시스템 로그를 사용하여 클라우드로 이벤트 전송

시스템 로그를 통한 통합 관련 정보

Firepower 릴리스 6.3부터는 시스템 로그를 사용하여, 지원되는 이벤트를 Firepower 디바이스에서 Cisco Cloud로 전송할 수 있습니다. 사내 Cisco Security Services Proxy(CSSP) 서버를 설정하고 시스템 로그 메시지가 이 프록시로 전송되도록 디바이스를 구성해야 합니다.

10분마다 프록시가 수집된 이벤트를 보안 서비스 익스체인지(SSE)로 포워딩하며, 여기서는 이벤트를 SecureX에 표시되는 인시던트로 자동 또는 수동으로 승격할 수 있습니다.

시스템 로그를 이용한 통합 요구사항

요구 사항 유형	요건
Firepower 디바이스	지원되는 Firepower 소프트웨어 버전을 실행하는 모든 디바이스
Firepower 버전	6.3 이상
사용할 SecureX 클라우드에서의 계정	SecureX 액세스에 필요한 필수 계정의 내용을 참조하십시오.

요구 사항 유형	요건
라이선싱	이 통합에는 특별한 라이선스가 필요하지 않습니다. 하지만 다음 경우를 고려하십시오. • SecureX에 전송할 이벤트를 생성하려면 Firepower 시스템에 라이선스가 있어야 합니다. 자세한 내용은 https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-licensing-information-listing.html 섹션을 참조해 주십시오. • 이 기능은 Firepower 평가판 라이선스에서는 지원되지 않습니다. • 사용자의 환경에서는 에어갭 환경에 구축할 수 없습니다.
일반	Firepower 시스템이 이벤트를 예상대로 생성하고 있습니다.

시스템 로그를 이용해 **Cisco Cloud**에 이벤트를 전송하는 방법

참고 디바이스가 이미 클라우드에 이벤트를 전송 중인 경우, 다시 전송하도록 구성할 필요가 없습니다. SecureX 및 Cisco SecureX Threat Response (이전에는 Cisco Threat Response)는 동일한 이벤트 데이터 집합을 사용합니다.

	수행해야 할 작업	추가 정보
단계	전송할 이벤트, 해당 이벤트를 전송하는 방법, 사용할 지역 클라우드 등에 대해 결정합니다.	다음 항목을 참조하십시오. Firepower 및 통합에 대한 중요 정보 SecureX
단계	요구 사항을 충족합니다.	시스템 로그를 이용한 통합 요구사항, 1 페이지의 내용을 참조하십시오.
단계	디바이스 관리 및 이벤트 필터링에 사용할, SecureX용 플랫폼인 보안 서비스 익스체인지(SSE)에 액세스합니다.	Access(액세스) 보안 서비스 익스체인지, 4 페이지의 내용을 참조하십시오.
단계	Cisco Security Services Proxy(CSSP) 서버를 설치하고 구성합니다.	보안 서비스 익스체인지에서 무료 설치 프로그램과 지침을 다운로드합니다. SSE의 브라우저 창 오른쪽 상단에 있는 Tools 버튼(🛠)에서 **Downloads(**다운로드**)**를 선택합니다.

	수행해야 할 작업	추가 정보
단계	보안 서비스 익스체인지에서 기능을 활성화합니다.	**Cloud Services(**클라우드 서비스**)**를 클릭하고 다음 옵션을 활성화합니다. • **Cisco SecureX Threat Response** • 이벤팅 서비스
단계	지원되는 이벤트에 대한 시스템 로그 메시지를 프록시 서버로 전송하도록 Firepower 디바이스를 구성합니다.	• FDM(Firepower Device Manager)에서 관리하는 디바이스의 경우: FDM 온라인 도움말의 '침입 이벤트에 대한 시스템 로그 구성'에서 관련 정보를 참조하십시오. • Firepower Management Center(FMC)에서 관리하는 디바이스의 경우: FMC 온라인 도움말의 '외부 도구를 이용한 이벤트 분석' 장에 있는 시스템 로그 관련 정보를 참조하십시오.
단계	Firepower 제품에서 메시지가 각 이벤트를 생성한 디바이스를 식별하는지 확인합니다.	• Firepower Device Manager에서 다음을 수행합니다. **Device(**디바이스**) > Hostname(**호스트 이름**)**에서 호스트 이름을 지정합니다. • Firepower Management Center에서 다음을 수행합니다. Platform Settings(플랫폼 설정)의 시스템 로그 **Settings(**시스템 로그 설정**)** 탭에서 시스템 로그 디바이스 **ID**를 활성화하고 식별자를 지정합니다.
단계	Firepower 시스템에서 지원되는 이벤트를 생성할 때까지 기다립니다.	--
단계	보안 서비스 익스체인지에 이벤트가 예상대로 표시되는지 확인하고 필요하다면 문제 해결을 진행합니다.	참조: • 이벤트가 (시스템 로그를 통해) 보안 서비스 익스체인지에 도달하는지 확인합니다., 5 페이지 • 시스템 로그 통합 문제 해결, 5 페이지

