이벤트 검색

다음 주제에서는 워크플로내의 이벤트를 검색하는 방법을 설명합니다.

이벤트 검색

Firepower System은 데이터베이스 테이블에 이벤트로 저장되는 정보를 생성합니다. 이벤트에는 어플라이언스가 이벤트를 생성하도록 만든 활동을 설명하는 여러 필드가 포함되어 있습니다. 다양한 이벤트 유형에 대해 환경에 맞춤 설정된 검색을 생성하고 나중에 다시 사용할 수 있도록 저장할 수 있습니다.

검색을 저장할 때 이름을 지정하고 검색을 사용자만 사용할 수 있는지 어플라이언스의 모든 사용자가 사용할 수 있는지 지정합니다. 맞춤형 사용자 역할을 위한 데이터 제한으로 검색을 사용하려면 반드시 비공개 검색으로 저장해야 합니다. 전에 검색을 저장한 경우, 이를 로드하여 필요한 수정을 한 다음 검색을 시작할 수 있습니다. 맞춤형 분석 대시보드 위젯, 보고서 템플릿, 사용자 지정 사용자 역할도 저장된 검색을 사용할 수 있습니다. 저장한 검색은 Search(검색) 페이지에서 삭제할 수 있습니다.

일부 이벤트 유형의 경우, Firepower System은 예제 역할을 하고 네트워크에 대한 중요한 정보에 빠르게 액세스하도록 도와주는 사전 정의된 검색을 제공합니다. 네트워크 환경에 대해 사전 정의된 검색 내에서 필드를 수정한 다음 나중에 다시 사용하기 위해 저장할 수 있습니다.

사용할 수 있는 검색 기준은 검색 유형에 따라 다를 수 있지만 원리는 동일합니다. 검색은 모든 필드에 지정된 검색 기준에 일치하는 레코드만 반환합니다.

참고 맞춤형 테이블을 검색하려면 약간 다른 절차가 필요합니다.

관련 항목

맞춤형 테이블 검색

검색 제약 조건

각 데이터베이스 테이블에는 테이블에 대해 정의된 필드에 적용할 검색 제약 조건 값을 입력할 수 있는, 자체 검색 페이지가 있습니다. 필드 유형에 따라 와일드필드 문자 또는 숫자 값 범위 같은 특수 구문을 사용해 기준을 지정할 수 있습니다.

검색 결과는 열 레이아웃의 각 테이블 필드를 표시하는 워크플로 페이지에 표시됩니다. 워크플로 페이지에 열로 표시되지 않는 필드를 이용해 일부 데이터베이스 테이블을 추가로 검색할 수도 있습니다. 워크플로 페이지 상의 결과를 볼 때 검색 결과에 적용되는 제약을 확인하려면, 확장 화살표(▸)을 클릭하여 활성 검색 제약을 확인합니다.

일반 검색 제약 조건

이벤트를 검색하는 경우 다음 일반 지침을 따르십시오.

- 대부분의 필드에는 부분 일치 검색에 와일드 카드가 필요합니다. 모든 필드에서 이러한 검색에 와일드 카드를 사용할 수 있습니다.

  검색 내 와일드카드 및 특수문자, 3 페이지의 내용을 참조하십시오.

- 모든 필드에 부정(!)을 사용할 수 있습니다.
- 모든 필드에 쉼표로 구분된 검색 값의 목록을 사용할 수 있습니다. 지정된 필드에 나열된 값 중 하나를 포함하는 레코드는 검색 기준과 일치합니다.
- 모든 필드에 따옴표로 감싸고 쉼표로 구분한 목록을 검색 값으로 사용할 수 있습니다.
  - 단일 값만을 포함할 수 있는 필드의 경우, 따옴표 내에 지정된 정확한 문자열을 포함하는 지정된 필드의 레코드가 검색 기준과 일치합니다. 예를 들어 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `"A"` 또는 `"B"` 또는 `"C, D, E"`가 포함된 레코드와 일치합니다. 따라서 가능한 값으로 쉼표를 포함하는 필드에서 일치를 확인할 수 있습니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 따옴표로 감싸고 쉼표로 구분한 모든 값을 포함하는 지정된 필드의 레코드가 해당 검색 기준과 일치합니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 검색 기준에 단일 값은 물론 따옴표로 감싸고 쉼표로 구분한 목록도 포함할 수 있습니다. 예를 들어 하나 이상의 이러한 문자를 포함할 수 있는 필드에서 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `A` 또는 `B`, 또는 `C, D, E` 모두가 포함된 레코드와 일치합니다.
- 해당 필드에 대해 사용할 수 있는 정보가 없는 이벤트를 식별하려면 필드에 `n/a`를 지정합니다. 해당 필드가 채워지는 이벤트를 식별하려면 `!n/a`를 사용합니다.
- 많은 숫자 필드 앞에 초과(>), 이상(>=), 미만(<), 이하(<=), 같음(=) 또는 같지 않음(<>) 연산자를 붙일 수 있습니다.

