네트워크 검색 정책

다음 주제에서는 네트워크 검색 정책을 생성, 설정, 관리하는 방법을 설명합니다.

개요: 네트워크 검색 정책

management center의 네트워크 검색 정책에서는 시스템이 조직의 네트워크 자산에서 데이터를 수집하는 방법과 모니터링해야 할 네트워크 세그먼트 및 포트를 제어합니다.

다중 도메인 구축의 경우, 각 리프 도메인에는 독립적인 네트워크 검색 정책이 있습니다. 네트워크 검색 정책 규칙 및 기타 설정은 도메인 간에 공유, 계승, 복사할 수 없습니다. 새 도메인을 생성할 때마다, 시스템은 기본 설정을 이용해 새 도메인의 네트워크 검색 정책을 생성합니다. 원하는 모든 사용자 설정을 새 정책에 명시적으로 적용해야 합니다.

정책 내의 검색 규칙은 트래픽의 네트워크 데이터를 바탕으로 검색 데이터를 생성하기 위해 시스템이 모니터링할 네트워크와 포트를, 그리고 정책을 구축할 영역을 지정합니다. 규칙 내에서는 호스트, 애플리케이션 및 신뢰할 수 없는 사용자의 검색 여부를 구성할 수 있습니다. 검색에서 네트워크와 영역을 제외하는 규칙을 생성할 수 있습니다. NetFlow 엑스포터에서 데이터 검색을 설정하고 네트워크에서 사용자 데이터가 검색되는 트래픽에 대한 프로토콜을 제한할 수 있습니다.

네트워크 검색 정책에는 관찰되는 모든 트래픽에서 애플리케이션을 검색하도록 설정되는, 단일 기본 규칙이 적용됩니다. 규칙은 네트워크, 영역 또는 포트를 제외하지 않으며, 호스트와 사용자 검색은 설정되지 않습니다. 그리고 규칙은 NetFlow 엑스포터를 모니터링하도록 설정되지 않습니다. 기본적으로 이 정책은 매니지드 디바이스가 management center에 등록될 때 구축됩니다. 호스트 또는 사용자 데이터 수집을 시작하려면, 검색 규칙을 추가 또는 수정하고 디바이스에 정책을 다시 적용해야 합니다.

네트워크 검색의 범위를 조정하려면 추가 검색 규칙을 생성하고 기본 규칙을 수정 또는 제거할 수 있습니다.

각각의 매니지드 디바이스에 대한 액세스 컨트롤 정책은 해당 디바이스에 대해 사용자가 허용하는 트래픽, 즉 네트워크 검색으로 모니터링할 수 있는 트래픽을 정의합니다. 액세스 컨트롤을 사용하여 특정 트래픽을 차단하면 시스템은 해당 트래픽에서 호스트, 사용자 또는 애플리케이션 활동을 검토할 수 없습니다. 예를 들어 액세스 컨트롤 정책이 소셜 네트워킹 애플리케이션에 대한 액세스를 차단하면, 시스템은 해당 애플리케이션에 대한 검색 데이터를 제공하지 않습니다.

검색 규칙에서 트래픽 기반 사용자 검색을 활성화하면, 애플리케이션 프로토콜 모음을 이용하는 트래픽 내 사용자 로그인 활동을 통해 신뢰할 수 없는 사용자를 탐지할 수 있습니다. 필요한 경우 모든 규칙에서 특정 프로토콜에서의 검색을 비활성화할 수 있습니다. 일부 프로토콜을 비활성화하면 management center 모델과 연결된 사용자 제한에 도달하는 것을 방지하여, 다른 프로토콜의 사용자에 대해 사용할 수 있는 사용자 카운트를 확보할 수 있습니다.

고급 네트워크 검색 설정을 사용하면 어떤 데이터를 기록할지, 검색 데이터를 어떻게 저장할지, 어떤 IOC(indications of compromise) 규칙을 활성화할지, 영향 평가에 어떤 취약성 매핑을 사용할지, 소스에서 충돌하는 검색 데이터를 제공할 경우 어떤 일이 발생할지를 관리할 수 있습니다. 모니터링할 호스트 입력 및 NetFlow 엑스포터의 소스를 추가할 수도 있습니다.

네트워크 검색 정책 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

Leaf

사용자 역할

- 관리자
- 검색 관리자

네트워크 검색 맞춤 설정

Firepower System에서 수집하는 네트워크 트래픽에 대한 정보는 시스템이 이 정보를 연계하여 가장 소중하고 가장 중요한 네트워크의 호스트를 식별할 때 가장 가치 있게 사용됩니다.

예를 들어 SuSE Linux의 맞춤형 버전을 실행하는 디바이스가 네트워크에 여러 개 있는 경우 시스템은 해당 운영체제를 식별할 수 없으므로 호스트에 취약성을 매핑할 수 없습니다. 그러나 시스템에 SuSE Linux에 대한 취약성 목록이 있음을 알고 있다면, 호스트 중 하나에 대한 맞춤형 핑거프린트를 생성한 다음 동일한 운영체제를 실행하는 다른 호스트의 식별에 이를 사용할 수 있습니다. 핑거프린트에 SuSE Linux에 대한 취약성 목록의 매핑을 포함하여, 해당 목록을 핑거프린트와 일치하는 각 호스트와 연결할 수 있습니다.

호스트 입력 기능을 사용하여 서드파티 시스템의 호스트 데이터를 네트워크 맵에 직접 입력할 수도 있습니다. 그러나 서드파티 운영체제나 애플리케이션 데이터는 취약성 정보에 자동으로 매핑되지 않습니다. 서드파티 운영체제, 서버 및 애플리케이션 프로토콜 데이터를 사용하여 호스트에 대한 취약성을 보고 영향 상관관계를 수행하려면, 서드파티 시스템의 벤더 및 버전 정보를 VDB(취약성 데이터베이스)에 나열된 벤더 및 버전에 매핑해야 합니다. 호스트 입력 데이터를 지속적으로 유지 관리할 수도 있습니다. 애플리케이션 데이터를 Firepower System 벤더 및 버전 정의에 매핑해도, 가져온 서드파티 취약성은 클라이언트 또는 웹 애플리케이션에 대한 영향 평가에 사용되지 않습니다.

시스템이 네트워크의 호스트에서 실행되는 애플리케이션 프로토콜을 식별할 수 없는 경우, 포트나 패턴을 기반으로 시스템이 애플리케이션을 식별하도록 하는 사용자 정의 애플리케이션 프로토콜 탐지기를 생성할 수 있습니다. 특정 애플리케이션 탐지기를 가져오고 활성화 및 비활성화하여 Firepower System의 애플리케이션 탐지 기능을 한층 더 맞춤화할 수 있습니다.

Nmap 활성 스캐너의 스캔 결과를 사용하여 운영체제 및 애플리케이션 데이터의 탐지를 교체하거나 취약성 목록을 서드파티 취약성으로 보강할 수도 있습니다. 시스템에서는 애플리케이션의 ID를 확인하기 위해 여러 소스의 데이터를 조정할 수 있습니다.

네트워크 검색 정책 설정

다중 도메인 구축의 경우, 각 도메인에는 별도의 네트워크 검색 정책이 있습니다. 사용자 계정이 여러 도메인을 관리할 수 있다면, 정책을 설정할 리프 도메인으로 전환합니다.

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** 정책의 다음 구성 요소를 설정합니다.

- 검색 규칙 - 네트워크 검색 규칙 구성, 4 페이지 섹션을 참조하십시오.
- 사용자에 대한 트래픽 기반 탐지 - 트래픽 기반 사용자 탐지 구성, 13 페이지 섹션을 참조하십시오.
- 고급 네트워크 검색 옵션 - 고급 네트워크 검색 옵션 설정, 14 페이지 섹션을 참조하십시오.
- 맞춤형 운영체제 정의(핑거프린트) - 클라이언트에 대한 맞춤형 핑거프린트 생성 및 서버에 대한 맞춤형 핑거프린트 생성 섹션을 참조하십시오.

