외부 툴을 사용하여 이벤트 분석

Cisco SecureX와의 통합

단일한 보안 창인 SecureX 클라우드 포털을 통해 모든 Cisco 보안 제품의 데이터를 보고 작업할 수 있습니다. SecureX를 통해 제공되는 툴을 사용하여 위협 추적 및 조사 등을 강화하십시오.

SecureX에 대한 자세한 내용은 http://www.cisco.com/c/en/us/products/security/securex.html의 내용을 참조하십시오.

Firepower를 SecureX와 통합하려면 https://cisco.com/go/firepower-securex-documentation에 있는 *Firepower* 및 *SecureX* 통합 가이드를 참조하십시오.

다음을 이용한 이벤트 분석 Cisco SecureX Threat Response

Cisco SecureX Threat Response는 이전에는 CTR (Cisco Threat Response)로 알려졌습니다.

Firepower를 포함해 여러 제품에서 집계한 데이터를 사용하여 인시던트를 분석할 수 있는, Cisco Cloud의 통합 플랫폼인 Cisco SecureX Threat Response을(를) 사용하여 위협을 빠르게 탐지하고, 조사하고 응답할 수 있습니다.

- Cisco SecureX Threat Response에 대한 일반 정보는 다음을 참조하십시오

  https://www.cisco.com/c/en/us/products/security/threat-response.html.

- Cisco SecureX Threat Response과 Firepower 통합에 대한 자세한 지침은 다음을 참조하십시오.
- https://cisco.com/go/firepower-ctr-integration-docs의 *Firepower* 및 *Cisco SecureX Threat Response* 통합 가이드.

Cisco SecureX Threat Response에서 이벤트 데이터 보기

시작하기 전에

- https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html의 *Firepower* 및 *Cisco SecureX Threat Response* 통합 가이드의 설명과 같이 통합을 설정합니다.
- Cisco SecureX Threat Response의 온라인 도움말을 검토해 위협을 찾고, 조사하고, 조치하는 방법을 확인하십시오.
- Cisco SecureX Threat Response에 액세스하려면 자격 증명이 필요합니다.

프로시저

단계 **1** Firepower Management Center에서 다음 중 하나를 수행합니다.

- 특정 이벤트에서 Cisco SecureX Threat Response(으)로 피벗하는 방법:

  a. **Analysis(분석) > Intrusions(침입)** 메뉴에서 지원되는 이벤트를 나열하는 페이지로 이동합니다.

  b. 소스 또는 대상 IP 주소를 마우스 오른쪽 버튼으로 클릭하고 **View in SecureX(SecureX**에서 보기**)**를 선택합니다.

- 일반적인 이벤트 정보 확인 방법:

  a. **System(**시스템**) > Integrations(**통합**) > Cloud Services(**클라우드 서비스**)**로 이동합니다.

  b. 링크를 클릭해 Cisco SecureX Threat Response의 이벤트를 확인합니다.

단계 **2** 메시지가 표시되면 Cisco SecureX Threat Response에 로그인합니다.

웹 기반 리소스를 사용한 이벤트 조사

상황별로 크로스 실행 기능을 사용하면 Firepower Management Center 외부에 있는 웹 기반 리소스의 잠재 위협에 관한 자세한 정보를 빠르게 확인할 수 있습니다. 예를 들어 다음 작업을 할 수 있습니다.

- 알려졌거나 의심스러운 위협에 관한 정보를 게시하는, Cisco 또는 서드파티 클라우드가 호스트한 서비스에서 의심스러운 소스 IP 주소를 조회합니다.

- 조직의 기록 로그에서 특정 위협의 과거 인스턴스를 찾습니다(조직이 해당 데이터를 SIEM(Security Information and Event Management) 애플리케이션에 저장하는 경우).
- 파일 경로 정보를 포함한 특정 파일 관련 정보를 찾습니다(조직이 Cisco AMP for Endpoints를 구축한 경우).

이벤트를 조사할 때, Firepower Management Center의 이벤트 뷰어나 대시보드에서 이벤트를 클릭하면 외부 리소스의 관련 정보로 바로 이동할 수 있습니다. 이렇게 하면 특정 이벤트 관련 정보를 해당 이벤트의 IP 주소, 포트, 프로토콜, 도메인 및 SHA 256 해시를 기반으로 빠르게 수집할 수 있습니다.

예를 들어 Top Attackers(상위 공격자) 대시보드 위젯을 찾는 중이며, 나열된 소스 IP 주소 중 하나에 관한 자세한 정보를 찾고 싶다고 가정하겠습니다. Talos가 이 IP 주소에 대해 게시하는 정보를 봐야 하니, "Talos IP" 리소스를 선택합니다. Talos 웹 사이트가 이 특정 IP 주소 관련 정보가 있는 페이지를 엽니다.

Cisco와 서드파티 위협 정보 서비스에 대한 사정 정의된 링크 모음에서 하나를 선택하고, 맞춤형 링크를 다른 웹 기반 서비스에 추가하고, SIEM 또는 웹 인터페이스가 있는 다른 제품에 추가합니다. 일부 리소스는 계정 또는 제품 구매를 요구할 수도 있습니다.

상황별 크로스 실행 리소스 관리 정보

Analysis(분석) > Advanced(고급) > Contextual Cross-Launch(상황별 크로스 실행) 페이지를 이용해 외부 웹 기반 리소스를 관리합니다.

예외: 다음에 대한 교차 실행 링크 설정 Stealthwatch, 6 페이지의 절차에 따라 Stealthwatch 어플라이언스에 대한 교차 실행 링크를 관리합니다.

Cisco가 제공하는 사정 정의된 리소스에는 Cisco 로고가 표시됩니다. 나머지 링크는 서드파티 리소스입니다.

필요 없는 리소스는 비활성화하거나 삭제할 수 있으며, 이름을 변경할 수도 있습니다. 리소스가 목록 맨 아래에 정렬되도록 소문자 "z"로 시작하는 이름을 지정하는 식입니다. 교차 실행 리소스를 비활성화하면 모든 사용자에 대해 비활성화됩니다. 삭제한 리소스는 다시 설치할 수 없지만 다시 만들 수는 있습니다.

리소스를 추가하려면 상황별 크로스 실행 리소스 추가, 4 페이지 섹션을 참조하십시오.

맞춤형 상황별 크로스 실행 리소스 요구 사항

맞춤형 상황별로 크로스 실행 리소스를 추가하는 경우:

- 웹 브라우저를 통해 리소스를 액세스할 수 있어야 합니다.
- Http 및 https 프로토콜만 지원됩니다.
- GET 요청만 지원됩니다. POST 요청은 지원되지 않습니다.
- URL의 변수 인코딩은 지원되지 않습니다. IPv6 주소는 콜론 구분자 인코딩을 요구할 수 있지만, 대부분의 서비스는 이러한 인코딩을 요구하지 않습니다.
- 사전 정의된 리소스를 포함한 리소스를 100개까지 설정할 수 있습니다.

- 교차 실행을 생성하려면 관리자 또는 보안 분석가 사용자여야 하지만 읽기 전용 보안 분석가로 사용할 수도 있습니다.

상황별 크로스 실행 리소스 추가

보안 인텔리전스 서비스나 SIEM(Security Information and Event Management) 툴 같은 상황별로 크로스 실행 리소스를 추가할 수 있습니다.

다중 도메인 구축의 경우, 상위 도메인의 리소스는 보고 사용할 수 있지만 현재 도메인의 리소스는 생성 및 편집만 할 수 있습니다. 전체 도메인의 총 리소스 수는 100개로 제한됩니다.

시작하기 전에

- Stealthwatch 어플라이언스에 링크를 추가하는 경우 이 절차를 생략하고 다음에 대한 교차 실행 링크 설정 Stealthwatch, 6 페이지의 내용을 참조하십시오..
- 맞춤형 상황별 크로스 실행 리소스 요구 사항, 3 페이지의 내용을 참조하십시오.
- 링크할 리소스에 필요하다면, 계정과 액세스에 필요한 자격 증명을 생성 또는 획득합니다. 선택적으로, 액세스가 필요한 각 사용자에게 자격 증명을 할당하고 배포합니다.
- 링크할 리소스에 대한 쿼리 링크의 구문을 확인합니다.

