호스트 ID 소스

다음 주제는 호스트 ID 소스 관련 정보를 제공합니다.

개요: 호스트 데이터 수집

Firepower System에서는 네트워크를 이동하는 트래픽을 수동으로 모니터링할 때 특정 패킷 헤더 값과 기타 네트워크 트래픽의 고유한 데이터를 설정된 정의(핑거프린트라고 함)와 비교하여 네트워크의 호스트에 대한 다음과 같은 정보를 확인합니다.

- 호스트의 수 및 유형(브리지, 라우터, 로드 밸런서 및 NAT 디바이스 같은 네트워크 디바이스 포함)
- 네트워크의 검색 지점에서 호스트로의 홉(hop) 수를 비롯한 기본 네트워크 토폴로지 데이터
- 호스트에서 실행 중인 운영체제
- 호스트의 애플리케이션 및 이러한 애플리케이션과 연결된 사용자

시스템이 호스트의 운영체제를 식별하지 못한다면, 맞춤형 클라이언트나 서버 핑거프린트를 만들 수 있습니다. 시스템은 이러한 핑거프린트를 사용하여 새 호스트를 식별합니다. 핑거프린트를 VDB(취약성 데이터베이스)의 시스템에 매핑하면 맞춤형 핑거프린트를 사용하여 호스트가 식별될 때마다 적절한 취약성 정보를 표시할 수 있습니다.

참고 모니터링하는 네트워크 트래픽에서 호스트 데이터를 수집하는 일 외에도, 시스템은 내보낸 NetFlow 기록에서 호스트 데이터를 수집할 수 있으며, 사용자는 Nmap 스캔과 호스트 입력 기능을 이용해 호스트 데이터를 능동적으로 추가할 수 있습니다.

호스트 ID 소스 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든, Leaf뿐인 사용자 지정 핑거 프린팅은 예외입니다.

사용자 역할

- 관리자
- 검색 관리자, 서드 파티 데이터 및 사용자 지정 매핑은 예외입니다.

시스템에서 탐지할 수 있는 호스트 운영체제 결정

핑거프린트할 수 있는 정확한 운영체제를 확인하려면, 맞춤형 OS 핑거프린트를 생성하는 중에 표시되는 사용 가능한 핑거프린트 목록을 확인하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

단계 **2** **Custom Operating Systems(**맞춤형 운영체제**)**를 클릭합니다.

단계 **3** **Create Custom Fingerprint(**맞춤형 핑거프린트 만들기**)**를 클릭합니다.

단계 **4** **OS Vulnerability Mappings(**운영체제 취약성 매핑**)** 섹션의 드롭다운 목록에 표시되는 옵션 목록을 확인합니다. 이러한 옵션은 시스템이 핑거프린트할 수 있는 운영체제입니다.

다음에 수행할 작업

필요하다면 호스트 운영체제 식별, 3 페이지 섹션을 참조하십시오.

호스트 운영체제 식별

시스템이 호스트의 운영체제를 올바르게 식별하지 못한다면(예를 들어 호스트 프로파일에서 "알 수 없음"으로 표시되거나 올바르게 식별되지 않는다면), 아래 방법을 시도해 보십시오.

프로시저

다음 방법 중 하나를 수행합니다.

- 네트워크 검색 ID 충돌 설정을 확인합니다.
- 호스트에 대한 맞춤형 핑거프린트를 만듭니다.
- 호스트에 대한 Nmap 스캔을 실행합니다.
- 호스트 입력 기능을 이용해 데이터를 네트워크로 가져옵니다.
- 수동으로 운영체제 정보를 입력합니다.

맞춤형 핑거프린팅

시스템에는 시스템이 탐지하는 각 호스트에서 운영체제를 식별하는 데 사용하는 운영체제 핑거프린트가 포함되어 있습니다. 그러나 운영체제와 일치하는 핑거프린트가 없기 때문에 시스템은 간혹 호스트 운영체제를 식별하지 못하거나 잘못 식별합니다. 이 문제를 바로잡으려면 알 수 없거나 잘못 식별된 운영체제에 고유한 운영체제 특성 패턴을 제공하는 맞춤형 핑거프린트를 생성하여, 식별 목적으로 운영체제의 이름을 제공해야 합니다.

시스템이 호스트의 운영체제를 확인할 수 없으면 호스트에 대한 취약성도 식별할 수 없습니다. 시스템은 각 호스트에 대한 취약성 목록을 운영체제 핑거프린트에서 가져오기 때문입니다. 예를 들어 Microsoft Windows를 실행하는 호스트를 탐지하는 경우 시스템은 탐지된 Windows 운영체제를 기반으로 해당 호스트에 대한 호스트 프로파일을 추가하는 저장된 Microsoft Windows 취약성 목록을 가지고 있습니다.

예를 들어 Microsoft Windows의 새 베타 버전을 실행하는 디바이스가 네트워크에 여러 개 있는 경우 시스템은 해당 운영체제를 식별하거나 호스트에 취약성을 매핑할 수 없습니다. 그러나 시스템에 Microsoft Windows에 대한 취약성 목록이 있음을 알고 있다면, 호스트 중 하나에 대한 맞춤형 핑거프린트를 생성해 동일한 운영체제를 실행하는 다른 호스트의 식별에 이를 활용할 수 있습니다. 핑거프린트에 Microsoft Windows에 대한 취약성 목록의 매핑을 포함하여, 해당 목록을 핑거프린트와 일치하는 각 호스트와 연결할 수 있습니다.

맞춤형 핑거프린트를 생성할 때, management center은(는) 동일한 운영체제를 실행하는 호스트의 해당 핑거프린트와 관련된 취약성 집합을 나열합니다. 생성한 맞춤형 핑거프린트에 취약성이 매핑되어 있지 않으면, 시스템은 핑거프린트를 사용하여 사용자가 핑거프린트에서 제공하는 맞춤형 운 체제 정보를 할당합니다. 이전에 탐지한 호스트에서 나오는 새 트래픽을 확인하면, 시스템은 새 핑거프

린트 정보를 이용해 호스트를 업데이트합니다. 또한 시스템은 새 핑거프린트를 이용해 새로운 호스트와 호스트를 처음으로 탐지했을 때의 운영체제를 식별합니다.

맞춤형 핑거프린트를 만들기 전에, 호스트가 올바르게 식별되지 않는 이유를 파악하여 맞춤형 핑거프린트가 실용적인 해결책인지 결정해야 합니다.

시스템에서 두 가지 유형의 핑거프린트를 생성할 수 있습니다.

- 클라이언트 핑거프린트 - 호스트가 네트워크의 다른 호스트에서 실행 중인 TCP 애플리케이션에 연결될 때 전송하는 SYN 패킷을 기반으로 운영체제를 식별합니다.
- 서버 핑거프린트 - 실행 중인 TCP 애플리케이션에 대한 수신 연결에 응답하기 위해 호스트가 사용하는 SYN-ACK 패킷을 기반으로 운영체제를 식별합니다.

참고 클라이언트 및 서버 핑거프린트가 동일한 호스트와 일치한다면 클라이언트 핑거프린트를 사용합니다.

핑거프린트를 생성한 후에는 활성화해야 시스템이 해당 핑거프린트를 호스트와 연결할 수 있습니다.

관련 항목

클라이언트에 대한 맞춤형 핑거프린트 생성, 7 페이지
서버에 대한 맞춤형 핑거프린트 생성, 9 페이지

핑거프린트 관리

핑거프린트를 생성 및 활성화한 후에는 원하는 대로 내용을 수정하거나 취약성 매핑을 추가할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Custom Operating Systems(**맞춤형 운영체제**)**를 클릭합니다. 핑거프린트 생성을 위해 데이터를 기다리는 시스템은 핑거프린트가 생성될 때까지 10초마다 페이지를 자동으로 새로 고칩니다.

단계 **3** 맞춤형 핑거프린트를 관리합니다.

- 활성화/비활성화 - 핑거프린트 활성화 및 비활성화, 5 페이지에 설명된 대로 핑거프린트를 활성화하거나 비활성화합니다.
- 생성 - 클라이언트에 대한 맞춤형 핑거프린트 생성, 7 페이지 및 서버에 대한 맞춤형 핑거프린트 생성, 9 페이지에 설명된 대로 핑거프린트를 생성합니다.
- 편집 - 활성 핑거프린트 편집, 5 페이지 및 비활성 핑거프린트 편집, 6 페이지에 설명된 대로 핑거프린트를 편집합니다.

- 삭제 - 삭제할 핑거프린트 옆에 있는 **Delete(**삭제**)** ( )을 클릭하고 **OK(**확인**)**를 눌러 확인합니다. 비활성화된 지문만 삭제할 수 있습니다.

핑거프린트 활성화 및 비활성화

맞춤형 핑거프린트는 반드시 활성화해야 시스템에서 이를 사용하여 호스트를 식별할 수 있습니다. 새 핑거프린트가 활성화되면 시스템은 이전에 검색된 호스트를 새 핑거프린트를 이용해 다시 식별하고 새 호스트를 검색합니다.

핑거프린트 사용을 중지하고 싶다면 먼저 비활성화해야 합니다. 핑거프린트를 비활성화하면 사용은 중지되지만 시스템에서 삭제되지는 않습니다. 핑거프린트를 비활성화하면 운영체제는 핑거프린트를 사용하는 호스트에 대해 unknown(알 수 없음)으로 표시됩니다. 호스트가 다시 탐지되고 다른 활성 핑거프린트와 일치한다면, 호스트는 해당 활성 핑거프린트로 식별됩니다.

핑거프린트를 삭제하면 시스템에서 완전히 제거됩니다. 비활성화한 핑거프린트는 삭제할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Custom Operating Systems(**맞춤형 운영체제**)**를 클릭합니다.

단계 **3** 활성화하거나 비활성화할 핑거프린트 옆에 있는 슬라이더를 클릭합니다.

참고 생성한 핑거프린트가 유효한 경우에만 활성화 옵션을 사용할 수 있습니다. 슬라이더를 사용할 수 없다면 핑거프린트를 다시 생성해 보십시오.

활성 핑거프린트 편집

핑거프린트가 활성 상태이면 핑거프린트 이름, 설명, 맞춤형 운영체제 표시 등을 수정하고 추가 취약성을 매핑할 수 있습니다.

핑거프린트 이름, 설명, 맞춤형 운영체제 표시 등을 수정하고 추가 취약성을 매핑할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** 맞춤형 운영체제를 클릭합니다.

단계 **3** 편집할 핑거프린트 옆에 있는 **Edit(**수정**)** (✎)을 클릭합니다.

단계 **4** 필요하다면 핑거프린트 이름, 설명 및 맞춤형 OS 표시를 수정합니다.

단계 **5** 취약성 매핑을 삭제하려면 페이지의 **Pre-Defined OS Product Maps(**사전 정의된 운영체제 제품 맵**)** 섹션에서 매핑 옆에 있는 **Delete(**삭제**)**를 클릭합니다.

단계 **6** 취약성 매핑에 대한 운영체제를 더 추가하려면 **Product(**제품**)**를 선택하고, 해당하는 경우 **Major Version(**주 버전**)**, **Minor Version(**부 버전**)**, **Revision Version(**개정 버전**)**, **Build(**빌드**)**, **Patch(**패치**)**, **Extension(**확장**)**을 선택한 다음 **Add OS Definition(**운영체제 정의 추가**)**를 클릭합니다.

취약성 매핑이 **Pre-Defined OS Product Maps(**사전 정의된 운영체제 제품 맵**)** 목록에 추가됩니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

비활성 핑거프린트 편집

핑거프린트가 비활성 상태이면 핑거프린트의 모든 요소를 수정한 후 Secure Firewall Management Center에 다시 제출할 수 있습니다. 여기에는 핑거프린트 유형, 목적지 IP 주소와 포트, 취약성 매핑 등 핑거프린트 생성 시 지정한 모든 속성이 포함됩니다. 비활성 핑거프린트를 편집하고 다시 제출하면 시스템에 다시 제출되며, 클라이언트 핑거프린트인 경우 활성화하기 전에 어플라이언스에 트래픽을 다시 전송해야 합니다. 비활성 핑거프린트에 대해서는 단일 취약성 매핑만 선택할 수 있습니다. 핑거프린트를 활성화한 후 추가 운영체제 및 버전을 취약성 목록에 매핑할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Custom Operating Systems(**맞춤형 운영체제**)**를 클릭합니다.

단계 **3** 편집할 핑거프린트 옆에 있는 **Edit(**수정**)** (✎)을 클릭합니다.

단계 **4** 필요한 대로 핑거프린트를 수정합니다.

- 클라이언트 핑거프린트를 수정하는 경우에는 클라이언트에 대한 맞춤형 핑거프린트 생성, 7 페이지 섹션을 참조하십시오.
- 서버 핑거프린트를 수정하는 경우에는 서버에 대한 맞춤형 핑거프린트 생성, 9 페이지 섹션을 참조하십시오.

단계 **5** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 클라이언트 핑거프린트를 수정한 경우 호스트에서 (핑거프린트를 수집하는) 어플라이언스로 트래픽을 전송해야 합니다.

클라이언트에 대한 맞춤형 핑거프린트 생성

클라이언트 핑거프린트는 호스트가 네트워크의 다른 호스트에서 실행 중인 TCP 애플리케이션에 연결될 때 전송하는 SYN 패킷을 기반으로 운영체제를 식별합니다.

management center이(가) 모니터링되는 호스트와 직접 연결되지 않은 경우, management center가 관리하며 클라이언트 핑거프린트 속성을 지정할 때 핑거프린트 처리할 호스트와 가장 가까운 디바이스를 지정할 수 있습니다.

핑거프린트 처리를 시작하기 전에 핑거프린트 처리할 호스트에 대한 다음 정보를 확인하십시오.

