호스트 프로파일

다음 주제에서는 호스트 프로파일을 사용하는 방법에 설명합니다.

호스트 프로파일에 대한 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자

- 보안 분석가

호스트 프로파일

호스트 프로파일은 시스템이 단일 호스트에 대해 수집한 모든 정보를 완벽하게 보여줍니다. 호스트 프로파일을 액세스하려면

- 아무 네트워크 맵 보기에서 해당 프로파일로 이동합니다.
- 모니터링되는 네트워크 상의 호스트 IP 주소를 포함하는 아무 이벤트 보기에서 해당 프로파일로 이동합니다.

호스트 프로파일은 탐지한 호스트 또는 디바이스에 대한 (호스트 이름 또는 MAC 주소 같은) 기본 정보를 제공합니다. 라이선스 및 시스템 설정에 따라, 호스트 프로파일은 다음 정보를 제공하기도 합니다.

- 호스트에서 실행 중인 운영체제
- 호스트에서 실행 중인 서버
- 호스트에서 실행 중인 클라이언트 및 웹 애플리케이션
- 호스트에서 실행 중인 프로토콜
- 호스트의 보안 침해 지표(IOC) 태그
- 호스트의 VLAN 태그
- 네트워크에서의 최근 24시간 동안의 사용자 활동
- 호스트와 관련된 규정준수 허용리스트 위반
- 호스트에 대한 가장 최근의 악성코드 이벤트
- 호스트와 관련된 취약성
- 호스트에 대한 Nmap 스캔 결과

호스트 속성은 프로파일에도 나열됩니다. 호스트 속성을 사용하면 네트워크 환경에서 중요한 방법으로 호스트를 분류할 수 있습니다. 예를 들어, 다음이 가능합니다.

- 호스트가 위치한 건물을 나타내는 호스트 속성을 할당합니다.
- 호스트 중요도 특성을 사용하여 특정 호스트의 비즈니스 중요도를 할당하고 호스트 중요도를 기반으로 상관관계 정책 및 알림을 맞춤화합니다.

호스트 프로파일에서 해당 호스트에 적용된 기존 호스트 속성을 보고 호스트 속성 값을 수정합니다.

적응형 프로파일 업데이트을(를) 수동 침입 방지 배포의 일부로 사용하는 경우, 시스템이 트래픽을 수정하는 방식을 호스트와 서버 및 호스트를 실행하는 클라이언트의 운영체제에 가장 적합하게 조정할 수 있습니다.

선택적으로, 호스트 프로파일에서 Nmap 스캔을 수행하여 호스트 프로파일의 서버 및 운영체제 정보를 보강할 수도 있습니다. Nmap 스캐너는 호스트를 적극적으로 조사하여 호스트에서 실행 중인 운영체제와 서버에 대한 정보를 가져옵니다. 스캔 결과는 호스트에 대한 운영체제 및 서버 ID의 목록에 추가됩니다.

관련 항목

호스트 프로파일 보기, 3 페이지

호스트 프로파일 제한

사용할 수 없는 호스트

네트워크의 모든 호스트에 대해 호스트 프로파일을 이용할 수 있는 것은 아닙니다. 대표적인 가능한 원인:

- 시간 초과되어 호스트가 네트워크 맵에서 삭제됨
- 호스트 제한에 도달함
- 호스트가 네트워크 검색 정책에서 모니터링하지 않는 네트워크 세그먼트에 상주함

사용할 수 없는 정보

호스트 프로파일에 표시되는 정보는 호스트 유형 및 호스트에 대해 사용 가능한 정보에 따라 달라질 수 있습니다.

예를 들면 다음과 같습니다.

- 시스템에서 비 IP 기반 프로토콜(예: STP, SNAP, IPX)을 탐지한 경우, 호스트는 네트워크 맵에 MAC 호스트로 추가되는데 이 경우 IP 호스트에 비해 사용 가능한 정보가 훨씬 적습니다.
- 시스템에서는 내보낸 NetFlow 기록에서 네트워크 맵에 호스트를 추가할 수 있지만, 이러한 호스트에 사용할 수 있는 정보는 제한됩니다. NetFlow와 매니지드 디바이스 데이터의 차이점의 내용을 참조하십시오.

(VRF를 실행하는 구축**)** 단일 **IP** 주소가 여러 호스트를 나타낼 수 있습니다**.**

VRF를 실행하는 디바이스에서 호스트를 보고했다면, 단일 IP 주소가 실제로는 여러 호스트를 나타낼 수 있습니다. VRF는 중복 IP 주소가 있는 여러 네트워크를 모니터링할 수 있으므로, 동일한 IP 주소가 서로 다른 네트워크에 존재할 수 있습니다.

호스트 프로파일 보기

프로시저

다음 2가지 옵션을 사용할 수 있습니다.

- 네트워크 맵에서 프로파일을 보려는 호스트의 IP 주소로 드릴다운합니다.

- 이벤트 보기에서 프로필을 보려는 호스트의 IP 주소 옆에 있는 **Host Profile(**호스트 프로파일**)** 또는 **Compromised Host(**손상된 호스트**)**를 클릭합니다.

호스트 프로파일의 기본 호스트 정보

각 호스트 프로파일은 탐지된 호스트 또는 기타 디바이스에 대한 기본 정보를 제공합니다.

다음은 각각의 기본 호스트 프로파일 필드에 대한 설명입니다.

도메인

호스트와 연결된 도메인.

IP 주소

호스트와 연결된 모든 IP 주소(IPv4 및 IPv6). 시스템은 호스트와 연결된 IP 주소를 탐지하며, 지원되는 경우 동일한 호스트에 의해 사용되는 여러 IP 주소를 그룹화합니다. IPv6 호스트에는 흔히 2개 이상의 IPv6 주소(로컬 전용 및 전역 라우팅 가능)가 있으며 IPv4 주소도 있을 수 있습니다. IPv4 전용 호스트에는 여러 개의 IPv4 주소가 있을 수 있습니다.

호스트 프로파일에는 해당 호스트와 연결된 모든 탐지된 IP 주소가 나열됩니다. 사용 가능한 경우, 라우팅 가능한 호스트 IP 주소에는 해당 주소에 연결된 지오로케이션 데이터를 나타내는 국가 코드 및 플래그 아이콘도 포함될 수 있습니다.

기본적으로 처음 3개 주소만 표시됩니다. 호스트의 모든 주소를 표시하려면 **show all(**모두 표시**)**을 클릭하십시오.

호스트 이름

알려진 경우 호스트의 정규화된 도메인 이름.

NetBIOS 이름

사용 가능한 경우 호스트의 NetBIOS 이름. Microsoft Windows 호스트는 물론 Macintosh, Linux 또는 NetBIOS를 사용하도록 구성된 기타 플랫폼은 NetBIOS 이름을 가질 수 있습니다. 예를 들어 Samba 서버로 구성된 Linux 호스트는 NetBIOS 이름을 가질 수 있습니다.

디바이스**(**홉**)**

다음 중 하나에 해당합니다.

- 네트워크 검색 정책에 정의된 대로 호스트가 상주하는 네트워크에 대한 보고 디바이스 또는
- 호스트를 네트워크 맵에 추가한 NetFlow 데이터를 처리한 디바이스

디바이스 이름 뒤에 호스트를 탐지한 디바이스와 호스트 자체 간 네트워크 홉의 수가 괄호로 표시됩니다. 여러 디바이스가 호스트를 볼 수 있는 경우 보고 디바이스는 굵은 글꼴로 표시됩니다.

이 필드가 비어 있는 경우는 다음 중 하나입니다.

- 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.

MAC 주소(TTL)

호스트의 탐지된 MAC 주소 및 관련 NIC 공급업체, NIC의 하드웨어 공급업체와 현재 TTL(time-to-live) 값은 괄호로 표시됩니다.

여러 디바이스가 호스트를 탐지한 경우, 이를 보고한 디바이스와 상관없이 management center에서는 호스트에 연결된 모든 MAC 주소 및 TTL 값을 표시합니다.

MAC 주소가 굵은 글꼴로 표시된 경우, MAC 주소는 호스트의 실제/참/기본 MAC 주소이며, ARP 및 DHCP 트래픽을 통한 탐지에 의해 IP 주소에 확실히 연결됩니다.

굵은 글꼴로 표시되지 않은 MAC 주소는 호스트의 IP 주소에 확실히 연결될 수 없는 보조 주소입니다. 예를 들어 Firepower 디바이스는 자신의 네트워크 세그먼트에 있는 호스트의 MAC 주소만 획득할 수 있으므로 Firepower 디바이스가 직접 연결되지 않은 네트워크 세그먼트에서 트래픽이 시작되는 경우, 관찰된 MAC 주소(즉, 라우터 MAC 주소)는 호스트의 보조 MAC 주소로 표시됩니다.

