애플리케이션 탐지

다음 주제에서는 Firepower System 애플리케이션 탐지를 설명합니다.

개요: 애플리케이션 탐지

Firepower System은 IP 트래픽을 분석할 때 네트워크에서 일반적으로 사용되는 애플리케이션 식별을 시도합니다. 애플리케이션 인식은 애플리케이션 제어에 중요한 요소입니다.

시스템에서는 세 가지 유형의 애플리케이션을 탐지합니다.

- HTTP 및 SSH 등의 애플리케이션 프로토콜은 호스트 간 통신을 나타냅니다.
- 웹 브라우저 및 이메일 클라이언트 등의 클라이언트는 호스트웨어에서 실행되는 소프트웨어를 나타냅니다.
- MPEC 비디오 및 Facebook 등의 웹 애플리케이션은 HTTP 트래픽에 대한 요청 RUL 또는 콘텐츠를 나타냅니다.

시스템은 탐지기에서 지정된 특성에 따라 네트워크 트래픽에서 애플리케이션을 식별합니다. 예를 들어 시스템은 패킷 헤더 내 ASCII 패턴에 의해 애플리케이션을 식별할 수 있습니다. 또한 SSL(Secure Socket Layers) 프로토콜 탐지기는 보안 세션의 정보를 사용하여 세션에서 애플리케이션을 식별합니다.

Firepower System에는 두 가지 소스의 애플리케이션 탐지기가 있습니다.

- 시스템 제공 탐지기는 웹 애플리케이션, 클라이언트, 애플리케이션 프로토콜을 탐지합니다.

  애플리케이션(및 운영 체제)의 시스템 제공 탐지기 사용 여부는 Firepower System 및 설치한 VDB 버전에 따라 다릅니다. 신규 및 업데이트된 탐지기 정보는 릴리스 정보 및 참고 자료에서 확인할 수 있습니다. 전문 서비스에서 작성한 개별 탐지기를 가져올 수도 있습니다.

- 사용자 정의 애플리케이션 프로토콜 탐지기는 사용자가 생성한 것으로 웹 애플리케이션, 클라이언트, 애플리케이션 프로토콜을 탐지합니다.

내장된 애플리케이션 프로토콜 탐지기를 통해 애플리케이션 프로토콜을 탐지할 수 있으며 클라이언트의 탐지를 기반으로 애플리케이션 프로토콜의 존재를 암시합니다.

시스템은 네트워크 검색 정책에서 정의된 대로 모니터링되는 네트워크의 호스트에서 실행되는 애플리케이션 프로토콜만 식별합니다. 예를 들어 모니터링하지 않는 원격 사이트의 FTP 서버에 내부 호스트가 액세스하는 경우 시스템은 애플리케이션 프로토콜을 FTP로 식별하지 않습니다. 반면 원격 또는 내부 호스트가 모니터링 중인 FTP 서버에 액세스하면 시스템은 애플리케이션 프로토콜을 분명하게 식별할 수 있습니다.

시스템이 모니터링되는 호스트에서 모니터링되지 않는 서버에 연결하기 위해 사용되는 클라이언트를 식별할 수 있는 경우, 시스템은 클라이언트의 해당 애플리케이션 프로토콜을 식별하지만 해당 프로토콜을 네트워크 맵에 추가하지 않습니다. 애플리케이션 탐지가 발생하려면 클라이언트 세션에는 서버의 응답이 포함되어야 합니다.

시스템이 탐지하는 각 애플리케이션의 특성 정의는 애플리케이션 특성의 내용을 참조하십시오. 시스템은 해당 특성을 사용해 애플리케이션 필터라는 애플리케이션 그룹을 생성합니다. 애플리케이션 필터는 액세스 제어를 수행하고 보고서와 대시보드 위젯에서 사용되는 데이터 및 검색 결과를 제한합니다.

또한 내보낸 NetFlow 기록, Nmap 활성 스캐닝, 호스트 인풋 기능에 사용되는 애플리케이션 탐지기 데이터를 보완할 수 있습니다.

관련 항목

애플리케이션 제어 구성 모범 사례
애플리케이션 탐지기 기초, 2 페이지

애플리케이션 탐지기 기초

Firepower System은 *application detectors(*애플리케이션 탐지기*)*를 사용하여 네트워크 상의 자주 사용하는 애플리케이션을 식별합니다. Detectors(탐지기) 페이지(**Policies(**정책**)** > **Application Detectors(**애플리케이션 탐지기**)**)를 이용해 탐지기 목록을 확인하고 탐지 기능을 맞춤형할 수 있습니다.

탐지기를 수정하거나 탐지기 유형에 따라 탐지기 상태(활성화 또는 비활성화)를 바꿀 수 있습니다. 시스템은 애플리케이션 트래픽을 분석하는 데 활성 탐지기만 사용합니다.

참고 Cisco에서 제공하는 탐지기는 Firepower System 및 VDB 업데이트에 따라 변경될 수 있습니다. 업데이트된 탐지기 관련 정보는 릴리즈 노트와 참고 자료에서 확인할 수 있습니다.

참고 Firepower 애플리케이션 식별을 위해 포트는 의도적으로 나열되지 않습니다. 애플리케이션의 연결 포트는 대부분의 애플리케이션이 포트에 구속되지 않으므로 Cisco의 애플리케이션에 대해 보고되지 않습니다. Cisco 플랫폼의 탐지 기능은 네트워크의 모든 포트에서 실행 중인 서비스를 식별할 수 있습니다.

Cisco가 제공하는 내부 탐지기

내부 탐지기는 클라이언트, 웹 애플리케이션 및 애플리케이션 프로토콜 트래픽에 대한 특수 카테고리의 탐지기입니다. 내부 탐지기는 시스템 업데이트와 함께 제공되며 항상 작동합니다.

애플리케이션이 클라이언트 관련 활동을 탐지할 목적으로 설계한 내부 탐지기와 일치하며 특정한 클라이언트 탐지기가 존재하지 않는다면, 일반 클라이언트가 보고될 수 있습니다.

Cisco가 제공하는 클라이언트 탐지기

클라이언트 탐지기는 클라이언트 트래픽을 탐지하고 VDB 또는 시스템 업데이트를 통해 전달되며, Cisco Professional Services의 가져오기를 위해 제공됩니다. 클라이언트 탐지기를 활성화 또는 비활성화할 수 있습니다. 가져온 클라이언트 탐지기만 내보낼 수 있습니다.

Cisco가 제공하는 웹 애플리케이션 탐지기

웹 애플리케이션 탐지기는 HTTP 트래픽 페이로드의 웹 애플리케이션을 탐지하며 VDB 또는 시스템 업데이트를 통해 전달됩니다. 웹 애플리케이션 탐지기는 항상 작동합니다.

