에 해당합니다.

- 호스트에서 실행 중인 운영 체제의 ID에 대한 시스템의 신뢰도 비율 - 시스템에서 탐지한 호스트

- 100% - 호스트 입력 기능 또는 Nmap 스캐너 등 활성 소스에 의해 식별된 운영 체제
- `unknown` - 시스템이 운영 체제 ID를 확인할 수 없는 호스트 및 NetFlow 데이터를 기반으로 네트워크 맵에 추가된 호스트

이 필드를 검색할 경우 `n/a`를 입력하여 NetFlow 데이터에 기반한 네트워크 맵에 추가된 호스트를 포함합니다.

Notes(참고)

Notes 호스트 속성의 사용자 정의 내용.

도메인

호스트와 연결된 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

Device(디바이스)

트래픽을 탐지한 매니지드 디바이스를 입력하거나, NetFlow 또는 호스트 입력 데이터를 처리한 디바이스를 입력합니다.

이 필드가 비어 있는 경우, 다음 조건 중 하나가 사실에 해당합니다.

- 네트워크 검색 정책에 정의된 대로, 호스트 상주 네트워크를 명시적으로 모니터링하지 않는 디바이스에 의해 호스트가 네트워크 맵에 추가되었습니다.
- 호스트가 호스트 입력 기능으로 추가되었으며 시스템에 의해 탐지되지 않았습니다.

개수

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

관련 항목

이벤트 검색
운영 체제 ID 충돌

선택한 호스트에 대한 트래픽 프로파일 생성

트래픽 프로파일은 네트워크의 트래픽 프로파일로, 지정한 기간에 수집된 연결 데이터를 기반으로 합니다. 트래픽 프로파일을 생성한 후에는 프로파일을 기준으로 새 트래픽을 평가하여, 정상적인 것처럼 보일 수 있는 비정상적인 네트워크 트래픽을 탐지할 수 있습니다.

지정한 호스트 그룹에 대한 트래픽 프로파일을 생성하려면 Hosts 페이지를 사용할 수 있습니다. 트래픽 프로파일은 지정한 호스트 중 하나가 호스트를 시작하는 것으로 탐지된 연결을 기반으로 합니다. 프로파일을 생성하고자 하는 호스트를 격리하려면 정렬 또는 검색 기능을 사용할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** 호스트 워크플로의 테이블 보기에서 트래픽 프로파일을 생성하려는 호스트 옆에 있는 확인란을 선택합니다.

단계 **2** 페이지의 하단에서 **Create Traffic Profile(**트래픽 프로파일 생성**)**을 클릭합니다.

단계 **3** 특정 요구에 맞게 트래픽 프로파일을 수정 및 저장합니다.

관련 항목

트래픽 프로파일 소개

선택한 호스트를 기반으로 규정준수 허용리스트 생성

규정준수 허용리스트를 사용하면 네트워크에서 허용한 운영체제와 클라이언트, 네트워크, 전송 또는 애플리케이션 프로토콜을 지정할 수 있습니다.

지정한 호스트 그룹의 호스트 프로파일을 기반으로 규정준수 허용리스트를 생성하려면 Hosts(호스트) 페이지를 사용하면 됩니다. 허용리스트를 생성하고자 사용하려는 호스트를 격리하려면 정렬 또는 검색 기능을 사용할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** 호스트 워크플로우의 테이블 보기에서 허용리스트를 생성하려는 호스트 옆에 있는 확인란을 선택합니다.

단계 **2** 페이지의 하단에서 **Create(**생성**)**허용 목록를 클릭합니다.

단계 **3** 특정 요구에 맞게 허용리스트를 수정 및 저장합니다.

관련 항목

컴플라이언스 허용 목록 소개

호스트 속성 데이터

Firepower System은 탐지한 호스트에 대한 정보를 수집하고 이 정보를 사용하여 호스트 프로파일을 작성합니다. 그러나 분석가에게 제공하고자 하는, 네트워크의 호스트에 대한 추가 정보가 있을 수 있습니다. 호스트 프로파일에 메모를 추가하거나, 호스트의 비즈니스 중요도를 설정하거나, 선택한 다른 정보를 제공할 수 있습니다. 이러한 각각의 정보를 호스트 속성이라고 합니다.

호스트 프로파일 자격에 호스트 속성을 사용할 수 있습니다. 이러한 속성은 트래픽 프로파일 작성 중에 수집하는 데이터를 제한하며, 상관관계 규칙을 트리거할 조건을 제한할 수도 있습니다. 상관관계 규칙에 대한 응답에 속성 값을 설정할 수도 있습니다.

관련 항목

호스트 속성 보기, 24 페이지
세트 속성값 교정 구성

호스트 속성 보기

management center를 사용하면 시스템에서 탐지한 호스트의 테이블을 호스트 속성과 함께 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 보기를 조작할 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.

호스트 속성에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 탐지된 모든 호스트 및 해당 속성을 나열하는 호스트 속성의 테이블 보기를 포함하며, 제약 조건에 맞는 모든 호스트에 대한 호스트 프로파일이 포함된 호스트 보기 페이지에서 종료되는 사전 정의 워크플로를 사용할 수 있습니다.

특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** 호스트 속성 데이터에 액세스합니다.

- 사전 정의된 워크플로를 사용 중인 경우 **Analysis(분석)** > **Hosts(호스트)** > **Host Attributes(호스트 속성)**를 선택합니다.
- 호스트 속성의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(워크플로 전환)**를 클릭한 다음 **Attributes(속성)**를 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(워크플로 전환)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 7 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(호스트 속성 데이터 필드, 24 페이지 참조).
- 특정 호스트에 호스트 속성을 할당합니다(선택한 호스트에 대해 호스트 속성 설정, 25 페이지 참조).

호스트 속성 데이터 필드

MAC 주소에 의해서만 식별되는 호스트는 속성 테이블에 표시되지 않습니다.

다음은 호스트 속성 테이블에서 보고 검색할 수 있는 필드에 대한 설명입니다.

IP Address(IP 주소)

호스트와 연결된 IP 주소

Current User(현재 사용자**)**

현재 호스트에 로그인한 사용자의 사용자 ID(사용자 이름)

권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다. 또한 권한 없는 사용자가 호스트의 현재 사용자인 경우, 해당 사용자를 사용자 제어에 사용할 수 없습니다.

Host Criticality(호스트 심각도**)**

엔터프라이즈에 사용자가 할당하는 호스트의 중요도. 정책 위반 및 응답을 이벤트와 관련된 호스트의 중요도에 맞추려면 상관관계 규칙 및 정책에 호스트 중요도를 사용할 수 있습니다. Low, Medium, High 또는 None의 호스트 중요도를 할당할 수 있습니다.

Notes(참고**)**

다른 분석가에게 보여줄 호스트에 대한 정보.

임의의 사용자 정의 호스트 속성, 컴플라이언스 허용 목록 대상 포함

사용자 정의 호스트 속성의 값. 호스트 속성 테이블에는 각 사용자 정의 호스트 속성에 대한 필드가 포함되어 있습니다.

도메인

호스트와 연결된 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

개수

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

관련 항목

이벤트 검색

선택한 호스트에 대해 호스트 속성 설정

호스트 워크플로에서 사전 정의된 호스트 속성 및 사용자 정의 호스트 속성을 구성할 수 있습니다.

프로시저

단계 **1** 호스트 워크플로에서 호스트 속성을 추가하려는 호스트의 옆에 있는 확인란을 선택합니다.

팁 정렬 및 검색 기능을 사용하여, 특정 속성을 할당할 호스트를 격리합니다.

단계 **2** 페이지의 하단에서 **Set Attributes(**속성 설정**)**를 클릭합니다.

단계 **3** 선택적으로, 선택한 호스트의 호스트 중요도를 설정합니다. **None(**없음**)**, **Low(**낮음**)**, **Medium(**중간**)** 또는 **High(**높음**)**를 선택할 수 있습니다.

단계 **4** 필요한 경우, 텍스트 상자에서 선택한 호스트의 호스트 프로파일에 메모를 추가합니다.

단계 **5** 선택적으로, 이미 구성한 사용자 정의 호스트 속성을 설정합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

보안 침해 지표 데이터

시스템은 다양한 유형의 데이터(침입 이벤트, 보안 인텔리전스, 연결 이벤트, 파일 또는 악성코드 이벤트)를 상호 연결하여 모니터링되는 네트워크의 호스트가 악의적인 수단에 의해 보안이 침해될 가능성이 있는지를 확인합니다. 이벤트 데이터의 특정 조합 및 빈도는 영향받는 호스트에서 IOC(보안 침해 지표) 태그를 트리거합니다.이러한 호스트의 IP 주소는 이벤트 보기에서 빨간색의 보안 침해된 호스트 아이콘으로 표시됩니다.

보안 침해 가능성이 있는 호스트가 식별되면 해당 보안 침해에 연결된 사용자에게도 태그가 지정됩니다. 이러한 사용자는 이벤트 보기에서 빨간색 사용자 아이콘으로 표시됩니다.

악성코드가 포함된 파일이 IOC로 태그가 지정된 지 300초 내에 다시 발견되는 경우, 또 다른 IOC가 생성되지 않습니다. 동일한 파일이 300초 이상 지나 발견되는 경우에는 새 IOC가 생성됩니다.

보안 침해 지표로 이벤트에 태그를 지정하도록 시스템을 구성하려면 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 보안 침해 지표 규칙 활성화를 참조하십시오.

관련 항목

서버 ID 수정

보안 침해 지표 데이터 보기 및 작업

management center을 사용하여 IOC가 표시된 테이블을 볼 수 있습니다. 찾고 있는 정보에 따라 이벤트 보기를 조작합니다.

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

사용하는 워크플로에 따라 표시되는 페이지가 달라집니다. 제약 조건을 충족하는 모든 호스트 또는 사용자의 호스트 또는 사용자 프로파일이 포함된 프로파일 보기에서 사전 정의된 IOC 워크플로가 종료됩니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

시작하기 전에

- 시스템에서 보안 침해 지표(Indications of compromise, IOC)를 탐지하고 태깅하려면 네트워크 검색 정책에서 IOC 기능을 활성화하고 하나 이상의 IOC 규칙을 활성화해야 합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 보안 침해 지표 규칙 활성화를 참조하십시오.
- 활성 ID 정책에서 사용자를 식별해야 합니다.

프로시저

단계 **1** 웹 인터페이스의 어느 위치가 요구 사항을 충족하는 정보를 제공하는지 확인합니다.

다음 위치를 사용하여 보안 침해 지표 데이터를 보거나 보안 침해 데이터 작업을 할 수 있습니다.