네트워크 검색 규칙

네트워크 검색 규칙을 사용하면 원하는 특정 데이터만 포함하도록 네트워크 맵에 대해 검색되는 정보를 맞춤화할 수 있습니다. 네트워크 검색 정책의 규칙은 차례로 평가됩니다. 모니터링 기준을 중첩하여 규칙을 생성할 수 있지만, 그렇게 하면 시스템 성능에 영향이 미칠 수 있습니다.

호스트 또는 네트워크를 모니터링에서 제외하면 해당 호스트 또는 네트워크는 네트워크 맵에 나타나지 않으며 그에 대한 이벤트도 보고되지 않습니다. 그러나 로컬 IP에 대한 호스트 검색 규칙이 비활성화된 경우 탐지 엔진 인스턴스는 기존 호스트 데이터를 사용하는 대신 각 플로우에서 데이터를 새로 구축하므로 처리 부하가 더 큰 영향을 받습니다.

Cisco는 로드 밸런서(또는 로드 밸런서의 특정 포트) 및 NAT 디바이스를 모니터링에서 제외할 것을 권장합니다. 이러한 디바이스는 잘못된 이벤트를 과도하게 생성하여 데이터베이스를 채우고 management center에 과부하를 가져올 수 있습니다. 예를 들어 모니터링되는 NAT 디바이스는 단기간에 운영체제의 여러 업데이트를 표시할 수 있습니다. 로드 밸런서 및 NAT 디바이스의 IP 주소를 알고 있으면 모니터링에서 이들을 제외할 수 있습니다.

팁 시스템은 네트워크 트래픽을 검토하여 다수의 로드 밸런서 및 NAT 디바이스를 식별할 수 있습니다.

또한 맞춤형 서버 핑거프린트를 생성해야 할 경우, 핑거프린트 생성 중인 호스트와 통신하는 데 사용하는 IP 주소를 모니터링에서 일시적으로 제외해야 합니다. 이렇게 하지 않으면 네트워크 맵 및 검색 이벤트 보기가 해당 IP 주소로 표시되는 호스트에 대한 부정확한 정보와 뒤섞이게 됩니다. 핑거프린트를 생성한 후에는 IP 주소를 다시 모니터링하도록 정책을 구성할 수 있습니다.

또한 Cisco는 NetFlow 엑스포터 및 매니지드 디바이스를 이용해 같은 네크워트 세그먼트를 모니터링하지 않을 것을 권장합니다. 중첩되지 않는 규칙으로 네트워크 검색 정책을 구성하는 것이 이상적이지만, 시스템은 매니지드 디바이스에 의해 생성된 중복 연결 로그를 삭제합니다. 그러나 매니지드 디바이스와 NetFlow 엑스포터를 모두 이용해 탐지한 검색에 대한 중복되는 연결 로그는 삭제할 수 없습니다.

네트워크 검색 규칙 구성

호스트 및 애플리케이션 데이터의 검색을 요구에 맞춤화하도록 검색 규칙을 구성할 수 있습니다.

시작하기 전에

- 네트워크 데이터를 검색하려는 트래픽에 대한 연결을 로깅해야 합니다(Cisco Secure Firewall Management Center 관리 가이드의 연결 로깅 모범 사례 참조).
- 내보낸 NetFlow 레코드를 수집하려면 네트워크 검색 정책에 NetFlow 엑스포터 추가, 20 페이지에 설명된 대로 NetFlow 엑스포터를 추가합니다.
- 검색 성능 그래프를 보려면 검색 규칙에서 호스트, 사용자, 애플리케이션을 활성화해야 합니다. (시스템 성능에 영향을 줄 수 있습니다.)

팁 대부분의 경우 Cisco는 RFC 1918에서 주소 검색을 제한합니다.

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** **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 **3** 규칙에 대한 **Action(**작업**)**을 작업 및 검색된 자산, 5 페이지에 설명된 대로 설정합니다.

단계 **4** 선택적 검색 매개변수 설정:

- 특정 네트워크에 대한 규칙 작업을 제한합니다(모니터링되는 네트워크 제한, 6 페이지 참조).
- 특정 영역의 트래픽에 대한 규칙 작업을 제한합니다(네트워크 검색 규칙의 영역 구성, 11 페이지 참조).
- 모니터링에서 포트를 제외합니다(네트워크 검색 규칙에서 포트 제외, 9 페이지 참조).
- NetFlow 데이터 검색에 대한 규칙을 구성합니다(NetFlow 데이터 검색에 대한 규칙 구성, 7 페이지 참조).

단계 **5** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

작업 및 검색된 자산

검색 규칙을 구성할 때에는 규칙에 대한 작업을 선택해야 합니다. 이러한 작업의 영향은 매니지드 디바이스 또는 NetFlow 엑스포터에서 데이터를 검색하는 데 규칙을 사용하는지 여부에 따라 달라집니다.

다음 표에서는 이러한 두 시나리오에서 지정된 작업 설정과 함께 규칙에 의해 어떤 자산이 검색되는지에 대해 설명합니다.

표 ***1:*** 검색 규칙 작업

작업	옵션	매니지드 디바이스	**NetFlow** 엑스포터
제외	--	지정된 네트워크를 모니터링에서 제외합니다. 연결의 소스 또는 대상 호스트가 검색에서 제외되면 연결이 기록되기는 하지만 제외된 호스트에 대해 검색 이벤트가 생성되지 않습니다.	지정된 네트워크를 모니터링에서 제외합니다. 연결의 소스 또는 대상 호스트가 검색에서 제외되면 연결이 기록되기는 하지만 제외된 호스트에 대해 검색 이벤트가 생성되지 않습니다.
파악	호스트	검색 이벤트를 기반으로 호스트를 네트워크 맵에 추가합니다. (선택 사항, 사용자 검색이 활성화된 경우 필수.)	NetFlow 레코드를 기반으로 호스트를 네트워크 맵에 추가하고 연결을 로깅합니다. (필수)

작업	옵션	매니지드 디바이스	**NetFlow** 엑스포터
파악	애플리케이션	애플리케이션 탐지기를 기반으로 애플리케이션을 네트워크 맵에 추가합니다. 애플리케이션 검색 없이는 규칙에서 호스트 또는 사용자를 검색할 수 없습니다. (필수)	NetFlow 레코드 및 `/etc/sf/services`의 포트 애플리케이션 프로토콜 상관관계를 기준으로 애플리케이션 프로토콜을 네트워크 맵에 추가합니다. (선택 사항)
파악	사용자	사용자를 사용자 테이블에 추가하고, 네트워크 검색 정책에 구성된 사용자 프로토콜의 트래픽 기반 탐지를 기준으로 사용자 활동을 로깅합니다. (선택 사항)	해당 없음
NetFlow 연결 기록	--	해당 없음	NetFlow 연결만 기록합니다. 호스트나 애플리케이션은 검색하지 않습니다.

매니지드 디바이스 트래픽을 모니터링할 규칙을 사용하려면 애플리케이션 로깅이 필요합니다. 사용자를 모니터링할 규칙을 사용하려면 호스트 로깅이 필요합니다. 내보낸 NetFlow 레코드를 모니터링할 규칙을 사용하려면 사용자를 로깅하도록 규칙을 구성할 수 없으며, 로깅 애플리케이션은 선택 사항입니다.

참고 시스템은 네트워크 검색 정책의 **Action(**작업**)** 설정을 기준으로, 내보낸 NetFlow 레코드에서 연결을 탐지합니다. 시스템은 액세스 제어 정책 설정을 기준으로 매니지드 디바이스 트래픽에서 연결을 탐지합니다.

