교정

다음 주제는 교정 설정 관련 정보를 제공합니다.

교정 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모두

사용자 역할

- 관리자
- 검색 관리자

교정 소개

교정은 Firepower System이 상관관계 위반에 대한 응답으로 실행하는 프로그램입니다.

교정을 실행하면, 시스템은 교정 상태 이벤트를 생성합니다. 교정 상태 이벤트는 교정 이름, 상관관계 정책 및 이를 트리거한 규칙, 종료 상태 메시지 등의 상세정보를 포함합니다.

시스템은 여러 교정 모듈을 지원합니다.

- Cisco ISE ANC(Adaptive Network Control) - 상관관계 정책 위반과 관련된 ISE 설정 ANC 정책을 적용하거나 지웁니다.
- Cisco IOS Null Route - 상관관계 정책 위반과 관련된 호스트 또는 네트워크로 전송된 트래픽을 차단(Cisco IOS 버전 12.0 이상 필수)
- Nmap Scanning(Nmap 스캐닝) - 호스트를 스캔해 실행 중인 운영체제와 서버 확인
- Set Attribute Value(속성 값 설정) - 상관관계 정책 위반과 관련된 호스트에서 호스트 속성 설정

팁 다른 작업을 수행하는 맞춤형 모듈을 설치할 수 있습니다(*Firepower System Remediation API* 설명서 참조).

교정 구현

교정을 구현하려면, 먼저 선택한 모듈에 대한 인스턴스를 하나 이상 만들어야 합니다. 모듈당 여러 인스턴스를 만들 수 있으며, 이때 각 인스턴스는 저마다 다르게 설정됩니다. 예를 들어 Cisco IOS Null Route 교정 모듈을 사용하여 여러 라우터와 통신하려면, 해당 모듈이 인스턴스 다수를 설정해야 합니다.

그런 다음 정책 위반 시 수행할 작업을 설명하는 여러 교정을 각 인스턴스에 추가합니다.

마지막으로, 교정을 상관관계 정책에 있는 규칙과 연결해 시스템이 상관관계 정책 위반에 대한 응답으로 교정을 실행하게 합니다.

교정 및 멀티 테넌시

다중 도메인 구축의 경우에는, 어떤 도메인 레벨에서도 맞춤형 교정 모듈을 설치할 수 있습니다. 시스템 제공 모듈은 Global(전역) 도메인에 속합니다.

상위 도메인에서 생성한 인스턴스에는 교정을 추가할 수 없지만, 비슷하게 설정한 인스턴스를 현재 도메인에 생성하고 해당 인스턴스에 교정을 추가할 수는 있습니다. 상위 도메인에서 생성한 교정을 상관관계 응답으로 사용할 수도 있습니다.

관련 항목

Secure Firewall Management Center 알림 응답
Nmap 스캐닝
규칙 및 허용 리스트에 응답 추가

Cisco ISE EPS 교정

ISE 구축에서 EPS(Endpoint Protection Service)를 활성화하고 설정하면, ISE를 사용하여 교정을 실행하도록 management center을(를) 설정할 수 있습니다. 완벽하게 구성되면, ISE EPS 교정은 상관관계 정책 위반과 관련된 소스 또는 목적지 호스트에서 다음 **Mitigation Actions(**완화 작업**)**을 실행합니다.

- **`quarantine`(**격리**)** - 엔드포인트의 네트워크 액세스를 제한 또는 거부

- **unquarantine(**격리 해제**)** - 엔드포인트의 격리 상태를 역전하고 네트워크에 대한 모든 액세스를 허가
- **shutdown(**종료**)** - 엔드포인트의 NAS(network attached system) 포트를 비활성화해 네트워크에서 분리

또한 특정 IP 주소를 ISE EPS 교정에서 제외할 수 있습니다.

참고 ISE 버전 및 구성은 ISE를 사용할 수 있는 방법에 영향을 미칩니다. 예를 들어 ISE-PIC를 사용하여 ISE EPS 교정을 수행할 수는 없습니다. 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *ISE/ISE-PIC*를 이용한 사용자 제어 장을 참고하십시오.

