

# 보안 클라우드 분석에서 Cisco XDR로 전환

## 목차

- [핵심 변경 사항](#)
- [즉각적인 조치 및 중요 날짜](#)
- [사용 중단, 변경 또는 사용 불가](#)
- [고객 준비도 체크리스트](#)
- [새로운 XDR 환경에서 원하는 방식 찾기](#)
- [탐지, 사고 및 관찰 활용 사례](#)
- [알림, 내보내기, 웹후크 및 자동화](#)
- [텔레메트리 소스 및 소스별 컷오버](#)
- [설정, 조정, 감시 목록 및 자산 컨텍스트](#)
- [센서, 클라우드 통합, 운영 상태](#)
- [기록 데이터, 보고 및 관리](#)
- [API 및 맞춤형 통합](#)
- [완료된 전환 항목](#)

## 핵심 변경 사항

Secure Cloud Analytics 사용자 환경은 2026년 10월 24일에 더 이상 제공되지 않습니다. Cisco XDR은 SCA 파생 탐지, 조사, 자산 상황, 알림, 내보내기 및 관련 워크플로의 운영 인터페이스가 됩니다.



주의: 전용 SCA-XDR 고객 전환 프로그램은 9월 30일에 종료될 예정이며, 2026년 10월 24일은 SCA 사용자 인터페이스의 계획된 사용 중단 날짜로 남아 있습니다. Cisco XDR을 지금 활성화하면 아래에서 설명하는 준비 작업을 완료할 수 있습니다.

## 즉각적인 조치 및 중요 날짜

무슨 일이 일어나고 있고, 이제 어떻게 해야 하나요?

| 상태   | 필요한 조치                                                                                                                            |
|------|-----------------------------------------------------------------------------------------------------------------------------------|
| 세부사항 | Cisco는 SCA 사용자 환경을 중단하고 SCA 파생 기능을 Cisco XDR로 전환합니다. 텔레메트리 및 분석은 활동, 탐지, 사고, 조사, 자산 컨텍스트, 응답 및 자동화를 위한 보다 광범위한 XDR 워크플로의 일부가 됩니다. |

|       |                                                                                                                            |
|-------|----------------------------------------------------------------------------------------------------------------------------|
| 고객 조치 | XDR 활성화, SCA 테넌트 연결, 액세스 검증, 일상적인 작업에 XDR 탐지 및 인시던트 사용, 소스 원격 측정 컷오버에 대한 활동 사용, XDR 워크플로 테스트, 2026년 10월 24일 이전에 기록 정보 내보내기 |
|-------|----------------------------------------------------------------------------------------------------------------------------|

몇일 정도에 계획을 세워야 하나요?

| 날짜            | 마일스톤                                                    | 의미                                          |
|---------------|---------------------------------------------------------|---------------------------------------------|
| 2026년 9월 15일  | 선택한 고객을 위한 AWS 및 Azure 구성 설정                            | 영향을 받는 미국 및 EMEA 고객은 권장 XDR 구성 방법으로 이동합니다.  |
| 2026년 9월 30일  | 전용 SCA-XDR 고객 전환 프로그램 종료                                | 프로그램이 종료되기 전에 엔타이틀먼트, 프로비저닝 및 준비 작업을 완료합니다. |
| 2026년 10월 7일  | AWS CloudTrail, Azure Activity Log, GCP Audit Log 탐지    | XDR에서 이러한 소스 작동                             |
| 2026년 10월 14일 | 맞춤형 이벤트 탐지 컷오버; XDR에서 사용 가능한 인시던트 조정, 감시 목록 및 엔터티 그룹 구성 | 관련 워크플로 및 구성을 XDR로 이동합니다.                   |
| 2026년 10월 21일 | NetFlow 탐지 컷오버                                          | XDR에서 NetFlow 탐지 작업                         |
| 2026년 10월 24일 | SCA 사용자 경험을 더 이상 사용할 수 없음                               | 이 날짜 전에 XDR로 이동을 완료하고 기록 데이터를 내보냅니다.        |

