

Transizione da Secure Cloud Analytics a Cisco XDR

Sommario

[La modifica della chiave](#)

[Azioni immediate e date critiche](#)

[Informazioni su ritiro, modifica o non disponibile](#)

[Elenco di controllo per la preparazione dei clienti](#)

[Trovare la strada giusta nella nuova esperienza XDR](#)

[Rilevamenti, incidenti e casi di utilizzo dell'osservazione](#)

[Notifiche, esportazioni, webhook e automazione](#)

[Fonti di telemetria e cutover origine per origine](#)

[Impostazioni, ottimizzazione, liste di controllo e contesto delle risorse](#)

[Sensori, integrazioni cloud e integrità operativa](#)

[Dati cronologici, reporting e amministrazione](#)

[API e integrazioni personalizzate](#)

[Elementi di transizione completati](#)

La modifica della chiave

L'esperienza utente di Secure Cloud Analytics non sarà più disponibile il 24 ottobre 2026. Cisco XDR diventa l'interfaccia operativa per rilevamenti, indagini, contesto degli asset, notifiche, esportazioni e flussi di lavoro correlati derivati da SCA.



Attenzione: Il programma di transizione clienti dedicato SCA-to-XDR terminerà il 30 settembre, mentre il 24 ottobre 2026 rimane la data prevista per il deprecato programma dell'interfaccia utente SCA. Attivare Cisco XDR per consentire al team di completare le azioni di preparazione descritte di seguito.

Azioni immediate e date critiche

Cosa sta succedendo, e cosa dovrei fare ora?

Stato	Azione richiesta
-------	------------------

Dettagli	Cisco sta ritirando l'esperienza utente SCA e sta spostando le funzionalità derivate da SCA in Cisco XDR. La telemetria e l'analisi fanno parte di flussi di lavoro XDR più ampi per attività, rilevamenti, incidenti, indagini, contesto delle risorse, risposta e automazione.
Azione cliente	Attivare XDR, collegare il tenant SCA, convalidare l'accesso, utilizzare Rilevamenti e incidenti XDR per le operazioni quotidiane, utilizzare Attività per i clienti di telemetria sorgente, testare i flussi di lavoro XDR ed esportare le informazioni cronologiche prima del 24 ottobre 2026.

Quali date devo pianificare in giro?

Data	Cardine	Significato
15 settembre 2026	Configurazione di AWS e Azure per i clienti selezionati	I clienti statunitensi ed EMEA interessati passano al metodo di configurazione XDR consigliato.
30 settembre 2026	Chiusura del programma dedicato di transizione dei clienti SCA-to-XDR	Completare le azioni relative ai diritti, al provisioning e alla preparazione prima della chiusura del programma.
7 ottobre 2026	Rilevamenti AWS CloudTrail, Azure Activity Log e GCP Audit Log interrotti	Utilizzare queste sorgenti in XDR
14 ottobre 2026	Rilevamenti di eventi personalizzati interrotti; Configurazione di Incident Tuning, liste di controllo e gruppi di entità disponibile in XDR.	Spostare i workflow e le configurazioni correlati in XDR
21 ottobre 2026	Rilevamenti NetFlow interrotti	Eseguire i rilevamenti NetFlow in XDR
24 ottobre 2026	Esperienza utente SCA non più disponibile	Completare lo spostamento in XDR ed esportare i dati cronologici prima di questa data.

Cosa succede se non si esegue alcuna operazione o non si esegue il provisioning di XDR?

Stato	Non consigliato
Dettagli	Se non si attiva e non si collega Cisco XDR prima di rimuovere l'esperienza utente SCA, non sarà possibile accedere a SCA e non sarà disponibile l'esperienza XDR sostitutiva per i flussi di lavoro derivati da SCA, rilevamenti, indagini, integrazioni o dati cronologici. In attesa vengono inoltre comprese l'attivazione, la configurazione utente, la convalida del flusso di lavoro e la modifica operativa nella parte finale della transizione.
Azione cliente	Attivare e connettere ora XDR in modo che il team possa completare la configurazione dell'utente, la convalida del flusso di lavoro e la preparazione dell'esportazione prima del 30 settembre 2026. L'interfaccia SCA rimane destinata all'obsolescenza il 24 ottobre 2026; senza un tenant XDR connesso, non è disponibile alcuna esperienza XDR sostitutiva al termine dell'accesso SCA.

