Overstap van Secure Cloud Analytics naar Cisco XDR

Inhoud

De belangrijkste verandering

De Secure Cloud Analytics-gebruikerservaring is vanaf 24 oktober 2026 niet meer beschikbaar. Cisco XDR wordt de operationele interface voor SCA-afgeleide detecties, onderzoeken, activacontext, meldingen, exporten en gerelateerde workflows.

⚠ Waarschuwing: Het speciale SCA-naar-XDR-klantovergangsprogramma wordt gepland om te sluiten op 30 september, terwijl 24 oktober 2026 de streefdatum blijft voor de geplande afschrijving van de SCA-gebruikersinterface. Activeer Cisco XDR nu zodat uw team de onderstaande acties voor gereedheid kan uitvoeren.

Onmiddellijke acties en kritieke datums

Wat gebeurt er en wat moet ik nu doen?

Status	Actie vereist

Details	Cisco stopt met de SCA-gebruikerservaring en verplaatst SCA-afgeleide mogelijkheden naar Cisco XDR. Telemetrie en analytics worden onderdeel van bredere XDR-workflows voor activiteiten, detecties, incidenten, onderzoeken, activacontext, respons en automatisering.
Actie van klant	Activeer XDR, sluit de SCA-tenant aan, valideer de toegang, gebruik XDR-detecties en -incidenten voor dagelijkse bewerkingen, gebruik Activiteiten voor brontelemetriecutovers, test XDR-workflows en exporteer historische informatie vóór 24 oktober 2026.

Welke data moet ik plannen?

dateren	mijlpaal	Wat dit betekent
15 september 2026	AWS- en Azure-configuratie voor geselecteerde klanten	Getroffen Amerikaanse en EMEA-klanten gaan over op de aanbevolen XDR-configuratiemethode.
30 september 2026	Speciale SCA-naar-XDR-klantovergangsprogramma wordt afgesloten	Voltooi de acties voor rechten, voorzieningen en gereedheid voordat het programma wordt afgesloten.
7 oktober 2026	AWS CloudTrail, Azure Activity Log en GCP Audit Log-detecties worden doorgesneden	Bedien deze bronnen in XDR.
14 oktober 2026	Aangepaste detecties van gebeurtenissen worden doorgesneden; de configuratie van incidentafstemming, controlelijsten en entiteitsgroepen is beschikbaar in XDR	Verplaats gerelateerde workflows en configuraties naar XDR.
21 oktober 2026	NetFlow-detecties doorgesneden	Bedien NetFlow-detecties in XDR.
24 oktober 2026	SCA-gebruikerservaring niet meer beschikbaar	Voltooi de overstap naar XDR en exporteer historische gegevens vóór deze datum.

Wat gebeurt er als ik niets doe of geen XDR heb geleverd?

Status	Niet aanbevolen
Details	Als u Cisco XDR niet activeert en verbindt voordat de SCA-gebruikerservaring is verwijderd, verliest u toegang tot SCA en hebt u niet de vervangende XDR-ervaring beschikbaar voor uw van SCA afgeleide workflows, detecties, onderzoeken, integraties of historische gegevens. Wachten comprimeert ook activering, gebruikersinstelling, workflowvalidatie en operationele verandering in het laatste deel van de overgang.
Actie van klant	Activeer en sluit XDR nu aan, zodat uw team de gebruikersinstelling, workflowvalidatie en exportvoorbereiding vóór 30 september 2026 kan voltooien. De SCA-interface blijft gericht op afschrijving op 24 oktober 2026; zonder een aangesloten XDR-tenant is er geen vervangende XDR-ervaring beschikbaar wanneer de SCA-toegang eindigt.

Wat is met pensioen gaan, veranderen of niet beschikbaar

Welke SCA-concepten worden expliciet niet in dezelfde vorm voortgezet?

Status	Verandering of pensionering
Details	• SCA gebruikerservaring: verwijderd 24 oktober 2026. • Legacy SCA webhook gedrag: vervangen door XDR workflows. • SCA-observatie: geen één-op-één XDR-functie. • Subnetgevoeligheid: vervangen door concepten voor de prioritering van activa. • Entiteitsgroepen: vervangen door activalabels, activagroepen en waardeclassering. • Snoozed-detectie-instellingen: niet gemigreerd; gebruik Incident Tuning indien beschikbaar. • Klantgestuurd prioriteitsgedrag voor waarschuwingen: niet behouden. • Sommige rapportages, pagina's met lager gebruik en functies: met pensioen of vervangen door XDR-native ervaringen.

Welke rapportage- of integratieposten worden naar verwachting afgeschreven of verplaatst?