Cisco가 제공하는 애플리케이션 프로토콜**(**포트**)** 탐지기

포트 기반 애플리케이션 프로토콜 탐지기는 잘 알려진 포트를 사용하여 네트워크 트래픽을 식별합니다. 이러한 탐지기는 VDB 또는 시스템 업데이트를 통해 전달되며, Cisco Professional Services의 가져오기를 위해 제공됩니다. 애플리케이션 프로토콜 탐지기를 활성화 또는 비활성화할 수 있으며, 탐지기 정의를 확인해 맞춤형 탐지기의 기본 토대로 사용할 수 있습니다.

Cisco가 제공하는 애플리케이션 프로토콜**(Firepower)** 탐지기

Firepower 기반 애플리케이션 프로토콜 탐지기는 Firepower 애플리케이션 핑거프린트를 사용해 네트워크 트래픽을 분석하며 VDB 또는 시스템 업데이트를 통해 전달됩니다. 애플리케이션 프로토콜 탐지기를 활성화 또는 비활성화할 수 있습니다.

맞춤형 애플리케이션 탐지기

맞춤형 애플리케이션 탐지기는 패턴 기반 탐지기입니다. 클라이언트, 웹 애플리케이션 또는 애플리케이션 프로토콜 트래픽의 패킷에 있는 패턴을 탐지합니다. 사용자는 가져온 탐지기와 맞춤형 탐지기에 대한 완전한 제어 권한을 갖습니다.

웹 인터페이스에서 애플리케이션 프로토콜 식별

아래 테이블은 탐지한 애플리케이션 프로토콜을 시스템이 식별하는 방법을 설명합니다.

표 *1:* 애플리케이션 프로토콜의 시스템 식별

식별	설명
애플리케이션 프로토콜 이름	애플리케이션 프로토콜이 다음 조건을 충족하면 management center은(는) 이름이 있는 애플리케이션 프로토콜을 식별합니다. • 애플리케이션 프로토콜이 시스템에 의해 긍정적으로 식별된 경우 • 애플리케이션 프로토콜이 NetFlow 데이터를 통해 식별되었으며 `/etc/sf/services`에 포트 애플리케이션 프로토콜 상관관계가 있는 경우 • 애플리케이션 프로토콜이 호스트 입력 기능을 통해 수동으로 식별된 경우 • 애플리케이션 프로토콜이 Nmap 또는 다른 활성 소스에 의해 식별된 경우
`pending`	시스템이 애플리케이션을 긍정적으로도 부정적으로도 식별할 수 없는 경우 management center은(는) 애플리케이션 프로토콜을 `pending`으로 식별합니다. 대부분의 경우 시스템은 보류 중인 애플리케이션을 식별하려면 더 많은 데이터를 수집 및 분석해야 합니다. Application Details 및 Servers 테이블과 호스트 프로파일에서 `pending` 상태는 (탐지된 클라이언트 또는 웹 애플리케이션 트래픽에서 추론하는 대신) 특정 애플리케이션 프로토콜 트래픽이 탐지된 애플리케이션 프로토콜에 대해서만 나타납니다.
`unknown`	management center은(는) 다음과 같은 경우 애플리케이션 프로토콜을 `unknown(알 수 없음)`으로 식별합니다. • 애플리케이션이 시스템의 어떤 탐지기와도 일치하지 않는 경우. • 애플리케이션 프로토콜이 NetFlow 데이터를 통해 식별되었지만 `/etc/sf/services`에 포트 애플리케이션 프로토콜 상관관계가 없는 경우. • Snort에서 세션을 종료했지만 디바이스에 계속 남아 있습니다. 여기서 트래픽은 방화벽을 통과할 수 있지만 애플리케이션은 탐지되지 않습니다.
공백	사용 가능한 모든 탐지된 데이터가 검토되었지만 애플리케이션 프로토콜이 식별되지 않았습니다. Application Details 및 Servers 테이블과 호스트 프로파일에서, 탐지된 애플리케이션 프로토콜이 없는 비 HTTP 일반 클라이언트 트래픽에 대해 애플리케이션 프로토콜은 비어 있게 됩니다.

클라이언트 탐지의 암시적 애플리케이션 프로토콜 탐지

모니터링되지 않는 서버에 액세스하는 모니터링되는 호스트가 사용하는 클라이언트를 시스템이 식별할 수 있는 경우, management center은(는) 클라이언트와 상응하는 애플리케이션 프로토콜이 연결에 사용되고 있다고 추론합니다. 시스템은 모니터링되는 네트워크에서만 애플리케이션을 추적하므로, 일반적으로 연결 로그에는 모니터링되는 호스트가 모니터링되지 않는 서버에 액세스하는 연결에 대한 애플리케이션 프로토콜 정보가 포함되지 않습니다.

이 프로세스, 즉 암시작 애플리케이션 프로토콜 탐지는 다음과 같은 결과를 유발합니다.

- 시스템은 이러한 서버에 대해 New TCP Port 또는 New UDP Port 이벤트를 생성하지 않으므로 Servers 테이블에 서버가 나타나지 않습니다. 또한 이러한 애플리케이션 프로토콜의 탐지를 기준으로 사용하여 검색 이벤트 알림 또는 상관관계 규칙을 트리거할 수 없습니다.
- 애플리케이션 프로토콜은 호스트와 연결되지 않으므로 호스트 프로파일의 상세정보을 볼 수 없거나, 서버 ID를 설정할 수 없거나, 트래픽 프로파일 또는 상관관계 규칙에 대한 호스트 프로파일 자격에서 해당 정보를 사용할 수 없습니다. 또한 시스템은 이러한 유형의 탐지를 기반으로 취약성을 호스트와 연결하지 않습니다.

하지만 연결에 존재하는 애플리케이션 프로토콜 정보에 대한 상관관계 이벤트를 트리거할 수는 있습니다. 또한 연결 로그에서 애플리케이션 프로토콜 정보를 사용하여 연결 추적기 및 트래픽 프로파일을 생성할 수 있습니다.

호스트 제한 및 검색 이벤트 로깅

클라이언트, 서버 또는 웹 애플리케이션을 탐지하면, 시스템은 연결된 호스트가 이미 최대 클라이언트, 서버 또는 웹 애플리케이션 수에 도달하지 않은 경우 검색 이벤트를 생성합니다.

호스트 프로파일은 호스트당 클라이언트 최대 16개, 서버 100개, 웹 애플리케이션 100개를 표시합니다.

클라이언트, 서버 또는 웹 애플리케이션의 탐지에 의존하는 작업은 이 제한의 영향을 받지 않습니다. 예를 들어 서버를 트리거하도록 구성된 액세스 컨트롤 규칙은 여전히 연결 이벤트를 기록합니다.

애플리케이션 탐지 특별 고려 사항

SFTP

SFTP 트래픽을 탐지하려면 동일한 규칙에서도 SSH를 탐지해야 합니다.

Squid

다음과 같은 경우 시스템은 Squid 서버 트래픽을 분명하게 식별합니다.

- 시스템은 모니터링되는 네트워크 호스트에서 프록시 인증이 활성화된 Squid 서버로의 연결을 탐지하거나
- 모니터링되는 네트워크의 Squid 프록시 서버에서 대상 시스템(클라이언트가 정보 또는 다른 리소스를 요청하는 대상 서버)으로의 연결을 탐지한 경우

그러나 다음과 같은 경우 시스템은 Squid 서비스 트래픽을 식별할 수 없습니다.

