상관관계 정책

다음 주제에서는 상관관계 정책과 규칙을 설정하는 방법을 설명합니다.

상관관계 정책 및 규칙 소개

상관관계 기능을 이용하면 상관관계 정책을 바탕으로 네트워크에 대한 위협에 실시간으로 반응할 수 있습니다.

상관관계 정책 위반은 네트워크 상의 활동이 활성 상관관계 정책 내의 상관관계 규칙이나 규정준수 허용 목록을 트리거할 때 발생합니다.

상관관계 규칙

활성 상관관계 정책에서 상관관계 규칙이 트리거되면, 시스템은 상관관계 이벤트를 생성합니다. 상관관계 규칙은 다음 조건이 충족될 때 트리거됩니다.

- 시스템이 특정 유형의 이벤트(연결, 침입, 악성코드, 검색, 사용자 활동 등)를 생성합니다.
- 네트워크 트래픽이 자체 일반 프로파일에서 벗어납니다.

다음 방법으로 상관관계 규칙을 제한할 수 있습니다.

- 트리거링 이벤트와 관련된 호스트의 호스트 프로파일에서 정보를 사용하여 규칙을 제한하려면 호스트 프로파일 자격을 추가합니다.
- 규칙의 초기 기준이 충족된 후 시스템이 특정 연결 추적을 시작할 수 있도록 하려면 상관관계 규칙에 연결 추적기를 추가합니다. 그러면 추적된 연결이 추가 조건을 충족하는 경우에만 상관관계 이벤트가 생성됩니다.

- 특정 사용자 또는 사용자 그룹을 추적하려면 상관관계 규칙에 사용자 자격을 추가합니다. 예를 들어 특정 사용자의 트래픽 또는 특정 부서의 트래픽에 대해서만 트리거하도록 상관관계 규칙을 제한할 수 있습니다.
- 스누즈 기간을 추가합니다. 상관관계 규칙이 트리거될 때, 스누즈 기간 때문에 규칙이 지정된 간격 동안 다시 트리거되지 않을 수도 있습니다. 유휴 기간이 경과하면 규칙을 다시 트리거하고 새 스누즈 기간을 시작할 수 있습니다.
- 비활성 기간을 추가합니다. 비활성 기간 중에는 상관관계 규칙이 트리거되지 않습니다.

구축을 허가받지 않고도 상관과계 규칙을 구성할 수 있지만, 허가받지 않은 구성 요소를 사용하는 규칙은 트리거되지 않습니다.

컴플라이언스 허용 목록

규정준수 허용 목록은 네트워크에서 허용할 운영체제, 애플리케이션(웹 및 클라이언트), 프로토콜을 지정합니다. 호스트가 활성 상관관계 정책에서 사용하는 허용 목록을 위반하는 경우, 시스템은 허용 목록 이벤트를 생성합니다.

상관관계 응답

상관관계 정책 위반에 대한 응답은 단순 알림 및 다양한 교정(호스트 스캔 등)을 포함합니다. 각 상관관계 규칙 또는 허용 리스트를 단일 응답 또는 응답 그룹에 연결할 수 있습니다.

네트워크 트래픽이 여러 규칙 또는 허용 리스트를 트리거하는 경우 각 규칙 및 허용 리스트와 연결된 모든 응답이 시작됩니다.

상관관계 및 멀티 테넌시

다중 도메인 구축의 경우, 각 도메인 레벨에서 사용 가능한 규칙, 허용 목록과 응답을 이용해 어떤 도메인 수준에서도 상관관계 정책을 생성할 수 있습니다. 상위 도메인 관리자는 도메인 내부 또는 도메인 간에서 상관관계를 수행할 수 있습니다.

- 도메인을 이용한 상관관계 규칙 제한은 해당 도메인의 하위 항목에서 보고하는 이벤트와 일치합니다.
- 상위 도메인 관리자는 도메인 간의 호스트를 평가하는 규정준수 허용 목록을 생성할 수 있습니다. 동일한 허용 목록에서 다른 도메인에 있는 다른 서브넷을 대상으로 지정할 수 있습니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 일반적인 설정(IP 주소, VLAN 태그, 사용자 이름 등)으로 도메인 간 상관관계 규칙을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

관련 항목

컴플라이언스 허용 목록 소개

Secure Firewall Management Center 알림 응답

교정 소개

컴플라이언스 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자

상관관계 정책 설정

상관관계 규칙, 규정준수 허용리스트, 알림 응답 및 교정을 사용하여 상관관계 정책을 만듭니다.

다중 도메인 구축의 경우에는, 각 도메인 레벨에서 사용 가능한 구성 요소 설정을 이용해 어떤 도메인 수준에서도 상관관계 정책을 생성할 수 있습니다.

각 상관관계 정책에, 그리고 해당 정책에서 사용하는 각 규칙과 허용리스트에 우선순위를 할당할 수 있습니다. 규칙 및 허용리스트 우선순위는 상관관계 정책 우선순위를 재정의합니다. 네트워크 트래픽이 상관관계 정책을 위반하는 경우, 그에 따른 상관관계 이벤트는 위반한 규칙이나 허용리스트에 자체 우선순위가 없다면 정책 우선순위 값을 표시합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Correlation(**상관관계**)**을(를) 선택합니다.

단계 **2** **Create Policy(**정책 생성**)**를 클릭합니다.

단계 **3** **Policy Name(**정책 이름**)** 및 **Policy Desription(**정책 설명**)**을 입력합니다.

단계 **4** **Default Priority(**기본 우선순위**)** 드롭다운 목록에서 정책의 우선순위를 선택합니다. 규칙 우선순위만 사용하려면 **None(**없음**)**을 선택합니다.

단계 **5** **Add Rules(**규칙 추가**)**를 클릭하고, 정책에서 사용할 규칙 및 허용리스트를 확인한 다음 **Add(**추가**)**를 클릭합니다.

단계 **6** 각 규칙 또는 허용리스트의 **Priority(**우선순위**)** 목록에서 우선순위를 선택합니다.

- 1~5의 운선순위 값
- **None**
- **Default(**기본**)** - 정책의 기본 우선순위 사용

단계 **7** 규칙 및 허용 리스트에 응답 추가, 4 페이지에 설명된 대로 규칙 및 허용리스트에 응답을 추가합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 슬라이더를 클릭하여 정책을 활성화합니다.

규칙 및 허용 리스트에 응답 추가

각 상관관계 규칙 또는 허용 리스트를 단일 응답 또는 응답 그룹에 연결할 수 있습니다. 네트워크 트래픽이 여러 규칙 또는 허용 리스트를 트리거하는 경우 각 규칙 및 허용 리스트와 연결된 모든 응답이 시작됩니다. 트래픽 프로파일 변경에 대한 응답으로 사용되는 경우에는 Nmap 치료가 시작되지 않습니다.

다중 도메인 구축에서는 현재 도메인 또는 상위 도메인에서 생성된 응답을 사용할 수 있습니다.

프로시저

단계 **1** 상관관계 정책 편집기에서 응답을 추가하려는 규칙 또는 허용 목록 옆에 있는 응답()를 클릭합니다.

단계 **2** Unassigned Responses(미할당 응답) 아래에서 규칙 또는 허용 리스트가 트리거될 때 시작할 응답을 선택하고 위로 화살표(^)를 클릭합니다.

단계 **3** **Update(**업데이트**)**를 클릭합니다.

관련 항목

Secure Firewall Management Center 알림 응답
교정 소개

상관관계 정책 관리

활성 상관관계 정책에 적용된 변경사항은 즉시 적용됩니다.

상관관계 정책을 활성화하면, 시스템은 즉시 이벤트를 처리하고 응답을 트리거합니다. 시스템은 최초, 활성화 이후 평가에서는 규정 미준수 호스트에 대한 허용리스트 이벤트를 생성하지 않습니다.

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 상관관계 정책을 표시하며, 이러한 정책은 편집할 수 있습니다. 상위 도메인의 선택된 상관관계 정책도 표시되지만, 이러한 대상은 편집할 수는 없습니다. 하위 도메인에서 생성된 상관관계 정책을 보고 편집하려면 해당 도메인으로 전환하십시오.

참고 상위 도메인의 컨피그레이션이 이름, 매니지드 디바이스 등 관련이 없는 도메인에 대한 정보를 표시하는 경우 상위 도메인의 컨피그레이션은 표시되지 않습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Correlation(**상관관계**)**을(를) 선택합니다.

단계 **2** 상관관계 정책 관리:

- Activate(활성화) 또는 Deactivate(비활성화) - 슬라이더를 클릭합니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.
- 생성 - **Create Policy(**정책 생성**)**를 클릭합니다(상관관계 정책 설정, 3 페이지 참조).
- 편집 - **Edit(**수정**)** ( )을 클릭합니다. 상관관계 정책 설정, 3 페이지의 내용을 참조하십시오. **View(**보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.
- 삭제 - **Delete(**삭제**)** ( )을(를) 클릭합니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

상관관계 규칙 설정

단순한 상관관계 규칙은 특정 유형의 이벤트 발생만 요구합니다. 그 이상의 상세 조건은 입력하지 않아도 됩니다. 예를 들어 트래픽 프로파일 변경 기반의 상관관계 규칙에는 조건이 전혀 필요하지 않습니다. 여러 조건이 적용되며 제한이 추가된 복잡한 상관관계 규칙을 만들 수도 있습니다.

상관관계 규칙 트리거 기준, 호스트 프로파일 자격, 사용자 자격 또는 연결 추적기를 생성할 때 구문은 각기 다르지만 원리는 동일합니다.

참고 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 이벤트와 일치하는 상위 도메인을 기준으로 상관관계 규칙을 제한합니다.

시작하기 전에

- 구축이 상관관계 이벤트를 트리거하는 데 사용할 정보 유형을 수집하고 있는지 확인합니다. 예를 들어 개별 연결 또는 연결 요약 이벤트에 사용 가능한 정보는 탐지 방법, 로깅 방법, 이벤트 유형 등 여러 요인에 따라 달라집니다. 시스템에서는 내보낸 NetFlow 기록에서 네트워크 맵에 호스트를 추가할 수 있지만, 이러한 호스트에 사용할 수 있는 정보는 제한됩니다. NetFlow와 매니지드 디바이스 데이터의 차이점의 내용을 참조하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Correlation(**상관관계**)**을(를) 선택하고 **Rule Management(**규칙 관리**)**을 클릭합니다.

단계 **2** **Create Rule(**규칙 생성**)**을 클릭합니다.

단계 **3** **Rule Name(**규칙 이름**)** 및 **Rule Description(**규칙 설명**)**을 입력합니다.

단계 **4** 원한다면 규칙에 대한 **Rule Group(**규칙 그룹**)**을 선택합니다.

단계 **5** 기본 이벤트 유형을 선택하고, 원한다면 상관관계 규칙에 대한 추가 트리거 기준을 지정합니다. 다음 기본 이벤트 유형을 선택할 수 있습니다.

- 침입 이벤트 발생 - 침입 이벤트 트리거 기준 구문, 7 페이지 섹션을 참조하십시오.
- 악성 코드 이벤트 발생 - 악성코드 이벤트 트리거 기준 구문, 10 페이지 섹션을 참조하십시오.
- 검색 이벤트 발생 - 검색 이벤트 트리거 기준 구문, 11 페이지 섹션을 참조하십시오.
- 사용자 활동 탐지됨 - 사용자 활동 이벤트 트리거 기준 구문, 14 페이지 섹션을 참조하십시오.
- 호스트 입력 이벤트 발생 - 호스트 입력 이벤트 트리거 기준 구문, 15 페이지 섹션을 참조하십시오.
- 연결 이벤트 발생 - 연결 이벤트 트리거 기준 구문, 16 페이지 섹션을 참조하십시오.
- 트래픽 프로파일 변경사항 - 트래픽 프로파일 변경 구문, 20 페이지 섹션을 참조하십시오.

단계 **6** 선택적으로, 다음 중 하나 또는 전부를 추가해 상관관계 규칙을 추가로 제한합니다.