- 이벤트 뷰어(분석 메뉴 아래) - 연결, 보안 인텔리전스, 침입, 악성코드, IOC 검색 이벤트 보기는 이벤트가 IOC를 트리거했는지 여부를 나타냅니다. IOC 규칙을 트리거한 Secure Endpoint에 의해 생성된 악성코드 이벤트는 이벤트 유형 `AMP IOC`를 가지며, 보안 침해를 지정하는 이벤트 하위 유형과 함께 표시됩니다.
- 대시보드 - 대시보드에서는 Summary Dashboard(요약 대시보드)의 Threats(위협)에 호스트 및 사용자별 IOC 태그가 기본적으로 표시됩니다. Custom Analysis 위젯은 IOC 데이터를 기반으로 하는 사전 설정을 제공합니다.
- Context Explorer - Context Explorer의 Indications of Compromise(보안 침해 지표) 섹션에는 IOC 카테고리별 호스트의 그래프 및 호스트별 IOC 카테고리의 그래프가 표시됩니다.
- 네트워크 맵 페이지 - Analysis(분석) > Hosts(호스트) > Network Map(네트워크 맵) 아래의 Indications of Compromise(보안 침해 지표)는 보안 침해 유형과 IP 주소에 따라 보안 침해 가능성이 있는 네트워크의 호스트를 그룹화합니다.
- 네트워크 파일 분석 경로 세부 정보 페이지 - Analysis(분석) > Files(파일) > Network File Trajectory(네트워크 파일 분석 경로) 아래 나열된 파일 세부 정보 페이지를 사용하여 네트워크에서 보안 침해 지표를 추적할 수 있습니다.
- 호스트 보안 침해 지표 페이지 - Analysis(분석) > Hosts(호스트) 메뉴 아래의 Host Indications of Compromise(호스트 보안 침해 지표) 페이지에는 IOC 태그에 따라 그룹화된 모니터링되는 호스트가 나열됩니다. 이 페이지의 워크플로를 사용하여 데이터로 드릴다운합니다.
- 사용자 보안 침해 지표 페이지 - Analysis(분석) > Users(사용자) 메뉴 아래의 User Indications of Compromise(사용자 보안 침해 지표) 페이지에는 IOC 태그에 따라 그룹화된 잠재적 IOC 이벤트에 연결된 사용자가 나열됩니다. 이 페이지의 워크플로를 사용하여 데이터로 드릴다운합니다.
- 호스트 프로파일 페이지 - 보안 침해 가능성이 있는 호스트의 호스트 프로파일에는 해당 호스트에 연결된 모든 IOC 태그가 표시되며, 이를 사용하여 IOC 태그를 확인하고 IOC 규칙 상태를 구성할 수 있습니다.
- 사용자 프로파일 페이지 - 잠재적 IOC 이벤트에 연결된 사용자의 사용자 프로파일에는 해당 사용자에 연결된 모든 IOC 태그가 표시되며, 이를 사용하여 IOC 태그를 확인하고 IOC 규칙 상태를 구성할 수 있습니다. (management center 웹 인터페이스에서는 사용자 프로파일에 "User Identity" 레이블이 지정됩니다.)

단계 **2** 해당하는 경우 다음 중 하나를 수행하고 이 절차의 나머지 단계를 사용합니다.

옵션	설명
호스트에서 IOC를 조사하려면 다음을 수행합니다.	• 사전 정의된 워크플로를 사용 중인 경우 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Indications of Compromise(**보안 침해 지표 **(IoC))**를 선택합니다.

옵션	설명
	• 호스트 IOC 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭한 다음 **Host Indications of Compromise(**호스트 보안 침해 지표**)**를 선택합니다.
사용자와 관련된 IOC를 조사하려면 다음을 수행합니다.	• 사전 정의된 워크플로를 사용 중인 경우 **Analysis > Users > Indications of Compromise(**분석 > 사용자 > 보안 침해 지표**)**를 선택합니다. • 사용자 IOC 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭한 다음 **User Indications of Compromise(**사용자 보안 침해 지표**)**를 선택합니다.

단계 **3** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 7 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(보안 침해 지표 데이터 필드, 28 페이지 참조).
- Host Indications of Compromise(호스트 보안 침해 지표) 페이지에서: **IP Address(IP** 주소**)** 열의 **Compromised Host(**보안 침해된 호스트**)**를 클릭하여 보안 침해된 호스트의 호스트 프로파일을 봅니다.
- User Indications of Compromise(사용자 보안 침해 지표) 페이지에서: **User(**사용자**)** 열의 빨간색 사용자를 클릭하여 보안 침해와 관련된 사용자 프로파일을 봅니다.
- 목록에 더 이상 나타나지 않도록 IOC 이벤트를 확인된 것으로 표시합니다. 이렇게 하려면 수정할 IOC 이벤트 옆에 있는 확인란을 선택한 다음 **Mark Resolved(**확인된 것으로 표시**)**를 클릭합니다.
- **First Seen(**처음 확인 날짜**)** 또는 **Last Seen(**마지막 확인 날짜**)** 열에서 **View(**보기**)** (👁)을 클릭하여 IOC를 트리거한 이벤트의 세부사항을 봅니다.
- 더 많은 옵션 보기: 테이블의 값을 마우스 오른쪽 단추로 클릭합니다.

보안 침해 지표 데이터 필드

다음은 호스트 또는 사용자 보안 침해 지표(Indications of compromise, IOC) 테이블의 필드입니다. 모든 IOC 관련 테이블에 전체 필드가 포함되어 있지는 않습니다.

IP Address(IP 주소**)(**호스트 **IOC** 데이터를 볼 경우**)**

IOC를 트리거한 호스트와 연결된 IP 주소.

User(사용자**)(**사용자 **IOC** 데이터를 볼 경우**)**

IOC를 트리거한 이벤트와 연결된 사용자의 사용자 이름, 영역, 인증 소스.

카테고리

표시된 감염 유형에 대한 짧은 설명(예: `Malware Executed` 또는 `Impact 1 Attack`).

이벤트 유형

특정 IOC와 연결된 식별자로, 이를 트리거한 이벤트를 가리킴.

설명

침해 가능성이 있는 호스트에 미치는 영향에 대한 설명(예: `This host may be under remote control`(이 호스트가 원격 제어 상태일 수 있습니다) 또는 `Malware has been executed on this host`(이 호스트에서 악성코드가 실행되었습니다)).

First Seen/Last Seen(최초 확인**/**최종 확인**)**

IOC를 트리거하는 이벤트가 발생한 최초의/가장 최근의 날짜 및 시간.

Domain(도메인**)**

IOC를 트리거한 호스트의 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

관련 항목

이벤트 검색

단일 호스트 또는 사용자에 대한 보안 침해 지표 규칙 상태 수정

네트워크 검색 정책에서 활성화된 경우 보안 침해 지표 규칙은 모니터링되는 네트워크의 모든 호스트 및 해당 네트워크의 IOC 이벤트와 연결된 권한 있는 사용자에게 적용됩니다. 개별 호스트 또는 사용자에 대한 규칙을 비활성화하여 유용하지 않은 IOC 태그를 방지할 수 있습니다(예: DNS 서버에 IOC 태그를 표시하지 않으려는 경우). 적용 가능한 네트워크 검색 정책에서 규칙이 비활성화된 경우, 특정 호스트 또는 사용자에 대해 해당 규칙을 활성화할 수 없습니다. 특정 호스트에 대한 규칙을 비활성화할 경우 동일한 이벤트에 관련된 사용자에 대한 태깅에는 영향을 미치지 않으며, 그 반대의 경우에도 마찬가지입니다.

프로시저

단계 **1** 호스트 또는 사용자 프로파일의 **Indications of Compromise(**보안 침해 지표**)** 섹션으로 이동합니다.

단계 **2** **Edit Rule States(**규칙 상태 수정**)**를 클릭합니다.

단계 **3** 규칙의 **Enabled** 열에서 슬라이더를 클릭하여 규칙을 활성화 또는 비활성화합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

보안 침해 지표 태그의 소스 이벤트 보기

호스트 프로 파일 및 사용자 프로 파일의 보안 침해 지표 섹션을 사용 하 여 IOC 태그를 트리거한 이벤트를 빠르게 이동할 수 있습니다. 이러한 이벤트를 분석하면 보안 침해 위협을 해결하기 위해 조치가 필요한지 및 필요한 조치를 결정하는 데 필요한 정보를 얻을 수 있습니다.

IOC 태그의 타임스탬프 옆에 있는 **View(**보기**)** ( )을 클릭하면 IOC 태그를 트리거한 이벤트만 표시하도록 제한된, 관련 이벤트 유형에 대한 이벤트의 테이블 보기로 이동합니다.

사용자 IOC의 첫 번째 인스턴스만 management center에 표시됩니다. 후속 인스턴스는 DNS 서버에 의해 포착됩니다."

프로시저

단계 **1** 호스트 또는 사용자 프로파일에서 **Indications of Compromise(**보안 침해 지표**)** 섹션으로 이동합니다.

단계 **2** 조사하려는 IOC 태그의 **First Seen** 또는 **Last Seen** 열에서 **View(**보기**)** ( )을 클릭합니다.

보안 침해 지표 태그 해결

보안 침해 지표(IOC) 태그에 의해 표시된 위협을 분석 및 해결했거나 IOC 태그가 오탐인 것으로 확인되는 경우, 이벤트를 해결된 것으로 표시할 수 있습니다. 해결된 것으로 표시된 이벤트는 호스트 프로파일 및 사용자 프로파일에서 제거됩니다. 프로파일의 활성 IOC 태그가 모두 해결되면 보안 침해된 호스트 또는 사용자가 보안 침해와 관련되었다는 빨간색 사용자 아이콘이 더 이상 나타나지 않습니다. 해결된 IOC에 대해 여전히 IOC 트리거링 이벤트가 표시될 수 있습니다.

IOC 태그를 트리거한 이벤트가 반복되는 경우, 호스트 또는 사용자에 대해 IOC 규칙을 비활성화하지 않았다면 태그가 다시 설정됩니다.

프로시저

단계 **1** 호스트 또는 사용자 프로파일에서 **Indications of Compromise(**보안 침해 지표**)** 섹션으로 이동합니다.

단계 **2** 다음 2가지 옵션을 사용할 수 있습니다.

- 개별 IOC 태그를 해결된 것으로 표시하려면 해결하려는 태그의 오른쪽에 있는 **Delete(**삭제**)** ( )을 클릭합니다.
- 프로파일의 모든 IOC 태그를 해결된 것으로 표시하려면 **Mark All Resolved(**모두 해결된 것으로 표시**)**를 클릭합니다.

서버 데이터

시스템은 모니터링되는 네트워크 세그먼트의 호스트에서 실행 중인 모든 서버에 대한 정보를 수집합니다. 이 정보에는 다음이 포함됩니다.