모니터링되는 네트워크

검색 규칙을 사용하면 지정된 네트워크의 호스트에서 나가고 들어오는 트래픽에서만 모니터링되는 자산의 검색이 이루어집니다. 검색 규칙에서는 모니터링할 네트워크 내 IP 주소에 대해서만 생성되는 이벤트와 함께, 지정된 네트워크 내에 하나 이상의 IP 주소를 가지고 있는 연결에 대해 검색이 이루어집니다. 기본 검색 규칙은 관찰하는 모든 트래픽(IPv4 트래픽은 `0.0.0.0/0`, IPv6 트래픽은 `::/0`)에서 애플리케이션을 검색합니다.

NetFlow 검색을 처리하고 연결 데이터만 기록하도록 규칙을 설정하면, 시스템은 지정된 네트워크의 IP 주소에 대한 연결도 기록합니다. 네트워크 검색 규칙은 NetFlow 네트워크 연결을 기록하는 유일한 방법입니다.

모니터링할 네트워크를 지정하기 위해 네트워크 개체 또는 개체 그룹을 사용할 수도 있습니다.

모니터링되는 네트워크 제한

모든 검색 규칙에는 하나 이상의 네트워크를 포함해야 합니다.

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** **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 **3** 열려 있지 않은 경우 **Networks(**네트워크**)**를 클릭합니다.

단계 **4** 필요한 경우, 검색 규칙 컨피그레이션 동안 네트워크 개체 생성, 8 페이지에 설명된 대로 Available Networks(사용 가능한 네트워크) 목록에 네트워크 개체를 추가합니다.

참고 네트워크 검색 정책에서 사용된 네트워크 개체를 수정할 경우, 컨피그레이션 변경 사항을 구축할 때까지 변경 사항이 검색에 영향을 미치지 않습니다.

단계 **5** 네트워크를 지정합니다.

- **Available Networks(**사용 가능한 네트워크**)** 목록에서 네트워크를 선택합니다.

  팁 네트워크가 목록에 즉시 나타나지 않으면 다시 로드 아이콘(**Reload(**다시 로드**)**( ))을 클릭합니다.

- Available Networks(사용 가능한 네트워크) 라벨 아래의 텍스트 상자에 IP 주소를 입력합니다.

단계 **6** **Add(**추가**)**를 클릭합니다.

단계 **7** 필요한 경우, 이전의 두 단계를 반복하여 네트워크를 더 추가합니다.

단계 **8** **Save(**저장**)**를 클릭하여 변경 사항을 저장합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

NetFlow 데이터 검색에 대한 규칙 구성

Firepower System은 NetFlow 엑스포터의 데이터를 사용하여 연결 및 검색 이벤트를 생성하고, 호스트 및 애플리케이션 데이터를 네트워크 맵에 추가할 수 있습니다.

검색 규칙에서 NetFlow 엑스포터를 선택하면, 지정된 네트워크에 대한 NetFlow 데이터의 검색으로 규칙이 제한됩니다. NetFlow 디바이스를 선택하면 사용 가능한 규칙 작업이 변경되므로 규칙 동작의 다른 측면을 구성하기 전에 NetFlow 디바이스를 모니터링하도록 선택합니다. NetFlow 엑스포터 모니터링에는 포트 제외를 구성할 수 없습니다.

시작하기 전에

- 네트워크 검색 정책에 NetFlow 지원 디바이스를 추가합니다(네트워크 검색 정책에 NetFlow 엑스포터 추가, 20 페이지 참조).

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** **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 **3** **NetFlow Device(NetFlow** 디바이스**)**를 선택합니다.

단계 **4** **Netflow Device(NetFlow** 디바이스**)** 드롭다운 목록에서 모니터링할 NetFlow 엑스포터의 IP 주소를 선택합니다.

단계 **5** Firepower System의 매니지드 디바이스에서 수집할 NetFlow 데이터의 유형을 지정합니다.

- 연결 전용 — **Action(**작업**)** 드롭다운 목록에서 `Log NetFlow Connections(NetFlow 연결 로깅)`를 선택합니다.
- 호스트, 애플리케이션, 연결 — **Action(**작업**)** 드롭다운 목록에서 `Discover(검색)`를 선택합니다. 시스템에서 **Hosts(**호스트**)** 확인란을 자동으로 확인하고 연결 데이터의 수집을 활성화합니다. 필요한 경우, **Application(**애플리케이션**)** 확인란을 선택하여 애플리케이션 데이터를 수집할 수 있습니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

검색 규칙 컨피그레이션 동안 네트워크 개체 생성

재사용 가능한 네트워크 개체 및 그룹의 목록에 네트워크 개체를 추가하면, 검색 규칙에 표시되는 사용 가능한 네트워크 목록에 새로운 네트워크 개체를 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** **Networks(**네트워크**)**에서 **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 **3** **Available Networks(**사용 가능한 네트워크**)** 옆의 **Add(**추가**)** (+)을 클릭합니다.

단계 **4** 네트워크 개체 생성에 설명된 대로 네트워크 개체를 생성합니다.

단계 **5** 네트워크 검색 규칙 구성, 4 페이지에 설명된 대로 네트워크 검색 규칙 추가를 완료합니다.

포트 제외

호스트를 모니터링에서 제외할 수 있는 것처럼, 특정 포트도 모니터링에서 제외할 수 있습니다. 예를 들면 다음과 같습니다.

- 로드 밸런서는 짧은 기간에 동일한 포트에서 여러 애플리케이션을 보고할 수 있습니다. 포트를 모니터링에서 제외하도록 네트워크 검색 규칙을 구성할 수 있습니다(예: 웹 팜을 처리하는 로드 밸런서의 포트 80 제외).
- 조직에서는 특정 포트 범위를 사용하는 맞춤형 클라이언트를 사용할 수 있습니다. 이 클라이언트의 트래픽이 잘못된 이벤트를 과도하게 생성하면 해당 포트를 모니터링에서 제외할 수 있습니다. 마찬가지로, DNS 트래픽을 모니터링하지 않도록 결정할 수도 있습니다. 이 경우 검색 정책이 포트 53을 모니터링하지 않도록 규칙을 설정할 수 있습니다.

제외할 포트를 추가할 때 Available Ports(사용 가능한 포트) 목록에서 재사용 가능한 포트 개체의 사용 여부를 결정하거나, 포트를 소스 또는 대상 제외 목록에 직접 추가하거나, 재사용 가능한 새 포트를 만든 다음 제외 목록으로 이동할 수 있습니다.

참고 NetFlow 데이터 검색을 처리하는 규칙에서는 포트를 제외할 수 없습니다.

네트워크 검색 규칙에서 포트 제외

NetFlow 데이터 검색을 처리하는 규칙에서는 포트를 제외할 수 없습니다.

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** **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 **3** **Port Exclusions(**포트 제외**)**를 클릭합니다.

단계 **4** 필요한 경우, 검색 규칙 컨피그레이션 동안 포트 개체 생성, 10 페이지에 설명된 대로 Available Ports(사용 가능한 포트) 목록에 포트 개체를 추가합니다.

단계 **5** 다음 방법 중 하나를 사용하여 특정 소스 포트를 모니터링에서 제외합니다.

- **Available Ports(**사용 가능한 포트**)** 목록에서 하나 이상의 포트를 선택하고 **Add to Source(**소스에 추가**)**를 클릭합니다.
- 포트 개체를 추가하지 않고 특정 소스 포트로부터 트래픽을 제외하려면 **Selected Source Ports(**선택된 소스 포트**)** 목록에서 **Protocol(**프로토콜**)**을 선택하고 **Port(**포트**)** 번호(1 ~ 65535)를 입력하고 **Add(**추가**)**를 클릭합니다.

단계 **6** 다음 방법 중 하나를 사용하여 특정 대상 포트를 모니터링에서 제외합니다.