아무것도 하지 않거나 XDR을 프로비저닝하지 않은 경우 어떻게 됩니까?

|       |                                                                                                                                                                                       |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 상태    | 권장하지 않음                                                                                                                                                                               |
| 세부사항  | SCA 사용자 환경이 제거되기 전에 Cisco XDR을 활성화하여 연결하지 않으면 SCA에 액세스할 수 없으며 SCA 파생 워크플로, 탐지, 조사, 통합 또는 기록 데이터에 사용할 수 있는 대체 XDR 환경이 없습니다. 대기 기능은 또한 활성화, 사용자 설정, 워크플로 검증 및 운영 변경을 전환의 최종 부분으로 압축합니다. |
| 고객 조치 | 팀이 2026년 9월 30일 이전에 사용자 설정, 워크플로 유효성 검사 및 내보내기 준비를 완료할 수 있도록 지금 XDR을 활성화하고 연결합니다. SCA 인터페이스는 2026년 10월 24일 종단 대상으로 유지됩니다. 연결된 XDR 테넌트가 없으면 SCA 액세스가 종료될 때 사용 가능한 대체 XDR 환경이 없습니다.     |

사용 중단, 변경 또는 사용 불가

어떤 SCA 개념이 동일한 형태로 명시적으로 지속되지 않습니까?

|      |                                                                                                                                                                 |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 상태   | 변경 또는 처분                                                                                                                                                        |
| 세부사항 | <ul style="list-style-type: none"> <li>SCA 사용자 환경: 2026년 10월 24일 삭제됨</li> <li>레거시 SCA 웹후크 동작: XDR 워크플로로 대체됩니다.</li> <li>SCA 관찰 경험: 일대일 XDR 기능이 아닙니다.</li> </ul> |

|  |                                                                                                                                                                                                                                                                                                               |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <ul style="list-style-type: none"> <li>• 서브넷 감도: 자산 가치 우선순위 지정 개념으로 대체됩니다.</li> <li>• 엔티티 그룹: 자산 레이블, 자산 그룹 및 값 점수로 교체됩니다.</li> <li>• 스누징된 탐지 설정: 마이그레이션되지 않음; 사용 가능한 경우 인시던트 조정을 사용합니다.</li> <li>• 고객 제어 알림 우선 순위 동작: 보존되지 않습니다.</li> <li>• 일부 보고, 사용량이 적은 페이지 및 기능: XDR 네이티브 경험으로 대체되거나 폐기되었습니다.</li> </ul> |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

더 이상 사용되지 않거나 이동해야 하는 보고 또는 통합 항목은 무엇입니까?

| 상태   | 예상 변경                                                                                                                                                           |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 세부사항 | 클라우드 상태 감시 목록, Kubernetes 모니터링, AWS 시각화/대시보드/세션 검색/IP 검색 경험, Meraki 및 Umbrella 컨텍스트 통합, 이메일 기반 월간 보고서 및 일별 알림 요약이 포함됩니다. 이 목록은 각 레거시 페이지에 대해 일대일 교체를 약속하지 않습니다. |

이 마이그레이션에서 나에게 묻지않는 것은 무엇입니까?

| 상태   | 이 유형의 작업 없음                                                                                                                            |
|------|----------------------------------------------------------------------------------------------------------------------------------------|
| 세부사항 | Cisco는 고객에게 기존 네트워크 센서를 재배포하거나, UX 마이그레이션만을 위해 클라우드 로그 수집을 재구성하거나, 지원되는 표준 탐지 컨피그레이션 객체를 수동으로 재생성하거나, SCA를 장기적 병렬 콘솔로 보존하도록 요구하지 않습니다. |