- 서버 이름
- 서버가 사용하는 애플리케이션 및 네트워크 프로토콜
- 서버 공급업체 및 버전
- 서버를 실행하는 호스트와 연결된 IP 주소.
- 서버 통신 포트

시스템은 서버를 탐지하면 연결된 호스트가 이미 최대 서버 수에 도달하지 않은 경우 검색 이벤트를 생성합니다. management center 웹 인터페이스를 사용하여 서버 이벤트를 보고, 검색하고, 삭제할 수 있습니다.

상관관계 규칙의 기반을 서버 이벤트에 둘 수도 있습니다. 예를 들어, 시스템이 호스트 중 하나에서 실행 중인 채팅 서버(예: ircd)를 검색할 경우 상관관계 규칙을 트리거할 수 있습니다.

시스템에서는 내보낸 NetFlow 기록에서 네트워크 맵에 호스트를 추가할 수 있지만, 이러한 호스트에 사용할 수 있는 정보는 제한됩니다. NetFlow와 매니지드 디바이스 데이터의 차이점의 내용을 참조하십시오.

서버 데이터 보기

management center를 사용하면 탐지한 서버의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 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.

서버에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 모든 사전 정의 워크플로는 제약 조건을 충족하는 모든 호스트에 대한 호스트 프로파일이 포함된 호스트 보기에서 종료됩니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** 서버 데이터에 액세스합니다.

- 사전 정의된 워크플로를 사용 중인 경우 **Analysis(분석)** > **Hosts(호스트)** > **Servers(서버)**를 선택합니다.
- 서버의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭한 다음 **Servers(서버)**를 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 7 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(서버 데이터 필드, 32 페이지 참조).
- 수정할 서버에 대한 이벤트 옆에 있는 확인란을 선택한 다음 **Set Server Identity(서버 ID 설정)**를 클릭합니다.

- 옵션을 보려면 테이블에서 항목을 마우스 오른쪽 버튼으로 클릭합니다. (옵션을 제공하지 않는 열도 있습니다.)

서버 데이터 필드

다음은 서버에서 보고 검색할 수 있는 필드에 대한 설명입니다.

Last Used(최종 사용**)**

네트워크에서 서버가 마지막으로 사용된 날짜 및 시간, 또는 호스트 입력 기능을 사용하여 서버가 원래 업데이트된 날짜 및 시간. Last Used 값은 적어도 네트워크 검색 정책에서 구성한 업데이트 간격만큼 그리고 시스템이 서버 정보 업데이트를 탐지할 때 업데이트됩니다.

IP Address(IP 주소**)**

서버를 실행하는 호스트와 연결된 IP 주소.

Port(포트**)**

서버가 실행 중인 포트.

Protocol(프로토콜**)**

서버에서 사용하는 네트워크 또는 전송 프로토콜.

애플리케이션 프로토콜

다음 중 하나에 해당합니다.

- 서버에 대한 애플리케이션 프로토콜의 이름
- `pending` - 여러 이유 중 하나 때문에 시스템이 서버를 긍정적으로 또는 부정적으로 식별할 수 없는 경우
- `unknown` - 시스템이 알려진 서버 핑거프린트를 기반으로 서버를 식별할 수 없는 경우 또는 서버가 호스트 입력을 통해 추가되었고 애플리케이션 프로토콜을 포함하지 않은 경우

Category, Tags, Risk, or Business Relevance for Application Protocols(애플리케이션 프로토콜의 카테고리**,** 태그**,** 위험 또는 사업 타당성**)**

애플리케이션 프로토콜에 할당된 카테고리, 태그, 위험 레벨 및 비즈니스 연관성. 특정 데이터 집합에 집중하려면 이러한 필터를 사용할 수 있습니다.

Vendor(벤더**)**

다음 중 하나에 해당합니다.

- 시스템, Nmap, 다른 활성 소스 등에 의해 식별된 서버 공급업체 또는 호스트 입력 기능을 사용하여 지정한 서버 공급업체

- blank - 시스템이 알려진 서버 핑거프린트를 기반으로 공급업체를 식별할 수 없는 경우 또는 NetFlow 데이터를 사용하여 서버가 네트워크 맵에 추가된 경우

Version(버전**)**

다음 중 하나에 해당합니다.

- 시스템, Nmap, 다른 활성 소스 등에 의해 식별된 서버 공급업체 또는 호스트 입력 기능을 사용하여 지정한 서버 버전
- blank - 시스템이 알려진 서버 핑거프린트를 기반으로 버전을 식별할 수 없는 경우 또는 NetFlow 데이터를 사용하여 서버가 네트워크 맵에 추가된 경우

Web Application(웹 애플리케이션**)**

HTTP 트래픽에서 시스템에 의해 탐지된 페이로드 내용을 기반으로 하는 웹 애플리케이션. `HTTP`의 애플리케이션 프로토콜은 탐지하지만 특정 웹 애플리케이션은 탐지하지 못하는 경우 시스템은 일반 웹 브라우징 지정을 제공합니다.

Category, Tags, Risk, or Business Relevance for Web Applications(웹 애플리케이션의 카테고리**,** 태그**,** 위험 또는 사업 타당성**)**

웹 애플리케이션에 할당된 카테고리, 태그, 위험 레벨 및 비즈니스 연관성. 특정 데이터 집합에 집중하려면 이러한 필터를 사용할 수 있습니다.

Hits(히트**)**

서버에 액세스한 횟수. 호스트 입력 기능을 사용하여 추가된 서버의 경우 이 값은 항상 0입니다.

Source Type(소스 유형**)**

다음 값 중 하나:

- 사용자: user_name
- 애플리케이션: app_name
- 스캐너: scanner_type(네트워크 검색 구성을 통해 추가된 Nmap 또는 스캐너)
- Firepower System에서 탐지된 서버의 `Firepower`, `Firepower Port Match` 또는 `Firepower Pattern Match`
- NetFlow 데이터를 사용하여 추가된 서버의 `NetFlow`

도메인

서버를 실행하는 호스트의 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

Device(디바이스)

트래픽을 탐지한 매니지드 디바이스를 입력하거나, NetFlow 또는 호스트 입력 데이터를 처리한 디바이스를 입력합니다.

Current User(현재 사용자)

현재 호스트에 로그인한 사용자의 사용자 ID(사용자 이름)

권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다. 또한 권한 없는 사용자가 호스트의 현재 사용자인 경우, 해당 사용자를 사용자 제어에 사용할 수 없습니다.

개수

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

관련 항목

이벤트 검색

애플리케이션 및 애플리케이션 상세정보 데이터

모니터링되는 호스트가 다른 호스트에 연결되면, 시스템은 많은 경우 어떤 애플리케이션이 사용되었는지를 확인할 수 있습니다. Firepower System에서는 이메일, 인스턴트 메시징, 피어 투 피어, 웹 애플리케이션 및 기타 유형의 애플리케이션 사용을 탐지합니다.

탐지된 각 애플리케이션에 대해 시스템은 애플리케이션을 사용한 IP 주소, 제품, 버전, 탐지된 사용 횟수 등을 로깅합니다. 웹 인터페이스를 사용하여 애플리케이션 이벤트를 보고, 검색하고, 삭제할 수 있습니다. 또한 호스트 입력 기능을 사용하여 호스트의 애플리케이션 데이터를 업데이트할 수 있습니다.

어떤 애플리케이션이 어떤 호스트에서 실행 중인지 안다면, 이를 통해 호스트 프로파일 자격을 생성할 수 있습니다. 이 자격은 트래픽 프로파일 작성 중에 수집하는 데이터를 제한하며, 상관관계 규칙을 트리거할 조건을 제한할 수도 있습니다. 상관관계 규칙의 기반을 애플리케이션 탐지에 둘 수도 있습니다. 예를 들어 직원이 특정 메일 클라이언트를 사용하도록 하려면, 호스트 중 하나에서 다른 메일 클라이언트가 실행 중임을 시스템에서 탐지할 때 상관관계 규칙을 트리거할 수 있습니다.

각 Firepower System 업데이트의 릴리스 노트와 각 VDB 업데이트의 권고를 꼼꼼히 읽으면 Firepower의 애플리케이션 탐지기에 대한 최신 정보를 얻을 수 있습니다.

분석을 위해 애플리케이션 데이터를 수집 및 저장하려면 네트워크 검색 정책에서 애플리케이션 탐지를 활성화하십시오.

애플리케이션 데이터 보기

management center를 사용하면 탐지한 애플리케이션의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 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.

애플리케이션에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** 애플리케이션 데이터에 액세스합니다.

- 사전 정의된 워크플로를 사용 중인 경우 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Application Details(**애플리케이션 세부 정보**)**를 선택합니다.
- 애플리케이션 세부사항의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭한 다음 **Clients(**클라이언트**)**를 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 7 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(애플리케이션 데이터 필드, 35 페이지 참조).
- 클라이언트, 애플리케이션 프로토콜 또는 웹 애플리케이션 옆에 있는 **Application Detail View(**애플리케이션 세부 사항 보기**)**를 클릭하여 특정 애플리케이션의 Application Detail View(애플리케이션 세부 사항 보기)를 엽니다.
- 이벤트 값에서 마우스 오른쪽 버튼으로 클릭하여 시스템 외부에서 소스의 데이터를 봅니다. 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.
- 테이블에서 이벤트 값을 마우스 오른쪽 버튼으로 클릭하고 Cisco 또는 서드파티 인텔리전스 소스에서 선택하여 이벤트에 대한 인텔리전스를 수집합니다. 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.

애플리케이션 데이터 필드

알려진 클라이언트, 애플리케이션 프로토콜 또는 웹 애플리케이션에 대한 트래픽을 탐지하면 시스템은 애플리케이션 및 이를 실행하는 호스트에 대한 정보를 기록합니다.

다음은 애플리케이션 테이블에서 보고 검색할 수 있는 필드에 대한 설명입니다.

Application(애플리케이션**)**

탐지된 애플리케이션의 이름

IP Address(IP 주소)

애플리케이션을 사용하는 호스트와 연결된 IP 주소

유형

애플리케이션 유형:

애플리케이션 프로토콜

호스트 간의 통신을 나타냅니다.

클라이언트 애플리케이션

호스트에서 실행 중인 소프트웨어를 나타냅니다.

Web Applications

HTTP 트래픽에 대한 콘텐츠 또는 요청 URL을 나타냅니다.

카테고리

가장 중요한 기능을 설명하는 일반 애플리케이션 분류. 각 애플리케이션은 적어도 하나의 카테고리에 속합니다.

태그

애플리케이션에 대한 추가 정보. 애플리케이션에는 0부터 원하는 수만큼의 태그를 포함할 수 있습니다.

위험

조직의 보안 정책을 거스를 수 있는 용도로 애플리케이션이 사용될 가능성. 애플리케이션 위험의 범위는 Very Low(매우 낮음)에서 Very High(매우 높음)까지입니다.