- **Available Ports(**사용 가능한 포트**)** 목록에서 하나 이상의 포트를 선택하고 **Add to Destination(**대상에 추가**)**을 클릭합니다.
- 포트 개체를 추가하지 않고 특정 대상 포트로부터 트래픽을 제외하려면 **Selected Destination Ports(**선택된 대상 포트**)** 목록에서 **Protocol(**프로토콜**)**을 선택하고 **Port(**포트**)** 번호를 입력하고 **Add(**추가**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭하여 변경 사항을 저장합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

검색 규칙 컨피그레이션 동안 포트 개체 생성

시스템의 어디서든 사용할 수 있는 재사용 가능한 포트 개체 및 그룹의 목록에 포트 개체를 추가하면, 검색 규칙에 표시되는 사용 가능한 포트 목록에 새로운 포트 개체를 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** Networks(네트워크)에서 **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 **3** **Port Exclusions(**포트 제외**)**를 클릭합니다.

단계 **4** Available Ports(사용 가능한 포트) 목록에 포트를 추가하려면 **Add(**추가**)** (+)를 클릭합니다.

단계 **5** **Name(**이름**)**을 입력합니다.

단계 **6** 제외할 트래픽의 프로토콜을 **Protocol(**프로토콜**)** 필드에 지정합니다.

단계 **7** 모니터링에서 제외할 포트를 **Port(**포트**)** 필드에 입력합니다.

단일 포트를 지정할 수도 있고, 대시(-)를 사용하여 포트 범위를 지정하거나, 쉼표로 구분된 포트 목록 및 포트 범위를 지정할 수도 있습니다. 허용되는 값의 범위는 1~65535입니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

단계 **9** 포트가 목록에 즉시 나타나지 않으면 **Refresh(**새로 고침**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

네트워크 검색 규칙의 영역

성능 개선을 위해, 규칙 내 영역이 규칙에서 모니터링할 네트워크에 물리적으로 연결된 매니지드 디바이스에 센싱 인터페이스를 포함하도록 검색 규칙을 설정할 수 있습니다.

그러나 네트워크 설정 변경 사항에 대해 항상 지속적으로 알림을 받지는 못할 수도 있습니다. 네트워크 관리자는 별도의 알림 없이 라우팅 또는 호스트 변경을 통해 네트워크 설정을 수정할 수 있으며, 이 경우 적절한 네트워크 검색 정책 설정의 최신 상태를 유지하기가 어려울 수 있습니다. 매니지드 디바이스의 센싱 인터페이스가 네트워크에 어떻게 물리적으로 연결되는지 모른다면, 영역 설정을 기본값으로 유지하십시오. 이 기본값은 시스템이 검색 규칙을 구축 내 모든 영역에 구축하게 합니다. (제외되는 영역이 없다면, 시스템은 검색 정책을 모든 영역에 구축합니다.)

네트워크 검색 규칙의 영역 구성

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** **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 **3** **Zones(**영역**)**를 클릭합니다.

단계 **4** **Available Zones(**사용 가능한 영역**)** 목록에서 영역을 선택합니다.

단계 **5** **Save(**저장**)**를 클릭하여 변경 사항을 저장합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

트래픽 기반 탐지 ID 소스

트래픽 기반 탐지는 시스템에서 지원하는 유일한 권한 없는 ID 소스입니다. 매니지드 디바이스가 구성된 경우 지정한 네트워크에서 LDAP, AIM, POP3, IMAP, Oracle, SIP(VoIP), FTP, HTTP, MDNS 및 SMTP 로그인을 탐지합니다. 트래픽 기반 탐지에서 수집된 데이터는 사용자 인식에만 사용할 수 있습니다. 권한 있는 ID 소스와 달리, 네트워크 검색 정책의 트래픽 기반 탐지는 트래픽 기반 사용자 탐지 구성, 13 페이지에 설명된 대로 구성합니다.

다음과 같은 제한 사항을 참고하십시오.

- 트래픽 기반 탐지는 LDAP 연결에 대한 Kerberos 로그인만 LDAP 인증으로 해석합니다. 매니지드 디바이스는 SSL이나 TLS 등의 프로토콜을 사용하는 암호화된 LDAP 인증을 탐지할 수 없습니다.
- 트래픽 기반 탐지는 OSCAR 프로토콜만을 사용하여 AIM 로그인을 탐지합니다. TOC2를 사용하여 AIM 로그인을 탐지할 수는 없습니다.

- 트래픽 기반 탐지는 SMTP 로깅을 제한할 수 없습니다. 이는 사용자가 SMTP 로그인을 기반으로 데이터베이스에 추가되지 않기 때문입니다. 시스템이 SMTP 로그인을 탐지하더라도 데이터베이스에 일치하는 이메일 주소의 사용자가 이미 있지 않으면 로그인이 기록되지 않습니다.

트래픽 기반 탐지는 실패한 로그인 시도도 기록합니다. 실패한 로그인 시도는 데이터베이스의 사용자 목록에 새 사용자를 추가하지 않습니다. 트래픽 기반 탐지로 탐지된 실패한 로그인 활동에 대한 사용자 활동 유형은 **Failed User Login(**실패한 사용자 로그인**)**입니다.

참고 시스템은 실패한 HTTP 로그인과 성공한 HTTP 로그인을 구분할 수 없습니다. HTTP 사용자 정보를 보려면 트래픽 기반 탐지 컨피그레이션에서 **Capture Failed Login Attempts(**실패한 로그인 시도 캡처**)**를 활성화해야 합니다.

주의 네트워크 검색 정책을 사용하여 HTTP, FTP 또는 MDNS 프로토콜을 통한 신뢰할 수 없는 트래픽 기반 사용자 탐지를 활성화하거나 비활성화 구성 변경 사항을 배포할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort 재시작 트래픽 동작을 참조하십시오.

트래픽 기반 탐지 데이터

디바이스가 트래픽 기반 탐지를 사용하여 로그인을 탐지하면 다음 정보를 management center로 전송하여 사용자 활동으로 로깅됩니다.

- 로그인에서 확인된 사용자 이름
- 로그인 시간
- 로그인과 관련된 IP 주소. 사용자 호스트(LDAP, POP3, IMAP 및 AIM 로그인), 서버(HTTP, MDNS, FTP, SMTP 및 Oracle 로그인) 또는 세션 시작 주체(SIP 로그인)의 IP 주소일 수 있습니다.
- 사용자의 이메일 주소(POP3, IMAP, SMTP 로그인용)
- 로그인을 탐지한 디바이스의 이름

사용자가 이전에 탐지된 적이 있는 경우, management center에서는 해당 사용자의 로그인 기록을 업데이트합니다. management center는 POP3 및 IMAP 로그인의 이메일 주소를 사용하여 LDAP 사용자와의 상관관계를 분석합니다. 예를 들어 management center에서 새로운 IMAP 로그인을 탐지하고 IMAP 로그인의 이메일 주소가 기존 LDAP 사용자와 일치할 경우, IMAP 로그인에서는 신규 사용자를 생성하지 않고 해당 LDAP 사용자의 내역을 업데이트합니다.

사용자가 이전에 탐지된 적이 없는 경우, management center에서는 해당 사용자를 사용자 데이터베이스에 추가합니다. 이러한 로그인 이벤트에는 management center에서 다른 로그인 유형과의 상관관계를 분석할 수 있는 데이터가 없으므로, 고유한 AIM, SIP, Oracle 로그인에서는 항상 새로운 사용자 레코드를 생성합니다.

management center에서는 다음과 같은 경우 사용자 활동 또는 사용자 신원을 기록하지 않습니다.

- 해당 로그인 유형을 무시하도록 네트워크 검색 정책을 구성한 경우
- 매니지드 디바이스에서 SMTP 로그인을 탐지했지만 사용자 데이터베이스에 일치하는 이메일 주소를 보유한 이전에 탐지된 LDAP, POP3 또는 IMAP 사용자가 없는 경우

사용자 데이터가 사용자 테이블에 추가됩니다.