  브라우저를 통해 리소스에 액세스하고, 필요에 따라 해당 리소스에 대한 문서를 사용하여 쿼리 링크가 찾아야 할 정보 유형(예 IP 주소)의 샘플을 검색하는 데 필요한 쿼리 링크를 작성합니다

  쿼리를 실행하고 브라우저의 위치 표시줄에서 결과 URL을 복사합니다.

  예를 들어 쿼리 URL이 **`https://www.talosintelligence.com/reputation_center/lookup?search=10.10.10.10`**일 수 있습니다.

프로시저

단계 **1** **Analysis(**분석**) > Advanced(**고급**) > Contextual Cross-Launch(**상황별 크로스 실행**)**를 선택합니다.

단계 **2** **New Cross-Launch(**새 크로스 실행**)**를 클릭합니다.

표시되는 양식에서, 별표가 있는 필드는 값을 입력해야 합니다.

단계 **3** 고유한 리소스 이름을 입력합니다.

단계 **4** 리소스의 작업 URL 문자열을 복사해 **URL Template(URL** 템플릿**)** 필드에 붙여넣습니다.

단계 **5** 쿼리 문자열의 특정 데이터(IP 주소 등)를 적절한 변수로 교체합니다. 커서를 놓은 다음 변수(예: **ip**)를 한 번 클릭하여 변수를 삽입합니다.

위의 "Before You Begin(시작하기 전에)" 색션에서, 결과 URL은 **`https://www.talosintelligence.com/reputation_center/lookup?search={ip}`**일 것입니다. 상황별로 크로스 실행 링크를 사용하는 경우, URL의 {ip} 변수는 이벤트 뷰어 또는 대시보드에서 사용자가 오른쪽 클릭한 IP 주소로 교체됩니다.

각 변수에 대한 설명을 보려면 커서를 변수 위에 올리십시오.

하나의 툴이나 서비스로 여러 상황별로 크로스 실행 링크를 만들 수 있으며, 이 경우 각 항목에 다른 변수를 사용해야 합니다.

단계 **6** 예시 데이터로 링크를 테스트하려면 예제 데이터를 사용한 테스트( )을 클릭합니다.

단계 **7** 문제를 해결합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

상황별 크로스 실행을 이용한 이벤트 조사

시작하기 전에

액세스하는 리소스가 자격 증명을 요구하는 경우, 해당 자격 증명이 있는지 확인하십시오.

프로시저

단계 **1** 이벤트를 표시하는 Firepower Management Center의 다음 페이지 중 하나로 이동합니다.

- 대시보드(**Overview(**개요**) > Dashboards(**대시보드**)**) 또는
- 이벤트 뷰어 페이지(이벤트의 테이블을 포함하는 **Analysis(**분석**)** 메뉴의 아무 메뉴 옵션)

단계 **2** 관심 있는 이벤트를 오른쪽 클릭하고 사용할 상황별로 크로스 실행 리소스를 선택합니다.

필요한 경우 콘텍스트 메뉴를 내려 사용할 수 있는 옵션을 모두 확인합니다

오른쪽 클릭한 데이터 유형에 따라 표시되는 옵션이 달라집니다. 예를 들어 IP 주소를 오른쪽 클릭하면 IP 주소 관련 상황별로 크로스 실행 옵션만 표시됩니다.

따라서 예를 들어 Cisco Talos에서 Top Attackers(상위 공격자) 대시보드 위젯의 소스 IP 주소 관련 위협 정보를 얻으려면, **Talos SrcIP** 또는 **Talos IP**를 선택합니다.

리소스에 여러 변수가 있는 경우, 해당 리소스를 선택하는 옵션은 포함된 각 변수에 대한 단일 유효 값이 있는 이벤트에서만 사용할 수 있습니다.

별도의 브라우저 창에 상황별로 크로스 실행 리소스가 열립니다.

쿼리하는 데이터 양, 리소스의 속도 및 요구 등의 요소에 따라 쿼리 처리에 시간이 오래 걸릴 수도 있습니다.

단계 **3** 필요한 경우 리소스에 로그인합니다.

다음에 대한 교차 실행 링크 설정 **Stealthwatch**

Firepower의 이벤트 데이터에서 Stealthwatch 어플라이언스의 관련 데이터로 교차 실행할 수 있습니다. Stealthwatch 제품에 대한 자세한 내용은 https://www.cisco.com/c/en/us/products/security/security-analytics-logging/index.html의 내용을 참조하십시오.

상황별 교차 실행에 대한 일반적인 정보는 상황별 크로스 실행을 이용한 이벤트 조사, 5 페이지의 내용을 참조하십시오.

Stealthwatch 어플라이언스에 대한 일련의 교차 실행 링크를 빠르게 설정하려면 이 절차를 사용합니다.

참고

- 나중에 해당 링크를 변경해야 하는 경우 이 절차로 돌아갑니다. 상황별 교차 실행 목록 페이지에서는 직접 변경할 수 없습니다.
- 상황별 크로스 실행 리소스 추가, 4 페이지의 절차를 사용하여 Stealthwatch 어플라이언스에 교차 실행하는 추가 링크를 수동으로 생성할 수 있지만 해당 링크는 자동으로 생성된 리소스와 무관하므로 수동으로 관리(삭제, 업데이트 등)해야 합니다.

시작하기 전에

Stealthwatch 어플라이언스가 구축되어 실행되고 있어야 합니다.

Cisco Security Analytics 및 로깅(온프레미스) 을 사용하여 Stealthwatch 어플라이언스에 Firepower 데이터를 전송하려면 Stealthwatch 어플라이언스의 원격 데이터 스토리지의 내용을 참조하십시오.

프로시저

단계 **1** **System(**시스템**) > Logging(**로깅**) > Security Analytics & Logging(**보안 분석 및 로깅**)**을 선택합니다.

단계 **2** 기능을 활성화합니다.

단계 **3** Stealthwatch 어플라이언스의 호스트 이름이나 IP 주소, 포트를 입력합니다.

기본 포트는 443입니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

단계 **5** 새 교차 실행 링크를 확인합니다. **Analysis(**분석**) > Advanced(**고급**) > Contextual Cross-Launch(**상황별 교차 실행**)**를 선택합니다.

변경이 필요한 경우 이 절차로 돌아갑니다. 상황별 교차 실행 목록 페이지에서는 직접 변경할 수 없습니다.

다음에 수행할 작업

이벤트에서 Stealthwatch 이벤트 뷰어로 교차 실행하려면 Stealthwatch 자격 증명이 필요합니다.

FMC 이벤트 뷰어 또는 대시보드의 이벤트에서 교차 실행하려면 관련 이벤트의 테이블 셀을 마우스 오른쪽 버튼으로 클릭하고 적절한 옵션을 선택합니다.

쿼리하는 데이터 양, Stealthwatch 관리 콘솔의 속도 및 요구 등에 따라 쿼리를 처리하는 데 시간이 오래 걸릴 수도 있습니다.

Security Events(보안 이벤트)에 대한 시스템 로그 메시지 전송 정보

연결, 보안 인텔리전스, 침입, 파일 및 악성코드 이벤트 관련 데이터를 시스템 로그를 통해 SIEM(Security Information and Event Management) 툴 또는 에 전송할 수 있습니다.

때로는 이러한 이벤트를 Snort® 이벤트라고 지칭하기도 합니다.

보안 이벤트 데이터를 시스템 로그로 전송하는 시스템 설정 정보

보안 이벤트 시스템 로그를 전송하도록 시스템을 설정하려면, 다음 항목을 알고 있어야 합니다.

- 보안 이벤트 시스템 로그 메시지 구성 모범 사례, 7 페이지
- 보안 이벤트 시스템 로그에 대한 설정 위치, 12 페이지
- 보안 이벤트 Syslog 메시지에 적용되는 FTD 플랫폼 설정
- 정책에서 시스템 로그 설정을 변경하는 경우, 변경사항은 재구축해야 효력을 발휘합니다.

보안 이벤트 시스템 로그 메시지 구성 모범 사례

디바이스 및 버전	설정 위치
모두	시스템 로그를 사용하거나 이벤트를 외부에 저장하려는 경우, 정책 및 규칙 이름과 같은 개체 이름에 특수 문자를 사용하지 마십시오. 개체 이름은 수신 애플리케이션에서 구분자로 사용할 수 있는 특수 문자(예: 쉼표)를 포함해서는 안 됩니다.