호스트 유형

호스트, 모바일 디바이스, 탈옥 모바일 디바이스, 라우터, 브리지, NAT 디바이스 또는 로드 밸런서 등 시스템이 탐지한 디바이스의 유형.

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.
- 시스템이 모바일 디바이스를 구분하기 위해 사용하는 방법은 다음과 같습니다.
- 모바일 디바이스의 모바일 브라우저에서 HTTP 트래픽의 User-Agent(사용자 에이전트) 문자열 분석
- 특정 모바일 애플리케이션의 HTTP 트래픽 모니터링

네트워크 디바이스 또는 모바일 디바이스로 식별되지 않는 디바이스는 호스트로 분류됩니다.

최종 확인

호스트의 IP 주소가 마지막으로 탐지된 날짜 및 시간.

Current User(현재 사용자**)**

가장 최근에 이 호스트에 로그인한 사용자.

기존의 현재 사용자가 권한 있는 사용자가 아닌 경우, 호스트에 로그인한 권한 없는 사용자는 호스트에서 현재 사용자로만 등록됩니다.

보기

연결, 검색, 악성코드 및 침입 이벤트 데이터의 보기에 대한 링크. 해당 이벤트 유형에 대해 기본 워크플로를 사용하며 호스트와 관련된 이벤트를 표시하도록 제한됩니다. 가능한 경우 이러한 이벤트에는 호스트와 연결된 모든 IP 주소가 포함됩니다.

호스트 프로파일의 운영 체제

시스템은 호스트에 의해 생성되는 트래픽에서 네트워크 및 애플리케이션 스택을 분석하거나 사용자 에이전트에 의해 보고된 호스트 데이터를 분석하여 호스트에서 실행되는 운영 체제의 ID를 수동적으로 탐지합니다. 시스템은 또한 Nmap 스캐너 또는 호스트 입력 기능을 통해 가져온 애플리케이션 데이터 등의 다른 소스에서 운영 체제 정보를 취합합니다. 사용할 ID를 결정할 때 시스템은 각 ID 소스에 할당된 우선순위를 고려합니다. 기본적으로 사용자 입력의 우선순위가 가장 높고, 그다음은 애플리케이션 또는 스캐너 소스, 그다음은 검색된 ID입니다.

트래픽 및 기타 ID 소스는 더 구체적인 ID에 대해 충분한 정보를 제공하지 않으므로 때때로 시스템은 특정한 운영 체제보다는 일반적인 운영 체제 정의를 제공합니다. 시스템은 가능한 한 가장 자세한 정의를 사용하기 위해 여러 소스의 정보를 취합합니다.

운영 체제는 호스트의 취약성 목록과 호스트를 대상으로 하는 이벤트에 대한 이벤트 영향 상관 관계에 영향을 미치기 때문에 더 구체적인 운영 체제 정보를 수동으로 제공하는 것이 좋습니다. 또한 운영 체제에 수정(예: 서비스 팩 및 업데이트)이 적용되었음을 나타낼 수 있고, 수정에 의해 해결된 취약성을 무효화할 수 있습니다.

예를 들어 시스템에서 호스트의 운영 체제를 Microsoft Windows 2003으로 식별했지만 실제로 호스트에서는 Microsoft Windows XP Professional 서비스 팩 2가 실행되고 있음을 알고 있는 경우, 운영 체제 ID를 올바르게 설정할 수 있습니다. 운영 체제 ID를 더 구체적으로 설정하면 호스트의 취약성 목록이 세부적으로 조정되므로, 해당 호스트에 대한 영향 상관 관계가 더 구체적이고 정확해집니다.

시스템이 호스트의 운영 체제 정보를 탐지하고 그 정보가 활성 소스에 의해 제공된 현재 운영 체제 ID와 충돌하는 경우, ID 충돌이 발생합니다. ID 충돌이 발생하면 시스템에서는 취약성과 영향 상관 관계에 두 ID를 모두 사용합니다.

NetFlow 엑스포터가 모니터링하는 호스트의 네트워크 맵에 검색 데이터를 추가하도록 네트워크 검색 정책을 구성할 수 있습니다. 하지만 호스트 입력 기능을 사용하여 운영 체제 ID를 설정하지 않는 한 사용할 수 있는 이러한 호스트의 운영 체제 데이터는 없습니다.

활성화된 네트워크 검색 정책의 규정준수 허용리스트를 위반하는 운영체제가 호스트에서 실행되고 있는 경우, management center에서는 해당 운영체제 정보를 허용리스트 **Violation(**위반**)**으로 표시합니다. 또한 탈옥 모바일 디바이스가 활성 허용리스트를 위반하면 디바이스의 운영체제 옆에 아이콘이 나타납니다.

호스트의 운영 체제 ID에 대해 맞춤형 표시 문자열을 설정할 수 있습니다. 그러면 해당 표시 문자열이 호스트 프로파일에 사용됩니다.

참고 호스트의 운영체제 정보를 변경하면 규정준수 허용리스트 준수도 변경될 수 있습니다.

네트워크 디바이스의 호스트 프로파일에서 Operating Systems 섹션의 레이블이 Systems로 변경되며 추가 Hardware 열이 나타납니다. Systems 아래에 하드웨어 플랫폼에 대한 값이 나열되면 해당 시스템은 네트워크 디바이스 뒤에서 탐지된 하나 이상의 모바일 디바이스를 나타냅니다. 모바일 디바이스에는 하드웨어 플랫폼 정보가 있을 수도 있고 없을 수도 있지만, 모바일 디바이스가 아닌 시스템에 대해서는 하드웨어 플랫폼 정보가 탐지되지 않습니다.

다음은 호스트 프로파일에 표시되는 운영 체제 정보 필드에 대한 설명입니다.

Hardware(하드웨어)

모바일 디바이스용 하드웨어 플랫폼.

OS Vendor/Vendor

운영 체제의 공급업체입니다.

OS Product/Product

다음 값 중 하나:

- 모든 소스에서 수집한 ID 데이터에 기반할 때 호스트에서 실행되고 있을 가능성이 가장 높다고 판단되는 운영 체제
- 시스템이 아직 운영 체제를 식별하지 못했고 사용 가능한 다른 ID 데이터가 없는 경우 `Pending`
- 시스템이 운영 체제를 식별할 수 없고 운영 체제에 대해 사용 가능한 다른 ID 데이터가 없는 경우 `unknown`

참고 호스트의 운영 체제를 시스템이 탐지할 수 없는 경우 Cisco Secure Firewall Management Center 디바이스 구성 가이드호스트 *ID* 소스 장을 참고하십시오.

OS Version/Version

운영 체제 버전. 호스트가 탈옥 모바일 디바이스인 경우, 버전 뒤에 괄호로 `Jailbroken`이 표시됩니다.

소스

다음 값 중 하나:

- 사용자: user_name
- 애플리케이션: app_name

- 스캐너: scanner_type (Nmap 또는 기타 스캐너)
- Firepower

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

운영 체제 ID 보기

호스트에 대해 추가되거나 검색된 특정 운영 체제 ID를 볼 수 있습니다. 시스템은 호스트에 대한 현재 ID를 확인하기 위해 소스 우선순위를 사용합니다. ID 목록에서 현재 ID는 굵은 글꼴로 강조 표시됩니다.

View(보기**)**는 호스트에 여러 운영체제 ID가 존재하는 경우에만 사용할 수 있습니다.

프로시저

단계 **1** 호스트 프로파일의 **Operating System(**운영 체제**)** 또는 **Operating System Conflicts(**운영 체제 충돌**)** 섹션에서 **View(**보기**)**를 클릭합니다.

단계 **2** 호스트 프로파일의 운영 체제, 6 페이지에 설명된 정보를 봅니다.

단계 **3** 원하는 경우, 운영체제 ID 옆에 있는 **Delete(**삭제**)** ( )를 클릭합니다.

참고 Cisco가 탐지한 운영 체제 ID는 삭제할 수 없습니다.

시스템은 Operating System Identity Information(운영 체제 ID 정보) 팝업 창에서 ID를 삭제하고, 해당되는 경우, 호스트 프로파일에서 운영 체제의 현재 ID를 업데이트합니다.