## 고객 준비도 체크리스트

1. 전환 프로그램이 종료되기 전에 준비 작업을 완료할 수 있도록 Cisco XDR을 활성화하고 2026년 9월 30일 전에 기존 SCA 테넌트를 연결합니다.
2. XDR에서 사용자를 만들고, 로그인을 확인하고, 적절한 액세스를 확인합니다.
3. 탐지, 사고, 활동, 조사, 자산 인사이트/장치 인사이트를 검토합니다.
4. 모든 SCA 웹훅, 내보내기, 알림, SIEM/SOAR 전달 및 사용자 정의 자동화를 XDR 워크플로 또는 다른 XDR 운영 표면에 매핑합니다.
5. 각 소스를 사용할 수 있게 되면 Activities(활동)에서 필요한 소스 텔레메트리를 검증합니다.
6. 각 소스 컷오버 전에 필수 탐지 및 응답 플레이북을 검증합니다.
7. 서브넷 민감도, 엔티티 그룹, 스누징, 알림 우선 순위, 감시 목록, 스캐너 규칙, 신뢰할 수 있는 네트워크, 자산 가치 우선 순위 등을 검토합니다.
8. 레거시 보고서, SCA 전용 페이지, API 종속성 인벤토리 대체 또는 내보내기 요구 사항을 파악합니다.
9. 2026년 10월 24일 이전에 필요한 경고, 관찰, 원시 로그, 컨피그레이션 레코드 및 보고서를 내 보냅니다.

## 새로운 XDR 환경에서 원하는 방식 찾기

SCA 고객은 Cisco XDR을 사용할 수 있습니까?

|       |                                                                                        |
|-------|----------------------------------------------------------------------------------------|
| 상태    | 전환의 일부로 사용 가능                                                                          |
| 세부사항  | 기존 SCA 고객은 전환의 일부로 Cisco XDR을 사용할 수 있습니다. 의도한 결과는 핵심 워크플로가 XDR로 이동하는 동안 SCA 가치를 지속합니다. |
| 고객 조치 | Cisco XDR을 활성화하고 기존 SCA 테넌트를 연결한 다음 도움이 필요한 경우 Cisco XDR 활성화 프로세스를 사용합니다.              |

Cisco XDR에서 SCA 기능은 어디에 상주합니까?

|                           |                               |
|---------------------------|-------------------------------|
| SCA 기능                    | XDR 대상                        |
| 경고 및 경고 워크플로              | XDR 탐지 및 인시던트                 |
| 관찰 및 이벤트 중심 조사            | XDR 작업 및 XDR 조사               |
| 이벤트 뷰어                    | XDR 조사 및 작업                   |
| 장치 컨텍스트                   | 자산 인사이트/장치 인사이트               |
| 웹 후크, 공지, 내보내기 및 다운스트림 전달 | XDR 워크플로                      |
| 탐지 컨피그레이션                 | 각 설정이 중요 시점에 도달할 때의 XDR 구성 환경 |

SCA는 계속 일용 콘솔 형태로 사용할 수 있습니까?

|      |                                                                                                |
|------|------------------------------------------------------------------------------------------------|
| 상태   | 아니요                                                                                            |
| 세부사항 | SCA 사용자 경험은 2026년 10월 24일에 제거될 예정입니다. 중첩 기간을 사용하여 XDR 운영 모델을 실행하고 워크플로를 검증하고 Runbook을 업데이트합니다. |

탐지, 사고 및 관찰 활용 사례

탐지 시스템이 단순히 일대일 방식으로 이동하는 것일까요?

|       |                                                                                                               |
|-------|---------------------------------------------------------------------------------------------------------------|
| 상태    | 모델 변경                                                                                                         |
| 세부사항  | 아니요. Cisco는 기존의 모든 SCA 알림을 변경되지 않은 XDR 객체로 복사하는 대신 탐지 콘텐츠와 운영 모델을 발전시키고 있습니다. 이름, 논리, 증거, 상관관계, 결과가 달라질 수 있다. |
| 고객 조치 | XDR 탐지 결과, 증거 및 사고 상관관계를 작동해야 하는 보안 시나리오와 비교 평가합니다. 이름 일치만 수락으로 사용하지 마십시오.                                    |