디바이스 및 버전	설정 위치
Firepower Threat Defense	1. **Devices(**디바이스**) > Platform Settings(**플랫폼 설정**) > Threat Defense Settings(**위협 방어 설정**) > Syslog(**시스템 로그**)**에서 FTD 플랫폼 설정을 구성합니다. 보안 이벤트 Syslog 메시지에 적용되는 FTD 플랫폼 설정도 참조하십시오. 2. 액세스 컨트롤 정책 Logging(로깅) 탭에서, FTD 플랫폼 설정 사용을 선택합니다. 3. (침입 이벤트의 경우) 액세스 제어 정책 Logging(로깅) 탭의 설정을 사용하도록 침입 정책을 구성합니다. (기본값입니다.) 이런 설정을 재정의하는 것은 권장하지 않습니다. 자세한 내용은 FTD 디바이스에서 보안 이벤트 시스템 로그 메시지 보내기, 8 페이지의 내용을 참조하십시오.
기타 모든 디바이스	1. 알림 응답을 생성합니다. 2. 알림 응답을 사용하도록 액세스 제어 정책 Logging(로깅)을 설정합니다. 3. (침입 이벤트) 침입 정책에서 시스템 로그 설정을 구성합니다. 자세한 내용은 클래식 디바이스에서 보안 이벤트 시스템 로그 메시지 보내기, 11 페이지의 내용을 참조하십시오.

FTD 디바이스에서 보안 이벤트 시스템 로그 메시지 보내기

이 절차에서는 FTD 디바이스에서 보안 이벤트(연결, 보안 인텔리전스, 침입, 파일 및 악성코드 이벤트)에 대한 시스템 로그 메시지를 전송하기 위한 모범 사례 설정을 설명합니다.

참고 대부분의 FTD 시스템 로그 설정은 보안 이벤트에 적용되지 않습니다. 이 절차에 설명된 옵션만 설정하십시오.

시작하기 전에

- Firepower Management Center에서 보안 이벤트를 생성하도록 정책을 설정하고 표시될 것으로 예상되는 이벤트가 Analysis(분석) 메뉴의 해당 테이블에 나타나는지 확인합니다.
- 시스템 로그 서버 IP 주소, 포트 및 프로토콜(UDP 또는 TCP)을 수집합니다.
- 디바이스가 시스템 로그 서버에 연결할 수 있는지 확인합니다.
- 시스템 로그 서버가 원격 메시지를 수락할 수 있는지 확인합니다.

- 연결 로깅에 대한 중요 정보는 연결 로깅의 관련 챕터를 참조하십시오.

프로시저

단계 **1** FTD 디바이스에 대한 시스템 로그 설정을 구성합니다.

a) **Devices(**디바이스**) > Platform Settings(**플랫폼 설정**)**를 클릭합니다.
b) FTD 디바이스와 연결된 플랫폼 설정 정책을 편집합니다.
c) 왼쪽 탐색 창에서 시스템 로그를 클릭합니다.
d) **Syslog Servers(**시스템 로그 서버**)**를 클릭하고 **Add(**추가**)**를 클릭하여 서버, 프로토콜, 인터페이스 및 관련 정보를 입력합니다.

이 페이지의 옵션에 대한 질문이 있는 경우 Syslog 서버 설정을 참조하십시오.

e) **Syslog Settings(**시스템 로그 설정**)**를 클릭하고 다음 설정을 구성합니다.

- **Syslog** 메시지에서 타임스탬프 활성화
- 타임스탬프 형식
- **Syslog** 디바이스 **ID** 활성화

f) **Logging Setup(**로깅 설정**)**을 클릭합니다.
g) **Send syslogs in EMBLEM format(EMBLEM** 형식으로 시스템 로그 전송**)** 여부를 선택합니다.
h) 설정을 **Save(**저장**)**합니다.

단계 **2** 액세스 제어 정책(파일 및 악성코드 로깅 포함)에 대한 일반 로깅 설정을 구성합니다.

a) **Policies(**정책**) > Access Control(**액세스 제어**)**을 클릭합니다.
b) 해당 액세스 제어 정책을 편집합니다.
c) **Logging(**로깅**)**을 클릭합니다.
d) **FTD 6.3** 이상**:** 디바이스에 구축된 **FTD** 플랫폼 설정 정책에 설정된 시스템 로그 설정을 사용합니다**.**를 선택합니다.
e) (선택 사항) **Syslog Severity(**시스템 로그 심각도**)**를 선택합니다.
f) 파일 및 악성코드 이벤트를 전송하려면 **Send Syslog messages for File and Malware(**파일 및 악성코드 이벤트에 대해 시스템 로그 메시지 전송**)**를 선택합니다.
g) **Save(**저장**)**를 클릭합니다.

단계 **3** 액세스 제어 정책에 대한 보안 인텔리전스 이벤트에 대한 로깅을 활성화합니다.

a) 동일한 액세스 제어 정책에서 **Security Intelligence(**보안 인텔리전스**)** 탭을 클릭합니다.
b) 다음 각 위치에서 로깅( )를 클릭하여 연결의 시작과 끝 및 시스템 로그 서버를 활성화합니다.

- **DNS Policy(DNS** 정책**)** 옆.
- **Block List(**차단 목록**)** 상자에서 **Networks(**네트워크**)** 및 **URL**에 대해.

c) **Save(**저장**)**를 클릭합니다.

단계 **4** 액세스 제어 정책에서 각 규칙에 대해 syslog 로깅을 활성화합니다.

a) 동일한 액세스 제어 정책에서 **Rules(**규칙**)** 탭을 클릭합니다.
b) 편집할 규칙을 클릭합니다.
c) 규칙에서 **Logging(**로깅**)** 탭을 클릭합니다.
d) 연결의 시작 또는 종료를 기록할지 아니면 둘 다 기록 할지를 선택합니다.

(연결 로깅은 많은 양의 데이터를 생성합니다. 시작과 끝을 모두 로깅하면 데이터 양이 약 2배 증가합니다. 모든 연결을 처음과 끝에서 모두 로깅할 수있는 것은 아닙니다.)

e) 파일 이벤트를 로깅할 경우 **Log Files(**로그 파일**)**를 선택합니다.
f) **Syslog Server(**시스템 로그 서버**)**를 활성화합니다.
g) 규칙이 **"Using default syslog configuration in Access Control Logging(**세스 제어 기록에서 기본 시스템 로그 컨피그레이션 사용**)"**인지 확인합니다.
h) **Add(**추가**)**를 클릭합니다.
i) 정책의 각 규칙에 대해 반복합니다.

단계 **5** 침입 이벤트를 전송할 경우, 다음을 수행합니다.

a) 액세스 제어 정책과 연결된 침입 정책으로 이동합니다.
b) 침입 정책에서 **Advanced Settings(**고급 설정**) > Syslog Alerting(**시스템 로그 알림**) > Enabled(**활성화**)**를 선택합니다.
c) 필요한 경우 **Edit(**편집**)**을 클릭합니다.
d) 옵션을 입력합니다.

옵션	값
로깅 호스트	다른 시스템 로그 메시지를 전송하는 것 이외의 다른 시스템 로그 서버로 침입 이벤트 시스템 로그 메시지를 보내지 않는 한 위에서 구성한 설정을 사용하려면 이 필드를 비워 두십시오.
기능	이 설정은 이 페이지에서 Logging Host(로깅 호스트)를 지정한 경우에만 적용할 수 있습니다. 자세한 내용은 시스템 로그 알림 시설를 참조하십시오.
심각도	이 설정은 이 페이지에서 Logging Host(로깅 호스트)를 지정한 경우에만 적용할 수 있습니다. 자세한 내용은 Syslog 심각도 레벨를 참조하십시오.

e) **Back(**뒤로**)**을 클릭합니다.
f) 탐색창에서 **Policy Information(**정책 정보**)**을 클릭합니다.
g) **Commit Changes(**변경 커밋**)**를 클릭합니다.

다음에 수행할 작업

- (선택 사항) 개별 정책 및 규칙에 대해 서로 다른 로깅 설정을 구성합니다.

연결 및 보안 인텔리전스 이벤트에 대한 시스템 로그 설정 위치(모든 디바이스), 12 페이지의 해당 테이블 행을 참조하십시오.

이러한 설정에는 시스템 로그 알림 응답이 필요하며, 이는 Syslog 알림 응답 생성에 설명된 대로 구성됩니다. 이 절차에서 설정한 플랫폼 설정은 사용하지 않습니다.