팁 길고 복잡한 값(SHA-256 해시 값 등)을 이용해 필드를 검색하는 경우, 소스 자료에서 검색 기준을 복사해 검색 페이지의 적절한 필드에 붙여넣을 수 있습니다.

검색 내 와일드카드 및 특수문자

연결 및 보안 인텔리전스 이벤트의 모든 텍스트 필드 및 기타 이벤트 유형의 대부분의 텍스트 필드에서 검색할 때 텍스트 필드에서 부분 일치를 검색하려면 문자열에서 지정되지 않은 문자를 나타내는 별표(*)가 필요합니다. 별표가 없는 검색은 이러한 필드의 정확한 일치 검색입니다. 와일드 카드가 필요하지 않은 필드에서도 부분 일치 검색에는 항상 와일드 카드를 사용하는 것이 좋습니다.

예를 들어 `example.com`, `www.example.com` 또는 `department.example.com`을 찾으려면 `*.example.com`으로 검색합니다. 대부분의 경우 `example.com`을 검색하면 `example.com`만 반환됩니다.

영숫자 외의 문자를 검색하려면(별표 문자 포함) 검색 문자열을 따옴표로 감싸십시오. 예를 들어 다음 문자열을 검색하려면

```
Find an asterisk (*)
```

다음을 입력합니다.

```
"Find an asterisk (*)"
```

검색 내 개체 및 애플리케이션 필터

Firepower System에서는 네트워크 설정의 일부로 사용할 수 있는 명명된 개체, 개체 그룹 및 애플리케이션 필터를 생성할 수 있습니다. 검색을 수행하거나 저장할 때 이러한 개체, 그룹 및 필터를 검색 기준으로 사용할 수 있습니다.

검색을 수행하면 개체, 개체 그룹 및 애플리케이션 필터가 `${object_name}`의 형식으로 나타납니다. 예를 들어 개체 이름이 `ten_ten_network`인 네트워크 개체는 검색에 `${ten_ten_network}`로 나타납니다.

검색 기준으로 개체를 사용할 수 있는 검색 필드 옆에 나타나는 개체( )를 클릭할 수 있습니다.

관련 항목

개체 관리자

검색 내 시간 제약 조건

시간 값을 입력하는 검색 기준 필드에서 허용되는 형식은 다음 표에 나와 있습니다.

표 *1:* 검색 필드의 시간 사양

시간 형식	예
`today [at HH:MMam|pm]`	현재 `today at 12:45pm`
`YYYY-DDMM- HH:MM:SS`	`2006-03-22 14:22:59`

다음 연산자 중 하나를 시간 값 앞에 사용할 수 있습니다.

표 2: 시간 사양 연산자

운영자	예	설명
<	`< 2006-03-22 14:22:59`	2006년 3월 22일 오후 2:23 이전 타임스탬프의 이벤트를 반환합니다.
>	`> today at 2:45pm`	오늘 오후 2:45 이후 타임스탬프의 이벤트를 반환합니다.

검색 내 IP 주소

검색에서 IP 주소를 지정할 때에는 개별 IP 주소, 쉼표로 구분된 주소 목록, 주소 블록, 또는 하이픈(-)으로 구분된 IP 주소 범위를 입력할 수 있습니다. 또한 부정을 사용할 수 있습니다.

침입 이벤트, 연결 데이터 및 상관 관계 이벤트 검색과 같은 IPv6을 지 원하는 검색의 경우 IPv4 및 IPv6 주소와 CIDR/접두사 길이 주소 블록을 임의의 조합으로 입력할 수 있습니다. IP 주소별로 호스트를 검색하면 하나 이상의 IP 주소가 검색 기준과 일치하는 모든 호스트가 결과에 포함됩니다. 즉, IPv6 주소를 검색하면 기본 주소가 IPv4인 호스트가 반환될 수 있습니다.