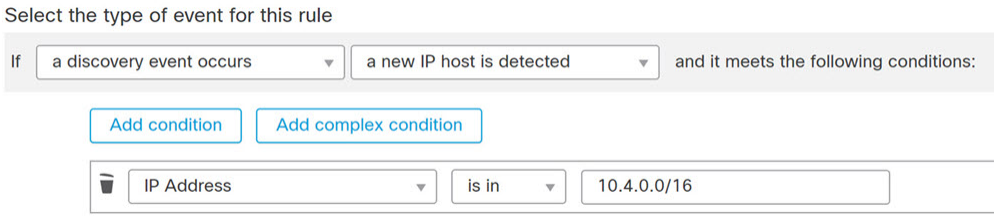
- 호스트 프로파일 자격 - **Add Host Profile Qualification(**호스트 프로파일 자격 추가**)**을 클릭합니다(상관관계 호스트 프로파일 자격 구문, 22 페이지 참조).
- 연결 추적기 - **Add Connection Tracker(**연결 추적기 추가**)**를 클릭합니다(연결 추적기, 26 페이지 참조).
- 사용자 자격 - **Add User Qualification(**사용자 자격 추가**)**을 클릭합니다(사용자 자격 구문, 25 페이지 참조).
- 스누즈 기간 - Rule Options(규칙 옵션)에서 **Snooze(**스누즈**)** 텍스트 필드와 드롭다운 목록을 이용해 시스템에 규칙 트리거 후 상관관계 규칙을 다시 트리거할 때까지 기다려야 하는 기간을 정의합니다.
- 비활성 기간 - Rule Options(규칙 옵션)에서 **Add Inactive Period(**비활성 기간 추가**)**를 클릭합니다. 텍스트 필드와 드롭다운 목록을 사용하여, 시스템이 상관관계 규칙에 대한 네트워크 트래픽 평가를 억제하도록 할 시기와 빈도를 지정합니다.

팁 유휴 기간을 제거하려면 간격을 **0**으로 지정합니다(초, 분 또는 시간).

단계 **7** **Save Rule(**규칙 저장**)**을 클릭합니다.

단순 상관관계 규칙 예시

다음의 단순 상관관계 규칙은 특정 서브넷에서 새 호스트가 탐지되면 트리거됩니다. 카테고리가 IP 주소를 나타낼 때 **is in** 또는 **is not in**을 연산자로 선택하면, IP 주소가 CIDR 등의 특수 표기법으로 표현된 IP 주소 블록에서 *is in* 상태인지 *is not in* 상태인지를 지정할 수 있습니다.



다음에 수행할 작업

- 상관관계 정책 설정, 3 페이지에 설명된 대로 상관관계 정책의 규칙을 사용합니다.

관련 항목

상관관계 규칙 관리, 37 페이지
상관관계 규칙 빌드 메커니즘, 34 페이지
스누즈 및 비활성 기간, 34 페이지
NetFlow와 매니지드 디바이스 데이터의 차이점

침입 이벤트 트리거 기준 구문

다음 표에서는 기본 이벤트로 침입 이벤트를 선택할 경우 상관관계 규칙 조건을 작성하는 방법에 대해 설명합니다.

표 *1:* 침입 이벤트 구문

다음을 지정할 경우...	연산자를 선택하고...
액세스 제어 정책	침입 이벤트를 생성한 침입 정책을 사용하는 액세스 컨트롤 정책을 하나 이상 선택합니다.
액세스 제어 규칙 이름	침입 이벤트를 생성한 침입 정책을 사용하는 액세스 컨트롤 규칙의 이름 전체 또는 일부를 입력합니다.
애플리케이션 프로토콜	침입 이벤트와 관련된 애플리케이션 프로토콜을 하나 이상 선택합니다.
애플리케이션 프로토콜 카테고리	애플리케이션 프로토콜 카테고리를 하나 이상 선택합니다.
분류	하나 이상의 분류를 선택합니다.
클라이언트	침입 이벤트와 관련된 클라이언트를 하나 이상 선택합니다.
클라이언트 카테고리	클라이언트의 카테고리를 하나 이상 선택합니다.
Destination Country(목적지 국가) 또는 Source Country(소스 국가)	침입 이벤트에서 소스 또는 목적지 IP 주소와 관련된 국가를 하나 이상 선택합니다.

다음을 지정할 경우...	연산자를 선택하고...
목적지 IP, 소스 IP, 소스 IP 및 목적지 IP 모두, 또는 소스 IP 나 목적지 IP	단일 IP 주소 또는 주소 블록을 입력합니다.
대상 포트/ICMP 코드 또는 소스 포트/ICMP 유형	소스 트래픽의 포트 번호나 ICMP 코드 또는 대상 트래픽의 포트 번호나 ICMP 유형을 입력합니다.
디바이스	이벤트를 생성했을 가능성이 있는 디바이스를 하나 이상 선택합니다.
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.
Egress Interface(이그레스 인터페이스) 또는 Ingress Interface(인그레스 인터페이스)	하나 이상의 인터페이스를 선택합니다.
Egress Security Zone(이그레스 보안 영역) 또는 Ingress Security Zone(인그레스 보안 영역)	보안 영역 또는 터널 영역을 하나 이상 선택합니다.
생성자 ID	전처리기를 하나 이상 선택합니다.
영향 플래그	침입 이벤트에 할당된 영향 레벨을 선택합니다. 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.
인라인 결과	침입 정책 위반에 따라 시스템이 패킷을 삭제했는지 또는 삭제할 가능성이 있는지를 선택합니다. 시스템은 인라인, 스위치드 또는 라우티드 구축의 패킷을 삭제할 수 있습니다. 침입 규칙 상태나 침입 정책의 삭제 작업에 상관없이, 수동 구축(인라인 설정이 탭 모드에 있는 경우 포함)에서는 패킷을 삭제하지 않습니다.
침입 정책	침입 이벤트를 생성한 침입 정책을 하나 이상 선택합니다.
IOC 태그	침입 이벤트의 결과로 침해 지표 태그가 설정되었는지를 선택합니다.
우선순위	규칙 우선순위를 선택합니다. 규칙 기반 침입 이벤트의 경우 우선순위는 `priority` 키워드의 값 또는 `classtype` 키워드의 값에 해당합니다. 기타 침입 이벤트의 경우, 우선순위는 디코더 또는 프리프로세서에 의해 결정됩니다.

다음을 지정할 경우...	연산자를 선택하고...
프로토콜	http://www.iana.org/assignments/protocol-numbers에 열거된 전송 프로토콜의 이름 또는 번호를 입력합니다.
규칙 메시지	규칙 메시지의 전체 또는 일부를 입력합니다.
규칙 SID	단일 Snort ID(SID) 또는 쉼표로 구분된 여러 SID를 입력합니다. 연산자로 **is in** 또는 **is not in**을 선택하는 경우 다중 선택 팝업 윈도우를 사용할 수 없습니다. 쉼표로 구분된 SID 목록을 입력해야 합니다.
규칙 유형	규칙이 로컬인지를 지정합니다. 로컬 규칙에는 맞춤형 표준 텍스트 침입 규칙, 수정된 표준 텍스트 규칙, 수정된 헤더 정보와 함께 규칙을 저장했을 때 생성된 공유 개체 규칙의 새 인스턴스가 포함됩니다.
SSL 실제 작업	시스템이 암호화된 연결을 처리한 방법을 나타내는 SSL 규칙 작업을 선택합니다.
SSL 인증서 핑거프린트	트래픽을 암호화하는 데 사용된 인증서의 핑거프린트를 입력하거나, 핑거프린트와 연결된 주체 CN을 선택합니다.
SSL 인증서 주체 일반 이름(CN)	세션 암호화에 사용된 인증서의 주체 CN 전체 또는 일부를 입력합니다.
SSL 인증서 주체 국가(C)	세션 암호화에 사용된 인증서의 주체 국가 코드를 하나 이상 선택합니다.
SSL 인증서 주체 조직(O)	세션 암호화에 사용된 인증서의 주체 조직 이름 전체 또는 일부를 입력합니다.
SSL 인증서 주체 조직 단위(OU)	세션 암호화에 사용된 인증서의 주체 조직 단위 이름 전체 또는 일부를 입력합니다.
SSL 흐름 상태	트래픽을 해독하려는 시스템의 결과를 기반으로 상태를 하나 이상 선택합니다.
사용자 이름	침입 이벤트의 소스 호스트에 로그인한 사용자의 사용자 이름을 입력합니다.
VLAN ID	침입 이벤트를 트리거한 패킷에 관련된 가장 안쪽의 VLAN ID를 입력합니다.
웹 애플리케이션	침입 이벤트와 관련된 웹 애플리케이션을 하나 이상 선택합니다.
웹 애플리케이션 카테고리	웹 애플리케이션 카테고리를 하나 이상 선택합니다.

관련 항목

- 침입 이벤트 필드
- Firepower System IP 주소 규칙

악성코드 이벤트 트리거 기준 구문

악성코드 이벤트의 상관관계 규칙에 기반을 두려면, 먼저 사용할 악성코드 이벤트의 유형을 지정해야 합니다. 사용자의 선택에 따라 사용할 수 있는 트리거 기준 집합이 결정됩니다. 다음 중에서 선택할 수 있습니다.

- **by endpoint-based malware detection(**엔드포인트 기반 악성코드 탐지 이용**)**(엔드포인트용 AMP를 이용한 탐지)
- **by network-based malware detection(**네트워크 기반 악성코드 탐지 이용**)**(네트워크용 AMP를 이용한 탐지)
- **by retrospective network-based malware detection(**회귀적 네트워크 기반 악성코드 탐지 이용**)**(네트워크용 AMP를 이용한 회귀적 탐지)

다음 표에서는 기본 이벤트로 악성코드 이벤트를 선택할 경우 상관관계 규칙 조건을 작성하는 방법에 대해 설명합니다.

표 *2:* 악성코드 이벤트 구문

다음을 지정할 경우...	연산자를 선택하고...
애플리케이션 프로토콜	악성코드 이벤트와 관련된 애플리케이션 프로토콜을 하나 이상 선택합니다.
애플리케이션 프로토콜 카테고리	애플리케이션 프로토콜 카테고리를 하나 이상 선택합니다.
클라이언트	악성코드 이벤트와 관련된 클라이언트를 하나 이상 선택합니다.
클라이언트 카테고리	클라이언트의 카테고리를 하나 이상 선택합니다.
Destination Country(목적지 국가) 또는 Source Country(소스 국가)	악성코드 이벤트에서 소스 또는 목적지 IP 주소와 관련된 국가를 하나 이상 선택합니다.
목적지 IP, 호스트 IP 또는 소스 IP	단일 IP 주소 또는 주소 블록을 입력합니다.
대상 포트/ICMP 코드	대상 트래픽의 포트 번호 또는 ICMP 코드를 입력합니다.
속성	**Malware(**악성코드**)**나 **Custom Detection(**맞춤형 탐지**)** 중 하나 또는 둘 다를 선택합니다.
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.
이벤트 유형	엔드포인트용 AMP가 탐지한 악성코드 이벤트와 관련된 이벤트 유형을 하나 이상 선택합니다.
파일 이름	파일의 이름을 입력합니다.

다음을 지정할 경우...	연산자를 선택하고...
파일 유형	파일 형식을 선택합니다.
파일 유형 카테고리	파일 유형 카테고리를 하나 이상 선택합니다.
IOC 태그	악성코드 이벤트의 결과로 침해 지표 태그가 **is** 또는 **is not**으로 설정되었는지를 선택합니다.
SHA-256	파일의 SHA-256 해시 값을 입력하거나 붙여넣습니다.
SSL 실제 작업	시스템이 암호화된 연결을 처리한 방법을 나타내는 SSL 규칙 작업을 선택합니다.
SSL 인증서 핑거프린트	트래픽을 암호화하는 데 사용된 인증서의 핑거프린트를 입력하거나, 핑거프린트와 연결된 주체 CN을 선택합니다.
SSL 인증서 주체 일반 이름(CN)	세션 암호화에 사용된 인증서의 주체 CN 전체 또는 일부를 입력합니다.
SSL 인증서 주체 국가(C)	세션 암호화에 사용된 인증서의 주체 국가 코드를 하나 이상 선택합니다.
SSL 인증서 주체 조직(O)	세션 암호화에 사용된 인증서의 주체 조직 이름 전체 또는 일부를 입력합니다.
SSL 인증서 주체 조직 단위(OU)	세션 암호화에 사용된 인증서의 주체 조직 단위 이름 전체 또는 일부를 입력합니다.
SSL 흐름 상태	트래픽을 해독하려는 시스템의 결과를 기반으로 상태를 하나 이상 선택합니다.
소스 포트/ICMP 유형	소스 트래픽의 포트 번호 또는 ICMP 유형을 입력합니다.
웹 애플리케이션	악성코드 이벤트와 관련된 웹 애플리케이션을 하나 이상 선택합니다.
웹 애플리케이션 카테고리	웹 애플리케이션 카테고리를 하나 이상 선택합니다.