- 모니터링되는 네트워크의 호스트가 프록시 인증이 비활성화된 Squid 서버에 연결하거나,
- Squid 프록시 서버가 HTTP 응답에서 헤더 필드를 제거하도록 구성된 경우

SSL 애플리케이션 탐지

시스템은 세션 내 애플리케이션 프로토콜, 클라이언트 애플리케이션, 또는 웹 애플리케이션을 식별하기 위해 SSL(Secure Socket Layers) 세션의 세션 정보를 사용할 수 있는 애플리케이션 탐지기를 제공합니다.

시스템이 암호화된 연결을 탐지하면 가능한 경우 해당 연결을 SMTPS 등의 일반 HTTPS 연결 또는 보다 특정한 보안 프로토콜로 표시합니다. 시스템이 SSL 세션을 탐지하면 `SSL 클라이언트`를 세션에 대한 연결 이벤트의 클라이언트 필드에 추가합니다 세션에 대한 웹 애플리케이션이 확인될 경우, 시스템에서는 트래픽에 대한 검색 이벤트를 생성합니다.

SSL 애플리케이션 트래픽의 경우 관리되는 디바이스는 서버 인증서에서 일반 이름을 탐지하고 이를 SSL 호스트 패턴의 클라이언트 또는 웹 애플리케이션과 일치시킬 수 있습니다. 시스템이 특정 클라이언트를 식별하는 경우 `SSL 클라이언트`가 해당 클라이언트의 이름으로 변경됩니다.

SSL 애플리케이션 트래픽이 암호화되므로 시스템은 암호화된 스트림에 있는 애플리케이션 데이터가 아닌 인증서의 정보만 사용하여 식별 작업을 수행합니다. 이러한 이유로 인해 SSL 호스트 패턴에서 애플리케이션을 만든 회사만 식별할 수 있는 경우가 간혹 있으므로, 같은 회사에서 제작한 SSL 애플리케이션의 경우 동일한 식별 과정을 거쳤을 수 있습니다.

HTTPS 세션이 HTTP 세션 내에서 실행되는 등의 일부 경우에는 관리되는 디바이스가 클라이언트 측 패킷의 클라이언트 인증서에서 서버 이름을 탐지합니다.

SSL 애플리케이션 식별을 활성화하려면 응답자 트래픽을 모니터링하는 액세스 제어 규칙을 생성해야 합니다. 그러한 규칙에는 SSL 애플리케이션에 대한 애플리케이션 조건 또는 SSL 인증서의 URL을 사용하는 URL 조건이 있어야 합니다. 네트워크 검색 시 응답자 IP 주소는 네트워크 검색 정책에서 모니터링할 네트워크에 반드시 있지 않아도 됩니다. 액세스 제어 정책 설정은 트래픽의 식별 여부를 결정합니다. SSL 애플리케이션에 대해 탐지기를 식별하려면, 애플리케이션 탐지기 목록 또는 액세스 제어 규칙에서 애플리케이션 조건을 추가할 때 `SSL protocol` 태그별로 필터링할 수 있습니다.

참조된 웹 애플리케이션

웹 서버는 종종 광고 서버인 다른 웹 사이트에 대한 트래픽을 가끔 참조합니다. 네트워크에서 발생하는 참조된 트래픽의 문맥을 더 잘 이해할 수 있도록, 시스템은 참조된 세션에 대한 이벤트의 **Web Application(**웹 애플리케이션**)** 필드에 트래픽을 참조한 웹 애플리케이션을 나열합니다. VDB에는 알려진 참조 사이트의 목록이 포함되어 있습니다. 시스템이 이 사이트 중 하나의 트래픽을 탐지하면 해당 트래픽에 대한 이벤트와 함께 참조 사이트가 저장됩니다. 예를 들어 Facebook을 통해 액세스하는 광고가 실제로 Advertising.com에 호스팅되면 탐지된 Advertising.com 트래픽은 Facebook 웹 애플리케이션에 연결됩니다. 시스템은 또한 웹사이트가 다른 사이트에 단순 링크를 제공하는 등의 경우 참조하는 URL을 탐지할 수 있습니다. 이 경우 참조하는 URL이 참조된 이벤트 필드에 나타납니다.

참조하는 애플리케이션이 존재하는 경우 이벤트에는 트래픽에 대한 웹 애플리케이션으로 나열되는 반면 URL은 참조 사이트를 나타냅니다. 위의 예에서 해당 트래픽에 대한 연결 이벤트의 웹 애플리케이션은 Facebook일 수 있지만 URL은 Advertising.com입니다. 참조하는 웹 애플리케이션이 탐지되지 않거나 호스트가 스스로를 참조하거나 참조 연결이 있는 경우 참조하는 웹 애플리케이션이 웹 애플리케이션에 표시될 수 있습니다. 대시보드에서 웹 애플리케이션의 연결 및 바이트 카운트에는 웹 애플리케이션이 스스로 참조한 트래픽과 연결된 세션이 포함됩니다.

참조된 트래픽에 대해 특별히 작동하는 규칙을 생성하는 경우 참조하는 애플리케이션보다 참조된 애플리케이션에 대한 조건을 추가해야 합니다. 예를 들어 Facebook에서 참조되는 Advertising.com 트

래픽을 차단하려면 Advertising.com 애플리케이션에 대한 액세스 제어 규칙에 애플리케이션 조건을 추가합니다.

Snort 2 및 Snort 3의 애플리케이션 탐지

Snort 2에서는 액세스 제어 정책의 제약 조건 및 네트워크 검색 정책의 네트워크 필터를 통해 애플리케이션 탐지를 활성화하거나 비활성화할 수 있습니다. 그러나 액세스 제어 정책의 제약 조건은 네트워크 필터를 재정의하고 애플리케이션 탐지를 활성화할 수 있습니다. 예를 들어 네트워크 검색 정책에서 네트워크 필터를 정의했으며 액세스 제어 정책에 SSL, URL SI, DNS SI 등 애플리케이션 탐지가 필요한 제약 조건이 있는 경우 이러한 네트워크 검색 필터가 재정의되고 모든 네트워크가 애플리케이션 탐지를 위해 모니터링됩니다. 이 Snort 2 기능은 Snort 3에서 지원되지 않습니다.

참고 AC 정책의 다른 구성에서 AppID가 모든 트래픽을 모니터링하도록 요구하지 않는 경우 네트워크 검색 정책 필터에 정의된 특정 네트워크 서브넷에서만 AppID 검사를 활성화한다는 점에서 Snort 3은 이제 Snort 2와 동등합니다.

Snort 3에서는 기본적으로 모든 네트워크에 대해 애플리케이션 탐지가 항상 활성화되어 있습니다. 애플리케이션 탐지를 비활성화하려면 다음을 수행합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택하고 edit policy(정책 수정)를 클릭하여 애플리케이션 규칙을 삭제합니다.