ISE EPS 작업에 대한 자세한 내용은 *Cisco Identity Services Engine* 사용자 설명서를 참조하십시오.

ISE EPS 교정 설정

소스 또는 목적지 호스트에서 ISE EPS 교정을 실행하여 상관관계 정책 위반에 응답할 수 있습니다.

참고 ISE-PIC는 ISE EPS 치료를 수행할 수 없습니다.

시작하기 전에

- ISE 서버에서 EPS 작업을 설정합니다.
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 ISE/PIC 구성에 대한 장을 참조하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.
단계 **2** ISE EPS 인스턴스 추가, 3 페이지에 설명된 대로 pxGrid 완화 인스턴스를 추가합니다.
단계 **3** ISE EPS 교정 추가, 4 페이지에 설명된 대로 ISE EPS 교정을 하나 이상 추가합니다.

다음에 수행할 작업

- 규칙 및 허용 리스트에 응답 추가에 설명된 대로 상관관계 정책 위반에 대한 응답으로 교정을 할당합니다.

ISE EPS 인스턴스 추가

ISE EPS 인스턴스를 생성해 개별 교정을 유형별로 그룹화합니다.

프로시저

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

단계 **2** **Add a New Instance(**새 인스턴스 추가**)** 목록에서 **pxGrid Mitigation(v1.0)**을 모듈 유형으로 선택하고 **Add(**추가**)**를 클릭합니다.

단계 **3** **Instance Name(**인스턴스 이름**)**과 **Description(**설명**)**을 입력합니다.

단계 **4** **Enable Logging(**기록 활성화**)** 옵션을 설정해 시스템 기록을 활성화 또는 비활성화합니다.

단계 **5** **Create(**생성**)**를 클릭합니다.

다음에 수행할 작업

- 속성값 설정 교정 추가, 11 페이지에 설명된 대로 ISE EPS 교정을 생성합니다.

관련 항목

Firepower System IP 주소 규칙

ISE EPS 교정 추가

인스턴스에서 ISE EPS 교정을 하나 이상 생성해 상관관계 정책 위반과 관련된 소스 또는 목적지 호스트에서 다음 **Mitigation Actions(**완화 작업**)**을 실행합니다.

다중 도메인 구축에서는 상위 도메인에서 생성된 인스턴스에 치료를 추가할 수 없습니다.

시작하기 전에

- ISE EPS 인스턴스 추가, 3 페이지에 설명된 대로 ISE EPS 인스턴스를 생성합니다.

프로시저

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

단계 **2** 교정을 추가하려는 인스턴스 옆에 있는 **View(**보기**)** ( )를 클릭합니다.

단계 **3** **Configured Remediations(**설정한 교정**)** 섹션에서 **Mitigate Destination(**목적지 완화**)** 또는 **Mitigate Source(**소스 완화**)**를 선택하고 **Add(**추가**)**를 클릭합니다.

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

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

단계 **5** **Mitigation Action(**완화 작업**)**: **`quarantine`(**격리**)**, **`unquarantine`(**격리 해제**)** 또는 **`shutdown`(**종료**)** 을 선택합니다.

단계 **6** (선택 사항) 교정에서 IP 주소 또는 범위를 제외하려면 **Allow List(**허용 목록**)** 상자에 입력합니다.

단계 **7** **Create(**생성**)**를 클릭하고 **Done(**완료**)**을 클릭합니다.

다음에 수행할 작업

- 상관관계 정책 위반에 대한 응답으로 치료를 할당합니다. 규칙 및 허용 리스트에 응답 추가를 참조하십시오.

Cisco IOS Null Route 교정

Cisco IOS Null Route 교정 모듈을 이용하면 Cisco의 "null route" 명령을 사용하여 IP 주소 또는 주소 범위를 차단할 수 있습니다. 이렇게 하면 라우터의 NULL 인터페이스로 라우팅하여 호스트나 네트워크에 전송한 모든 트래픽이 삭제됩니다. 위반 호스트 또는 네트워크에서 전송된 트래픽은 차단되지 않습니다.