경고 워크플로에 XDR 인시던트 또는 탐지를 사용해야 합니까?

|       |                                                                                                                          |
|-------|--------------------------------------------------------------------------------------------------------------------------|
| 상태    | 결과별로 선택                                                                                                                  |
| 세부사항  | 인시던트 대응, 애널리스트 알림, 분류, 에스컬레이션, 케이스 관리, 공동 대응에 인시던트 활용 개별 검색 결과, 탐지 레벨 내보내기, M2M 자동화에 Detections를 사용합니다. 활동은 텔레메트리 표면입니다. |
| 고객 조치 | 필요에 따라 인시던트에서 인시던트 알림 및 응답 프로세스가 트리거되도록                                                                                  |

|  |                                                              |
|--|--------------------------------------------------------------|
|  | Runbook 업데이트 자세한 분석, 내보내기 및 찾기 수준 자동화를 위해 Detections를 사용합니다. |
|--|--------------------------------------------------------------|

관찰 기반 활용 사례는 계속 진행됩니까?

|       |                                                                                                    |
|-------|----------------------------------------------------------------------------------------------------|
| 상태    | 일대일 아님                                                                                             |
| 세부사항  | 레거시 관찰 이름, UI 객체 또는 트리거 조건이 남아 있다고 가정하지 마십시오. 대상은 활동, 탐지, 사고 및 더 광범위한 상관관계를 통해 동등하거나 개선된 지원 범위입니다. |
| 고객 조치 | 2026년 10월 24일 이전에 Runbook, 대시보드 및 자동화의 종속성을 파악하고 업데이트합니다.                                          |

NetFlow에 주로 의존하여 EDR을 구축할 수 없는 경우에는 어떻게 됩니까?

|       |                                                                                           |
|-------|-------------------------------------------------------------------------------------------|
| 상태    | 아직 범위 내                                                                                   |
| 세부사항  | 기존 네트워크 센서 및 수집은 계속 작동하며, 마이그레이션된 네트워크 탐지를 계속 사용하는 데 EDR 구축이 필요하지 않습니다.                   |
| 고객 조치 | XDR 탐지, 검색 결과, 인시던트, 인시던트 조정 및 사용 가능한 자산 컨텍스트를 사용합니다. 엔드포인트 가시성의 제약이 심할 경우 구축별 지침을 요청합니다. |

## 알림, 내보내기, 웹훅 및 자동화

SCA 웹훅은 어떻게 됩니까?

|       |                                                                                                                                                    |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 상태    | 마이그레이션 및 테스트                                                                                                                                       |
| 세부사항  | XDR 자동화 워크플로는 알림, 내보내기 및 다운스트림 자동화를 위한 장기적인 제어 지점입니다. 대상 내보내기 경로는 OCSF에 맞춰져 있으며 기존 SCA Alerts and Observations 모델보다 더 완벽한 상황 탐지 세부 정보를 제공할 수 있습니다. |
| 고객 조치 | 웹훅이 사람, SIEM, SOAR 또는 다른 시스템에 탐지 정보를 보내는 경우 XDR 워크플로에서 해당 동작을 다시 만들고 테스트합니다.                                                                       |

탐지 및 인시던트 워크플로의 차이점은 무엇입니까?

|      |                                                                                                                                   |
|------|-----------------------------------------------------------------------------------------------------------------------------------|
| 상태   | 일치 트리거 사용                                                                                                                         |
| 세부사항 | 데이터 이동, 내보내기 및 머신 소비에 탐지 지향 워크플로를 사용합니다. 더 광범위한 운영 활동 및 이메일, Slack 또는 Webex와 같은 사람 알림에 인시던트 지향 워크플로를 사용합니다. 둘 다 내보내기를 지원할 수 있습니다. |