	수행해야 할 작업	추가 정보
단계	보안 서비스 익스체인지에서 중요한 이벤트를 자동으로 승격하도록 시스템을 구성합니다.	중요 이벤트 승격을 자동화하지 않는 경우 SecureX에서 이벤트를 보려면 수동으로 검토하고 승격해야 할 수 있습니다. 이벤트 승격에 관한 정보는 보안 서비스 익스체인지에서 온라인 도움말의 정보를 참조하십시오. SSE에 액세스하는 방법은 Access(액세스) 보안 서비스 익스체인지의 내용을 참조하십시오.
단계	(선택 사항) 보안 서비스 익스체인지에서 중요하지 않은 특정 이벤트의 자동 삭제를 구성합니다.	이벤트 필터링에 관한 정보는 보안 서비스 익스체인지에서 온라인 도움말의 정보를 참조하십시오. SSE에 액세스하는 방법은 Access(액세스) 보안 서비스 익스체인지의 내용을 참조하십시오.
단계	SecureX에서 Firepower 모듈을 추가합니다.	SecureX에서 **Integration Modules(**통합 모듈**) > Available Integration Modules(**사용 가능한 통합 모듈**)**로 이동하여 Firepower 모듈을 추가합니다. 이 모듈에 관한 자세한 내용은 SecureX의 온라인 도움말을 참조하십시오.

Access(액세스) 보안 서비스 익스체인지

시작하기 전에

브라우저에서 팝업 차단을 비활성화합니다.

프로시저

단계 **1** 브라우저 창에서 사용자의SecureX 클라우드로 이동합니다.

- 북미 클라우드: https://securex.us.security.cisco.com
- 유럽 클라우드: https://securex.eu.security.cisco.com
- 아시아 클라우드: https://securex.apjc.security.cisco.com

단계 **2** SecureX, AMP for Endpoints, Cisco Threat Grid 또는 Cisco Security 계정 관련 자격 증명을 사용하여 로그인합니다.

계정 자격 증명은 지역 클라우드마다 다릅니다.

단계 **3** 보안 서비스 익스체인지(으)로 이동합니다.

Integrations(통합**) > Devices(**디바이스**) > Manage Devices(**디바이스 관리**)**를 선택합니다.

보안 서비스 익스체인지 가 새 브라우저 창에서 열립니다.

이벤트가 (시스템 로그를 통해) 보안 서비스 익스체인지에 도달하는지 확인합니다.

시작하기 전에

예상한 이벤트가 Firepower에 정상적으로 표시되는지 확인합니다.

프로시저

단계 **1** 메시지가 프록시에서 보안 서비스 익스체인지(으)로 포워딩될 수 있도록, Firepower 디바이스가 지원되는 이벤트를 탐지한 후 15분 동안 기다립니다.

단계 **2** Access(액세스) 보안 서비스 익스체인지, 4 페이지.

단계 **3** 보안 서비스 익스체인지에서 **Events(**이벤트**)**를 클릭합니다.

단계 **4** 디바이스에서 이벤트를 찾습니다.

예상한 이벤트가 표시되지 않는다면 시스템 로그 통합 문제 해결, 5 페이지의 팁을 참조하고 시스템 로그를 이용해 Cisco Cloud에 이벤트를 전송하는 방법, 2 페이지에서 다시 확인해 보십시오.

시스템 로그 통합 문제 해결

이벤트가 CSSP에 도달하지 않습니다.

디바이스가 네트워크의 CSSP에 연결할 수 있는지 확인합니다.

클라우드에 액세스하는 데 문제가 있습니다.

- 클라우드 계정을 활성화한 직후 이 통합 구성을 시도했는데 통합 구현에서 문제가 발생했다면, 1~2시간 기다린 다음 클라우드 계정에 로그인하십시오.
- 계정에 연결된 지역 클라우드의 URL에 액세스하는지 확인합니다.

예상 이벤트가 이벤트 목록에 없습니다.

다음을 확인합니다.

- Events(이벤트) 페이지에서 **Refresh(**새로고침**)** 버튼을 눌러 목록을 새로고칩니다.
- 예상한 이벤트가 Firepower에 표시되는지 확인합니다.

- SSE의 **Cloud Services(**클라우드 서비스**)** 페이지에 있는 **Eventing(**이벤팅**)** 설정에서 자동 삭제(필터링을 통한 이벤트 제거) 구성을 확인합니다.
- 이벤트를 전송하는 지역 클라우드를 보고 있는지 확인합니다.

시스템 로그 필드 관련 질문

시스템 로그 필드 및 설명에 관한 내용은 https://www.cisco.com/c/en/us/support/security/defense-center/products-system-message-guides-list.html에 있는 *Cisco Firepower Threat Defense* 시스템 로그 메시지 가이드를 참조하십시오.

일부 이벤트가 **SecureX** 타일에서 누락됨

전역 차단 또는 허용 목록을 포함하여 FMC에서 맞춤형 보안 인텔리전스 개체를 사용하는 경우 해당 개체를 사용하여 처리되는 이벤트를 자동으로 승격하도록 SSE를 구성해야 합니다. 이벤트를 인시던트로 승격하는 정보는 SSE의 온라인 도움말을 참조하십시오. .