현재 운영 체제 ID 설정

Firepower System 웹 인터페이스를 사용하여 호스트의 현재 운영 체제 ID를 설정할 수 있습니다. 웹 인터페이스를 통해 ID를 설정하면 취약성 평가 및 영향 상관 관계에 ID가 사용될 수 있도록 다른 모든 ID 소스가 재정의됩니다. 그러나 사용자가 운영 체제를 수정한 후 시스템에서 호스트에 대해 충돌하는 운영 체제 ID를 탐지하면 운영 체제 충돌이 발생합니다. 이 경우 사용자가 충돌을 해결할 때까지 두 운영 체제 모두 현재 운영 체제로 간주됩니다.

프로시저

단계 **1** 호스트 프로파일의 **Operating System(**운영 체제**)** 섹션에서 **Edit(**수정**)**를 클릭합니다.

단계 **2** 다음과 같은 몇 가지 옵션이 있습니다.

- 호스트 입력을 통해 현재 운영 체제 ID를 확인하려면 **OS Definition(OS** 정의**)** 드롭다운 목록에서 **Current Definition(**현재 정의**)**을 선택하고 6단계로 건너뜁니다.
- **OS Definition(OS** 정의**)** 드롭다운 목록에서 현재 운영 체제 ID에 대한 변형을 선택하고 6단계로 건너뜁니다.

- **OS Definition(OS** 정의**)** 드롭다운 목록에서 **User-Defined(**사용자 정의**)**를 선택하고 3단계를 계속 진행합니다.

단계 **3** 원하는 경우, **Use Custom Display String(**맞춤형 표시 문자열 사용**)**을 선택하고 **Vendor String(**공급업체 문자열**)**, **Product String(**제품 문자열**)** 및 **Version String(**버전 문자열**)** 필드에 표시할 맞춤형 문자열을 수정합니다.

단계 **4** 원하는 경우, 다른 공급업체의 운영 체제로 변경하려면 **Product(**제품**)** 드롭다운 목록에서 **Vendor(**공급업체**)**를 선택합니다.

단계 **5** 원하는 경우, 운영 체제 제품 릴리스 수준을 구성하려면 **Major(**메이저**)**, **Minor(**마이너**)**, **Revision(**수정**)**, **Build(**빌드**)**, **Patch(**패치**)** 및 **Extension(**확장**)** 드롭다운 목록에서 선택합니다.

단계 **6** 원하는 경우, 운영 체제의 수정이 적용되었음을 표시하려면 **Configure Fixes(**수정 구성**)**를 클릭합니다.

단계 **7** 드롭다운 목록에서 해당 수정을 선택하고 **Add(**추가**)**를 클릭합니다.

단계 **8** 원하는 경우, **Patch(**패치**)** 및 **Extension(**확장**)** 드롭다운 목록을 사용하여 관련 패치와 확장을 추가합니다.

단계 **9** **Finish(**종료**)**를 클릭합니다.

관련 항목

운영 체제 ID 충돌, 9 페이지

운영 체제 ID 충돌

현재 ID가 스캐너, 애플리케이션, 사용자 등의 활성 소스에 의해 제공된 경우, 시스템이 탐지한 새 ID가 현재 ID와 충돌하면 운영 체제 ID 충돌이 발생합니다.

충돌하는 운영 체제 ID 목록은 호스트 프로파일에서 굵은 글꼴로 표시됩니다.

시스템 웹 인터페이스를 통해 ID 충돌을 해결하고 호스트의 현재 운영 체제 ID를 설정할 수 있습니다. 웹 인터페이스를 통해 ID를 설정하면 취약성 평가 및 영향 상관 관계에 ID가 사용될 수 있도록 다른 모든 ID 소스가 재정의됩니다.

충돌하는 운영 체제 ID를 현재 ID로 만들기

프로시저

단계 **1** 호스트 프로파일의 **Operating System(**운영 체제**)** 섹션으로 이동합니다.

단계 **2** 다음 2가지 옵션을 사용할 수 있습니다.

- 호스트의 운영 체제로 설정하려는 운영 체제 ID 옆에 있는 **Make Current(**현재 **ID**로 만들기**)**를 클릭합니다.
- 현재 ID로 지정하지 않으려는 ID가 활성 소스에서 온 것이면 원하지 않는 ID를 삭제합니다.

운영 체제 ID 충돌 해결

프로시저

단계 1 호스트 프로파일의 **Operating System(**운영 체제**)** 섹션에서 **Resolve(**해결**)**를 클릭합니다.

단계 2 다음 옵션을 이용할 수 있습니다.

- 호스트 입력을 통해 현재 운영 체제 ID를 확인하려면 **OS Definition(OS** 정의**)** 드롭다운 목록에서 **Current Definition(**현재 정의**)**을 선택하고 6단계로 건너뜁니다.
- **OS Definition(OS** 정의**)** 드롭다운 목록에서 충돌하는 운영 체제 ID 중 하나의 변형을 선택하고 6단계로 건너뜁니다.
- **OS Definition(OS** 정의**)** 드롭다운 목록에서 **User-Defined(**사용자 정의**)**를 선택하고 3단계를 계속 진행합니다.

단계 3 원하는 경우, **Use Custom Display String(**맞춤형 표시 문자열 사용**)**을 선택하고 **Vendor String(**공급업체 문자열**)**, **Product String(**제품 문자열**)** 및 **Version String(**버전 문자열**)** 필드에 표시할 맞춤형 문자열을 입력합니다.

단계 4 원하는 경우, 다른 공급업체의 운영 체제로 변경하려면 **Product(**제품**)** 드롭다운 목록에서 **Vendor(**공급업체**)**를 선택합니다.

단계 5 원하는 경우, 운영 체제 제품 릴리스 수준을 구성하려면 **Major(**메이저**)**, **Minor(**마이너**)**, **Revision(**수정**)**, **Build(**빌드**)**, **Patch(**패치**)** 및 **Extension(**확장**)** 드롭다운 목록에서 선택합니다.

단계 6 원하는 경우, 운영 체제의 수정이 적용되었음을 표시하려면 **Configure Fixes(**수정 구성**)**를 클릭합니다.

단계 7 적용한 수정을 수정 목록에 추가합니다.

단계 8 **Finish(**종료**)**를 클릭합니다.

호스트 프로파일의 서버

호스트 프로파일의 서버 섹션에는 모니터링되는 네트워크의 호스트에서 탐지되거나 내보낸 NetFlow 레코드에서 추가되거나 스캐너 또는 호스트 입력 기능 같은 활성 소스를 통해 추가된 서버가 나열됩니다.

목록은 호스트당 최대 100개의 서버를 포함할 수 있습니다. 이 제한에 도달하면 호스트에서 서버를 삭제하거나 서버가 시간 초과될 때까지 소스의 새 서버 정보(능동이든 수동이든)가 폐기됩니다.

Nmap을 사용하여 호스트를 스캔하면 Nmap은 열린 TCP 포트에서 실행되는, 전에 탐지되지 않은 서버의 결과를 Servers(서버) 목록에 추가합니다. Nmap 스캔을 수행하거나 Nmap 결과를 가져오는 경우, 호스트 프로파일에 Scan Results(스캔 결과) 섹션도 나타나며, 여기에 Nmap 스캔에 의해 호스트에서 탐지된 서버 정보가 나열됩니다. 또한 네트워크 맵에서 호스트가 삭제되면 호스트에 대한 해당 서버의 Nmap 스캔 결과가 삭제됩니다.

참고 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 프로파일의 서버 작업 프로세스는 프로파일에 액세스하는 방법에 따라 달라집니다.

- 네트워크 맵을 통해 드릴다운하여 호스트 프로파일에 액세스하는 경우, 굵은 글꼴로 강조 표시된 서버 이름과 함께 해당 서버에 대한 세부사항이 나타납니다. 호스트의 다른 서버에 대한 세부사항을 보려면 해당 서버 이름 옆에 있는 **View(**보기**)** ( )를 클릭합니다.
- 다른 방법으로 호스트 프로필에 액세스하는 경우, Servers(서버) 섹션을 확장하고 세부 사항을 보려는 서버 옆에 있는 **View(**보기**)** ( )를 클릭합니다.

참고 활성화된 상관관계 정책의 규정준수 허용리스트를 위반하는 서버가 호스트에서 실행되고 있는 경우, management center에서는 규정을 준수하지 않는 서버를 허용리스트 **Violation(**위반**)**으로 표시합니다.

다음은 Servers(서버) 목록의 열에 대한 설명입니다.

프로토콜

서버가 사용하는 프로토콜의 이름.

Port(포트**)**

서버가 실행하는 포트.

애플리케이션 프로토콜

다음 중 하나에 해당합니다.