트래픽 기반 탐지 전략

가장 완전한 사용자 정보를 제공할 수 있을 것 같은 사용자들에게 집중할 수 있도록 사용자 활동을 검색하는 프로토콜을 제한하여 탐지되는 총 사용자 수를 줄일 수 있습니다. 프로토콜 탐지를 제한하면 정리되지 않은 사용자 이름을 최소화하고 management center의 스토리지 공간을 보존하는 데 도움이 됩니다.

트래픽 기반 탐지 프로토콜을 선택할 경우 다음 사항을 고려하십시오.

- AIM, POP3, IMAP 등의 프로토콜을 통해 사용자 이름을 가져오는 경우 계약직원, 방문자, 기타 손님 등의 네트워크 액세스 때문에 조직과 관련이 없는 사용자 이름이 포함될 수 있습니다.
- AIM, Oracle, SIP 로그인은 외부 사용자 레코드를 생성할 수 있습니다. 이러한 로그인 유형은 LDAP 서버에서 시스템이 가져오는 사용자 메타데이터와도 연결되지 않고, 매니지드 디바이스에서 탐지하는 기타 로그인 유형에 포함된 정보와도 연결되지 않으므로 이 문제가 발생합니다. 따라서 management center는 이러한 사용자를 다른 사용자 유형과 상호 연결할 수 없습니다.

트래픽 기반 사용자 탐지 구성

네트워크 검색 규칙에서 트래픽 기반 사용자 탐지를 활성화하면 호스트 검색이 자동으로 활성화됩니다. 트래픽 기반 탐지에 대한 자세한 내용은 트래픽 기반 탐지 ID 소스, 11 페이지를 참조하십시오.

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** **Users(**사용자**)**를 클릭합니다.

단계 **3** **Edit(**수정**)** (✎) 버튼을 클릭합니다.

단계 **4** 로그인을 탐지하려는 프로토콜에 대한 확인란을 선택하거나, 로그인을 탐지하지 않으려는 프로토콜에 대한 확인란을 선택 취소합니다.

단계 **5** 필요에 따라 LDAP, POP3, FTP 또는 IMAP 트래픽에서 탐지되는 실패한 로그인 시도를 기록하거나 HTTP 로그인에 대한 사용자 정보를 캡처하려면 **Capture Failed Login Attempts(**실패한 로그인 시도 캡처**)** 체크 박스를 선택합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

주의 네트워크 검색 정책을 사용하여 HTTP, FTP 또는 MDNS 프로토콜을 통한 신뢰할 수 없는 트래픽 기반 사용자 탐지를 활성화하거나 비활성화 구성 변경 사항을 배포할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort 재시작 트래픽 동작을 참조하십시오.

- 네트워크 검색 규칙 구성, 4 페이지에 설명된 대로 사용자를 검색할 네트워크 검색 규칙을 구성합니다.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

고급 네트워크 검색 옵션 설정

네트워크 검색 정책의 Advanced(고급)에서는 어떤 이벤트를 탐지할지, 검색 데이터를 얼마 동안 보존하고 얼마나 자주 업데이트할지, 영향 상관관계에 어떤 취약성 매핑을 사용할지, 운영체제 및 서버 ID 충돌을 어떻게 해결할지 등 정책 전반의 설정을 구성할 수 있습니다. 또한 다른 소스에서 데이터를 가져올 수 있도록 호스트 입력 소스 및 NetFlow 엑스포터를 추가할 수 있습니다.

참고 데이터베이스 이벤트는 검색 및 사용자 활동 이벤트가 시스템 설정에서 설정되도록 제한합니다.

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** **Advanced(**고급**)**를 클릭합니다.

단계 **3** 수정할 설정 옆에 있는 **Edit(**수정**)** ( ) 또는 **Add(**추가**)** ( )을 클릭합니다.

- 데이터 스토리지 설정 - 네트워크 검색 데이터 스토리지 설정, 22 페이지에 설명된 대로 설정을 업데이트합니다.
- 이벤트 로깅 설정 - 네트워크 검색 이벤트 기록 설정, 22 페이지에 설명된 대로 설정을 업데이트합니다.
- 일반 설정 - 네트워크 검색 일반 설정 구성, 15 페이지에 설명된 대로 설정을 업데이트합니다.
- ID 충돌 설정 - 네트워크 검색 ID 충돌 확인 설정, 17 페이지에 설명된 대로 설정을 업데이트합니다.
- 침해 지표 설정 - 보안 침해 지표 규칙 활성화, 19 페이지에 설명된 대로 설정을 업데이트합니다.

- NetFlow 엑스포터 - 네트워크 검색 정책에 NetFlow 엑스포터 추가, 20 페이지에 설명된 대로 설정을 업데이트합니다.
- 운영체제 및 서버 ID 소스 - 네트워크 검색 OS 및 서버 ID 소스 추가, 23 페이지에 설명된 대로 설정을 업데이트합니다.
- 영향 평가에 사용할 취약성 - 네트워크 검색 취약성 영향 평가 활성화, 18 페이지에 설명된 대로 설정을 업데이트합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

네트워크 검색 일반 설정

일반 설정은 시스템이 네트워크 맵을 업데이트하는 빈도 및 검색 중 서버 배너의 캡처 여부를 제어합니다.

배너 캡처

시스템이 서버 벤더 및 버전("배너")을 광고하는 네트워크 트래픽에서 헤더 정보를 저장하도록 하려면 이 확인란을 선택합니다. 이 정보는 수집하는 정보에 추가 콘텍스트를 제공할 수 있습니다. 서버 상세정보에 액세스하여 호스트에 대해 수집된 서버 배너에 액세스할 수 있습니다.

업데이트 간격

호스트의 IP 주소 중 하나가 마지막으로 표시된 시간, 애플리케이션이 사용된 시간 또는 애플리케이션의 히트 수 등의 정보를 시스템이 업데이트하는 간격입니다. 기본 설정은 3,600초(1시간)입니다.

업데이트 시간 초과의 간격을 더 낮게 설정하면 호스트 표시에 더 정확한 정보가 제공되지만, 네트워크 이벤트가 더 많이 생성됩니다.

네트워크 검색 일반 설정 구성

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** **Advanced(**고급**)**를 클릭합니다.

단계 **3** **General Settings(**일반 설정**)** 옆의 **Edit(**수정**)** ( )을(를) 클릭합니다.

단계 **4** 네트워크 검색 일반 설정, 15 페이지에 설명된 대로 설정을 업데이트합니다.

단계 **5** **Save(**저장**)**를 클릭하여 일반 설정을 저장합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

네트워크 검색 ID 충돌 설정

시스템은 운영체제와 서버에 대한 핑거프린트를 트래픽 내 패턴과 일치시켜, 호스트에서 실행 중인 운영체게와 애플리케이션을 확인합니다. 가장 신뢰할 수 있는 운영체제 및 서버 ID 정보를 제공하기 위해 시스템은 여러 소스에서 온 핑거프린트 정보를 맞춰봅니다.

시스템은 운영체제 ID를 도출하고 신뢰도 값을 할당하기 위해 모든 수동 데이터를 사용합니다.

기본적으로 ID 충돌이 없으면, 스캐너 또는 서드파티 애플리케이션에 의해 추가된 ID 데이터가 Firepower System에 의해 탐지된 ID 데이터를 재정의합니다. 우선순위별로 스캐너 및 서드파티 애플리케이션 핑거프린트 소스의 순위를 매기려면 Identity Sources 설정을 사용할 수 있습니다. 시스템은 각 소스에 대해 하나의 ID를 보유하지만, 우선순위가 가장 높은 서드파티 애플리케이션 또는 스캐너 소스의 데이터만 현재 ID로 사용됩니다. 그러나 우선순위와 상관없이 사용자 입력 데이터가 스캐너 및 서드파티 애플리케이션 데이터를 재정의한다는 점에 유의하십시오.