단계 **2** **Policies(**정책**)** > **SSL**을 선택하고 Delete(삭제)를 클릭하여 SSL 정책을 삭제합니다.

단계 **3** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**를 선택하고 delete(삭제)를 클릭하여 네트워크 검색 정책을 삭제합니다.

단계 **4** **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택하고 edit policy(정책 편집)를 클릭한 다음 **Security Intelligence(**보안 인텔리전스**)** > **URLs** 탭을 선택하여 URL Allow(허용) 또는 Block(차단) 목록을 삭제합니다.

단계 **5** 기본 DNS 규칙은 삭제할 수 없으므로 **Policies(**정책**)** > **DNS**를 선택하고 edit(편집)를 클릭한 다음 enabled(활성화됨) 확인란의 선택을 취소하여 DNS 정책을 비활성화합니다.

단계 **6** 액세스 제어 정책의 **Advanced(**고급**)** 설정에서 *Enable Threat Intelligence Director(Threat Intelligence Director* 활성화*)* 및 *Enable Reputation Enforcement on DNS traffic(DNS* 트래픽에 대한 평판 적용 활성화*)* 옵션을 비활성화합니다.

단계 **7** 액세스 제어 정책을 저장하고 구축합니다.

애플리케이션 탐지 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 검색 관리자

맞춤형 애플리케이션 탐지기

네트워크에서 맞춤형 애플리케이션을 이용한다면, 애플리케이션을 식별하는 데 필요한 정보를 시스템에 제공하는 맞춤형 웹 애플리케이션, 클라이언트 또는 애플리케이션 프로토콜 탐지기를 만들 수 있습니다. 애플리케이션 탐지기 유형은 **Protocol(**프로토콜**)**, **Type(**유형**)**, **Direction(**방향**)** 필드에서 선택한 내용에 따라 결정됩니다.

서버 트래픽에서 애플리케이션 프로토콜의 탐지 및 식별을 시작하려면, 클라이언트 세션에 시스템에 대한 서버의 Responder 패킷이 포함되어야 합니다. UDP 트래픽의 경우 시스템은 Responder 패킷의 소스를 서버로 지정합니다.

또 다른 management center에서 이미 탐지기를 생성한 경우 이를 내보낸 다음 이 management center(으)로 가져올 수 있습니다. 그런 다음 가져온 탐지기를 필요에 맞게 편집할 수 있습니다. 맞춤형 탐지기는 물론 Cisco Professional Services에서 제공한 탐지기도 내보내고 가져올 수 있습니다. 하지만 다른 유형의 Cisco 제공 탐지기는 내보내거나 가져올 수 없습니다.

맞춤형 애플리케이션 탐지기 및 사용자 정의 애플리케이션 필드

다음 필드를 이용해 사용자 정의 애플리케이션 탐지기 및 맞춤형 애플리케이션을 설정할 수 있습니다.

맞춤형 애플리케이션 탐지기 필드**:** 일반

다음 필드를 사용하여 기본 및 고급 맞춤형 애플리케이션 탐지기를 설정합니다.

애플리케이션 프로토콜

탐지할 애플리케이션 프로토콜입니다. 시스템이 제공한 애플리케이션일 수도 있고 사용자 정의 애플리케이션일 수도 있습니다.

애플리케이션이 액티브 인증에서 면제될 수 있게 하려면(ID 규칙에서 설정되게 하려면), **User-Agent Exclusion(**사용자-에이전트 제외**)** 태그가 있는 애플리케이션 프로토콜을 선택하거나 생성해야 합니다.

설명

애플리케이션 탐지기에 대한 설명입니다.

이름

애플리케이션 탐지기의 이름입니다.

탐지기 유형

탐지기의 유형(기본 또는 고급)입니다. 기본 애플리케이션 탐지기는 웹 인터페이스에서 일련의 필드로 생성됩니다. 고급 애플리케이션 탐지기는 외부에서 생성되며 맞춤형 .lua 파일로 업로드됩니다.

맞춤형 애플리케이션 탐지기 필드**:** 탐지 패턴

다음 필드를 사용하여 기본 맞춤형 애플리케이션 탐지기의 탐지 패턴을 설정합니다.

Direction(방향**)**

탐지기가 검사해야 하는 트래픽의 소스(**Client(**클라이언트**)** 또는 **Server(**서버**)** 입니다.

Offset(오프셋**)**

패킷 페이로드 시작 지점을 기준으로 한 패킷 위치(단위: 바이트)로, 시스템이 패킷 검색을 시작해야 하는 위치를 말합니다.

패킷 페이로드는 바이트 0에서 시작되므로, 패킷 페이로드의 시작 부분부터 진행할 바이트의 수에서 1을 뺀 값으로 오프셋을 계산합니다. 예를 들어 패킷의 5번째 비트에서 패턴을 검색하려면 **Offset** 필드에 4를 입력합니다.

패턴

선택한 **Type(**유형**)**과 연결된 패턴 문자열입니다.

포트

탐지기가 검사해야 하는 트래픽의 포트입니다.

프로토콜

탐지할 프로토콜입니다. 프로토콜 선택에 따라 **Type(**유형**)**과 **URL** 필드 중 무엇을 표시할지가 결정됩니다.

프로토콜(그리고 경우에 따라 **Type(**유형**)** 및 **Direction(**방향**)** 필드의 후속 선택 사항)에 따라 사용자가 생성하는 애플리케이션 탐지기 유형이 결정됩니다(웹 애플리케이션, 클라이언트 또는 애플리케이션 프로토콜).

탐지기 유형	프로토콜	유형 또는 방향
웹 애플리케이션	HTTP	**Type(**유형**)**은 **Content Type(**콘텐츠 유형**)** 또는 **URL**임
	RTMP	Any(모든)
	SSL	Any(모든)
Client(클라이언트)	HTTP	**Type(**유형**)**은 **User Agent(**사용자 에이전트**)** 임
	SIP	Any(모든)
	TCP 또는 UDP	**Direction(**방향**)**은 **Client(**클라이언트**)** 임
애플리케이션 프로토콜	TCP 또는 UDP	**Direction(**방향**)**은 **Server(**서버**)** 임

유형

입력한 패턴 문자열의 유형입니다. 표시되는 옵션은 선택한 **Protocol(**프로토콜**)**에 따라 달라집니다. **RTMP**를 프로토콜로 선택한 경우, **URL** 필드가 **Type(**유형**)** 필드 대신 표시됩니다.

참고 **User Agent(**사용자 에이전트**)**를 **Type(**유형**)**으로 선택한 경우, 시스템은 자동으로 애플리케이션 **Tag(**태그**)**를 **User-Agent Exclusion(**사용자-에이전트 제외**)**으로 설정합니다.