- 호스트 또는 management center을(를) 가져오기 위해 사용할 디바이스 간 네트워크 홉의 수 (Cisco는 management center 또는 디바이스를 호스트가 연결된 것과 동일한 서브넷에 연결할 것을 적극 권장합니다.)
- 호스트가 상주하는 네트워크에 연결된 네트워크 인터페이스(management center 또는 디바이스)
- 호스트의 실제 운영체제 벤더, 제품 및 버전
- 클라이언트 트래픽을 생성하기 위해 호스트에 액세스

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Custom Operating Systems(**맞춤형 운영체제**)**를 클릭합니다.

단계 **3** **Create Custom Fingerprint(**맞춤형 핑거프린트 만들기**)**를 클릭합니다.

단계 **4** **Device(**디바이스**)** 드롭다운 목록에서 핑거프린트 수집에 사용할 management center 또는 디바이스를 선택합니다.

단계 **5** **Fingerprint Name(**핑거프린트 이름**)**을 입력합니다.

단계 **6** **Fingerprint Description(**핑거프린트 설명**)**을 입력합니다.

단계 **7** **Fingerprint Type(**핑거프린트 유형**)** 목록에서 **Client(**클라이언트**)**를 선택합니다.

단계 **8** **Target IP Address(**목적지 **IP** 주소**)** 필드에 핑거프린트 처리할 호스트의 IP 주소를 입력합니다.

핑거프린트는 (호스트의 다른 IP 주소가 아닌) 사용자가 지정하는 호스트 IP 주소를 통과하는 트래픽만을 기반으로 합니다.

단계 **9** 핑거프린트를 수집하기 위해 선택했던 디바이스와 호스트 간 네트워크 홉의 수를 **Target Distance(**대상 거리**)** 필드에 입력합니다.

주의 이 값은 호스트에 대한 물리적 네트워크 홉의 실제 숫자여야 하며, 시스템에 의해 탐지된 홉의 수와 같을 수도 있고 다를 수도 있습니다.

단계 **10** 호스트가 상주하는 네트워크 세그먼트에 연결된 네트워크 인터페이스를 **Interface(**인터페이스**)** 목록에서 선택합니다.

주의 여러 가지 이유로, Cisco는 매니지드 디바이스의 센싱 인터페이스를 핑거프린트에 사용하지 않을 것을 권장합니다. 첫째, 센싱 인터페이스가 span 포트에 있으면 핑거프린트가 작동하지 않습니다. 또한 디바이스에서 센싱 인터페이스를 사용하면 디바이스는 핑거프린트를 수집하는 데 걸리는 시간 동안 네트워크의 모니터링이 중단됩니다. 하지만 관리 인터페이스 또는 기타 사용 가능한 네트워크 인터페이스를 이용하면 핑거프린트 수집을 수행할 수 있습니다. 디바이스에서 어떤 인터페이스가 센싱 인터페이스인지 모르는 경우, 핑거프린트 처리에 사용 중인 특정 모델의 *Installation Guide(*설치 안내서*)*를 참조하십시오.

단계 **11** 핑거프린트 처리된 호스트에 대한 호스트 프로파일에 맞춤형 정보를 표시하려면(또는 핑거프린트 처리할 호스트가 **OS Vulnerability Mappings(**운영체제 취약성 매핑**)** 섹션에 상주하지 않는 경우), **Use Custom OS Display(**맞춤형 운영체제 표시 사용**)**를 선택하고 다음에 대해 호스트 프로파일에 표시할 값을 제공합니다.

- **Vendor String** 필드에 운영체제의 벤더 이름을 입력합니다. 예를 들어 Microsoft Windows의 벤더는 Microsoft입니다.
- **Product String** 필드에 운영체제의 제품 이름을 입력합니다. 예를 들어 Microsoft Windows 2000의 제품 이름은 Windows입니다.
- **Version String** 필드에 운영체제의 버전 번호를 입력합니다. 예를 들어 Microsoft Windows 2000의 버전 번호는 2000입니다.

단계 **12** OS Vulnerability Mappings섹션에서 취약성 매핑에 사용할 운영 체제, 제품 및 버전을 선택합니다.

핑거프린트를 사용하여 매칭 호스트에 대한 취약성을 식별하려는 경우 또는 맞춤형 운영체제 표시 정보를 할당하지 않은 경우 이 섹션에서 **Vendor(**벤더**)** 및 **Product(**제품**)** 값을 지정해야 합니다.

운영체제의 모든 버전에 대해 취약성을 매핑하려면 **Vendor(**벤더**)** 및 **Product(**제품**)** 값만 지정하십시오.

참고 선택한 운영체제에 **Major Version(**주 버전**)**, **Minor Version(**부 버전**)**, **Revision Version(**개정 버전**)**, **Build(**빌드**)**, **Patch(**패치**)** 및 **Extension(**확장**)** 드롭다운 목록의 옵션이 모두 적용되지는 않을 수도 있습니다. 또한 핑거프린트 처리하려는 운영체제와 일치하는 정의가 목록에 나타나지 않으면 해당 값을 비워둘 수도 있습니다. 핑거프린트에서 OS 취약성 매핑을 생성하지 않으면 시스템은 핑거프린트에 의해 식별되는 호스트가 포함된 취약성 목록을 할당하는 데 핑거프린트를 사용할 수 없습니다.

예제**:**

예를 들어 맞춤형 핑거프린트를 통해 Redhat Linux 9의 취약성 목록을 매칭 호스트에 할당하려면 벤더로 **Redhat, Inc.**, 제품으로 **Redhat Linux**, 주 버전으로 **9**를 선택합니다.

예제**:**

Palm OS의 모든 버전을 추가하려면 **Vendor(**벤더**)** 목록에서 **PalmSource, Inc.**, **Product(**제품**)** 목록에서 **Palm OS**를 선택하고 다른 모든 목록은 기본 설정으로 두십시오.

단계 **13** **Create(**생성**)**를 클릭합니다.

상태에서 `New(신규)`가 잠시 표시된 후 `Pending(대기 중)`으로 변경되며, 핑거프린트가 트래픽을 확인할 때까지는 계속 대기 중으로 표시됩니다. 트래픽이 확인되면 상태는 `Ready(준비)`로 변경됩니다.

Custom Fingerprint(맞춤형 핑거프린트) 상태 페이지는 문제의 호스트에서 데이터를 수신할 때까지 10초마다 갱신합니다.

단계 **14** 목적지 IP 주소로 지정된 IP 주소를 사용하여, 핑거프린트 처리하려는 호스트에 액세스하고 어플라이언스에 대한 TCP 연결을 시작합니다.

정확한 핑거프린트를 생성하려면 핑거프린트를 수집하는 어플라이언스에 트래픽이 표시되어야 합니다. 스위치를 통해 연결된 경우 어플라이언스 외의 시스템에 대한 트래픽은 시스템에 표시되지 않을 수 있습니다.

예제**:**

예를 들어 핑거프린트 처리할 호스트에서 management center의 웹 인터페이스에 액세스하거나 호스트에서 management center의 SSH에 액세스합니다. SSH를 사용한다면 아래 명령을 사용하십시오. 여기서 localIPv6address는 7단계에서 지정되었고 현재 호스트에 할당된 IPv6 주소이며, DCmanagementIPv6address는 management center의 관리 IPv6 주소입니다. Custom Fingerprint(맞춤형 핑거프린트) 페이지가 다시 로드되어 “Ready(준비)” 상태가 됩니다.

```
ssh -b localIPv6address DCmanagementIPv6address
```

다음에 수행할 작업

- 핑거프린트 활성화 및 비활성화, 5 페이지에 설명된 대로 핑거프린트를 활성화합니다.

서버에 대한 맞춤형 핑거프린트 생성

서버 핑거프린트는 실행 중인 TCP 애플리케이션에 대한 수신 연결에 응답하기 위해 호스트가 사용하는 SYN-ACK 패킷을 기반으로 운영체제를 식별합니다. 시작하기 전에 핑거프린트 처리할 호스트에 대한 다음 정보를 확인하십시오.

- 호스트와 핑거프린트를 가져오기 위해 사용할 어플라이언스 간 네트워크 홉의 수 Cisco는 어플라이언스의 미사용 인터페이스를 호스트가 연결된 것과 동일한 서브넷에 연결할 것을 적극 권장합니다.
- 호스트가 상주하는 네트워크에 연결된 (어플라이언스 상의) 네트워크 인터페이스
- 호스트의 실제 운영체제 공급업체, 제품 및 버전
- 현재 사용되고 있지 않으며 호스트가 있는 네트워크에서 인증된 IP 주소

팁 management center이(가) 모니터링되는 호스트와 직접 연결되지 않은 경우 서버 핑거프린트 속성을 지정할 때 핑거프린트 처리할 호스트와 가장 가까운 매니지드 디바이스를 지정할 수 있습니다.

프로시저

단계 1 **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 2 **Custom Operating Systems(**맞춤형 운영체제**)**를 클릭합니다.

단계 3 **Create Custom Fingerprint(**맞춤형 핑거프린트 만들기**)**를 클릭합니다.

단계 4 **Device(**디바이스**)** 목록에서 핑거프린트 수집에 사용할 management center 또는 매니지드 디바이스를 선택합니다.

단계 5 **Fingerprint Name(**핑거프린트 이름**)**을 입력합니다.

단계 6 **Fingerprint Description(**핑거프린트 설명**)**을 입력합니다.

단계 7 **Fingerprint Type(**핑거프린트 유형**)** 목록에서 **Server(**서버**)**를 선택해 서버 핑거프린트 옵션을 표시합니다.

단계 8 **Target IP Address(**목적지 **IP** 주소**)** 필드에 핑거프린트 처리할 호스트의 IP 주소를 입력합니다.

핑거프린트는 (호스트의 다른 IP 주소가 아닌) 사용자가 지정하는 호스트 IP 주소를 통과하는 트래픽만을 기반으로 합니다.

주의 버전 5.2 이상을 실행하는 어플라이언스에서만 IPv6 핑거프린트를 캡처할 수 있습니다.

단계 9 핑거프린트를 수집하기 위해 선택했던 디바이스와 호스트 간 네트워크 홉의 수를 **Target Distance(**대상 거리**)** 필드에 입력합니다.

주의 이 값은 호스트에 대한 물리적 네트워크 홉의 실제 숫자여야 하며, 시스템에 의해 탐지된 홉의 수와 같을 수도 있고 다를 수도 있습니다.

단계 10 호스트가 상주하는 네트워크 세그먼트에 연결된 네트워크 인터페이스를 **Interface(**인터페이스**)** 목록에서 선택합니다.

주의 여러 가지 이유로, Cisco는 매니지드 디바이스의 센싱 인터페이스를 핑거프린트에 사용하지 않을 것을 권장합니다. 첫째, 센싱 인터페이스가 span 포트에 있으면 핑거프린트가 작동하지 않습니다. 또한 디바이스에서 센싱 인터페이스를 사용하면 디바이스는 핑거프린트를 수집하는 데 걸리는 시간 동안 네트워크의 모니터링이 중단됩니다. 하지만 관리 인터페이스 또는 기타 사용 가능한 네트워크 인터페이스를 이용하면 핑거프린트 수집을 수행할 수 있습니다. 디바이스에서 어떤 인터페이스가 센싱 인터페이스인지 모르는 경우, 핑거프린트 처리에 사용 중인 특정 모델의 *Installation Guide(*설치 안내서*)*를 참조하십시오.

단계 11 **Get Active Ports(**활성 포트 얻기**)**를 클릭합니다.

단계 12 핑거프린트를 수집하기 위해 선택한 디바이스가 연결을 시작하도록 할 포트를 **Server Port(**서버 포트**)** 필드에 입력하거나, **Get Active Ports(**활성 포트 얻기**)** 드롭다운 목록에서 포트를 선택합니다.

호스트에 대해 열려 있음을 확인한 서버 포트라면 무엇이든 사용할 수 있습니다(예: 호스트가 웹 서버를 실행 중인 경우 80).

단계 **13** 호스트와의 통신을 시도하기 위해 사용할 IP 주소를 **Source IP Address(**소스 **IP** 주소**)** 필드에 입력합니다.

네트워크에서 사용하도록 인증되었지만 현재 사용되고 있지 않은 소스 IP 주소(예: 현재 사용되고 있지 않은 DHCP 풀 주소)를 사용해야 합니다. 이렇게 하면 핑거프린트를 생성하는 동안 일시적으로 다른 호스트를 오프라인으로 탐색하지 않아도 됩니다.

핑거프린트를 생성하는 동안에는 네트워크 검색 정책에서 해당 IP 주소의 모니터링을 제외해야 합니다. 이렇게 하지 않으면 네트워크 맵 및 검색 이벤트 보기가 해당 IP 주소로 표시되는 호스트에 대한 부정확한 정보와 뒤섞이게 됩니다.

단계 **14** **Source Subnet Mask(**소스 서브넷 마스크**)** 필드에 사용 중인 IP 주소의 서브넷 마스크를 입력합니다.

단계 **15** **Source Gateway(**소스 게이트웨이**)** 필드가 나타나면 호스트에 대한 경로를 설정하기 위해 사용해야 할 기본 게이트웨이 IP 주소를 입력합니다.

단계 **16** 핑거프린트 처리된 호스트에 대한 호스트 프로파일에 맞춤형 정보를 표시하려면 또는 사용하려는 핑거프린트 이름이 OS Definition(운영체제 정의) 섹션에 없다면 Custom OS Display(맞춤형 운영체제 표시) 섹션에서 **Use Custom OS Display(**맞춤형 운영체제 표시 사용**)**를 선택합니다.

호스트 프로파일에 표시할 다음에 대한 값을 제공합니다.

- **Vendor String** 필드에 운영체제의 벤더 이름을 입력합니다. 예를 들어 Microsoft Windows의 벤더는 Microsoft입니다.
- **Product String** 필드에 운영체제의 제품 이름을 입력합니다. 예를 들어 Microsoft Windows 2000의 제품 이름은 Windows입니다.
- **Version String** 필드에 운영체제의 버전 번호를 입력합니다. 예를 들어 Microsoft Windows 2000의 버전 번호는 2000입니다.