관련 항목

파일 및 악성코드 이벤트 필드
Firepower System IP 주소 규칙

검색 이벤트 트리거 기준 구문

검색 이벤트의 상관관계 규칙에 기반을 두려면, 먼저 사용할 검색 이벤트의 유형을 지정해야 합니다. 사용자의 선택에 따라 사용할 수 있는 트리거 기준 집합이 결정됩니다. 다음 표는 선택할 수 있는 검색 이벤트 유형을 나열합니다.

홉이 변경되는 경우 또는 호스트 제한에 도달하여 시스템이 새 호스트를 삭제하는 경우에는 상관관계 규칙을 트리거할 수 없습니다. 그러나 유형과 상관없이 검색 이벤트가 발생할 때 규칙을 트리거하려면 **there is any type of event(**아무 유형의 이벤트가 존재함**)**를 선택합니다.

표 *3:* 상관관계 규칙 트리거 기준 대 검색 이벤트 유형

옵션 선택	이 검색 이벤트 유형 사용
클라이언트가 변경됨	클라이언트 업데이트
클라이언트의 시간이 초과됨	클라이언트 시간 초과
호스트 IP 주소 재사용됨	DHCP: IP 주소 재할당
호스트 한도에 도달하여 호스트가 삭제됨	호스트 삭제됨: 호스트 한도 도달함
호스트가 네트워크 장치로 식별됨	네트워크 디바이스로 호스트 유형 변경됨
호스트의 시간이 초과됨	호스트 시간 초과
호스트 IP 주소가 변경됨	DHCP: IP 주소 변경됨
NETBIOS 이름 변경이 탐지됨	NETBIOS 이름 변경
새 클라이언트가 탐지됨	새 클라이언트
새 IP 호스트가 탐지됨	새 호스트
새 MAC 주소가 탐지됨	호스트에 대해 추가 MAC 탐지됨
새 MAC 호스트가 탐지됨	새 호스트
새 네트워크 프로토콜이 탐지됨	새 네트워크 프로토콜
새 전송 프로토콜이 탐지됨	새 전송 프로토콜
aTCP 포트가 닫힘	TCP 포트 닫힘
TCP 포트의 시간이 초과됨	TCP 포트 시간 초과
UDP 포트가 닫힘	UDP 포트 닫힘
UDP 포트의 시간이 초과됨	UDP 포트 시간 초과
VLAN 태그가 업데이트됨	VLAN 태그 정보 업데이트
IOC가 설정됨	보안 침해 지표
열린 TCP 포트가 탐지됨	새 TCP 포트
열린 UDP 포트가 탐지됨	새 UDP 포트
호스트에 대한 OS 정보가 변경됨	새 OS
호스트에 대한 OS 또는 서버 ID에 충돌이 발생함	ID 충돌
호스트에 대한 OS 또는 서버 ID의 시간이 초과됨	ID 시간 초과

옵션 선택	이 검색 이벤트 유형 사용
아무 유형의 이벤트가 존재함	아무 이벤트 유형
MAC 주소에 대한 새 정보가 있음	MAC 정보 변경
TCP 서버에 대한 새 정보가 있음	TCP 서버 정보 업데이트
UDP 서버에 대한 새 정보가 있음	UDP 서버 정보 업데이트

다음 표에서는 기본 이벤트로 검색 이벤트를 선택할 경우 상관관계 규칙 조건을 작성하는 방법에 대해 설명합니다.

표 *4:* 검색 이벤트 구문

다음을 지정할 경우...	연산자를 선택하고...
애플리케이션 프로토콜	애플리케이션 프로토콜을 하나 이상 선택합니다.
애플리케이션 프로토콜 카테고리	애플리케이션 프로토콜 카테고리를 하나 이상 선택합니다.
애플리케이션 포트	애플리케이션 프로토콜 포트 번호를 입력합니다.
클라이언트	클라이언트를 하나 이상 선택합니다.
클라이언트 카테고리	클라이언트의 카테고리를 하나 이상 선택합니다.
클라이언트 버전	클라이언트의 버전 번호를 입력합니다.
디바이스	검색 이벤트를 생성했을 가능성이 있는 장치를 하나 이상 선택합니다.
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.
하드웨어	모바일 디바이스의 하드웨어 모델을 입력합니다. 예를 들어 일치하는 모든 Apple iPhone을 찾으려면 **`iPhone`**을 입력합니다.
호스트 유형	호스트 유형을 하나 이상 선택합니다. 호스트를 선택하거나 여러 네트워크 디바이스 유형 중 하나를 선택할 수 있습니다.
IP 주소 또는 새 IP 주소	단일 IP 주소 또는 주소 블록을 입력합니다.
탈옥됨	이벤트의 호스트가 탈옥 모바일 디바이스이면 **Yes(**예**)**, 아니면 **No(**아니오**)**를 선택합니다.
MAC 주소	호스트의 MAC 주소 전체 또는 일부를 입력합니다. 예를 들어 특정 하드웨어 제조업체 디바이스의 MAC 주소가 0A:12:34로 시작하는 것을 알고 있다면 연산자로 **begins with**를 선택하고 값으로 **`0A:12:34`**를 입력할 수 있습니다.

다음을 지정할 경우...	연산자를 선택하고...
MAC 유형	MAC 주소가 **ARP/DHCP Detected**인지 여부를 선택합니다. 즉 시스템에서 MAC 주소를 호스트에 속한 것(**ARP/DHCP Detected**)으로 확실하게 식별했는지, 또는 매니지드 디바이스와 호스트 간에 라우터가 있다는 등의 이유로 여러 호스트가 해당 MAC 주소를 갖는지(**is not ARP/DHCP Detected**) 여부를 선택합니다.
MAC 벤더	검색 이벤트를 트리거한 네트워크 트래픽에 의해 사용된 NIC의 MAC 하드웨어 벤더 이름 전체 또는 일부를 입력합니다.
모바일	이벤트의 호스트가 모바일 디바이스이면 **Yes(예)**, 아니면 **No(아니오)**를 선택합니다.
NETBIOS 이름	호스트의 NetBIOS 이름을 입력합니다.
네트워크 프로토콜	네트워크 프로토콜 번호를 http://www.iana.org/assignments/ethernet-numbers에 표시된 대로 입력합니다.
OS 이름	운영체제 이름을 하나 이상 선택합니다.
OS 벤더	운영체제 벤더를 하나 이상 선택합니다.
OS 버전	운영체제 버전을 하나 이상 선택합니다.
프로토콜 또는전송 프로토콜	http://www.iana.org/assignments/protocol-numbers에 열거된 전송 프로토콜의 이름 또는 번호를 입력합니다.
소스	(운영체제와 서버 ID의 변경 및 시간 초과에 대한) 호스트 입력 데이터의 소스를 선택합니다.
소스 유형	(운영체제와 서버 ID의 변경 및 시간 초과에 대한) 호스트 입력 데이터의 소스 유형을 선택합니다.
VLAN ID	이벤트와 관련된 호스트 VLAN ID를 입력합니다.
웹 애플리케이션	웹 애플리케이션을 선택합니다.

관련 항목

검색 이벤트 유형
검색 이벤트 필드
Firepower System IP 주소 규칙

사용자 활동 이벤트 트리거 기준 구문

사용자 활동의 상관관계 규칙에 기반을 두려면, 먼저 사용할 사용자 활동의 유형을 선택해야 합니다. 사용자의 선택에 따라 사용할 수 있는 트리거 기준 집합이 결정됩니다. 다음 중에서 선택할 수 있습니다.

- 새 사용자 **ID**가 탐지됨
- 사용자가 호스트에 로그인함

다음 표에서는 기본 이벤트로 사용자 활동 이벤트를 선택할 경우 상관관계 규칙 조건을 작성하는 방법에 대해 설명합니다.

표 *5:* 사용자 활동 구문

다음을 지정할 경우...	연산자를 선택하고...
디바이스	사용자 활동을 탐색했을 가능성이 있는 디바이스를 하나 이상 선택합니다.
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.
IP 주소	단일 IP 주소 또는 주소 블록을 입력합니다.
사용자 이름	사용자 이름을 입력합니다.

관련 항목

사용자 활동 데이터 필드

Firepower System IP 주소 규칙

호스트 입력 이벤트 트리거 기준 구문

호스트 입력 이벤트의 상관관계 규칙에 기반을 두려면, 먼저 사용할 호스트 입력 이벤트의 유형을 지정해야 합니다. 사용자의 선택에 따라 사용할 수 있는 트리거 기준 집합이 결정됩니다. 다음 표는 선택할 수 있는 호스트 입력 이벤트 유형을 나열합니다.

사용자 정의 호스트 속성의 정의를 추가, 삭제 또는 변경할 때나 취약성 영향 자격을 설정할 때는 상관관계 규칙을 트리거할 수 없습니다.

표 *6:* 상관관계 규칙 트리거 기준 호스트 입력 이벤트 유형

옵션 선택	이 이벤트 유형에서 규칙을 트리거
클라이언트가 추가됨	클라이언트 추가
클라이언트가 삭제됨	클라이언트 삭제
호스트가 추가됨	호스트 추가
프로토콜이 추가됨	프로토콜 추가
프로토콜이 삭제됨	프로토콜 삭제
스캔 결과가 추가됨	스캔 결과 추가
서버 정의가 설정됨	서버 정의 설정
서버가 추가됨	포트 추가

옵션 선택	이 이벤트 유형에서 규칙을 트리거
서버가 삭제됨	포트 삭제
취약성이 유효하지 않음으로 표시됨	취약성 설정 유효하지 않음
취약성이 유효함으로 표시됨	취약성 설정 유효함
주소가 삭제됨	호스트/네트워크 삭제
속성 값이 삭제됨	호스트 특성 삭제 값
속성 값이 설정됨	호스트 특성 설정 값
운영체제 정의가 설정됨	운영 시스템 정의 설정
호스트 중요도가 설정됨	호스트 중요도 설정

다음 표에서는 기본 이벤트로 호스트 입력 이벤트를 선택할 경우 상관관계 규칙 조건을 작성하는 방법에 대해 설명합니다.

표 *7:* 호스트 입력 이벤트 구문

다음을 지정할 경우...	연산자를 선택하고...
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.
IP 주소	단일 IP 주소 또는 주소 블록을 입력합니다.
소스	호스트 입력 데이터의 소스를 선택합니다.
소스 유형	호스트 입력 데이터의 소스 유형을 선택합니다.

관련 항목

호스트 입력 이벤트 유형
검색 이벤트 필드
Firepower System IP 주소 규칙

연결 이벤트 트리거 기준 구문

연결 이벤트의 상관관계 규칙에 기반을 두려면, 먼저 사용할 연결 이벤트의 유형을 지정해야 합니다. 연결 이벤트에 사용 가능한 정보는 시스템에서 연결을 로깅한 방법, 이유 및 시기에 따라 달라질 수 있습니다. 다음 중에서 선택할 수 있습니다.

- 연결 시작 또는 종료 시
- 연결 시작 시

- 연결 종료 시

다음 표에서는 기본 이벤트로 연결 이벤트를 선택할 경우 상관관계 규칙 조건을 작성하는 방법에 대해 설명합니다.