Informazioni su ritiro, modifica o non disponibile

Quali concetti SCA non continuano esplicitamente nella stessa forma?

Stato	Modifica o ritiro
Dettagli	• Esperienza utente SCA: rimosso il 24 ottobre 2026. • Comportamento webhook SCA legacy: sostituito da workflow XDR. • Esperienza di osservazione SCA: non una funzione XDR one-to-one. • Sensibilità subnet: sostituito da concetti di assegnazione di priorità valore asset. • Gruppi di entità: sostituito da etichette, gruppi di cespiti e scoring del valore. • Impostazioni rilevamento posticipato: non migrati; utilizzare Incident Tuning quando disponibile. • Comportamento di priorità degli avvisi controllato dal cliente: non mantenuti. • Alcune funzioni e pagine di reporting, di utilizzo ridotto: ritirato o sostituito da esperienze XDR native.

Quali elementi di reporting o integrazione devono essere deprecati o spostati?

Stato	Modifica prevista
Dettagli	Gli esempi includono watchlist sulla postura del cloud, monitoraggio di Kubernetes, visualizzazioni/dashboard/esperienze di ricerca di sessioni/IP di AWS, integrazioni di contesto di Meraki e Umbrella, report mensili basati su e-mail e riepiloghi giornalieri degli avvisi. Questo elenco non prevede la sostituzione uno per uno di ogni pagina legacy.

Cosa non mi viene chiesto in questa migrazione?

Stato	Nessuna azione di questo tipo
Dettagli	Cisco non chiede ai clienti di reinstallare i sensori di rete esistenti, riconfigurare l'acquisizione del log del cloud esclusivamente per la migrazione UX, ricreare manualmente gli oggetti di configurazione supportati per il rilevamento standard o mantenere SCA come console parallela a lungo termine.

Elenco di controllo per la preparazione dei clienti

1. Attivare Cisco XDR e collegare il tenant SCA esistente prima del 30 settembre 2026, in modo che il team possa completare le azioni di preparazione prima della chiusura del programma di transizione.
2. Creare utenti, convalidare l'accesso e confermare l'accesso appropriato in XDR.
3. Analisi di rilevamenti, incidenti, attività, analisi e informazioni dettagliate sugli

asset/informazioni sui dispositivi.

4. Mappatura di ogni webhook SCA, esportazione, notifica, handoff SIEM/SOAR e automazione personalizzata su workflow XDR o su un'altra superficie operativa XDR.
5. Convalidare la telemetria di origine necessaria in Attività quando ciascuna origine diventa disponibile.
6. Convalidare i rilevamenti richiesti e i playbook di risposta prima di ogni passaggio alla sorgente.
7. Esaminare la sensibilità della subnet, i gruppi di entità, l'effetto Posponi, la priorità degli avvisi, le liste di controllo, le regole dello scanner, le reti attendibili e la definizione di priorità per il valore degli asset.
8. Inventario dei report legacy, delle pagine solo SCA e delle dipendenze API; identificare alternative o requisiti per l'esportazione.
9. Esportare avvisi, osservazioni, registri non elaborati, record di configurazione e report richiesti prima del 24 ottobre 2026.

Trovare la strada giusta nella nuova esperienza XDR

I clienti SCA hanno diritto a Cisco XDR?

Stato	Disponibile come parte della transizione
Dettagli	I clienti SCA esistenti hanno diritto a Cisco XDR come parte della transizione. Il risultato previsto è un valore SCA continuo mentre i flussi di lavoro principali passano a XDR.
Azione cliente	Attivare Cisco XDR, collegare il tenant SCA esistente e utilizzare il processo di attivazione Cisco XDR se è necessaria assistenza.

Dove si trovano le funzioni SCA in Cisco XDR?

