네트워크 검색 개요

다음 주제에서는 네트워크 검색에 대해 설명합니다.

호스트, 애플리케이션 및 사용자 데이터 탐지 정보

Firepower System은 네트워크 검색과 *ID* 정책을 이용해 네트워크 상의 트래픽에 대한 호스트, 애플리케이션, 사용자 데이터를 수집합니다. 특정 유형의 검색 및 ID 데이터를 이용해 네트워크 자산에 대한 포괄적인 맵을 만들고, 포렌식 분석과 행동 프로파일링 및 액세스 컨트롤을 수행하고, 취약성을 완화하고 취약성에 대처하며, 조직이 취약한 부분을 활용할 수 있습니다.

호스트 및 애플리케이션 데이터

호스트와 애플리케이션 데이터는 네트워크 검색 정책의 설정을 바탕으로 호스트 ID 소스 및 애플리케이션 탐지기가 수집합니다. 매니지드 디바이스는 사용자가 지정한 네트워크 세그먼트의 트래픽을 관찰합니다.

자세한 내용은 호스트 및 애플리케이션 탐지 기초, 2 페이지를 참고하십시오.

사용자 데이터

사용자 데이터는 네트워크 검색 및 ID 정책에 따라 사용자 ID 소스가 수집합니다. 이 데이터는 사용자 인식과 사용자 제어에 활용할 수 있습니다.

자세한 내용은 사용자 ID 정보를 참고하십시오.

로그 검색 및 ID 데이터를 이용하면 다음과 같은 Firepower System의 다양한 기능을 활용할 수 있습니다.

- 네트워크 맵 보기 - 호스트와 네트워크 디바이스, 호스트 특성, 애플리케이션 프로토콜 또는 취약성을 그룹화하여 네트워크 자산 및 토폴로지를 자세히 볼 수 있습니다.
- 애플리케이션 및 사용자 제어 수행 - 애플리케이션, 영역, 사용자, 사용자 그룹, ISE 속성 조건을 이용해 액세스 컨트롤 규칙을 작성합니다.
- 호스트 프로파일 보기 - 탐지된 호스트에 사용할 수 있는 모든 정보를 완전하게 보여줍니다.

- 대시보드 보기 - (가장 중요한) 네트워크 자산과 사용자 활동을 한눈에 보는 기능을 제공합니다.
- 시스템이 로깅한 검색 이벤트 및 사용자 활동에 대한 자세한 정보를 확인합니다.
- 호스트 및 서버나 이들이 실행하는 클라이언트를 취약한 익스플로잇에 연결합니다.

  이렇게 하면 취약성을 확인 및 완화하고, 침입 이벤트가 네트워크에 주는 영향을 평가하고, 침입 규칙 상태를 조정해 네트워크 자산에 대한 보호를 극대화할 수 있습니다.
- 시스템이 특정 영향 플래그와 함께 침입 이벤트를 생성하거나 특정 검색 이벤트를 생성할 경우 이메일, SNMP 트랩 또는 시스템 로그를 통해 알림을 전송합니다.
- 허용되는 운영체제, 클라이언트, 애플리케이션 프로토콜 및 프로토콜의 허용리스트로 조직의 규정준수를 모니터링합니다.
- 시스템이 검색 이벤트를 생성하거나 사용자 활동을 탐지할 때 상관관계 이벤트를 트리거 및 생성하는 규칙으로 상관관계 정책을 생성합니다.
- 적용 가능한 경우 NetFlow 로깅 및 사용 연결도 사용합니다.

호스트 및 애플리케이션 탐지 기초

호스트 및 애플리케이션 탐지를 수행 하려면 네트워크 검색 정책을 구성할 수 있습니다.

자세한 내용은 개요: 호스트 데이터 수집 및 개요: 애플리케이션 탐지의 내용을 참조하십시오.

운영 체제 및 호스트 데이터의 수동 탐지

수동 탐지는 네트워크 트래픽을(그리고 내보낸 전체 NetFlow 데이터를) 분석해 네트워크 맵을 작성하는, 시스템의 기본 방법입니다. 수동 탐지는 운영체제와 실행 중인 애플리케이션 같은, 네트워크 자산에 대한 상황에 맞는 정보를 제공합니다.