유형 선택	문자열 특징
ASCII	문자열은 ASCII 인코딩됩니다.
공용 이름	문자열은 서버 응답 메시지 내 commonName 필드의 값입니다.
콘텐츠 유형	문자열은 서버 응답 헤더 내 콘텐츠 유형 필드의 값입니다.
16진수	문자열은 16 진수 표기법으로 표시됩니다.
조직 단위	문자열은 서버 응답 메시지 내 organizationName 필드의 값입니다.
SIP 서버	문자열은 메시지 헤더 내 From 필드의 값입니다.
SSL 호스트	문자열은 ClientHello 메시지 내 server_name 필드의 값입니다.

유형 선택	문자열 특징
URL	문자열은 URL입니다. 참고 탐지기는 사용자가 입력한 문자열이 URL 전체 섹션이라고 가정합니다. 예를 들어 **cisco.com**을 입력하면 **www.cisco.com/support** 및 **www.cisco.com**과는 일치하지만 **www.wearecisco.com**과는 일치하지 않습니다.
사용자 에이전트	문자열은 GET 요청 헤더 내 사용자-에이전트 필드의 값입니다. SIP 프로토콜에도 사용 가능하며 문자열은 SIP 메시지 헤더 내 사용자-에이전트 필드의 값임을 나타냅니다.

URL

RTMP 패킷의 C2 메시지 내 swfURL 필드의 전체 URL 또는 URL 섹션입니다. 이 필드는 **RTMP**를 **Protocol(**프로토콜**)**로 선택했을 때 **Type(**유형**)** 필드 대신 표시됩니다.

참고 탐지기는 사용자가 입력한 문자열이 URL 전체 섹션이라고 가정합니다. 예를 들어 **cisco.com**을 입력하면 **www.cisco.com/support** 및 **www.cisco.com**과는 일치하지만 **www.wearecisco.com**과는 일치하지 않습니다.

사용자 정의 애플리케이션 필드

다음 필드를 사용하여 기본 및 고급 맞춤형 애플리케이션 탐지기에서 사용자 정의 애플리케이션을 설정합니다.

사업 타당성

조직의 비즈니스 운영(레크리에이션과 반대) 상황 내에서 애플리케이션이 사용될 가능성(**Very High(**매우 높음**)**, **High(**높음**)**, **Medium(**중간**)**, **Low(**낮음**)** 또는 **Very Low(**매우 낮음**)**)입니다. 애플리케이션에 가장 알맞은 옵션을 선택합니다.

범주

가장 중요한 기능을 설명하는 일반 애플리케이션 분류

설명

애플리케이션에 대한 설명입니다.

이름

애플리케이션의 이름입니다.

위험

애플리케이션이 조직의 보안 정책과 상반되는 용도로 사용될 가능성(**Very High(**매우 높음**)**, **High(**높음**)**, **Medium(**중간**)**, **Low(**낮음**)** 또는 **Very Low(**매우 낮음**)**)입니다. 애플리케이션에 가장 알맞은 옵션을 선택합니다.

태그

애플리케이션에 관한 추가 정보를 제공하는, 하나 이상의 미리 정의된 태그입니다. 애플리케이션이 액티브 인증에서 면제될 수 있게 하려면(ID 규칙에서 설정되게 하려면), **User-Agent Exclusion**(사용자-에이전트 제외) 태그를 애플리케이션에 추가해야 합니다.

맞춤형 애플리케이션 탐지기 설정

기본 또는 고급 맞춤형 애플리케이션 탐지기를 설정할 수 있습니다.

프로시저

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

단계 **2** **Create a Custom Detector**(맞춤형 탐지기 생성)를 클릭합니다.

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

단계 **4** **Application Protocol**(애플리케이션 프로토콜)을 선택합니다. 다음 옵션을 이용할 수 있습니다.

- 기존 애플리케이션 프로토콜에 대한 탐지기를 생성하는 경우(예: 비표준 포트에서 특정 애플리케이션 프로토콜을 탐지하려는 경우), 드롭다운 목록에서 애플리케이션 프로토콜을 선택합니다.
- 사용자 정의 애플리케이션에 대한 탐지기를 생성하는 경우에는 사용자 정의 애플리케이션 생성, 13 페이지에서 설명하는 절차를 따르십시오.

단계 **5** **Detector Type**(탐지기 유형)을 선택합니다.

단계 **6** **OK**(확인)를 클릭합니다.

단계 **7** 탐지 패턴 또는 탐지 기준 또는 암호화된 가시성 엔진 프로세스 할당을 구성합니다.

- 기본 탐지기를 설정하는 경우에는, 기본 탐지기에서 탐지 패턴 지정, 14 페이지에 설명된 대로 미리 설정한 **Detection Patterns**(탐지 패턴)를 지정합니다.
- 고급 탐지기를 설정하는 경우에는, 고급 탐지기에서 탐지 기준 지정, 15 페이지에 설명된 대로 맞춤형 **Detection Criteria**(탐지 기준)를 지정합니다.
- EVE(Encrypted Visibility Engine) 탐지기를 구성하는 경우 EVE 프로세스 할당 지정, 16 페이지에 설명된 대로 맞춤형 EVE 프로세스 할당을 지정합니다.

  주의 고급 맞춤형 탐지기는 복잡하며 유효한 .lua 파일을 구성하는 방법을 알아야 합니다. 잘못 설정된 탐지기는 성능이나 탐지 기능에 악영향을 줄 수 있습니다.

단계 **8** 원한다면 **Packet Captures**(패킷 캡처)를 이용해 맞춤형 애플리케이션 프로토콜 탐지기 테스트, 17 페이지에 설명된 대로 새 탐지기를 테스트합니다.

단계 **9** **Save**(저장)를 클릭합니다.

참고 애플리케이션을 액세스 컨트롤 규칙에 포함하면 탐지기가 자동으로 활성화되며, 사용 중인 동안에는 비활성화할 수 없습니다.

다음에 수행할 작업

- 탐지기 활성화 및 비활성화, 20 페이지에 설명된 대로 탐지기를 활성화합니다.

관련 항목

맞춤형 애플리케이션 탐지기 및 사용자 정의 애플리케이션 필드, 8 페이지

사용자 정의 애플리케이션 생성

여기서 생성하는 애플리케이션, 카테고리 및 태그는 액세스 컨트롤 규칙과 애플리케이션 필터 개체 관리자에서도 사용할 수 있습니다.

⚠

주의 사용자 정의 애플리케이션을 생성하면 구축 단계를 거치지 않고 Snort 프로세스가 바로 재시작합니다. 시스템은 계속 진행하면 모든 매니지드 디바이스에서의 Snort 프로세스가 재시작한다고 경고합니다. 재시작은 현재 도메인 또는 현재 도메인의 하위 도메인에 있는 모든 매니지드 디바이스에서 진행됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort 재시작 트래픽 동작을 참고하십시오.

시작하기 전에

- 맞춤형 애플리케이션 탐지기 설정, 12 페이지에 설명된 대로 맞춤형 애플리케이션 프로토콜 탐지기 설정을 시작합니다.

프로시저

단계 **1** Create Detector(탐지기 생성) 페이지에서 **Add(**추가**)**를 클릭합니다.

단계 **2** **Name(**이름**)**을 입력합니다.

단계 **3** **Description(**설명**)**을 입력합니다.