- 애플리케이션 프로토콜의 이름
- 여러 이유 중 하나 때문에 시스템이 애플리케이션 프로토콜을 긍정적으로 또는 부정적으로 식별할 수 없는 경우 `pending`
- 알려진 애플리케이션 프로토콜 지문을 기반으로 시스템이 애플리케이션 프로토콜을 식별할 수 없거나 서버 추가 없이 포트 정보와 함께 취약성을 추가하여 호스트 입력을 통해 해당 서버가 추가된 경우 `unknown`

마우스를 애플리케이션 프로토콜 이름 위로 이동하면 태그가 표시됩니다.

Vendor and Version

시스템, Nmap 또는 다른 활성 소스에 의해 식별되었거나 호스트 입력 기능을 통해 수집된 벤더 및 버전. 사용 가능한 소스 중 ID를 제공한 소스가 없으면 필드는 비어 있게 됩니다.

호스트 프로파일의 서버 상세정보

management center는 서버당 최대 16개의 수동 탐지 ID를 나열합니다. 수동 탐지 소스에는 네트워크 검색 데이터 및 NetFlow 레코드가 포함됩니다. 시스템이 서버에 대해 여러 공급업체 또는 버전을 탐지하는 경우 해당 서버는 여러 수동 ID를 가질 수 있습니다. 예를 들어 웹 서버가 서버 소프트웨어와 동일한 버전을 실행하지 않는 경우, 매니지드 디바이스와 웹 서버 팜 간 로드 밸런서를 사용하면 시스템은 HTTP에 대해 여러 수동 ID를 식별하게 될 수 있습니다. management center는 사용자 입력, 스캐너 또는 기타 애플리케이션 등 활성 소스에서 오는 서버 ID의 수를 제한하지 않습니다.

현재 ID는 management center에서 굵은 글꼴로 표시됩니다. 시스템은 호스트에 취약성을 할당하고, 영향 평가를 수행하고, 호스트 프로파일 자격 및 규정준수 허용리스트에 대해 작성된 상관관계 규칙을 평가하는 등 여러 용도로 서버의 현재 ID를 사용합니다.

서버 세부사항에는 선택한 서버에 대해 알려진 업데이트된 하위 서버 정보도 표시될 수 있습니다.

서버 세부사항에는 서버 배너도 표시될 수 있습니다. 이 배너는 호스트 프로파일에서 서버를 볼 때 서버 세부사항 아래에 표시됩니다. 서버 배너는 서버 식별에 도움이 될 수 있는, 서버에 대한 추가 정보를 제공합니다. 공격자가 고의로 서버 배너 문자열을 변경하면 시스템이 서버를 식별하지 못하거나 잘못된 서버를 탐지할 수 있습니다. 서버 배너에는 서버에 대해 탐지된 첫 번째 패킷의 처음 256바이트가 표시됩니다. 이러한 정보는 시스템에서 서버를 처음 탐지할 때 한 번만 수집됩니다. 배너 내용은 왼쪽에는 16진수로, 오른쪽에는 ASCII로 표시되어 두 열에 나타납니다.

참고 서버 배너를 보려면 네트워크 검색 정책에서 **Capture Banners(**배너 캡처**)** 확인란을 활성화해야 합니다. 이 옵션은 기본적으로 비활성화되어 있습니다.

호스트 프로파일의 서버 세부정보 섹션에는 다음 정보가 포함됩니다.

프로토콜

서버가 사용하는 프로토콜의 이름.

Port(포트**)**

서버가 실행하는 포트.

Hits(히트**)**

매니지드 디바이스 또는 Nmap 스캐너에 의해 서버가 탐지된 횟수. 호스트 입력을 통해 가져온 서버에 대한 트래픽을 시스템에서 탐지하지 못하면 해당 서버의 히트 수는 0입니다.

Last Used(최종 사용**)**

서버가 마지막으로 탐지된 시간 및 날짜. 시스템이 서버에 대해 새 트래픽을 탐지하지 못하면 호스트 입력 데이터의 마지막 사용 시간은 초기 데이터 가져오기 시간을 반영합니다. 호스트 입력 기능을 통해 가져온 스캐너 및 애플리케이션 데이터는 management center 구성에 따라 시간 초과되지만 management center 웹 인터페이스를 통한 사용자 입력은 시간 초과되지 않습니다.

애플리케이션 프로토콜

알려진 경우, 서버에서 사용하는 애플리케이션 프로토콜의 이름.

Vendor(벤더**)**

서버 공급업체. 공급업체가 알려지지 않은 경우 이 필드는 나타나지 않습니다.

버전

서버 버전. 버전이 알려지지 않은 경우 이 필드는 나타나지 않습니다.

소스

다음 값 중 하나:

- 사용자: user_name
- 애플리케이션: app_name
- 스캐너: scanner_type (Nmap 또는 기타 스캐너)
- 시스템에서 탐지된 어플라이언스의 `Firepower`, `Firepower Port Match` 또는 `Firepower Pattern Match`
- NetFlow 레코드에서 네트워크 맵에 추가된 서버의 `NetFlow`

시스템에서는 서버의 ID를 확인하기 위해 여러 소스의 데이터를 조정할 수 있습니다.

서버 상세정보 보기

프로시저

호스트 프로파일의 **Servers(**서버**)** 섹션 옆에 있는 **View(**보기**)** ( )을 클릭합니다.

서버 **ID** 수정

호스트의 서버에 대한 ID 설정을 수동으로 업데이트하고, 수정으로 해결된 취약성을 제거하도록 호스트에 적용한 수정을 구성할 수 있습니다. 서버 ID를 삭제할 수도 있습니다.

ID를 삭제해도 서버는 삭제되지 않습니다(유일한 ID를 삭제하는 경우에도). ID를 삭제하면 Server Detail(서버 세부정보) 팝업 창에서 ID가 제거되며, 해당되는 경우 호스트 프로파일에서 서버의 현재 ID가 업데이트됩니다.

Cisco가 관리하는 디바이스에 의해 추가된 서버 ID는 수정 또는 삭제할 수 없습니다.

프로시저

단계 **1** 호스트 프로파일의 **Servers(**서버**)** 섹션으로 이동합니다.

단계 **2** Server Details(서버 세부정보) 팝업 창을 열려면 **View(**보기**)**를 클릭합니다.

단계 **3** 서버 ID를 삭제하려면 제거할 서버 ID 옆에 있는 **Delete(**삭제**)** ( )을 클릭합니다.

단계 **4** 서버 ID를 수정하려면 서버 목록에서 서버 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **5** 다음 2가지 옵션을 사용할 수 있습니다.

- **Select Server Type(**서버 유형 선택**)** 드롭다운 목록에서 현재 정의를 선택합니다.
- **Select Server Type(**서버 유형 선택**)** 드롭다운 목록에서 서버 유형을 선택합니다.

단계 **6** 원하는 경우, 해당 서버 유형에 대한 공급업체와 제품만 나열하려면 **Restrict by Server Type(**서버 유형으로 제한**)** 확인란을 선택합니다.

단계 **7** 원하는 경우, 서버 이름과 버전을 맞춤 설정하려면 **Use Custom Display String(**맞춤형 표시 문자열 사용**)**을 선택하고 **Vendor String(**공급업체 문자열**)**과 **Version String(**버전 문자열**)**을 입력합니다.

단계 **8** **Product Mappings(**제품 매핑**)** 섹션에서 사용할 운영 체제, 제품 및 버전을 선택합니다.

예제**:**

예를 들어 서버를 Red Hat Linux 9에 매핑하려면 공급업체로 **Redhat, Inc.**, 제품으로 **Redhat Linux**, 버전으로 **9**를 선택합니다.

단계 **9** 서버 수정이 적용되었음을 표시하려면 **Configure Fixes(**수정 구성**)**를 클릭하고 해당 서버에 적용하려는 패치를 수정 목록에 추가합니다.

단계 **10** **Finish(**종료**)**를 클릭합니다.

서버 ID 충돌 해결

애플리케이션이나 스캐너 같은 활성 소스가 서버의 ID 데이터를 호스트에 추가한 후 시스템이 해당 포트에서 서버 ID가 충돌함을 나타내는 트래픽을 탐지하면 서버 ID 충돌이 발생합니다.

프로시저

단계 **1** 호스트 프로파일에서 **Servers(**서버**)** 섹션으로 이동합니다.

단계 **2** 서버 옆에 있는 해결 아이콘을 클릭합니다.

단계 **3** **Select Server Type(**서버 유형 선택**)** 드롭다운 목록에서 서버 유형을 선택합니다.