모니터링하는 호스트에서 오는 트래픽이 호스트의 운영체제에 대한 결정적 증거를 제공하지 않는다면, 네트워크 맵은 가장 가능성이 높은 운영체제를 표시합니다. 예를 들어 NAT 디바이스는 호스트가 NAT 디바이스 "뒤에" 있기 때문에, 여러 운영체제를 실행하는 것처럼 보일 수 있습니다. 판단의 정확도를 높이기 위해 시스템은 탐지한 운영체제 각각에 자신이 할당한 신뢰도 값과, 탐지한 운영체제 간의 보강 데이터 양을 사용합니다.

참고 시스템은 보고된 "알 수 없는" 애플리케이션과 운영체제는 판단할 때 고려하지 않습니다.

수동 탐지가 네트워크 자산을 올바르게 식별하지 못한다면, 매니지드 디바이스의 배치를 확인해 보십시오. 맞춤형 운영체제 지문과 맞춤형 애플리케이션 탐지기를 이용해 시스템의 수동 탐지 기능을 강화할 수도 있습니다. 또한 트래픽 분석에 기반을 두지 않지만 대신 스캔 결과 및 기타 정보 소스를 이용해 네트워크 맵을 바로 업데이트할 수 있는, 능동 탐지를 사용하는 방법도 있습니다.

운영 체제 및 호스트 데이터의 활성 탐지

능동 탐지는 활성 소스가 수집한 호스트 정보를 네트워크 맵에 추가합니다. 예를 들어 Nmap 스캐너를 사용하면 네트워크에서 대상으로 삼은 호스트를 능동적으로 스캔할 수 있습니다. Nmap은 호스트 상의 운영체제와 애플리케이션을 검색합니다.

또한 호스트 입력 기능을 사용하면 호스트 입력 데이터를 네트워크 맵에 능동적으로 추가할 수 있습니다. 호스트 입력 데이터에는 두 가지 카테고리가 있습니다.

- 사용자 입력 데이터 - Firepower System 사용자 인터페이스 통해 추가한 데이터입니다. 사용자 인터페이스를 통해 호스트의 운영체제나 애플리케이션 ID를 수정할 수 있습니다.
- 호스트 입력된 데이터를 가져오기-데이터 명령행 유틸리티를 사용 하 여 가져옵니다.

시스템은 각 활성 소스에 대해 하나의 ID를 유지합니다. 예를 들어 Nmap 스캔 인스턴스를 실행하면 이전 스캔 결과가 새 스캔 결과로 교체됩니다. 그러나 Nmap 스캔을 실행한 다음 그 결과를 명령줄을 통해 가져온 클라이언트의 데이터로 교체하면, 시스템은 Nmap 결과의 ID와 가져오기 클라이언트의 ID를 모두 유지합니다. 그런 다음 시스템은 네트워크 검색 정책에 설정된 우선순위를 사용하여 어떤 능동 ID를 현재 ID로 사용할 것인지 결정합니다.

사용자 입력은 서로 다른 사용자가 입력했다 하더라도 하나의 소스로 간주됩니다. 예를 들어 UserA가 호스트 프로파일을 통해 운영체제를 설정한 다음 UserB가 호스트 프로파일을 통해 정의를 변경하면, UserB가 설정한 정의가 유지되고 UserA가 설정한 정의는 폐기됩니다. 또한 사용자 입력은 다른 모든 활성 소스를 재정의하며, 존재하는 경우 현재 ID로 사용됩니다.

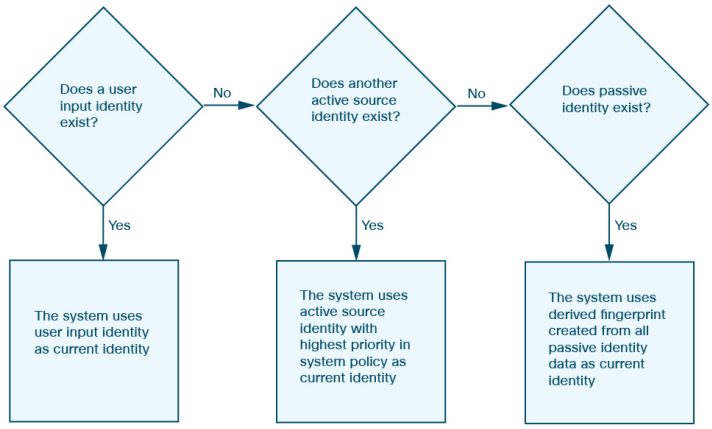
애플리케이션 및 운영 체제에 대한 현재 ID

호스트에 있는 애플리케이션 또는 운영체제의 현재 *ID*는 시스템이 가장 정확할 것이라고 판단하는 ID입니다.