SIEM, SOAR 또는 맞춤형 다운스트림 통합에 대한 변경 사항은 무엇입니까?

|      |                                                                                                                                   |
|------|-----------------------------------------------------------------------------------------------------------------------------------|
| 상태   | 검토 필요                                                                                                                             |
| 세부사항 | SCA별 Webhook, Payload, Alert Name 또는 Export가 변경되지 않고 계속된다고 가정하지 마십시오. 대상 내보내기 경로는 OCSF에 맞춰져 있으며 더욱 완전하고 상황별 탐지 세부 정보를 제공할 수 있습니다. |

|       |                                                                       |
|-------|-----------------------------------------------------------------------|
| 고객 조치 | 종속성을 XDR 워크플로 및 XDR 데이터 모델로 마이그레이션한 다음 다운스트림 수신 및 Runbook 동작을 테스트합니다. |
|-------|-----------------------------------------------------------------------|

### NVM 알림 및 내보내기를 변경해야 합니까?

|       |                                                                                                            |
|-------|------------------------------------------------------------------------------------------------------------|
| 상태    | NVM 컷오버 완료                                                                                                 |
| 세부사항  | NVM 탐지는 2026년 5월에 XDR로 이동했습니다. 레거시 NVM 웹후크 패턴에 의존하는 고객은 2026년 5월 15일 컷오버까지 알림 및 내보내기를 XDR 워크플로로 이동해야 했습니다. |
| 고객 조치 | 계속해서 NVM에 대한 XDR 워크플로 패턴을 사용하고 검증합니다.                                                                      |

### 소스 컷오버 전에 무엇을 테스트해야 합니까?

|       |                                                                                                                          |
|-------|--------------------------------------------------------------------------------------------------------------------------|
| 상태    | 필수 준비도 검사                                                                                                                |
| 고객 조치 | 각 소스에 대해 탐지 또는 인시던트 트리거, 알림 또는 내보내기 페이로드, 다운스트림 수신, 필터링 또는 라우팅 규칙, 업데이트된 Runbook 응답을 테스트합니다. 소스가 SCA 환경을 종료하기 전에 테스트합니다. |

## 텔레메트리 소스 및 소스별 컷오버

### XDR 활동에서 텔레메트리를 언제 사용할 수 있습니까?

| 날짜           | 텔레메트리 중요 시점                                      | 고객 조치                     |
|--------------|--------------------------------------------------|---------------------------|
| 2026년 8월 19일 | 활동의 ONA 데이터 텔레메트리                                | ONA 텔레메트리 검토를 시작합니다.      |
| 2026년 8월 26일 | 활동의 CTB 데이터 텔레메트리                                | CTB 텔레메트리 검토를 시작합니다.      |
| 2026년 9월 16일 | AWS VPC 플로우 로그, Azure 플로우 로그 및 GCP VPC 플로우 로그 활동 | 클라우드 플로우 텔레메트리 검토를 시작합니다. |
| 2026년 9월 23일 | XDR의 AWS 소스 구성                                   | 해당하는 경우 XDR 구성 환경을 사용합니다. |
| 2026년 9월 30일 | AWS CloudTrail, Azure 활동 로그 및 GCP 감사 로그 활동       | 감사 로그 텔레메트리 검토를 시작합니다.    |

### 네트워크 센서를 재배포하거나 클라우드 로그 수집을 재구성해야 합니까?

|           |                                                                                                                                |
|-----------|--------------------------------------------------------------------------------------------------------------------------------|
| 상태        | 아니요, UX 마이그레이션에만 해당되지 않음                                                                                                       |
| 세부사항      | 기존 네트워크 센서 및 클라우드 로그 수집은 이 단계에서 계속 작동하며, 사용자 환경 및 탐지가 XDR로 이동하기 때문에 재구축하거나 재구성할 필요가 없습니다.                                      |
| 중요한 예외 사항 | 센서 및 통합에서 사용하는 공용 IP 주소 또는 엔드포인트가 변경될 수 있습니다. 방화벽 규칙, 프록시 허용 목록 및 기타 네트워크 제어 검토 Cisco는 구성을 변경하기 전에 필요한 XDR 엔드포인트 세부 정보를 제공합니다. |