참고 검색 또는 호스트 입력 이벤트를 기반으로 하는 상관관계 규칙에 대한 응답으로 목적지 기반 교정을 사용하지는 마십시오. 이러한 이벤트는 소스 호스트와 연결됩니다.

주의 Cisco IOS 교정이 활성화되는 경우에는 시간 초과 기간이 없습니다. IP 주소 또는 네트워크를 차단 해제하려면, 라우팅 변경사항을 라우터에서 수동으로 삭제해야 합니다.

Cisco IOS 라우터에 대한 교정 설정

참고 검색 또는 호스트 입력 이벤트를 기반으로 하는 상관관계 규칙에 대한 응답으로 목적지 기반 교정을 사용하지는 마십시오. 이러한 이벤트는 소스 호스트와 연결됩니다.

주의 Cisco IOS 교정이 활성화되는 경우에는 시간 초과 기간이 없습니다. IP 주소 또는 네트워크를 차단 해제하려면, 라우팅 변경사항을 라우터에서 수동으로 삭제해야 합니다.

시작하기 전에

- Cisco 라우터가 Cisco IOS 12.0 이상을 실행 중인지 확인합니다.
- 라우터에 대한 레벨 15 관리 액세스가 있는지 확인합니다.

프로시저

단계 **1** Cisco 라우터 또는 IOS 소프트웨어와 함께 제공된 문서에 설명된 대로 Cisco 라우터에서 텔넷을 활성화합니다.

단계 **2** management center에서, 사용할 각 Cisco IOS 라우터에 대해 Cisco IOS Null Route 인스턴스를 추가합니다(Cisco IOS 인스턴스 추가, 6 페이지 참조).

단계 **3** 상관관계 정책이 위반될 때 라우터에서 이끌어낼 응답의 유형을 기반으로 각 인스턴스에 대한 교정을 생성합니다.

- Cisco IOS Block Destination 교정 추가, 7 페이지
- Cisco IOS Block Destination Network 교정 추가, 8 페이지
- Cisco IOS Block Source 교정 추가, 9 페이지
- Cisco IOS Block Source Network 교정 추가, 9 페이지

다음에 수행할 작업

- 상관관계 정책 위반에 대한 응답으로 치료를 할당합니다. 규칙 및 허용 리스트에 응답 추가를 참조하십시오.

Cisco IOS 인스턴스 추가

여러 라우터로 교정을 전송하려는 경우 각 라우터에 대해 개별 인스턴스를 생성합니다.

시작하기 전에

- Cisco 라우터 또는 IOS 소프트웨어와 함께 제공된 문서에 설명된 대로 Cisco 라우터에서 텔넷 액세스를 설정합니다.

프로시저

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

단계 **2** **Add a New Instance(**새 인스턴스 추가**)** 목록에서 **Cisco IOS Null Route**를 선택하고 **Add(**추가**)**를 클릭합니다.

단계 **3** **Instance Name(**인스턴스 이름**)**과 **Description(**설명**)**을 입력합니다.

단계 **4** 교정에 대해 사용하려는 Cisco IOS 라우터의 IP 주소를 **Router IP** 필드에 입력합니다.

단계 **5** 라우터에 대한 텔넷 사용자 이름을 **Username(**사용자 이름**)** 필드에 입력합니다. 이 사용자는 라우터에 대한 레벨 15 관리 액세스 권한이 있어야 합니다.

단계 **6** 텔넷 사용자의 사용자 비밀번호를 **Connection Password(**연결 비밀번호**)** 필드에 입력합니다.

단계 **7** 텔넷 사용자의 활성 비밀번호를 **Enable Password(**비밀번호 활성화**)** 필드에 입력합니다. 이 비밀번호는 라우터의 특권 모드로 들어가기 위해 사용되는 비밀번호입니다.

단계 **8** 교정에서 제외할 IP 주소 또는 범위를 한 줄에 하나씩 **Allow List(**허용 목록**)** 필드에 입력합니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

단계 **9** **Create(**생성**)**를 클릭합니다.