시스템은 다음과 같은 용도로 운영체제 또는 애플리케이션에 대한 현재 ID를 사용합니다.

- 호스트에 취약성 할당
- 영향 평가
- 운영체제 식별, 호스트 프로파일 자격 및 규정준수 허용 목록에 대해 작성한 상관관계 규칙 평가 시
- 워크플로의 Hosts(호스트) 및 Servers(서버) 테이블 보기에서 표시
- 호스트 프로파일에서 표시
- Discovery Statistics(검색 통계) 페이지리 운영체제 및 애플리케이션 통계 계산

시스템은 어떤 능동 ID를 애플리케이션 또는 운영체제에 대한 현재 ID로 사용할지를 결정할 때 소스 우선순위를 사용합니다.



예를 들어 사용자가 호스트에서 운영체제를 Windows 2003 Server로 설정하면 Windows 2003 Server가 현재 ID가 됩니다. 해당 호스트의 Windows 2003 Server 취약성에 대한 공격에는 더 높은 영향이 지정되고, 호스트 프로파일의 해당 호스트에 대해 나열된 취약성에는 Windows 2003 Server 취약성이 포함됩니다.

데이터베이스에 호스트의 특정 운영체제 또는 특정 애플리케이션에 대한 여러 소스의 정보가 포함될 수 있습니다.

시스템은 데이터에 대한 소스가 가장 높은 소스 우선순위를 가지고 있을 때 운영체제 또는 애플리케이션 ID를 현재 ID로 취급합니다. 가능한 소스의 우선순위 순서는 다음과 같습니다.

1. 사용자

2. 스캐너 및 애플리케이션(네트워크 검색 정책에 설정됨)

3. 매니지드 디바이스

4 . Netflow 레코드

우선순위가 더 높은 새 애플리케이션 ID는 현재 ID보다 상세정보이 부족하면 현재 애플리케이션 ID를 재정의하지 않습니다.

또한 ID 충돌이 발생하는 경우 충돌의 해결은 네트워크 검색 정책의 설정 또는 수동 해결에 의존하게 됩니다.

현재 사용자 ID

시스템은 다른 사용자가 같은 호스트에 여러 번 로그인하는 경우를 탐지하면 특정 시점에 지정된 호스트에 한 명의 사용자만 로그인하며 호스트의 현재 사용자가 마지막 권한 있는 사용자 로그인이라고 가정합니다. 권한 없는 사용자 로그인만 호스트에 로그인한 경우, 권한 없는 최근 로그인이 현재 사용자로 간주됩니다. 원격 세션을 통해 여러 사용자가 로그인한 경우 서버에서 보고한 마지막 사용자가 management center에 보고됩니다.

같은 사용자가 동일 호스트에 여러 번 로그인했음이 탐지되는 경우 시스템은 특정 호스트에 대한 사용자의 첫 번째 로그인만 기록하고 이후의 로그인은 무시합니다. 개별 사용자가 특정 호스트에 로그인하는 유일한 사람인 경우, 시스템에서는 원래 로그인만 기록합니다.