단계 **17** OS Vulnerability Mappings섹션에서 취약성 매핑에 사용할 운영 체제, 제품 및 버전을 선택합니다.

핑거프린트를 사용하여 매칭 호스트에 대한 취약성을 식별하려는 경우 또는 맞춤형 운영체제 표시 정보를 할당하지 않은 경우 이 섹션에서 Vendor(벤더) 및 Product(제품) 이름을 지정해야 합니다.

운영체제의 모든 버전에 대해 취약성을 매핑하려면 벤더 및 제품 이름만 지정하십시오.

참고 선택한 운영체제에 **Major Version(**주 버전**)**, **Minor Version(**부 버전**)**, **Revision Version(**개정 버전**)**, **Build(**빌드**)**, **Patch(**패치**)** 및 **Extension(**확장**)** 드롭다운 목록의 옵션이 모두 적용되지는 않을 수도 있습니다. 또한 핑거프린트 처리하려는 운영체제와 일치하는 정의가 목록에 나타나지 않으면 해당 값을 비워둘 수도 있습니다. 핑거프린트에서 OS 취약성 매핑을 생성하지 않으면 시스템은 핑거프린트에 의해 식별되는 호스트가 포함된 취약성 목록을 할당하는 데 핑거프린트를 사용할 수 없습니다.

예제**:**

예를 들어 맞춤형 핑거프린트를 통해 Redhat Linux 9의 취약성 목록을 매칭 호스트에 할당하려면 벤더로 **Redhat, Inc.**, 제품으로 **Redhat Linux**, 버전으로 **9**를 선택합니다.

예제**:**

Palm OS의 모든 버전을 추가하려면 **Vendor(**벤더**)** 목록에서 **PalmSource, Inc.**, **Product(**제품**)** 목록에서 **Palm OS**를 선택하고 다른 모든 목록은 기본 설정으로 두십시오.

단계 **18** **Create(**생성**)**를 클릭합니다.
Custom Fingerprint(맞춤형 핑거프린트) 상태 페이지는 10초마다 갱신되며 “Ready(준비)” 상태로 다시 로드되어야 합니다.

참고 핑거프린트 처리 중에 대상 시스템이 응답을 중지하면 상태에 `ERROR: No Response` 메시지가 나타납니다. 이 메시지가 표시된다면 핑거프린트를 다시 제출하십시오. 3~5분 정도 기다렸다가(시간은 대상 시스템에 따라 달라질 수 있음) **Edit(**수정**)** ( )을 클릭하여 Custom Fingerprint(맞춤형 핑거프린트) 페이지에 액세스한 다음 **Create(**생성**)**를 클릭합니다.

다음에 수행할 작업

- 핑거프린트 활성화 및 비활성화, 5 페이지에 설명된 대로 핑거프린트를 활성화합니다.

호스트 입력 데이터

서드파티의 네트워크 맵 데이터를 가져와 네트워크 맵을 보강할 수도 있습니다. 또한 운영체제나 애플리케이션 ID를 수정하여 또는 애플리케이션 프로토콜, 프로토콜, 호스트 속성, 웹 인터페이스를 사용하는 클라이언트 등을 삭제하여 호스트 입력 기능을 사용할 수 있습니다.

시스템에서는 운영체제 또는 애플리케이션의 현재 ID를 확인하기 위해 여러 소스의 데이터를 조정할 수 있습니다.

영향받는 호스트가 네트워크 맵에서 제거되면 서드파티 취약성을 제외한 모든 데이터가 폐기됩니다. 스크립트 설정 또는 파일 가져오기에 대한 자세한 내용은 *Firepower System Host Input API* 설명서 섹션을 참조하십시오.

가져온 데이터를 영향 상관관계에 포함하려면 데이터를 데이터베이스의 운영체제 및 애플리케이션 정의에 매핑해야 합니다.

서드파티 데이터 사용 요구 사항

서드파티 시스템의 검색 데이터를 자신의 네트워크로 가져올 수 있습니다. 하지만 Cisco 권장사항, 적응형 프로파일 업데이트 또는 영향 평가처럼 침입 및 검색 데이터를 함께 사용하는 기능을 활성화하려면, 최대한 많은 요소를 대응하는 정의에 매핑해야 합니다. 서드파티 데이터 사용을 위한 다음 요구 사항을 고려해 보십시오.

- 네트워크 자산에 대한 특정 데이터가 포함된 서드파티 시스템이 있는 경우 호스트 입력 기능을 사용하여 해당 데이터를 가져올 수 있습니다. 그러나 서드파티에서 제품 이름을 다르게 지정할 수 있으므로 서드파티 벤더, 제품 및 버전을 해당 Cicso 제품 정의에 매핑해야 합니다. 제품을 매핑한 후에는 영향 상관관계를 허용하기 위해 management center 설정에서 영향 평가를 위한 취약성 매핑을 활성화해야 합니다. 버전 또는 벤더가 없는 애플리케이션 프로토콜의 경우 management center 설정에서 애플리케이션 프로토콜에 대한 취약성을 매핑해야 합니다.

- 서드파티에서 패치 정보를 가져오고 해당 패치에 의해 수정된 모든 취약성을 무효 상태로 표시하려면 서드파티 수정 이름을 데이터베이스의 수정 정의에 매핑해야 합니다. 그러면 수정에 의해 해결된 모든 취약성이 해당 수정을 추가한 호스트에서 제거됩니다.
- 서드파티에서 운영체제 및 애플리케이션 프로토콜 취약성을 가져와서 영향 상관관계에 사용하려면 서드파티 취약성 식별 문자열을 데이터베이스의 취약성에 매핑해야 합니다. 관련된 취약성이 있는 클라이언트가 많고 영향 평가에 클라이언트가 사용되지만, 서드파티 클라이언트 취약성을 가져와서 매핑할 수는 없습니다. 취약성을 매핑한 후에는 management center 설정에서 영향 평가를 위한 서드파티 취약성 매핑을 활성화해야 합니다. 벤더 또는 버전 정보가 없는 애플리케이션 프로토콜을 취약성에 매핑하려면 관리 사용자는 management center 설정에서 애플리케이션에 대한 취약성을 매핑해야 합니다.
- 애플리케이션 데이터를 가져와 영향 상관관계에 사용하려는 경우 각 애플리케이션 프로토콜에 대한 벤더 문자열을 해당 Cisco 애플리케이션 프로토콜 정의에 매핑해야 합니다.

관련 항목

서드파티 제품 매핑, 13 페이지
서드파티 제품 수정 매핑, 15 페이지
서드파티 취약성 매핑, 16 페이지
맞춤형 제품 매핑 생성, 17 페이지

서드파티 제품 매핑

사용자 입력 기능을 통해 서드파티의 데이터를 네트워크 맵에 추가할 때에는 서드파티에서 사용하는 공급업체, 제품 및 버전 이름을 Cisco 제품 정의에 매핑해야 합니다. 제품을 Cisco 정의에 매핑하면 이러한 정의에 따라 취약성이 할당됩니다.

마찬가지로 서드파티에서 패치 정보(예: 패치 관리 제품)를 가져오는 경우, 수정의 이름을 데이터베이스의 적절한 공급업체와 제품 그리고 해당 수정에 매핑해야 합니다.

서드파티 제품 매핑

서드파티의 데이터를 가져오는 경우 취약성을 할당하고 해당 데이터로 영향 상관관계를 수행하려면 Cisco 제품을 서드파티 이름에 매핑해야 합니다. 제품을 매핑하면 Cisco 취약성 정보가 서드파티 제품 이름과 연결되며, 이를 통해 시스템에서는 해당 데이터를 사용해 영향 상관관계를 수행할 수 있습니다.

호스트 입력 가져오기 기능을 사용하여 데이터를 가져올 경우 AddScanResult 기능을 사용하여 가져오는 동안 서드파티 제품을 운영체제 및 애플리케이션 취약성에 매핑해야 합니다.

예를 들어 Apache Tomcat을 애플리케이션으로 나열하는 서드파티의 데이터를 가져오며 해당 제품의 버전이 6임을 안다면, 다음 조건 하에 서드파티 맵을 추가할 수 있습니다.

- **Vendor Name(**벤더 이름**)**을 `Apache`로 설정합니다.
- **Product Name(**제품 이름**)**을 `Tomcat`으로 설정합니다.
- **Apache**를 **Vendor(**벤더**)** 드롭다운 목록에서 선택합니다.

- **Tomcat**을 **Product(**제품**)** 드롭다운 목록에서 선택합니다.
- **6**를 **Version(**버전**)** 드롭다운 목록에서 선택합니다.

이렇게 매핑하면 Apache Tomcat 6에 대한 취약성이 Apache Tomcat에 대한 애플리케이션 목록과 함께 호스트에 할당됩니다.

버전 또는 벤더가 없는 애플리케이션의 경우 Secure Firewall Management Center 설정에서 애플리케이션 유형에 대한 취약성을 매핑해야 합니다. 관련된 취약성이 있는 클라이언트가 많고 영향 평가에 클라이언트를 사용했지만, 서드파티 클라이언트 취약성을 가져와서 매핑할 수는 없습니다.

팁 또 다른 Secure Firewall Management Center에서 이미 서드파티 매핑을 생성한 경우 이를 내보낸 다음 이 management center로 가져올 수 있습니다. 그런 다음 가져온 매핑을 필요에 맞게 수정할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Application Detectors(**애플리케이션 탐지기**)**을(를) 선택합니다.

단계 **2** **User Third-Party Mappings(**사용자 서드파티 매핑**)**을 클릭합니다.

단계 **3** 다음 2가지 옵션을 사용할 수 있습니다.

- 생성 - 새 맵 집합을 생성하려면 **Create Product Map Set(**제품 맵 집합 생성**)**를 클릭합니다.
- 편집 - 기존 맵 집합을 편집하려면 수정할 맵 집합 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다. **View(**보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** **Mapping Set Name(**집합 이름 매핑**)**을 입력합니다.

단계 **5** **Description(**설명**)**을 입력합니다.

단계 **6** 다음 2가지 옵션을 사용할 수 있습니다.

- 생성 - 서드파티 제품을 매핑하려면 **Add Product Map(**제품 맵 추가**)**을 클릭합니다.
- 편집 - 기존 서드파티 제품 맵을 편집하려면 수정할 맵 집합 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다. **View(**보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **7** 서드파티 제품이 사용하는 **Vendor String**을 입력합니다.

단계 **8** 서드파티 제품이 사용하는 **Product String**을 입력합니다.

단계 **9** 서드파티 제품이 사용하는 **Version String**을 입력합니다.

단계 **10** Product Mappings(제품 매핑) 섹션에서 **Vendor(**벤더**)**, **Product(**제품**)**, **Major Version(**주 버전**)**, **Minor Version(**부 버전**)**, **Revision Version(**개정 버전**)**, **Build(**빌드**)**, **Patch(**패치**)**, **Extension(**확장**)** 필드의 취약성 매핑에 사용할 운영체제, 제품, 버전을 선택합니다.

예제**:**

서드파티 문자열로 이름이 구성된 제품을 실행 중인 호스트에서 Redhat Linux 9의 취약성을 사용하도록 하려면 벤더로 **Redhat, Inc.,** 제품으로 **Redhat Linux**, 버전으로 **9**를 선택합니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

서드파티 제품 수정 매핑

수정 이름을 데이터베이스에 있는 특별한 수정 집합에 매핑하면, 서드파티 패치 관리 애플리케이션에서 데이터를 가져와 호스트 집합에 수정을 적용할 수 있습니다. 수정 이름을 호스트로 가져오면 시스템은 해당 수정으로 해결된 모든 취약성을 해당 호스트에 대해 무효 상태로 표시합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Application Detectors(**애플리케이션 탐지기**)**을(를) 선택합니다.

단계 **2** **User Third-Party Mappings(**사용자 서드파티 매핑**)**을 클릭합니다.

단계 **3** 다음 2가지 옵션을 사용할 수 있습니다.

- 생성 - 새 맵 집합을 생성하려면 **Create Product Map Set(**제품 맵 집합 생성**)**를 클릭합니다.
- 편집 - 기존 맵 집합을 편집하려면 수정할 맵 집합 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다. **View(**보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** **Mapping Set Name(**집합 이름 매핑**)**을 입력합니다.

단계 **5** **Description(**설명**)**을 입력합니다.

단계 **6** 다음 2가지 옵션을 사용할 수 있습니다.

- 생성 - 서드파티 제품을 매핑하려면 **Add Fix Map(**수정 맵 추가**)**을 클릭합니다.
- 편집 - 기존 서드파티 제품 맵을 편집하려면 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다. **View(**보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **7** 매핑할 수정의 이름을 **Third-Party Fix Name(**서드파티 수정 이름**)** 필드에 입력합니다.

단계 **8** **Product Mappings(**제품 매핑**)** 섹션에서, 수정 매핑에 사용할 운영체제, 제품 및 버전을 다음 표에서 선택합니다.

- 벤더
- 제품
- 주 버전
- 부 버전
- 개정 버전
- 구축
- 패치
- 확장

예제**:**

매핑을 통해 Redhat Linux 9의 수정을 패치가 적용되는 호스트에 할당하려면 벤더로 **Redhat, Inc.**, 제품으로 **Redhat Linux**, 버전으로 **9**을 선택합니다.

단계 **9** **Save(**저장**)**를 클릭하여 수정 맵을 저장합니다.

서드파티 취약성 매핑

서드파티의 취약성 정보를 VDB에 추가하려면 가져온 각 취약성에 대한 서드파티 식별 문자열을 기존 SVID, Bugtraq 또는 SID에 매핑해야 합니다. 취약성에 대한 매핑을 생성하면 네트워크 맵에서 호스트로 가져온 모든 취약성에 대해 매핑이 제대로 작동하며, 그러한 취약성에 대해 영향 상관관계를 수행할 수 있게 됩니다.