CIDR 또는 접두사 길이 표기법을 사용하여 IP 주소 블록을 지정하려는 경우, Firepower System은 마스크 또는 접두사 길이에 의해 지정된 네트워크 IP 주소의 일부만 사용합니다. 예를 들어 `10.1.2.3/8`을 입력한 경우 Firepower System은 `10.0.0.0/8`을 사용합니다.

IP 주소는 네트워크 개체로도 표현할 수 있으므로, IP 주소 검색 기준으로 네트워크 개체를 사용하려면 IP 주소 검색 필드 옆에 나타나는 네트워크 추가 개체(+)을 클릭할 수 있습니다.

표 3: 허용되는 IP 주소 구문

지정할 주소	입력할 내용	예시
단일 IP 주소	IP 주소	`192.168.1.1` `2001:db8::abcd`
목록을 사용하여 여러 IP 주소	쉼표로 구분된 IP 주소의 목록 쉼표 전후에 공백을 추가하지 마십시오.	`192.168.1.1,192.168.1.2` `2001:db8::b3ff,2001:db8::0202`
CIDR 블록 또는 접두사 길이로 지정할 수 있는 IP 주소의 범위	IPv4 CIDR 또는 IPv6 접두사 길이 표기법으로 IP 주소 블록	`192.168.1.0/24` 192.168.1.0 네트워크에서 255.255.255.0(즉, 192.168.1.0~192.168.1.255)의 IP를 지정합니다.
CIDR 블록 또는 접두사로 지정할 수 없는 IP 주소의 범위	하이픈을 사용하여 IP 주소 범위 하이픈 전후에 공백을 추가하지 마십시오.	`192.168.1.1-192.168.1.5` `2001:db8::0202-2001:db8::8329`

지정할 주소	입력할 내용	예시

IP 주소 또는 IP 주소 범위를 지정하기 위한 기타 방법의 표기법	IP 주소, 블록 또는 범위 앞에 느낌표	`192.168.0.0/32,!192.168.1.10`
		`!2001:db8::/32`
		`!192.168.1.10,!2001:db8::/32`

차단되었거나 모니터링되는(하지만 차단되었을 수 있는) 호스트 호스트 프로파일 아이콘의 내용을 참조하십시오.	연결 및 보안 인텔리전스 이벤트의 이니시에이터 IP 및 응답자 IP 필드: • 블랙리스트 • • 모니터	--

관련 항목

Firepower System IP 주소 규칙

검색의 URL

URL을 검색할 때 와일드 카드를 포함합니다. 예를 들어 **`*example.com*`**을 사용하여 도메인의 모든 변형(예: **`https://example.com`**, **`division.example.com`** 및 **`example.com/division/`**)을 찾습니다.

검색 내 매니지드 디바이스

FMC에서만, 또는 실제 고가용성 또는 확장성 구성을 통해 디바이스를 그룹화하면 그룹의 이름을 검색했을 때 그룹 내의 모든 디바이스를 결과로 올바르게 반환합니다.

그룹, 디바이스 고가용성 쌍 또는 스택에 대한 일치를 발견하면, 시스템은 검색 수행을 위해 그룹, 디바이스 고가용성 쌍 또는 스택 이름을 적절한 회원 디바이스 이름으로 교체합니다. 장치 필드에 디바이스 그룹, 디바이스 고가용성 쌍 또는 스택을 사용하는 검색을 저장하면, 시스템은 장치 필드에 지정된 이름을 저장하고 검색이 실행될 때마다 디바이스 이름 교체를 수행합니다.

검색 내 포트

Firepower System은 검색에서 포트 번호에 대한 특정 구문을 허용합니다. 다음을 입력할 수 있습니다.

- 단일 포트 번호
- 쉼표로 구분된 포트 번호 목록
- 대시로 구분된 두 개의 포트 번호(포트 번호의 범위를 나타냄)
- 포트 번호 뒤에는 (침입 이벤트를 검색할 때만) 슬래시 (/)로 구분 된 프로토콜 약어
- 앞에 느낌표가 있는 포트 번호 또는 포트 번호의 범위(지정된 포트의 부정을 나타냄)

참고 포트 번호 또는 범위를 지정할 때는 공백을 사용하지 마십시오.

표 *4:* 포트 구문 예

예	설명
`21`	TCP와 UDP 이벤트를 비롯한 포트 21의 모든 이벤트를 반환합니다.
`!23`	포트 23의 이벤트를 제외한 모든 이벤트를 반환합니다.
`25/tcp`	포트 25의 모든 TCP 관련 침입 이벤트를 반환합니다.
`21/tcp,25/tcp`	포트 21과 25의 모든 TCP 관련 침입 이벤트를 반환합니다.
`21-25`	포트 21~25의 모든 이벤트를 반환합니다.