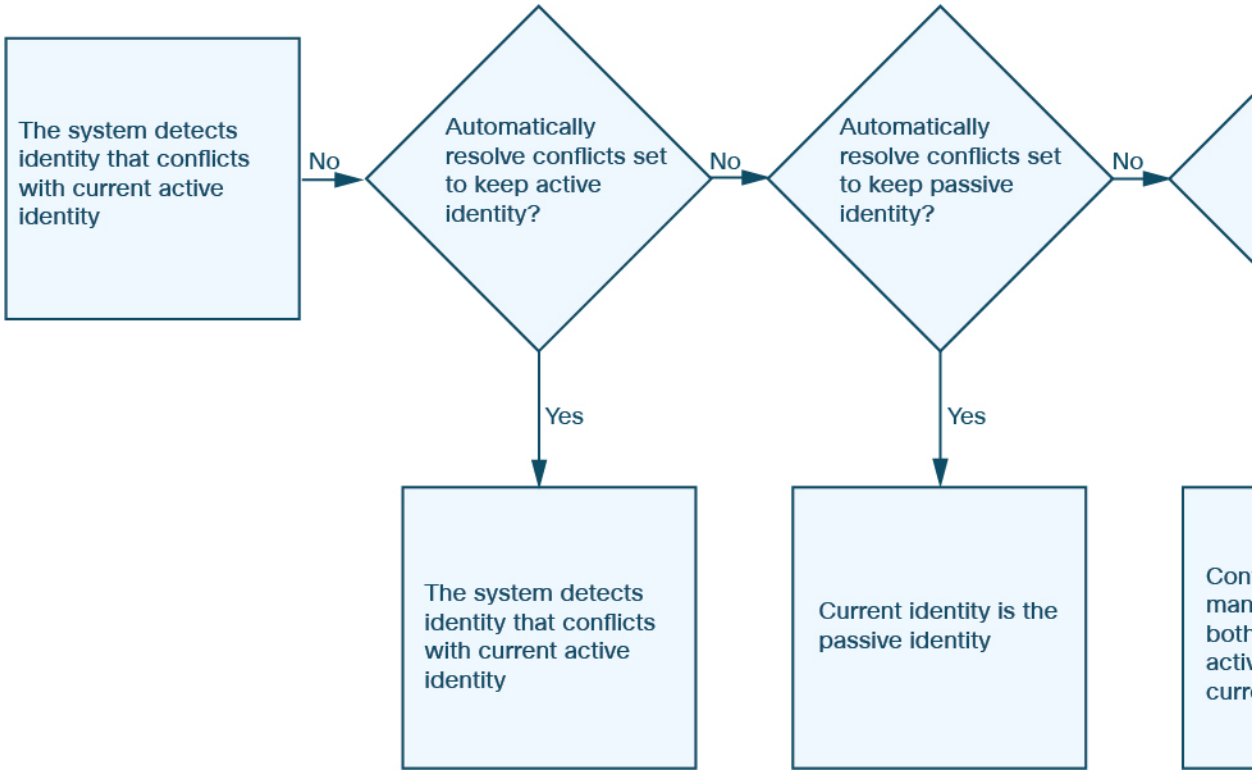
그러나 또 다른 사용자가 해당 호스트에 로그인하면 시스템에서는 새 로그인을 기록합니다. 그런 다음 원래 사용자가 다시 로그인하면 새 로그인이 기록됩니다.

애플리케이션 및 운영 체제 **ID** 충돌

시스템이 현재 능동 ID와 충돌하며 전에는 수동 ID로 보고되었던 새로운 수동 ID를 보고하면 *ID* 충돌이 발생합니다. 예를 들어 운영체제에 대한 이전 수동 ID가 Windows 2000으로 보고되면, Windows XP의 능동 ID가 현재 ID가 됩니다. 이후 시스템은 Ubuntu Linux 8.04.1의 새로운 수동 ID를 탐지합니다. 그러면 Windows XP와 Ubuntu Linux ID가 충돌하게 됩니다.

호스트의 운영체제 또는 호스트의 애플리케이션에서 ID 충돌이 발생하면, 시스템은 충돌이 해결될 때까지 충돌하는 두 ID를 모두 현재 ID로 나열하고 영향 평가에 두 ID를 모두 사용합니다.

관리자 권한이 있는 사용자는 항상 수동 ID를 사용하거나 항상 능동 ID를 사용하도록 선택하여 ID 충돌을 자동으로 해결할 수 있습니다. ID 충돌 자동 해결을 비활성화하지 않는 한 ID 충돌은 항상 자동으로 해결됩니다.