- 클래식 디바이스에 대한 보안 이벤트 시스템 로그 로깅을 설정하려면 클래식 디바이스에서 보안 이벤트 시스템 로그 메시지 보내기, 11 페이지의 내용을 참조하십시오.
- 변경을 완료한 경우, 매니지드 디바이스에 변경 사항을 구축합니다.

클래식 디바이스에서 보안 이벤트 시스템 로그 메시지 보내기

시작하기 전에

- 보안 이벤트를 생성하도록 정책을 설정합니다.
- 디바이스가 시스템 로그 서버에 연결할 수 있는지 확인합니다.
- 시스템 로그 서버가 원격 메시지를 수락할 수 있는지 확인합니다.
- 연결 로깅에 대한 중요 정보는 연결 로깅의 관련 챕터를 참조하십시오.

프로시저

단계 **1** 클래식 디바이스에 대한 알림 응답을 설정합니다.

Syslog 알림 응답 생성의 내용을 참조하십시오.

단계 **2** 액세스 제어 정책에서 시스템 로그 설정을 구성합니다.

a) **Policies(**정책**) > Access Control(**액세스 제어**)**을 클릭합니다.
b) 해당 액세스 제어 정책을 편집합니다.
c) **Logging(**로깅**)**을 클릭합니다.
d) **Send using specific syslog alert(**특정 시스템 로그 알림을 사용하여 전송**)**을 선택합니다.
e) 위에서 생성한 시스템 로그 알림을 선택합니다.
f) **Save(**저장**)**를 클릭합니다.

단계 **3** 파일 및 악성코드 이벤트를 전송할 경우, 다음을 수행합니다.

a) **Send Syslog messages for File and Malware events(**파일 및 악성코드 이벤트에 대한 시스템 로그 메시지 전송**)**를 선택합니다.
b) **Save(**저장**)**를 클릭합니다.

단계 **4** 침입 이벤트를 전송할 경우, 다음을 수행합니다.

a) 액세스 제어 정책과 연결된 침입 정책으로 이동합니다.
b) 침입 정책에서 **Advanced Settings(**고급 설정**) > Syslog Alerting(**시스템 로그 알림**) > Enabled(**활성화**)**를 선택합니다.
c) 필요한 경우, **Edit(**편집**)**을 클릭합니다.

d) 옵션을 입력합니다.

옵션	값
로깅 호스트	다른 시스템 로그 메시지를 전송하는 것 이외의 다른 시스템 로그 서버로 침입 이벤트 시스템 로그 메시지를 보내지 않는 한 위에서 구성한 설정을 사용하려면 이 필드를 비워 두십시오.
기능	이 설정은 이 페이지에서 Logging Host(로깅 호스트)를 지정한 경우에만 적용할 수 있습니다. 시스템 로그 알림 시설의 내용을 참조하십시오.
심각도	이 설정은 이 페이지에서 Logging Host(로깅 호스트)를 지정한 경우에만 적용할 수 있습니다. Syslog 심각도 레벨의 내용을 참조하십시오.

e) **Back(**뒤로**)**을 클릭합니다.
f) 탐색창에서 **Policy Information(**정책 정보**)**을 클릭합니다.
g) **Commit Changes(**변경 커밋**)**를 클릭합니다.

다음에 수행할 작업

- (선택 사항) 개별 액세스 제어 규칙에 대해 서로 다른 로깅 설정을 구성합니다. 연결 및 보안 인텔리전스 이벤트에 대한 시스템 로그 설정 위치(모든 디바이스), 12 페이지의 해당 테이블 행을 참조하십시오. 이러한 설정에는 Syslog 알림 응답 생성에 설명된 대로 구성된 시스템 로그 알림 응답이 필요합니다. 위에서 구성한 설정은 사용하지 않습니다.
- FTD 디바이스에 대한 보안 이벤트 시스템 로그 로깅을 설정하려면 FTD 디바이스에서 보안 이벤트 시스템 로그 메시지 보내기, 8 페이지의 내용을 참조하십시오.

보안 이벤트 시스템 로그에 대한 설정 위치

연결 및 보안 인텔리전스 이벤트에 대한 시스템 로그 설정 위치**(**모든 디바이스**)**

로깅 설정은 여러 곳에서 설정할 수 있습니다. 아래 표를 사용하여 필요한 옵션을 설정했는지 확인합니다.

중요

- 시스템 로그 설정은 신중하게 수행해야 하며, 다른 설정에서 상속받은 기본값을 사용할 때는 특히 주의해야 합니다. 아래 표에서 설명하듯이, 매니지드 디바이스 모델과 소프트웨어 버전에 따라 사용할 수 없는 옵션도 있습니다.
- 연결 로깅 설정 관련 중요 정보는 연결 로깅의 관련 챕터를 참조하십시오.

설정 위치	설명 및 상세정보
Devices(장치) > **Platform Settings**(플랫폼 설정), Threat Defense Settings(위협 방어 설정) 정책, **Syslog**(시스템 로그)	이 옵션은 Firepower Threat Defense(Firepower 위협 방어) 디바이스에만 적용됩니다. 여기서 구성하는 설정은 Access Control(액세스 컨트롤) 정책에 대한 Logging(기록) 설정에서 지정할 수 있으며, 이 표에 있는 나머지 정책과 규칙에서 사용하거나 재정의할 수 있습니다. 보안 이벤트 Syslog 메시지에 적용되는 FTD 플랫폼 설정, Syslog 정보 및 하위 항목을 참조하십시오.
Policies(정책) > **Access Control**(액세스 컨트롤), <각 정책>, **Logging**(기록)	여기서 구성하는 설정은 모든 연결 및 보안 인텔리전스 이벤트에 대한 시스템 로그의 기본 설정입니다. 단 이 표의 나머지 행에서 지정하는 위치에 있는 하위 정책 및 규칙에서 기본값을 재정의하는 경우는 예외입니다. FTD 디바이스의 권장 설정입니다. FTD Platform Settings(FTD 플랫폼 설정)를 사용합니다. 자세한 정보는 보안 이벤트 Syslog 메시지에 적용되는 FTD 플랫폼 설정, Syslog 정보 및 하위 항목을 참조하십시오. 다른 모든 디바이스의 필수 설정입니다. 시스템 로그 알림을 사용합니다. 시스템 로그 알림을 지정하는 경우에는 Syslog 알림 응답 생성 섹션을 참조하십시오. Logging(기록) 탭의 설정에 관한 자세한 내용은 액세스 제어 정책용 로깅 설정섹션을 참조하십시오.
Policies(정책) > **Access Control**(액세스 컨트롤), <각 정책>, **Rules**(규칙), **Default Action**(기본 작업) 행, 로깅( )	액세스 컨트롤 정책과 관련된 기본 작업의 기록 설정입니다. 액세스 제어 규칙 챕터 및 정책 기본 작업으로 연결 로깅의 기록 관련 정보를 참조하십시오.
Policies(정책) > **Access Control**(액세스 컨트롤), <각 정책>, **Rules**(규칙), <각 규칙>, **Logging**(기록)	액세스 컨트롤 정책의 특정 규칙에 대한 기록 설정입니다. 액세스 제어 규칙 챕터의 기록 관련 정보를 참조하십시오.

설정 위치	설명 및 상세정보
Policies(정책) > **Access Control**(액세스 컨트롤), <각 정책>, **Security Intelligence**(보안 인텔리전스), 로깅( )	보안 인텔리전스 차단 목록의 기록 설정입니다. 버튼을 클릭해 다음을 설정합니다. • DNS 차단 목록 로깅 옵션 • URL 차단 목록 로깅 옵션 • 네트워크 차단 목록 기록 옵션(차단 목록의 IP 주소용) 사전 요구 사항 섹션, 하위 항목 및 링크를 포함한 보안 인텔리전스 설정의 정보를 참조하십시오.
Policies(정책) > **SSL**, <각 정책>, **Default Action**(기본 작업) 행, 로깅( )	SSL 정책과 관련된 기본 작업의 기록 설정입니다. 정책 기본 작업으로 연결 로깅의 내용을 참조하십시오.
Policies(정책) > **SSL**, <각 정책>, <각 규칙>, **Logging**(로깅)	SSL 규칙에 대한 기록 설정입니다. TLS/SSL 규칙 구성 요소의 내용을 참조하십시오.
Policies(정책) > **Prefilter**(사전 필터), <각 정책>, **Default Action**(기본 작업) 행, 로깅( )	사전 필터 정책과 관련된 기본 작업의 기록 설정입니다. 정책 기본 작업으로 연결 로깅의 내용을 참조하십시오.
Policies(정책) > **Prefilter**(사전 필터), <각 정책>, <각 사전 필터 규칙>, **Logging**(기록)	사전 필터 정책의 각 사전 필터 규칙에 대한 기록 설정입니다. 터널 및 사전 필터 규칙 구성 요소의 내용을 참조하십시오.
Policies(정책) > **Prefilter**(사전 필터), <각 정책>, <각 터널 규칙>, **Logging**(기록)	사전 필터 정책의 각 터널 규칙에 대한 기록 설정입니다. 터널 및 사전 필터 규칙 구성 요소의 내용을 참조하십시오.
FTD 클러스터 설정에 대한 추가 시스템 로그 설정:	Firepower Threat Defense 클러스터링 챕터에는 시스템 로그에 대한 여러 참조자료가 있습니다. 챕터에서 "syslog"를 검색해 보십시오.