검색 내 이벤트 필드

이벤트를 검색하는 경우 검색 기준으로 다음 필드를 사용할 수 있습니다.

- 감사 로그 워크플로 필드
- 애플리케이션 데이터 필드
- 애플리케이션 세부사항 데이터 필드
- 캡처된 파일 필드
- 화이트 목록 이벤트 필드
- 연결 및 보안 인텔리전스 이벤트 필드
- 상관관계 이벤트 필드
- 검색 이벤트 필드
- 상태 이벤트 테이블
- 호스트 속성 데이터 필드
- 호스트 데이터 필드
- 파일 및 악성코드 이벤트 필드
- 침입 이벤트 필드
- 침입 규칙의 필드에 로그를 업데이트합니다.

- 교정 상태 테이블 필드
- Nmap 스캔 결과 필드
- 서버 데이터 필드
- 서드파티 취약성 데이터 필드
- 사용자 관련 필드
- 취약성 데이터 필드
- 화이트 목록 위반 필드

검색 수행

검색을 수행하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Search(**검색**)**를 선택합니다.

팁 워크플로의 아무 페이지에서 **Search(**검색**)**를 클릭해도 됩니다.

단계 **2** 테이블 드롭다운 목록에서 검색할 이벤트 또는 데이터 유형을 선택합니다.

단계 **3** 해당 필드에 검색 기준을 입력합니다. 사용 가능한 검색 기준에 대해 자세히 알아보려면 다음 섹션을 참조하십시오.

- 검색 제약 조건, 2 페이지
- 감사 로그 워크플로 필드
- 애플리케이션 데이터 필드
- 애플리케이션 세부사항 데이터 필드
- 캡처된 파일 필드
- 화이트 목록 이벤트 필드
- 연결 및 보안 인텔리전스 이벤트 필드
- 상관관계 이벤트 필드
- 검색 이벤트 필드
- 상태 이벤트 테이블
- 호스트 속성 데이터 필드
- 호스트 데이터 필드

- 파일 및 악성코드 이벤트 필드
- 침입 이벤트 필드
- 침입 규칙의 필드에 로그를 업데이트합니다.
- 교정 상태 테이블 필드
- Nmap 스캔 결과 필드
- 서버 데이터 필드
- 서드파티 취약성 데이터 필드
- 사용자 데이터 필드
- 사용자 활동 데이터 필드
- 취약성 데이터 필드
- 화이트 목록 위반 필드

단계 **4** 검색을 나중에 다시 사용하려면 검색 저장, 8 페이지에 설명된 대로 검색을 저장합니다.

단계 **5** 검색을 시작하려면 **Search(**검색**)**를 클릭합니다. 검색 결과가 시간으로 제한되어(적용 가능한 경우) 검색 중인 테이블에 대한 기본 워크플로우에 나타납니다.

다음에 수행할 작업

- 워크플로를 사용하여 검색 결과를 분석하는 방법은 워크플로 사용 섹션을 참조하십시오.

관련 항목

이벤트 보기 구성

검색 저장

검색을 저장하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 저장된 검색을 표시하며 이러한 검색은 수정할 수 있습니다. 상위 도메인에서 저장된 검색도 표시되지만, 이러한 검색은 수정할 수 없습니다. 하위 도메인에서 생성된 검색을 보고 수정하려면 해당 도메인으로 전환하십시오.

시작하기 전에

- 검색 수행, 7 페이지에 설명된 대로 검색 기준을 설정하거나, 저장된 검색 로드, 9 페이지에 설명된 대로 저장된 검색을 로드합니다.

프로시저

단계 **1** 자신만 액세스할 수 있도록 검색을 비공개로 저장하려면, Search(검색) 페이지에서 **Private(**비공개**)** 확인란을 선택합니다.

팁 맞춤형 사용자 역할을 위한 데이터 제한으로 검색을 사용하려면 반드시 비공개 검색으로 저장해야 합니다.

단계 **2** 다음 2가지 옵션을 사용할 수 있습니다.