관리자 권한이 있는 사용자는 ID 충돌이 발생할 경우 이벤트를 생성하도록 시스템을 구성할 수도 있습니다. 그러면 해당 사용자는 Nmap 스캔을 상관관계 응답으로 사용하는 상관관계 규칙을 이용해 상관관계 정책을 설정할 수 있습니다. 이벤트가 발생하면 Nmap은 호스트를 스캔하여 업데이트된 호스트 운영체제 및 애플리케이션 데이터를 가져옵니다.

NetFlow 데이터

NetFlow는 라우터를 통과하여 이동하는 패킷에 대한 통계를 제공하는 Cisco IOS 애플리케이션입니다. 이는 Cisco 네트워킹 디바이스에서 제공되며 Juniper, FreeBSD, OpenBSD 디바이스에도 임베디드될 수 있습니다.

NetFlow가 네트워크 디바이스에서 활성화된 경우, 디바이스의 데이터베이스(NetFlow 캐시)는 라우터를 통과하는 플로우의 레코드를 저장합니다. 시스템에서 연결이라고도 하는 플로우는 특정 포트, 프로토콜, 애플리케이션 프로토콜을 사용하여 소스 호스트와 대상 호스트 간의 세션을 나타내는 연속된 패킷입니다. 이 NetFlow 데이터를 내보내도록 네트워크 디바이스를 구성할 수 있습니다. 이 문서에서는 이러한 방식으로 구성된 네트워크 디바이스를 *NetFlow* 엑스포터라고 합니다.

매니지드 디바이스를 구성하여 NetFlow 엑스포터에서 레코드를 수집하고, 이러한 레코드의 데이터를 바탕으로 단방향 연결 종료 이벤트를 생성하고, 마지막으로 해당 이벤트를 management center에 전송하여 연결 이벤트 데이터베이스에 로깅할 수 있습니다. NetFlow 연결의 정보를 기반으로 호스트 및 애플리케이션 프로토콜 정보를 데이터베이스에 추가하도록 네트워크 검색 정책을 구성할 수도 있습니다.

매니지드 디바이스에 의해 직접 수집된 데이터를 보완하기 위해 이 검색 및 연결 데이터를 사용할 수 있습니다. 이는 매니지드 디바이스에서 모니터링할 수 없는 NetFlow 엑스포터 모니터링 네트워크를 보유하고 있는 경우 특히 유용합니다.

NetFlow 데이터를 사용하기 위한 요건

NetFlow 데이터 분석을 위해 Firepower System을 구성하기에 앞서 사용하려는 라우터 또는 기타 NetFlow 지원 디바이스에서 NetFlow 기능을 활성화하고 매니지드 디바이스의 센싱 인터페이스가 연결된 대상 네트워크로 NetFlow 데이터를 브로드캐스트하도록 디바이스를 구성해야 합니다.

Firepower System은 NetFlow 버전 5 및 NetFlow 버전 9 레코드를 모두 구문 분석할 수 있습니다. 데이터를 Firepower System으로 내보내려는 경우 NetFlow 엑스포터는 반드시 다음 버전 중 하나를 사용해야 합니다. 또한, 내보낸 NetFlow 템플릿과 레코드에 특정 필드가 있어야 합니다. NetFlow 엑스포터가 버전 9(맞춤 설정 가능)를 사용 중인 경우, 내보낸 템플릿과 레코드에 다음 필드가 포함되어 있는지 반드시 확인해야 합니다(순서는 상관없음).

- IN_BYTES (1)
- IN_PKTS (2)
- PROTOCOL (4)
- TCP_FLAGS (6)
- L4_SRC_PORT (7)
- IPV4_SRC_ADDR (8)
- L4_DST_PORT (11)
- IPV4_DST_ADDR (12)
- LAST_SWITCHED (21)

- FIRST_SWITCHED (22)
- IPV6_SRC_ADDR (27)
- IPV6_DST_ADDR (28)

Firepower System은 매니지드 디바이스를 NetFlow 데이터 분석에 사용하므로, NetFlow 엑스포터를 모니터링할 수 있는 하나 이상의 매니지드 디바이스를 구축에 포함해야 합니다. 내보낸 NetFlow 데이터를 수집할 수 있는 네트워크에 이러한 매니지드 디바이스에 있는 하나 이상의 센싱 인터페이스를 연결해야 합니다. 매니지드 디바이스의 센싱 인터페이스에는 일반적으로 IP 주소가 없기 때문에 시스템은 NetFlow 레코드의 직접 수집을 지원하지 않습니다.