침입 이벤트에 대한 시스템 로그의 설정 위치(FTD 디바이스)

다양한 위치에서 침입 정책의 시스템 로그 설정을 지정할 수 있으며, 선택적으로 액세스 컨트롤 정책 또는 FTD Platform Settings(FTD 플랫폼 설정)이나 양쪽 모두의 설정을 상속할 수도 있습니다.

설정 위치	설명 및 상세정보
Devices(장치**) > Platform Settings(**플랫폼 설정**)**, Threat Defense Settings(위협 방어 설정) 정책, **Syslog(**시스템 로그**)**	여기서 구성하는 시스템 로그 대상은 침입 정책의 기본값이 될 수 있는, 액세스 컨트롤 정책의 Logging(기록) 탭에서 지정할 수 있습니다. 보안 이벤트 Syslog 메시지에 적용되는 FTD 플랫폼 설정, Syslog 정보 및 하위 항목을 참조하십시오.
Policies(정책**) > Access Control(**액세스 컨트롤**)**, <각 정책>, **Logging(**기록**)**	침입 정책이 다른 기록 호스트를 지정하지 않는 경우, 침입 이벤트에 대한 시스템 로그 대상의 기본 설정입니다. 액세스 제어 정책용 로깅 설정의 내용을 참조하십시오.
Policies(정책**) > Intrusion(**침입**)**, <각 정책>, **Advanced Settings(**고급 설정**)**에서 **Syslog Alerting(**시스템 로그 알림**)**을 활성화하고 **Edit(**편집**)** 클릭	Logging(기록) 탭의 액세스 컨트롤 정책에 지정된 대상이 아닌 다른 시스템 로그 수집기를 지정하고 시설과 심각도를 지정하려면, 침입 이벤트를 위한 시스템 로그 알림 설정 섹션을 참조하십시오. 침입 정책에 설정된 **Severity(**심각도**)**나 **Facility(**시설**)** 또는 둘 다를 사용하고 싶다면, 정책에서 기록 호스트를 설정해야 합니다. 액세스 컨트롤 정책에서 지정하는 기록 호스트를 사용하는 경우, 침입 규칙에 지정된 심각도와 시설은 사용하지 않습니다.

침입 이벤트에 대한 시스템 로그의 설정 위치**(FTD** 이전 버전의 디바이스**)**

- (기본값) 액세스 컨트롤 정책액세스 제어 정책용 로깅 설정, 시스템 로그 알림을 지정하는 경우 (Syslog 알림 응답 생성 참조)
- 또는 침입 이벤트를 위한 시스템 로그 알림 설정 섹션을 참조하십시오.

기본적으로, 침입 정책은 액세스 컨트롤 정책의 Logging(로깅) 탭에 있는 설정을 사용합니다. FTD 이아닌 디바이스에 적용 가능한 설정이 구성되어 있지 않다면, 시스템 로그는 FTD 이외의 디바이스에는 전송되지 않으며 경고도 표시되지 않습니다.

파일 및 악성코드 이벤트에 대한 시스템 로그 설정 위치

설정 위치	설명 및 상세정보
액세스 컨트롤 정책에서 **Policies(**정책**) > Access Control(**액세스 컨트롤**)**, <각 정책>, **Logging(**기록**)**	파일 및 악성코드 이벤트에 대한 시스템 로그를 전송하도록 시스템을 설정하는 기본 위치입니다. FTD Platform Settings(FTD 플랫폼 설정)에서 시스템 로그 설정을 사용하지 않는다면, 알림 응답도 생성해야 합니다. Syslog 알림 응답 생성의 내용을 참조하십시오.
Firepower Threat Defense 플랫폼 설정에서 **Devices(**장치**) > Platform Settings(**플랫폼 설정**)**, Threat Defense Settings(위협 방어 설정) 정책, **Syslog(**시스템 로그**)**	이러한 설정은 지원되는 버전을 실행하는 Firepower Threat Defense(Firepower 위협 방어) 디바이스에만 적용되며, FTD 플랫폼 설정을 사용할 액세스 컨트롤 정책에서 Logging(기록) 탭을 설정한 경우에만 적용됩니다. 보안 이벤트 Syslog 메시지에 적용되는 FTD 플랫폼 설정, Syslog 정보 및 하위 항목을 참조하십시오.
액세스 컨트롤 규칙에서 **Policies(**정책**) > Access Control(**액세스 컨트롤**)**, <각 정책>, <각 규칙>, **Logging(**기록**)**	FTD Platform Settings(FTD 플랫폼 설정)에서 시스템 로그 설정을 사용하지 않는다면, 알림 응답도 생성해야 합니다. Syslog 알림 응답 생성의 내용을 참조하십시오.

Security(보안) 이벤트 시스템 로그 메시지 구조

FTD 에서 전송하는 보안 이벤트 메시지 예시(침입 이벤트)

```
  0        1              2              3        4  5     6

<37>2018-06-27 192.168.0.81 SFIMS : %FTD-5-430001:
192.168.1.10, DstIP: 192.168.1.102, SrcPort: 33994
Protocol: tcp, Priority: 2, GID: 133, SID: 17, Rev
Message: "DCE2_EVENT   SMB_INVALID_DSIZE", Classif
Potentially Bad Traffic, User: No Authentication R
Client: NetBIOS-ssn (SMB) client, ApplicationProto
(SMB), ACPolicy: test, NAPPolicy: Balanced Securit
Connectivity, InlineResult: Blocked
```

표 *1:* 보안 이벤트 시스템 로그 메시지의 구성 요소

샘플 메시지의 항목 수	헤더 요소	설명
0	PRI	알림의 기능 및 심각도를 모두 나타내는 우선 순위 값입니다. 이 값은 FMC 플랫폼 설정을 사용하여 EMBLEM 형식으로 로깅을 활성화한 경우에만 시스템 로그 메시지에 나타납니다. 액세스 제어 정책 Logging(로깅) 탭을 통해 침입 이벤트 로깅을 활성화하면 PRI 값이 시스템 로그 메시지에 자동으로 표시됩니다. EMBLEM 형식을 활성화하는 방법에 대한 자세한 내용은 로깅 활성화 및 기본 설정의 내용을 참조하십시오. PRI에 대한 자세한 내용은 RFC5424를 참조하십시오.
1	타임스탬프	디바이스에서 시스템 로그 메시지가 전송된 날짜와 시간입니다. • (FTD 장치에서 전송된 시스템 로그) 액세스 컨트롤 정책 및 그 하위 항목의 설정의 경우, 또는 이 형식을 FTD Platform Settings(FTD 플랫폼 설정)에서 사용하도록 지정한 경우 날짜 형식은 RFC 5424에 지정하는 ISO 8601 타임스탬프 형식에서 정의하는 형식(yyyy-MM-ddTHH:mm:ssZ)입니다. 여기서 Z는 UTC 시간대를 의미합니다. • (다른 모든 장치에서 전송된 시스템 로그) 액세스 컨트롤 정책 및 그 하위 항목의 설정의 경우, 날짜 형식은 RFC 5424에 지정하는 ISO 8601 타임스탬프 형식에서 정의하는 형식(yyyy-MM-ddTHH:mm:ssZ)입니다. 여기서 Z는 UTC 시간대를 의미합니다. • 그렇지 않은 경우에는 UTC 시간대의 월, 일, 시간이 되지만, 시간대는 표시되지 않습니다. FTD Platform Settings(FTD 플랫폼 설정)에서 타임스탬프 설정을 구성하는 방법은 Syslog 설정 섹션을 참조하십시오.