표 *8:* 연결 이벤트 구문

다음을 지정할 경우...	연산자를 선택하고...
액세스 제어 정책	연결을 로깅한 액세스 컨트롤 정책을 하나 이상 선택합니다.
액세스 제어 규칙 작업	연결을 로깅한 액세스 컨트롤 규칙과 관련된 작업을 하나 이상 선택합니다. 나중에 연결을 처리하는 기본 작업 또는 규칙과 상관없이, 네트워크 트래픽이 Monitor 규칙의 조건과 일치할 때 상관관계 이벤트를 트리거하려면 **Monitor**를 선택합니다.
액세스 제어 규칙	연결을 로깅한 액세스 컨트롤 규칙의 이름 전체 또는 일부를 입력합니다. 나중에 연결을 처리하는 기본 작업 또는 규칙과 상관없이, 연결 기준으로 조건이 일치한 Monitor 규칙의 이름을 입력할 수 있습니다.
애플리케이션 프로토콜	연결과 관련된 애플리케이션 프로토콜을 하나 이상 선택합니다.
애플리케이션 프로토콜 카테고리	애플리케이션 프로토콜 카테고리를 하나 이상 선택합니다.
클라이언트	클라이언트를 하나 이상 선택합니다.
클라이언트 카테고리	클라이언트의 카테고리를 하나 이상 선택합니다.
클라이언트 버전	클라이언트의 버전 번호를 입력합니다.
연결 지속시간	연결 이벤트의 기간을 초 단위로 입력합니다.
연결 유형	연결 이벤트를 획득한 방법에 따라 상관관계 규칙을 트리거할지 여부를 지정합니다. • 내보낸 NetFlow 데이터에서 생성한 연결 이벤트에 대해 **is**와 **Netflow**를 선택합니다. • Firepower System 매니지드 디바이스가 탐지한 연결 이벤트에 대하 **is not**과 **Netflow**를 선택합니다.
Destination Country(목적지 국가) 또는 Source Country(소스 국가)	연결 이벤트에서 소스 또는 목적지 IP 주소와 관련된 국가를 하나 이상 선택합니다.
디바이스	연결을 탐지했거나 (내보낸 NetFlow 기록에서 얻은 연결 데이터의 경우) 연결을 처리한 디바이스를 하나 이상 선택합니다.
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

다음을 지정할 경우...	연산자를 선택하고...
Egress Interface(이그레스 인터페이스) 또는 Ingress Interface(인그레스 인터페이스)	하나 이상의 인터페이스를 선택합니다.
Egress Security Zone(이그레스 보안 영역) 또는 Ingress Security Zone(인그레스 보안 영역)	보안 영역 또는 터널 영역을 하나 이상 선택합니다.
이니시에이터 바이트, 응답자 바이트 또는 전체 바이트	다음 중 하나를 입력합니다. • 전송한 바이트 수(이니시에이터 바이트) • 수신한 바이트 수(응답자 바이트) • 주고받은 바이트 수(전체 바이트)
이니시에이터 IP, 응답자 IP, 이니시에이터와 응답자 IP 모두, 또는 이니시에이터 IP나 응답자 IP	단일 IP 주소 또는 주소 블록을 지정합니다.
이니시에이터 패킷, 응답자 패킷 또는 총 패킷	다음 중 하나를 입력합니다. • 전송한 패킷 수(이니시에이터 패킷). • 수신한 패킷 수(응답자 패킷). • 주고받은 패킷 수(총 패킷)
이니시에이터 포트/ICMP 유형 또는 응답자 포트/ICMP 코드	이니시에이터 트래픽의 포트 번호나 ICMP 유형 또는 응답자 트래픽의 포트 번호나 ICMP 코드를 입력합니다.
IOC 태그	연결 이벤트 때문에 침해 지표 태그가 **is** 또는 **is not**으로 설정되었느지를 지정합니다.
NetBIOS 이름	연결에서 모니터링된 호스트의 NetBIOS 이름을 입력합니다.
NetFlow 디바이스	상관관계 규칙을 트리거하는 데 사용할 NetFlow 엑스포터의 IP 주소를 선택합니다. 네트워크 검색 정책에 어떤 NetFlow 엑스포터도 추가하지 않았다면, **NetFlow Device(NetFlow** 디바이스**)** 드롭다운 목록에는 아무것도 표시되지 않습니다.
사전 필터 정책	연결을 처리한 사전 필터 정책을 하나 이상 선택합니다.
이유	연결 이벤트와 관련된 이유를 하나 이상 선택합니다.

다음을 지정할 경우...	연산자를 선택하고...
보안 인텔리전스 범주	연결 이벤트와 관련된 보안 인텔리전스 카테고리를 하나 이상 선택합니다. 보안 인텔리전스 카테고리를 연결 종료 이벤트의 조건으로 사용하려면, 액세스 컨트롤 정책에서 해당 카테고리를 **Block**이 아닌 **Monitor**로 설정합니다.
SSL 실제 작업	시스템이 암호화된 연결을 처리한 방법을 나타내는 SSL 규칙 작업을 지정합니다.
SSL 인증서 핑거프린트	트래픽을 암호화하는 데 사용된 인증서의 핑거프린트를 입력하거나, 핑거프린트와 연결된 주체 CN을 선택합니다.
SSL 인증서 상태	세션 암호화에 사용된 인증서와 관련된 상태를 하나 이상 선택합니다.
SSL 인증서 주체 일반 이름(CN)	세션 암호화에 사용된 인증서의 주체 CN 전체 또는 일부를 입력합니다.
SSL 인증서 주체 국가(C)	세션 암호화에 사용된 인증서의 주체 국가 코드를 하나 이상 선택합니다.
SSL 인증서 주체 조직(O)	세션 암호화에 사용된 인증서의 주체 조직 이름 전체 또는 일부를 입력합니다.
SSL 인증서 주체 조직 단위(OU)	세션 암호화에 사용된 인증서의 주체 조직 단위 이름 전체 또는 일부를 입력합니다.
SSL 암호 그룹	세션 암호화에 사용된 암호 그룹을 하나 이상 선택합니다.
SSL 암호화된 세션	**Successfully Decrypted(**성공적으로 해독**)**를 선택합니다.
SSL 흐름 상태	트래픽을 해독하려는 시스템의 결과를 기반으로 상태를 하나 이상 선택합니다.
SSL 정책	암호화된 연결을 로깅한 SSL 정책을 하나 이상 선택합니다.
SSL 규칙 이름	암호화된 연결을 로깅한 SSL 규칙의 이름 전체 또는 일부를 입력합니다.
SSL 서버 이름	클라이언트가 암호화된 연결을 설정한 서버의 이름 전체 또는 일부를 입력합니다.
SSL URL 카테고리	암호화된 연결에서 방문한 URL의 URL 카테고리를 하나 이상 선택합니다.
SSL 버전	세션 암호화에 사용된 SSL 또는 TLS 버전을 하나 이상 선택합니다.
TCP 플래그	상관관계 규칙을 트리거하기 위해 연결 이벤트에 포함해야 할 TCP 플래그를 선택합니다. NetFlow에서 생성한 연결 데이터만 TCP 플래그를 가지고 있습니다.
전송 프로토콜	연결에 사용된 전송 프로토콜(**`TCP`** 또는 **`UDP`**)을 입력합니다.
터널/사전 필터 규칙	연결을 처리한 터널 또는 사전 필터 규칙 이름의 전체 또는 일부를 입력합니다.
URL	연결에서 방문한 URL 전체 또는 일부를 입력합니다.
URL 범주	연결에서 방문한 URL의 URL 카테고리를 하나 이상 선택합니다.
URL 평판	연결에서 방문한 URL의 URL 평판 값을 하나 이상 선택합니다.

다음을 지정할 경우...	연산자를 선택하고...
사용자 이름	연결의 두 호스트 중 하나에 로그인한 사용자의 사용자 이름을 입력합니다.
웹 애플리케이션	연결과 관련된 웹 애플리케이션을 하나 이상 선택합니다.
웹 애플리케이션 카테고리	웹 애플리케이션 카테고리를 하나 이상 선택합니다.

관련 항목

연결 및 보안 관련 연결 이벤트 필드

Firepower System IP 주소 규칙

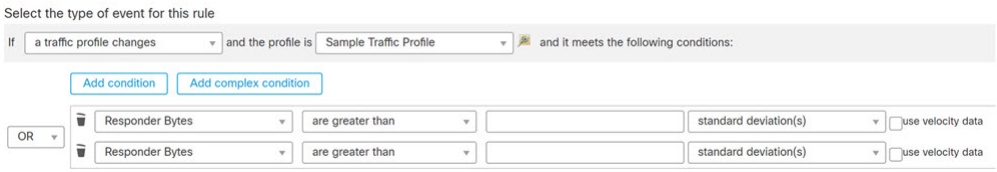
트래픽 프로파일 변경 구문

트래픽 프로파일 변경사항에 대한 상관관계 규칙을 기반으로 하려면, 먼저 사용할 트래픽 프로파일을 선택해야 합니다. 규칙은 네트워크 트래픽이 선택한 프로파일로 특성화되는 패턴에서 벗어날 때 트리거됩니다.

원시 데이터 또는 데이터에서 계산된 통계를 기반으로 규칙을 트리거할 수 있습니다. 예를 들어 네트워크를 통과하는 데이터의 양(바이트 단위로 측정됨)이 급증할 때(공격이나 기타 보안 정책 위반의 징후일 수 있음) 트리거되는 규칙을 작성할 수 있습니다. 다음의 경우 규칙이 트리거되도록 지정할 수 있습니다.

- 네트워크를 통과하는 바이트 수가 특정 바이트 수 위로 급증하는 경우
- 네트워크를 통과하는 바이트 수가 평균 트래픽 양의 위 또는 아래에서 표준 편차의 특정 수치 위로 급증하는 경우

  네트워크를 통과하는 바이트의 수가 표준 편차의 특정 수치(위 또는 아래)를 벗어날 때 트리거되는 규칙을 생성하려면 다음 그림에 보이는 것처럼 상한 또는 하한을 지정해야 합니다.



  통과하는 바이트 수가 평균 위에서 표준 편차의 특정 수보다 클 때 트리거되는 규칙을 생성하려면 그림에 보이는 첫 번째 조건만 사용하십시오.

  통과하는 바이트 수가 평균 아래에서 표준 편차의 특정 수보다 클 때 트리거되는 규칙을 생성하려면 두 번째 조건만 사용하십시오.

데이터 포인트 간 변경 속도를 기반으로 상관관계 규칙을 트리거하려면 **use velocity data(**속도 데이터 사용**)** 확인란을 선택합니다. 위의 예에서 속도 데이터를 사용한다면 다음과 같은 경우 규칙이 트리거되도록 지정할 수 있습니다.

- 네트워크를 통과하는 바이트의 양이 변경되어 평균 변경 속도 위에서 표준 편차의 특정 수치 위 또는 아래로 급증하는 경우

- 네트워크를 통과하는 바이트 수가 변경되어 특정 바이트 수 위로 급증하는 경우

다음 표에서는 기본 이벤트로 트래픽 프로파일 변경을 선택할 경우 상관관계 규칙에서 조건을 작성하는 방법에 대해 설명합니다.

표 ***9:*** 트래픽 프로파일 변경 구문

다음을 지정할 경우...	연산자를 선택하고 다음을 입력합니다.	그런 후에 다음 중 하나를 선택합니다.
연결 수	탐지된 총 연결 수 또는 규칙을 트리거하기 위해 탐지된 연결 수가 속해야 하는 평균 위 또는 아래 표준 편차의 수	연결 표준 편차
총 바이트, 이니시에이터 바이트 또는 응답자 바이트	다음 중 하나에 해당합니다. • 전송한 총 바이트(총 바이트) • 전송한 바이트 수(이니시에이터 바이트) • 수신한 바이트 수(응답자 바이트) 또는 규칙을 트리거하기 위해 위 기준 중 하나가 속해야 하는 평균 위 또는 아래 표준 편차의 수	바이트 표준 편차
총 패킷, 이니시에이터 패킷 또는 응답자 패킷	다음 중 하나에 해당합니다. • 전송한 총 패킷(총 패킷) • 전송한 패킷 수(이니시에이터 패킷) • 수신한 패킷 수(응답자 패킷) 또는 규칙을 트리거하기 위해 위 기준 중 하나가 속해야 하는 평균 위 또는 아래 표준 편차의 수	packets 표준 편차
고유한 이니시에이터	세션을 시작한 고유한 호스트의 수 또는 규칙을 트리거하기 위해 탐지된 고유한 이니시에이터 수가 속해야 하는 평균 위 또는 아래 표준 편차의 수	개시자 표준 편차

다음을 지정할 경우...	연산자를 선택하고 다음을 입력합니다.	그런 후에 다음 중 하나를 선택합니다.
고유한 응답자	세션에 응답한 고유한 호스트의 수 또는 규칙을 트리거하기 위해 탐지된 고유한 응답자 수가 속해야 하는 평균 위 또는 아래 표준 편차의 수	응답자 표준 편차

상관관계 호스트 프로파일 자격 구문

이벤트와 관련된 호스트의 호스트 프로파일을 기준으로 상관관계 규칙을 제한하려면 *host profile qualification(*호스트 프로파일 자격*)*을 추가합니다. 악성코드 이벤트, 트래픽 프로파일 변경 또는 새 IP 호스트 탐색에 대해 트리거되는 상관관계 규칙에 호스트 프로파일 자격을 추가할 수 없습니다.