Funzione SCA	destinazione XDR
Avvisi e flussi di lavoro avvisi	Rilevamenti e incidenti XDR
Osservazioni e indagini orientate agli eventi	XDR Activities e XDR Investigate
Visualizzatore eventi	Indagine e attività XDR
Contesto dispositivo	Asset Insights/Device Insights
Webhook, avvisi, esportazioni e consegne a valle	Flussi di lavoro XDR
Configurazione rilevamento	Configurazione di XDR nel momento in cui ogni impostazione raggiunge la fase cardine

SCA rimarrà disponibile come console per l'uso quotidiano parallelo?

Stato	No
Dettagli	La rimozione dell'esperienza utente SCA è prevista per il 24 ottobre 2026. Utilizzare

	il periodo di sovrapposizione per provare il modello operativo XDR, convalidare i flussi di lavoro e aggiornare i runbook.
--	--

Rilevamenti, incidenti e casi di utilizzo dell'osservazione

I rilevamenti si spostano semplicemente uno per uno?

Stato	Modifica del modello
Dettagli	No. Cisco sta modificando il contenuto di rilevamento e il modello operativo, anziché copiare ogni avviso SCA legacy come oggetto XDR non modificato. I nomi, la logica, le prove, la correlazione e i risultati possono cambiare.
Azione cliente	Valutare l'esito del rilevamento XDR, le prove e la correlazione degli incidenti rispetto allo scenario di sicurezza che è necessario utilizzare; non utilizzare la sola corrispondenza dei nomi come accettazione.

È consigliabile utilizzare gli incidenti o i rilevamenti XDR per il flusso di lavoro degli avvisi?

Stato	Scegli per risultato
Dettagli	Utilizzare Incidenti per la risposta umana, le notifiche degli analisti, la valutazione, l'escalation, la gestione dei casi e la risposta coordinata. Utilizzare i rilevamenti per i singoli risultati, le esportazioni a livello di rilevamento e l'automazione da macchina a macchina. Le attività sono la superficie di telemetria.
Azione cliente	Aggiornare i runbook in modo che le notifiche umane e i processi di risposta siano attivati dagli incidenti, se del caso; utilizzare Rilevamenti per l'analisi dettagliata, le esportazioni e l'automazione del livello di individuazione.

I casi di utilizzo basati sull'osservazione continueranno?

Stato	Non uno a uno
Dettagli	Non presumere che il nome dell'osservazione, l'oggetto UI o la condizione di trigger legacy rimarranno. L'obiettivo è una copertura equivalente o migliorata tramite attività, rilevamenti, incidenti e una correlazione più ampia.
Azione cliente	Identificare e aggiornare le dipendenze in runbook, dashboard e automazione prima del 24 ottobre 2026.

Cosa succede se si utilizza principalmente NetFlow e non si riesce a distribuire EDR?

Stato	Ancora nell'ambito
Dettagli	I sensori di rete e l'acquisizione esistenti rimangono funzionali e l'implementazione EDR non è necessaria per continuare a utilizzare i rilevamenti di rete migrati.
Azione cliente	Utilizzare Rilevamenti XDR, Risultati, Incidenti, Regolazione degli incidenti e contesto delle risorse disponibili. Richiedere indicazioni specifiche per la

	distribuzione se la visibilità dell'endpoint è soggetta a vincoli elevati.
--	--

Notifiche, esportazioni, webhook e automazione

Cosa succede ai webhook SCA?

Stato	Migrazione e test
Dettagli	I workflow automatizzati XDR rappresentano il punto di controllo a lungo termine per le notifiche, le esportazioni e l'automazione a valle. Il percorso di esportazione di destinazione è allineato a OCSF e può fornire dettagli di rilevamento contestuale più completi rispetto al modello legacy di avvisi e osservazioni SCA.
Azione cliente	Se un webhook invia informazioni di rilevamento a utenti, SIEM, SOAR o a un altro sistema, ricreare e testare tale comportamento nei flussi di lavoro XDR.