샘플 메시지의 항목 수	헤더 요소	설명
2	메시지를 보낸 디바이스 또는 인터페이스입니다. 다음을 선택할 수 있습니다. • 인터페이스의 IP 주소 • 디바이스 호스트 이름 • 맞춤형 디바이스 식별자	(FTD 디바이스 전송된 시스템 로그 전용) 시스템 로그 메시지가 FTD Platform Settings(FTD 플랫폼 설정)을 사용하여 전송된 경우, 이것은 **Enable Syslog Device ID(**시스템 로그 디바이스 **ID)** 옵션(지정한 경우)의 **Syslog Settings(**시스템 로그 설정**)**에서 설정한 값입니다. 그렇지 않은 경우, 이 요소는 헤더에 존재하지 않습니다. FTD Platform Settings(FTD 플랫폼 설정)에서 이 설정을 구성하는 방법은 Syslog 설정 섹션을 참조하십시오.
3	맞춤형 값	알림 응답을 사용하여 메시지를 전송한 경우, 이것은 메시지를 전송한 알림 응답에서 설정한 **Tag(**태그**)** 값입니다(설정한 경우). (Syslog 알림 응답 생성 참조) 그렇지 않은 경우, 이 요소는 헤더에 존재하지 않습니다.
4	%FTD %NGIPS	메시지를 전송한 디바이스의 유형입니다. • %FTD는 Firepower Threat Defense(Firepower 위협 방어)입니다. • %NGIPS는 다른 모든 디바이스입니다.
5	심각도	메시지를 트리거한 정책의 시스템 로그 설정에서 지정한 심각도입니다. 심각도 설명은 심각도 레벨 또는 Syslog 심각도 레벨 섹션을 참조하십시오.
6	이벤트 유형 식별자	• 430001: 침입 이벤트 • 430002: 연결 시작 시 기록된 연결 이벤트 • 430003: 연결 종료 시 기록된 연결 이벤트 버전 6.4 이상을 실행하는 디바이스에서 전송한 메시지의 경우, 다음 이벤트 유형 ID도 사용합니다. • 430004: 파일 이벤트 • 430005: 파일 악성코드 이벤트

샘플 메시지의 항목 수	헤더 요소	설명
--	기능	보안 이벤트 시스템 로그 메시지의 시설, 19 페이지의 내용을 참조하십시오.
--	메시지의 나머지 부분	필드와 값은 콜론으로 구분합니다. 비어 있거나 알 수 없는 값이 있는 필드는 메시지에서 생략됩니다. 필드 설명은 다음을 참조하십시오. • 연결 및 보안 인텔리전스 이벤트 필드. • 침입 이벤트 필드 • 파일 및 악성코드 이벤트 필드 참고 필드 설명 목록은 시스템 필드와 이벤트 뷰어(Firepower Management Center 웹 인터페이스의 Analysis(분석) 메뉴에 있는 메뉴 옵션)에 표시되는 필드를 모두 포함합니다. 시스템 로그를 통해 사용할 수 있는 필드에는 다음과 같은 레이블이 지정됩니다. 이벤트 뷰어에 표시되는 필드 중 일부는 시스템 로그를 통해 사용할 수 없습니다. 또한 이벤트 뷰어에 포함되지 않는(하지만 검색을 통해 사용할 수 있는) 시스템 로그 필드도 있으며, 결합되거나 분리된 필드도 존재합니다.

보안 이벤트 시스템 로그 메시지의 시설

일반적으로 시설 값은 보안 이벤트의 시스템 로그 메시지와는 무관합니다. 그러나 Facility(시설)이 필요하다면, 다음 표를 사용하십시오.

디바이스	시설을 연결 이벤트에 포함하는 방법	시설을 침입 이벤트에 포함하는 방법	시스템 로그 메시지에서의 위치
FTD	FTD Platform Settings(FTD 플랫폼 설정)에서 EMBLEM 옵션을 사용합니다. FTD Platform Settings(FTD 플랫폼 설정)를 사용하여 시스템 로그 메시지를 전송하는 경우, 연결 이벤트에 대한 시설은 언제나 **ALERT**입니다.	FTD Platform Settings(FTD 플랫폼 설정)에서 EMBLEM 옵션을 사용하거나 침입 규칙의 시스템 로그 설정을 사용하여 기록을 구성합니다. 침입 정책을 사용하는 경우에는 침입 정책 설정에서 기록 호스트를 지정해야 합니다.	시설은 메시지 헤더에는 표시되지 않지만, 시스템 수집기는 RFC 5424, 섹션 6.2.1을 바탕으로 값을 끌어낼 수 있습니다.
FTD 이외의 디바이스	알림 응답을 사용합니다.	침입 정책 고급 설정의 시스템 로그 설정을 사용하거나 액세스 컨트롤 정책 Logging(기록) 탭에서 식별한 응답 알림을 사용합니다.	

자세한 내용은 침입 시스템 로그 알림에 대한 시설 및 Severities(심각도) 및 Syslog 알림 응답 생성의 내용을 참조하십시오.

Firepower System 로그 메시지 유형

Firepower는 다음 테이블에서 설명하는 것처럼 여러 시스템 로그 데이터 유형을 전송할 수 있습니다.

시스템 로그 데이터 유형	확인
FMC의 감사 로그	시스템 로그로의 감사 로그 스트리밍 및 시스템 감사 챕터
기본 디바이스(7000/8000 시리즈, ASA FirePOWER, NGIPSv)의 감사 로그	클래식 디바이스에서의 감사 로그 스트리밍 및 시스템 감사 챕터 CLI 명령: syslog
디바이스 상태 및 FTD의 네트워크 관련 로그	Syslog 정보 및 하위 항목
연결, 보안 인텔리전스 및 FTD 디바이스의 침입 이벤트 로그	보안 이벤트 데이터를 시스템 로그로 전송하는 시스템 설정 정보, 7 페이지.
연결, 보안 인텔리전스 및 기본 디바이스의 침입 이벤트 로그	보안 이벤트 데이터를 시스템 로그로 전송하는 시스템 설정 정보, 7 페이지
파일 및 악성코드 이벤트 로그	보안 이벤트 데이터를 시스템 로그로 전송하는 시스템 설정 정보, 7 페이지

보안 이벤트에 대한 시스템 로그 제한 사항

- 시스템 로그를 사용하거나 이벤트를 외부에 저장하려는 경우, 정책 및 규칙 이름과 같은 개체 이름에 특수 문자를 사용하지 마십시오. 개체 이름은 수신 애플리케이션에서 구분자로 사용할 수 있는 특수 문자(예: 쉼표)를 포함해서는 안 됩니다.
- 이벤트가 시스템 로그 수집기에 표시될 때까지 최대 15분이 걸릴 수 있습니다.
- 다음 파일 및 악성코드 이벤트의 데이터는 시스템 로그를 통해 사용할 수 없습니다.
  - 회귀 이벤트
  - AMP for Endpoints(엔드포인트용 AMP)가 생성한 이벤트

eStreamer 서버 스트리밍

Event Streamer(eStreamer)를 사용하면 여러 종류의 이벤트 데이터를 Firepower Management Center 또는 7000 또는 8000 Series 디바이스에서 맞춤 개발된 클라이언트 애플리케이션으로 스트리밍할 수 있습니다. 자세한 내용은 *Firepower System Event Streamer* 통합 가이드를 참고하십시오.

eStreamer 서버로 사용할 어플라이언스가 외부 클라이언트로 eStreamer 이벤트의 스트리밍을 시작하기 전에 이벤트를 클라이언트로 전송하고, 클라이언트에 대한 정보를 제공하고, 통신 설정 시 사용할 인증 자격 증명 집합을 생성하도록 eStreamer 서버를 구성해야 합니다. 어플라이언스의 사용자 인터페이스에서 이 모든 작업을 수행할 수 있습니다. 설정이 저장되면, 선택한 이벤트는 요청 시 eStreamer 클라이언트에 전달됩니다.

eStreamer 서버가 이벤트를 요청하는 클라이언트에 전송할 수 있는 이벤트 유형을 제어할 수 있습니다.