상관관계가 발생하도록 하려면 서드파티 취약성에 대한 영향 상관관계를 활성화해야 합니다. 버전 또는 벤더가 없는 애플리케이션의 경우 Secure Firewall Management Center 설정에서 애플리케이션 유형에 대한 취약성을 매핑해야 합니다.

관련된 취약성이 있는 클라이언트가 많고 영향 분석에 클라이언트가 사용되지만, 영향 평가에는 서드파티 클라이언트 취약성을 사용할 수 없습니다.

팁 또 다른 Secure Firewall Management Center에서 이미 서드파티 매핑을 생성한 경우 이를 내보낸 다음 이 management center로 가져올 수 있습니다. 그런 다음 가져온 매핑을 필요에 맞게 수정할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Application Detectors(**애플리케이션 탐지기**)**을(를) 선택합니다.

단계 **2** **User Third-Party Mappings(**사용자 서드파티 매핑**)**을 클릭합니다.

단계 **3** 다음 2가지 옵션을 사용할 수 있습니다.

- 생성 - 새로운 취약성 집합을 생성하려면 **Create Vulnerability Map Set(**취약성 맵 집합 생성**)**를 클릭합니다.
- 편집 - 기존 취약성 집합을 수정하려면 취약성 집합 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다. **View(**보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** **Add Vulnerability Map(**취약성 맵 추가**)**을 클릭합니다.

단계 **5** **Vulnerability ID(**취약성 **ID)** 필드에 취약성에 대한 서드파티 ID를 입력합니다.

단계 **6** **Vulnerability Description(**취약성 설명**)**을 입력합니다.

단계 **7** 선택 사항:

- **Snort Vulnerability ID Mappings(Snort** 취약성 **ID** 매핑**)** 필드에 Snort ID을(를) 입력합니다.
- **SVID Mappings(SVID** 매핑**)** 필드에 레거시 취약성 ID를 입력합니다.

- **Bugtraq Vulnerability ID Mappings(Bugtraq** 취약성 **ID** 매핑**)** 필드에 Bugtraq 식별 번호를 입력합니다.

단계 **8** **Add(**추가**)**를 클릭합니다.

관련 항목

네트워크 검색 취약성 영향 평가 활성화

맞춤형 제품 매핑

제품 매핑을 사용해 서드파티에 의한 서버 입력이 적절한 Cisco 정의와 연결되었는지 확인할 수 있습니다. 제품 매핑을 정의 및 활성화하면, 매핑된 벤더 문자열이 있는 모니터링되는 호스트의 모든 서버 또는 클라이언트는 맞춤형 제품 매핑을 사용합니다. 따라서 서버의 벤더, 제품 및 버전을 명시적으로 설정하는 대신 특정 벤더 문자열로 네트워크 맵에 있는 모든 서버에 대해 취약성을 매핑할 수도 있습니다.

맞춤형 제품 매핑 생성

시스템이 서버를 VDB의 벤더나 제품에 매핑하지 못한다면, 수동으로 매핑을 생성할 수 있습니다. 맞춤형 제품 매핑을 활성화하면 시스템은 지정한 벤더 및 제품에 대한 취약성을, 해당 벤더 문자열이 발생하는 네트워크 맵의 모든 서버에 매핑합니다.

참고 맞춤형 제품 매핑은 애플리케이션 데이터의 소스(예: Nmap, 호스트 입력 기능 또는 Firepower System 자체)와 상관없이 애플리케이션 프로토콜의 모든 경우에 적용됩니다. 그러나 호스트 입력 기능을 사용하여 가져온 데이터에 대한 서드파티 취약성 매핑이 맞춤형 제품 매핑을 통해 설정한 매핑과 충돌하면, 서드파티 취약성 매핑은 맞춤형 제품 매핑을 재정의하며 입력이 발생할 경우 서드파티 취약성 매핑 설정을 사용합니다.

제품 매핑의 목록을 생성한 다음, 각 목록을 활성화 또는 비활성화하여 여러 매핑의 사용을 동시에 활성화 또는 비활성화할 수 있습니다. 매핑할 벤더를 지정하면 시스템은 해당 벤더의 제품만 포함하도록 제품 목록을 업데이트합니다.

맞춤형 제품 매핑을 생성한 후에는 맞춤형 제품 매핑 목록을 활성화해야 합니다. 맞춤형 제품 매핑의 목록을 활성화하면, 시스템은 지정된 벤더 문자열이 발생할 때 모든 서버를 업데이트합니다. 호스트 입력 기능을 통해 가져온 데이터의 경우, 이 서버에 대해 제품 매핑을 이미 명시적으로 설정하지 않았다면 취약성이 업데이트됩니다.

예를 들어 회사에서 Apache Tomcat 웹 서버에 대한 배너를 `Internal Web Server`를 읽도록 수정하면, 벤더 문자열 `Internal Web Server`를 벤더 **Apache** 및 제품 **Tomcat**에 매핑한 다음 해당 매핑이 포함된 목록을 활성화할 수 있습니다. `Internal Web Server`라는 레이블의 서버가 나타나는 모든 호스트는 데이터베이스에 Apache Tomcat에 대한 취약성을 포함합니다.

팁 이 기능을 사용하면 규칙에 대한 SID를 또 다른 취약성에 매핑하여 취약성을 로컬 침입 규칙에 매핑할 수 있습니다.

프로시저

단계 1 **Policies(**정책**)** > **Application Detectors(**애플리케이션 탐지기**)**을(를) 선택합니다.
단계 2 **Custom Product Mappings(**맞춤형 제품 매핑**)**를 클릭합니다.
단계 3 **Create Custom Product Mapping List(**맞춤형 제품 매핑 목록**)**을 클릭합니다.
단계 4 **Custom Product Mapping List Name(**맞춤형 제품 매핑 목록 이름**)**을 입력합니다.
단계 5 **Add Vendor String(**벤더 문자열 추가**)**를 클릭합니다.
단계 6 선택한 벤더 및 제품 값에 매핑해야 할 애플리케이션을 식별하는 벤더 문자열을 **Vendor String** 필드에 입력합니다.
단계 7 매핑하고자 하는 벤더를 **Vendor(**벤더**)** 드롭다운 목록에서 선택합니다.
단계 8 매핑하고자 하는 제품을 **Product(**제품**)** 드롭다운 목록에서 선택합니다.
단계 9 **Add(**추가**)**를 클릭하여 매핑된 벤더 문자열을 목록에 추가합니다.
단계 10 선택적으로, 벤더 문자열 매핑을 목록에 더 추가하려면 필요에 따라 4~8단계를 반복합니다.
단계 11 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 맞춤형 제품 매핑 목록을 활성화합니다. 자세한 내용은 맞춤형 제품 매핑 활성화 및 비활성화, 19 페이지를 참고하십시오.

맞춤형 제품 매핑 목록 편집

벤더 문자열을 추가 또는 제거하거나 목록 이름을 변경하여 기존의 맞춤형 제품 매핑 목록을 수정할 수 있습니다.

프로시저

단계 1 **Policies(**정책**)** > **Application Detectors(**애플리케이션 탐지기**)**을(를) 선택합니다.
단계 2 **Custom Product Mappings(**맞춤형 제품 매핑**)**를 클릭합니다.
단계 3 편집할 제품 매핑 목록 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

View(보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 4 맞춤형 제품 매핑 생성, 17 페이지에 설명된 대로 목록을 변경합니다.

단계 **5** 완료하면 **Save(**저장**)**를 클릭합니다.

맞춤형 제품 매핑 활성화 및 비활성화

맞춤형 제품 매핑의 전체 목록 사용을 동시에 활성화 또는 비활성화할 수 있습니다. 맞춤형 제품 매핑 목록을 활성화하면, 매니지드 디바이스에 의해 탐지되었든 호스트 입력 기능을 통해 가져왔든, 해당 목록의 각 매핑이 지정된 벤더 문자열이 있는 모든 애플리케이션에 적용됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **Application Detectors(**애플리케이션 탐지기**)**을(를) 선택합니다.

단계 **2** **Custom Product Mappings(**맞춤형 제품 매핑**)**를 클릭합니다.

단계 **3** 맞춤형 제품 매핑 목록 옆에 있는 슬라이더를 클릭해 매핑을 활성화하거나 비활성화합니다.

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

호스트 입력 클라이언트 설정

호스트 입력 기능을 이용하면 다른 어플라이언스에서 실행 중인 클라이언트 프로그램에서 management center의 네트워크 맵을 업데이트할 수 있습니다. 예를 들어 네트워크 맵에서 호스트를 추가 또는 삭제하거나, 호스트 OS 및 서비스 정보를 업데이트하는 식입니다. 자세한 내용은 *Firepower System Host Input API* 설명서를 참고하십시오.

원격 클라이언트를 실행하기 전에 Host Input Client(호스트 입력 클라이언트) 페이지에서 클라이언트를 management center의 피어 데이터베이스에 추가해야 합니다. 또한 management center에서 생성된 인증 인증서를 클라이언트에 복사해야 합니다. 이상의 완료하려면 클라이언트를 management center에 연결할 수 있습니다.

다중 도메인 구축에서는 모든 도메인에서 클라이언트를 만들 수 있습니다. 인증 인증서가 있으면 클라이언트는 클라이언트 인증서의 도메인과 완결된 모든 리프 도메인에 대한 네트워크 앱 업데이트를 전송할 수 있습니다. 상위 도메인에 대한 인증서를 만든다면(또는 하위 도메인 추가 후 인증서 도메인이 상위 도메인이 된다면), 해당 인증서를 사용하는 모든 클라이언트는 *Firepower System Host Input API* 설명서에 설명된 대로 각 트랜잭션을 이용해 대상 리프 도메인을 지정해야 합니다.

Host Input Client(호스트 입력 클라이언트)는 현재 도메인과 연결된 클라이언트만 표시하므로, 인증서를 다운로드하거나 취소하려면 클라이언트가 생성된 도메인으로 전환해야 합니다.

이 연결은 TLS 1.2를 사용합니다.

프로시저

단계 **1** **Integration(**통합**)** > **Other Integrations(**기타 통합**)**을(를) 선택합니다.

단계 **2** **Host Input Client(**호스트 입력 클라이언트**)**를 클릭합니다.

단계 **3** **Create Client(**클라이언트 생성**)**를 클릭합니다.

단계 **4** **Hostname(**호스트 이름**)** 필드에 호스트 입력 클라이언트를 실행하는 호스트의 IP 주소 또는 호스트 이름을 입력합니다.

참고 DNS 확인을 설정하지 않은 경우, IP 주소를 사용해야 합니다.

단계 **5** 인증서 파일을 암호화하려면, **Password(**비밀번호**)** 필드에 비밀번호를 입력합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.
호스트 입력 서비스는 이제 management center의 포트 8307에 대한 호스트의 액세스를 허용하며, 클라이언트-서버 인증 중에 사용할 인증 인증서를 생성합니다.

단계 **7** 인증서 파일 옆에 있는 **Download(**다운로드**)** ( )를 클릭합니다.

단계 **8** SSL/TLS 인증을 위해 클라이언트에서 사용하는 디렉터리에 인증서 파일을 저장합니다.

단계 **9** 클라이언트에 대한 액세스를 취소하려면 제거할 호스트 옆에 있는 삭제 **Delete(**삭제**)** ( )를 클릭합니다.

Nmap 스캐닝

Firepower System 네트워크 트래픽의 패시브 분석을 통해 네트워크 맵을 기반 으로합니다. 이 수동 분석을 통해 얻은 정보가 유지할 수 있는 경우에 따라 시스템 조건에 따라 완료 합니다. 그러나 호스트 전체 정보를 확보 하는 데 적극적으로 검색할 수 있습니다. 예를 들어, 호스트가 열린 포트에서 실행 중인 서버를 가지고 있지만 시스템이 네트워크를 모니터링하는 동안 서버가 트래픽을 수신하거나 전송하지 않은 경우, 시스템은 해당 서버에 대한 정보를 네트워크 맵에 추가하지 않습니다. 그러나 활성 스캐너를 사용하여 해당 호스트를 직접 검색하면 프레즌스 서버를 탐지할 수 있습니다.

Firepower System Nmap™, 네트워크 탐사 및 보안 감사 오픈 소스 활성 스캐너는 통합됩니다.

Nmap을 사용하여 호스트를 검색할 때 시스템은 다음과 같이 합니다.

- 해당 호스트에 대 한 호스트 프로 파일의 서버 목록에 이전에 탐지 개방 포트 서버를 추가합니다. 호스트 프로파일에는 필터링되거나 닫힌 TCP 포트 또는 UDP 포트에서 검색된 서버가 검색 결과 섹션에 나열되어 있습니다. Nmap은 기본적으로 1660개 이상의 TCP 포트를 검색합니다.

  시스템이 Nmap 검사에서 식별 된 서버와 해당 서버 정의 하는 경우 시스템은 해당 Cisco 서버 정의를 서버에 대 한 Nmap 사용 하 여 이름을 매핑합니다.

- 검색 결과를 1500개 이상의 알려진 운영 체제 지문과 비교하여 운영 체제를 결정하고 각 운영 체제에 점수를 부여합니다. 호스트에 할당된 운영 체제는 점수가 가장 높은 운영 체제 지문입니다.

  시스템은 Nmap 운영 체제 이름을 Cisco 운영 체제 정의에 매핑합니다.

- 서버를 추가 및 운영 체제에 대 한 호스트에는 취약성을 할당합니다.

참고:

- Nmap이 호스트 프로파일에 결과를 추가하기 전에 호스트가 네트워크 맵에 존재해야 합니다.

- 호스트가 네트워크 맵에서 삭제되면 해당 호스트에 대한 Nmap 검색 결과가 모두 삭제됩니다.

팁 일부 검색 옵션(예: 포트 스캔)은 대역폭이 낮은 네트워크에 상당한 부하를 가할 수 있습니다. 네트워크 사용량이 적은 기간 동안 실행되도록 이와 같은 예약을 스캔합니다.