## 소스 탐지는 언제 중단됩니까?

| 상태   | 소스별 일정                                                                                                                                                                                                                                                          |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 세부사항 | <p>컷오버 시 해당 소스에 대한 텔레메트리 및 탐지는 더 이상 SCA 사용자 환경을 통해 사용할 수 없습니다.</p> <ul style="list-style-type: none"><li>• 2026년 10월 7일: AWS CloudTrail, Azure Activity Log 및 GCP 감사 로그 탐지.</li><li>• 2026년 10월 14일: 맞춤형 이벤트 탐지.</li><li>• 2026년 10월 21일: NetFlow 탐지.</li></ul> |

## 설정, 조정, 감시 목록 및 자산 컨텍스트

### 탐지 컨피그레이션이 마이그레이션됩니까?

| 상태    | 단계별 마이그레이션                                                                                                                           |
|-------|--------------------------------------------------------------------------------------------------------------------------------------|
| 세부사항  | <p>지원되는 표준 컨피그레이션 객체는 더 광범위한 탐지 엔진 전환의 일부로 마이그레이션될 것으로 예상됩니다. NVM 탐지 설정이 2026년 5월에 XDR로 이동했습니다. 다른 설정은 해당 기능을 사용할 수 있게 되면 전환됩니다.</p> |
| 고객 조치 | <p>Cisco에서 구축에 대한 특정 지침을 게시하지 않는 한 마이그레이션에 대한 표준 설정만 수동으로 다시 생성하지 마십시오.</p>                                                          |

### 서브넷 민감도, 엔티티 그룹 및 Snooze를 대체하는 것은 무엇입니까?

| 상태   | 개념 변경                                                                                                                                                                                                                                                                                                                                                  |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 세부사항 | <ul style="list-style-type: none"><li>• 서브넷 감도: Asset Insights/Device Insights의 디바이스 가치 우선순위 점수로 대체됨 2026년 9월 30일까지 XDR Device Insights에서 예약됩니다.</li><li>• 엔티티 그룹: 2026년 10월 14일에 XDR Device Insights에서 예약된 구성 기존 그룹은 자산 레이블 및 값 점수가 우선순위 지정에 사용되는 레이블로 마이그레이션합니다.</li><li>• 다시 알림: 유틸 설정은 마이그레이션되지 않습니다. 인시던트 튜닝은 2026년 10월 14일에 제공될 예정입니다.</li></ul> |

### 워치리스트는 언제 이동합니까?

| 상태    | 2026년 10월 14일 예정                                                                                                 |
|-------|------------------------------------------------------------------------------------------------------------------|
| 세부사항  | <p>감시 목록 구성은 2026년 10월 14일 XDR에서 사용할 수 있도록 예약되어 있습니다. 기존 감시 목록은 마이그레이션되지만 논리를 보존하는 동안 용어와 규칙 표현이 변경될 수 있습니다.</p> |
| 고객 조치 | <p>전환 중에 감시 목록 종속 규칙, 억제 및 워크플로를 검증합니다.</p>                                                                      |

### SCA에서와 마찬가지로 경고 우선 순위를 설정할 수 있습니까?

|      |                                                           |
|------|-----------------------------------------------------------|
| 상태   | 아니요                                                       |
| 세부사항 | 경고 우선 순위는 Cisco 위협 연구를 사용하여 설정되며 고객이 관리하는 오탐 억제 제어가 아닙니다. |