시스템이 Identity Sources 설정에 나열된 활성 스캐너나 서드파티 애플리케이션 소스 또는 Firepower System 사용자에게서 온 기존 ID와 충돌하는 ID를 탐지하면 ID 충돌이 발생합니다. 기본적으로 ID 충돌은 자동으로 해결되지 않으므로, 호스트 프로파일을 통해 또는 호스트를 다시 스캔하거나 새 ID 데이터를 다시 추가하여 수동 ID를 재정의함으로써 충돌을 해결해야 합니다. 하지만 수동 ID나 활성를 유지하여 충돌을 자동으로 해결하도록 시스템을 설정할 수 있습니다.

ID 충돌 이벤트 생성

ID 충돌이 발생할 때 시스템의 이벤트 생성 여부를 지정합니다.

충돌 자동 해결

Automatically Resolve Conflicts(충돌 자동 해결**)** 드롭다운 목록에서 다음 중 하나를 선택합니다.

- **Disabled(**비활성**)** - ID 충돌의 수동 충돌 해결을 강제 실행하려는 경우
- **Identity(ID)** - ID 충돌 발생 시 시스템이 수동 핑거프린트를 사용하게 하려는 경우
- **Keep Active(**활성 상태 유지**)** - ID 충돌 발생 시 시스템이 우선순위가 가장 높은 활성 소스의 현재 ID를 사용하게 하려는 경우

네트워크 검색 ID 충돌 확인 설정

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 **Advanced(**고급**)**를 클릭합니다.

단계 3 **Identity Conflict Settings(ID** 충돌 설정**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 4 네트워크 검색 ID 충돌 설정, 16 페이지에 설명된 대로 Edit Identity Conflict Settings(ID 충돌 설정 편집) 팝업 윈도우의 설정을 업데이트합니다.

단계 5 **Save(**저장**)**를 클릭하여 ID 충돌 설정을 저장합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

네트워크 검색 취약성 영향 평가 옵션

시스템에서 침입 이벤트로 영향 상관관계를 수행하는 방법을 구성할 수 있습니다. 선택 항목은 다음과 같습니다.

- 시스템 기반 취약성 정보를 사용하여 영향 상관관계를 수행하려면 **Use Network Discovery Vulnerability Mappings(**네트워크 검색 취약성 매핑 사용**)** 확인란을 선택합니다.
- 서드파티 취약성 참조를 사용하여 영향 상관관계를 수행하려면 **Use Third-Party Vulnerability Mappings(**서드파티 취약성 매핑 사용**)** 확인란을 선택합니다. 자세한 내용은 *Firepower System Host Input API* 설명서을 참조하십시오.

확인란 하나 또는 둘 다를 선택할 수 있습니다. 시스템이 침입 이벤트를 생성하며 선택한 취약성 매핑 집합의 취약성과 함께 이벤트 관련 호스트에 서버나 운영체제가 있는 경우, 침입 이벤트는 Vulnerable (level 1: red) 영향 아이콘으로 표시됩니다. 벤더 또는 버전 정보가 없는 서버의 경우 management center 설정에서 취약성 매핑을 활성화해야 합니다.

두 확인란을 모두 선택 취소한 경우 침입 이벤트는 Vulnerable (level 1: red) 영향 아이콘으로 표시되지 않습니다.

관련 항목

서드파티 취약성 매핑

네트워크 검색 취약성 영향 평가 활성화

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** **Advanced(**고급**)**를 클릭합니다.

단계 **3** **Vulnerabilities to use for Impact Assessment(**충격 평가에 사용할 취약성**)** 옆의 **Edit(**수정**)** ( )을 클릭합니다.

단계 **4** 네트워크 검색 취약성 영향 평가 옵션, 17 페이지에 설명된 대로 Edit Vulnerability Settings(취약성 설정 편집) 팝업 윈도우의 설정을 업데이트합니다.

단계 **5** 취약성 설정을 저장하려면 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

보안 침해 지표

시스템은 네트워크 검색 정책에서 IOC 규칙을 사용하여 악의적인 수단에 의해 침해될 가능성이 높은 호스트를 식별합니다. 호스트가 이러한 시스템 제공 규칙에 제정된 조건을 충족하면, 시스템은 호스트에 침해 지표(IOC) 태그를 지정합니다. 관련된 규칙을 *IOC* 규칙이라고 합니다. 각 IOC 규칙은 IOC 태그 유형 중 하나에 대응합니다. *IOC* 태그는 가능성이 높은 침해의 특성을 지정합니다.

management center은(는) 다음 중 하나가 발생하면 관련된 호스트 및 사용자 을(를) 태그할 수 있습니다.

- 시스템은 침입, 연결, Security Intelligence(보안 인텔리전스), 파일 또는 악성 이벤트를 이용해, 모니터링되는 네트워크 및 네트워크 트래픽과 관련해 수집한 데이터를 상호 연결하고 잠재 IOC 발생 여부를 확인합니다.
- management center은(는) AMP 클라우드를 통해 엔드포인트 구축을 위한 IOC 데이터를 AMP에서 가져올 수 있습니다. 이 데이터는 호스트 자체에 대한 활동(예: 개별 프로그램에 의해 또는 개별 프로그램에서 수행되는 작업)을 검토하므로, 네트워크 전용 데이터에서는 할 수 없는 위협 가능성에 대한 통찰력을 제공할 수 있습니다. 사용자 편의를 위해, management center은(는) Cisco가 AMP 클라우드를 통해 개발한 새로운 IOC 태그 일체를 자동으로 획득합니다.

이 기능을 설정하려면 보안 침해 지표 규칙 활성화, 19 페이지 섹션을 참조하십시오.

IOC 태그가 있는 호스트를 설명하는 호스트 IOC 데이터와 규정준수 허용리스트에 대한 상관관계 규칙을 작성할 수도 있습니다.

태그가 지정된 IOC를 조사하고 사용하는 방법은 Cisco Secure Firewall Management Center 관리 가이드을 참조하십시오.

보안 침해 지표 규칙 활성화

시스템에서 보안 침해 지표(Indications of compromise, IOC)를 탐지하고 태그하도록 하려면 먼저 네트워크 검색 정책에서 하나 이상의 IOC 규칙을 활성화해야 합니다. 각 IOC 규칙은 한 유형의 IOC 태그에 해당하며 모든 IOC 규칙은 Cisco에서 사전 정의합니다. 원본 규칙은 사용자가 생성할 수 없습니다. 네트워크 및 조직의 필요에 따라 규칙의 일부 또는 전체를 활성화할 수 있습니다. 예를 들어, Microsoft Excel과 같은 소프트웨어를 사용하는 호스트가 모니터링되는 네트워크에 나타나지 않으면 Excel 기반 위협에 해당하는 IOC 태그를 활성화하지 않을 수 있습니다.

팁 개별 호스트 또는 관련 사용자에 대한 IOC 규칙을 비활성화하려면 Cisco Secure Firewall Management Center 관리 가이드의 검색 이벤트 장을 참조하십시오.

시작하기 전에

IOC 규칙은 시스템의 기타 구성 요소 및 AMP for Endpoints에서 제공한 데이터를 기반으로 트리거되므로, 이러한 구성 요소는 IOC 규칙에 올바르게 라이선스를 부여하고 구성하여 IOC 태그를 설정해야 합니다. 활성화할 IOC 규칙과 연결된 시스템 기능을 활성화합니다(예: 침입 탐지 및 방지(IPS) 및 AMP(Advanced Malware Protection)). IOC 규칙의 연결된 기능이 활성화되지 않으면 관련 데이터가 수집되지 않으며 규칙을 트리거할 수 없습니다.

