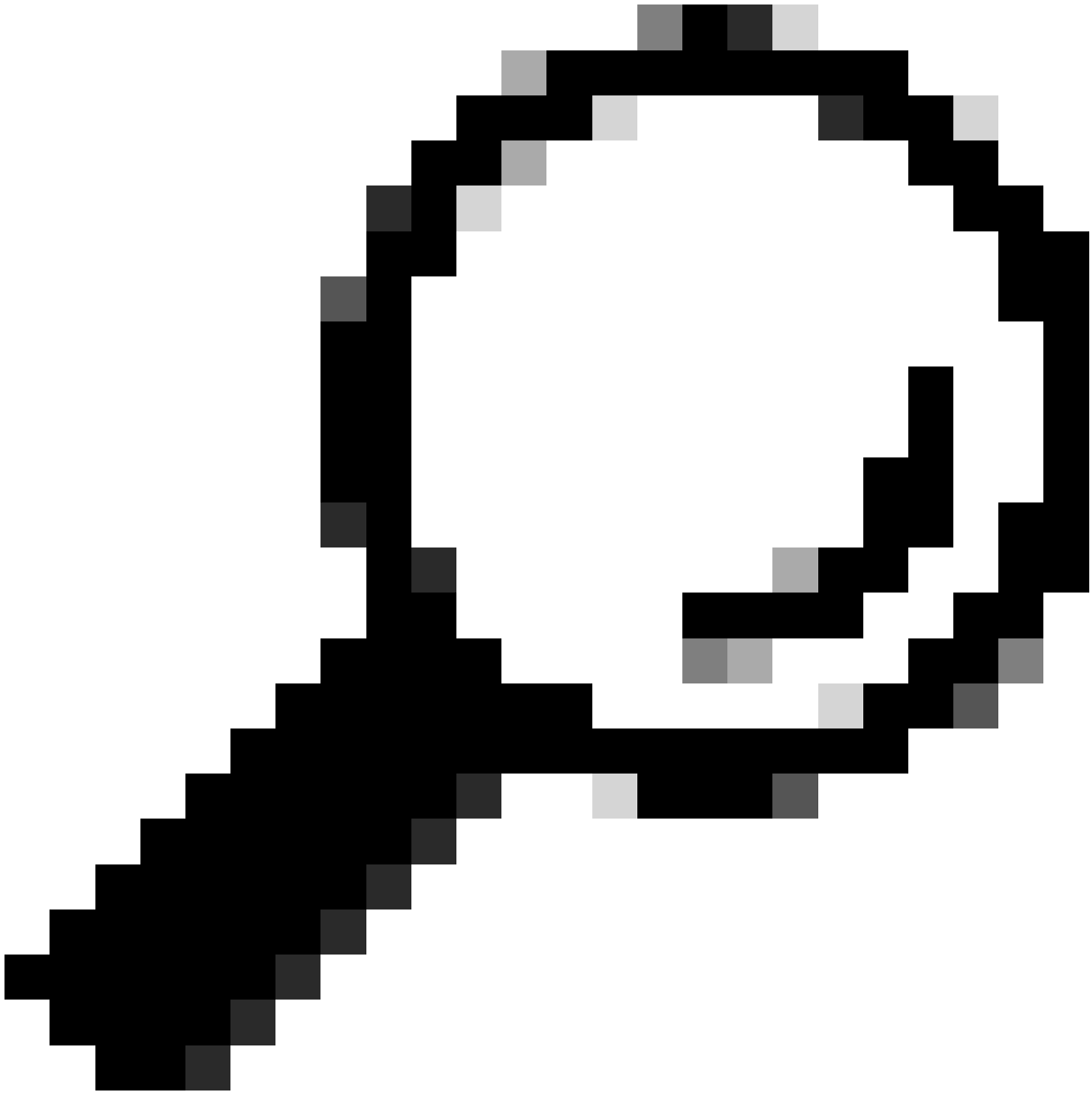
Secure Network Analytics 외부 연결 이해 가이드

목차

소개

이 가이드를 사용하여 특정 Secure Network Analytics 기능이 신속하게 작동하는 데 필요한 외부 연결을 검토할 수 있습니다. 이러한 외부 연결은 도메인 또는 엔드포인트가 될 수 있습니다. 도메인은 인터넷, 일반적으로 웹 사이트 또는 서비스에서 리소스를 식별하는 데 사용되는 이름입니다. 엔드포인트는 네트워크를 통해 통신하는 실제 디바이스 또는 노드입니다. 이 설명서에서는 웹 서비스를 중점적으로 다루므로 이러한 서비스는 URL로 표시됩니다. 이 표에는 외부 연결 URL이 알파벳 순으로 나열되어 있습니다.