Status	Verwachte verandering
Details	Voorbeelden hiervan zijn een observatielijst voor de houding van de cloud, Kubernetes-monitoring, AWS-visualisatie / dashboard / sessie-zoek / IP-zoekervaringen, Meraki- en Umbrella-contextintegraties en maandelijkse e-mailrapporten en dagelijkse waarschuwingsoverzichten. Deze lijst belooft geen één-op-één vervanging voor elke legacy-pagina.

Wat wordt er niet van mij gevraagd in deze migratie?

Status	Geen actie van dit type
Details	Cisco vraagt klanten niet om bestaande netwerksensoren opnieuw te implementeren, cloudlogininname uitsluitend voor de UX-migratie te herconfigureren, handmatig ondersteunde standaarddetectie-configuratieobjecten opnieuw te maken of SCA te behouden als een parallelle console voor de lange termijn.

Controlelijst voor gereedheid van klant

1. Activeer Cisco XDR en sluit de bestaande SCA-huurder aan vóór 30 september 2026, zodat uw team de voorbereidingsacties kan voltooien voordat het overgangsprogramma wordt

afgesloten.
2. Gebruikers maken, aanmelden valideren en de juiste toegang in XDR bevestigen.
3. Detecties, incidenten, activiteiten, onderzoeken en inzichten in bedrijfsmiddelen / apparaatinzichten bekijken.
4. Kaart elke SCA-webhook, export, melding, SIEM / SOAR-overdracht en aangepaste automatisering aan XDR-workflows of een ander XDR-werkoppervlak.
5. Valideer de vereiste brontelemetrie in Activiteiten zodra elke bron beschikbaar komt.
6. Valideer de vereiste detecties en responsplaybooks vóór elke broncode.
7. Beoordeel subnetgevoeligheid, entiteitsgroepen, Snooze, alarmprioriteit, Watchlists, scannerregels, vertrouwde netwerken en prioritering van de waarde van activa.
8. Inventariseer bestaande rapporten, alleen SCA-pagina's en API-afhankelijkheden; identificeer alternatieven of exporteisen.
9. Vereiste meldingen, opmerkingen, onbewerkte logbestanden, configuratieregistraties en rapporten exporteren vóór 24 oktober 2026.

De weg vinden in de nieuwe XDR-ervaring

Hebben SCA-klanten recht op Cisco XDR?

Status	Beschikbaar als onderdeel van de transitie
Details	Bestaande SCA-klanten hebben recht op Cisco XDR als onderdeel van de transitie. Het beoogde resultaat is een continue SCA-waarde terwijl de kernworkflows overgaan op XDR.
Actie van klant	Activeer Cisco XDR, sluit de bestaande SCA-tenant aan en gebruik het Cisco XDR-activeringsproces als er hulp nodig is.

Waar landen mijn SCA-functies in Cisco XDR?

SCA-functie	XDR-bestemming
Waarschuwingen en waarschuwingsworkflows	XDR-detecties en -incidenten
Waarnemingen en event-georiënteerd onderzoek	XDR-activiteiten en XDR-onderzoek
gebeurtenisviewer	XDR Onderzoeken en activiteiten
Context van medisch hulpmiddel	Asset Insights / Device Insights
Webhooks, kennisgevingen, export en downstream levering	XDR-workflows
Detectieconfiguratie	XDR-configuratie wordt ervaren wanneer elke instelling zijn mijlpaal bereikt

Blijft SCA beschikbaar als een parallelle console voor dagelijks gebruik?

Status	Nee

Details	De SCA-gebruikerservaring zal naar verwachting op 24 oktober 2026 worden verwijderd. Gebruik de overlappingsperiode om het XDR-besturingssysteem te oefenen, werkstromen te valideren en werkmappen bij te werken.

Detecties, incidenten en observatie use cases

Bewegen detecties gewoon een-op-een?

Status	Modelwijziging
Details	Nee. Cisco ontwikkelt detectie-inhoud en het besturingssysteem in plaats van elke bestaande SCA-waarschuwing te kopiëren als een onveranderd XDR-object. Namen, logica, bewijs, correlatie en uitkomsten kunnen veranderen.
Actie van klant	Evalueer de uitkomst van de XDR-detectie, het bewijs en de incidentcorrelatie ten opzichte van het beveiligingsscenario dat u moet gebruiken; gebruik naammatching niet alleen als acceptatie.

Moet ik XDR-incidenten of -detecties gebruiken voor mijn waarschuwingsworkflow?