### 센서, 클라우드 통합, 운영 상태

FTD, ISE, AWS, Azure 또는 GCP 통합은 그대로 유지됩니까?

|       |                                                                                                                                     |
|-------|-------------------------------------------------------------------------------------------------------------------------------------|
| 상태    | 비즈니스 크리티컬 경로 검증                                                                                                                     |
| 세부사항  | 모든 통합이 동일한 UI, 워크플로 또는 컨피그레이션 방법을 유지한다고 가정하지 마십시오. GCP 구성이 이미 XDR에 있습니다. AWS와 Azure가 다음으로 전환합니다. 온프레미스 센서 관련 마이그레이션 항목은 10월에 이동합니다. |
| 고객 조치 | 제품별 지침에 따라 FTD, ISE 격리, 보강, SAL 연결 워크플로 및 기타 비즈니스 크리티컬 통합을 검증합니다.                                                                   |

센서 상태, 라이브니스, 플로우 딜리버리, 볼륨을 동일한 방식으로 모니터링할 수 있습니까?

|       |                                                                                     |
|-------|-------------------------------------------------------------------------------------|
| 상태    | 준비도 검토                                                                              |
| 세부사항  | Cisco는 전환 과정에서 센서 및 수집 작업을 유지 관리하지만, 모든 SCA 모니터링 페이지나 워크플로가 일대일 마이그레이션을 약속하지는 않습니다. |
| 고객 조치 | 종속된 상태, 프로토콜, 플로우 볼륨 및 전달 검사를 인벤토리화하고 해당 XDR 운영 경로를 검증합니다.                          |

ONA 또는 CTB 이미지 배포, 대상 URL, 서비스 키 또는 공용 IP 주소가 변경됩니까?

|       |                                                                                               |
|-------|-----------------------------------------------------------------------------------------------|
| 상태    | 네트워크 종속성 검토                                                                                   |
| 세부사항  | Cisco는 이 단계에서 센서 재구축을 요구하지 않지만, 소스가 XDR로 전환됨에 따라 텔레메트리 대상이 변경될 수 있습니다.                        |
| 고객 조치 | 관련 소스 컷오버 전에 방화벽 규칙, 프록시 허용 목록, 대상 URL 및 서비스 키 종속성을 검토합니다. 게시된 마이그레이션 지침 없이 예방 센서를 변경하지 마십시오. |

### 기록 데이터, 보고 및 관리

SCA 사용자 환경이 꺼지면 기록 SCA 데이터는 어떻게 됩니까?

|      |                                                                                                                                                                                                            |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 상태   | 2026년 10월 24일 이전 수출                                                                                                                                                                                        |
| 세부사항 | SCA 인터페이스를 통한 기록 데이터 액세스는 사용자 환경이 제거되면 종료됩니다. 원시 텔레메트리는 탐지 마이그레이션 경로를 통해 미리 XDR에 수집되지만, SCA는 기록 검색을 위한 장기적인 위치는 아닙니다. <ul style="list-style-type: none"> <li>알림 및 관찰은 SCA 콘솔에서 CSV로 내보낼 수 있습니다.</li> </ul> |

|  |                                                                                                                                                         |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <ul style="list-style-type: none"> <li>필요한 경우 네트워크 트래픽 및 클라우드 로그를 포함한 원시 로그를 CSV로 내보낼 수 있습니다.</li> <li>내보내기 전에 감사, 포렌식 및 증거 보존 요구 사항을 정의합니다.</li> </ul> |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------|

### 모든 SCA 보고 기능이 XDR로 이동됩니까?

|       |                                                                                                |
|-------|------------------------------------------------------------------------------------------------|
| 상태    | 일부 폐기되거나 교체된 제품                                                                                |
| 세부사항  | 일부 보고 기능, 사용량이 적은 페이지 및 레거시 기능은 XDR 네이티브 탐지, 조사, 활동 및 Asset Insights 경험으로 폐기되거나 교체될 것으로 예상됩니다. |
| 고객 조치 | 운영 필수 보고서를 지금 인벤토리화하고 XDR 환경, 내보내기 또는 교체 워크플로를 식별합니다.                                          |