단계 **4** 원하는 경우, 해당 서버 유형에 대한 공급업체와 제품만 나열하려면 **Restrict by Server Type(**서버 유형으로 제한**)** 확인란을 선택합니다.

단계 **5** 원하는 경우, 서버 이름과 버전을 맞춤 설정하려면 **Use Custom Display String(**맞춤형 표시 문자열 사용**)**을 선택하고 **Vendor String(**공급업체 문자열**)**과 **Version String(**버전 문자열**)**을 입력합니다.

단계 **6** **Product Mappings(**제품 매핑**)** 섹션에서 사용할 운영 체제, 제품 및 버전을 선택합니다.

예제**:**

예를 들어 서버를 Red Hat Linux 9에 매핑하려면 공급업체로 **Redhat, Inc.**, 제품으로 **Redhat Linux**, 버전으로 **9**를 선택합니다.

단계 **7** 서버 수정이 적용되었음을 표시하려면 **Configure Fixes(**수정 구성**)**를 클릭하고 해당 서버에 적용하려는 패치를 수정 목록에 추가합니다.

단계 **8** **Finish(**종료**)**를 클릭합니다.

호스트 프로파일의 웹 애플리케이션

호스트 프로파일의 Web Application(웹 애플리케이션) 섹션에는 네트워크의 호스트에서 실행 중이라고 시스템이 식별하는 클라이언트 및 웹 애플리케이션이 표시됩니다. 시스템은 수동 탐지 소스와 능동 탐지 소스의 클라이언트 및 웹 애플리케이션 정보를 식별할 수 있지만 NetFlow 레코드에서 추가된 호스트에 대한 정보는 제한됩니다.

이 섹션의 세부 정보는 호스트에서 탐지되는 애플리케이션의 제품 및 버전, 사용 가능한 클라이언트 또는 웹 애플리케이션 정보, 그리고 애플리케이션 사용이 마지막으로 탐지된 시간을 표시합니다.

이 섹션은 호스트에서 실행 중인 클라이언트를 최대 16개 나열합니다. 이 한계에 도달하면 사용자가 호스트에서 클라이언트 애플리케이션을 삭제하거나 비활성(클라이언트 시간 초과)으로 인해 시스템이 호스트 프로파일에서 클라이언트를 삭제할 때까지 능동 및 수동 소스의 새 클라이언트 정보가 삭제됩니다.

또한 탐지된 각 웹 브라우저에 대해 시스템은 액세스된 처음 100개의 웹 애플리케이션을 표시합니다. 이 한계에 도달하면 다음과 같이 될 때까지 능동 및 수동 소스의 해당 브라우저에 연결된 새 웹 애플리케이션이 삭제됩니다.

- 웹 브라우저 클라이언트 애플리케이션이 시간 초과됨, 또는
- 호스트 프로파일에서 웹 애플리케이션과 관련된 애플리케이션 정보 삭제

활성화된 상관관계 정책의 규정 준수 허용 목록을 위반하는 애플리케이션이 호스트에서 실행되고 있는 경우, Firepower Management Center에서는 규정을 준수하지 않는 애플리케이션을 허용 목록 위반으로 표시합니다.

팁 호스트의 특정 애플리케이션에 연결된 연결 이벤트를 분석하려면 애플리케이션 옆에 있는 **Logging(**로깅**)** ()을 클릭합니다. 연결 이벤트에 대한 기본 설정 워크플로의 첫 번째 페이지가 나타나고 애플리케이션의 유형, 제품 및 버전에 의해 제한되는 연결 이벤트 및 호스트의 IP 주소를 보여줍니다. 연결 이벤트에 대한 기본 설정 워크플로가 없다면 선택해야 합니다.

다음은 호스트 프로파일에 나타나는 애플리케이션 정보에 대한 설명입니다.

애플리케이션 프로토콜

애플리케이션(HTTP 브라우저, DNS 클라이언트 등)이 사용하는 애플리케이션 프로토콜을 표시합니다.

클라이언트

Firepower System에 의해 식별되거나 Nmap에 의해 캡처되거나 호스트 입력 기능을 통해 획득된 경우, 페이로드에서 추출되는 클라이언트 정보. 사용 가능한 소스 중 ID를 제공한 소스가 없으면 필드는 비어 있게 됩니다.

버전

클라이언트의 버전을 표시합니다.

웹 애플리케이션

웹 브라우저의 경우 시스템이 http 트래픽에서 탐지한 콘텐츠. 웹 애플리케이션 정보는 Firepower System에 의해 식별되거나 Nmap에 의해 캡처되거나 호스트 입력 기능을 통해 수집된 특정 콘텐츠 유형(예: WMV 또는 QuickTime)을 나타냅니다. 사용 가능한 소스 중 ID를 제공한 소스가 없으면 필드는 비어 있게 됩니다.

호스트 프로파일에서 웹 애플리케이션 삭제

호스트 프로파일에서 애플리케이션을 삭제하여 호스트에서 실행되고 있지 않은 애플리케이션을 제거할 수 있습니다. 호스트에서 애플리케이션을 삭제하면 해당 호스트는 허용 목록 규정 준수 상태로 전환될 수 있습니다.

참고 해당 애플리케이션이 다시 탐지되면 네트워크 맵 및 호스트 프로파일에 다시 추가됩니다.

프로시저

단계 **1** 호스트 프로파일에서 **Applications(**애플리케이션**)** 섹션으로 이동합니다.

단계 **2** 삭제할 애플리케이션 옆에 있는 **Delete(**삭제**)** ( )을 클릭합니다.

호스트 프로파일의 호스트 프로토콜

각 호스트 프로파일에는 호스트와 연결된 네트워크 트래픽에서 탐지된 프로토콜에 대한 정보가 포함되어 있습니다. 이 정보에는 다음이 포함됩니다.

프로토콜

호스트가 사용하는 프로토콜의 이름.

레이어

프로토콜이 실행되는 네트워크 레이어(`Network` 또는 `Transport`).

호스트 프로파일에 표시되는 프로토콜이 활성화된 상관관계 정책의 규정준수 허용리스트를 위반하는 경우, management center에서는 규정을 준수하지 않는 프로토콜을 허용리스트 위반으로 표시합니다.

호스트에서 실행되고 있지 않음을 알고 있는 프로토콜이 호스트 프로파일에 나열되는 경우, 해당 프로토콜을 삭제할 수 있습니다. 호스트에서 프로토콜을 삭제하면 해당 호스트가 규정준수 허용리스트를 준수하게 될 수 있습니다.

참고 시스템은 해당 프로토콜을 다시 탐지하면 네트워크 맵 및 호스트 프로파일에 다시 추가합니다.

호스트 프로파일에서 프로토콜 삭제

프로시저

단계 **1** 호스트 프로파일의 **Protocols(**프로토콜**)** 섹션으로 이동합니다.

단계 **2** 삭제할 프로토콜 옆에 있는 **Delete(**삭제**)** ( )를 클릭합니다.

호스트 프로파일의 보안 침해 지표

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.

호스트 프로파일의 Indications of Compromise(보안 침해 지표) 섹션에는 호스트에 대한 모든 보안 침해 지표 태그가 표시됩니다.

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

보안 침해 지표를 사용하는 방법에 대한 자세한 내용은 보안 침해 지표 데이터 및 해당 항목의 하위 항목을 참조하십시오.

호스트 프로파일의 VLAN 태그

호스트가 VLAN(Virtual LAN)의 멤버인 경우 호스트 프로파일의 VLAN Tag(VLAN 태그) 섹션이 나타납니다.

물리적 네트워크 장비는 종종 VLAN을 사용하여 서로 다른 네트워크 블록에서 논리적 네트워크 세그먼트를 생성합니다. 시스템은 802.1q VLAN 태그를 탐지하고 각각에 대해 다음과 같은 정보를 표시합니다.

- **VLAN ID**는 호스트가 멤버인 VLAN을 식별합니다. 802.1q VLAN의 경우 0~4095 사이의 정수일 수 있습니다.
- **Type**은 VLAN 태그를 포함하는 캡슐화된 패킷을 식별하며, 이더넷 또는 토큰 링일 수 있습니다.
- **Priority**는 VLAN 태그의 우선순위를 식별하며, 범위는 0~7의 정수이고 7이 가장 높은 우선순위입니다.

VLAN 태그가 패킷 내에 중첩된 경우 시스템은 가장 안쪽의 VLAN 태그를 처리하고 management center는 이를 표시합니다. 시스템은 ARP 및 DHCP 트래픽을 통해 식별하는 MAC 주소에 대해서만 VLAN 태그 정보를 수집하고 표시합니다.