Status	Kiezen op resultaat
Details	Gebruik incidenten voor menselijke respons, meldingen van analisten, triage, escalatie, casemanagement en gecoördineerde respons. Gebruik detecties voor individuele bevindingen, export op detectieniveau en machine-to-machine automatisering. Activiteiten is het oppervlak van de telemetrie.
Actie van klant	Werk runbooks bij zodat menselijke meldingen en responsprocessen worden geactiveerd vanuit incidenten, waar van toepassing; gebruik detecties voor gedetailleerde analyse, export en automatisering op vindniveau.

Zullen op observatie gebaseerde gebruiksgevallen blijven bestaan?

Status	Niet één-op-één
Details	Ga er niet vanuit dat de bestaande observatienaam, het UI-object of de triggervoorwaarde blijven bestaan. Het doel is gelijkwaardig of verbeterde dekking door middel van activiteiten, detecties, incidenten en bredere correlatie.
Actie van klant	Identificeer en update afhankelijkheden in runbooks, dashboards en automatisering vóór 24 oktober 2026.

Wat als ik voornamelijk afhankelijk ben van NetFlow en geen EDR kan implementeren?

Status	Nog steeds in scope
Details	Bestaande netwerksensoren en -opname blijven functioneel en de EDR-implementatie is niet vereist om de gemigreerde netwerkdetecties te blijven gebruiken.
Actie van	Gebruik XDR-detecties, bevindingen, incidenten, incidentafstemming en

klant	beschikbare activacontext. Vraag implementatiespecifieke richtlijnen aan als de zichtbaarheid van het eindpunt sterk beperkt is.

Meldingen, export, webhooks en automatisering

Wat gebeurt er met SCA webhooks?

Status	Migreren en testen
Details	XDR Automate-workflows zijn het controlepunt op lange termijn voor meldingen, exporten en downstream-automatisering. Het doelexportpad is OCSF-uitgelijnd en kan meer volledige contextuele detectiedetails bieden dan het oudere SCA-waarschuwings- en observatiemodel.
Actie van klant	Als een webhook detectiegegevens naar mensen, SIEM, SOAR of een ander systeem stuurt, kunt u dat gedrag opnieuw maken en testen in XDR-workflows.

Wat is het verschil tussen detectie en incident workflows?

Status	Gebruik de overeenkomende trigger
Details	Gebruik detectiegerichte workflows voor gegevensverplaatsing, export en machineverbruik. Gebruik incidentgerichte workflows voor bredere operationele activiteiten en menselijke meldingen zoals e-mail, Slack of Webex. Beide kunnen de export ondersteunen.

Wat verandert er voor SIEM-, SOAR- of aangepaste downstream-integraties?

Status	Beoordeling vereist
Details	Ga er niet vanuit dat een SCA-specifieke webhook, payload, waarschuwingsnaam of export ongewijzigd zal blijven. Het doelexportpad is OCSF-uitgelijnd en kan meer volledige en contextuele detectiedetails bieden.
Actie van klant	Migreer afhankelijkheden naar XDR-workflows en het XDR-gegevensmodel en test vervolgens het downstream ontvangst- en runbookgedrag.

Moet ik NVM-meldingen en -exporten wijzigen?

Status	NVM-cutover voltooid
Details	NVM-detecties verplaatst naar XDR in mei 2026. Klanten die vertrouwen op het oudere webhook-patroon van NVM, moesten meldingen en exporten naar XDR-workflows verplaatsen tegen de coutover van 15 mei 2026.
Actie van klant	Blijf het XDR-workflowpatroon voor NVM gebruiken en valideren.

Wat moet ik testen voordat ik een source cutover krijg?

Status	Vereiste gereedheidscontrole

Actie van klant	Test voor elke bron de detectie- of incidenttrigger, de melding of exportpayload, de downstream ontvangst-, filter- of routeringsregels en de bijgewerkte runbook-respons. Test voordat de bron de SCA-ervaring verlaat.

Telemetriebronnen en source-by-source cutovers

Wanneer is telemetrie beschikbaar in XDR-activiteiten?

dateren	Telemetrie-mijlpaal	Actie van klant
19 augustus 2026	ONA data telemetrie in Activiteiten	Begin met het beoordelen van ONA telemetrie.
26 augustus 2026	CTB-datatelemetrie in activiteiten	Begin met het beoordelen van CTB-telemetrie.
16 september 2026	AWS VPC Flow Logs, Azure Flow Logs en GCP VPC Flow Logs in Activiteiten	Begin met het beoordelen van cloud flow telemetrie.
23 september 2026	AWS-bronconfiguratie in XDR	Gebruik waar van toepassing de XDR-configuratie.
30 september 2026	AWS CloudTrail, Azure Activity Logs en GCP Audit Logs in Activiteiten	Begin met het beoordelen van audit-log telemetrie.

