Transición de Secure Cloud Analytics a Cisco XDR

Contenido

El cambio clave

La experiencia de usuario de Secure Cloud Analytics ya no estará disponible el 24 de octubre de 2026. Cisco XDR se convierte en la interfaz operativa para las detecciones, investigaciones, el contexto de recursos, las notificaciones, las exportaciones y los flujos de trabajo relacionados derivados de SCA.

⚠ Precaución: Está previsto que el programa de transición de clientes de SCA a XDR se cierre el 30 de septiembre, mientras que el 24 de octubre de 2026 sigue siendo la fecha prevista para la desaprobación de la interfaz de usuario de SCA. Active Cisco XDR ahora para que su equipo pueda completar las acciones de preparación que se describen a continuación.

Acciones inmediatas y fechas críticas

¿Qué está pasando y qué debo hacer ahora?

Estado	Acción requerida
Detalles	Cisco está retirando la experiencia de usuario de SCA y trasladando las funciones derivadas de SCA a Cisco XDR. La telemetría y los análisis forman parte de flujos de trabajo XDR más amplios para actividades, detecciones, incidentes, investigaciones, contexto de recursos, respuestas y automatización.
Acción del cliente	Active XDR, conecte al arrendatario de SCA, valide el acceso, utilice detecciones e incidentes XDR para las operaciones diarias, utilice actividades para traslados de telemetría de origen, pruebe flujos de trabajo XDR y exporte información histórica antes del 24 de octubre de 2026.

¿Qué fechas debo planificar?

Fecha	Hito	Qué significa esto
15 de septiembre de 2026	Configuración de AWS y Azure para clientes seleccionados	Los clientes afectados de EE. UU. y EMEA optan por el método de configuración XDR recomendado.
30 de septiembre de 2026	Se cierra el programa de transición de cliente de SCA a XDR dedicado	Complete las acciones de autorización, aprovisionamiento y preparación antes de que se cierre el programa.
7 de octubre de 2026	Las detecciones de AWS CloudTrail, Azure Activity Log y GCP Audit Log se cortan	Utilice estas fuentes en XDR
14 de octubre de 2026	Detecciones de eventos personalizados cortadas; Configuración de ajustes de incidentes, listas de observación y grupos de entidades disponible en XDR.	Traslade los flujos de trabajo y configuraciones relacionados a XDR.
21 de octubre de 2026	Detección de NetFlow interrumpida	Operar detecciones de NetFlow en XDR
24 de octubre de 2026	La experiencia del usuario de SCA ya no está disponible	Complete el traslado a XDR y exporte los datos históricos antes de esta fecha.

¿Qué ocurre si no realizo ninguna acción o no he suministrado XDR?

Estado	No recomendado
Detalles	Si no activa y conecta Cisco XDR antes de que se elimine la experiencia de usuario de SCA, perderá el acceso a SCA y no dispondrá de la experiencia XDR de sustitución para sus flujos de trabajo, detecciones, investigaciones, integraciones o datos históricos derivados de SCA. La espera también comprime la activación, la configuración del usuario, la validación del flujo de trabajo y el cambio operativo en la parte final de la transición.

Acción del cliente	Active y conecte XDR ahora para que su equipo pueda completar la configuración del usuario, la validación del flujo de trabajo y la preparación de la exportación antes del 30 de septiembre de 2026. La interfaz de SCA seguirá en desuso el 24 de octubre de 2026; sin un arrendatario XDR conectado, no hay ninguna experiencia XDR de sustitución disponible cuando finaliza el acceso a SCA.

Elementos que se retiran, cambian o no están disponibles

¿Qué conceptos de SCA no continúan explícitamente en la misma forma?

Estado	Cambio o retirada
Detalles	• Experiencia de usuario de SCA: eliminado el 24 de octubre de 2026. • Comportamiento de webhook de SCA heredado: sustituidos por flujos de trabajo XDR. • SCA Experiencia de observación: no es una función de XDR uno a uno. • Sensibilidad de subred: sustituidos por conceptos de priorización del valor de los activos. • Grupos de entidades: sustituidos por etiquetas de activos, grupos de activos y puntuación de valor. • Configuración de detección pospuesta: no migrado; utilice Ajuste de incidentes cuando esté disponible. • Comportamiento de prioridad de alerta controlado por el cliente: no se conserva. • Algunos informes, páginas de menor uso y funciones: retirados o sustituidos por experiencias nativas de XDR.

¿Qué elementos de informes o de integración se espera que queden obsoletos o que se trasladen?