단계 **4** **Business Relevance(**사업 타당성**)**를 선택합니다.

단계 **5** **Risk(**위험**)**를 선택합니다.

단계 **6** 카테고리를 추가하려면 Categories 옆에 있는 **Add(**추가**)**를 클릭하고 새 카테고리 이름을 입력하거나, **Categories(**카테고리**)** 드롭다운 목록에서 기존 카테고리를 선택합니다.

단계 **7** 선택 사항으로, 태그를 추가하려면 Tags(태그) 옆에 있는 **Add(**추가**)**를 클릭하고 새 태그 이름을 입력하거나 **Tags(**태그**)** 드롭다운 목록에서 기존 태그를 선택합니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 맞춤형 애플리케이션 탐지기 설정, 12 페이지에 설명된 대로 맞춤형 애플리케이션 프로토콜 탐지기 설정을 계속 진행합니다. 시스템이 탐지기를 이용해 트래픽을 분석하려면 먼저 탐지기를 저장하고 활성화해야 합니다.

관련 항목

맞춤형 애플리케이션 탐지기 및 사용자 정의 애플리케이션 필드, 8 페이지

기본 탐지기에서 탐지 패턴 지정

특정 패턴 문자열의 애플리케이션 프로토콜 패킷 헤더를 검색하도록 맞춤형 애플리케이션 프로토콜 탐지기를 설정할 수 있습니다. 여러 패턴을 검색하도록 탐지기를 구성할 수도 있습니다. 이 경우 애플리케이션 프로토콜을 긍정적으로 식별하려면 애플리케이션 프로토콜 트래픽은 탐지기에 대한 모든 패턴을 매칭해야 합니다.

애플리케이션 프로토콜 탐지기는 ASCII 또는 16진수 패턴을 검색할 수 있습니다(임의의 오프셋 사용).

시작하기 전에

- 맞춤형 애플리케이션 탐지기 설정, 12 페이지에 설명된 대로 맞춤형 애플리케이션 프로토콜 탐지기 설정을 시작합니다.

프로시저

단계 **1** Detection Patterns(탐지 패턴) 섹션의 Create Detector(탐지기 생성) 페이지에서 **Add(**추가**)**를 클릭합니다.

단계 **2** 탐지기가 검사해야 하는 트래픽의 **Protocol(**프로토콜**)**을 선택합니다.

단계 **3** 탐지할 패턴 **Type(**유형**)**을 지정합니다.

단계 **4** 지정한 **Type(**유형**)**과 일치하는 **Pattern String(**패턴 문자열**)**을 입력합니다.

단계 **5** 원한다면 **Offset(**오프셋**)**을 입력합니다(단위: 바이트).

단계 **6** 사용하는 포트를 기준으로 애플리케이션 프로토콜 트래픽을 식별하려면 **Port(s)(**포트**)** 필드에 1~65535 범위의 포트를 입력합니다. 여러 포트를 사용하려면 쉼표로 구분합니다.

단계 **7** 원한다면 **Direction(**방향**)**을 선택합니다. **`Client(`**클라이언트**`)`** 또는 **`Server(`**서버**`)`**를 선택할 수 있습니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

팁 패턴을 삭제하려면 삭제할 패턴 옆에 있는 **Delete(**삭제**)** ( )을 클릭합니다.

다음에 수행할 작업

- 맞춤형 애플리케이션 탐지기 설정, 12 페이지에 설명된 대로 맞춤형 애플리케이션 프로토콜 탐지기 설정을 계속 진행합니다. 시스템이 탐지기를 이용해 트래픽을 분석하려면 먼저 탐지기를 저장하고 활성화해야 합니다.

관련 항목

고급 탐지기에서 탐지 기준 지정, 15 페이지

고급 탐지기에서 탐지 기준 지정

주의 고급 맞춤형 탐지기는 복잡하며 유효한 .lua 파일을 구성하는 방법을 알아야 합니다. 잘못 설정된 탐지기는 성능이나 탐지 기능에 악영향을 줄 수 있습니다.

주의 신뢰할 수 없는 소스의 .lua 파일을 업로드하지 마십시오.

맞춤형.lua 파일은 맞춤형 애플리케이션 탐지기 설정을 포함합니다. 맞춤형 .lua 파일을 생성하려면 lua 프로그래밍 언어를 잘 알고 Cisco의 C-lua API에 익숙해야 합니다. Cisco는 다음을 이용해 .lua 파일을 준비할 것을 적극 권장합니다.

- lua 프로그래밍 언어에 대한 서드파티 지침 및 참조 자료
- 오픈 소스 탐지기 개발자 안내서: https://www.snort.org/downloads
- OpenAppID Snort 커뮤니티 리소스: http://blog.snort.org/search/label/openappid

참고 시스템은 시스템 호출이나 파일 I/O를 참조하는 .lua 파일은 지원하지 않습니다.

시작하기 전에

- 맞춤형 애플리케이션 탐지기 설정, 12 페이지의 설명에 따라 사용자 정의 애플리케이션 프로토콜 탐지기 설정을 시작합니다.
- 비교 가능한 탐지기에 대한 .lua 파일을 다운로드하고 조사해 유효한 .lua 파일 생성을 준비합니다. 탐지기 파일 다운로드에 관한 자세한 내용은 탐지기 상세정보 보기 또는 다운로드, 18 페이지 섹션을 참조하십시오.
- 맞춤형 애플리케이션 탐지기 설정을 포함하는 유효한 .lua 파일을 생성합니다.

프로시저

단계 **1** Detection Criteria(탐지 기준) 섹션에 있는 고급 맞춤형 애플리케이션 탐지기의 Create Detector(탐지기 생성) 페이지에서 **Add(추가)**를 클릭합니다.

단계 **2** **Browse...(찾기...)**를 클릭해 **.lua** 파일로 이동하고 파일을 다운로드합니다.

단계 **3** **OK(확인)**를 클릭합니다.

다음에 수행할 작업

- 맞춤형 애플리케이션 탐지기 설정, 12 페이지에 설명된 대로 맞춤형 애플리케이션 프로토콜 탐지기 설정을 계속 진행합니다. 시스템이 탐지기를 이용해 트래픽을 분석하려면 먼저 탐지기를 저장하고 활성화해야 합니다.

관련 항목

기본 탐지기에서 탐지 패턴 지정, 14 페이지

EVE 프로세스 할당 지정

EVE(암호화된 가시성 엔진)에서 탐지한 프로세스를 신규 또는 기존 애플리케이션에 매핑하도록 맞춤형 애플리케이션 탐지기를 구성할 수 있습니다.

시작하기 전에

- 맞춤형 애플리케이션 탐지기 설정, 12 페이지에 설명된 대로 맞춤형 애플리케이션 프로토콜 탐지기 설정을 시작합니다.

프로시저

단계 **1** Create Detector(탐지기 생성) 페이지의 Encrypted Visibility Engine Process Assignments(암호화된 가시성 엔진 프로세스 할당) 섹션에서 **Add(추가)**를 클릭합니다.