호스트 프로파일 자격을 작성할 때 먼저 상관관계 규칙을 제한하는 데 사용할 호스트를 지정해야 합니다. 선택할 수 있는 호스트는 규칙의 기본 이벤트 유형에 따라 달라집니다 .

- 연결 이벤트 - **Responder Host(**응답자 호스트**)** 또는 **Initiator Host(**이니시에이터 호스트**)**를 선택합니다.
- 침입 이벤트 - **Destination Host(**목적지 호스트**)** 또는 **Source Host(**소스 호스트**)**를 선택합니다.
- 검색 이벤트, 호스트 입력 이벤트 또는 사용자 활동 - **Host(**호스트**)**를 선택합니다.

다음 표에서는 상관관계 규칙에 대한 호스트 프로파일 자격을 만드는 방법을 설명합니다.

표 ***10:*** 호스트 프로파일 자격 구문

다음을 지정할 경우...	연산자를 선택하고...
애플리케이션 프로토콜 >애플리케이션 프로토콜	애플리케이션 프로토콜을 선택합니다.
애플리케이션 프로토콜 >애플리케이션 포트	애플리케이션 프로토콜 포트 번호를 입력합니다.
애플리케이션 프로토콜 >프로토콜	프로토콜을 선택합니다.
애플리케이션프로토콜카테고리	카테고리를 선택합니다.
클라이언트 > 클라이언트	클라이언트를 선택합니다.
클라이언트 > 클라이언트 버전	클라이언트 버전을 입력합니다.
클라이언트 카테고리	카테고리를 선택합니다.

다음을 지정할 경우...	연산자를 선택하고...
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다.이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.
하드웨어	모바일 디바이스의 하드웨어 모델을 입력합니다. 예를 들어 일치하는 모든 Apple iPhone을 찾으려면 **`iPhone`**을 입력합니다.
호스트 중요도	호스트 중요도를 선택합니다.
호스트 유형	호스트 유형을 하나 이상 선택합니다. 일반 호스트를 선택하거나 여러 네트워크 디바이스 유형 중 하나를 선택할 수 있습니다.
IOC 태그	침해 지표 태그를 하나 이상 선택합니다.
탈옥됨	이벤트의 호스트가 탈옥 모바일 디바이스이면 **Yes(**예**)**, 아니면 **No(**아니오**)**를 선택합니다.
MAC 주소 > MAC 주소	호스트의 MAC 주소 전체 또는 일부를 입력합니다.
MAC 주소 > MAC 유형	MAC 유형이 ARP/DHCP Detected인지 여부를 선택합니다. • 시스템이 MAC 주소가 호스트에 속한 것으로 명확하게 확인함**(is ARP/DHCP Detected)** • 디바이스와 호스트 간에 라우터가 있다는 등의 이유로, 시스템이 MAC 주소가 있는 다양한 호스트를 확인함**(is not ARP/DHCP Detected)** • MAC 유형이 올바르지 않음**(is any)**
MAC 벤더	호스트에서 사용하는 하드웨어의 MAC 벤더 전체 또는 일부를 입력합니다.
모바일	이벤트의 호스트가 모바일 디바이스이면 **Yes(**예**)**, 아니면 **No(**아니오**)**를 선택합니다.
NetBIOS 이름	호스트의 NetBIOS 이름을 입력합니다.
네트워크 프로토콜	네트워크 프로토콜 번호를 http://www.iana.org/assignments/ethernet-numbers에 표시된 대로 입력합니다.
운영체제 > OS 벤더	운영체제 벤더 이름을 하나 이상 선택합니다.
운영체제 > OS 이름	운영체제 이름을 하나 이상 선택합니다.
운영체제 > OS 버전	운영체제 버전을 하나 이상 선택합니다.
전송 프로토콜	http://www.iana.org/assignments/protocol-numbers에 열거된 전송 프로토콜의 이름 또는 번호를 입력합니다.
VLAN ID	호스트의 VLAN ID 번호를 입력합니다.
웹 애플리케이션	웹 애플리케이션을 선택합니다.
웹 애플리케이션 카테고리	카테고리를 선택합니다.

다음을 지정할 경우...	연산자를 선택하고...
사용 가능한 모든 호스트 속성(기본 규정준수 허용리스트 호스트 속성 포함)	호스트 속성 유형에 맞는 적절한 값을 입력하거나 선택합니다.

암시적 또는 일반 클라이언트를 사용하여 호스트 프로파일 자격 구축

시스템이 뒤에 클라이언트가 붙는 애플리케이션 프로토콜 이름(HTTPS 클라이언트 등)을 이용해 탐지 클라이언트를 보고하는 경우, 해당 클라이언트는 암시적 또는 일반 클라이언트가 됩니다. 이 경우 시스템은 특정 클라이언트를 탐지하지 않지만, 서버 응답 트래픽을 기준으로 클라이언트 존재를 추론합니다.

암시적 또는 일반 클라이언트를 사용하여 호스트 프로파일 자격을 생성하려면, 클라이언트가 아닌 응답자 호스트에서 실행하는 애플리케이션 프로토콜을 이용해 제한해야 합니다.

이벤트 데이터를 사용하여 호스트 프로파일 자격 작성

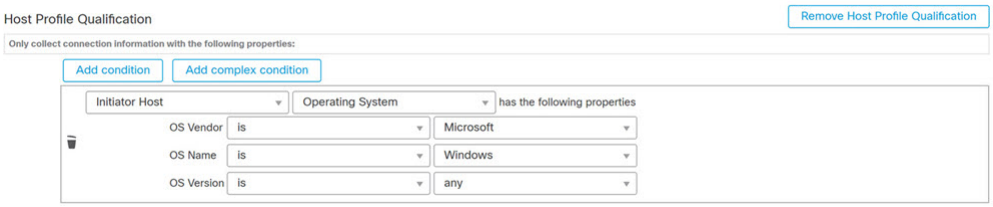
호스트 프로파일 자격을 구성할 때는 상관관계 규칙의 기본 이벤트에서 제공하는 데이터를 자주 사용하게 됩니다.

예를 들어 모니터링되는 호스트 중 하나에서 특정 브라우저를 사용하는 것을 시스템이 탐지할 때 상관관계 규칙이 트리거된다고 가정해보겠습니다. 그리고 이러한 사용을 탐지할 때, 브라우저 버전이 최신 버전이 아니라면 이벤트를 생성하려 합니다.

Client(클라이언트**)**가 **Event Client(**이벤트 클라이언트**)**지만 **Client Version(**클라이언트 버전**)**이 최신 버전이 아닐 경우에만 규칙이 트리거되도록 호스트 프로파일 자격을 이 상관관계 규칙에 추가할 수 있습니다.

호스트 프로파일 자격 예

다음 호스트 프로파일 자격은 규칙의 기반이 되는 검색 이벤트와 관련된 호스트가 Microsoft Windows 버전을 실행하는 경우에만 규칙이 트리거되는 방식으로 상관관계 규칙을 제한합니다.



관련 항목

호스트 데이터 필드

사용자 자격 구문

연결, 침입, 검색 또는 호스트 입력 이벤트를 사용하여 상관관계 규칙을 트리거하는 경우, 이벤트와 관련된 사용자의 ID를 기반으로 규칙을 제한할 수 있습니다. 이러한 제약을 *user qualification(*사용자 자격*)*이라고 합니다. 예를 들어 소스 또는 대상 사용자의 ID가 영업 부서 사용자인 경우에만 트리거되도록 상관관계 규칙을 제한할 수 있습니다.

트래픽 프로파일 변경 또는 사용자 활동 탐색에 대해 트리거되는 상관관계 규칙에 사용자 자격을 추가할 수 없습니다. 또한 시스템은 management center-ID 영역에서 형성된 서버 연결을 통해 사용자 상세정보를 획득합니다. 데이터베이스의 일부 사용자에 대해서는 이 정보를 이용하지 못할 수 있습니다.

사용자 자격을 작성할 때 먼저 상관관계 규칙을 제한하는 데 사용할 ID를 지정해야 합니다. 선택할 수 있는 ID는 규칙의 기본 이벤트 유형에 따라 달라집니다 .

- 연결 이벤트 - 이니시에이터에서의 **ID** 또는 응답자에서의 **ID**를 선택합니다.
- 침입 이벤트 - 목적지에서의 **ID** 또는 소스에서의 **ID**를 선택합니다.
- 검색 이벤트 - 호스트에서의 **ID**를 선택합니다.
- 호스트 입력 이벤트 - 호스트에서의 **ID**를 선택합니다.

다음 표에서는 상관관계 규칙에 대한 사용자 자격을 만드는 방법을 설명합니다.

표 ***11:*** 사용자 자격 구문

다음을 지정할 경우...	연산자를 선택하고...
인증 프로토콜	사용자 탐지에 사용한 인증 프로토콜(또는 사용자 유형) 프로토콜을 선택합니다.
부서	부서를 입력합니다.
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.
이메일	이메일 주소를 입력합니다.
이름	이름을 입력합니다.
성	성을 입력합니다.
전화 번호	전화번호를 입력합니다.
사용자 이름	사용자 이름을 입력합니다.

관련 항목

사용자 데이터 필드

연결 추적기

규칙의 초기 기준이 충족되면(호스트 프로파일 및 사용자 자격 포함) 시스템이 특정 연결 추적을 시작할 수 있도록, 연결 추적기는 상관관계 규칙을 제한합니다. 추적된 연결이 지정 기간 동안 수집된 추가 기준을 충족할 경우 시스템은 규칙에 대해 상관관계 이벤트를 생성합니다.

팁 연결 추적기는 일반적으로 매우 구체적인 트래픽을 모니터링하며, 트리거될 경우 지정된 기간에만 실행됩니다. 일반적으로 폭넓은 네트워크 트래픽을 모니터링하고 영구적으로 실행되는 트래픽 프로파일을 연결 추적기와 비교해보십시오.

연결 추적기는 두 가지 방법으로 이벤트를 생성할 수 있습니다.

조건이 충족될 때 즉시 실행되는 연결 추적기

네트워크 트래픽이 추적기의 조건을 충족하자마자 상관관계 규칙이 실행되도록 연결 추적기를 구성할 수 있습니다. 이러한 상황이 발생하면 시스템은 시간 초과 기간이 만료되지 않았더라도 이 연결 추적기 인스턴스에 대한 연결 추적을 중지합니다. 상관관계 규칙을 트리거한 동일한 정책 위반 유형이 다시 발생하면 시스템은 새 연결 추적기를 생성합니다.

하지만 네트워크 트래픽이 연결 추적기의 조건을 충족하기 전에 시간이 만료되면 시스템은 상관관계 이벤트를 생성하지 않으며, 동시에 해당 규칙 인스턴스에 대한 연결 추적을 중지합니다.

예를 들어 연결 추적기는 특정 유형의 연결이 지정된 기간 내에 지정된 횟수보다 더 많이 발생하는 경우에만 상관관계 이벤트를 생성함으로써 일종의 이벤트 임계값 역할을 할 수 있습니다. 또는 초기 연결 이후 시스템에서 과도한 데이터 전송을 탐지하는 경우에만 상관관계 이벤트를 생성할 수 있습니다.

시간 초과 기간 끝에 실행되는 연결 추적기

전체 시간 초과 기간에 수집된 데이터에 의존하도록, 따라서 시간 초과 기간이 끝날 때까지 실행될 수 없도록 연결 추적기를 구성할 수 있습니다.

예를 들어 일정 기간 동안 특정 바이트 수 미만이 탐지될 때 실행되도록 연결 추적기를 구성하는 경우, 시스템은 기간이 지날 때까지 기다렸다가 네트워크 트래픽이 해당 조건을 충족하면 이벤트를 생성합니다.