검색에 사용되는 기본 Nmap 기술에 대한 자세한 내용은 http://insecure.org/의 Nmap 설명서를 참조하십시오.

Nmap 교정 옵션

Nmap 교정을 생성하여 Nmap 스캔에 대한 설정을 정의합니다. Nmap 교정은 상관관계 정책에서 응답으로 사용하거나, 온디맨드 방식으로 실행하거나, 특정 시간에 실행되도록 예약할 수 있습니다.

Nmap 제공 서버 및 운영체제 데이터는 또 다른 Nmap 스캔을 실행할 때까지 고정 상태로 유지됩니다. Nmap을 사용하여 호스트에서 운영체제 및 서버 데이터를 스캔하려는 경우 Nmap 제공 운영체제 및 서버 데이터를 최신 상태로 유지하기 위해 정기적인 예약 스캔을 설정할 수 있습니다.

다음 표에서는 Nmap 교정에서 구성할 수 있는 옵션에 대해 설명합니다.

표 *1: Nmap* 교정 옵션

옵션	설명	해당 **Nmap** 옵션
이벤트에서 어떤 주소를 스캔하겠습니까?	상관관계 규칙에 대한 응답으로 Nmap 스캔을 사용할 때 이벤트의 어떤 주소를 스캔할 것인지, 소스 호스트 주소인지 대상 호스트 주소인지 아니면 둘 다인지를 제어하는 다음 옵션 중 하나를 선택합니다. • **Scan Source and Destination Addresses(**소스 및 대상 주소 스캔**)**는 이벤트에서 소스 IP 주소 및 대상 IP 주소로 표시되는 호스트를 스캔합니다. • **Scan Source Address Only(**소스 주소만 스캔**)**은 이벤트의 소스 IP 주소가 나타내는 호스트를 스캔합니다. • **Scan Destination Address Only(**대상 주소만 스캔**)**은 이벤트의 대상 IP 주소가 나타내는 호스트를 스캔합니다.	해당 없음

옵션	설명	해당 Nmap 옵션
스캔 유형	Nmap이 포트를 스캔하는 방법을 선택합니다. • **TCP Syn** 스캔은 완전한 TCP 핸드셰이크를 사용하지 않은 채 수천 개의 포트에 빠르게 연결합니다. 이 옵션을 사용하면 TCP 연결을 시작하기만 하고 완료하지 않음으로써, `admin` 계정이 원시 패킷 액세스 권한을 가지고 있거나 IPv6이 실행되지 않고 있는 호스트의 스텔스(stealth) 모드에서 빠르게 스캔할 수 있습니다. 호스트가 TCP Syn 스캔에서 전송된 Syn 패킷을 인식하면 Nmap은 연결을 재설정합니다. • **TCP Connect** 스캔은 `connect()` 시스템 호출을 사용하여 호스트의 운영체제를 통한 연결을 엽니다. management center 또는 매니지드 디바이스의 `admin` 사용자가 호스트에 대한 원시 패킷 권한을 가지고 있지 않거나 현재 IPv6 네트워크를 스캔 중인 경우 TCP Connect 스캔을 사용할 수 있습니다. 즉, TCP Syn 스캔을 사용할 수 없는 상황에서는 이 옵션을 사용해야 합니다. • **TCP ACK** 스캔은 ACK 패킷을 전송하여 포트의 필터링 여부를 확인합니다. • **TCP Window** 스캔은 TCP ACK 스캔과 동일한 방식으로 작동하지만, 포트가 열렸는지 또는 닫혔는지도 확인할 수 있습니다. • **TCP Maimon** 스캔은 FIN/ACK 프로브를 사용하여 BSD에서 파생된 시스템을 식별합니다.	**TCP Syn**: `-sS` **TCP Connect**: `-sT` **TCP ACK**: `-sA` **TCP Window**: `-sW` **TCP Maimon**: `-sM`
UDP 포트 스캔	TCP 포트 외에 UDP 포트 스캔도 활성화합니다. UDP 포트 스캐닝은 시간이 많이 걸릴 수 있으므로 빠르게 스캔하려는 경우에는 이 옵션을 사용하지 마십시오.	`-sU`
이벤트의 포트 사용	상관관계 정책에서 교정을 응답으로서 사용하려는 경우, 교정이 상관관계 응답을 트리거하는 이벤트에 지정된 포트만 스캔하도록 설정합니다. • **On(**켜기**)**을 선택하면 Nmap 교정 설정에서 지정한 포트가 아닌 상관관계 이벤트의 포트를 스캔합니다. 상관관계 이벤트의 포트를 스캔하면, 교정은 사용자가 Nmap 교정 설정에서 지정한 IP 주소의 포트를 스캔합니다. 또한 이러한 포트는 교정의 동적 스캔 대상에 추가됩니다. • **Off(**끄기**)**를 선택하면 Nmap 교정 설정에서 지정한 포트만 스캔합니다. 또한 Nmap이 운영체제 정보 및 서버 정보를 수집할지 여부도 제어할 수 있습니다. 새 서버와 관련된 포트를 스캔하려면 **Use Port From Event(**이벤트의 포트 사용**)** 옵션을 활성화하십시오.	해당 없음

옵션	설명	해당 Nmap 옵션
보고 탐지 엔진 스캔	호스트를 보고한 탐지 엔진이 상주하는 어플라이언스에서 호스트를 스캔하도록 설정합니다. • 보고 탐지 엔진을 실행하는 어플라이언스에서 스캔하려면 **On(**켜기**)**을 선택합니다. • 교정에서 구성된 어플라이언스에서 스캔하려면 **Off(***끄기***)**를 선택합니다.	해당 없음
빠른 포트 스캔	스캐닝을 수행하는 디바이스의 `/var/sf/nmap/share/nmap/nmap-services` 디렉터리에 있는 `nmap-services` 파일에 나열된 TCP 포트만 스캔하고 다른 포트 설정은 무시하도록 설정합니다. 이 옵션은 **Port Ranges and Scan Order(**포트 범위 및 스캔 순서**)** 옵션과 함께 사용할 수 없습니다. • 스캐닝을 수행하고 다른 포트 설정은 무시하는 디바이스의 `/var/sf/nmap/share/nmap/nmap-services` 디렉터리에 있는 `nmap-services` 파일에 나열된 포트만 스캔하려면, **On(**켜기**)**을 선택합니다. • 모든 TCP 포트를 스캔하려면 **Off(***끄기***)**를 선택합니다.	`-F`
포트 범위 및 스캔 순서	Nmap 포트 사양 구문을 사용하여 스캔할 특정 포트를 설정하고 스캔 순서를 지정합니다. 이 옵션은 **Fast Port Scan(**빠른 포트 스캔**)** 옵션과 함께 사용할 수 없습니다.	`-p`
벤더 및 버전 정보에 대한 열린 포트 탐색	서버 벤더 및 버전 정보의 탐지를 활성화합니다. 열린 포트에서 서버 벤더 및 버전 정보를 조사하면 Nmap은 서버 식별에 사용하는 서버 데이터를 얻게 됩니다. 그런 다음 해당 서버에 대한 Cisco 서버 데이터를 교체합니다. • 호스트의 열린 포트에서 서버 정보를 스캔하여 서버 벤더 및 버전을 식별하려면 **On(**켜기**)**을 선택합니다. • 호스트에 대한 Cisco 서버 정보를 계속해서 사용하려면 **Off(***끄기***)**를 선택합니다.	`-sV`
서비스 버전 강도	서비스 버전에 대한 Nmap 프로브의 강도를 선택합니다. • 시간이 오래 걸리지만 정확도 높은 스캔을 위해 더 많은 프로브를 사용하려면 더 높은 숫자를 선택합니다. • 정확도는 떨어지지만 시간은 적게 걸리는 스캔을 위해 더 적은 프로브를 사용하려면 더 낮은 숫자를 선택합니다.	`--version-intensity` <intensity>

옵션	설명	해당 Nmap 옵션
운영체제 탐지	호스트에 대한 운영체제 정보의 탐지를 활성화합니다. 호스트에 대한 운영체제의 탐지를 구성하면 Nmap은 호스트를 스캔하고 그 결과를 사용하여 각 운영체제에 대한 점수를 생성합니다. 이 점수는 운영체제가 호스트에서 실행되고 있을 가능성을 반영합니다. • 호스트에서 운영체제를 식별하기 위한 정보를 스캔하려면 **On(**켜기**)**을 선택합니다. • 호스트에 대한 Cisco 운영체제 정보를 계속해서 사용하려면 **Off(***끄기***)**를 선택합니다.	-o
모든 호스트를 온라인으로 취급	호스트 검색 프로세스를 건너뛰고 대상 범위의 모든 호스트에서 포트 스캔을 실행하도록 설정합니다. 이 옵션을 활성화하면 Nmap은 **Host Discovery Method(**호스트 검색 방법**)** 및 **Host Discovery Port List(**호스트 검색 포트 목록**)**에 대한 설정을 무시합니다. • 호스트 검색 프로세스를 건너뛰고 대상 범위의 모든 호스트에서 포트 스캔을 실행하려면 **On(**켜기**)**을 선택합니다. • **Host Discovery Method(**호스트 검색 방법**)** 및 **Host Discovery Port List(**호스트 검색 포트 목록**)**에 대한 설정을 사용하여 호스트 검색을 수행하고 사용할 수 없는 호스트에 대한 포트 스캔은 건너뛰려면 **Off(***끄기***)**를 선택합니다.	-PN

옵션	설명	해당 Nmap 옵션
호스트 검색 방법	대상 범위의 모든 호스트에 대해 **Host Discovery Port List(**호스트 검색 포트 목록**)**에 나열된 포트에서(포트가 나열되지 않은 경우 해당 호스트 검색 방법에 대한 기본 포트에서) 호스트 검색을 수행하려면 선택합니다. 그러나 **Treat All Hosts As Online(**모든 호스트를 온라인으로 취급**)**도 활성화한 경우 **Host Discovery Method(**호스트 검색 방법**)** 옵션은 효과가 없으며 호스트 검색이 수행되지 않습니다. 호스트가 있으며 사용 가능한지를 알아보기 위해 Nmap으로 테스트할 때 사용할 방법을 선택합니다. • **TCP SYN** 옵션은 SYN 플래그가 설정된 빈 TCP 패킷을 전송하고 응답을 받으면 호스트가 사용 가능한 상태인 것으로 인식합니다. TCP SYN은 기본적으로 포트 80을 스캔합니다. 스테이트풀 방화벽 규칙이 있는 방화벽에서는 TCP SYN 스캔을 차단할 가능성이 적습니다. • **TCP ACK** 옵션은 ACK 플래그가 설정된 빈 TCP 패킷을 전송하고 응답을 받으면 호스트가 사용 가능한 상태인 것으로 인식합니다. TCP ACK도 기본적으로 포트 80을 스캔합니다. 스테이트리스 방화벽 규칙이 있는 방화벽에서는 TCP ACK 스캔을 차단할 가능성이 적습니다. • **UDP** 옵션은 UDP 패킷을 전송하고, 닫힌 포트에서 포트 도달 불가 응답이 돌아오면 호스트가 사용 가능한 상태인 것으로 간주합니다. UDP는 기본적으로 포트 40125를 스캔합니다.	**TCP SYN**: `-PS` **TCP ACK**: `-PA` **UDP**: `-PU`
호스트 검색 포트 목록	호스트 검색을 수행할 때 스캔할 포트의 맞춤형 목록을 쉼표로 구분하여 지정합니다.	호스트 검색 방법에 대한 포트 목록
기본 NSE 스크립트	호스트 검색 및 서버/운영체제/취약성 탐지에 대한 Nmap 스크립트의 기본 세트 실행을 활성화합니다. 기본 스크립트 목록은 https://nmap.org/nsedoc/categories/default.html을 참조하십시오. • 기본 Nmap 스크립트 세트를 실행하려면 **On(**켜기**)**을 선택합니다. • 기본 Nmap 스크립트 세트를 건너뛰려면 **Off(**끄기**)**를 선택합니다.	`-sC`
타이밍 템플릿	스캔 프로세스의 타이밍을 선택합니다. 높은 숫자를 선택할수록 스캔의 범위가 줄고 속도가 빨라집니다.	**0**: `T0` (paranoid) **1**: `T1` (sneaky) **2**: `T2` (polite) **3**: `T3` (normal) **4**: `T4` (aggressive) **5**: `T5` (insane)

Nmap 스캔 지침

활성 스캐닝을 통해 귀중한 정보를 얻을 수 있지만 Nmap 등의 툴을 과용하면 네트워크 리소스에 과부하가 발생하거나 중요한 호스트가 충돌할 수도 있습니다. 활성 스캐너를 사용하는 동안에는 이러한 지침에 따라 반드시 필요한 호스트와 포트만 스캔할 수 있도록 스캐닝 전략을 세워야 합니다.

적절한 스캔 대상 선택

Nmap을 구성할 때 스캔할 호스트를 식별하는 스캔 대상을 생성할 수 있습니다. 스캔 대상에는 스캔할 단일 IP 주소, CIDR 블록 또는 IP 주소의 옥텟 범위, IP 주소 범위, IP 주소의 목록이나 범위는 물론 호스트의 포트도 포함됩니다.

다음과 같은 방법으로 대상을 지정할 수 있습니다.