팁: 이 표에는 외부 연결 URL이 알파벳순으로 나열되어 있습니다.

외부 연결

외부 연결 URL	목적
https://analytics.int.obsrvbl.com	Secure Cloud Analytics 서비스와의 텔레메트리 데이터 교환을 위해 Secure Network Analytics에서 사용됩니다.

https://api.apj.sse.itd.cisco.com	APJC(아시아 태평양, 일본, 중국) 리전의 AWS(Amazon Web Services)로 데이터를 전송하기 위해 Cisco에서 요청합니다. Cisco XDR에 경고를 전달할 때 그리고 고객 서비스 메트릭에 사용할 때 사용됩니다.
https://api.eu.sse.itd.cisco.com	유럽(EU) 리전의 경우 Amazon Web Services(AWS)로 데이터를 전송하기 위해 Cisco에서 요구합니다. Cisco XDR에 경고를 전달할 때 그리고 고객 서비스 메트릭에 사용할 때 사용됩니다.
https://api-sse.cisco.com	미국(US) 리전의 Amazon Web Services(AWS)로 데이터를 전송하기 위해 Cisco에서 요구하는 사항입니다. Cisco XDR에 알림을 전달할 때 그리고 고객 서비스/성공 메트릭을 위해 사용됩니다.
https://apix.cisco.com	직접 소프트웨어 다운로드 기능을 위해 Secure Network Analytics에서 사용됩니다.
https://dex.sse.itd.cisco.com	고객 성공 메트릭을 보내고 수집하

	는 데 필요합니다 .
https://est.sco.cisco.com	고객 성공 메트릭을 보내고 수집하는 데 필요합니다 .
https://eventing-ingest.sse.itd.cisco.com	고객 성공 메트릭을 보내고 수집하는 데 필요합니다 .
https://feodotracker.abuse.ch/downloads/ipblocklist.txt	Threat Feed에 필요합니다. Threat Feed는 Analytics가 활성화된 경우 Secure Network Analytics 경고 및 관찰에 사용됩니다.
https://id.cisco.com	직접 소프트웨어 다운로드 기능을 위해 Secure Network Analytics에서 사용됩니다.
https://intelligence.sourcefire.com/auto-update/auto-dl.cgi/00:00:00:00:00:00/Download/files/ip-filter.gz	Threat Feed에 필요합니다. Threat Feed는 Analytics가 활성화된 경우 Secure Network Analytics 경고 및 관찰에 사용됩니다.
https://intelligence.sourcefire.com/auto-update/auto-dl.cgi/00:00:00:00:00:00/Download/files/url-filter.gz	Threat Feed에 필요합니다. Threat Feed는 Analytics가 활성화된 경우 Secure Network Analytics 경고 및 관찰에 사용됩니다.
https://lancope.flexnetoperations.com/control/lncp/LancopeDownload	Secure Network Analytics Threat Intelligence

	Feed에 필요하며, Secure Network Analytics 경보 및 보안 이벤트에 사용됩니다. 이를 위해서는 Secure Network Analytics Threat Intelligence Feed 라이센스가 필요합니다.
https://mx*.sse.itd.cisco.com	고객 성공 메트릭을 보내고 수집하는 데 필요합니다.
https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json	Analytics가 활성화된 경우 알림에 대한 MITER 정보에 액세스할 수 있습니다.
https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobile-attack.json	Analytics가 활성화된 경우 알림에 대한 MITER 정보에 액세스할 수 있습니다.
https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json	Analytics가 활성화된 경우 알림에 대한 MITER 정보에 액세스할 수 있습니다.
https://s3.amazonaws.com/onconfig/global-blacklist	Required Threat Feed(필수 위협 피드). 분석이 활성화된 경우 Secure Network Analytics 경고 및 관찰에 사용됩니다.
https://sensor.anz-prod.obsrvbl.com	APJC(아시아 태평양, 일본, 중국) 리전의 AWS(Amazon Web Services)로 데이터를 전송하기 위해 Cisco에서 요청합니다.