연결 추적기 추가

시작하기 전에

- 연결, 침입, 검색, 사용자 ID 또는 호스트 입력 이벤트를 기반으로 상관관계 규칙을 생성합니다. 악성코드 이벤트 또는 트래픽 프로파일 변경을 기반으로 하는 규칙에는 연결 추적기를 추가할 수 없습니다.

프로시저

단계 **1** 상관관계 규칙 편집기에서 **Add Connection Tracker(**연결 추적기 추가**)**를 클릭합니다.

단계 **2** 추적할 연결을 지정합니다(연결 추적기 구문, 27 페이지 참조).

단계 **3** 추적한 연결을 바탕으로, 상관관계 이벤트를 생성할 시점을 지정합니다(연결 추적기 이벤트 구문, 30 페이지 참조).

단계 **4** 추적기의 조건을 달성해야 하는 간격(단위: 초, 분 또는 시간)을 지정합니다.

연결 추적기 구문

다음 표에서는 추적하고자 하는 연결의 종류를 지정하는 연결 추적기 조건을 작성하는 방법에 대해 설명합니다.

표 ***12:*** 연결 추적기 구문

다음을 지정할 경우...	연산자를 선택하고...
액세스 제어 정책	추적할 연결을 처리한 액세스 컨트롤 정책을 하나 이상 선택합니다.
액세스 제어 규칙 작업	추적할 연결을 로깅한 액세스 컨트롤 규칙과 관련된 액세스 컨트롤 규칙 작업을 하나 이상 선택합니다. 나중에 연결을 처리하는 기본 작업 또는 규칙과 상관없이, Monitor 규칙의 조건과 일치하는 연결을 추적하려면 **Monitor**를 선택합니다.
액세스 제어 규칙 이름	추적할 연결을 로깅한 액세스 컨트롤 규칙의 이름 전체 또는 일부를 입력합니다. Monitor 규칙과 일치하는 연결을 추적하려면 Monitor 규칙의 이름을 입력하십시오. 나중에 연결을 처리하는 기본 작업 또는 규칙과 상관없이 시스템은 연결을 추적합니다.
애플리케이션 프로토콜	애플리케이션 프로토콜을 하나 이상 선택합니다.
애플리케이션 프로토콜 카테고리	애플리케이션 프로토콜 카테고리를 하나 이상 선택합니다.
클라이언트	클라이언트를 하나 이상 선택합니다.
클라이언트 카테고리	클라이언트 카테고리를 하나 이상 선택합니다.
클라이언트 버전	클라이언트 버전을 입력합니다.
연결 지속시간	연결 이벤트 지속시간을 초 단위로 입력합니다.

다음을 지정할 경우...	연산자를 선택하고...
연결 유형	연결 이벤트를 획득한 방법에 따라 상관관계 규칙을 트리거할지 여부를 지정합니다. • 내보낸 NetFlow 기록에서 생성한 연결 이벤트에 대해 **is**와 **Netflow**를 선택합니다. • Firepower System 매니지드 디바이스가 탐지한 연결 이벤트에 대하 **is not**과 **Netflow**를 선택합니다.
Destination Country(목적지 국가) 또는 Source Country(소스 국가)	국가를 하나 이상 선택합니다.
디바이스	탐지된 연결을 추적하려는 디바이스를 하나 이상 선택합니다. NetFlow 연결을 추적하려면 내보낸 NetFlow 기록의 연결 데이터를 처리하는 디바이스를 선택합니다.
Ingress Interface(인그레스 인터페이스) 또는 Egress Interface(이그레스 인터페이스)	하나 이상의 인터페이스를 선택합니다.
Ingress Security Zone(인그레스 보안 영역) 또는 Egress Security Zone(이그레스 보안 영역)	보안 영역 또는 터널 영역을 하나 이상 선택합니다.
이니시에이터 IP, 응답자 IP 또는 이니시에이터/응답자 IP	단일 IP 주소 또는 주소 블록을 입력합니다.
이니시에이터 바이트, 응답자 바이트 또는 전체 바이트	다음 중 하나를 입력합니다. • 전송한 바이트 수(이니시에이터 바이트) • 수신한 바이트 수(응답자 바이트) • 전송 및 수신된 바이트 수(총 바이트)
이니시에이터 패킷, 응답자 패킷 또는 총 패킷	다음 중 하나를 입력합니다. • 전송한 패킷 수(이니시에이터 패킷) • 수신한 패킷 수(응답자 패킷) • 전송 및 수신된 패킷 수(총 패킷)
이니시에이터 포트/ICMP 유형 또는 응답자 포트/ICMP 코드	이니시에이터 트래픽의 포트 번호나 ICMP 유형 또는 응답자 트래픽의 포트 번호나 ICMP 코드를 입력합니다.
IOC 태그	침해 지표 태그가 **is** 또는 **is not**으로 설정되었는지를 선택합니다.
NETBIOS 이름	연결에서 모니터링된 호스트의 NetBIOS 이름을 입력합니다.

다음을 지정할 경우...	연산자를 선택하고...
NetFlow 디바이스	추적할 NetFlow 엑스포터의 IP 주소를 선택합니다. 네트워크 검색 정책에 어떤 NetFlow 엑스포터도 추가하지 않았다면, NetFlow Device(NetFlow 디바이스) 드롭다운 목록에는 아무것도 표시되지 않습니다.
사전 필터 정책	추적할 연결을 처리한 사전 필터 정책을 하나 이상 선택합니다.
이유	추적할 연결과 관련된 이유를 하나 이상 선택합니다.
보안 인텔리전스 범주	추적할 연결과 관련된 보안 인텔리전스 카테고리를 하나 이상 선택합니다.
TCP 플래그	추적을 위해 연결에 반드시 포함해야 하는 TCP 플래그를 선택합니다. 내보낸 NetFlow 기록에서 생성한 연결만 TCP 플래그 데이터를 가지고 있습니다.
전송 프로토콜	연결에 사용된 전송 프로토콜을 선택합니다.
URL	추적할 연결에서 방문한 URL 전체 또는 일부를 입력합니다.
URL 범주	추적할 연결에서 방문한 URL의 URL 카테고리를 하나 이상 선택합니다.
URL 평판	추적할 연결에서 방문한 URL의 URL 평판 값을 하나 이상 선택합니다.
사용자 이름	추적할 연결의 두 호스트 중 하나에 로그인한 사용자의 사용자 이름을 입력합니다.
웹 애플리케이션	웹 애플리케이션을 하나 이상 선택합니다.
웹 애플리케이션 카테고리	웹 애플리케이션 카테고리를 하나 이상 선택합니다.

이벤트 데이터를 사용하여 연결 추적기 구축

연결 추적기를 구성할 때는 상관관계 규칙의 기본 이벤트에서 제공하는 데이터를 자주 사용하게 됩니다.

예를 들어 시스템이 새 클라이언트를 탐지할 때 상관관계 규칙이 트리거된다고 가정해 봅시다. 이러한 유형의 상관관계 규칙에 연결 추적기를 추가하면, 시스템은 기본 이벤트를 참조하는 제약 조건으로 추적기를 자동으로 채웁니다.

- **Initiator/Responder IP(**이니시에이터/응답자 **IP)**는 **Event IP Address(**이벤트 **IP** 주소**)**로 설정됩니다.
- **Client(**클라이언트**)**는 **Event Client(**이벤트 클라이언트**)**로 설정됩니다.

팁 특정 IP 주소 또는 IP 주소 블록의 연결을 추적하려면 **switch to manual entry(**수동 입력으로 전환**)**를 클릭하여 IP를 수동으로 지정하십시오. 이벤트의 IP 주소를 사용하는 방식으로 돌아가려면 **switch to event fields(**이벤트 필드로 전환**)**를 클릭합니다.

관련 항목

연결 및 보안 관련 연결 이벤트 필드

Firepower System IP 주소 규칙

연결 추적기 이벤트 구문

다음 표에서는 추적 중인 연결을 기반으로 상관관계 이벤트를 생성하고자 하는 시기를 지정하는 연결 추적기 조건의 작성 방법에 대해 설명합니다.

표 ***13:*** 연결 추적기 이벤트 구문

다음을 지정할 경우...	연산자를 선택하고 다음을 입력합니다.
연결 수	탐지된 총 연결 수
SSL 암호화된 세션 수	탐지된 총 SSL 또는 TLS 암호화 세션의 수를 입력합니다.
총 바이트, 이니시에이터 바이트 또는 응답자 바이트	다음 중 하나에 해당합니다. • 전송한 총 바이트(총 바이트) • 전송한 바이트 수(이니시에이터 바이트) • 수신한 바이트 수(응답자 바이트)
총 패킷, 이니시에이터 패킷 또는 응답자 패킷	다음 중 하나에 해당합니다. • 전송한 총 패킷(총 패킷) • 전송한 패킷 수(이니시에이터 패킷) • 수신한 패킷 수(응답자 패킷)
고유 이니시에이터 또는 고유 응답자	다음 중 하나에 해당합니다. • 탐지된 세션을 시작한 고유한 호스트의 수(고유 이니시에이터) • 탐지된 연결에 응답한 고유한 호스트의 수(고유 응답자)

외부 호스트의 과도한 연결에 대한 샘플 구성

네트워크 10.1.0.0/16에 중요한 파일을 보관하며, 이 네트워크 외부의 호스트는 일반적으로 네트워크 내부의 호스트에 대해 연결을 시작하지 않는 시나리오를 고려해 보십시오. 네트워크 외부에서 더러 연결이 시작되었지만, 2분 내에 4개 이상의 연결이 시작되면 문제가 있는 것으로 판단했습니다.

다음 그림의 규칙에서는, 10.1.0.0/16 네트워크 외부에서 네트워크 내부로 연결이 시작될 때 시스템이 해당 조건을 충족하는 연결의 추적을 시작하는 것을 알 수 있습니다. 이제 시스템이 해당 서명과 일치하는 4개의 연결(원래 연결 포함)을 2분 내에 탐지할 경우 시스템은 상관관계 이벤트를 생성합니다.

Rule Information

Add User

Rule Name: Archive Connections - Outside

Rule Description: Trigger on 4 ouside connections tc

Rule Group: Ungrouped

Select the type of event for this rule

If: a connection event occurs | at either the beginning or the en | and it meets the following conditions:

Add condition | Add complex condition

OR

Initiator IP | is not in | 10.1.0.0/16

Responder IP | is in | 10.1.0.0/16

Connection Tracker

... start tracking connections that meet the following conditions:

Add condition | Add complex condition

AND

Initiator IP | is not in | 10.1.0.0/16

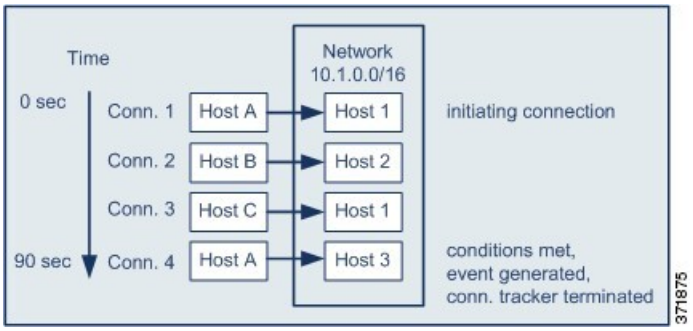
Responder IP | is in | 10.1.0.0/16

... and generate an event if:

Add condition | Add complex condition

total | Number of Connections | are greater than or equal to | 4

다음 다이어그램은 네트워크 트래픽이 위의 상관관계 규칙을 트리거하는 방법을 보여줍니다.



이 예에서 시스템은 상관관계 규칙의 기본 조건을 충족한 연결, 즉 10.1.0.0/16 네트워크 외부 호스트에서 네트워크 내부 호스트로의 연결을 탐지했습니다. 여기에서 연결 추적기가 생성됩니다.