단계 **2** **Process Name(프로세스 이름)** 및 **Minimum Process Confidence(최소 프로세스 신뢰도)** 값을 입력합니다.

참고 **Process Name(프로세스 이름)** 필드에 텍스트를 입력할 수 있으며 대/소문자를 구분합니다. 값은 EVE에서 탐지한 정확한 프로세스 이름과 일치해야 합니다. **Minimum Process Confidence(최소 프로세스 신뢰도)**는 0~100의 숫자일 수 있습니다. 이는 Connection Events(연결 이벤트)의 **Encrypted Visibility Process Confidence Score(암호화된 가시성 프로세스 신뢰도 점수)** 필드에 표시되는 숫자입니다.

Encrypted Visibility Process Confidence Score(암호화된 가시성 프로세스 신뢰도 점수) 필드에 대한 자세한 내용은 Cisco Firepower Management Center 관리 가이드의 연결 및 보안 인텔리전스 이벤트 필드 섹션을 참조하십시오.

단계 **3** **Save(**저장**)**를 클릭합니다.

단계 **4** Application Detector(애플리케이션 탐지기) 목록 페이지에서 생성한 탐지기를 활성화합니다. 자세한 내용은 탐지기 활성화 및 비활성화, 20 페이지를 참고하십시오. 탐지기를 활성화하면 탐지기 파일이 FMC에 등록된 모든 FTD에 푸시됩니다.

다음에 수행할 작업

- 맞춤형 애플리케이션 탐지기 설정, 12 페이지에 설명된 대로 맞춤형 애플리케이션 프로토콜 탐지기 설정을 계속 진행합니다. 시스템이 탐지기를 이용해 트래픽을 분석하려면 먼저 탐지기를 저장하고 활성화해야 합니다.

맞춤형 애플리케이션 프로토콜 탐지기 테스트

탐지하려는 애플리케이션 프로토콜에서 온 트래픽의 패킷을 포함하는 패킷 캡처(pcap) 파일이 있는 경우 pcap 파일을 기준으로 맞춤형 애플리케이션 프로토콜 탐지기를 테스트할 수 있습니다. Cisco는 불필요한 트래픽이 없는 단순하고 깔끔한 pcap 파일 사용을 권장합니다.

Pcap 파일은 256KB 이하여야 합니다. 그보다 큰 pcap 파일을 기준으로 탐지기를 테스트하면, management center은(는) 파일을 자동으로 자른 다음 불완전한 파일을 테스트합니다. 파일을 이용해 탐지기를 테스트하려면 먼저 pcap에 있는 해결되지 않은 체크섬을 수정해야 합니다.

시작하기 전에

- 맞춤형 애플리케이션 탐지기 설정, 12 페이지에 설명된 대로 맞춤형 애플리케이션 프로토콜 탐지기를 설정합니다.

프로시저

단계 **1** Packet Captures(패킷 캡처) 섹션의 Create Detector(탐지기 생성) 페이지에서 **Add(**추가**)**를 클릭합니다.

단계 **2** 팝업 윈도우에서 pcap 파일을 찾아 **OK(**확인**)**를 클릭합니다.

단계 **3** pcap 파일의 내용을 기준으로 탐지기를 테스트하려면 pcap 파일 옆에 있는 Evaluate(평가)를 클릭합니다. 테스트의 성공 여부를 나타내는 메시지가 표시됩니다.

단계 **4** 선택적으로, 추가 pcap 파일을 기준으로 탐지기를 테스트하려면 1~3단계를 반복합니다.

팁 pcap 파일을 삭제하려면 삭제할 파일 옆에 있는 **Delete(**삭제**)** ( )를 클릭합니다.

다음에 수행할 작업

- 맞춤형 애플리케이션 탐지기 설정, 12 페이지에 설명된 대로 맞춤형 애플리케이션 프로토콜 탐지기 설정을 계속 진행합니다. 시스템이 탐지기를 이용해 트래픽을 분석하려면 먼저 탐지기를 저장하고 활성화해야 합니다.

탐지기 상세정보 보기 또는 다운로드

탐지기 목록을 사용하여 애플리케이션 탐지기 상세정보(모든 탐지기에 해당)를 확인하고 탐지기 상세정보를 다운로드할 수 있습니다(맞춤형 애플리케이션 탐지기에만 해당).

프로시저

단계 **1** 애플리케이션 탐지기 상세정보를 확인하려면 다음 하나를 수행하십시오.

- https://www.cisco.com/c/en/us/support/security/defense-center/products-technical-reference-list.html에서 관련 VDB 버전에 대한 *Cisco Firepower* 애플리케이션 탐지기 참조를 확인하십시오.
- a. **Policies(**정책**)** > **Application Detectors(**애플리케이션 탐지기**)**을(를) 선택합니다.

  b. 목록을 필터링해 특정 탐지기를 찾습니다.

  c. 클릭합니다. **Information(**정보**)** (ⓘ)

단계 **2** 맞춤형 애플리케이션 탐지기에 대한 탐지기 세부 사항을 다운로드하려면 **Download(**다운로드**)** (⬇)를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 설정이 상위 도메인에 속하거나 필요한 권한이 없는 것입니다.

탐지기 목록 정렬

기본적으로 Detectors(탐지기) 페이지에는 탐지기가 이름별 알파벳순으로 나열됩니다. 열 제목 옆에 있는 위쪽 또는 아래쪽 화살표는 페이지가 해당 방향에서 해당 열을 기준으로 정렬된다는 것을 나타냅니다.

프로시저

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

단계 **2** 적절한 컬럼 헤드를 클릭합니다.

탐지기 목록 필터링

프로시저

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

단계 **2** 탐지기 목록에 대한 필터 그룹, 19 페이지에서 설명하는 필터 그룹 중 하나를 확장하고 필터 옆에 있는 확인란을 선택합니다. 그룹의 모든 필터를 선택하려면 그룹 이름을 마우스 오른쪽 버튼으로 클릭하고 **Check All(**모두 선택**)**을 선택합니다.

단계 **3** 필터를 제거하려면 **Filters(**필터**)** 필드의 필터 이름에서 **Remove(**제거**)** (✕)를 클릭하거나 필터 목록에서 필터를 비활성화합니다. 그룹의 모든 필터를 제거하려면 그룹 이름을 마우스 오른쪽 버튼으로 클릭하고 **Uncheck All(**모두 선택 해제**)**을 선택합니다.

단계 **4** 필터를 모두 제거하려면, 탐지기에 적용된 목록 옆에 있는 **Clear all(**모두 선택 취소**)**을 클릭합니다.

탐지기 목록에 대한 필터 그룹

탐지기 목록을 필터링할 때는 여러 필터 그룹을 독립적으로나 조합해서 사용할 수 있습니다.

이름

입력한 문자열이 들어 있는 이름이나 설명의 탐지기를 찾습니다. 문자열은 영숫자나 특수 문자를 포함할 수 있습니다.

사용자 지정 필터

개체 관리 페이지에서 생성된 맞춤형 애플리케이션 필터와 일치하는 탐지기를 찾습니다.