Qual è la differenza tra il rilevamento e il flusso di lavoro relativo agli incidenti?

Stato	Utilizzare il trigger corrispondente
Dettagli	Utilizzo di workflow orientati al rilevamento per lo spostamento dei dati, le esportazioni e il consumo delle macchine. Utilizzo di workflow orientati agli incidenti per attività operative più ampie e notifiche umane, ad esempio e-mail, margine di flessibilità o Webex. Entrambe possono sostenere le esportazioni.

Quali sono le modifiche per le integrazioni SIEM, SOAR o downstream personalizzate?

Stato	Revisione richiesta
Dettagli	Non presumere che un webhook, un payload, un nome di avviso o un'esportazione specifici di SCA continueranno senza modifiche. Il percorso di esportazione di destinazione è allineato a OCSF ed è in grado di fornire dettagli di rilevamento più completi e contestuali.
Azione cliente	Eseguire la migrazione delle dipendenze nei flussi di lavoro XDR e nel modello di dati XDR, quindi verificare il comportamento dell'incasso a valle e del runbook.

È necessario modificare le notifiche e le esportazioni NVM?

Stato	Cambio di immagini NVM completato
Dettagli	I rilevamenti NVM sono stati trasferiti a XDR nel maggio 2026. I clienti che si affidano al modello di webhook NVM legacy hanno avuto bisogno di spostare le notifiche e le esportazioni verso i flussi di lavoro XDR entro il 15 maggio 2026.
Azione cliente	Continuare a utilizzare e convalidare il modello di flusso di lavoro XDR per NVM.

Cosa è necessario verificare prima di un'interruzione dell'origine?

Stato	Verifica della preparazione richiesta
Azione cliente	Per ogni origine, eseguire il test delle regole di attivazione del rilevamento o degli incidenti, del payload di notifica o esportazione, della ricezione a valle, del filtro o del routing e della risposta aggiornata del runbook. Eseguire la prova prima che la sorgente lasci l'esperienza SCA.

Fonti di telemetria e cutover origine per origine

Quando sarà disponibile la telemetria nelle attività XDR?

Data	Cardine di telemetria	Azione cliente
19 agosto 2026	Telemetria dei dati ONA nelle attività	Inizia a rivedere la telemetria dell'ONA.
26 agosto 2026	Telemetria dei dati CTB nelle attività	Inizia a rivedere la telemetria CTB.
16 settembre 2026	Log di flusso VPC AWS, log di flusso di Azure e log di flusso VPC GCP in attività	Inizia l'analisi della telemetria del flusso del cloud.
23 settembre 2026	Configurazione origine AWS in XDR	Utilizzare l'esperienza di configurazione XDR, se applicabile.
30 settembre 2026	AWS CloudTrail, log attività di Azure e log di controllo GCP nelle attività	Iniziare l'analisi della telemetria del log di controllo.

È necessario reinstallare i sensori di rete o riconfigurare l'acquisizione del log del cloud?

Stato	No, non solo per la migrazione UX
Dettagli	I sensori di rete esistenti e l'acquisizione di registri cloud rimangono funzionali in questa fase e non devono essere reinstallati o riconfigurati solo perché l'esperienza utente e i rilevamenti sono in fase di passaggio a XDR.
Eccezione importante	Gli indirizzi IP pubblici o gli endpoint utilizzati dai sensori e dalle integrazioni possono cambiare. Verificare le regole firewall, gli elenchi di autorizzazioni proxy e altri controlli di rete. Cisco fornirà i dettagli dell'endpoint XDR richiesti prima che sia necessaria una modifica alla configurazione.

Quando i rilevamenti delle fonti vengono interrotti?

Stato	Pianificazione specifica dell'origine
Dettagli	Al cutover, la telemetria e i rilevamenti per quella fonte non sono più disponibili per l'uso tramite l'esperienza utente di SCA. 7 ottobre 2026: Rilevamenti AWS CloudTrail, Azure Activity Log e GCP Audit Log. 14 ottobre 2026: Rilevamenti eventi personalizzati.