표 ***2: eStreamer*** 서버가 전송할 수 있는 이벤트 유형

이벤트 유형	설명
침입 이벤트	매니지드 디바이스에서 생성된 침입 이벤트
침입 이벤트 패킷 데이터	침입 이벤트와 관련된 패킷
침입 이벤트 추가 데이터	HTTP 프록시 또는 로드 밸런서를 통해 웹 서버에 연결하는 클라이언트의 원래 IP 주소와 같은 침입 이벤트와 관련된 추가 데이터
검색 이벤트	네트워크 검색 이벤트
상관관계 및 화이트리스트 이벤트	상관관계 및 컴플라이언스 화이트 목록 이벤트
영향 플래그 알림	다음이 생성한 영향 알림 FMC
사용자 이벤트	사용자 이벤트

이벤트 유형	설명
악성코드 이벤트	악성코드 이벤트
파일 이벤트	파일 이벤트
연결 이벤트	모니터링되는 호스트와 기타 모든 호스트 간의 세션 트래픽에 대한 정보입니다.

시스템 로그 및 eStreamer의 보안 이벤트 비교

일반적으로, eStreamer에 큰 투자를 하지 않은 조직은 시스템 로그 대신 eStreamer를 사용하여 보안 이벤트 데이터를 외부적으로 관리해야 합니다.

시스템 로그	**eStreamer**
맞춤형 필요 없음	각 릴리스의 변경사항을 수용하려면 상당한 수준의 맞춤형 및 유지관리가 필요함
표준	Proprietary
시스템 로그 표준은 데이터 손실을 방지하지 않으며, UDP를 사용할 때는 더욱 그렇습니다.	데이터 손실 방지
디바이스에서 직접 전송	FMC에서 전송하며, 처리 오버헤드 추가
파일 및 악성코드 이벤트, 연결 이벤트(보안 인텔리전스 이벤트 포함) 및 침입 이벤트를 지원합니다.	eStreamer 서버 스트리밍, 21 페이지에 나열된 모든 이벤트 유형을 지원합니다.
일부 이벤트 데이터는 FMC에서만 전송할 수 있습니다. (시스템 로그가 아닌) eStreamer로만 전송된 데이터, 22 페이지의 내용을 참조하십시오.	디바이스에서 시스템 로그를 통해 직접 전송될 수 없는 데이터를 포함합니다. (시스템 로그가 아닌) eStreamer로만 전송된 데이터, 22 페이지의 내용을 참조하십시오.

(시스템 로그가 아닌) eStreamer로만 전송된 데이터

다음 데이터는 에서만 사용할 수 있으며, 따라서 디바이스에서 시스템 로그를 통해 전송할 수 없습니다.Firepower Management Center

- 패킷 로그
- 침입 이벤트 추가 데이터 이벤트

  자세한 내용은 eStreamer 서버 스트리밍, 21 페이지의 내용을 참조하십시오.
- 통계 및 통합 이벤트
- 네트워크 검색 이벤트

- 사용자 활동 및 로그인 이벤트
- 상관관계 이벤트
- 악성코드 이벤트:
  - 회귀 판정
  - 관련 SHA 정보가 디바이스에 이미 동기화되어 있지 않은 경우 ThreatName 및 분류
- 다음 필드:
  - Impact 및 ImpactFlag 필드

    자세한 내용은 eStreamer 서버 스트리밍, 21 페이지의 내용을 참조하십시오.
  - IOC_Count 필드
- 대부분의 원시 ID 및 UUID입니다.

  예외
  - 연결 이벤트에 대한 시스템 로그는 FirewallPolicyUUID, FirewallRuleID, TunnelRuleID, MonitorRuleID, SI_CategoryID, SSL_PolicyUUID, SSL_RuleID가 포함됩니다.
  - 침입 이벤트의 시스템 로그는 IntrusionPolicyUUID, GeneratorID, SignatureID를 포함합니다.
- 확장 메타데이터(다음을 포함하되 이에 제한되지 않음):
  - LDAP에서 제공한 사용자 상세정보(전체 이름, 부서, 전화 번호 등)

    시스템 로그는 이벤트의 사용자 이름만 제공합니다.
  - SSL 인증 상세정보 같은 상태 기반 정보

    시스템 로그는 인증서 지문과 같은 기본 정보를 제공하지만, cert CN 같은 다른 인증서 세부 정보는 제공하지 않습니다.
  - 앱 태그 및 범주 같은 자세한 애플리케이션 정보

    시스템 로그는 애플리케이션 이름만 제공합니다.

  일부 메타데이터 메시지에는 개체에 대한 추가 정보도 포함됩니다.
- 지오로케이션 정보

eStreamer 이벤트 유형 선택

eStreamer Event Configuration(eStreamer 이벤트 설정**)** 확인란는 eStreamer 서버가 전송할 수 있는 이벤트를 제어합니다. 클라이언트에서는 여전히 eStreamer 서버로 전송하는 요청 메시지에서 수신하고자 하는 이벤트 유형을 구체적으로 요청해야 합니다. 자세한 내용은 *Firepower System Event Streamer* 통합 가이드을 참조하십시오.

다중 도메인 구축에서는 어떤 도메인 수준에서도 eStreamer 이벤트 설정을 구성할 수 있습니다. 그러나 상위 도메인이 특정 이벤트 유형을 활성화했다면, 하위 도메인에서는 이벤트 유형을 비활성화할 수 없습니다.

FMC 및 7000 및 8000 Series 디바이스에 대해 이 작업을 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Integration(**통합**)**를 선택합니다.

단계 **2** **eStreamer**를 클릭합니다.

단계 **3** eStreamer 서버 스트리밍, 21 페이지에 설명된 대로, **eStreamer Event Configuration(eStreamer** 이벤트 설정**)**에서 eStreamer가 요청 클라이언트로 전달하도록 할 이벤트 유형 옆에 있는 확인란을 선택하거나 선택 해제합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

eStreamer 클라이언트 커뮤니케이션 설정

eStreamer가 eStreamer 이벤트를 클라이언트에 전송하려면, 먼저 eStreamer 페이지에서 클라이언트를 eStreamer 서버의 피어 데이터베이스에 추가해야 합니다. 또한 eStreamer 서버에서 생성된 인증 인증서를 클라이언트에 복사해야 합니다. 이상의 단계를 완료하면 eStreamer 서비스를 다시 시작하지 않고도 클라이언트를 eStreamer 서버에 연결할 수 있습니다.

다중 도메인 구축에서는 모든 도메인에서 eStreamer 클라이언트를 만들 수 있습니다. 인증 인증서를 이용하면 클라이언트가 클라이언트 인증서의 도메인 및 하위 도메인의 이벤트만 요청하게 할 수 있습니다. eStreamer 설정 페이지는 현재 도메인과 연결된 클라이언트만 표시하므로, 인증서를 다운로드하거나 취소하려면 클라이언트가 생성된 도메인으로 전환해야 합니다.

FMC 및 7000 및 8000 Series 디바이스에 대해 이 작업을 수행하려면 관리자 또는 검색 관리자 사용자여야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Integration(**통합**)**를 선택합니다.

단계 **2** **eStreamer**를 클릭합니다.

단계 **3** **Create Client(**클라이언트 생성**)**를 클릭합니다.

단계 **4** **Hostname(**호스트 이름**)** 필드에 eStreamer 클라이언트를 실행하는 호스트의 IP 주소 또는 호스트 이름을 입력합니다.

참고 DNS 확인을 설정하지 않은 경우, IP 주소를 사용해야 합니다.

단계 **5** 인증서 파일을 암호화하려면, **Password(**비밀번호**)** 필드에 비밀번호를 입력합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

이제 eStreamer 서버는 호스트가 eStreamer 서버의 포트 8302에 액세스하는 것을 허용하고 클라이언트-서버 인증 중에 사용할 인증 인증서를 만듭니다.

단계 **7** 인증서 파일을 다운로드하려면 클라이언트 호스트 이름 옆에 있는 다운로드( )을 클릭합니다.

단계 **8** SSL 인증을 위해 클라이언트가 사용한 적절한 디렉터리에 인증서 파일을 저장합니다.

단계 **9** 클라이언트에 대한 액세스를 취소하려면, 제거할 호스트 옆에 있는 삭제( )을 클릭합니다.

eStreamer 서비스를 다시 시작할 필요가 없으며, 액세스는 즉시 취소됩니다.