다음에 수행할 작업

- Cisco IOS Block Destination 교정 추가, 7 페이지, Cisco IOS Block Destination Network 교정 추가, 8 페이지, Cisco IOS Block Source 교정 추가, 9 페이지, Cisco IOS Block Source Network 교정 추가, 9 페이지에 설명된 대로 상관관계 정책이 사용할 특정 교정을 추가합니다.

관련 항목

Firepower System IP 주소 규칙

Cisco IOS Block Destination 교정 추가

Cisco IOS Block Destination 교정은 라우터에서 상관관계 정책 위반과 관련된 목적지 호스트로 전송된 트래픽을 차단합니다. 검색 또는 호스트 입력 이벤트를 기반으로 하는 상관관계 규칙에 대한 응답으로 목적지 기반 교정을 사용하지는 마십시오. 이러한 이벤트는 소스 호스트와 연결됩니다.

다중 도메인 구축에서는 상위 도메인에서 생성된 인스턴스에 치료를 추가할 수 없습니다.

시작하기 전에

- Cisco IOS 인스턴스 추가, 6 페이지의 설명대로 Cisco IOS 인터페이스를 추가합니다.

프로시저

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

단계 **2** 교정을 추가하려는 인스턴스 옆에 있는 **View(**보기**)** ( )를 클릭합니다.

단계 **3** **Configured Remediations(**설정한 교정**)** 섹션에서 **Block Destination(**목적지 차단**)**을 선택하고 **Add(**추가**)**를 클릭합니다.

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

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

단계 **5** **Create(**생성**)**를 클릭하고 **Done(**완료**)**을 클릭합니다.

다음에 수행할 작업

- 상관관계 정책 위반에 대한 응답으로 치료를 할당합니다. 규칙 및 허용 리스트에 응답 추가를 참조하십시오.

Cisco IOS Block Destination Network 교정 추가

Cisco IOS Block Destination Network 교정은 라우터에서 상관관계 정책 위반과 관련된 목적지 호스트의 네트워크로 전송된 트래픽을 차단합니다. 검색 또는 호스트 입력 이벤트를 기반으로 하는 상관관계 규칙에 대한 응답으로 목적지 기반 교정을 사용하지는 마십시오. 이러한 이벤트는 소스 호스트와 연결됩니다.

다중 도메인 구축에서는 상위 도메인에서 생성된 인스턴스에 치료를 추가할 수 없습니다.

시작하기 전에

- Cisco IOS 인스턴스 추가, 6 페이지의 설명대로 Cisco IOS 인터페이스를 추가합니다.

프로시저

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

단계 **2** 교정을 추가하려는 인스턴스 옆에 있는 **View(**보기**)** ( )를 클릭합니다.

단계 **3** **Configured Remediations(**설정한 교정**)** 섹션에서 **Block Destination Network(**목적지 네트워크 차단**)**를 선택하고 **Add(**추가**)**를 클릭합니다.

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

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

단계 **5** **Netmask(**넷마스크**)** 필드에 서브넷 마스크를 입력하거나 CIDR 표기법을 사용하여 트래픽을 차단할 네트워크를 설명합니다.

예를 들어 단일 호스트가 규칙을 트리거했을 때 전체 Class C 네트워크에 대한 트래픽을 차단하려면 (권장 사항이 아님) 넷마스크로 `255.255.255.0` 또는 `24`를 사용합니다.

또 다른 예로, 트리거하는 IP 주소를 포함하는 30개 주소에 대한 트래픽을 차단하려면 넷마스크로 `255.255.255.224` 또는 `27`을 지정합니다. 이 경우 IP 주소 `10.1.1.15`가 교정을 트리거하면 `10.1.1.1`과 `10.1.1.30` 사이의 모든 IP 주소가 차단됩니다. 트리거하는 IP 주소만 차단하려면 필드를 비워두거나, `32`를 입력하거나, `255.255.255.255`를 입력합니다.

단계 **6** **Create(**생성**)**를 클릭하고 **Done(**완료**)**을 클릭합니다.

다음에 수행할 작업

- 상관관계 정책 위반에 대한 응답으로 치료를 할당합니다. 규칙 및 허용 리스트에 응답 추가를 참조하십시오.