- IPv6 호스트의 경우
  - 정확한 IP 주소(예: `2001:DB8:1:178:ABCD`)
- IPv4 호스트의 경우
  - 정확한 IP 주소(예: `192.168.1.101`) 또는 쉼표나 공백으로 구분한 IP 주소의 목록
  - CIDR 표기법을 사용한 IP 주소 블록(예를 들어 `192.168.1.0/24`는 192.168.1.1과 192.168.1.254(포함) 사이의 254개 호스트를 스캔함)
  - 옥텟 범위 주소 지정을 사용한 IP 주소 범위(예를 들어 `192.168.0-255.1-254`는 .0 또는 .255로 끝나는 주소를 제외한 192.168.x.x 범위의 모든 주소를 스캔함)
  - 하이픈을 사용한 IP 주소 범위(예를 들어 `192.168.1.1 - 192.168.1.5`는 192.168.1.1과 192.168.1.5(포함) 사이의 6개 호스트를 스캔함)
  - 쉼표나 공백으로 구분한 주소 목록 또는 범위(예를 들어 `192.168.1.0/24, 194.168.1.0/24`는 192.168.1.1과 192.168.1.254(포함) 사이의 254개 호스트 및 194.168.1.1과 194.168.1.254(포함) 사이의 254개 호스트를 스캔함)

Nmap 스캔을 위한 이상적인 스캔 대상에는 시스템이 식별할 수 없는 운영체제의 호스트, 식별되지 않은 서버의 호스트 또는 네트워크에서 최근에 탐지되지 않은 호스트가 포함됩니다. 네트워크 맵에 이미 존재하지 않는 호스트에 대한 네트워크 맵에는 Nmap 결과를 추가할 수 없습니다.

⚠

주의

- Nmap 제공 서버 및 운영체제 데이터는 또 다른 Nmap 스캔을 실행할 때까지 고정 상태로 유지됩니다. Nmap을 이용해 호스트를 스캔하기로 했다면, 스캔을 정기적으로 예약하십시오.
- 호스트가 네트워크 맵에서 삭제되면 모든 Nmap 검사 결과가 삭제됩니다.
- 사용자는 대상을 스캔할 권한이 있어야 합니다. 자신 또는 자신의 회사에 속하지 않은 호스트를 스캔하기 위해 Nmap을 사용하는 것은 불법일 수 있습니다.

스캔할 적절한 포트 선택

설정하는 각 스캔 대상에 대해 스캔할 포트를 선택할 수 있습니다. 각 대상에서 스캔해야 할 정확한 포트 집합을 식별하려면 개별 포트 번호, 포트 범위 또는 포트 번호와 포트 범위의 시리즈를 지정할 수 있습니다.

기본적으로 Nmap은 1~1024의 TCP 포트를 스캔합니다. 상관관계 정책에서 교정을 응답으로서 사용하려는 경우, 교정이 상관관계 응답을 트리거하는 이벤트에 지정된 포트만 스캔하게 할 수 있습니다. 온디맨드 방식으로 또는 예약된 작업으로 교정을 실행하는 경우 또는 이벤트에서 포트를 사용하지 않는 경우 다른 포트 옵션을 사용하여 어떤 포트를 스캔할지 결정할 수 있습니다. `nmap-services` 파일에 나열된 TCP 포트만 스캔하고 다른 포트 설정은 무시하도록 선택할 수 있습니다. TCP 포트 외에 UDP 포트도 스캔할 수 있습니다. UDP 포트 스캐닝은 시간이 많이 걸릴 수 있으므로 빠르게 스캔하려는 경우에는 이 옵션을 사용하지 마십시오. 스캔할 특정 포트 또는 포트 범위를 선택하려면 포트를 식별하기 위한 Nmap 포트 사양 구문을 사용하십시오.

호스트 검색 옵션 설정

호스트에 대한 포트 스캔을 시작하기 전에 호스트 검색 수행 여부를 결정할 수 있습니다. 또는 스캔하려는 모든 호스트가 온라인 상태라고 가정할 수 있습니다. 모든 호스트를 온라인 상태로 취급하지 않으려는 경우 원하는 호스트 검색 방법을 선택할 수 있으며, 필요에 따라 호스트 검색 중 스캔할 포트 목록을 맞춤형할 수 있습니다. 호스트 검색은 나열된 포트에서 운영체제 또는 서버 정보를 조사하지 않습니다. 특정 포트에 대한 응답을 사용하여 호스트가 활성 상태이며 사용 가능한지만 확인합니다. 호스트 검색을 수행했는데 호스트가 사용 가능하지 않으면 Nmap은 해당 호스트에서 포트를 스캔하지 않습니다.

예: Nmap을 사용하여 알 수 없는 운영 체제 확인

이 예에서는 알 수 없는 운영체제를 확인하도록 설계된 Nmap 설정을 안내합니다. Nmap 설정 전체 과정은 Nmap 스캔 관리, 29 페이지 섹션을 참조하십시오.

시스템이 네트워크에 있는 호스트의 운영체제를 확인할 수 없다면, Nmap을 사용하여 호스트를 능동적으로 스캔할 수 있습니다. Nmap은 스캔에서 얻은 정보를 사용하여 가능한 운영체제를 평가합니다. 그런 다음 호스트 운영체제 식별의 점수가 가장 높은 운영체제를 사용합니다.

Nmap을 사용하여 새 호스트에서 운영체제와 서버 정보를 확인하면 시스템은 스캔된 호스트에서 해당 정보를 모니터링하지 않습니다. Nmap을 사용하여 호스트를 검색하고 시스템에서 알 수 없는 운영체제가 포함된 것으로 표시한 호스트의 서버 운영체제를 검색하는 경우 유사한 호스트 그룹을 식별할 수 있습니다. 그런 다음 이들 중 하나를 기반으로 맞춤형 핑거프린트를 생성하여, Nmap 스캔을 기반으로 호스트에서 실행 중임을 알고 있는 운영체제의 핑거프린트와 연결할 수 있습니다. 가능하면 Nmap과 같은 서드파티 소스를 통해 고정 데이터를 입력하기보다 맞춤형 핑거프린트를 사용하십시오. 맞춤형 핑거프린트를 사용하면 시스템은 계속해서 호스트 운영체제를 모니터링하고 필요 시 업데이트할 수 있기 때문입니다.

이 예에서는 다음 작업을 수행하게 됩니다.

1. Nmap 스캔 인스턴스 추가, 30 페이지에 설명된 대로 스캔 인스턴스를 설정합니다.
2. 다음 설정을 사용하여 Nmap 교정을 생성합니다.
   - **Use Port From Event(**이벤트의 포트 사용**)**를 활성화해 새 서버와 관련된 포트를 스캔합니다.

- **Detect Operating System(**운영체제 탐지**)**를 활성화해 호스트에 대한 운영체제 정보를 탐지합니다.
- **Probe open ports for vendor and version information(**벤더 및 버전 정보에 대한 열린 포트 탐색**)**을 활성화해 서버 벤더 및 버전 정보를 탐지합니다.
- 호스트가 존재하는 것을 아는 경우 **Treat All Hosts as Online(**모든 호스트를 온라인으로 취급**)**을 활성화합니다.

3. 시스템이 알려지지 않은 운영체제의 호스트를 탐지할 때 트리거되는 상관관계 규칙을 생성합니다. 이 규칙은 검색 이벤트가 발생할 때,호스트의 **OS** 정보가 변경될 때, 그리고 **OS** 이름을 알 수 없음 조건을 충족할 때 트리거됩니다.
4. 상관관계 규칙이 포함된 상관관계 정책을 생성합니다.
5. 상관관계 정책에서, 2단계에서 생성한 Nmap 교정을 3단계에서 생성한 규칙에 추가합니다.
6. 상관관계 정책을 활성화합니다.
7. 네트워크 검색이 다시 시작되고 네트워크 맵이 재작성되도록 네트워크 맵의 호스트를 삭제합니다.
8. 하루나 이틀 후, 상관관계 정책에 의해 생성된 이벤트를 검색합니다. 호스트에서 탐지된 운영체제에 대한 Nmap 결과를 분석하여 네트워크에 시스템이 인식하지 못한 특별한 호스트 설정에 있는지 알아봅니다.
9. Nmap 결과가 동일한 알 수 없는 운영체제의 호스트를 찾으면 그러한 호스트 중 하나에 대해 맞춤형 핑거프린트를 생성하고 향후 유사한 호스트를 식별하는 데 사용합니다.

관련 항목

Nmap 교정 생성, 34 페이지
Nmap 스캔 결과, 38 페이지
클라이언트에 대한 맞춤형 핑거프린트 생성, 7 페이지

예: Nmap을 사용하여 새 호스트에 응답

이 예에서는 새 호스트에 응답하도록 설계된 Nmap 설정을 안내합니다. Nmap 설정 전체 과정은 Nmap 스캔 관리, 29 페이지의 내용을 참조하십시오.

침입 가능성이 있는 서브넷에서 시스템이 새 호스트를 탐지하면, 이에 대한 정확한 취약성 정보가 있는지 확인하기 위해 해당 호스트를 스캔할 수 있습니다.

그렇게 하려면 이 서브넷에 새 호스트가 나타날 때 이를 탐지하고 호스트에서 Nmap 스캔을 수행하는 교정을 실행하는 상관관계 정책을 생성 및 활성화하면 됩니다.

이렇게 하려면 다음 작업을 수행해야 합니다.

1. Nmap 스캔 인스턴스 추가, 30 페이지에 설명된 대로 스캔 인스턴스를 설정합니다.
2. 다음 설정을 사용하여 Nmap 교정을 생성합니다.
   - **Use Port From Event(**이벤트의 포트 사용**)**를 활성화해 새 서버와 관련된 포트를 스캔합니다.

- **Detect Operating System(**운영체제 탐지**)**를 활성화해 호스트에 대한 운영체제 정보를 탐지합니다.
- **Probe open ports for vendor and version information(**벤더 및 버전 정보에 대한 열린 포트 탐색**)**을 활성화해 서버 벤더 및 버전 정보를 탐지합니다.
- 호스트가 존재하는 것을 아는 경우 **Treat All Hosts as Online(**모든 호스트를 온라인으로 취급**)**을 활성화합니다.

3. 시스템이 특정 서브넷에서 새 호스트를 탐지할 때 트리거되는 상관관계 규칙을 생성합니다. 규칙은 검색 이벤트가 발생할 때 및 새 호스트가 탐지될 때 트리거되어야 합니다.
4. 상관관계 규칙이 포함된 상관관계 정책을 생성합니다.
5. 상관관계 정책에서, 2단계에서 생성한 Nmap 교정을 3단계에서 생성한 규칙에 추가합니다.
6. 상관관계 정책을 활성화합니다.
7. 새 호스트에 대한 알림이 제공되면 해당 호스트 프로파일에서 Nmap 스캔의 결과를 확인하고 호스트에 적용되는 취약성을 해결합니다.

정책을 활성화하면, 교정 상태 보기(**Analysis(**분석**)** > **Correlation(**상관관계**)** > **Status(**상태**)**)를 주기적으로 확인해 교정 시작 시기를 확인할 수 있습니다. 교정의 동적 스캔 대상은 서버 탐지의 결과로서 스캔한 호스트의 IP 주소를 포함해야 합니다. Nmap에서 탐지한 운영체제와 서버를 기반으로, 그러한 호스트의 호스트 프로파일을 검토하여 호스트에 대해 해결해야 할 취약성이 있는지 알아보십시오.

주의 대규모 동적 네트워크가 있는 경우 새 호스트 탐지가 너무 빈번하여 스캔 사용에 응답하지 못할 수 있습니다. 리소스 과부하를 피하려면 자주 발생하는 이벤트에 대한 응답으로 Nmap 스캔을 사용하지 마십시오. 또한 Nmap을 사용하여 새 호스트에서 운영체제와 서버 정보를 확인하면 Cisco는 스캔된 호스트에서 해당 정보를 모니터링하지 않습니다.

관련 항목

Nmap 교정 생성, 34 페이지

Nmap 스캔 관리

Nmap 스캔을 사용하려면 최소한 Nmap 스캔 인터페이스와 Nmap 교정은 설정해야 합니다. Nmap 스캔 대상 설정은 선택사항입니다.

프로시저

단계 **1** Nmap 스캔 설정:

- Nmap 스캔 인스턴스 추가, 30 페이지에 설명된 대로 Nmap 스캔 인스턴스를 추가합니다.
- Nmap 교정 생성, 34 페이지에 설명된 대로 Nmap 교정을 생성합니다.
- 선택적으로, Nmap 스캔 대상 추가, 32 페이지에 설명된 대로 Nmap 스캔 대상을 추가합니다.

단계 2 Nmap 스캔 실행:

- 온디맨드 Nmap 스캔 실행, 37 페이지에 설명된 대로 온디맨드 Nmap 스캔을 실행합니다.
- Cisco Secure Firewall Management Center 관리 가이드의 *Nmap* 스캔 자동화에 설명된 대로 자동 Nmap 스캔을 구성합니다.
- Cisco Secure Firewall Management Center 관리 가이드의 *Nmap* 스캔 예약 에 설명된 대로 자동 Nmap 스캔을 예약합니다.

다음에 수행할 작업

- 관련 작업을 확인해 진행 중인 Nmap 스캔을 모니터링합니다. Cisco Secure Firewall Management Center 관리 가이드의 작업 메시지 보기를 참조하십시오 .
- 선택적으로, 스캔을 개선합니다.
  - Nmap 스캔 인스턴스 편집, 31 페이지에 설명된 대로 Nmap 스캔 인스턴스를 편집합니다.
  - Nmap 스캔 대상 편집, 33 페이지에 설명된 대로 Nmap 스캔 대상을 편집합니다.
  - Nmap 교정 편집, 36 페이지에 설명된 대로 Nmap 교정을 편집합니다.

Nmap 스캔 인스턴스 추가

네트워크에서 취약성을 스캔하기 위해 사용할 각 Nmap 모듈에 대해 별도의 스캔 인스턴스를 설정할 수 있습니다. Secure Firewall Management Center의 로컬 Nmap 모듈 및 원격으로 스캔을 실행하기 위해 사용할 디바이스에 대해 스캔 인스턴스를 설정할 수 있습니다. 원격 디바이스에서 스캔을 실행하는 경우에도, 각 스캔의 결과는 스캔을 구성하는 management center에 항상 저장됩니다. 미션 크리티컬 호스트에 대한 악의적인 스캔 또는 실수로 이루어지는 스캔을 방지하려면, 인스턴스로 스캔해서는 안 되는 호스트를 나타내기 위해 인스턴스에 대한 블랙리스트를 생성할 수 있습니다.