	21 ottobre 2026: Rilevamenti NetFlow.
--	---

Impostazioni, ottimizzazione, liste di controllo e contesto delle risorse

Verrà eseguita la migrazione delle configurazioni di rilevamento?

Stato	Migrazione per fasi
Dettagli	La migrazione degli oggetti di configurazione standard supportati è prevista nell'ambito della più ampia transizione del motore di rilevamento. Le impostazioni di rilevamento NVM sono state spostate su XDR a maggio 2026; le altre impostazioni vengono modificate non appena le relative capacità diventano disponibili.
Azione cliente	Non ricreare manualmente le impostazioni standard solo per la migrazione a meno che Cisco non pubblichi un'istruzione specifica per la distribuzione.

Cosa sostituisce la sensibilità subnet, i gruppi di entità e l'opzione Posponi?

Stato	Cambiamenti concettuali
Dettagli	- Sensibilità subnet: sostituito da punteggio assegnazione priorità valore dispositivo in Asset Insights/Device Insights; in XDR Device Insights entro il 30 settembre 2026. - Gruppi di entità: configurazione pianificata in XDR Device Insights il 14 ottobre 2026; i gruppi esistenti passano a Etichette, con etichette di asset e punteggi di valore utilizzati per la definizione delle priorità. - Posponi: le impostazioni posticipate non vengono migrate; Incident Tuning sarà disponibile dal 14 ottobre 2026.

Quando si spostano le liste di controllo?

Stato	In programma il 14 ottobre 2026
Dettagli	La configurazione della lista di controllo sarà disponibile in XDR il 14 ottobre 2026. Verrà eseguita la migrazione degli elenchi di controllo esistenti, ma la terminologia e la presentazione delle regole potrebbero cambiare durante il mantenimento della logica.
Azione cliente	Convalidare le regole dipendenti dalla lista di controllo, l'eliminazione e i workflow durante la transizione.

È ancora possibile impostare la priorità dell'avviso come in SCA?

Stato	No
Dettagli	La priorità degli avvisi è impostata a livello hardware utilizzando la ricerca sulle

	minacce Cisco e non è un controllo della soppressione dei falsi positivi gestito dal cliente.
--	---

Sensori, integrazioni cloud e integrità operativa

Le integrazioni FTD, ISE, AWS, Azure o GCP rimarranno invariate?

Stato	Convalida dei percorsi business-critical
Dettagli	Non presupporre che ogni integrazione mantenga la stessa interfaccia utente, lo stesso workflow o lo stesso metodo di configurazione. La configurazione GCP è già in XDR; AWS e Azure stanno per passare alla fase successiva; gli elementi di migrazione relativi ai sensori interni verranno spostati a ottobre.
Azione cliente	Convalida di FTD, quarantena ISE, arricchimento, flussi di lavoro collegati a SAL e altre integrazioni business-critical sulla base di linee guida specifiche del prodotto.

È possibile monitorare lo stato dei sensori, la vivacità, la distribuzione del flusso e il volume allo stesso modo?

Stato	Valutazione della fattibilità
Dettagli	Cisco mantiene le operazioni di acquisizione e gestione dei sensori durante la transizione, ma non tutte le pagine di monitoraggio SCA o i flussi di lavoro sono impegnati nella migrazione uno a uno.
Azione cliente	Inventario dello stato, del protocollo, del volume di flusso e dei controlli di consegna da cui dipende e convalida il percorso operativo XDR.

La distribuzione delle immagini ONA o CTB, gli URL di destinazione, le chiavi di servizio o gli indirizzi IP pubblici verranno modificati?

Stato	Verifica dipendenze di rete
Dettagli	In questa fase Cisco non richiede la reimplementazione del sensore, ma le destinazioni di telemetria potrebbero cambiare con la transizione delle origini a XDR.
Azione cliente	Esaminare le regole del firewall, gli elenchi di autorizzazioni proxy, gli URL di destinazione e le dipendenze della chiave del servizio prima del passaggio all'origine pertinente. Non effettuare modifiche preventive ai sensori senza aver pubblicato le istruzioni di migrazione.