Moet ik netwerksensoren opnieuw implementeren of de opname van cloudlogs opnieuw configureren?

Status	Niet alleen voor UX-migratie
Details	Bestaande netwerksensoren en cloudlog-inname blijven tijdens deze fase functioneel en hoeven niet opnieuw te worden geïmplementeerd of geconfigureerd alleen omdat de gebruikerservaring en detecties naar XDR worden verplaatst.
Belangrijke uitzondering	Openbare IP-adressen of eindpunten die door sensoren en integraties worden gebruikt, kunnen veranderen. Controleer de firewallregels, proxytoleranties en andere netwerkbesturingselementen; Cisco zal de vereiste XDR-eindpuntgegevens verstrekken voordat een configuratiewijziging vereist is.

Wanneer worden brondetecties stopgezet?

Status	Bronspecifiek schema
Details	Bij Cutover zijn telemetrie en detecties voor die bron niet langer beschikbaar voor gebruik via de SCA-gebruikerservaring. • 7 oktober 2026: detecties van AWS CloudTrail, Azure Activity Log en GCP Audit Log. • 14 oktober 2026: Aangepaste Gebeurtenisdetecties. • 21 oktober 2026: NetFlow-detecties.

Instellingen, afstemming, watchlists en asset context

Worden mijn detectieconfiguraties gemigreerd?

Status	Gefaseerde migratie
Details	De verwachting is dat ondersteunde standaardconfiguratieobjecten zullen migreren als onderdeel van de bredere detectie-motortransitie. NVM-detectie-instellingen verplaatst naar XDR in mei 2026; andere instellingen worden overgezet naarmate hun mogelijkheid beschikbaar wordt.
Actie van klant	Maak de standaardinstellingen niet handmatig opnieuw uitsluitend voor de migratie, tenzij Cisco een specifieke instructie voor uw implementatie publiceert.

Wat vervangt subnetgevoeligheid, entiteitsgroepen en Snooze?

Status	Concepten veranderen
Details	• Subnetgevoeligheid: vervangen door prioriteitsscore voor apparaatwaarde in Asset Insights / Device Insights; gepland in XDR Device Insights op 30 september 2026. • Entiteitsgroepen: configuratie gepland in XDR Device Insights op 14 oktober 2026; bestaande groepen migreren naar Labels, waarbij asset labels en waardecortering worden gebruikt voor prioritering. • Snooze: Snoozed-instellingen worden niet gemigreerd; Incident Tuning is gepland om beschikbaar te komen op 14 oktober 2026.

Wanneer bewegen de watchlists?

Status	Gepland op 14 oktober 2026
Details	De configuratie van de watchlist is beschikbaar in XDR op 14 oktober 2026. Bestaande watchlists worden gemigreerd, maar de terminologie en de regelpresentatie kunnen veranderen zolang de logica behouden blijft.
Actie van klant	Valideren van regels, onderdrukking en werkstromen die afhankelijk zijn van de watchlist tijdens de overgang.

Kan ik nog steeds alarmprioriteit instellen zoals ik deed in SCA?

Status	Nee
Details	Alert prioriteit is hard-set met behulp van Cisco bedreiging onderzoek en is niet een door de klant beheerde vals-positieve onderdrukking controle.

Sensoren, cloudintegraties en operationele gezondheid

Blijven FTD, ISE, AWS, Azure of GCP-integraties ongewijzigd?

Status	Bedrijfskritieke paden valideren
Details	Ga er niet vanuit dat elke integratie dezelfde gebruikersinterface, workflow of configuratiemethode behoudt. GCP-configuratie is al in XDR; AWS en Azure gaan de volgende stap; on-premises sensorgerelateerde migratieitems verplaatsen zich in oktober.
Actie van klant	Valideer FTD, ISE-quarantaine, verrijking, SAL-gekoppelde workflows en andere bedrijfskritieke integraties tegen productspecifieke richtlijnen.

Kan ik de gezondheid, levensduur, stroomafgifte en volume van de sensor op dezelfde manier bewaken?

Status	Gereedheidsevaluatie
Details	Cisco onderhoudt de sensor- en inname-operatie tijdens de overgang, maar niet elke SCA-monitoringspagina of -workflow is toegewijd om één voor één te migreren.
Actie van klant	Inventariseer de gezondheids-, protocol-, flow-volume- en leveringscontroles waarvan u afhankelijk bent en valideer hun XDR-besturingssysteem.