일부 네트워크 디바이스에서 사용 가능한 Sampled NetFlow 기능은 디바이스를 통과하는 패킷의 하위 집합에 대해서만 NetFlow 통계를 수집합니다. 이 기능을 활성화하면 네트워크 디바이스에서 CPU 사용률이 향상될 수 있지만, Firepower System의 분석을 위해 수집하는 NetFlow 데이터에 영향을 줄 수 있습니다.

NetFlow와 매니지드 디바이스 데이터의 차이점

NetFlow 데이터로 표시되는 트래픽은 직접 분석되지 않습니다. 대신, 내보낸 NetFlow 레코드를 연결 로그 및 호스트/애플리케이션 프로토콜 데이터로 변환합니다.

따라서 변환된 NetFlow 데이터와 매니지드 디바이스에서 직접 수집된 검색 및 연결 데이터 간에는 몇 가지 차이점이 있습니다. 다음 항목을 필요로 하는 분석을 수행할 경우 이러한 차이점에 유의해야 합니다.

- 탐지된 연결 수에 대한 통계
- 운영 체제 및 기타 호스트 관련 정보(취약성 포함)
- 클라이언트 정보, 웹 애플리케이션 정보, 공급업체 및 버전 서버 정보를 비롯한 애플리케이션 데이터
- 연결에서 어떤 호스트가 이니시에이터이고 어떤 호스트가 응답자인지 파악

네트워크 검색 정책과 액세스 제어 정책 비교

네트워크 검색 정책의 규칙을 사용하여 연결 로깅을 비롯한 NetFlow 데이터 수집을 구성합니다. 반면, 매니지드 디바이스에서 탐지된 연결에 대한 연결 로깅은 액세스 제어 규칙별로 구성합니다.

연결 이벤트 유형

NetFlow 데이터 수집은 액세스 제어 규칙이 아닌 네트워크에 연결되므로 시스템이 로깅하는 NetFlow 연결을 세분화된 방식으로 제어할 수 없습니다.

NetFlow 데이터는 보안 인텔리전스 이벤트를 생성할 수 없습니다.

NetFlow 기반 연결 이벤트는 연결 이벤트 데이터베이스에만 저장할 수 있으며 시스템 로그 또는 SNMP 트랩 서버로 전송할 수 없습니다.

모니터링되는 세션별로 생성되는 연결 이벤트 수

매니지드 디바이스에서 직접 탐지된 연결의 경우 연결의 시작이나 끝 중 하나 또는 시작과 끝 둘 다에서 양방향 연결 이벤트를 로깅하도록 액세스 제어 규칙을 구성할 수 있습니다.

반면, 내보낸 NetFlow 레코드는 단방향 연결 데이터를 포함하므로 시스템은 처리하는 각 NetFlow 레코드에 대해 최소 두 개의 연결 이벤트를 생성합니다. 따라서 NetFlow 데이터 기반의 각 연결에 대해 요약의 연결 수가 2씩 증가하므로, 네트워크에서 실제로 발생하는 연결 수보다 많은 개수가 제공됩니다.

NetFlow 엑스포터는 연결이 계속 진행되는 중이라도 고정된 간격으로 레코드를 출력하므로, 세션이 오랫동안 실행되는 경우 여러 레코드를 내보낼 수 있으며 각 레코드가 연결 이벤트를 생성합니다. 예를 들어 NetFlow 엑스포터가 5분마다 내보내기를 실행하는데 특정 연결이 12분 동안 지속될 경우 해당 세션에 대해 연결 이벤트 6개가 생성됩니다.

- 첫 번째 5분 동안 이벤트 쌍 하나
- 두 번째 5분 동안 이벤트 쌍 하나
- 연결이 종료될 때 마지막 쌍

호스트 및 운영 체제 데이터

NetFlow 데이터에서 네트워크 맵에 추가되는 호스트에는 운영 체제, NetBIOS 또는 호스트 유형(호스트 디바이스 또는 네트워크 디바이스) 정보가 없습니다. 그러나 호스트 입력 기능을 사용하여 호스트의 운영 체제를 수동으로 설정할 수 있습니다.