Splunk의 이벤트 분석

Splunk용 Cisco Secure Firewall(f.k.a. Firepower)(이전 명칭: Splunk용 Cisco Firepower App)를 외부 툴로 사용하여 Firepower 이벤트 데이터를 표시하고 사용하여 네트워크에서 위협을 추적하고 조사할 수 있습니다.

eStreamer가 필요합니다. 고급 기능입니다. eStreamer 서버 스트리밍, 21 페이지를 참조하십시오.

자세한 내용은 https://cisco.com/go/firepower-for-splunk를 참고하십시오.

IBM QRadar의 이벤트 분석

IBM QRadar용 Cisco Firepower 앱을 대체 방법으로 사용하여 이벤트 데이터를 표시하고 네트워크에 대한 위협을 분석, 추적 및 조사할 수 있습니다.

eStreamer가 필요합니다. 이는 고급 기능입니다. eStreamer 서버 스트리밍, 21 페이지를 참조하십시오.

자세한 내용은 https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/QRadar/integration-guide-for-the-cisco-firepower-app-for-ibm-qradar.html를 참고하십시오.

외부 툴을 사용한 이벤트 데이터 분석 기록

기능	버전	세부 사항
데이터를 보기 위한 교차 실행 Stealthwatch	6.7	이 기능을 사용하면 Analysis(분석) > Contextual Cross-Launch(상황별 교차 실행) 페이지에서 Stealthwatch 어플라이언스에 대한 여러 항목을 빠르게 생성할 수 있습니다. 이러한 항목을 사용하면 관련 이벤트를 마우스 오른쪽 버튼으로 클릭하여 Stealthwatch를 교차 실행하고 교차 시작한 데이터 지점과 관련된 정보를 표시할 수 있습니다. 새 메뉴 항목: System(시스템) > Logging(로깅) > Security Analytics and Logging(보안 분석 및 로깅) Stealthwatch로 이벤트 전송을 설정할 새 페이지입니다.
추가 필드 유형에서 상황별 교차 실행	6.7	이제 다음과 같은 추가 이벤트 데이터 유형을 사용하여 외부 애플리케이션으로 교차 실행할 수 있습니다. • 액세스 제어 정책 • 침입 정책 • 애플리케이션 프로토콜 • 클라이언트 애플리케이션 • 웹 애플리케이션 • 사용자 이름(영역 포함) 새로운 메뉴 옵션: 이제 Analysis(분석) 메뉴 아래의 페이지에서 대시보드 위젯 및 이벤트 테이블의 이벤트에 대한 위의 데이터 유형을 마우스 오른쪽 버튼으로 클릭하면 상황별 교차 실행 옵션을 사용할 수 있습니다. 지원되는 플랫폼: Firepower Management Center

기능	버전	세부 사항
IBM QRadar와의 통합	6.0 이상	IBM QRadar 사용자는 새로운 Firepower 전용 앱을 통해 이벤트 데이터를 분석할 수 있습니다. 사용 가능한 기능은 Firepower 버전에 따라 달라집니다. IBM QRadar의 이벤트 분석, 25 페이지의 내용을 참조하십시오.

개선 사항은 다음에 통합됩니다. Cisco SecureX Threat Response	6.5	• 지역 클라우드 지원:
		  • 미합중국(북미)
		  • 유럽
		• 추가 이벤트 유형 지원:
		  • 파일 및 악성코드 이벤트
		  • 높은 우선순위 연결 이벤트
		  다음과 관련된 연결 이벤트입니다.
		  • 침입 이벤트
		  • 보안 인텔리전스 이벤트
		  • 파일 및 악성코드 이벤트
		수정된 화면: **System(**시스템**) > Integration(**통합**) > Cloud Service(**클라우드 서비스**)**의 새 옵션
		지원 플랫폼: 이 버전에서는 직접 통합 또는 시스템 로그의 형태로 모든 디바이스를 지원합니다.

시스템 로그	6.5	이제 AccessControlRuleName 필드를 침입 이벤트 시스템 로그 메시지에서 사용할 수 있습니다.
통합 Cisco Security Packet Analyzer	6.5	이 기능의 지원은 삭제되었습니다.

기능	버전	세부 사항
통합 Cisco SecureX Threat Response	6.3(시스템 로그를 통해, 프록시 수집기 사용) 6.4(직접)	Firepower 침입 이벤트 데이터를 다른 소스의 데이터와 통합해 Cisco SecureX Threat Response의 강력한 분석 도구를 사용하여 네트워크상의 위협을 통합적으로 확인합니다. 수정된 화면(버전 6.4): **System(**시스템**) > Integration(**통합**) > Cloud Services(**클라우드 서비스**)**의 새 옵션 지원되는 플랫폼: 버전 6.3(시스템 로그를 통해) 또는 6.4를 실행하는 Firepower Threat Defense 디바이스
파일 및 악성코드 이벤트에 대한 시스템 로그 지원	6.4	이제 완전히 인증된 파일 및 악성코드 이벤트 데이터를 시스템 로그를 통해 매니지드 디바이스에서 전송할 수 있습니다. 수정된 화면: **Policies(**정책**) > Access Control(**액세스 제어**) > Access Control(**액세스 제어**) > Logging(**로깅**)** 지원 되는 플랫폼: 버전 6.4를 실행하는 모든 매니지드 디바이스
Splunk와의 통합	모든 6.x 버전 지원.	Splunk 사용자는 새로운 별도의 Splunk 앱인 Splunk용 Cisco Secure Firewall(f.k.a. Firepower)을(를) 사용하여 이벤트를 분석할 수 있습니다. 사용 가능한 기능은 Firepower 버전에 따라 달라집니다. Splunk의 이벤트 분석, 25 페이지의 내용을 참조하십시오.

기능	버전	세부 사항
통합 Cisco Security Packet Analyzer	6.3	도입된 기능: 이벤트와 관련된 패킷의 Cisco Security Packet Analyzer을(를) 즉시 쿼리하고, 클릭하여 Cisco Security Packet Analyzer의 결과를 검사하거나 다운로드해 다른 외부 도구에서 분석합니다. 새 화면: **System(**시스템**)** > **Integration(**통합**)** > **Packet Analyzer(**패킷 분석기**)** **Analysis(**분석**)** > **Advanced(**고급**)** > **Packet Analyzer Queries(**패킷 분석기 쿼리**)** 새 메뉴 옵션: Dashboard(대시보드) 페이지와 Analysis(분석) 메뉴의 페이지에 있는 이벤트를 오른쪽 클릭할 때 나타나는 **Query Packet Analyzer(**쿼리 패킷 분석기**)** 지원되는 플랫폼: Firepower Management Center
상황별 크로스 실행	6.3	도입된 기능: 이벤트를 오른쪽 클릭해 사전 정의 또는 맞춤형 URL 기반 외부 리소스에서 관련 정보를 찾습니다. 새 화면: **Analysis(**분석**)** > **Advanced(**고급**)** > **Contextual Cross-Launch(**상황별 크로스 실행**)** 새 메뉴 옵션: Dashboard(대시보드) 페이지와 Analysis(분석) 메뉴의 페이지에 있는 이벤트를 오른쪽 클릭할 때 나타나는 여러 옵션 지원되는 플랫폼: Firepower Management Center

기능	버전	세부 사항
연결 및 침입 이벤트용 시스템 로그 메시지	6.3	통합되고 단순화된 새로운 설정을 사용하여, 시스템 로그를 통해 완전히 인증된 연결 및 침입 이벤트를 외부 스토리지로 전송하는 기능 이제 메시지 헤더가 표준화되었고 이벤트 유형 식별자를 포함하며, 알 수 없거나 값이 없는 필드는 생략되기 때문에 미시지가 서로 비슷해집니다. 지원되는 플랫폼: • 모든 새 기능: 버전 6.3을 실행하는 FTD 디바이스 • 일부 새 기능: 버전 6.3을 실행하는 FTD 이외의 디바이스 • 소수의 새 기능: 버전 6.3 미만을 실행하는 모든 디바이스. 자세한 내용은 Security Events(보안 이벤트)에 대한 시스템 로그 메시지 전송 정보, 7 페이지 및 하위 항목의 주제를 참조하십시오.
eStreamer	6.3	eStreamer 콘텐츠를 Host Identity Sources(호스트 ID 소스) 챕터에서 이 챕터로 옮기고, eStreamer와 시스템 로그를 비교한 요약을 추가했습니다.