기존 스캔 인스턴스와 동일한 이름의 스캔 인스턴스를 추가할 수는 없습니다.

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 스캔 인스턴스를 표시하며 이러한 인스턴스는 편집할 수 있습니다. 상위 도메인에서 생성된 스캔 인스턴스도 표시되지만, 이러한 인스턴스는 편집할 수 없습니다. 하위 도메인에서 생성된 스캔 인스턴스를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 1 다음 방법 중 하나를 사용하여 Nmap 스캔 인스턴스 목록에 액세스합니다.

- **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.
- **Policies(**정책**)** > **Actions(**작업**)** > **Scanners(**스캐너**)**을(를) 선택합니다.

단계 2 교정 추가:

- 첫 번째 방법으로 목록에 액세스했다면, Add a New Instance(새 인스턴스 추가) 섹션을 찾은 다음 드롭다운 목록에서 Nmap Remediation 모듈을 선택하고 **Add(**추가**)**를 클릭합니다.
- 두 번째 방법으로 목록에 액세스했다면 **Add Nmap Instance(Nmap** 인스턴수 추가**)**를 클릭합니다.

단계 **3** **Instance Name(**인스턴스 이름**)**을 클릭합니다.

단계 **4** **Description(**설명**)**을 입력합니다.

단계 **5** 선택적으로, 다음 명령문을 사용하여 이 검색 인스턴스로 스캔해서는 안 되는 호스트 또는 네트워크를 **Exempted hosts(**제외 호스트**)** 필드에 지정합니다.

- IPv6 호스트의 경우 정확한 IP 주소(예: `2001:DB8::fedd:eeff`)
- IPv4 호스트의 경우 정확한 IP 주소(예: `192.168.1.101`) 또는 CIDR 표기법을 사용하는 IP 주소 블록(예: `192.168.1.0/24`는 `192.168.1.1`과 `192.168.1.254` 사이(포함)의 254개 호스트를 스캔함)
- 주소 값을 부정하기 위해 느낌표(!)를 사용할 수는 없습니다.

참고 스캔 대상을 블랙리스트에 추가된 네트워크에 있는 호스트로 구체적으로 지정하는 경우 해당 스캔은 실행되지 않습니다.

단계 **6** 선택적으로, management center 대신 원격 디바이스에서 스캔을 실행하려면 management center 웹 인터페이스에서 디바이스의 Information(정보) 페이지 **Remote Device Name(**원격 디바이스 이름**)** 필드에 나타나는 디바이스의 IP 주소 또는 이름을 지정합니다.

단계 **7** **Create(**생성**)**를 클릭합니다.
시스템이 인스턴스 생성을 완료하면, 편집 모드에 인스턴스가 표시됩니다.

단계 **8** 선택적으로, Nmap 교정을 인스턴스에 추가합니다. 이렇게 하려면 인스턴스의 Configured Remediations(설정된 교정) 섹션을 찾은 다음 **Add(**추가**)**를 클릭하고 Nmap 교정 생성, 34 페이지에 설명된 대로 교정을 생성해야 합니다.

단계 **9** **Cancel(**취소**)**을 클릭하여 인스턴스 목록으로 돌아갑니다.

참고 **Scanners(**스캐너**)** 옵션을 통해 Nmap 스캔 인터페이스 목록에 액세스했다면, 추가한 인스턴스에 교정을 추가해야 해당 인스터스가 시스템에서 표시됩니다. 교정을 추가하지 않은 인스턴스를 확인하려면 **Instances(**인스턴스**)** 메뉴 옵션을 이용해 목록에 액세스하십시오.

Nmap 스캔 인스턴스 편집

스캔 인스턴스를 편집할 때 인스턴스와 관련된 교정을 확인, 추가, 삭제할 수 있습니다. 인스턴스에 프로파일된 Nmap 모듈을 더 이상 사용하지 않으려는 경우 Nmap 스캔 인스턴스를 삭제할 수 있습니다. 스캔 인스턴스를 삭제할 때 해당 인스턴스를 사용하는 교정도 삭제할 수 있습니다.

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 스캔 인스턴스를 표시하며 이러한 인스턴스는 편집할 수 있습니다. 상위 도메인에서 생성된 스캔 인스턴스도 표시되지만, 이러한 인스턴스는 편집할 수 없습니다. 하위 도메인에서 생성된 스캔 인스턴스를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 1 다음 방법 중 하나를 사용하여 Nmap 스캔 인스턴스 목록에 액세스합니다.

- **Policies(정책) > Actions(작업) > Instances(인스턴스)**을(를) 선택합니다.
- **Policies(정책) > Actions(작업) > Scanners(스캐너)**을(를) 선택합니다.

단계 2 편집할 인스턴스 옆에 있는 **View(보기)** ( )을 클릭합니다.

단계 3 Nmap 스캔 인스턴스 추가, 30 페이지에 설명된 대로 스캔 인스턴스 설정을 변경합니다.

단계 4 **Save(저장)**를 클릭합니다.

단계 5 **Done(완료)**을 클릭합니다.

다음에 수행할 작업

- 선택적으로, 스캔 인스턴스에 새 교정을 추가할 수 있습니다(다음 참조). Nmap 교정 생성, 34 페이지
- 선택적으로, 인스턴스에 연결된 교정을 편집할 수 있습니다(Nmap 교정 편집, 36 페이지 참조).
- 선택적으로, 인스턴스에 연결된 교정을 삭제할 수 있습니다(온디맨드 Nmap 스캔 실행, 37 페이지 참조).
- 선택적으로, 스캔 인스턴스 옆에 있는 **Delete(삭제)** ( )을 클릭하여 인스턴스를 삭제할 수 있습니다.

Nmap 스캔 대상 추가

Nmap 모듈을 구성할 때 온디맨드 또는 예약된 스캔을 수행할 호스트와 포트를 식별하는 스캔 대상을 생성 및 저장할 수 있습니다. 그러면 매번 새로운 스캔 대상을 작성할 필요가 없습니다. 스캔 대상에는 스캔할 단일 IP 주소 또는 IP 주소 블록은 물론 호스트의 포트도 포함됩니다. Nmap 대상에 대해 Nmap 옥텟 범위 주소 지정 또는 IP 주소 범위를 사용할 수도 있습니다. Nmap 옥텟 범위 주소 지정에 대한 자세한 내용은 http://insecure.org에서 제공하는 Nmap 설명서를 참조하십시오.

참고:

- 다수의 호스트가 포함된 스캔 대상을 스캔하는 데에는 많은 시간이 소요될 수 있습니다. 해결책은 한 번에 더 적은 수의 호스트를 스캔하는 것입니다.
- Nmap 제공 서버 및 운영체제 데이터는 또 다른 Nmap 스캔을 실행할 때까지 고정 상태로 유지됩니다. Nmap을 이용해 호스트를 스캔하기로 했다면, 스캔을 정기적으로 예약하십시오. 호스트가 네트워크 맵에서 삭제되면 모든 Nmap 검사 결과가 삭제됩니다.
- 다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 스캔 대상을 표시하며 이러한 규칙은 편집할 수 있습니다. 상위 도메인에서 생성된 스캔 대상도 표시되지만, 이러한 대상은 편집할 수는 없습니다. 하위 도메인의 스캔 대상을 보고 편집하려면 해당 도메인으로 전환하십시오.

프로시저

단계 1 **Policies(**정책**)** > **Actions(**작업**)** > **Scanners(**스캐너**)**을(를) 선택합니다.

단계 2 툴바에서 **Targets(**대상**)**를 클릭합니다.

단계 3 **Create Scan Target(**스캔 대상 생성**)**을 클릭합니다.

단계 4 이 스캔 대상에 사용할 이름을 **Name(**이름**)** 필드에 입력합니다.

단계 5 **IP Range(IP** 범위**)** 문자함에는 Nmap 스캔 지침, 26 페이지에서 설명하는 구문을 사용하여 스캔할 호스트를 지정합니다.

참고 스캔 대상에서 IP 주소나 범위의 목록에 쉼표를 사용하는 경우, 대상을 저장할 때 쉼표는 공백으로 변환됩니다.

단계 6 스캔할 포트를 **Ports(**포트**)** 필드에 지정합니다.

1~65535의 값을 사용하여 다음 중 하나를 입력할 수 있습니다.

- 포트 번호
- 쉼표로 구분된 포트 목록
- 대시로 구분된 포트 번호의 범위
- 대시로 구분된, 쉼표로 구분된 포트 번호의 범위

단계 7 **Save(**저장**)**를 클릭합니다.

Nmap 스캔 대상 편집

팁 특정 IP 주소를 스캔하기 위해 교정을 사용하고자 하지만 호스트가 교정을 실행한 상관관계 정책 위반과 관련되어 있기 때문에 IP 주소가 대상에 추가된 경우, 교정의 동적 스캔 대상을 편집할 수 있습니다.

나열된 호스트를 더 이상 스캔하지 않으려면 스캔 대상을 삭제하십시오.

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 스캔 대상을 표시하며 이러한 규칙은 편집할 수 있습니다. 상위 도메인에서 생성된 스캔 대상도 표시되지만, 이러한 대상은 편집할 수는 없습니다. 하위 도메인의 스캔 대상을 보고 편집하려면 해당 도메인으로 전환하십시오.

프로시저

단계 1 **Policies(**정책**)** > **Actions(**작업**)** > **Scanners(**스캐너**)**을(를) 선택합니다.

단계 2 툴바에서 **Targets(**대상**)**를 클릭합니다.

단계 3 편집하려는 스캔 대상 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

View(보기**)** ()이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** 필요한 대로 수정합니다. 자세한 내용은 Nmap 스캔 대상 추가, 32 페이지를 참고하십시오.

단계 **5** **Save(**저장**)**를 클릭합니다.

단계 **6** 선택적으로 스캔 대상 옆에 있는 **Delete(**삭제**)** ()을 클릭하여 대상을 삭제할 수 있습니다.

Nmap 교정 생성

Nmap 교정은 기존 Nmap 스캔 인스턴스에 추가하는 방법으로만 생성할 수 있습니다. 교정은 스캔에 대한 설정을 정의합니다. Nmap 교정은 상관관계 정책에서 응답으로 사용하거나, 온디맨드 방식으로 실행하거나, 특정 시간에 예약한 작업으로 실행할 수 있습니다.

Nmap 제공 서버 및 운영체제 데이터는 또 다른 Nmap 스캔을 실행할 때까지 고정 상태로 유지됩니다. Nmap을 이용해 호스트를 스캔하기로 했다면, 스캔을 정기적으로 예약하십시오. 호스트가 네트워크 맵에서 삭제되면 모든 Nmap 검사 결과가 삭제됩니다.

Nmap 기능에 대한 자세한 내용은 http://insecure.org에서 제공하는 Nmap 설명서를 참조하십시오.

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 Nmap 교정을 표시하며, 이러한 교정은 편집할 수 있습니다. 상위 도메인에서 생성된 Nmap 교정도 표시되지만, 이러한 교정은 수정할 수 없습니다. 하위 도메인의 Nmap 교정을 보고 편집하려면 해당 도메인으로 전환하십시오.

시작하기 전에

- Nmap 스캔 인스턴스 추가, 30 페이지의 설명에 따라 Nmap 스캔 인스턴스를 추가합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.

단계 **2** 교정을 추가할 인스턴스 옆에 있는 **View(**보기**)** ()을 클릭합니다.

단계 **3** Configured Remediations(설정된 교정) 섹션에서 **Add(**추가**)**를 클릭합니다.

단계 **4** **Remediation Name(**교정 이름**)**을 입력합니다.

단계 **5** **Description(**설명**)**을 입력합니다.

단계 **6** 침입 이벤트, 연결 이벤트 또는 사용자 이벤트를 트리거하는 상관관계 규칙에 대한 응답으로 이 교정을 사용하려는 경우 **Scan Which Address(es) From Event(**이벤트에서 어떤 주소를 스캔하시겠습니까**)?** 옵션을 설정합니다.

팁 검색 이벤트 또는 호스트 입력 이벤트에서 트리거되는 상관관계 규칙에 대한 응답으로 이 교정을 사용하려는 경우, 기본적으로 교정은 이벤트와 관련된 호스트의 IP 주소를 스캔합니다. 이 옵션은 설정할 필요가 없습니다.

참고 트래픽 프로파일 변경을 트리거하는 상관관계 규칙에는 Nmap 교정을 응답으로서 할당하지 마십시오.

단계 **7** **Scan Type(**스캔 유형**)** 옵션을 설정합니다.

단계 **8** 선택적으로, TCP 포트 외에 UDP 포트도 스캔하려면 **Scan for UDP ports(UDP** 포트 스캔**)** 옵션에 대해 **On(**켜기**)**을 선택합니다.

팁 UDP 포트스캔은 TCP 포트스캔보다 시간이 더 걸립니다. 스캔 속도를 높이려면 이 옵션을 비활성화하십시오.

단계 **9** 상관관계 정책 위반에 대한 응답으로 이 교정을 사용하려는 경우 **Use Port From Event(**이벤트의 포트 사용**)** 옵션을 설정합니다.

단계 **10** 상관관계 정책 위반에 대한 응답으로 이 교정을 사용하고 이벤트를 탐지한 탐지 엔진을 실행하는 어플라이언스를 사용하여 스캔을 실행하려는 경우 **Scan from reporting detection engine(**보고 탐지 엔진에서 스캔**)** 옵션을 설정합니다.

단계 **11** **Fast Port Scan(**빠른 포트 스캔**)** 옵션을 설정합니다.

단계 **12** Nmap 포트 사양 구문을 사용하여 기본적으로 스캔할 포트를 원하는 스캔 순서대로 **Port Ranges and Scan Order(**포트 범위 및 스캔 순서**)** 필드에 입력합니다.

다음 형식을 사용합니다.