침입 이벤트를 트리거한 트래픽에서 탐지된 Application Protocol Risk, Client Risk, Web Application Risk의 세 가지 중 최고(사용 가능한 경우).

Business Relevance(사업 타당성)

조직의 비즈니스 운영(레크리에이션과 반대) 컨텍스트 내에서 애플리케이션이 사용될 가능성. 애플리케이션 비즈니스 연관성의 범위는 Very Low(매우 낮음)에서 Very High(매우 높음)까지입니다.

침입 이벤트를 트리거한 트래픽에서 탐지된 Application Protocol Business Relevance, Client Business Relevance, Web Application Business Relevance의 세 가지 중 최저(사용 가능한 경우).

Current User(현재 사용자)

현재 호스트에 로그인한 사용자의 사용자 ID(사용자 이름)

권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에

의해서만 현재 사용자가 변경됩니다. 또한 권한 없는 사용자가 호스트의 현재 사용자인 경우, 해당 사용자를 사용자 제어에 사용할 수 없습니다.

Domain(도메인**)**

애플리케이션을 사용하는 호스트의 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

개수

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

관련 항목

이벤트 검색

애플리케이션 세부사항 데이터 보기

management center를 사용하면 탐지한 애플리케이션 세부사항의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 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.

애플리케이션 세부사항에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 두 가지 사전 정의 워크플로가 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** 애플리케이션 세부사항 데이터에 액세스합니다.

- 사전 정의된 워크플로를 사용 중인 경우 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Application Details(**애플리케이션 세부 정보**)**를 선택합니다.
- 애플리케이션 세부사항의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭한 다음 **Clients(**클라이언트**)**를 선택하십시오.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 7 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(애플리케이션 세부사항 데이터 필드, 38 페이지 참조).
- 클라이언트 옆에 있는 **Application Detail View(**애플리케이션 세부사항 보기**)** 를 클릭하여 특정 애플리케이션의 애플리케이션 세부사항 보기를 엽니다.
- 이벤트 값에서 마우스 오른쪽 버튼으로 클릭하여 시스템 외부에서 이용할 수 있는 소스의 데이터를 봅니다. 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.

- 테이블에서 이벤트 값을 마우스 오른쪽 버튼으로 클릭하고 Cisco 또는 서드파티 인텔리전스 소스에서 선택하여 이벤트에 대한 인텔리전스를 수집합니다. 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.

애플리케이션 세부사항 데이터 필드

알려진 클라이언트, 애플리케이션 프로토콜 또는 웹 애플리케이션에 대한 트래픽을 탐지하면 시스템은 애플리케이션 및 이를 실행하는 호스트에 대한 정보를 기록합니다.

다음은 애플리케이션 세부사항 테이블에서 보고 검색할 수 있는 필드에 대한 설명입니다.

Last Used(최종 사용)

애플리케이션이 마지막으로 사용된 시간 또는 호스트 입력 기능을 사용하여 애플리케이션 데이터가 업데이트된 시간. Last Used 값은 적어도 네트워크 검색 정책에서 구성한 업데이트 간격만큼 그리고 시스템이 애플리케이션 정보 업데이트를 탐지할 때 업데이트됩니다.

IP Address(IP 주소)

애플리케이션을 사용하는 호스트와 연결된 IP 주소

클라이언트

애플리케이션의 이름. 시스템이 애플리케이션 프로토콜을 탐지했지만 특정 클라이언트를 탐지하지 못한 경우, 일반 이름을 제공하기 위해 애플리케이션 프로토콜 이름에 `client`가 첨부됩니다.

버전

애플리케이션의 버전

Category, Tags, Risk, or Business Relevance for Clients, Application Protocols, and Web Applications(클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션의 카테고리, 태그, 위험 또는 사업 타당성)

애플리케이션에 할당된 카테고리, 태그, 위험 레벨 및 비즈니스 연관성. 특정 데이터 집합에 집중하려면 이러한 필터를 사용할 수 있습니다.

Application Protocol(애플리케이션 프로토콜)

애플리케이션에서 사용하는 애플리케이션 프로토콜. 시스템이 애플리케이션 프로토콜을 탐지했지만 특정 클라이언트를 탐지하지 못한 경우, 일반 이름을 제공하기 위해 애플리케이션 프로토콜 이름에 `client`가 첨부됩니다.

Web Application(웹 애플리케이션**)**

HTTP 트래픽에서 시스템에 의해 탐지된 페이로드 내용 또는 URL을 기반으로 하는 웹 애플리케이션. HTTP의 애플리케이션 프로토콜은 탐지하지만 특정 웹 애플리케이션은 탐지하지 못하는 경우 시스템은 여기에서 일반 웹 브라우징 지정을 제공합니다.

Hits(히트**)**

시스템이 사용 중인 애플리케이션을 탐지한 횟수. 호스트 입력 기능을 사용하여 추가된 애플리케이션의 경우 이 값은 항상 0입니다.

Domain(도메인**)**

애플리케이션을 사용하는 호스트의 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

Domain(디바이스**)**

애플리케이션 세부사항을 포함하는 검색 이벤트를 생성한 디바이스.

Current User(현재 사용자**)**

현재 호스트에 로그인한 사용자의 사용자 ID(사용자 이름)

권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다. 또한 권한 없는 사용자가 호스트의 현재 사용자인 경우, 해당 사용자를 사용자 제어에 사용할 수 없습니다.

개수

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

관련 항목

이벤트 검색

취약성 데이터

시스템에는 자체 취약성 추적 데이터베이스가 포함되어 있습니다. 이 데이터베이스를 시스템의 핑거프린트 인식 기능과 함께 사용하면 네트워크의 호스트에 연결된 취약성을 식별할 수 있습니다. 호스트에서 실행 중인 운영 체제, 서버 및 클라이언트는 연결된 취약성 집합이 서로 다릅니다.

management center를 사용하여 다음을 수행할 수 있습니다.

- 각 호스트의 취약성을 추적하고 검토합니다.
- 호스트를 패치하거나 그 밖의 방법으로 호스트가 취약성에 대해 면역력이 있다고 판단한 후 취약성을 비활성화합니다.

서버가 사용하는 애플리케이션 프로토콜이 management center 구성에서 매핑되어 있지 않으면 공급업체가 없는 서버 및 버전이 없는 서버의 취약성은 매핑되지 않습니다. 공급업체가 없는 클라이언트 및 버전이 없는 클라이언트의 취약성은 매핑할 수 없습니다.

관련 항목

서버의 취약성 매핑

취약성 데이터 필드

언급된 경우를 제외하고 이러한 필드는 **Analysis(**분석**) > Hosts(**호스트**) > Vulnerabilities(**취약점**)** 아래의 모든 페이지에 표시됩니다.

개수

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

CVE ID

MITRE CVE(Common Vulnerabilities and Exposures) 데이터베이스(https://cve.mitre.org/)의 취약성에 연결된 식별 번호.

NVD(National Vulnerability Database)에서 이 취약점에 대한 세부 정보를 보려면 CVE ID를 마우스 오른쪽 버튼으로 클릭하고 **View description in NVD(NVD**에서 설명 보기**)**를 선택합니다.

게시 날짜

취약성이 게시된 날짜입니다.

설명

NVD(National Vulnerability Database)의 취약점에 대한 간략한 설명입니다.

전체 설명을 보려면 CVE ID를 마우스 오른쪽 버튼으로 클릭하고 **View description in NVD(NVD**에서 설명 보기**)**를 선택하여 NVD(National Vulnerability Database)에서 세부 정보를 봅니다.

영향

"취약점 영향"(아래)을 참조하십시오.

영향 자격

이 필드는 Vulnerability Details(취약점 세부 사항) 페이지에서만 사용할 수 있습니다.

드롭다운 목록을 사용하여 취약성을 활성화 또는 비활성화합니다. management center는 영향 상관관계에서 비활성화된 취약성을 무시합니다.

여기서 지정하는 설정은 시스템 전체에서 취약성의 취급 방법을 결정하며, 값을 선택한 호스트 프로파일로 제한되지 않습니다.

원격

취약성이 원격으로 악용될 수 있는지 여부(TRUE/FALSE)를 나타냅니다.

심각도

NVD(National Vulnerability Database)의 기본 점수 및 CVSS(Common Vulnerability Scoring System) 점수입니다.

Snort ID

Snort ID(SID) 데이터베이스의 취약성에 연결된 ID 번호입니다. 즉, 침입 규칙이 특정 취약성을 악용하는 네트워크 트래픽을 탐지할 수 있으면 해당 취약성은 침입 규칙의 SID와 연결됩니다.

취약성은 둘 이상의 SID와 연결될 수 있습니다(SID와 연결되지 않을 수도 있음). 취약성이 둘 이상의 SID에 연결된 경우, 취약성 테이블에는 각 SID에 대한 행이 포함됩니다.

SVID

시스템에서 취약성 추적에 사용하는 취약성 ID 번호.

이 취약점에 대한 세부 정보를 보려면 **View(**보기**)** ( )을(를) 클릭합니다.

취약점 영향**/**영향

0에서 10까지의 범위에서 취약성의 심각도를 나타내며, 10이 가장 심각합니다.

관련 항목

이벤트 검색

취약성 비활성화

취약성을 비활성화하면 시스템은 해당 취약성을 사용하여 침입 영향 상관관계를 평가할 수 없습니다. 네트워크의 호스트에 패치를 적용하거나 그 밖의 방법으로 호스트가 취약성의 영향을 받지 않는다고 판단한 후 취약성을 비활성화할 수 있습니다. 시스템이 해당 취약성의 영향을 받는 새 호스트를 검색하면, 이 취약성은 해당 호스트에 대해 유효한 것으로 간주됩니다(따라서 자동으로 비활성화되지 않음).

IP 주소로 제한되지 않은 취약성 워크플로 내에서 취약성을 비활성화하면 네트워크에서 탐지된 모든 호스트에 대해 취약성이 비활성화됩니다. 취약성 워크플로 내의 취약성은 다음에서만 비활성화할 수 있습니다.

- 기본 취약성 워크플로의 두 번째 페이지인 **Vulnerabilities on the Network(**네트워크의 취약성**)**. 여기에는 네트워크의 호스트에 해당되는 취약성만 표시됩니다.
- 검색을 사용하여 IP 주소를 기반으로 제한한 맞춤형 또는 사전 정의된 취약성 워크플로의 페이지.

네트워크 맵을 사용하거나 호스트의 호스트 프로파일을 사용하거나 취약성을 비활성화하려는 호스트의 IP 주소를 기반으로 취약성 워크플로를 제한하여 단일 호스트의 취약성을 비활성화할 수 있습

니다. 연결된 IP 주소가 여러 개인 호스트의 경우, 이 기능은 해당 호스트의 선택된 단일 IP에만 적용됩니다.