예를 들면 VLAN이 프린터로만 구성되어 있고 시스템이 해당 VLAN에서 Microsoft Windows 2000 운영 체제를 탐지하는 경우에는 VLAN 태그 정보가 유용할 수 있습니다. VLAN 정보는 또한 시스템이 좀 더 정확한 네트워크 맵을 생성하는 데에도 도움이 됩니다.

호스트 프로파일의 사용자 기록

호스트 프로파일의 사용자 기록 부분은 사용자 활동의 마지막 24시간을 그래프로 보여줍니다. 일반적인 사용자는 저녁에 로그오프하고 호스트 리소스를 다른 사용자와 공유할 것입니다. 이메일 확인을 위한 요청 등 정기적인 로그인 요청은 짧은 일반 막대로 표시됩니다. 사용자 ID의 목록에는 사용자 로그인이 탐지된 시점을 나타내는 막대 그래프가 제공됩니다. 권한 없는 로그인의 경우에는 막대 그래프가 회색입니다.

시스템은 권한 없는 사용자의 호스트 로그인을 해당 호스트의 IP 주소와 연결하여, 사용자가 호스트의 사용자 기록에 나타나도록 합니다. 그러나 동일한 호스트에서 권한 있는 사용자 로그인이 탐지되면 권한 있는 사용자 로그인과 연결된 사용자가 호스트 IP 주소의 연결 관계를 인수하며, 권한 없는 새 사용자 로그인은 호스트 IP 주소와 사용자의 연결 관계를 중단하지 않습니다. 네트워크 검색 정책에서 실패한 로그인의 캡처를 구성하는 경우 목록에는 호스트 로그인에 실패한 사용자가 포함됩니다.

호스트 프로파일의 호스트 속성

호스트 속성을 사용하면 네트워크 환경에서 중요한 방법으로 호스트를 분류할 수 있습니다. Firepower System에는 3가지 속성이 존재합니다.

- 사전 정의된 호스트 속성
- 컴플라이언스 허용 리스트 호스트 속성
- 사용자 정의 호스트 속성

사전 정의된 속성을 설정하거나 사용자 정의 호스트 속성을 생성한 후에는, 호스트 속성 값을 할당해야 합니다.

참고 호스트 속성은 어떤 도메인 레벨에서도 정의할 수 있습니다. 현재 및 상위 도메인에서 생성된 호스트 속성을 할당할 수 있습니다.

사전 정의된 호스트 속성

management center은(는) 사전 정의된 호스트 속성 2개를 제공합니다.

호스트 중요도

이 속성을 사용하여 특정 호스트의 비즈니스 중요도를 지정하고 상관관계 응답을 호스트 중요도에 맞게 조정하십시오. 예를 들어 조직의 메일 서버가 일반적인 사용자 워크스테이션보다 비즈니스에 더 중요하다고 생각한다면 메일 서버에는 High, 다른 주요 비즈니스 디바이스에는 Medium, 기타 호스트에는 Low 값을 할당할 수 있습니다. 그런 다음 영향받는 호스트의 중요도를 기반으로 서로 다른 알림을 생성하는 상관관계 정책을 생성할 수 있습니다.

Notes(참고**)**

이 호스트 한정 속성을 사용하여 다른 분석가에게 보여줄 호스트에 대한 정보를 기록하십시오. 예를 들어 운영체제의 패치되지 않은 이전 버전이 있는 테스트용 컴퓨터가 네트워크에 있는 경우, Notes 기능을 사용하여 시스템을 의도적으로 패치하지 않았음을 표시할 수 있습니다.

허용 목록 호스트 속성

자동으로 생성되는 각 규정 준수 허용 목록은 허용 목록과 동일한 이름으로 호스트 속성을 생성합니다. 가능한 허용 목록 호스트 속성은 다음과 같습니다.

- Compliant - 허용 목록을 준수하는 호스트를 식별합니다.
- Non-Compliant - 허용 목록을 위반하는 호스트를 식별합니다.
- Not Evaluated - 허용 목록의 유효한 대상이 아니거나 어떤 이유로든 평가되지 않은 호스트를 식별합니다.

허용 목록 호스트 속성 값을 수정하거나 허용 목록 호스트 속성을 삭제할 수 없습니다.

사용자 정의 호스트 속성

사전 정의된 호스트 속성 또는 컴플라이언스 허용 목록 호스트 속성에서 사용하는 것과는 다른 기준을 이용해 호스트를 식별하고 싶다면, 사용자 정의 호스트 속성을 사용하면 됩니다. 예를 들어, 다음이 가능합니다.

- 호스트에 물리적 위치 식별자(예: 시설 코드, 도시 또는 방 번호)를 할당합니다.

- 특정 호스트의 담당 시스템 관리자가 누구인지를 나타내는 Responsible Party Identifier(담당자 식별자)를 할당합니다. 호스트와 관련된 문제가 탐지될 때 올바른 시스템 관리자에게 알림을 전송하도록 상관관계 규칙 및 정책을 구성할 수 있습니다.
- 호스트의 IP 주소를 기반으로 사전 정의된 목록에서 호스트로 값을 자동으로 할당합니다. 이 기능은 네트워크에 처음으로 표시되는 새 호스트에 값을 할당할 때 유용하게 활용할 수 있습니다.

사용자 정의 호스트 속성은 호스트 프로파일 페이지에 나타나며, 여기서 호스트 단위로 값을 할당할 수 있습니다. 다음 작업도 가능합니다.

- 상관관계 정책 및 검색에서 속성을 사용합니다.
- 호스트 속성 테이블 보기에서 속성을 보고 이를 기반으로 보고서를 생성합니다.

사용자 정의 호스트 속성의 유형은 다음과 같습니다.

텍스트

텍스트 문자열을 호스트에 수동으로 할당할 수 있습니다.

정수

양의 정수 범위의 첫 번째와 마지막 숫자를 지정한 다음 이러한 숫자 중 하나를 호스트에 수동으로 할당할 수 있습니다.

목록

문자열 값의 목록을 생성한 다음 이러한 값 중 하나를 호스트에 수동으로 할당할 수 있습니다. 호스트의 IP 주소를 기반으로 호스트에 값을 자동으로 할당할 수도 있습니다.

여러 IP 주소가 있는 호스트에서 한 IP 주소를 기반으로 값을 자동 할당하면, 그 호스트와 연결된 모든 주소에 해당 값이 적용됩니다. Host Attributes(호스트 속성) 테이블을 볼 때는 이러한 점에 유의해야 합니다.

목록 값을 자동으로 할당하는 경우에는 일반적인 IP 주소가 아닌 네트워크 개체 사용을 고려해 보십시오. 이 방법을 이용하면 관리 용이성을 개선할 수 있으며, 특히 재정의를 활성화한 개체가 하위 도메인 관리자가 자신의 로컬 환경에 맞게 상위 설정을 조정하도록 허용하는 다중 도메인 구축에서 더욱 효과적입니다. 다중 도메인 구축의 경우에는, 자동 할당된 목록을 상위 도메인 수준에서 정의하며 하위 도메인이 중복되는 IP 주소를 사용할 때 의도하지 않은 호스트가 매칭되지 않도록 주의하십시오.

URL

URL 값을 호스트에 수동으로 할당할 수 있습니다.

사용자 정의 호스트 속성을 삭제하면 이를 사용하는 모든 호스트 프로파일에서 해당 속성이 제거됩니다.

텍스트 또는 URL 기반 호스트 속성 생성

프로시저

단계 1 **Analysis**(분석) > **Hosts**(호스트) > **Host Attributes**(호스트 속성)을(를) 선택합니다.
단계 2 **Host Attribute Management**(호스트 속성 관리)를 클릭합니다.
단계 3 **Create Attribute**(속성 생성)를 클릭합니다.
단계 4 **Name**(이름)을 입력합니다.
단계 5 사용자 정의 호스트 속성, 19 페이지에 설명된 대로 생성하려는 속성의 **Type**(유형)을 선택합니다.
단계 6 **Save**(저장)를 클릭합니다.

정수 기반 호스트 속성 생성

정수 기반 호스트 속성을 정의할 때는 호스트가 허용하는 숫자 범위를 지정해야 합니다.

프로시저

단계 1 **Analysis**(분석) > **Hosts**(호스트) > **Host Attributes**(호스트 속성)을(를) 선택합니다.
단계 2 **Host Attribute Management**(호스트 속성 관리)를 클릭합니다.
단계 3 **Create Attribute**(속성 생성)를 클릭합니다.
단계 4 **Name**(이름)을 입력합니다.
단계 5 사용자 정의 호스트 속성, 19 페이지에 설명된 대로 생성하려는 속성의 **Type**(유형)을 선택합니다.
단계 6 호스트에 할당할 수 있는 최소 정수 값을 **Min**(최소) 필드에 입력합니다.
단계 7 호스트에 할당할 수 있는 최대 정수 값을 **Max**(최대) 필드에 입력합니다.
단계 8 **Save**(저장)를 클릭합니다.