Estado	Cambio esperado
Detalles	Algunos ejemplos son la lista de seguimiento del estado de la nube, la supervisión de Kubernetes, las experiencias de visualización/panel/búsqueda de sesiones/búsqueda por IP de AWS, las integraciones de contexto de Meraki y Umbrella, los informes mensuales basados en correo electrónico y los resúmenes de alertas diarios. Esta lista no promete un reemplazo uno por uno para cada página heredada.

¿Qué es lo que no se me pide en esta migración?

Estado	Ninguna acción de este tipo
Detalles	Cisco no solicita a los clientes que vuelvan a implementar los sensores de red existentes, reconfiguren la ingestión del registro en la nube únicamente para la migración de UX, vuelvan a crear manualmente los objetos de configuración de detección estándar compatibles o conserven SCA como una consola paralela a

	largo plazo.

Lista de comprobación de preparación del cliente

1. Active Cisco XDR y conecte el arrendatario de SCA existente antes del 30 de septiembre de 2026, para que su equipo pueda completar las acciones de preparación antes de que se cierre el programa de transición.
2. Cree usuarios, valide el inicio de sesión y confirme el acceso adecuado en XDR.
3. Revise las detecciones, incidentes, actividades, investigaciones y perspectivas sobre recursos/perspectivas sobre dispositivos.
4. Asigne cada webhook de SCA, exportación, notificación, transferencia de SIEM/SOAR y automatización personalizada a flujos de trabajo XDR u otra superficie operativa XDR.
5. Valide la telemetría de origen necesaria en Actividades a medida que cada origen esté disponible.
6. Valide las detecciones y los cuadernos de respuestas necesarios antes de cada transición de origen.
7. Revise la sensibilidad de subred, los grupos de entidades, la demora, la prioridad de alertas, las listas de comprobaciones, las reglas del analizador, las redes de confianza y la priorización del valor de los activos.
8. Inventariar informes heredados, páginas solo de SCA y dependencias de API; identificar alternativas o requisitos de exportación.
9. Exportar alertas, observaciones, registros sin procesar, registros de configuración e informes necesarios antes del 24 de octubre de 2026.

Encontrando el camino en la nueva experiencia XDR

¿Los clientes de SCA tienen derecho a Cisco XDR?

Estado	Disponible como parte de la transición
Detalles	Los clientes existentes de SCA tienen derecho a Cisco XDR como parte de la transición. El resultado previsto es un valor de SCA continuo mientras los flujos de trabajo principales se trasladan a XDR.
Acción del cliente	Active Cisco XDR, conecte el arrendatario SCA existente y utilice el proceso de activación de Cisco XDR si necesita ayuda.

¿Dónde aterrizan mis funciones de SCA en Cisco XDR?

función SCA	destino XDR
Alertas y flujos de trabajo de alertas	Detecciones e incidentes XDR
Observaciones e investigación orientada a los acontecimientos	Actividades XDR e investigación XDR
Visor de eventos	Investigación y actividades de XDR
Contexto del dispositivo	Asset Insights/Device Insights

Webhooks, avisos, exportaciones y entrega descendente	flujos de trabajo XDR
Configuración de detección	Experiencias de configuración XDR a medida que cada configuración alcanza su hito

¿Seguirá SCA disponible como consola paralela de uso diario?

Estado	No
Detalles	La eliminación de la experiencia del usuario de SCA está programada para el 24 de octubre de 2026. Utilice el período de solapamiento para practicar el modelo operativo XDR, validar flujos de trabajo y actualizar runbooks.

Detecciones, incidentes y casos prácticos de observación

¿Las detecciones simplemente se mueven una a una?

Estado	Cambio de modelo
Detalles	No. Cisco está desarrollando el contenido de detección y el modelo operativo en lugar de copiar cada alerta SCA antigua como un objeto XDR sin modificar. Los nombres, la lógica, la evidencia, la correlación y los resultados pueden cambiar.
Acción del cliente	Evalúe el resultado de la detección de XDR, las pruebas y la correlación de incidentes en relación con el escenario de seguridad que necesita para funcionar. no utilice la coincidencia de nombres como aceptación.

¿Debo utilizar incidentes o detecciones XDR para el flujo de trabajo de alertas?