다중 도메인 구축에서 상위 도메인의 취약성을 비활성화하면 모든 하위 도메인에서 해당 취약성이 비활성화됩니다. 취약성이 상위 도메인에서 활성화된 경우, 리프 도메인은 디바이스에서 해당 취약성을 활성화하거나 비활성화할 수 있습니다.

관련 항목

개별 호스트용 취약성 비활성화
개별 취약성 비활성화
다중 취약성 비활성화, 43 페이지

취약성 데이터 보기

management center를 사용하여 취약성의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

취약성에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 취약성의 테이블 보기를 포함하는 사전 정의 워크플로를 사용할 수 있습니다. 탐지된 호스트가 취약성을 보이는지 여부와 상관없이 테이블 보기에는 데이터베이스의 각 취약성에 대한 행이 포함되어 있습니다. 사전 정의 워크플로의 두 번째 페이지에는 네트워크에서 탐지된 호스트에 적용되는 각 취약성의 행(비활성화하지 않은)이 포함되어 있습니다. 사전 정의 워크플로는 제약 조건을 충족하는 모든 취약성에 대한 자세한 설명이 포함된 취약성 세부사항 보기에서 종료됩니다.

팁 단일 호스트 또는 호스트 집합에 적용되는 취약성을 보려면 호스트의 IP 주소 또는 IP 주소 범위를 지정하여 취약성 검색을 수행하십시오.

특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

취약성 테이블은 다중 도메인 구축에서 도메인에 의해 제한되지 않습니다.

프로시저

단계 **1** 취약성 테이블에 액세스합니다.

- 사전 정의된 취약성 워크플로를 사용 중인 경우 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Vulnerabilities(**취약성**)**를 선택합니다.
- 취약성의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)**를 클릭한 다음 **Vulnerabilities(**취약성**)**를 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 7 페이지 참조).
- 현재 취약한 호스트의 침입 영향 상관관계에 더 이상 사용되지 않도록 취약성을 비활성화합니다(다중 취약성 비활성화, 43 페이지 참조).

- SVID 열에서 **View(**보기**)** ( )을 클릭하여 취약성의 세부사항을 봅니다. 또는 취약성 ID를 제한하고 취약성 세부사항 페이지로 드릴다운합니다. 취약성 세부사항 보기, 43 페이지에서 추가 세부 정보를 보는 옵션을 참조하십시오.
- 제목을 마우스 오른쪽 버튼으로 클릭하고 **Show Full Text(**전체 텍스트 표시**)**를 선택하여 취약성 제목의 전체 텍스트를 확인합니다.

취약성 세부사항 보기

프로시저

다음 방법 중 하나로 취약성 세부사항을 볼 수 있습니다.

- **Analysis(**분석**)** > **Hosts(**호스트**)** > **Vulnerabilities(**취약성**)**를 선택하고 SVID 옆에 있는 **View(**보기**)** ( )를 클릭합니다.
- **Analysis(**분석**)** > **Hosts(**호스트**)** > **Third-Party Vulnerabilities(**서드파티 취약성**)**를 선택하고 SVID 옆에 있는 **View(**보기**)** ( )를 클릭합니다.
- **Analysis(**분석**)** > **Hosts(**호스트**)** > **Network Map(**네트워크 맵**)**를 선택하고 **Vulnerabilities(**취약성**)**을 클릭합니다.
- 취약성의 영향을 받는 호스트의 프로필을 보고(**Analysis(**분석**)** > **Hosts(**호스트**)** > **Network Map(**네트워크 맵**)**, **Hosts(**호스트**)**를 클릭하고, 드릴다운해서 조사하는 호스트를 클릭합니다), 프로필의 **Vulnerabilities(**취약성**)** 섹션을 확장합니다.
- **Analysis(**분석**)> Hosts(**호스트**)> Vulnerabilities(**취약성**)** 아래의 테이블에서 **CVE ID** 열의 값을 마우스 오른쪽 버튼으로 클릭하고 **View description in NVD(NVD**에서 설명보기**)**를 선택하여 NVD(National Vulnerabilities Database) 웹 사이트에서 해당 CVE를 봅니다.

다중 취약성 비활성화

IP 주소로 제한되지 않은 취약성 워크플로 내에서 취약성을 비활성화하면 네트워크에서 탐지된 모든 호스트에 대해 취약성이 비활성화됩니다.

다중 도메인 구축에서 상위 도메인의 취약성을 비활성화하면 모든 하위 도메인에서 해당 취약성이 비활성화됩니다. 취약성이 상위 도메인에서 활성화된 경우, 리프 도메인은 디바이스에서 해당 취약성을 활성화하거나 비활성화할 수 있습니다.

프로시저

단계 **1** 취약성 테이블에 액세스합니다.

- 사전 정의된 취약성 워크플로를 사용 중인 경우 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Vulnerabilities(**취약성**)**를 선택합니다.

- 취약성의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)**를 클릭한 다음 **Vulnerabilities(**취약성**)**를 선택합니다.

단계 **2** **Vulnerabilities on the Network(**네트워크의 취약성**)**를 클릭합니다.

단계 **3** 비활성화하려는 취약성 옆의 확인란을 선택합니다.

단계 **4** 페이지 하단의 **Review(**검토**)**를 클릭합니다.

관련 항목

개별 호스트용 취약성 비활성화
개별 취약성 비활성화

서드파티 취약성 데이터

Firepower System에는 자체 취약성 추적 데이터베이스가 포함되어 있습니다. 이 데이터베이스를 시스템의 핑거프린트 인식 기능과 함께 사용하면 네트워크의 호스트에 연결된 취약성을 식별할 수 있습니다.

서드파티 애플리케이션에서 가져온 네트워크 맵 데이터로 시스템의 취약성 데이터를 보강할 수 있습니다. 그러려면 조직이 스크립트를 작성하거나 명령줄 파일 가져오기를 만들어 데이터를 가져올 수 있어야 합니다. 자세한 내용은 *Firepower System Host Input API* 설명서을 참조하십시오.

가져온 데이터를 영향 상관관계에 포함하려면 서드파티 취약성 정보를 데이터베이스의 운영 체제 및 애플리케이션 정의에 매핑해야 합니다. 서드파티 취약성 정보를 클라이언트 정의에 매핑할 수는 없습니다.

서드파티 취약성 데이터 보기

호스트 입력 기능을 사용하여 서드파티 취약성 데이터를 가져왔으면 management center를 사용하여 서드파티 취약성의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 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.

서드파티 취약성에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 두 가지 사전 정의 워크플로가 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** 서드파티 취약성 데이터에 액세스합니다.

- 사전 정의된 워크플로를 사용 중인 경우 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Third-Party Vulnerabilities(**서드파티 취약성**)**를 선택합니다.

- 서드파티 취약성의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용하는 경우, **(switch workflow)(**워크플로 전환**)**를 클릭한 다음 **Vulnerabilities by Source(**소스별 취약성**)** 또는 **Vulnerabilities by IP Address(IP** 주소별 취약성**)**를 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 7 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(서드파티 취약성 데이터 필드, 45 페이지 참조).
- SVID 열에서 **View(**보기**)** (👁)를 클릭하여 서드파티 취약성의 취약성 세부 사항을 봅니다. 또는 취약성 ID를 제한하고 취약성 세부사항 페이지로 드릴다운합니다.

서드파티 취약성 데이터 필드

다음은 서드파티 취약성 테이블에서 보고 검색할 수 있는 필드에 대한 설명입니다.

Vulnerability Source

서드파티 취약성의 소스(예: QualysGuard 또는 NeXpose).

취약성 **ID**

소스의 취약성과 연결된 ID 번호.

IP 주소

취약성의 영향을 받는 호스트와 연결된 IP 주소.

Port(포트**)**

취약성이 특정 포트에서 실행 중인 서버와 연결된 경우 포트 번호.

Bugtraq ID

Bugtraq 데이터베이스의 취약성과 관련된 ID 번호입니다. (http://www.securityfocus.com/bid/)

CVE ID

MITRE CVE(Common Vulnerabilities and Exposures) 데이터베이스(https://cve.mitre.org/)의 취약성에 연결된 식별 번호.

SVID

시스템이 취약성 추적에 사용하는 레거시 취약성 식별 번호.

SVID에 대한 취약성 세부사항에 액세스하려면 **View(**보기**)** (👁)을 클릭합니다.

Snort ID

Snort ID(SID) 데이터베이스의 취약성에 연결된 ID 번호입니다. 즉, 침입 규칙이 특정 취약성을 악용하는 네트워크 트래픽을 탐지할 수 있으면 해당 취약성은 침입 규칙의 SID와 연결됩니다.

취약성은 둘 이상의 SID와 연결될 수 있습니다(SID와 연결되지 않을 수도 있음). 취약성이 둘 이상의 SID에 연결된 경우, 취약성 테이블에는 각 SID에 대한 행이 포함됩니다.

직함

취약성의 제목입니다.

설명

취약성에 대한 간단한 설명.

도메인

취약성이 있는 호스트의 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

개수

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

관련 항목

이벤트 검색

활성 세션, 사용자 및 사용자 활동 데이터

ID 소스는 활성 세션 데이터, 사용자 데이터, 사용자 활동 데이터를 수집합니다. 데이터는 개별 사용자 관련 워크플로에 표시됩니다.

- 활성 세션 - 이 워크플로는 네트워크의 모든 현재 사용자 세션을 표시합니다. 여러 활성 세션을 동시에 실행하는 단일 사용자는이 테이블에서 여러 행을 차지합니다. 이 워크플로에 표시되는 사용자 데이터 유형에 대한 자세한 내용은 활성 세션 데이터, 54 페이지를 참조하십시오.
- 사용자 - 이 워크플로는 네트워크에서 보이는 모든 사용자를 표시합니다. 단일 사용자는 이 테이블에서 단일 행을 차지합니다. 이 워크플로에 표시되는 사용자 데이터 유형에 대한 자세한 내용은 사용자 데이터, 55 페이지를 참조하십시오.
- 사용자 활동 - 이 워크플로는 네트워크에서 보이는 모든 사용자 활동을 표시합니다. 사용자 활동의 인스턴스가 여러 개 있는 단일 사용자는 이 테이블에서 여러 행을 차지합니다. 이 워크플로에 표시되는 사용자 활동 유형에 대한 자세한 내용은 사용자 활동 데이터, 58 페이지를 참조하십시오.

이러한 워크플로를 채우는 사용자 ID 소스에 대한 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참조하십시오.

사용자 관련 필드

사용자 관련 데이터는 활성 세션, 사용자, 사용자 활동 테이블에 표시됩니다.