응용프로그램 데이터

매니지드 디바이스에서 직접 탐지하는 연결의 경우, 시스템은 연결의 패킷을 검토하여 애플리케이션 프로토콜, 클라이언트 및 웹 애플리케이션을 식별할 수 있습니다.

시스템은 NetFlow 레코드를 처리할 때 애플리케이션 프로토콜 ID를 추정하기 위해 `/etc/sf/services`의 포트 상관관계를 사용합니다. 그러나 그러한 애플리케이션 프로토콜에 대한 공급업체 또는 버전 정보가 없으며, 연결 로그에는 세션에서 사용된 클라이언트 또는 웹 애플리케이션에 대한 정보가 포함되지 않습니다. 그러나 호스트 입력 기능을 사용해 이러한 정보를 수동으로 제공할 수 있습니다.

단순한 포트 상관관계는, 비표준 포트에서 실행 중인 애플리케이션 프로토콜이 식별되지 않거나 잘못 식별될 수 있음을 의미합니다. 또한 상관관계가 존재하지 않는 경우 시스템은 연결 로그에서 애플리케이션 프로토콜을 `unknown`으로 표시합니다.

취약성 매핑

호스트 입력 기능을 사용하여 호스트의 운영 체제 ID 또는 애플리케이션 프로토콜 ID를 수동으로 설정하지 않으면 시스템이 NetFlow 엑스포터에서 모니터링하는 호스트에 취약성을 매핑할 수 없습니다. NetFlow 연결에는 클라이언트 정보가 없으므로 클라이언트 취약성을 NetFlow 데이터에서 생성된 호스트와 연결할 수 없습니다.

연결의 이니시에이터 및 Responder 정보

매니지드 디바이스에서 직접 탐지하는 연결의 경우, 시스템은 어떤 호스트가 이니시에이터(또는 소스)인지, 그리고 어떤 호스트가 responder(또는 대상)인지를 식별할 수 있습니다. 그러나 NetFlow 데이터에는 이니시에이터 또는 responder 정보가 포함되어 있지 않습니다.

시스템은 NetFlow 기록을 처리할 때 특정 알고리즘을 사용하여 각 호스트에서 사용 중인 포트 및 해당 포트가 잘 알려진 포트인지 여부를 기반으로 이 정보를 확인합니다.

- 사용 중인 두 포트 모두 잘 알려진 포트이거나 둘 다 잘 알려진 포트가 아닌 경우 시스템은 낮은 번호의 포트를 사용하는 호스트를 responder로 간주합니다.
- 호스트 중 하나만 잘 알려진 포트인 경우 시스템은 이 호스트를 responder로 간주합니다.

따라서 잘 알려진 포트는 1~1023 범위의 포트이거나 매니지드 디바이스에서 `/etc/sf/services`에 애플리케이션 프로토콜 정보를 포함하는 포트입니다.

또한 매니지드 디바이스에서 직접 탐지된 연결의 경우 해당 연결 이벤트에 다음과 같이 두 개의 바이트 수가 기록됩니다.

- **Initiator Bytes(**이니시에이터 바이트**)** 필드에는 전송된 바이트가 기록됩니다.
- **Responder Bytes(Responder** 바이트**)** 필드에는 수신된 바이트가 기록됩니다.

단방향 NetFlow 레코드를 기반으로 하는 연결 이벤트는 한 개의 바이트 수만 포함합니다. 시스템은 포트 기반 알고리즘에 따라 이 개수를 **Initiator Bytes(**이니시에이터 바이트**)** 또는 **Responder Bytes(Responder** 바이트**)**에 할당합니다. 다른 필드는 0으로 설정됩니다. NetFlow 레코드의 연결 요약(집계된 연결 데이터)을 확인하는 경우에는 두 필드에 모두 정보가 입력되어 있을 수 있습니다.

NetFlow 전용 연결 이벤트 필드

일부 필드는 NetFlow 레코드에서 생성된 연결 이벤트에만 표시됩니다.에서 참조하십시오.