### 마이그레이션의 완전성을 어떻게 입증해야 합니까?

|       |                                                                                                                                     |
|-------|-------------------------------------------------------------------------------------------------------------------------------------|
| 상태    | 증명 객체 정의                                                                                                                            |
| 고객 조치 | 필수 기록 및 증거를 정의하고, 2026년 10월 24일 이전에 필요한 SCA 기록을 내보내고, 각 필수 소스에 대해 XDR 가시성을 검증합니다. 이 전환은 고객이 관리하는 대량 시스템을 별도의 시스템으로 다시 가져오는 것이 아닙니다. |

### SCA 측에 저장된 관리자 정보는 어떻게 됩니까?

|       |                                                                                |
|-------|--------------------------------------------------------------------------------|
| 상태    | 서비스 해제 전 문서                                                                    |
| 세부사항  | 고객이 볼 수 있는 구성, 관리 정보 또는 SCA에 저장된 기록이 2026년 10월 24일 이후에도 계속 사용 가능하다고 가정하지 마십시오. |
| 고객 조치 | 관리, 감사 또는 기록 참조에 필요한 내용을 내보내거나 문서화하고 XDR을 대상 운영 인터페이스로 사용합니다.                  |

## API 및 맞춤형 통합

### Get Observations API, SCA Devices API 또는 기타 SCA 관련 API를 대체하는 것은 무엇입니까?

|       |                                                                                                                                     |
|-------|-------------------------------------------------------------------------------------------------------------------------------------|
| 상태    | 인벤토리 종속성                                                                                                                            |
| 세부사항  | Cisco는 모든 SCA API에 대한 최종 일대일 API 대체 매트릭스를 게시하지 않았습니다. 활동, 탐지, 사고, 워크플로, Asset Insights/Device Insights 및 XDR Investigate에 대해 계획합니다. |
| 고객 조치 | 현재 직접 종속성을 인벤토리화하고 레거시 엔드포인트 이름이 2026년 10월 24일 이후에도 계속 사용 가능한 것으로 가정하지 않습니다.                                                        |

### 기존의 인시던트 생성 방법 및 맞춤형 자동화는 어떻게 됩니까?

|      |                                                  |
|------|--------------------------------------------------|
| 상태   | 전환으로 처리                                          |
| 세부사항 | FAQ에서 모든 레거시 인시던트 생성 방법 또는 API에 대해 약정된 공개 감가상각 날 |

|       |                                                                                                                                        |
|-------|----------------------------------------------------------------------------------------------------------------------------------------|
|       | 짜를 설정하는 것은 아닙니다. 대상 방향은 XDR 사용자 지정 보안 이벤트 및 탐지, XDR 모델에서 인시던트 생성, 결과 관리를 위한 인시던트 조정입니다.                                                |
| 고객 조치 | SCA 관찰, 경고 이름, 디바이스, 웹후크, 내보내기 또는 보고서를 사용하는 모든 자동화를 XDR 워크플로, 탐지, 인시던트, 활동 또는 Asset Insights 활용 사례에 매핑합니다. 관련 소스 컷오버 전에 엔드 투 엔드 동작 테스트 |

## 완료된 전환 항목

### NVM 탐지 마이그레이션

|    |                                                                                                         |
|----|---------------------------------------------------------------------------------------------------------|
| 상태 | 🔹🔹 완료                                                                                                   |
| 해결 | NVM 탐지 및 관련 탐지 설정은 2026년 5월에 XDR로 이동했습니다. 레거시 NVM 알림 및 내보내기에 의존하는 고객은 XDR 워크플로를 사용하고 워크플로 패턴을 검증해야 합니다. |

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.