목록 기반 호스트 속성 생성

목록 기반 호스트 속성을 정의할 때에는 목록의 각 값을 제공해야 합니다. 이러한 값에는 영숫자 문자, 공백 및 기호가 포함될 수 있습니다.

프로시저

단계 1 **Analysis**(분석) > **Hosts**(호스트) > **Host Attributes**(호스트 속성)을(를) 선택합니다.
단계 2 **Host Attribute Management**(호스트 속성 관리)를 클릭합니다.

단계 **3** **Create Attribute(**속성 생성**)**를 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

단계 **5** 사용자 정의 호스트 속성, 19 페이지에 설명된 대로 생성하려는 속성의 **Type(**유형**)**을 선택합니다.

단계 **6** 목록에 값을 추가하려면 **Add Value(**값 추가**)**를 클릭합니다.

단계 **7** 추가하려는 첫 번째 값을 **Name(**이름**)** 필드에 입력합니다.

단계 **8** 원하는 경우, 방금 추가한 속성 값을 호스트에 자동 할당하려면 **Add Networks(**네트워크 추가**)**를 클릭합니다.

단계 **9** 추가한 값을 **Value(**값**)** 드롭다운 목록에서 선택합니다.

단계 **10** 이 값을 자동 할당할 IP 주소 블록을 나타내는 IP 주소와 네트워크 마스크(IPv4)를 **IP Address(IP** 주소**)** 및 **Netmask(**넷마스크**)** 필드에 입력합니다.

단계 **11** 목록에 값을 더 추가하여 IP 주소 블록에 속하는 새 호스트에 자동으로 할당하려면 6~10단계를 반복합니다.

단계 **12** **Save(**저장**)**를 클릭합니다.

호스트 속성값 설정

미리 정의된 호스트 속성 및 사용자 정의 호스트 속성의 값을 설정할 수 있습니다. 시스템에서 생성된 컴플라이언스 허용 호스트 속성의 값은 설정할 수 없습니다.

프로시저

단계 **1** 수정하려는 호스트 프로파일을 엽니다.

단계 **2** **Attributes(**속성**)** 섹션에서 **Edit Attributes(**속성 수정**)**를 클릭합니다.

단계 **3** 원하는 대로 속성을 업데이트합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

호스트 프로파일의 허용 목록 위반

규정 준수 허용 목록(또는 허용 목록)는 특정 서브넷에서 실행 가능한 운영 체제, 애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션 및 프로토콜을 지정할 수 있는 기준 집합입니다.

활성 상관관계 정책에 허용 목록을 추가한 경우 시스템이 호스트에서 허용 목록 위반을 탐지하면, management center는 허용 목록 이벤트(특정 상관관계 이벤트 유형)를 데이터베이스에 로깅합니다. 이러한 각 허용 목록 이벤트는 특정 호스트가 어떻게, 왜 허용 목록을 위반했는지를 나타내는 허용목록 위반과 연결됩니다. 호스트가 하나 이상의 허용 목록을 위반하면 호스트 프로필에서 두 가지 방법으로 이러한 위반을 볼 수 있습니다.

첫째, 호스트 프로필은 호스트에 연결된 모든 개별 허용 목록 위반을 나열합니다.

다음은 호스트 프로필에 표시되는 허용 목록 위반 정보에 대한 설명입니다.

유형

위반의 유형, 즉 위반이 발생한 원인(규정을 준수하지 않는 운영 체제, 애플리케이션, 서버 또는 프로토콜).

이유

위반의 특정 이유. 예를 들어 Microsoft Windows 호스트만 허용하는 허용 목록이 있는 경우, 호스트 프로파일에는 호스트에서 실행 중인 현재 운영 체제(예: `Linux 2.4, 2.6`)가 표시됩니다.

허용 목록

위반과 연결된 허용 목록의 이름.

둘째, 운영 체제, 애플리케이션, 프로토콜 및 서버와 관련된 섹션에서 management center는 규정을 준수하지 않는 요소를 허용 목록 위반 아이콘으로 표시합니다. 예를 들어 Microsoft Windows 호스트만 허용하는 허용 목록의 경우, 호스트 프로필은 해당 호스트의 운영 체제 정보 옆에 허용 목록 위반 아이콘을 표시합니다.

참고 호스트의 프로필을 사용하여 규정 준수 허용 목록에 대한 공유 호스트 프로필을 생성할 수 있습니다.

공유 허용 목록 호스트 프로파일 생성

규정 준수 허용 목록 공유 호스트 프로필은 여러 허용 목록에 걸쳐 대상 호스트에서 실행 가능한 운영 체제, 애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션 및 프로토콜을 지정합니다. 여러 개의 허용 목록을 생성하지만 동일한 호스트 프로파일을 사용하여 허용 목록 전반에 걸쳐 특정 운영체제를 실행하는 호스트를 평가하려는 경우, 공유 호스트 프로파일을 사용합니다.

알려진 IP 주소가 있는 호스트의 호스트 프로필을 사용하여 규정 준수 허용 목록이 사용할 수 있는 공유 호스트 프로필을 생성할 수 있습니다. 그러나 시스템이 호스트의 운영 체제를 아직 식별하지 못한 경우에는 개별 호스트의 호스트 프로파일을 기반으로 공유 호스트 프로파일을 생성할 수 없습니다.

프로시저

단계 **1** 호스트 프로파일에서 **Generate(**생성**)**허용 목록 **Profile(**프로파일**)**을 클릭합니다.

단계 **2** 특정 요구에 맞게 공유 호스트 프로파일을 수정 및 저장합니다.

관련 항목

허용 리스트 호스트 프로필 빌드

호스트 프로파일의 악성코드 탐지

Most Recent Malware Detections(가장 최근의 악성코드 탐지) 섹션에는 호스트가 악성코드 파일을 주고받은 가장 최근의 악성코드 이벤트가 최대 100개까지 나열됩니다. 호스트 프로파일에는 네트워크 기반 악성코드 이벤트(악성코드 대응 에 의해 생성)와 엔드포인트 기반 악성코드 이벤트(AMP for Endpoints에 의해 생성)가 모두 나열됩니다.

파일이 악성코드로 소급 식별된 파일 이벤트에 호스트가 관련된 경우, 악성코드 식별이 발생한 후 파일이 전송된 원래 이벤트가 악성코드 탐지 목록에 나타납니다. 악성코드로 식별된 파일이 악성코드가 아닌 것으로 소급 결정되면 해당 파일과 연결된 악성코드 이벤트가 더 이상 목록에 나타나지 않습니다. 예를 들어 파일에 `Malware(악성코드)` 속성이 있고 해당 속성이 `Clean(정상)`으로 변경되면 해당 파일의 이벤트는 호스트 프로파일의 악성코드 탐지 목록에서 제거됩니다.

호스트 프로필에서 악성코드 탐지를 볼 때 **Malware(**악성코드**)**를 클릭하여 해당 호스트의 악성코드 이벤트를 볼 수 있습니다.

다음은 호스트 프로파일의 Most Recent Malware Detections(가장 최근의 악성코드 탐지) 섹션에 있는 열에 대한 설명입니다.

시간

이벤트가 생성된 날짜 및 시간

파일이 악성코드로 소급 식별된 이벤트의 경우, 악성코드가 식별된 시간이 아니라 원래 이벤트의 시간을 나타냅니다.

호스트 역할

탐지된 악성코드 전송에서 호스트의 역할(발신자 또는 수신자). AMP for Endpoints에 의해 생성된 악성코드 이벤트("엔드포인트 기반 악성코드 이벤트")의 경우, 호스트는 항상 수신자입니다.

위협 이름

탐지된 악성코드의 이름.

파일 이름

악성코드 파일의 이름.

파일 유형

`PDF` 또는 `MSEXE` 등의 파일 형식.

호스트 프로파일의 취약성

호스트 프로파일의 Vulnerabilities(취약성) 섹션에는 해당 호스트에 영향을 미치는 취약성이 나열됩니다. 이러한 취약성은 시스템이 호스트에서 탐지한 운영 체제, 서버, 애플리케이션에 기반합니다.