Estado	Elegir por resultado
Detalles	Utilice los incidentes para la respuesta humana, las notificaciones de analistas, la clasificación, la derivación, la gestión de casos y la respuesta coordinada. Utilice las detecciones para obtener conclusiones individuales, exportaciones de nivel de detección y automatización máquina a máquina. Las actividades son la superficie de telemetría.
Acción del cliente	Actualizar runbooks para que las notificaciones humanas y los procesos de respuesta se activen desde Incidentes cuando sea apropiado; utilice Detecciones para obtener análisis detallados, exportaciones y automatización a nivel de búsqueda.

¿Continuarán los casos prácticos basados en la observación?

Estado	No uno a uno
Detalles	No asuma que el nombre de la observación heredada, el objeto de la interfaz de usuario o la condición del desencadenador permanecerán. El objetivo es una cobertura equivalente o mejorada a través de actividades, detecciones, incidentes y una correlación más amplia.

Acción del cliente	Identifique y actualice las dependencias en runbooks, paneles y automatización antes del 24 de octubre de 2026.

¿Qué sucede si dependo principalmente de NetFlow y no puedo implementar EDR?

Estado	Aún en ámbito
Detalles	Los sensores de red existentes y la ingestión permanecen funcionales y no se requiere la implementación de EDR para continuar utilizando las detecciones de red migradas.
Acción del cliente	Utilice detecciones XDR, hallazgos, incidentes, ajuste de incidentes y contexto de recursos disponibles. Solicite orientación específica para la implementación si la visibilidad de los terminales está muy restringida.

Notificaciones, exportaciones, webhooks y automatización

¿Qué ocurre con los webhooks de SCA?

Estado	Migrar y probar
Detalles	Los flujos de trabajo XDR Automate son el punto de control a largo plazo para las notificaciones, las exportaciones y la automatización descendente. La ruta de exportación de destino está alineada con OCSF y puede proporcionar detalles de detección contextual más completos que el modelo anterior de alertas y observaciones de SCA.
Acción del cliente	Si un webhook envía información de detección a personas, SIEM, SOAR u otro sistema, vuelva a crear y pruebe ese comportamiento en los flujos de trabajo XDR.

¿Cuál es la diferencia entre flujos de trabajo de detección e incidentes?

Estado	Utilizar el desencadenador coincidente
Detalles	Utilice flujos de trabajo orientados a la detección para el movimiento de datos, las exportaciones y el consumo de máquinas. Utilice flujos de trabajo orientados a incidentes para actividades operativas y notificaciones humanas más amplias, como correo electrónico, Slack o Webex. Ambos pueden respaldar las exportaciones.

¿Qué cambia para las integraciones SIEM, SOAR o descendentes personalizadas?

Estado	Revisión obligatoria
Detalles	No asuma que un webhook, carga, nombre de alerta o exportación específicos de SCA continuarán sin cambios. La ruta de exportación de destino está alineada con OCSF y puede proporcionar detalles de detección más completos y contextuales.
Acción del cliente	Migre dependencias a flujos de trabajo XDR y al modelo de datos XDR y, a continuación, pruebe el comportamiento de la recepción descendente y del runbook.

¿Tengo que cambiar las notificaciones y exportaciones de NVM?

Estado	Transición a NVM finalizada
Detalles	Las detecciones de NVM se trasladaron a XDR en mayo de 2026. Los clientes que confiaban en el patrón de webhook de NVM heredado necesitaban trasladar las notificaciones y las exportaciones a los flujos de trabajo XDR antes de la transición del 15 de mayo de 2026.
Acción del cliente	Continuar utilizando y validando el patrón de flujo de trabajo XDR para NVM.

¿Qué debo probar antes de una transición de origen?

Estado	Comprobación de preparación necesaria
Acción del cliente	Para cada origen, pruebe el desencadenador de detección o incidente, la carga útil de notificación o exportación, la recepción descendente, las reglas de filtrado o enrutamiento y la respuesta de runbook actualizada. Realice la prueba antes de que el origen abandone la experiencia de SCA.

Fuentes de telemetría y traslados fuente por fuente

¿Cuándo estará disponible la telemetría en las actividades de XDR?

Fecha	Hito de telemetría	Acción del cliente
19 de agosto de 2026	Telemetría de datos ONA en Actividades	Comience a revisar la telemetría de ONA.
26 de agosto de 2026	Telemetría de datos de CTB en Actividades	Comience a revisar la telemetría de CTB.
16 de septiembre de 2026	Registros de flujo de AWS VPC, Azure Flow Logs y GCP VPC Flow Logs en actividades	Comience a revisar la telemetría de flujo de la nube.
23 de septiembre de 2026	Configuración de fuente AWS en XDR	Utilice la experiencia de configuración XDR donde corresponda.
30 de septiembre de 2026	AWS CloudTrail, Azure Activity Logs y GCP Audit Logs en actividades	Comience a revisar la telemetría del registro de auditoría.