	Cisco XDR에 경고를 전달할 때 그리고 고객 서비스 메트릭에 사용할 때 사용됩니다.
https://sensor.eu-prod.obsrvbl.com	유럽(EU) 리전의 경우 Amazon Web Services(AWS)로 데이터를 전송하기 위해 Cisco에서 요구합니다. Cisco XDR에 경고를 전달할 때 그리고 고객 서비스 메트릭에 사용할 때 사용됩니다.
https://sensor.ext.obsrvbl.com	미국(US) 리전의 Amazon Web Services(AWS)로 데이터를 전송하기 위해 Cisco에서 요구하는 사항입니다. Cisco XDR에 경고를 전달할 때 그리고 고객 서비스 메트릭에 사용할 때 사용됩니다.
smartreceiver.cisco.com	Cisco Smart Software Licensing 액세스에 사용됩니다. 자세한 내용은 Smart Licensing Guide를 참조하십시오. 원하는 경우 대체 오프라인 라이센싱을 사용할 수 있습니다. 자세한 내용은 릴리스 정보를 참조하십시오.
https://software.cisco.com	직접 소프트웨어 다운로드 기능을

	위해 Secure Network Analytics에서 사용됩니다.
https://www.cisco.com	스마트 라이센싱, 클라우드 프록시 및 방화벽 연결 테스트에 사용되는 Cisco 도메인에 필요합니다.

추가 정보

특정 도메인 및 엔드포인트 연결이 사용되는 방법과 이유를 자세히 알아보려면 다음 항목을 참조하십시오.

- Cisco SSE(Secured Service Exchange)
- 직접 소프트웨어 다운로드(베타)
- 사접 ATT&CK® 프레임워크
- 위협 피드

Cisco SSE(Secured Service Exchange)

SSE 엔드포인트는 Cisco에서 고객 서비스 메트릭을 위해 Amazon Web Services(AWS)로 데이터를 전송하는 데 사용되며, Cisco XDR에 알림을 전달하는 경우에도 사용됩니다. 이는 다양합니다. SSE 커넥터에서 제공하는 서비스 검색 메커니즘을 사용하여 동적으로 이러한 엔드포인트를 검색합니다. Cisco XDR에 탐지를 게시할 때 Secure Network Analytics는 "xdr-data-platform"이라는 제목의 서비스와 해당 API 엔드포인트 "Events"를 검색하려고 시도합니다.

지역 및 호스트

운영 환경의 지역에 따라 호스트는 다음과 같습니다.

미국:

- https://api-sse.cisco.com
- https://sensor.ext.obsrvbl.com

EU:

- https://api.eu.sse.itd.cisco.com
- https://sensor.eu-prod.obsrvbl.com

APJC:

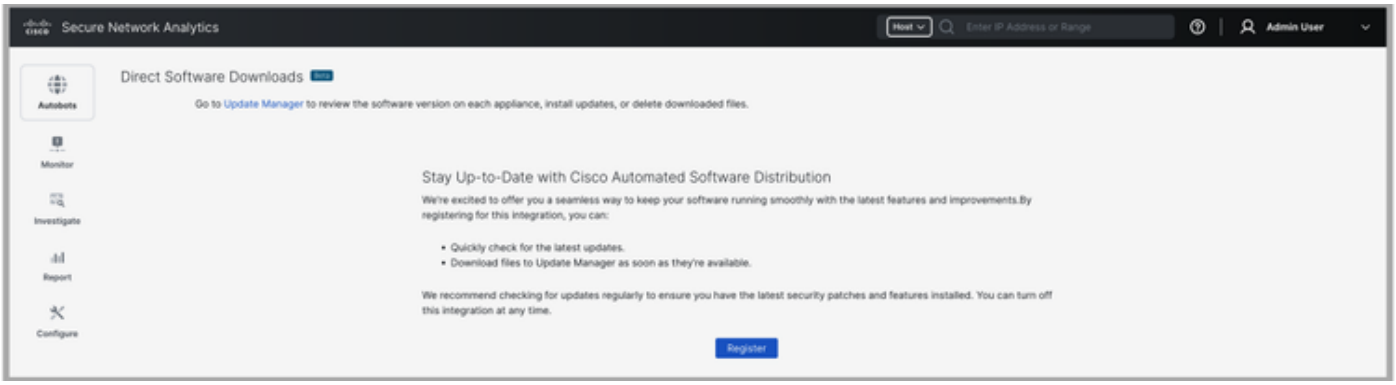
- https://api.apj.sse.itd.cisco.com
- https://sensor.anz-prod.obsrvbl.com

직접 소프트웨어 다운로드(베타)

직접 소프트웨어 다운로드 기능에서는 다음 연결을 사용합니다.