관련 항목

Firepower System IP 주소 규칙

Cisco IOS Block Source 교정 추가

Cisco IOS Block Source 교정은 라우터에서 상관관계 정책 위반과 관련된 소스 호스트로 전송된 트래픽을 차단합니다.

다중 도메인 구축에서는 상위 도메인에서 생성된 인스턴스에 치료를 추가할 수 없습니다.

시작하기 전에

- Cisco IOS 인스턴스 추가, 6 페이지의 설명대로 Cisco IOS 인터페이스를 추가합니다.

프로시저

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

단계 **2** 교정을 추가하려는 인스턴스 옆에 있는 **View(**보기**)** ( )를 클릭합니다.

단계 **3** **Configured Remediations(**설정한 교정**)** 섹션에서 **Block Source(**소스 차단**)**을 선택하고 **Add(**추가**)**를 클릭합니다.

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

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

단계 **5** **Create(**생성**)**를 클릭하고 **Done(**완료**)**을 클릭합니다.

다음에 수행할 작업

- 상관관계 정책 위반에 대한 응답으로 치료를 할당합니다. 규칙 및 허용 리스트에 응답 추가를 참조하십시오.

Cisco IOS Block Source Network 교정 추가

Cisco IOS Block Source Network 교정은 라우터에서 상관관계 정책 위반과 관련된 소스 호스트의 네트워크로 전송된 트래픽을 차단합니다.

다중 도메인 구축에서는 상위 도메인에서 생성된 인스턴스에 치료를 추가할 수 없습니다.

시작하기 전에

- Cisco IOS 인스턴스 추가, 6 페이지의 설명대로 Cisco IOS 인터페이스를 추가합니다.

프로시저

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

단계 **2** 교정을 추가하려는 인스턴스 옆에 있는 **View(**보기**)** ( )를 클릭합니다.

단계 **3** **Configured Remediations(**설정한 교정**)** 섹션에서 **Block Source Network(**소스 네트워크 차단**)**을 선택하고 **Add(**추가**)**를 클릭합니다.

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

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

단계 **5** **Netmask(**넷마스크**)** 필드에 서브넷 마스크를 입력하거나 트래픽을 차단할 네트워크를 설명하는 CIDR 표기법을 입력합니다.

예를 들어 단일 호스트가 규칙을 트리거했을 때 전체 Class C 네트워크에 대한 트래픽을 차단하려면 (권장 사항이 아님) 넷마스크로 `255.255.255.0` 또는 `24`를 사용합니다.

또 다른 예로, 트리거하는 IP 주소를 포함하는 30개 주소에 대한 트래픽을 차단하려면 넷마스크로 `255.255.255.224` 또는 `27`을 지정합니다. 이 경우 IP 주소 `10.1.1.15`가 교정을 트리거하면 `10.1.1.1`과 `10.1.1.30` 사이의 모든 IP 주소가 차단됩니다. 트리거하는 IP 주소만 차단하려면 필드를 비워두거나, `32`를 입력하거나, `255.255.255.255`를 입력합니다.

단계 **6** **Create(**생성**)**를 클릭하고 **Done(**완료**)**을 클릭합니다.

다음에 수행할 작업

- 상관관계 정책 위반에 대한 응답으로 치료를 할당합니다. 규칙 및 허용 리스트에 응답 추가를 참조하십시오.

관련 항목

Firepower System IP 주소 규칙

Nmap 스캔 교정

Firepower System은 네트워크 탐색 및 보안 감사를 위한 오픈 소스 활성 스캐너인 Nmap™과 통합됩니다. Nmap 교정을 사용하여 상관관계 정책 위반에 응답할 수 있으며, 이 경우 Nmap 스캔 교정이 트리거됩니다.

Nmap 스캔에 대한 자세한 정보는 Nmap 스캐닝 섹션을 참조하십시오.

속성 값 교정 설정

트리거링 이벤트가 발생한 호스트에서 호스트 속성 값을 설정하여 상관관계 정책 위반에 응답할 수 있습니다. 텍스트 호스트 속성의 경우에는 이벤트의 설명을 속성 값으로 사용할 수 있습니다.