¿Tengo que volver a implementar sensores de red o reconfigurar la ingestión de registros en la nube?

Estado	No, no solo para la migración de UX
Detalles	Los sensores de red existentes y la ingestión de registros en la nube siguen funcionando durante esta fase y no es necesario volver a implementarlos o

	configurarlos únicamente porque la experiencia del usuario y las detecciones se están trasladando a XDR.
Excepción importante	Las direcciones IP públicas o los terminales utilizados por los sensores y las integraciones pueden cambiar. Revisar las reglas de firewall, las listas de permisos de proxy y otros controles de red; Cisco proporcionará los detalles necesarios del terminal XDR antes de que sea necesario realizar un cambio de configuración.

¿Cuándo se cortan las detecciones de origen?

Estado	Programación específica del origen
Detalles	Al realizar la transición, la telemetría y las detecciones de esa fuente ya no están disponibles para su uso a través de la experiencia del usuario de SCA. • 7 de octubre de 2026: Detecciones de AWS CloudTrail, Azure Activity Log y GCP Audit Log. • 14 de octubre de 2026: Detecciones de eventos personalizados. • 21 de octubre de 2026: Detecciones de NetFlow.

Configuración, ajuste, listas de control y contexto de recursos

¿Se migrarán mis configuraciones de detección?

Estado	Migración por fases
Detalles	Se espera que los objetos de configuración estándar admitidos migren como parte de la transición más amplia del motor de detección. Los parámetros de detección de NVM se trasladaron a XDR en mayo de 2026; otros ajustes cambian a medida que su capacidad está disponible.
Acción del cliente	No vuelva a crear manualmente la configuración estándar únicamente para la migración a menos que Cisco publique una instrucción específica para la implementación.

¿Qué sustituye a la sensibilidad de subred, los grupos de entidades y la función Posponer?

Estado	Cambio de conceptos
Detalles	• Sensibilidad de subred: sustituida por la puntuación de prioridad de valor de dispositivo en Asset Insights/Device Insights; programado en XDR Device Insights para el 30 de septiembre de 2026. • Grupos de entidades: configuración programada en XDR Device Insights el 14 de octubre de 2026; los grupos existentes migran a las etiquetas, en las que las etiquetas de activos y la puntuación de valor se utilizan para la priorización. • Posponer: la configuración pospuesta no se migra; La optimización de

	incidentes está programada para estar disponible el 14 de octubre de 2026.

¿Cuándo se mueven las listas de observación?

Estado	Programado el 14 de octubre de 2026
Detalles	Está previsto que la configuración de la lista de observación esté disponible en XDR el 14 de octubre de 2026. Se migrarán las listas de observación existentes, pero la terminología y la presentación de reglas pueden cambiar mientras se conserva la lógica.
Acción del cliente	Valide las reglas, la supresión y los flujos de trabajo dependientes de la lista de comprobaciones durante la transición.

¿Puedo establecer la prioridad de alerta de la misma forma que lo hice en SCA?

Estado	No
Detalles	La prioridad de alerta se establece de forma rígida mediante la investigación de amenazas de Cisco y no es un control de supresión de falsos positivos gestionado por el cliente.

Sensores, integraciones en la nube y estado operativo

¿Se mantendrán sin cambios las integraciones de FTD, ISE, AWS, Azure o GCP?

Estado	Validar rutas vitales para la empresa
Detalles	No asuma que cada integración conserva la misma interfaz de usuario, flujo de trabajo o método de configuración. La configuración de GCP ya está en XDR; AWS y Azure se mueven a continuación; los elementos de migración relacionados con los sensores en las instalaciones se trasladarán en octubre.
Acción del cliente	Valide el FTD, la cuarentena de ISE, el enriquecimiento, los flujos de trabajo conectados a SAL y otras integraciones vitales para la empresa en función de la orientación específica del producto.

¿Puedo supervisar el estado del sensor, la actividad, el flujo y el volumen de la misma manera?

Estado	Revisión de preparación
Detalles	Cisco mantiene las operaciones de detección e ingestión durante la transición, pero no todas las páginas de supervisión o flujos de trabajo de SCA se comprometen a migrar una por una.
Acción del cliente	Realice un inventario de las comprobaciones de estado, protocolo, volumen de flujo y entrega de las que depende y valide su ruta de funcionamiento XDR.