호스트의 운영 체제 ID 또는 호스트의 애플리케이션 프로토콜 중 하나에 ID 충돌이 있는 경우, 시스템은 충돌이 해결될 때까지 두 ID에 대한 취약성을 나열합니다.

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

서버 공급업체 및 버전 정보는 대체로 트래픽에 포함되지 않습니다. 기본적으로 시스템은 트래픽을 보내고 받는 호스트에 대해 관련 취약성을 매핑하지 않습니다. 그러나 공급업체 또는 버전 정보가 없는 특정 애플리케이션 프로토콜에 대한 취약성을 매핑하도록 시스템을 구성할 수 있습니다.

호스트 입력 기능을 사용하여 네트워크의 호스트에 대한 서드파티 취약성 정보를 추가하는 경우 추가적인 Vulnerabilities(취약성) 섹션이 나타납니다. 예를 들어 QualysGuard Scanner에서 취약성을 가져오면 호스트 프로파일에 QualysGuard Vulnerabilities 섹션이 포함됩니다. 서드파티 취약성의 경우 호스트 프로파일의 해당 Vulnerabilities(취약성) 섹션에 표시되는 정보는 호스트 입력 기능을 사용하여 취약성 데이터를 가져올 때 제공한 정보로 제한됩니다.

서드파티 취약성을 운영 체제 및 애플리케이션 프로토콜과 연결할 수 있지만 클라이언트와는 연결할 수 없습니다. 서드파티 취약성 가져오기에 대한 자세한 내용은 *Firepower System Host Input API* 설명서를 참조하십시오.

다음은 호스트 프로파일의 Vulnerabilities(취약성) 섹션에 있는 열에 대한 설명입니다.

이름

취약성의 이름.

원격

취약성이 원격으로 악용될 수 있는지를 나타냅니다. 이 열이 비어 있으면 취약성 정의에 이 정보가 포함되지 않은 것입니다.

구성 요소

취약성과 관련된 운영 체제, 애플리케이션 프로토콜 또는 클라이언트의 이름.

Port(포트)

취약성이 지정된 포트에서 실행 중인 애플리케이션 프로토콜과 연결된 경우 포트 번호.

관련 항목

- 취약성 데이터 필드
- 취약성 비활성화

취약성 패치 다운로드

네트워크의 호스트에서 검색된 취약성을 완화하기 위한 패치를 다운로드할 수 있습니다.

프로시저

단계 **1** 패치를 다운로드할 호스트의 호스트 프로파일에 액세스합니다.

단계 **2** **Vulnerabilities(**취약성**)** 섹션을 확장합니다.

단계 **3** 패치를 적용할 취약성의 이름을 클릭합니다.

단계 **4** 취약성에 대한 패치의 목록을 표시하려면 **Fixes(**수정**)** 섹션을 확장합니다.

단계 **5** 다운로드할 패치 옆에 있는 **Download(**다운로드**)**를 클릭합니다.

단계 **6** 패치를 다운로드하고 영향받는 시스템에 적용합니다.

개별 호스트용 취약성 비활성화

호스트 취약성 편집기를 사용하여 호스트별로 취약성을 비활성화할 수 있습니다. 호스트에 대한 취약성을 비활성화할 경우 해당 호스트에 대한 영향 상관관계에는 여전히 사용되지만 영향 레벨은 자동으로 한 단계 줄어듭니다.

프로시저

단계 **1** 호스트 프로파일의 **Vulnerabilities(**취약성**)** 섹션으로 이동합니다.

단계 **2** **Edit Vulnerabilities(**취약성 수정**)**를 클릭합니다.

단계 **3** **Valid Vulnerabilities(**유효한 취약성**)** 목록에서 취약성을 선택하고 아래쪽 화살표를 클릭하여 **Invalid Vulnerabilities(**유효하지 않은 취약성**)** 목록으로 이동시킵니다.

팁 클릭하고 끌어 여러 인접 취약성을 선택할 수 있습니다. 또한 취약성을 두 번 클릭하여 다른 목록으로 이동시킬 수 있습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 원하는 경우, **Invalid Vulnerabilities(**유효하지 않은 취약성**)** 목록에서 **Valid Vulnerabilities(**유효한 취약성**)** 목록으로 취약성을 이동시켜 호스트의 취약성을 활성화합니다.

관련 항목

개별 취약성 비활성화, 27 페이지
다중 취약성 비활성화

개별 취약성 비활성화

호스트 프로파일에서 취약성을 비활성화하면 해당 취약성은 네트워크 맵의 모든 호스트에서 비활성화됩니다. 하지만 언제든 다시 활성화할 수 있습니다.

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 세부 정보에 액세스:

- 영향을 받는 호스트 프로파일에서 **Vulnerabilities(**취약성**)** 섹션을 확장하고 활성화 또는 비활성화하려는 취약성의 이름을 클릭합니다.
- 미리 정의된 워크플로우에서 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Vulnerabilities(**취약성**)**을 선택하고 클릭하고 활성화하거나 비활성화하려는 취약성 옆에 있는 **View(**보기**)** ( )를 클릭합니다.

단계 **2** **Impact Qualification** 드롭다운 목록에서 **Disabled(**비활성화**)**를 선택합니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

단계 **3** 네트워크 맵의 모든 호스트에 대해 **Impact Qualification** 값을 변경할 것인지 확인합니다.

단계 **4** **Done(**완료**)**을 클릭합니다.

다음에 수행할 작업

- 원하는 경우, 위의 단계를 수행하면서 **Impact Qualification** 드롭다운 목록에서 **Enabled(**활성화**)**를 선택하여 취약성을 활성화합니다.

관련 항목

개별 호스트용 취약성 비활성화, 26 페이지
다중 취약성 비활성화
운영 체제 ID 충돌, 9 페이지

호스트 프로파일의 스캔 결과

Nmap을 사용하여 호스트를 스캔하거나 Nmap 스캔에서 결과를 가져오면 그러한 결과는 스캔에 포함된 호스트의 호스트 프로파일에 나타납니다.

필터링되지 않은 열린 포트에서 실행되는 호스트 운영 체제 및 서버에 대해 Nmap이 수집하는 정보는 각각 호스트 프로파일의 Operating System(운영 체제) 및 Servers(서버) 섹션에 직접 추가됩니다. 또한

Nmap은 해당 호스트에 대한 스캔 결과의 목록을 Scan Results(스캔 결과) 섹션에 추가합니다. Scan Results(스캔 결과) 섹션이 프로파일에 나타나려면 스캔은 호스트에서 열린 포트를 찾아야 합니다.

각 결과는 정보의 소스, 스캔된 포트의 번호와 유형, 포트에서 실행되는 서버의 이름, Nmap에서 탐지한 추가 정보(예: 포트의 상태 또는 서버의 공급업체 이름) 등을 나타냅니다. UDP 포트를 스캔하는 경우, 해당 포트에서 탐지된 서버는 Scan Results(스캔 결과) 섹션에만 나타납니다.

호스트 프로파일에서 Nmap 스캔을 수행할 수 있습니다.

호스트 프로파일에서 호스트 스캔

호스트 프로파일에서 호스트에 대해 Nmap 스캔을 수행할 수 있습니다. 스캔이 완료되면 해당 호스트의 서버 및 운영 체제 정보가 호스트 프로파일에서 업데이트됩니다. 호스트 프로파일의 Scan Results(스캔 결과) 섹션에 스캔 결과가 추가됩니다.

⚠

주의 또 다른 Nmap 스캔을 실행하거나 우선순위가 더 높은 호스트 입력으로 재정의할 때까지 Nmap 제공 서버 및 운영 체제 데이터는 고정 상태로 유지됩니다. Nmap을 이용해 호스트를 스캔하기로 했다면, 스캔을 정기적으로 예약하십시오.

시작하기 전에

- Nmap 스캔 인스턴스를 추가합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 호스트 *ID* 소스 장의 내용을 참고하십시오.

프로시저

단계 **1** 호스트 프로파일에서 **Scan Host(**호스트 스캔**)**를 클릭합니다.

단계 **2** 호스트 스캔에 사용할 스캔 교정 옆에 있는 **Scan(**스캔**)**을 클릭합니다.

시스템이 호스트를 스캔하고 결과를 호스트 프로파일에 추가합니다.

관련 항목

Nmap 스캔 자동화

호스트 프로파일 기록

기능	버전	세부 사항
VRF 사용 시 제한 사항	6.6	사용자 환경에서 가상 라우팅 및 포워딩을 사용하는 경우 VRF가 중복 네트워크 공간을 포함할 수 있으므로 단일 IP 주소가 여러 호스트를 나타낼 수 있습니다. 지원되는 플랫폼: FMC