Zal de distributie van ONA- of CTB-afbeeldingen, bestemmings-URL's, servicesleutels of openbare IP-adressen veranderen?

Status	Netwerkafhankelijkheden controleren
Details	Cisco vereist in deze fase geen herimplementatie van sensoren, maar telemetriebestemmingen kunnen veranderen naarmate bronnen overgaan naar XDR.
Actie van klant	Controleer de firewallregels, proxy-toelatingslijsten, bestemmings-URL's en afhankelijkheden van de servicesleutel voordat u de relevante broncode selecteert. Breng geen preventieve sensorwijzigingen aan zonder gepubliceerde migratieinstructies.

Historische gegevens, rapportage en administratie

Wat gebeurt er met historische SCA-gegevens wanneer de SCA-gebruikerservaring wordt uitgeschakeld?

Status	Export voor 24 oktober 2026
Details	De toegang tot historische gegevens via de SCA-interface eindigt wanneer de gebruikerservaring wordt verwijderd. Ruwe telemetrie wordt vóór en via het detectiemigratiepad in XDR opgenomen, maar SCA is niet de langetermijnlocatie voor historische opvraging.

	• Waarschuwingen en waarnemingen kunnen worden geëxporteerd als CSV vanaf de SCA-console. • Ruwe logs, inclusief netwerkverkeer en cloudlogs, kunnen indien nodig als CSV worden geëxporteerd. • Definieer audit-, forensische en bewaringsbewijsvereisten voordat u exporteert.

Gaan alle SCA-rapportagefuncties naar XDR?

Status	Sommigen zijn gepensioneerd of vervangen
Details	Sommige rapportagefuncties, pagina's met een lager gebruik en oudere functies worden naar verwachting met pensioen gegaan of vervangen door XDR-native detecties, onderzoeken, activiteiten en inzichten in bedrijfsmiddelen.
Actie van klant	Inventariseer nu operationeel vereiste rapporten en identificeer de XDR-ervaring, export of vervangende workflow.

Hoe moet ik de volledigheid van de migratie aantonen?

Status	Definieer bewijsartefacten
Actie van klant	Definieer vereiste records en bewijsmateriaal, exporteer benodigde SCA-geschiedenis vóór 24 oktober 2026 en valideer XDR-zichtbaarheid voor elke vereiste bron. De overgang is geen door de klant beheerde bulkherinvoer in een afzonderlijk systeem.

Wat gebeurt er met beheerdersinformatie die is opgeslagen op de SCA-zijde?

Status	Document vóór ontmanteling
Details	Ga er niet vanuit dat de door de klant zichtbare configuratie, administratieve informatie of geschiedenis die is opgeslagen in SCA na 24 oktober 2026 beschikbaar blijft.
Actie van klant	Exporteer of documenteer alles wat nodig is voor administratie, audit of historische referentie en gebruik XDR als de doelinterface.

API's en aangepaste integraties

Wat vervangt de Get Observations API, SCA Devices API of andere SCA-specifieke API's?

Status	Voorraadafhankelijkheden
Details	Cisco heeft geen definitieve één-op-één API-vervangingsmatrix voor elke SCA API gepubliceerd. Plan rond activiteiten, detecties, incidenten, workflows, Asset Insights / Device Insights en XDR Investigate.
Actie van	Inventariseer nu directe afhankelijkheden en ga er niet vanuit dat legacy-

klant	eindpuntnamen beschikbaar blijven na 24 oktober 2026.

Wat gebeurt er met legacy incident-creatie methoden en aangepaste automatisering?

Status	Behandel als overgangsmaatregel
Details	De FAQ stelt geen vastgelegde publieke afschrijvingsdatum vast voor elke legacy-incidentcreatiemethode of API. De doelrichting is aangepaste XDR-beveiligingsgebeurtenissen en -detecties, het genereren van incidenten in het XDR-model en het afstemmen van incidenten voor resultaatbeheer.
Actie van klant	Breng elke automatisering die SCA-observaties, waarschuwingsnamen, apparaten, webhooks, exporten of rapporten gebruikt, in kaart in een XDR-workflow, detectie, incident, activiteit of Asset Insights-gebruikscase. Test end-to-end gedrag vóór de relevante broncode.

Afgeronde overgangsposten

NVM-detectiemigratie

Status	✅ Voltooid
resolutie	NVM-detecties en bijbehorende detectie-instellingen zijn in mei 2026 verplaatst naar XDR. Klanten die vertrouwen op oudere NVM-meldingen en -exporten, moeten XDR-workflows gebruiken en het workflowpatroon valideren.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.