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** **Advanced(**고급**)**를 클릭합니다.

단계 **3** **Indications of Compromise Settings(**감염 지표 설정**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **4** 전체 IOC 기능을 설정 또는 해제하려면 **Enable IOC** 옆에 있는 슬라이더를 클릭합니다.

단계 **5** 개별 IOC 규칙을 전역으로 활성화 또는 비활성화하려면 규칙의 **Enabled(**활성화됨**)** 열에 있는 슬라이더를 클릭합니다.

단계 **6** IOC 규칙 설정을 저장하려면 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

네트워크 검색 정책에 **NetFlow** 엑스포터 추가

시작하기 전에

- 사용하려는 NetFlow 엑스포터를 NetFlow 데이터에 설명된 대로 구성합니다.
- NetFlow 데이터를 사용하기 위한 요건에 설명된 기타 NetFlow 사전 요구 사항을 검토합니다.

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** **Advanced(**고급**)**를 클릭합니다.

단계 **3** **NetFlow Devices(NetFlow** 디바이스**)** 옆의 **Add(**추가**)** ( )을 클릭합니다.

단계 **4** 매니지드 디바이스로 NetFlow 데이터를 수집할 네트워크 디바이스의 IP 주소를 **IP Address(IP** 주소**)** 필드에 입력합니다.

단계 **5** 선택 사항:

- NetFlow 엑스포터를 더 추가하려면 이전의 두 단계를 반복합니다.
- **Delete(**삭제**)** ( )를 클릭하여 NetFlow 엑스포터를 제거합니다. 검색 규칙에서 NetFlow 엑스포터를 사용할 경우, Advanced(고급) 페이지에서 디바이스를 삭제하려면 먼저 규칙을 삭제해야 합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 네트워크 검색 규칙 구성, 4 페이지에 설명된 대로 NetFlow 트래픽을 모니터링할 네트워크 검색 규칙을 구성합니다.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

네트워크 검색 데이터 스토리지 설정

검색 데이터 저장소 설정에는 호스트 제한 및 시간 초과 설정을 포함합니다.

호스트 제한 도달 시

Secure Firewall Management Center가 모니터링할 수 있는 호스트, 즉 네트워크 맵에 저장할 수 있는 호스트 수는 모델에 따라 다릅니다. 호스트 제한 시 옵션은 호스트 제한에 도달했을 때 새 호스트를 탐지하는 경우의 동작을 제어합니다. 다음 작업을 수행할 수 있습니다.

호스트 제거

시스템은 오랫동안 비활성 상태인 호스트를 제거하고 새 호스트를 추가합니다. 이 설정이 기본 설정입니다.

새 호스트 추가 금지

시스템에서 새로 검색된 모든 호스트를 추적하지 않습니다. 시스템은 관리자가 도메인의 호스트 제한을 늘리거나 네트워크 맵에서 수동으로 호스트를 삭제하는 경우, 또는 시스템이 비활성화되어 시간 제한을 초과한 호스트를 식별하여 호스트가 제한 수 이하가 되면 새 호스트를 추적합니다.

다중 도메인 구축에서 리프 도메인은 모니터링되는 호스트의 사용 가능 풀을 공유합니다. 각 리프 도메인이 네트워크 맵을 채울 수 있도록 도메인 속성의 하위 도메인 레벨에서 호스트 제한을 설정할 수 있습니다. 각 리프 도메인에 자체 네트워크 검색 정책이 있으므로 각 리프 도메인은 시스템에서 새 호스트를 검색할 때 다음과 같이 고유한 동작을 제어합니다.

표 ***2:*** 멀티 테넌시의 호스트 제한 도달

설정	도메인 호스트 제한 설정은**?**	도메인 호스트 제한에 도달함	상위 도메인 호스트 제한에 도달함
호스트 제거	예	제한된 도메인에 있는 가장 오래된 호스트를 삭제합니다.	호스트를 삭제하도록 구성된 모든 하위 리프 도메인 중에서 가장 오래된 호스트를 삭제합니다. 호스트가 삭제되지 않는 경우 호스트를 추가하지 않습니다.
	아니요	해당 없음	일반 풀을 공유하고 호스트를 삭제하도록 구성된 모든 하위 리프 도메인 중 가장 오래된 호스트를 삭제합니다.
새 호스트 추가 금지	예 또는 아니오	호스트를 추가하지 않습니다.	호스트를 추가하지 않습니다.

호스트 시간 초과

시스템이 비활성화 상태의 호스트를 네트워크 맵에서 삭제하기까지의 경과 시간(분 단위). 기본 설정은 10080분(1주일)입니다. 개별 호스트 IP 및 MAC 주소는 개별적으로 시간이 초과되지만 호스트는 관련된 모든 주소가 시간 초과되기 전에는 네트워크 맵에서 사라지지 않습니다.

호스트의 조기 시간 초과를 방지하려면 호스트의 시간 제한 값이 네트워크 검색 정책 일반 설정의 업데이트 간격보다 긴지 확인합니다.

서버 시간 초과

시스템이 비활성화 상태의 서버를 네트워크 맵에서 삭제하기까지의 경과 시간(분 단위). 기본 설정은 10080분(1주일)입니다.

서버의 조기 시간 초과를 방지하려면 서비스의 시간 제한 값이 네트워크 검색 정책 일반 설정의 업데이트 간격보다 긴지 확인합니다.

클라이언트 애플리케이션 시간 초과

시스템이 비활성화 상태의 클라이언트를 네트워크 맵에서 삭제하기까지의 경과 시간(분 단위). 기본 설정은 10080분(1주일)입니다.

클라이언트의 조기 시간 초과를 방지하려면 클라이언트의 시간 제한 값이 네트워크 검색 정책 일반 설정의 업데이트 간격보다 긴지 확인합니다.

관련 항목

Firepower System 호스트 제한

네트워크 검색 데이터 스토리지 설정

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** **Advanced(**고급**)**를 클릭합니다.

단계 **3** **Network Discovery Data Storage Settings(**네트워크 검색 데이터 스토리지 설정**)** 옆에 있는 **Edit(**수정**)**(✎)을 클릭합니다.

단계 **4** 네트워크 검색 데이터 스토리지 설정, 20 페이지에 설명된 대로 Data Storage Settings(데이터 스토리지 설정) 대화 상자의 설정을 업데이트합니다.

단계 **5** **Save(**저장**)**를 클릭하여 데이터 스토리지 설정을 저장합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

네트워크 검색 이벤트 기록 설정

Event Logging Settings(이벤트 기록 설정)는 검색 및 호스트 입력 이벤트의 기록 여부를 제어합니다. 이벤트를 기록하지 않으면 이벤트 보기에서 검색할 수 없거나, 상관관계 규칙을 트리거하는 데 사용할 수 없습니다.

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 **Advanced(**고급**)**를 클릭합니다.

단계 3 **Event Logging Settings(**이벤트 기록 설정**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 4 Cisco Secure Firewall Management Center 관리 가이드의 검색 이벤트에서 설명하는 것처럼, 데이터베이스에 기록할 검색 및 호스트 입력 이벤트 유형 옆에 있는 확인란을 선택하거나 선택 취소합니다.

단계 5 **Save(**저장**)**를 클릭하여 이벤트 기록 설정을 저장합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

네트워크 검색 OS 및 서버 ID 소스 추가

네트워크 검색 정책의 Advanced(고급)에서 새 활성 소스를 추가하거나 기존 소스의 우선순위 또는 시간 초과 설정을 변경할 수 있습니다.

이 페이지에 스캐너를 추가한다고 해서 Nmap 스캐너에 대해 존재하는 모든 통합 기능이 추가되지는 않지만, 가져온 서드파티 애플리케이션 또는 스캔 결과를 통합하는 것은 가능합니다.