세트 속성값 교정 구성

프로시저

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

단계 **2** 속성값 설정 인스턴스 추가, 11 페이지에 설명된 대로 세트 속성 인스턴스를 생성합니다.

단계 **3** 속성값 설정 교정 추가, 11 페이지에 설명된 대로 세트 속성 교정을 추가합니다.

다음에 수행할 작업

- 상관관계 정책 위반에 대한 응답으로 치료를 할당합니다. 규칙 및 허용 리스트에 응답 추가를 참조하십시오.

관련 항목

사전 정의된 호스트 속성
사용자 정의 호스트 속성

속성값 설정 인스턴스 추가

프로시저

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

단계 **2** **Add a New Instance(**새 인스턴스 추가**)** 목록에서 **Set Attribute Value(**속성 값 설정**)**를 선택하고 **Add(**추가**)**를 클릭합니다.

단계 **3** **Instance Name(**인스턴스 이름**)**과 **Description(**설명**)**을 입력합니다.

단계 **4** **Create(**생성**)**를 클릭합니다.

다음에 수행할 작업

- 속성값 설정 교정 추가, 11 페이지에 설명된 대로 속성 설정 교정을 생성합니다.

속성값 설정 교정 추가

Set Attribute Value(속성 값 설정) 교정은 상관관계 정책 위반과 관련된 호스트에서 호스트 속성을 설정합니다. 설정할 각 속성값에 대한 교정을 생성합니다. 텍스트 속성의 경우에는 트리거링 이벤트의 설명을 속성 값으로 사용할 수 있습니다.

다중 도메인 구축에서는 상위 도메인에서 생성된 인스턴스에 치료를 추가할 수 없습니다.

시작하기 전에

- 속성값 설정 인스턴스 추가, 11 페이지에 설명된 대로 세트 속성 인스턴스를 생성합니다.

프로시저

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

단계 **2** 교정을 추가하려는 인스턴스 옆에 있는 **View(**보기**)** ( )를 클릭합니다.

단계 **3** **Configured Remediations(**설정한 교정**)** 섹션에서 **Set Attribute Value(**속성값 설정**)**를 선택하고 **Add(**추가**)**를 클릭합니다.

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

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

단계 **5** 소스 및 목적지 데이터가 있는 이벤트에 대한 응답으로 이 교정을 사용하려면, **Update Which Host(s) From Event(**이벤트의 호스트 업데이트**)** 옵션을 선택합니다.

단계 **6** 텍스트 속성의 경우에는 **Use Description From Event For Attribute Value(**속성값으로 이벤트의 설명 사용**)** 여부를 지정합니다.

- 이벤트의 설명을 속성값으로 사용하려면 **On(**설정**)**을 클릭하고 설정할 **Attribute Value(**속성값**)**를 입력합니다.
- 교정에 대한 **Attribute Value(**속성값**)** 설정을 속성값으로 사용하려면 **Off(**해제**)**를 선택합니다.

단계 **7** **Create(**생성**)**를 클릭하고 **Done(**완료**)**을 클릭합니다.

다음에 수행할 작업

- 상관관계 정책 위반에 대한 응답으로 치료를 할당합니다. 규칙 및 허용 리스트에 응답 추가를 참조하십시오.

교정 모듈 관리

다중 도메인 구축의 경우 시스템은 현재 도메인에 설치된 Nmap 교정 모듈을 표시하며, 이러한 모듈은 삭제할 수 있습니다. 상위 도메인에 설치된 모듈도 표시되지만, 이러한 모듈은 수정할 수 없습니다. 하위 도메인의 교정 모듈을 관리하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Modules(**모듈**)**을(를) 선택합니다.

단계 **2** 교정 모듈 관리:

- Configure(설정) - 모듈에 대한 Module Detail(모듈 상세정보) 페이지를 확인하고 모듈의 인스턴스와 교정을 설정하려면, **View(**보기**)** ( )을 클릭합니다. 다중 도메인 구축의 경우에는 Module Detail(모듈 상세정보) 페이지를 사용하여 상위 도메인에 설치된 모듈의 현재 도메인에 있는 인

스턴스를 추가, 삭제 또는 편집할 수 없습니다. 대신 Instances(인스턴스) 페이지(**Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**)를 사용하십시오(교정 인스턴스 관리, 13 페이지 참조).