¿Cambiarán la distribución de imágenes ONA o CTB, las URL de destino, las claves de servicio o las direcciones IP públicas?

Estado	Revisar dependencias de red
Detalles	Cisco no requiere la reimplementación de sensores en esta fase, pero los destinos de telemetría pueden cambiar a medida que las fuentes pasan a XDR.
Acción del cliente	Revise las reglas del firewall, las listas de permitidos de proxy, las URL de destino y las dependencias de clave de servicio antes de la transición de origen correspondiente. No realice cambios de sensor preventivos sin las instrucciones de migración publicadas.

Datos históricos, informes y administración

¿Qué ocurre con los datos de SCA históricos cuando se desactiva la experiencia del usuario de SCA?

Estado	Exportar antes del 24 de octubre de 2026
Detalles	El acceso a los datos históricos a través de la interfaz SCA finaliza cuando se elimina la experiencia del usuario. La telemetría en bruto se incorpora en XDR antes y a través de la ruta de migración de detección, pero SCA no es la ubicación a largo plazo para la recuperación histórica. • Las alertas y observaciones se pueden exportar como CSV desde la consola de SCA. • Los registros sin procesar, incluidos el tráfico de red y los registros en la nube, se pueden exportar como CSV si es necesario. • Defina los requisitos de auditoría, diagnóstico y pruebas de retención antes de exportar.

¿Se trasladarán todas las funciones de informes de SCA a XDR?

Estado	Algunos retirados o sustituidos
Detalles	Se espera que algunas funciones de generación de informes, páginas de menor uso y funciones heredadas se retiren o sustituyan por experiencias de detecciones nativas de XDR, investigación, actividades e información de activos.
Acción del cliente	Realice ahora un inventario de los informes que se requieren desde el punto de vista operativo e identifique la experiencia XDR, la exportación o el flujo de trabajo de sustitución.

¿Cómo puedo demostrar que la migración es completa?

Estado	Definir artefactos de prueba
Acción del	Defina los registros y las pruebas necesarias, exporte el historial de SCA necesario

cliente	antes del 24 de octubre de 2026 y valide la visibilidad de XDR para cada fuente requerida. La transición no consiste en una reimportación masiva gestionada por el cliente en un sistema independiente.

¿Qué ocurre con la información del administrador almacenada en el lado de SCA?

Estado	Documento antes de la clausura
Detalles	No asuma que la configuración visible para el cliente, la información administrativa o el historial almacenado en SCA permanecerán disponibles después del 24 de octubre de 2026.
Acción del cliente	Exporte o documente cualquier cosa necesaria para la administración, la auditoría o la referencia histórica, y utilice XDR como la interfaz operativa de destino.

API e integraciones personalizadas

¿Qué sustituye a las API Get Observations, SCA Devices o a otras API específicas de SCA?

Estado	Dependencias de inventario
Detalles	Cisco no ha publicado una matriz final de sustitución de API uno por uno para cada API de SCA. Planifique actividades, detecciones, incidentes, flujos de trabajo, Asset Insights/Device Insights y XDR Investigate.
Acción del cliente	Realice un inventario de las dependencias directas ahora y no asuma que los nombres de terminales heredados seguirán estando disponibles después del 24 de octubre de 2026.

¿Qué ocurre con los métodos de creación de incidentes antiguos y la automatización personalizada?

Estado	Tratar como transicional
Detalles	Las preguntas frecuentes no establecen una fecha de caducidad pública comprometida para cada método de creación de incidentes o API heredados. El objetivo son las detecciones y los eventos de seguridad personalizados de XDR, la generación de incidentes en el modelo XDR y el ajuste de incidentes para la gestión de resultados.
Acción del cliente	Asigne cada automatización que consuma observaciones de SCA, nombres de alertas, dispositivos, webhooks, exportaciones o informes a un caso práctico de XDR sobre flujo de trabajo, detección, incidente, actividad o Asset Insights. Pruebe el comportamiento de extremo a extremo antes de la transición de origen relevante.

Elementos de transición finalizados

Migración de detección de NVM

Estado	✅ Completado
Resolución	Las detecciones de NVM y los ajustes de detección relacionados se trasladaron a XDR en mayo de 2026. Los clientes que dependan de notificaciones y exportaciones de equipos NVM antiguos deberían utilizar flujos de trabajo XDR y validar el patrón de flujo de trabajo.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).