표 *1:* 활성 세션, 사용자, 사용자 활동 필드 설명

필드	설명	활성 세션 테이블	사용자 테이블	사용자 활동 테이블
활성 세션 수	사용자와 연결된 활성 세션의 수.	아니요	예	아니요
인증 유형	인증 유형: `No Authentication(인증 없음)`, `Passive Authentication(패시브 인증)`, `Active Authentication(액티브 인증)`, `Guest Authentication(게스트 인증)`, `Failed Authentication(실패한 인증)` 또는 `VPN Authentication(VPN 인증)` 각 인증 유형에 지원되는 ID 소스에 대한 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드를 참조하십시오.	예	아니요	예
정책에 사용 가능	**Yes** 값은 사용자 저장소(예: Active Directory)에서 사용자가 검색되었음을 의미합니다. **No** 값은 management center가 해당 사용자의 로그인 보고를 수신했지만 해당 사용자가 사용자 저장소에 없음을 의미합니다. 이것이 일어날 수 있는 한 가지 방법은 제외된 그룹의 사용자가 사용자 저장소에 로그인하는 경우입니다. 영역을 구성할 때 그룹이 다운로드되는 것을 차단할 수 있습니다. 정책에 사용할 수 없는 사용자는 management center에 기록되지만 매니지드 디바이스에 전송되지 않습니다.	아니요	예	아니요
개수	참고 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 **Count(개수)** 필드가 표시됩니다. 테이블에 따라 특정 행에 표시되는 정보와 일치하는 세션, 사용자 또는 활동 이벤트의 수입니다.	예	예	예
현재 **IP**	사용자가 로그인하는 호스트와 연결된 IP 주소. 사용자의 활성 세션이 없는 경우 사용자 테이블에서 이 필드는 비어 있습니다.	예	예	아니요

필드	설명	활성 세션 테이블	사용자 테이블	사용자 활동 테이블
부서	영역에서 가져온 사용자의 부서. 서버의 사용자와 명시적으로 연결된 부서가 없는 경우, 부서는 서버가 할당하는 기본 그룹으로 나열됩니다. 예를 들면 Active Directory에서는 `Users (ad)` 입니다. 다음과 같은 경우 이 필드는 비어 있습니다. • 영역을 구성하지 않은 경우. • management center에서는 management center 데이터베이스의 사용자를 LDAP 레코드와 상호 연결할 수 없는 경우(예: AIM, Oracle 또는 SIP 로그인을 통해 데이터베이스에 추가된 사용자의 경우).	예	예	아니요
설명	세션, 사용자 또는 사용자 활동에 대한 추가 정보(제공되는 경우).	아니요	아니요	예
디바이스	트래픽 기반 탐지 또는 액티브 인증 ID 소스에서 탐지된 사용자 활동의 경우, 사용자를 식별한 디바이스의 이름입니다. 다른 사용자 활동 유형의 경우, 관리하는 management center. 참고 고가용성 구축에서 VPN을 구성한 경우 활성 VPN 세션에 대해 표시되는 디바이스 이름은 사용자 세션을 식별한 기본 또는 보조 디바이스일 수 있습니다.	예	아니요	예
검색 애플리케이션	사용자를 탐지하는 데 사용된 애플리케이션 또는 프로토콜. • 트래픽 기반 탐지에서 탐지된 사용자 활동의 경우 다음 중 하나에 해당: ldap, pop3, imap, oracle, sip, ftp, http, mdns, aim. 참고 사용자는 SMTP 로그인에 기반한 데이터베이스에 추가되지 않습니다. • 모든 기타 사용자 활동의 경우: ldap	예	예	예

필드	설명	활성 세션 테이블	사용자 테이블	사용자 활동 테이블
현재 **IP** 도메인/도메인	활성 세션 테이블에서 사용자 활동이 탐지된 멀티테넌시 도메인. 사용자 테이블에서 사용자의 영역과 연결된 멀티테넌시 도메인. 사용자 활동 테이블에서 사용자 활동이 탐지된 멀티테넌시 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.	예	예	예
이메일	사용자의 이메일 주소. 다음과 같은 경우 이 필드는 비어 있습니다. • AIM 로그인을 통해 사용자가 데이터베이스에 추가된 경우. • LDAP 로그인을 통해 사용자가 데이터베이스에 추가되었으며 LDAP 서버의 사용자와 연결된 이메일 주소가 없는 경우.	예	예	아니요
종료 포트	TS 에이전트에서 사용자를 보고하고 세션이 현재 활성화된 경우, 이 필드는 사용자에게 할당된 포트 범위의 종료 값을 식별합니다. 사용자의 TS 에이전트 세션이 비활성화되어 있거나 다른 ID 소스에서 사용자를 보고한 경우 이 필드는 비어 있습니다.	예	아니요	예
엔드포인트 위치	ISE에서 식별된 사용자를 인증하기 위해 ISE가 사용되는 네트워크 디바이스의 IP 주소. ISE를 구성하지 않은 경우 이 필드는 비어 있습니다.	아니요	아니요	예
엔드포인트 프로파일	Cisco ISE에서 식별된 사용자의 엔드포인트 디바이스 유형. ISE를 구성하지 않은 경우 이 필드는 비어 있습니다.	아니요	아니요	예
이벤트	사용자 활동 이벤트 유형.	아니요	아니요	예

필드	설명	활성 세션 테이블	사용자 테이블	사용자 활동 테이블
이름	영역에서 가져온 사용자의 이름. 다음과 같은 경우 이 필드는 비어 있습니다. • 영역을 구성하지 않은 경우. • management center에서는 management center 데이터베이스의 사용자를 LDAP 레코드와 상호 연결할 수 없는 경우(예: AIM, Oracle 또는 SIP 로그인을 통해 데이터베이스에 추가된 사용자의 경우). • 서버의 사용자와 연결된 이름이 없는 경우.	예	예	아니요
IP 주소	**User Login(**사용자 로그인**)** 사용자 활동의 경우, 로그인과 관련된 IP 주소 또는 내부 IP 주소: • LDAP, POP3, IMAP, FTP, HTTP, MDNS, AIM 로그인 — 사용자 호스트의 주소 • SMTP 및 Oracle 로그인 — 서버의 주소 • SIP 로그인 — 세션 시작 주체의 주소 IP 주소가 연결되어 있다고 해서 사용자가 해당 IP 주소의 현재 사용자라는 의미는 아닙니다. 권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	아니요	아니요	예
성	영역에서 가져온 사용자의 성. 다음과 같은 경우 이 필드는 비어 있습니다. • 영역을 구성하지 않은 경우. • management center에서는 management center 데이터베이스의 사용자를 LDAP 레코드와 상호 연결할 수 없는 경우(예: AIM, Oracle 또는 SIP 로그인을 통해 데이터베이스에 추가된 사용자의 경우). • 서버의 사용자와 연결된 성이 없는 경우.	예	예	아니요

필드	설명	활성 세션 테이블	사용자 테이블	사용자 활동 테이블
최종 확인	사용자의 세션이 마지막으로 시작된(또는 사용자 데이터가 업데이트된) 날짜 및 시간.	예	예	아니요
로그인 시간	사용자의 세션이 시작된 날짜 및 시간.	예	아니요	아니요
전화	영역에서 가져온 사용자의 전화 번호. 다음과 같은 경우 이 필드는 비어 있습니다. • 영역을 구성하지 않은 경우. • management center에서는 management center 데이터베이스의 사용자를 LDAP 레코드와 상호 연결할 수 없는 경우(예: AIM, Oracle 또는 SIP 로그인을 통해 데이터베이스에 추가된 사용자의 경우). • 서버의 사용자와 연결된 전화 번호가 없는 경우.	예	예	아니요
영역	사용자와 연결된 ID 영역. 참고 Azure AD 영역 사용자의 활성 세션은 **Active Sessions(**활성 세션**)** 새 UI 레이아웃에만 표시되며 레거시 UI에는 표시되지 않습니다.	예	예	예
보안 그룹 태그	패킷이 신뢰할 수 있는 TrustSec 네트워크에 들어갔을 때 Cisco TrustSec에서 적용한 SGT(Security Group Tag) 속성. ISE를 구성하지 않은 경우 이 필드는 비어 있습니다.	아니요	아니요	예
세션 기간	**Login Time(**로그인 시간**)**과 현재 시간에서 계산된 사용자 세션의 기간.	예	아니요	아니요
시작 포트	TS 에이전트에서 사용자를 보고하고 세션이 현재 활성화된 경우, 이 필드는 사용자에게 할당된 포트 범위의 시작 값을 식별합니다. 사용자의 TS 에이전트 세션이 비활성화되어 있거나 다른 ID 소스에서 사용자를 보고한 경우 이 필드는 비어 있습니다.	예	아니요	예
시간	시스템이 사용자 활동을 탐지한 시간.	아니요	아니요	예

필드	설명	활성 세션 테이블	사용자 테이블	사용자 활동 테이블
사용자	이 필드에는 최소한 사용자의 영역 및 사용자 이름이 표시됩니다. 예를 들어 `Lobby\jsmith`의 경우 Lobby는 영역이고 jsmith는 사용자 이름입니다. 영역이 LDAP 서버에서 사용자 추가 데이터를 다운로드하고 시스템이 이를 사용자와 연결할 경우, 이 필드에는 또한 사용자의 이름, 성, 유형이 표시됩니다. 예를 들어 `John Smith (Lobby\jsmith, LDAP)`의 경우 John Smith는 사용자의 이름이고 LDAP는 유형입니다. 참고 트래픽 기반 탐지는 실패한 AIM 로그인을 기록할 수 있으므로, management center에서는 잘못된 AIM 사용자(예: 사용자가 사용자 이름의 철자를 잘못 쓴 경우)를 저장할 수 있습니다.	예	예	아니요
Username	사용자와 연결된 사용자 이름.	예	예	예
VPN 바이트 인	원격 액세스 VPN에서 보고된 사용자 활동의 경우, threat defense에서 원격 피어 또는 클라이언트로부터 수신된 총 바이트 수입니다. 참고 사용자의 VPN 세션이 종료되면 수신된 총 바이트 수를 볼 수 있습니다. 진행 중인 VPN 세션의 경우, 이는 동적 카운터가 아닙니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	아니요	아니요	예
VPN 바이트 아웃	원격 액세스 VPN에서 보고된 사용자 활동의 경우, threat defense에서 원격 피어 또는 클라이언트로 전송한 총 바이트 수입니다. 참고 사용자의 VPN 세션이 종료되면 전송한 총 바이트 수를 볼 수 있습니다. 진행 중인 VPN 세션의 경우, 이는 동적 카운터가 아닙니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	아니요	아니요	예
VPN 클라이언트 애플리케이션	원격 액세스 VPN에서 보고한 사용자 활동의 경우, 원격 사용자의 Cisco Secure Client의 AnyConnect VPN 애플리케이션입니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	예	아니요	예