- https://apix.cisco.com
- https://software.cisco.com
- https://id.cisco.com

이 새 기능을 사용하여 소프트웨어 및 패치 업데이트 파일을 Update Manager로 직접 다운로드하려면 cisco.com 사용자 ID(CCOID)를 사용하여 등록했는지 확인하십시오.
1. Manager에 로그인합니다.
2. 주 메뉴에서 구성 > 글로벌 > 중앙 관리를 선택합니다.
3. 갱신 관리자 탭을 클릭합니다.
4. Direct Software Downloads(직접 소프트웨어 다운로드) 링크를 클릭하여 등록 페이지를 엽니다.
5. 등록 버튼을 클릭하여 등록 프로세스를 시작합니다.



6. 제공된 링크를 클릭합니다.
7. [장치 활성화] 페이지로 이동합니다. 계속하려면 다음을 클릭합니다.
8. cisco.com 사용자 ID(CCOID)로 로그인합니다.
9. 활성화가 완료되면 "Device Activated(디바이스 활성화)" 메시지가 표시됩니다.
10. 관리자의 [직접 소프트웨어 다운로드] 페이지로 돌아가서 [계속]을 클릭합니다.
11. 약관을 읽고 동의하려면 EULA 및 K9 계약의 링크를 클릭합니다. 약관에 동의하면 계속을 클릭합니다.

직접 소프트웨어 다운로드에 대한 자세한 내용은 Cisco 지원에 문의하십시오

사접 ATT&CK® 프레임워크

MITER ATT&CK® 프레임워크는 실제 관찰을 기반으로 한 공격자 전술 및 기법에 대한 공개 지식 기반입니다. Secure Network Analytics 내에서 Analytics를 활성화한 경우 MITER 전술 및 기술은 사이버 보안 위협 인텔리전스, 탐지 및 대응을 지원합니다.

To make sure Analytics is enabled, choose **Configure** > **Detection** > **Analytics** from the main menu, then click *Analytics On*  .

다음 연결을 통해 Secure Network Analytics에서 MITER 정보에 액세스할 수 있습니다
경고문:

- https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json
- https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobileattack.json
- https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterpriseattack.json

위협 피드

Cisco Secure Network Analytics Threat Feed(이전의 Stealthwatch Threat Intelligence Feed)는 네트워크의 위협에 대한 글로벌 위협 피드의 데이터를 제공합니다. 피드는 자주 업데이트되며 악의적인 활동에 사용되는 것으로 알려진 IP 주소, 포트 번호, 프로토콜, 호스트 이름 및 URL을 포함합니다. 다음 호스트 그룹이 피드에 포함됩니다. C&C(command-and-control) 서버, bogons 및 Tor가 있습니다.

중앙 관리에서 위협 피드를 활성화하려면 도움말의 지침을 따르십시오.

1. 기본 Manager에 로그인합니다.
2. 구성 > 글로벌 > 중앙 관리를 선택합니다.
3. (도움말) 아이콘을 클릭합니다. 도움말을 선택합니다.
4. Appliance Configuration(어플라이언스 컨피그레이션) > Threat Feed(위협 피드)를 선택합니다.

Please note that you will configure the DNS server and firewall as part of the instructions. Also, if you have a failover configuration, you need to enable Threat Feed on your primary Manager and secondary Manager.

위협 피드에 대한 자세한 내용은 시스템 컨피그레이션 가이드를 참조하십시오.

지원 문의

기술 지원이 필요한 경우 다음 중 하나를 수행하십시오.

- 현지 Cisco 파트너에게 문의하십시오.
- Cisco 지원에 문의
- 웹을 통해 케이스를 열려면 http://www.cisco.com/c/en/us/support/index.html
- 전화 지원: 1-800-553-2447(미국)
- 전 세계 지원 번호: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.