- 로드한 검색의 새 버전을 저장하려는 경우에는 **Save As New(**신규로 저장**)**를 클릭합니다.
- 새 검색을 저장하거나 같은 이름을 이용해 맞춤형 검색을 덮어쓰려는 경우에는 **Save(**저장**)**를 클릭합니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

저장된 검색 로드

저장된 검색을 로드하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 저장된 검색을 표시하며 이러한 검색은 수정할 수 있습니다. 상위 도메인에서 저장된 검색도 표시되지만, 이러한 검색은 수정할 수 없습니다. 하위 도메인에서 생성된 검색을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Analysis(**분석**)** > **Search(**검색**)**을(를) 선택합니다.

팁 워크플로의 아무 페이지에서 **Search(**검색**)**를 클릭해도 됩니다.

단계 **2** 테이블 드롭다운 목록에서 검색할 이벤트 또는 데이터 유형을 선택합니다.

단계 **3** **Custom Searches(**맞춤형 검색**)** 목록 또는 **Predefined Searches(**사전 정의된 검색**)** 목록에서 로드하려는 검색을 선택합니다.

단계 **4** 다른 검색 기준을 사용하려는 경우에는 검색 제약 조건을 변경합니다.

단계 **5** 변경된 검색을 나중에 다시 사용하려면, 검색 저장, 8 페이지에 설명된 대로 검색을 저장합니다.

단계 **6** **Search(**검색**)**를 클릭합니다.

셸을 통해 쿼리 재정의

시스템 관리자는 Linux 셸 기반 쿼리 관리 도구를 사용해 오래 실행되는 쿼리를 찾아서 중지할 수 있습니다.

쿼리 관리 툴을 사용하면 지정된 기간(분)보다 오래 실행되는 쿼리를 찾아 중지할 수 있습니다. 쿼리를 중지하면 이벤트가 감사 로그 및 시스템 로그에 기록됩니다.

관리자 내부 사용자는 FMC CLI에 액세스할 수 있습니다. CLI 액세스를 허용하는 외부 인증 개체를 사용하는 경우 셸 액세스 필터와 일치하는 사용자는 CLI에도 로그인할 수 있습니다.

참고 웹 인터페이스에 검색 페이지를 열어 두면 쿼리가 중지되지 않습니다. 반환에 오랜 시간이 걸리는 쿼리는 쿼리 실행 중에 전체 시스템 성능에 영향을 미칩니다.

셸 기반 쿼리 관리 구문

장기 쿼리는 다음 구문을 사용하여 관리합니다.

```
query_manager [-v] [-l [minutes]] [-k query_id [...]] [--kill-all minutes]
```

표 ***5: query_manager Options(옵션)***

옵션	설명
`-h, --help`	간략한 도움말 메시지를 인쇄합니다.
`-l, --list [minutes]`	지정된 기간(분)보다 오래 걸린 모든 쿼리를 나열합니다. 기본적으로, 1분 이상 걸리는 모든 쿼리가 표시됩니다.
`-k, --kill query_id [...]`	전달된 ID가 있는 쿼리를 중단합니다. 이 옵션은 여러 ID를 이용할 수 있습니다.
`--kill-all minutes`	지정된 기간(분)보다 오래 걸린 모든 쿼리를 중단합니다.
`-v, --verbose`	전체 SQL 쿼리를 포함하여 출력을 자세히 표시합니다.

주의 시스템 보안을 위해 Cisco에서는 Linux 셸 사용자를 어플라이언스에서 추가로 설정하지 않도록 권장합니다.

오래 실행되는 쿼리 중지

CLI 액세스 권한이 있는 관리자 사용자 또는 외부 인증된 사용자여야 합니다.

프로시저

단계 **1** `ssh`를 통해 Firepower Management Center에 연결합니다.

단계 **2** CLI `expert` 명령을 사용하여 Linux 셸에 액세스합니다.

단계 **3** 셸 기반 쿼리 관리 구문, 10 페이지에 설명한 구문을 사용하여 `sudo` 아래에서 `query_manager`를 실행합니다.

이벤트 검색 히스토리

기능	버전	세부 사항
많은 필드에서 부분 일치 검색시 이제 와일드 카드가 필요합니다.	6.6	예를 들어 URL을 검색할 때 **`example.com`**의 모든 변형을 찾으려면 **`* example.com*`**을 사용합니다. 이 동작 변경 사항은 **Analysis(분석) > Search(검색)** 페이지에서 연결 또는 보안 인텔리전스 이벤트를 검색할 때 적용됩니다. 이 검색 페이지는 다른 페이지의 링크를 통해 액세스할 수도 있습니다. 부분 일치 검색에 와일드 카드가 필요하지 않은 필드에서는 선택적으로 사용할 수 있습니다. 영향을 받는 플랫폼: FMC