필드	설명	활성 세션 테이블	사용자 테이블	사용자 활동 테이블
VPN 클라이언트 국가	원격 액세스 VPN에서 보고한 사용자 활동의 경우, Secure Client VPN에서 보고된 국가 이름입니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	아니요	아니요	예
VPN 클라이언트 **OS**	원격 액세스 VPN에서 보고한 사용자 활동의 경우, Secure Client VPN에서 보고된 원격 사용자의 엔드포인트 운영 체제입니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	예	아니요	예
VPN 클라이언트 공개 **IP**	원격 액세스 VPN에서 보고한 사용자 활동의 경우, 공개적으로 라우팅 가능한 Secure Client VPN 디바이스의 IP 주소입니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	예	아니요	예
VPN 연결 지속 시간	원격 액세스 VPN에서 보고한 사용자 활동의 경우, 세션이 활성화된 총 시간(HH:MM:SS)입니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	아니요	아니요	예
VPN 연결 프로파일	원격 액세스 VPN에서 보고한 사용자 활동의 경우, VPN 세션에서 사용된 연결 프로파일(터널 그룹)의 이름입니다. 연결 프로파일은 원격 액세스 VPN 정책의 일부입니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	예	아니요	예
VPN 그룹 정책	원격 액세스 VPN에서 보고한 사용자 활동의 경우, VPN 세션을 설정했을 때 클라이언트에 할당된 그룹 정책의 이름입니다. 이러한 정책은 VPN 연결 프로파일과 연결된 정적으로 할당된 그룹 정책이거나, RADIUS가 인증에 사용된 경우 동적으로 할당된 그룹 정책입니다. RADIUS 서버에서 할당한 경우, 이 그룹 정책은 VPN 연결 프로파일에 구성된 고정 정책을 재정의합니다. 그룹 정책은 원격 액세스 VPN 정책의 사용자 그룹에 대한 일반 속성을 구성합니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	예	아니요	예
VPN 세션 유형	원격 액세스 VPN에서 보고한 사용자 활동의 경우, 세션의 유형(LAN 대 LAN 또는 원격)입니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	예	아니요	예

활성 세션 데이터

Analysis(분석**)** > **Users(**사용자**)** > **Active Sessions(**활성 세션**)** 워크플로에는 현재 사용자 세션에 대한 선택 정보가 표시됩니다. 네트워크의 한 사용자가 여러 세션을 동시에 실행 중인 경우, Firepower System은 세션이 다음과 같은 상태인지 여부를 고유하게 식별할 수 있습니다.

- 세션에 고유한 **IP Address(IP** 주소**)** 값이 있는지 식별합니다.
- 세션에 Cisco TS(Terminal Services) 에이전트에서 제공한 고유한 **Start Port(**시작 포트**)** 및 **End Port(**종료 포트**)** 값이 있는지 식별합니다.
- 세션에 고유한 **Current IP Domain(**현재 **IP** 도메인**)** 값이 있는지 식별합니다.
- 다른 ID 소스에서 인증되었는지 식별합니다.
- 다른 ID 영역과 연결되었는지 식별합니다.

시스템에 저장된 사용자 및 사용자 활동 데이터에 대한 자세한 내용은 사용자 데이터, 55 페이지 및 사용자 활동 데이터, 58 페이지를 참조하십시오.

일반적인 사용자 관련 이벤트 문제 해결 및 원격 액세스 VPN 문제 해결에 대한 자세한 내용은 영역 및 사용자 다운로드 트러블슈팅및 *VPN* 트러블슈팅을 참조하십시오.

활성 세션 데이터 보기

활성 세션의 테이블을 본 후, 찾고 있는 정보에 따라 이벤트 보기를 조작할 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.

사용자에게 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 탐지된 모든 사용자를 나열하는 사용자의 테이블 보기를 포함하며 사용자 세부사항 페이지에서 종료되는 사전 정의 워크플로를 사용할 수 있습니다. 사용자 세부사항 페이지는 제약 조건을 충족하는 모든 사용자에 대한 정보를 제공합니다.

프로시저

단계 **1** 사용자 데이터에 액세스합니다.

- 사전 정의 워크플로우를 사용하는 경우 **Analysis(**분석**)** > **Users(**사용자**)** > **Active Sessions(**활동 세션**)**를 클릭합니다.
- 활성 세션의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭한 다음, **Active Sessions(**활성 세션**)**를 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 7 페이지 참조).

- 테이블의 열에 대한 내용을 자세히 알아보십시오(활성 세션 데이터, 54 페이지 및 사용자 관련 필드, 47 페이지 참조).

사용자 데이터

ID 소스가 아직 데이터베이스에 없는 사용자의 사용자 로그인을 보고하면, 이러한 로그인 유형을 특별히 제한하지 않은 경우 해당 사용자는 데이터베이스에 추가됩니다.

시스템은 다음 중 한 가지 상황이 발생할 경우 사용자 데이터베이스를 업데이트합니다.

- management center의 사용자가 사용자 테이블에서 권한 없는 사용자를 수동으로 삭제합니다.
- ID 소스가 해당 사용자의 로그오프를 보고합니다.
- 영역은 영역의 **User Session Timeout: Authenticated Users(**사용자 세션 시간 초과**:** 인증된 사용자**)**, **User Session Timeout: Failed Authentication Users(**사용자 세션 시간 초과**:** 실패한 인증 사용자**)** 또는 **User Session Timeout: Guest Users(**사용자 세션 시간 초과**:** 게스트 사용자**)** 설정에서 지정된 대로 사용자 세션을 종료합니다.

참고 ISE/ISE-PIC를 구성한 경우, 사용자 테이블에 호스트 데이터가 표시될 수 있습니다. ISE/ISE-PIC에서는 호스트 탐지를 일부만 지원하므로, ISE에서 보고한 호스트 데이터를 사용하여 사용자 제어를 수행할 수 없습니다.

시스템에서 탐지한 사용자 로그인의 유형은 새로운 사용자에 대해 어떤 정보를 저장할지 결정합니다.

ID 소스	로그인 유형	저장되는 사용자 데이터
ISE/ISE-PIC	Active Directory LDAP RADIUS RSA	• 사용자 이름 • 현재 IP 주소 • SGT(Security Group Tag) — ISE-PIC에서 지원되지 않음 • 엔드포인트 프로파일/디바이스 유형 — ISE-PIC에서 지원되지 않음 • 엔드포인트 위치/위치 IP — ISE-PIC에서 지원되지 않음 • 유형(LDAP)

ID 소스	로그인 유형	저장되는 사용자 데이터
TS 에이전트	Active Directory	• 사용자 이름 • 현재 IP 주소 • 시작 포트 • 종료 포트 • 유형(LDAP)
캡티브 포털	Active Directory LDAP	• 사용자 이름 • 현재 IP 주소 • 유형(LDAP)
트래픽 기반 탐지	LDAP AIM Oracle SIP HTTP FTP MDNS	• 사용자 이름 • 현재 IP 주소 • 유형(AD)
	POP3 IMAP	• 사용자 이름 • 현재 IP 주소 • 이메일 주소 • 유형(`pop3` 또는 `imap`)

참고 이 테이블에는 Microsoft Azure Active Directory 사용자에 대한 데이터가 표시되지 않습니다.

사용자를 자동으로 다운로드하도록 영역을 구성할 경우, management center에서는 지정된 간격을 기준으로 서버를 쿼리합니다. 시스템에서 새 사용자 로그인을 탐지한 후 management center 데이터베이스에서 사용자 메타데이터를 업데이트하는 데 5~10분 정도 걸릴 수 있습니다. management center에서는 각 사용자에 대한 다음과 같은 정보 및 메타데이터를 얻습니다.

- 사용자 이름
- 이름 및 성
- 이메일 주소

- department
- 전화번호
- 현재 IP 주소
- SGT(Security Group Tag) - 제공되는 경우
- 엔드포인트 프로파일 - 제공되는 경우
- 엔드포인트 위치 - 제공되는 경우
- 시작 포트 - 제공되는 경우
- 종료 포트 - 제공되는 경우

management center에서 데이터베이스에 저장할 수 있는 사용자 수는 management center 모델에 따라 다릅니다. 권한 없는 사용자가 호스트에 로그인한 것이 탐지되면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 해당 호스트에서 권한 있는 사용자 로그인이 탐지되면, 또 다른 권한 있는 사용자 로그인만이 현재 사용자를 변경합니다.

AIM, Oracle, SIP 로그인의 트래픽 기반 탐지는 시스템이 LDAP 서버에서 가져오는 사용자 메타데이터와 연결되지 않으므로 중복 사용자 레코드를 생성합니다. 이러한 프로토콜의 중복 사용자 레코드로 인한 사용자 수 남용을 방지하려면, 해당 프로토콜을 무시하도록 트래픽 기반 탐지를 구성합니다.

데이터베이스에서 사용자를 검색하고 보고 삭제할 수 있습니다. 또한 데이터베이스에서 모든 사용자를 삭제할 수도 있습니다.

일반적인 사용자 관련 이벤트 문제 해결에 대한 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드을 참조하십시오.

사용자 데이터 보기

사용자의 테이블을 본 후, 찾고 있는 정보에 따라 이벤트 보기를 조작할 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.

사용자에게 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 탐지된 모든 사용자를 나열하는 사용자의 테이블 보기를 포함하며 사용자 세부사항 페이지에서 종료되는 사전 정의 워크플로를 사용할 수 있습니다. 사용자 세부사항 페이지는 제약 조건을 충족하는 모든 사용자에 대한 정보를 제공합니다.

프로시저

단계 **1** 사용자 데이터에 액세스합니다.

- 사전 정의된 워크플로를 사용 중인 경우 **Analysis(분석)** > **Users(사용자)** > **Users(사용자)**를 선택합니다.

- 사용자의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭한 다음 **Users(**사용자**)**를 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 7 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(사용자 관련 필드, 47 페이지 참조).

사용자 활동 데이터

시스템은 네트워크에서 사용자 활동의 세부사항을 전달하는 이벤트를 생성합니다. 시스템이 사용자 활동을 탐지하면 사용자 활동 데이터가 데이터베이스에 로깅됩니다. 사용자 활동을 보고 검색하고 삭제할 수 있습니다. 또한 데이터베이스에서 모든 사용자 활동을 삭제할 수도 있습니다.

사용자가 네트워크에 최초로 나타나면 시스템은 사용자 활동 이벤트를 로깅합니다. 해당 사용자가 다음번에 나타날 경우에는 새로운 사용자 활동 이벤트를 로깅하지 않습니다. 그러나 사용자의 IP 주소가 변경되면 시스템은 새로운 사용자 활동 이벤트를 로깅합니다.