작성자

탐지기를 생성한 사용자에 따라 탐지기를 찾습니다. 탐지기를 다음 기준으로 필터링할 수 있습니다.

- 맞춤형 탐지기를 생성하거나 가져온 개별 사용자
- Cisco - Cisco가 제공한 모든 탐지기를 나타냅니다. 단, 개별적으로 가져온 애드온 탐지기는 예외입니다(탐지기를 가져온 사용자는 탐지기의 작성자가 됩니다).
- **Any User** 0 Cisco에서 제공하지 않은 모든 탐지기를 나타냅니다.

주/도

상태(**Active** 또는 **Inactive**)에 따라 탐지기를 찾습니다.

유형

애플리케이션 탐지기 기초, 2 페이지에서 설명하는 것처럼 탐지기 유형에 따라 탐지기를 찾습니다.

프로토콜

탐지기가 검사하는 트래픽 프로토콜에 따라 탐지기를 찾습니다.

카테고리

탐지하는 애플리케이션에 할당된 카테고리에 따라 탐지기를 찾습니다.

태그

탐지하는 애플리케이션에 할당된 태그에 따라 탐지기를 찾습니다.

위험

탐지하는 애플리케이션에 할당된 위험(**Very High(**매우 높음**)**, **High(**높음**)**, **Medium(**중간**)**, **Low(**낮음**)** 및 **Very Low(**매우 낮음**)**에 따라 탐지기를 찾습니다.

사업 타당성

탐지하는 애플리케이션에 할당된 비즈니스 연관성(**Very High(**매우 높음**)**, **High(**높음**)**, **Medium(**중간**)**, **Low(**낮음**)** 및 **Very Low(**매우 낮음**)**에 따라 탐지기를 찾습니다.

다른 탐지기 페이지로 이동

프로시저

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

단계 **2** 다음 페이지를 보려면 **Right Arrow(**오른쪽 화살표**)** (>)을 클릭합니다.

단계 **3** 이전 페이지를 보려면 **Left Arrow(**왼쪽 화살표**)** (<)을 클릭합니다.

단계 **4** 다른 페이지를 보려면 페이지 번호를 입력하고 Enter를 누릅니다.

단계 **5** 마지막 페이지로 이동하려면 **Right End Arrow(**오른쪽 끝 화살표**)** (>|)을 클릭합니다.

단계 **6** 첫 페이지로 이동하려면 **Left End Arrow(**왼쪽 끝 화살표**)** (|<)을 클릭합니다.

탐지기 활성화 및 비활성화

네트워크 트래픽 분석에 사용할 수 있으려면 탐지기를 먼저 활성화해야 합니다. 기본적으로 모든 Cisco 제공 탐지기는 활성화되어 있습니다.

시스템의 탐지 기능을 보완하기 위해 포트마다 여러 애플리케이션 탐지기를 활성화할 수 있습니다.

정책의 액세스 제어 규칙에 애플리케이션이 포함되어 있고 정책이 구축될 때 해당 애플리케이션에 대한 활성 탐지기가 없으면 하나 이상의 탐지기가 자동으로 활성화됩니다. 마찬가지로, 구축된 정책에서 애플리케이션이 사용 중일 때 탐지기를 비활성화하여 해당 애플리케이션에 대한 활성 탐지기가 없어지면 탐지기를 비활성화할 수 없습니다.

팁 성능을 높이려면 사용하지 않을 애플리케이션 프로토콜, 클라이언트 또는 웹 애플리케이션 탐지기를 비활성화하십시오.

주의 맞춤형 애플리케이션 탐지기를 활성화하거나 비활성화하면 구축 프로세스를 거치지 않고 Snort 프로세스가 바로 재시작됩니다. 시스템은 계속 진행하면 모든 매니지드 디바이스에서의 Snort 프로세스가 재시작한다고 경고합니다. 재시작은 현재 도메인 또는 현재 도메인의 하위 도메인에 있는 모든 매니지드 디바이스에서 진행됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort 재시작 트래픽 동작을 참고하십시오.

프로시저

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

단계 **2** 활성화하거나 비활성화할 탐지기 옆에 있는 슬라이더를 클릭합니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

참고 일부 애플리케이션 탐지기는 다른 탐지기에 필요합니다. 이러한 탐지기 중 하나를 비활성화하면 여기에 의존하는 탐지기도 비활성화됨을 알리는 경고가 나타납니다.

맞춤형 애플리케이션 탐지기 편집

다음 절차를 이용해 맞춤형 애플리케이션 탐지기를 수정하십시오.

프로시저

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

단계 **2** 수정할 탐지기 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다. **View(**보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 맞춤형 애플리케이션 탐지기 설정, 12 페이지에 설명된 대로 탐지기를 변경합니다.

단계 **4** 탐지기의 상태에 따라 다음 저장 옵션을 사용할 수 있습니다.

- 비활성 탐지기를 저장하려면 **Save(**저장**)**를 클릭합니다.
- 비활성 탐지기를 새로운 비활성 탐지기로 저장하려면 **Save as New(**새 탐지기로 저장**)**를 클릭합니다.
- 활성 탐지기를 저장하고 바로 사용하려면 **Save and Reactivate(**저장 및 재활성화**)**를 클릭합니다.

  주의 사용자 정의 애플리케이션 탐지기를 저장하고 재활성화하면 구축 프로세스를 거치지 않고 Snort 프로세스가 바로 재시작됩니다. 시스템은 계속 진행하면 모든 매니지드 디바이스에서의 Snort 프로세스가 재시작한다고 경고합니다. 재시작은 현재 도메인 또는 현재 도메인의 하위 도메인에 있는 모든 매니지드 디바이스에서 진행됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort 재시작 트래픽 동작을 참고하십시오.

- 활성 탐지기를 새로운 비활성 탐지기로 저장하려면 **Save as New(**새 탐지기로 저장**)**를 클릭합니다.

탐지기 삭제

맞춤형 탐지기는 물론 Cisco Professional Services에서 제공한 추가 탐지기도 개별적으로 삭제할 수 있습니다. 다른 Cisco 제공 탐지기는 삭제할 수 없지만, 이중 다수는 비활성화할 수 있습니다.

참고 구축된 정책에서 탐지기를 사용하는 경우에는, 해당 탐지기를 삭제할 수 없습니다.

주의 활성화된 사용자 정의 애플리케이션 탐지기를 삭제하면 구축 프로세스를 거치지 않고 Snort 프로세스가 바로 재시작됩니다. 시스템은 계속 진행하면 모든 매니지드 디바이스에서의 Snort 프로세스가 재시작한다고 경고합니다. 재시작은 현재 도메인 또는 현재 도메인의 하위 도메인에 있는 모든 매니지드 디바이스에서 진행됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort 재시작 트래픽 동작을 참고하십시오.

프로시저

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

단계 **2** 삭제할 탐지기 옆에 있는 **Delete(**삭제**)** ( )를 클릭합니다. **View(**보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** **OK(**확인**)**를 클릭합니다.