Dati cronologici, reporting e amministrazione

Cosa succede ai dati cronologici di SCA quando l'esperienza utente di SCA si spegne?

Stato	Esportazioni prima del 24 ottobre 2026
-------	--

	L'accesso ai dati cronologici tramite l'interfaccia SCA termina quando l'esperienza utente viene rimossa. La telemetria non elaborata viene inserita in XDR prima e durante il percorso di migrazione del rilevamento, ma SCA non è la posizione a lungo termine per il recupero storico.
Dettagli	• Avvisi e osservazioni possono essere esportati come CSV dalla console SCA. • Se necessario, è possibile esportare come file CSV i registri non elaborati, inclusi il traffico di rete e i registri cloud. • Definizione dei requisiti relativi a verifiche, analisi legali e prove di conservazione prima dell'esportazione.

Tutte le funzioni di reporting SCA passeranno a XDR?

Stato	Alcuni ritirati o sostituiti
Dettagli	Alcune funzioni di reporting, le pagine a basso utilizzo e le funzioni legacy dovrebbero essere ritirate o sostituite da rilevamenti nativi di XDR, analisi, attività e analisi degli asset.
Azione cliente	Effettuare subito l'inventario dei report necessari per le operazioni e identificare l'esperienza XDR, l'esportazione o il flusso di lavoro di sostituzione.

Come è possibile dimostrare la completezza della migrazione?

Stato	Definire gli elementi di prova
Azione cliente	Definire i record e le prove richieste, esportare la cronologia SCA necessaria prima del 24 ottobre 2026 e convalidare la visibilità XDR per ogni origine richiesta. La transizione non è una reimportazione in blocco gestita dal cliente in un sistema separato.

Cosa succede alle informazioni dell'amministratore memorizzate sul lato SCA?

Stato	Documenta prima della rimozione delle autorizzazioni
Dettagli	Non presupporre che la configurazione visibile al cliente, le informazioni amministrative o la cronologia archiviate in SCA saranno disponibili dopo il 24 ottobre 2026.
Azione cliente	Esportare o documentare qualsiasi elemento necessario per l'amministrazione, il controllo o il riferimento cronologico e utilizzare XDR come interfaccia operativa di destinazione.

API e integrazioni personalizzate

Cosa sostituisce l'API Get Observations, l'API SCA Devices o altre API specifiche di SCA?

Stato	Dipendenze inventario
-------	-----------------------

Dettagli	Cisco non ha pubblicato una matrice di sostituzione delle API one-for-one finale per ciascuna API SCA. Pianificazione di attività, rilevamenti, incidenti, workflow, informazioni sugli asset/informazioni sui dispositivi e XDR Investigate.
Azione cliente	Le dipendenze dirette dell'inventario ora e non presuppongono che i nomi degli endpoint legacy rimangano disponibili dopo il 24 ottobre 2026.

Cosa succede ai metodi legacy per la creazione di incidenti e all'automazione personalizzata?

Stato	Considera come transitorio
Dettagli	Le domande frequenti (FAQ) non stabiliscono una data di deprecazione pubblica impegnata per ogni metodo o API legacy per la creazione di incidenti. La direzione di destinazione è rappresentata dai rilevamenti e dagli eventi di protezione personalizzati XDR, dalla generazione di incidenti nel modello XDR e dall'ottimizzazione degli incidenti per la gestione dei risultati.
Azione cliente	Mappare ogni automazione che utilizza osservazioni SCA, nomi di avviso, dispositivi, webhook, esportazioni o report in un caso di utilizzo di flusso di lavoro, rilevamento, incidente, attività o Asset Insights XDR. Verificare il comportamento completo prima del passaggio alla sorgente interessata.

Elementi di transizione completati

Migrazione del rilevamento NVM

Stato	◆◆ completato
Risoluzione	I rilevamenti NVM e le relative impostazioni di rilevamento sono stati trasferiti in XDR a maggio 2026. I clienti che si affidano a notifiche ed esportazioni NVM precedenti devono utilizzare i workflow XDR e convalidare il modello di workflow.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).