서드파티 애플리케이션 또는 스캐너에서 데이터를 가져오는 경우 소스의 취약성을 네트워크에서 탐지한 취약성에 매핑해야 합니다.

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 **Advanced(**고급**)**를 클릭합니다.

단계 3 **OS and Server Identity Sources(**운영체제 및 서버 **ID** 소스**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 4 새 소스를 추가하려면 **Add Source(**소스 추가**)**를 클릭합니다.

단계 5 **Name(**이름**)**을 입력합니다.

단계 6 드롭다운 목록에서 입력 소스 **Type(**유형**)**을 선택합니다.

- AddScanResult 기능을 사용하여 스캔 결과를 가져오려면 **Scanner(**스캐너**)**를 선택합니다.
- 스캔 결과를 가져오지 않으려는 경우에는 **Application(**애플리케이션**)**을 선택합니다.

단계 7 이 소스가 네트워크 맵에 ID가 추가되는 시간과 해당 ID가 삭제되는 시간 사이의 간격을 지정하려면 **Timeout(**시간 초과**)** 드롭다운 목록에서 **Hours(**시간**)**, **Days(**일**)** 또는 **Weeks(**주**)**를 선택하고 적절한 기간을 입력합니다.

단계 8 선택 사항:

- 특정 소스를 승격하여 운영체제 및 애플리케이션 ID가 목록에서 그 아래에 있는 소스에 사용되도록 하려면, 해당 소스를 선택하고 위쪽 화살표를 클릭합니다.
- 특정 소스를 강등하여 목록에서 그 위에 있는 소스가 제공하는 ID가 없는 경우에만 운영체제 및 애플리케이션 ID가 사용되도록 하려면, 해당 소스를 선택하고 아래쪽 화살표를 클릭합니다.
- 소스를 삭제하려면 소스 옆에 있는 **Delete(**삭제**)** ( )을 클릭합니다.

단계 **9** **Save(**저장**)**를 클릭하여 ID 소스 설정을 저장합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

관련 항목

서드파티 취약성 매핑

네트워크 검색 전략 문제 해결

시스템의 기본 탐지 기능을 변경하려면 먼저 어떤 호스트가 올바르게 식별되지 않는지, 그 이유가 무엇인지를 분석해야 합니다. 그래야만 어떤 해결책을 구현할지 결정할 수 있습니다.

매니지드 디바이스의 배치가 올바릅니까**?**

로드 밸런서, 프록시 서버 또는 NAT 디바이스 같은 네트워크 디바이스가 매니지드 디바이스 및 식별되지 않는/잘못 식별된 호스트 사이에 상주하는 경우, 맞춤형 핑거프린트를 사용하기보다는 매니지드 디바이스를 잘못 식별된 호스트에 더 가까이 두십시오. Cisco는 이 시나리오에서 맞춤형 핑거프린트의 사용을 권장하지 않습니다.

식별되지 않은 운영체제에 고유한 **TCP** 스택이 있습니까**?**

시스템에서 호스트를 잘못 식별하면 호스트가 잘못 식별된 이유를 조사하여, 맞춤형 핑거프린트를 생성 및 활성화할지 아니면 검색 데이터 대신 Nmap 또는 호스트 입력 데이터를 사용할지를 결정해야 합니다.

⚠

주의 잘못 식별된 호스트를 발견하면 맞춤형 핑거프린트를 생성하기 전에 먼저 지원 부서에 문의하십시오.

기본적으로 호스트가 시스템에서 탐지되지 않는 운영체제를 실행 중이며 TCP 스택 특성 파악 내용을 기존의 탐지된 운영체제와 공유하지 않는 경우에는 맞춤형 핑거프린트를 생성해야 합니다.

예를 들어 시스템이 식별할 수 없는 고유한 TCP 스택의 맞춤형된 Linux 버전을 가지고 있는 경우 맞춤형 핑거프린트를 생성하면 도움이 될 수 있습니다. 이렇게 하면 시스템은 스캔 결과나 서드파티 데이터를 사용하는 대신 호스트를 식별하고 지속적으로 모니터링할 수 있습니다. 이 경우 사용자가 직접 지속적, 능동적으로 데이터를 업데이트해야 합니다.

많은 오픈 소스 Linux 배포에서 동일한 커널이 사용되며, 시스템은 Linux 커널 이름을 사용하여 이들을 식별합니다. Red Hat Linux 시스템에 대해 사용자 핑거프린트를 생성하는 경우, 동일한 핑거프린트가 여러 Linux 배포 제품과 일치하기 때문에 다른 운영체제(예: Debian Linux, Mandrake Linux, Knoppix 등)도 Red Hat Linux로 표시될 수 있습니다.

모든 상황에 핑거프린트를 사용해서는 안 됩니다. 예를 들어 호스트의 TCP 스택이 다른 운영체제와 유사하거나 동일하게 수정되었을 수 있습니다. 예를 들어 Apple Mac OS X 호스트가 변경되어 핑거프린트가 Linux 2.4 호스트와 일치하게 되면 시스템은 이를 Mac OS X가 아닌 Linux 2.4로 식별합니다. Mac OS X 호스트의 맞춤형 핑거프린트를 생성하면, 적합한 모든 Linux 2.4 호스트가 Mac OS X 호스트로 잘못 식별될 수 있습니다. 이 경우 Nmap이 호스트를 올바르게 식별하면 해당 호스트에 대해 주기적인 Nmap 스캔을 예약할 수 있습니다.

호스트 입력을 사용하여 서드파티 시스템의 데이터를 가져오는 경우, 서드파티가 서버 및 애플리케이션 프로토콜을 설명하는 데 사용하는 벤더, 제품 및 버전 문자열을 해당 제품의 Cisco 정의에 매핑해야 합니다. 애플리케이션 데이터를 Firepower System 벤더 및 버전 정의에 매핑해도, 가져온 서드파티 취약성은 클라이언트 또는 웹 애플리케이션에 대한 영향 평가에 사용되지 않습니다.

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

Nmap 데이터의 경우 정기적인 Nmap 스캔을 예약할 수 있습니다. 호스트 입력 데이터의 경우 가져오기 또는 명령줄 유틸리티에 대해 Perl 스크립트를 정기적으로 실행할 수 있습니다. 그러나 활성 스캔 데이터 및 호스트 입력 데이터는 검색 데이터의 빈도로 업데이트되지 않을 수 있습니다.

Firepower System이 모든 애플리케이션을 식별할 수 있습니까**?**

호스트가 시스템에서 올바르게 식별되지만 미확인 애플리케이션을 포함하고 있는 경우, 애플리케이션 식별에 도움이 되도록 사용자 정의 탐지기를 생성하여 시스템에 포트 및 패턴 매칭 정보를 제공할 수 있습니다.

취약성을 수정하는 패치를 적용했습니까**?**

시스템이 호스트를 올바르게 식별하지만 적용된 수정을 반영하지 않는 경우 호스트 입력 기능을 사용하여 패치 정보를 가져올 수 있습니다. 패치 정보를 가져오면 수정 이름을 데이터베이스의 수정에 매핑해야 합니다.

서드파티 취약성을 추적하고자 합니까**?**

영향 상관관계에 사용하고자 하는 서드파티 시스템의 취약성 정보를 가지고 있는 경우, 서버 및 애플리케이션 프로토콜에 대한 서드파티 취약성 식별자를 Cisco 데이터베이스의 취약성 식별자에 매핑한 다음 호스트 입력 기능을 사용하여 취약성을 가져올 수 있습니다. 호스트 입력 기능 사용에 관한 자세한 정보는 *Firepower System Host Input API* 설명서 섹션을 참조하십시오. 애플리케이션 데이터를 Firepower System 벤더 및 버전 정의에 매핑해도, 가져온 서드파티 취약성은 클라이언트 또는 웹 애플리케이션에 대한 영향 평가에 사용되지 않습니다.