- 1~65535의 값을 지정합니다.
- 쉼표나 공백을 사용하여 포트를 구분합니다.
- 포트 범위를 표시하려면 하이픈을 사용합니다.
- TCP 및 UDP 포트를 모두 스캔하는 경우, 스캔할 TCP 포트의 목록 앞에는 T를 추가하고 UDP 포트의 목록 앞에는 U를 추가합니다.

참고 8단계에 설명된 대로, 상관관계 정책 위반에 대한 응답으로 교정이 실행되는 경우 **Use Port From Event(**이벤트의 포트 사용**)** 옵션은 이 설정을 재정의합니다.

예제**:**

UDP 트래픽에 대해 포트 53 및 111을 스캔하고 TCP 트래픽에 대해 포트 21~25를 스캔하려면 `U:53,111,T:21-25`를 입력합니다.

단계 **13** 열린 포트에서 서버 벤더 및 버전 정보를 탐색하려면 **Probe open ports for vendor and version information(**벤더 및 버전 정보에 대한 열린 포트 탐색**)**을 설정합니다.

단계 **14** 열린 포트를 탐색하려는 경우 **Service Version Intensity(**서비스 버전 강도**)** 드롭다운 목록에서 숫자를 선택하여 사용되는 프로브의 수를 설정합니다.

단계 **15** 운영체제 정보를 스캔하려면 **Detect Operating System(**운영체제 탐지**)**설정을 구성합니다.

단계 **16** 호스트 검색 발생 여부 및 포트 스캔을 사용 가능한 호스트에 대해서만 실행할지 여부를 결정하려면 **Treat All Hosts As Online(**모든 호스트를 온라인으로 취급**)**을 구성합니다.

단계 **17** Nmap이 호스트 가용성을 테스트할 때 사용할 방법을 설정하려면, **Host Discovery Method(**호스트 검색 방법**)** 드롭다운 목록에서 방법을 선택합니다.

단계 **18** 호스트 검색 중 맞춤형 포트 목록을 스캔하려면 선택한 호스트 검색 방법에 적절한 포트 목록을 쉼표로 구분하여 **Host Discovery Port List(**호스트 검색 포트 목록**)** 필드에 입력합니다.

단계 **19** 호스트 검색 및 서버, 운영체제, 취약성 검색에 대해 기본 Nmap 스크립트 세트를 사용할지 여부를 제어하려면 **Default NSE Scripts(**기본 **NSE** 스크립트**)** 옵션을 구성합니다.

팁 기본 스크립트 목록은 http://nmap.org/nsedoc/categories/default.html을 참조하십시오.

단계 **20** 스캔 프로세스의 시간을 설정하려면 **Timing Template(**타이밍 템플릿**)** 드롭다운 목록에서 타이밍 템플릿 숫자를 선택합니다.

빠르지만 범위가 좁은 스캔을 원한다면 높은 숫자를, 느리지만 범위가 넓은 스캔을 원한다면 낮은 숫자를 선택합니다.

단계 **21** **Create(**생성**)**를 클릭합니다.
시스템이 교정 생성을 완료하면, 편집 모드에 교정이 표시됩니다.

단계 **22** **Done(**완료**)**을 클릭하여 관련된 인스턴스로 돌아갑니다.

단계 **23** **Cancel(**취소**)**을 클릭하여 인스턴스 목록으로 돌아갑니다.

관련 항목

Nmap 교정 옵션, 21 페이지

Nmap 교정 편집

Nmap 교정에 대한 수정은 진행 중인 스캔에 영향을 미치지 않습니다. 새 설정은 다음 스캔이 시작될 때 적용됩니다. 더 이상 필요하지 않은 Nmap 교정은 삭제할 수 있습니다.

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 Nmap 교정을 표시하며, 이러한 교정은 편집할 수 있습니다. 상위 도메인에서 생성된 Nmap 교정도 표시되지만, 이러한 교정은 수정할 수 없습니다. 하위 도메인의 Nmap 교정을 보고 편집하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** 다음 방법 중 하나를 사용하여 Nmap 스캔 인스턴스 목록에 액세스합니다.

- **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.
- **Policies(**정책**)** > **Actions(**작업**)** > **Scanners(**스캐너**)**을(를) 선택합니다.

단계 **2** 편집하려는 교정에 액세스합니다.

- 첫 번째 방법으로 목록에 액세스했다면, 관련 인스턴스 옆에 있는 아이콘**(View(**보기**)** ( ))을 클릭한 다음 Configured Remediations(설정한 교정) 섹션에서 편집할 교정 옆에 있는 해당 아이콘을 다시 클릭합니다.
- 두 번째 방법으로 목록에 액세스했다면, 편집할 교정 옆에 있는 아이콘**(View(**보기**)** ( ))을 클릭합니다.

단계 **3** Nmap 교정 생성, 34 페이지에 설명된 대로 필요한 대로 수정합니다.

단계 **4** 변경사항을 저장하려면 **Save(**저장**)**를 클릭하고, 저장하지 않고 나가려면 **Done(**완료**)**을 클릭합니다.

단계 **5** 아니면 그 옆에 있는 아이콘**(Delete(**삭제**)** ( ))을 클릭하여 교정을 삭제할 수 있습니다.

온디맨드 Nmap 스캔 실행

필요할 때마다 온디맨드 Nmap 스캔을 실행할 수 있습니다. 스캔할 IP 주소와 포트를 입력하거나 기존 스캔 대상을 선택하여 온디맨드 스캔을 위한 대상을 지정할 수 있습니다.

Nmap 제공 서버 및 운영체제 데이터는 또 다른 Nmap 스캔을 실행할 때까지 고정 상태로 유지됩니다. Nmap을 이용해 호스트를 스캔하기로 했다면, 스캔을 정기적으로 예약하십시오. 호스트가 네트워크 맵에서 삭제되면 모든 Nmap 검사 결과가 삭제됩니다.

시작하기 전에

- 선택적으로, Nmap 스캔 대상을 추가합니다(Nmap 스캔 대상 추가, 32 페이지 참조).

프로시저

단계 **1** **Policies(정책)** > **Actions(작업)** > **Scanners(스캐너)**을(를) 선택합니다.

단계 **2** 스캔 수행에 사용할 Nmap 교정 옆에 있는 **Scan(스캔)**( )을 클릭합니다.

단계 **3** 선택적으로, 저장된 스캔 대상을 사용하여 스캔하려면 **Saved Targets(저장한 대상)** 드롭다운 목록에서 대상을 선택하고 **Load(로드)**를 클릭합니다.

단계 **4** **IP Range(s)(IP 범위)** 필드에서 스캔할 호스트의 IP 주소를 지정하거나 로드된 목록을 수정합니다.

참고:

- IPv4 주소의 호스트에 대해서는 여러 IP 주소를 쉼표로 구분하여 지정하거나 CIDR 표기법을 사용할 수 있습니다. 또한 앞에 느낌표(!)를 사용하여 IP 주소를 부정할 수 있습니다.
- IPv6 주소의 호스트에 대해서는 정확한 IP 주소를 사용해야 합니다. 범위는 지원되지 않습니다.

단계 **5** **Ports(포트)** 필드에서 스캔할 포트를 지정하거나 로드된 목록을 수정합니다.

포트 번호, 쉼표로 구분된 포트 목록 또는 대시로 구분된 포트 번호 범위를 입력할 수 있습니다.

단계 **6** 다중 도메인 구축의 경우에는 **Domain(도메인)** 필드를 사용하여 스캔을 수행할 리프 도메인을 지정합니다.

단계 **7** **Scan Now(지금 스캔)**를 클릭합니다.

다음에 수행할 작업

- 필요한 경우 작업 상태를 모니터링합니다. Cisco Secure Firewall Management Center 관리 가이드의 작업 메시지 보기를 참조하십시오.

Nmap 스캔 결과

진행 중인 Nmap 스캔을 모니터링하고, Firepower System을 통해 이전에 수행한 스캔의 결과나 Firepower System 외부에서 수행한 결과를 가져오고, 스캔 결과를 확인 및 분석할 수 있습니다.

로컬 Nmap 모듈을 사용하여 생성한 스캔 결과를 팝업 윈도우에서 렌더링된 페이지로서 볼 수 있습니다. Nmap 결과 파일을 원시 XML 형식으로 다운로드할 수도 있습니다.

또한 호스트 프로파일 및 네트워크 맵에서 Nmap으로 탐지한 운영체제 및 서버 정보를 볼 수 있습니다. 호스트의 스캔이 필터링된 포트 또는 닫힌 포트에서 서버에 대한 서버 정보를 생성하는 경우, 또는 스캔에서 운영체제 정보나 서버 섹션에 포함할 수 없는 정보를 수집하는 경우 호스트 프로파일의 Nmap Scan Results(Nmap 스캔 결과) 섹션에 그러한 결과가 포함됩니다.

Nmap 스캔 결과 보기

Nmap 스캔이 완료되면 스캔 결과 테이블을 볼 수 있습니다.

찾고 있는 정보에 따라 결과 보기를 조작할 수 있습니다. 스캔 결과에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 스캔 결과 테이블 보기를 포함하는 사전 정의 워크플로를 사용할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 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.

Nmap 버전 1.01 DTD(http://insecure.org에서 다운로드 가능)를 사용하여 Nmap 결과를 다운로드하고 볼 수 있습니다.

스캔 결과를 지울 수도 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Scanners(**스캐너**)**을(를) 선택합니다.

단계 **2** 툴바에서 **Scan Results(**스캔 결과**)**를 클릭합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- Cisco Secure Firewall Management Center 관리 가이드의이벤트 시간 제약 조건에 설명된 대로 시간 범위를 조정합니다.
- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 워크플로 제목 옆의 **(switch workflows)**를 클릭합니다.
- 스캔 결과를 팝업 창에서 렌더링된 페이지로서 보려면 스캔 작업 옆에 있는 **View(**보기**)**를 클릭합니다.
- 텍스트 편집기에서 원시 XML 코드를 볼 수 있도록 스캔 결과 파일의 복사본을 저장하려면 스캔 작업 옆에 있는 **Download(**다운로드**)**를 클릭합니다.
- 검사 결과를 정렬하려면 열 제목을 클릭합니다. 정렬 순서를 반대로 하려면 열 제목을 다시 클릭합니다.

- 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.

- 워크플로우에서 다음 페이지로 드릴다운하려면 Cisco Secure Firewall Management Center 관리 가이드의 드릴다운 페이지 사용을 참조하십시오.
- 스캔 인스턴스와 교정을 설정하려면 툴바에서 **Scanners(**스캐너**)**를 클릭하고 Nmap 스캔 관리, 29 페이지 섹션을 참조하십시오.
- 워크플로 페이지 내부와 페이지 사이를 이동하는 방법은 Cisco Secure Firewall Management Center 관리 가이드의 워크플로우 페이지 탐색 툴을 참조하십시오.
- 다른 이벤트 보기로 이동하여 연결된 이벤트를 보려면 **Jump to(**이동**)** 드롭다운 목록에서 확인할 이벤트 보기의 이름을 선택합니다.
- 스캔 결과를 검색하려면 해당 필드에 검색 기준을 입력합니다.

관련 항목

Nmap 스캔 결과 필드, 39 페이지

Nmap 스캔 결과 필드

Nmap 스캔을 실행할 때 management center은(는) 데이터베이스에서 스캔 결과를 수집합니다. 다음 표는 스캔 결과 테이블에서 확인하고 검색할 수 있는 필드를 설명합니다.

표 *2:* 검색 결과 필드

필드	설명
시작 시간	결과를 생성한 스캔이 시작된 날짜와 시간
종료 시간	결과를 생성한 스캔이 종료된 날짜와 시간
대상	결과를 생성한 스캔에 대한 스캔 대상의 IP 주소(DNS 확인이 활성화된 경우에는 호스트 이름)
스캔 유형	결과를 생성한 스캔의 유형을 나타내기 위한 서드파티 스캐너의 이름 또는 `Nmap`
스캔 모드	결과를 생성한 스캔의 모드 • `On Demand` - 온디맨드 방식으로 실행된 스캔의 결과 • `Imported` - 다른 시스템에서 실행하고 management center(으)로 가져온 스캔의 결과. • `Scheduled` - 예약 작업으로서 실행한 스캔의 결과

필드	설명
결과	스캔의 결과입니다.
도메인	스캔 대상의 도메인입니다. 이 필드는 다중 도메인 구축에서만 표시됩니다.

Nmap 스캔 결과 가져오기

Firepower System 외부에서 수행된 Nmap 스캔에 의해 생성된 XML 결과 파일을 가져올 수 있습니다. Firepower System.에서 전에 다운로드한 XML 결과 파일을 가져올 수도 있습니다. Nmap 스캔 결과를 가져오려면 결과 파일은 XML 형식이어야 하며 Nmap 버전 1.01 DTD를 준수해야 합니다. Nmap 결과 생성 및 Nmap DTD에 대한 자세한 내용은 http://insecure.org에서 제공하는 Nmap 설명서를 참조하십시오.

호스트가 네트워크 맵에 있어야만 Nmap이 결과를 호스트 프로파일에 추가할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Scanners(**스캐너**)**을(를) 선택합니다.

단계 **2** 툴바에서 **Import Results(**결과 가져오기**)**를 클릭합니다.

단계 **3** 다중 도메인 구축의 경우에는 **Domain(**도메인**)** 드롭다운 목록에서 리프 도메인을 선택해 가져온 결과를 저장할 곳을 지정합니다.

단계 **4** 결과 파일을 찾아보려면 **Browse(**찾기**)**를 클릭합니다.

단계 **5** Import Results(가져오기 결과) 페이지로 돌아온 후 **Import(**가져오기**)**를 클릭하여 결과를 가져옵니다.

호스트 ID 소스 기록

기능	버전	세부 사항
호스트 입력 데이터 기능에 대한 보안 개선	6.5	이제 FMC와 호스트 입력 클라이언트 간의 통신에 TLS 1.2를 사용합니다. 이 정보를 이용해 항목 호스트 입력 클라이언트 설정, 19 페이지을(를) 업데이트했습니다.