- Delete(삭제) - 사용하지 않은 맞춤형 모듈을 삭제하려면 **Delete(**삭제**)** ( )을 클릭합니다. 시스템 제공 모듈은 삭제할 수 없습니다.
- Install(설치) - 맞춤형 모듈을 설치하려면 **Choose File(**파일 선택**)**을 클릭하고, 모듈을 찾은 다음 **Install(**설치**)**을 클릭합니다. 자세한 내용은 *Firepower System Remediation API* 설명서를 참조하십시오.

교정 인스턴스 관리

Instances(인스턴스) 페이지는 모든 교정 모듈을 대상으로, 설정된 인스턴스를 모두 열거합니다.

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

상위 도메인에서 생성한 인스턴스에는 교정을 추가할 수 없지만, 비슷하게 설정한 인스턴스를 현재 도메인에 생성하고 해당 인스턴스에 교정을 추가할 수는 있습니다. 상위 도메인에서 생성한 교정을 상관관계 응답으로 사용할 수도 있습니다.

프로시저

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

단계 **2** 교정 인스턴스 관리:

- Add(추가) - 인스턴스를 추가하려면 인스턴스를 추가할 교정 모듈을 선택하고 **Add(**추가**)**를 클릭합니다. 시스템 제공 모듈의 경우에는 다음을 참조하십시오.
  - ISE EPS 인스턴스 추가, 3 페이지
  - Cisco IOS 인스턴스 추가, 6 페이지
  - Cisco Secure Firewall Management Center 디바이스 구성 가이드
  - 속성값 설정 인스턴스 추가, 11 페이지

  맞춤형 모듈 추가 관련 도움이 필요하다면 해당 모듈의 설명서(존재하는 경우)를 참조하십시오.
- Configure(구성) - 인스턴스 상세정보를 구성하고 교정을 인스턴스에 추가하려면 **View(**보기**)** ( )를 클릭합니다.
- Delete(삭제) - 사용하지 않는 인스턴스를 삭제하려면 **Delete(**삭제**)** ( )를 클릭합니다.

단일 교정 모듈 인스턴스 관리

Module Detail(모듈 상세정보) 페이지는 특정 교정 모듈에 대해 설정된 인스턴스와 교정을 모두 표시합니다.

다중 도메인 구축의 경우에는, 현재 도메인과 상위 도메인에 설치된 교정 모듈에 대한 Module Detail(모듈 상세정보) 페이지에 액세스할 수 있습니다. 그러나 Module Detail(모듈 상세정보) 페이지를 사용하여 상위 도메인에 설치된 모듈의 현재 도메인에 있는 인스턴스를 추가, 삭제 또는 편집할 수는 없습니다. 대신 Instances(인스턴스) 페이지(**Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**)를 사용하십시오(교정 인스턴스 관리, 13 페이지 참조).

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Modules(**모듈**)**을(를) 선택합니다.

단계 **2** 관리할 인스턴스가 있는 교정 모듈 옆에 있는 **View(**보기**)** ( )를 클릭합니다.

단계 **3** 교정 인스턴스 관리:

- Add(추가) - 인스턴스를 추가하려면 **Add(**추가**)**를 클릭합니다. 시스템 제공 모듈의 경우에는 다음을 참조하십시오.
  - ISE EPS 인스턴스 추가, 3 페이지
  - Cisco IOS 인스턴스 추가, 6 페이지
  - Cisco Secure Firewall Management Center 디바이스 구성 가이드
  - 속성값 설정 인스턴스 추가, 11 페이지

  맞춤형 모듈을 위한 인스턴스 추가 관련 도움이 필요하다면 해당 모듈의 설명서(존재하는 경우)를 참조하십시오.
- Configure(구성) - 인스턴스 상세정보를 구성하고 교정을 인스턴스에 추가하려면 **View(**보기**)** ( )를 클릭합니다.
- Delete(삭제) - 사용하지 않는 인스턴스를 삭제하려면 **Delete(**삭제**)** ( )를 클릭합니다.