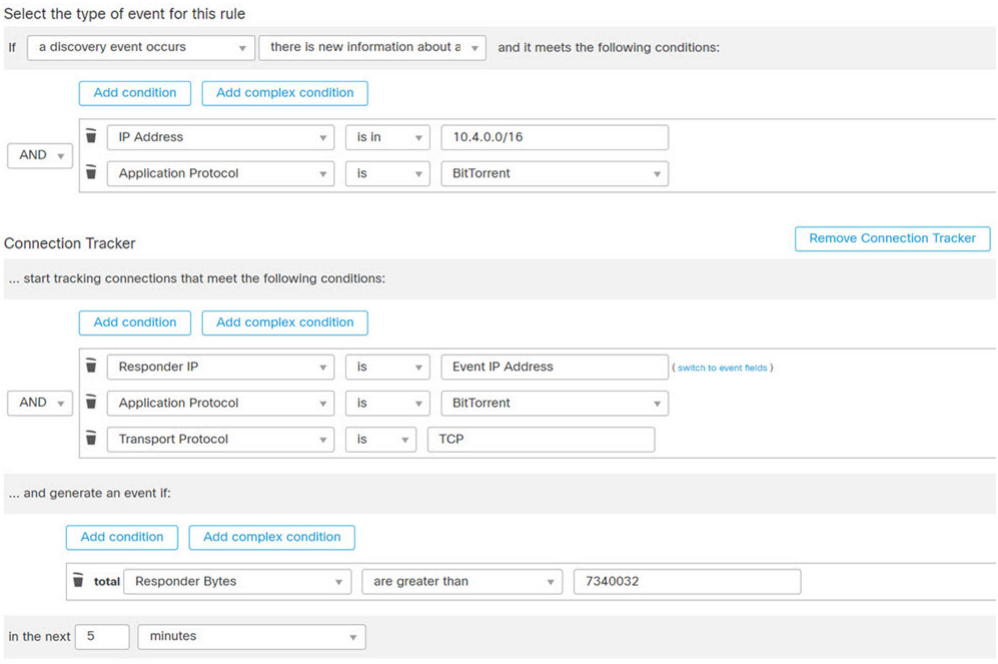
연결 추적기는 다음과 같이 처리됩니다.

- 먼저, 시스템은 네트워크 외부 Host A에서 네트워크 내부 Host 1로의 연결을 탐지하면 연결 추적을 시작합니다.
- 시스템은 연결 추적기 서명과 일치하는 연결을 2개 더 탐지합니다(Host B에서 Host 2, Host C에서 Host 1).
- 2분 시간 제한 내에 Host A가 Host 3에 연결되면 시스템은 4번째 해당 연결을 탐지하게 됩니다. 규칙 조건이 충족됩니다.
- 마지막으로, 시스템은 상관관계 이벤트를 생성하고 연결 추적을 중지합니다.

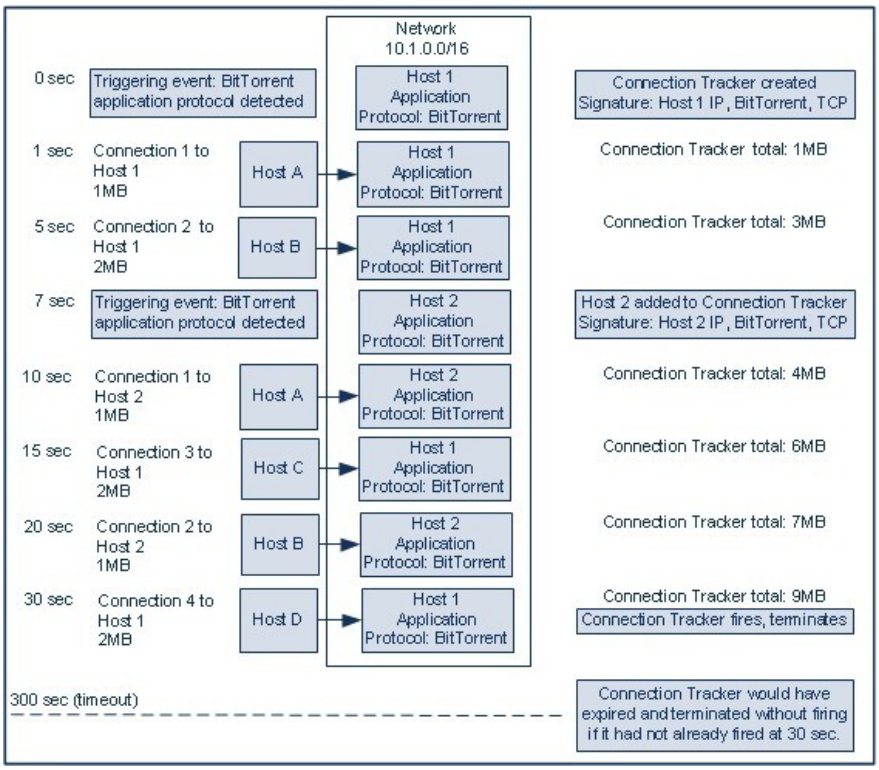
과도한 **BitTorrent** 데이터 전송에 대한 샘플 구성

모니터링되는 네트워크의 호스트에 대한 초기 연결 이후 시스템이 과도한 BitTorrent 데이터 전송을 탐지하는 경우 상관관계 이벤트를 생성하고자 하는 시나리오를 고려해보십시오.

다음 그림에서는 시스템이 모니터링되는 네트워크에서 BitTorrent 애플리케이션 프로토콜을 탐지할 때 트리거되는 상관관계 규칙을 보여줍니다. 이 규칙에는 모니터링되는 네트워크의 호스트(이 경우 10.1.0.0/16)가 초기 정책 위반 이후 5분 동안 BitTorrent를 통해 총 7MB(7340032바이트)가 넘는 데이터를 전송하는 경우 규칙이 트리거되도록 규칙을 제한하는 연결 추적기가 있습니다.



다음 다이어그램은 네트워크 트래픽이 위의 상관관계 규칙을 트리거하는 방법을 보여줍니다.



이 예에서 시스템은 두 호스트, 즉 Host 1과 Host 2에서 BitTorrent TCP 애플리케이션 프로토콜을 탐지했습니다. 이러한 두 호스트는 BitTorrent를 통해 4개의 다른 호스트(Host A, Host B, Host C, Host D)로 데이터를 전송합니다.

이 연결 추적기는 다음과 같이 처리됩니다.

- 먼저, 시스템은 Host 1에서 BitTorrent 애플리케이션 프로토콜을 탐지하면 0초 마커에서 연결 추적을 시작합니다. 시스템이 5분 내에(300초 마커까지) 7MB의 BitTorrent TCP 데이터가 전송되는 것을 탐지하지 못하면 연결 추적기가 만료됩니다.
- 5초에 Host 1이 서명과 일치하는 3MB의 데이터를 전송했습니다.
  - 1초 마커에 Host 1에서 Host A로 1MB(연결 추적기를 충족하기 위해 계산된 총 BitTorrent 트래픽 1MB)
  - 5초 마커에 Host 1에서 Host B로 2MB(총 3MB)
- 7초에 시스템은 Host 2에서 BitTorrent 애플리케이션 프로토콜을 탐지하고 해당 호스트에 대해서도 BitTorrent 연결 추적을 시작합니다.
- 20초에 시스템은 서명과 일치하는 추가 데이터가 Host 1과 Host2 모두에서 전송되는 것을 탐지했습니다.
  - 10초 마커에 Host 2에서 Host A로 1MB(총 4MB)
  - 15초 마커에 Host 1에서 Host C로 2MB(총 6MB)
  - 20초 마커에 Host 2에서 Host B로 1MB(총 7MB)

- Host 1과 Host 2에서 이제 총 7MB의 BitTorrent 데이터를 전송했지만, 전송된 총 바이트 수가 7MB(응답자 바이트가 **7340032** 초과**)**)보다 커야 하므로 규칙이 트리거되지 않습니다. 이 시점에 시스템이 추적기의 시간 초과 기간에 나머지 280초 동안 추가 BitTorrent 전송을 탐지하지 못하면, 추적기가 만료되고 시스템은 상관관계 이벤트를 생성하지 않습니다.
- 하지만 30초가 되면 시스템은 다른 BitTorrent 전송을 탐지하고, 규칙 조건이 충족됩니다.
  - 30초 마커에 Host 1에서 Host D로 2MB(총 9MB)
- 마지막으로, 시스템은 상관관계 이벤트를 생성합니다. 5분 기간이 만료되지 않았어도 시스템은 이 연결 추적기 인스턴스에 대한 연결 추적도 중지합니다. 이 시점에 BitTorrent TCP 애플리케이션 프로토콜을 사용하는 새 연결을 탐지하면 시스템은 새 연결 추적기를 생성합니다. 시스템은 세션이 끝날 때까지 연결 데이터를 집계하지 않으므로, Host 1이 총 2MB를 Host D로 전송한 후 상관관계 이벤트를 생성합니다.

스누즈 및 비활성 기간

상관관계 규칙에서 스누즈 기간을 구성할 수 있습니다. 상관관계 규칙이 트리거되면, 유휴 기간은 지정된 기간 동안(규칙 위반이 다시 발생해도) 규칙의 실행을 중지하도록 시스템에 지시합니다. 스누즈 기간이 경과하면 규칙을 다시 트리거할 수 있습니다(그리고 새 스누즈 기간을 시작할 수 있습니다).

예를 들면 트래픽을 생성해서는 안 되는 호스트가 네트워크에 있을지도 모릅니다. 시스템이 해당 호스트와 관련된 연결을 탐지할 때마다 트리거되는 간단한 상관관계 규칙은 호스트를 통과하는 네트워크 트래픽에 따라 짧은 기간에 여러 상관관계 이벤트를 생성할 수 있습니다. 정책 위반을 알리는 상관관계 이벤트의 수를 제한하려면 시스템이 해당 호스트와 관련하여 시스템이 탐지하는 첫 번째 연결(지정한 기간 내에)에 대해서만 상관관계 이벤트를 생성하도록 유휴 기간을 추가할 수 있습니다.

상관관계 규칙에서 비활성 시간도 설정할 수 있습니다. 비활성 기간 중에는 상관관계 규칙이 트리거되지 않습니다. 비활성 기간이 매일, 매주 또는 매월 반복되도록 설정할 수 있습니다. 예를 들어 호스트 운영체제 변경 사항을 찾기 위해 내부 네트워크에서 야간 Nmap 스캔을 수행할 수 있습니다. 이 경우 규칙이 잘못 트리거되지 않도록 스캔 시간 및 기간에 영향받는 상관관계 규칙에 대해 일일 비활성 기간을 설정할 수 있습니다.

상관관계 규칙 빌드 메커니즘

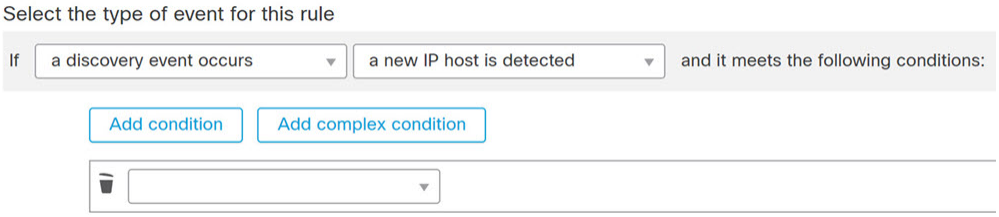
트리거 조건을 지정하여 상관관계 규칙을 작성합니다. 조건 내에서 사용할 수 있는 구문은 생성하는 요소에 따라 달라지지만, 그 원리는 동일합니다.

대부분의 조건은 카테고리, 연산자, 값이라는 3개 부분으로 구성됩니다.

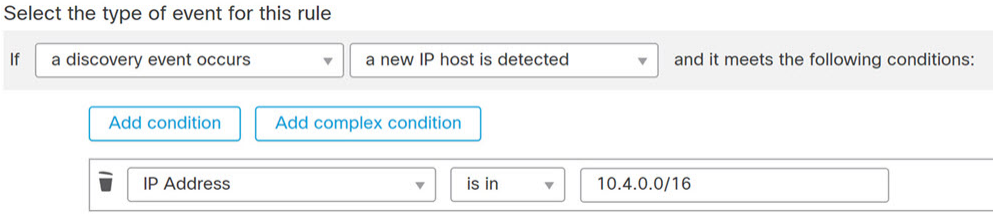
- 선택 가능한 카테고리는 상관관계 규칙 트리거, 호스트 프로파일 자격, 연결 추적기 또는 사용자 자격 중 어떤 것을 작성 중인지에 따라 달라집니다. 상관관계 규칙 트리거에서, 카테고리는 규칙에 대한 기본 이벤트 유형에 따라 달라집니다. 일부 조건은 여러 카테고리를 포함하는데, 각 카테고리마다 고유의 연산자와 값을 가질 수도 있습니다.
- 조건의 사용 가능한 연산자는 카테고리에 따라 달라집니다.