또한, 시스템은 사용자 활동을 다른 이벤트 유형과 서로 연관시킵니다. 예를 들어, 침입 이벤트는 이벤트 발생 시점에 소스 및 대상 호스트에 로그인한 사용자를 알려줄 수 있습니다. 이러한 상관관계를 통해 공격 대상인 호스트에 로그인한 사용자, 또는 내부 공격이나 포트스캔을 시작한 사용자를 알 수 있습니다.

상관관계 규칙에서 사용자 활동을 사용할 수도 있습니다. 사용자 활동 및 지정한 다른 기준을 기반으로 상관관계 규칙을 작성할 수 있습니다. 상관관계 정책에서 사용할 경우 이러한 규칙은 네트워크 트래픽이 조건을 충족하면 교정과 알림 응답을 실행합니다.

참고 ISE/ISE-PIC를 구성한 경우, 사용자 테이블에 호스트 데이터가 표시될 수 있습니다. ISE/ISE-PIC에서는 호스트 탐지를 일부만 지원하므로, ISE에서 보고한 호스트 데이터를 사용하여 사용자 제어를 수행할 수 없습니다.

다음은 네 가지 유형의 사용자 활동 데이터에 대한 설명입니다.

새로운 사용자 **ID**

시스템이 데이터베이스에 없는 알 수 없는 사용자의 로그인을 탐지할 경우 이 유형의 이벤트가 생성됩니다.

사용자가 네트워크에 최초로 나타나면 시스템은 사용자 활동 이벤트를 로깅합니다. 해당 사용자가 다음번에 나타날 경우에는 새로운 사용자 활동 이벤트를 로깅하지 않습니다. 그러나 사용자의 IP 주소가 변경되면 시스템은 새로운 사용자 활동 이벤트를 로깅합니다.

사용자 로그인

다음 중 하나가 발생할 경우 이 유형의 이벤트가 생성됩니다.

- 캡티브 포털(captive portal)은 성공 또는 실패한 사용자 인증을 수행합니다.
- 트래픽 기반 탐지는 성공 또는 실패한 사용자 로그인을 탐지합니다.

참고 트래픽 기반 탐지에서 탐지된 SMTP 로그인은 데이터베이스에 이미 일치하는 이메일 주소의 사용자가 있지 않은 한 기록되지 않습니다.

권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다.

캡티브 포털(captive portal) 또는 트래픽 기반 탐지를 사용할 경우, 실패한 사용자 로그인 및 실패한 사용자 인증 데이터에 대한 다음 사항에 유의하십시오.

- 트래픽 기반 탐지(LDAP, IMAP, FTP 및 POP3 트래픽)에서 보고한 실패한 로그인은 사용자의 테이블 보기가 아닌 사용자 활동의 테이블 보기에 표시됩니다. 알려진 사용자가 로그인에 실패한 경우, 시스템은 사용자 이름으로 해당 사용자를 식별합니다. 알 수 없는 사용자가 로그인에 실패한 경우, 시스템은 **Failed Authentication(**실패한 인증**)**을 사용자 이름으로 사용합니다.
- 캡티브 포털(captive portal)에서 보고한 실패한 인증은 사용자 활동의 테이블 보기 및 사용자의 테이블 보기에 모두 표시됩니다. 알려진 사용자가 인증에 실패한 경우, 시스템은 사용자 이름으로 해당 사용자를 식별합니다. 알 수 없는 사용자가 인증에 실패한 경우, 시스템은 사용자가 입력한 사용자 이름으로 해당 사용자를 식별합니다.

사용자 **ID** 삭제

데이터베이스에서 사용자를 수동으로 삭제할 경우 이 유형의 이벤트가 생성됩니다.

User Identity Dropped: User Limit Reached(사용자 **ID** 차단**:** 사용자 한계 도달**)**

시스템이 데이터베이스에 없는 사용자를 탐지했지만, management center 모델에서 확인된 데이터베이스의 사용자 최대 수에 도달했기 때문에 해당 사용자를 추가할 수 없는 경우 이 유형의 이벤트가 생성됩니다.

사용자 제한에 도달하면 대부분의 경우 시스템에서는 데이터베이스에 새 사용자를 추가하지 않습니다. 새 사용자를 추가하려면 데이터베이스에서 오래된 사용자 또는 비활성 사용자를 수동으로 삭제하거나 모든 사용자를 삭제해야 합니다.

그러나 시스템은 권한 있는 사용자를 선호합니다. 제한에 도달한 상태에서 시스템이 전에 탐지하지 못한 권한 있는 사용자의 로그인을 탐지하면, 오랫동안 비활성 상태를 유지한 권한 없는 사용자를 삭제하고 새로운 권한 있는 사용자를 대신 추가합니다.

사용자 보안 침해 지표 이벤트

다음과 같은 사용자 IOC 변경 사항은 사용자 활동 데이터베이스에 로깅됩니다.

- 보안 침해 지표가 해결된 경우
- 사용자에 대해 보안 침해 지표 규칙이 활성화 또는 비활성화된 경우

일반적인 사용자 관련 이벤트 문제 해결에 대한 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참조하십시오.

사용자 활동 데이터 보기

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

사용자 활동의 테이블을 본 후, 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다. 사용자 활동에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 사용자 활동의 테이블 보기를 포함하며 사용자 세부사항 페이지(제약 조건을 충족하는 모든 사용자에 대한 사용자 세부사항 포함)에서 종료되는 사전 정의 워크플로를 사용할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** 사용자 활동 데이터에 액세스합니다.

- 사전 정의된 워크플로를 사용 중인 경우 **Analysis(분석)** > **Users(사용자)** > **User Activity(사용자의 활동)**를 선택합니다.
- 사용자 활동의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 **(switch workflow)(워크플로 전환)**를 클릭한 다음 **User Activity(사용자 활동)**를 선택합니다.

팁 이벤트가 표시되지 않을 경우 시간 범위를 조정해야 할 수 있습니다. 타임 윈도우 변경을 참조하십시오.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(워크플로 전환)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 7 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(사용자 관련 필드, 47 페이지 참조).

사용자 프로파일 및 호스트 기록

User(사용자) 팝업 창을 통해 특정 사용자에 대해 자세히 알아볼 수 있습니다. 이 문서에서 "User Profile"이라고 하는 표시되는 페이지의 웹 인터페이스에서의 제목은 "User Identity"입니다.

다음에서 창을 표시할 수 있습니다.

- 사용자 데이터를 다른 종류의 이벤트와 연결하는 이벤트 보기
- 활성 세션의 테이블 보기
- 사용자의 테이블 보기

사용자 정보는 사용자 워크플로의 종료 페이지에도 나타납니다.

표시되는 사용자 데이터는 사용자의 테이블 보기에 표시되는 것과 동일합니다.

보안 침해 지표 섹션

이 섹션에 대한 정보는 다음을 참조하십시오.

- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 보안 침해 지표
- 보안 침해 지표 데이터 필드, 28 페이지
- 단일 호스트 또는 사용자에 대한 보안 침해 지표 규칙 상태 수정, 29 페이지
- 보안 침해 지표 태그 해결, 30 페이지
- 보안 침해 지표 태그의 소스 이벤트 보기, 30 페이지

호스트 기록 섹션

호스트 기록은 사용자 활동의 마지막 24시간을 그래프로 보여줍니다. 사용자가 로그인하고 로그오프한 호스트의 IP 주소 목록은 막대 그래프로 로그인 시간과 로그아웃 시간의 근사치를 계산합니다. 일반 사용자는 하루에 수차례 호스트에 로그인 및 로그오프할 수 있습니다. 예를 들어, 메일 서버에 대한 정기적인 자동 로그인은 여러 개의 짧은 세션으로 표시되고, 좀 더 긴 로그인(예: 근무 시간 중)은 더 긴 세션으로 표시될 수 있습니다.

트래픽 기반 탐지 또는 캡티브 포털을 사용하여 실패한 로그인을 캡처하는 경우, 호스트 기록에는 사용자가 로그인에 실패한 호스트도 포함됩니다.

호스트 기록을 생성하는 데 사용된 데이터는 사용자 기록 데이터베이스에 저장됩니다. 이 데이터베이스에는 기본적으로 1,000만 개의 사용자 로그인 이벤트가 저장됩니다. 특정 사용자에 대한 호스트 기록에 데이터가 없는 경우, 사용자가 비활성 상태이거나 데이터베이스 한도를 늘려야 할 수 있습니다.

관련 항목

사용자 데이터 필드

사용자 상세정보 및 호스트 기록 보기

프로시저

다음 2가지 옵션을 사용할 수 있습니다.

- 사용자를 나열하는 이벤트 보기에서 사용자 ID 옆에 표시되는 사용자 아이콘 또는 보안 침해 지표에 연결된 사용자의 경우, 빨간색 사용자 아이콘을 클릭합니다.

- 사용자 워크플로에서 Users 종료 페이지를 클릭합니다.

검색 이벤트 작업 히스토리

표 *2:*

기능	버전	최소 **Threat Defense**	세부 사항
취약점 페이지 변경	6.7	Any(모든)	

기능	버전	최소 **Threat Defense**	세부 사항
			Bugtraq 및 취약점 데이터는 더 이상 사용할 수 없습니다. 다음과 같이 변경되었습니다. • 현재 대부분의 취약점 데이터는 NVD(National Vulnerability Database)에서 제공됩니다. • 사용되지 않는 필드와 중복된 필드가 제거되었습니다. • 새 CVE ID 열이 테이블 보기에 추가되었으며 새 심각도 필드가 테이블 및 세부 사항 페이지에 추가되었습니다. • 이제 테이블에서 CVE ID를 마우스 오른쪽 버튼으로 클릭하여 NVD의 취약점에 대한 세부 정보를 볼 수 있습니다. • 테이블의 취약점 영향 열의 이름이 Impact로 변경되었습니다. (세부 사항 보기의 필드 이름은 변경되지 않습니다.) • Analysis(분석) > Hosts(호스트) > Network Map(네트워크 맵) > Hosts(호스트)에서 호스트 프로파일의 취약점을 볼 때 취약점에 대한 세부 정보(타사 취약점 제외)는 새로운 필드 집합을 사용합니다. • Bugtraq 옵션이 Analysis(분석) > Hosts(호스트) > Network Map(네트워크 맵) > Vulnerabilities(취약점) 페이지의 취약점 옵션에서 제거되었습니다. 수정된 화면: • Analysis(분석)> Hosts(호스트)> Vulnerabilities(취약점) 아래의 모든 페이지 • Hosts and Vulnerabilities(호스트 및 취약점) 탭의 Analysis(분석)> Hosts(호스트)> Network Map(네트워크 맵) 페이지

기능	버전	최소 **Threat Defense**	세부 사항
			지원되는 플랫폼: management center