- 조건의 값을 지정하는 데 사용 가능한 구문은 카테고리와 연산자에 따라 달라집니다. 텍스트 필드에 직접 값을 입력해야 하는 경우도 있습니다. 그 외의 경우에는 드롭다운 목록에서 값(복수의 값 가능)을 선택할 수 있습니다.

예를 들어 새 호스트가 탐지될 때마다 상관관계 이벤트를 생성하려면, 어떤 조건도 없는 매우 단순한 규칙을 생성할 수 있습니다.



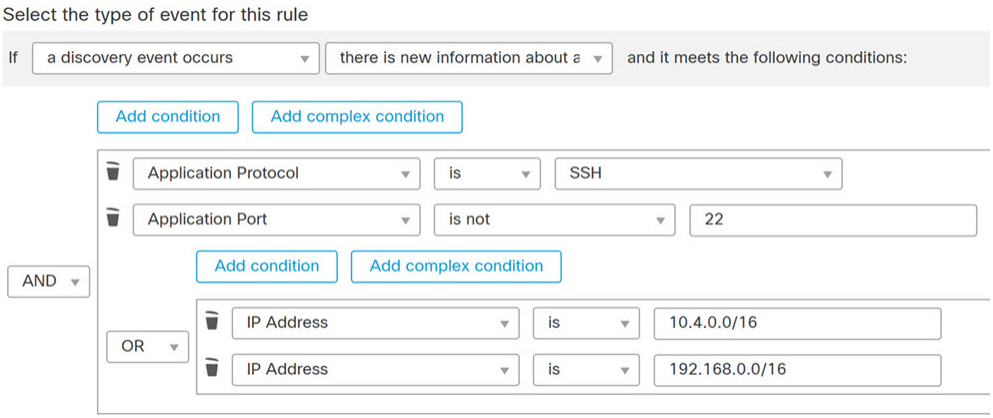
규칙을 더 제한하여 10.4.x.x 네트워크에서 새 호스트가 탐지되는 경우에만 이벤트를 생성하려는 경우 단일 조건을 추가할 수 있습니다.



여러 개의 조건을 포함할 경우 **AND** 또는 **OR** 연산자로 연결해야 합니다. 동일한 레벨의 조건은 함께 평가됩니다.

- **AND** 연산자를 사용하면 이 연산자가 제어하는 레벨의 모든 조건을 충족해야 합니다.
- **OR** 연산자를 사용하면 이 연산자가 제어하는 레벨의 조건 중 하나 이상을 충족해야 합니다.

10.4.x.x 네트워크 및 192.168.x.x 네트워크의 비표준 포트에서 SSH 활동을 탐지하는 다음 규칙에는 4개의 조건이 있으며, 그중 마지막 2개는 복합 조건입니다.



논리적으로, 이 규칙은 다음과 같이 평가됩니다.

```
(A and B and (C or D))
```

표 *14:* 규칙 평가

항목	조건의 내용
A	애플리케이션 프로토콜이 SSH임
B	애플리케이션 포트가 22가 아님
C	IP 주소는 10.0.0.0/8에 있음
D	IP 주소가 196.168.0.0/16에 있음

주의 자주 발생하는 이벤트에 대해 트리거되는 복잡한 상관관계 규칙을 평가하면 시스템 성능이 저하될 수 있습니다. 예를 들어 로깅된 모든 연결에 대해 시스템에서 반드시 평가해야 하는 다중 조건 규칙은 리소스 과부하를 일으킬 수 있습니다.

상관관계 규칙에 조건 추가 및 연결

프로시저

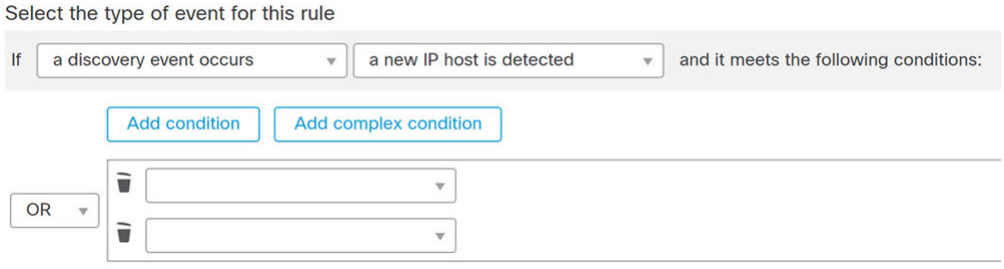
단계 **1** 상관관계 규칙 편집기에서 단순 또는 복합 조건을 추가합니다.

- 단순 - **Add condition(**조건 추가**)**을 클릭합니다.
- 복합 - **Add complex condition(**복합 조건 추가**)**을 클릭합니다.

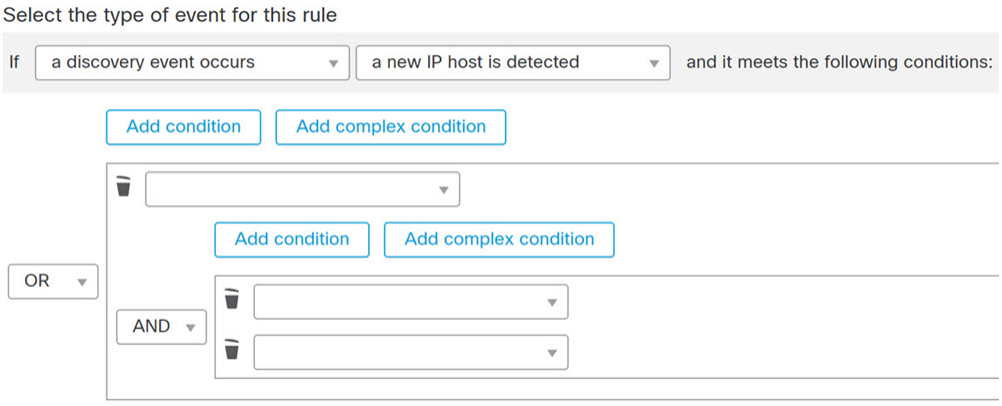
단계 **2** 조건 왼쪽에 있는 드롭다운 목록에서 **AND** 또는 **OR** 연산자를 선택해 조건을 연결합니다.

예**:** 단순 대 복합 조건

다음 그림은 두 가지 단순 조건이 **OR** 연산자로 결합된 상관관계 규칙을 보여줍니다.



다음 그림은 단순 조건 하나와 복합 조건 하나가 **OR** 연산자로 결합된 상관관계 규칙을 보여줍니다. 복합 조건은 **AND** 연산자로 결합된 단순 조건 2개로 구성됩니다.



상관관계 규칙 조건에 여러 값 사용

상관관계 조건을 작성할 때 조건 구문상 드롭다운 목록의 값 선택이 가능할 경우 대개는 목록에서 여러 값을 사용할 수 있습니다.

프로시저

단계 **1** 상관관계 규칙 편집기에서 조건을 작성하고, **is in** 또는 **is not in**을 연산자로 선택합니다.

단계 **2** 텍스트 필드의 아무 곳이나 클릭하거나 **Edit(**편집**)** 링크를 클릭합니다.

단계 **3** **Available(**사용 가능**)**에서 여러 값을 선택합니다. 클릭하고 드래그하여 인접한 여러 값을 선택할 수도 있습니다.

단계 **4** 오른쪽 화살표(>)를 클릭하여 선택한 항목을 **Selected**로 이동합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

상관관계 규칙 관리

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 상관관계 규칙 및 그룹을 표시하며, 이러한 정책은 편집할 수 있습니다. 상위 도메인의 선택된 상관관계 규칙 및 그룹도 표시되지만, 이러한 대상은 편집할 수는 없습니다. 하위 도메인에서 생성된 상관관계 규칙 및 그룹을 보고 편집하려면 해당 도메인으로 전환하십시오.

참고 상위 도메인의 컨피그레이션이 이름, 매니지드 디바이스 등 관련이 없는 도메인에 대한 정보를 표시하는 경우 상위 도메인의 컨피그레이션은 표시되지 않습니다.

활성 상관관계 정책의 규칙에 적용된 변경사항은 즉시 적용됩니다.

시작하기 전에

- 규칙을 삭제하려면 상관관계 정책 관리, 4 페이지에 설명된 대로 해당 규칙을 모든 상관관계 정책에서 삭제합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Correlation(**상관관계**)**을(를) 선택하고 **Rule Management(**규칙 관리**)**을 클릭합니다.

단계 **2** 규칙 관리:

- Create(생성) - **Create Rule(**규칙 생성**)**를 클릭합니다(상관관계 규칙 설정, 5 페이지 참조).
- Create Group(그룹 생성) - **Create Group(**그룹 생성**)**을 클릭하고, 그룹의 이름을 입력하고, **Save(**저장**)**를 클릭합니다. 그룹에 규칙을 추가하려면 규칙을 편집합니다.
- 편집 - **Edit(**수정**)** ( )을 클릭합니다. 상관관계 규칙 설정, 5 페이지의 내용을 참조하십시오. **View(**보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.
- Delete Rule or Rule Group(규칙 또는 규칙 그룹 삭제) - **Delete(**삭제**)** ( )을 클릭합니다. 규칙 그룹을 삭제하면 규칙의 그룹이 해제됩니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

상관관계 응답 그룹 설정

알림 및 교정의 상관관계 응답 그룹을 만든 다음, 해당 그룹을 활성화해 활성 상관관계 정책 내의 상관관계 규칙에 할당할 수 있습니다. 시스템은 네트워크 트래픽이 상관관계 규칙과 일치할 때 모든 그룹화된 응답을 실행합니다.

활성 상관관계 정책에서 사용하는 경우, 활성 그룹 또는 그룹화된 응답에 대한 변경사항은 즉시 적용됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **Correlation(**상관관계**)**을(를) 선택하고 **Groups(**그룹**)**를 클릭합니다.

단계 **2** **Create Group(**그룹 생성**)**을 클릭합니다.

단계 **3** **Name(**이름**)**을 입력합니다.

단계 **4** 생성 즉시 그룹을 활성화하려면 **Active(**활성**)** 확인란을 선택합니다.

비활성화된 그룹은 응답을 실행하지 않습니다.

단계 **5** 그룹에 대한 **Available Responses(**사용 가능한 응답**)**를 선택하고, 오른쪽 화살표(>)를 클릭해 응답을 **Responses in Group(**그룹 내 응답**)**으로 옮깁니다. 응답을 다른 방식으로 옮기려면 왼쪽 화살표(<)를 사용합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 생성과 동시에 활성화하지 않은 그룹을 지금 활성화하고 싶다면, 슬라이더를 클릭합니다.

관련 항목

Secure Firewall Management Center 알림 응답
교정 소개

상관관계 응답 그룹 관리

상관관계 정책에서 사용하지 않는 응답 그룹을 삭제할 수 있습니다. 응답 그룹을 삭제하면 관련 응답의 그룹이 해제됩니다. 응답 그룹을 삭제하지 않고 일시적으로 비활성화할 수도 있습니다. 이렇게 하면 그룹은 시스템에서 삭제되지 않지만 정책 위반 시 실행되지도 않습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 그룹을 표시하며 이러한 그룹은 수정할 수 있습니다. 상위 도메인에서 생성된 그룹도 표시되지만, 이러한 그룹은 수정할 수 없습니다. 하위 도메인에서 생성된 그룹을 보고 수정하려면 해당 도메인으로 전환하십시오.

사용 중인 활성 응답 그룹에 대한 변경사항은 즉시 적용됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **Correlation(**상관관계**)**을(를) 선택하고 **Groups(**그룹**)**를 클릭합니다.

단계 **2** 응답 그룹 관리:

- Activate(활성화) 또는 Deactivate(비활성화) - 슬라이더를 클릭합니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.
- Create(생성) - **Create Group(**그룹 생성**)**을 클릭합니다(상관관계 응답 그룹 설정, 38 페이지 참조).
- 편집 - **Edit(**수정**)** ( )을 클릭합니다. 상관관계 응답 그룹 설정, 38 페이지의 내용을 참조하십시오. **View(**보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.
- 삭제 - **Delete(**삭제**)** ( )을(를) 클릭합니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.