

從安全雲分析過渡到Cisco XDR

目錄

- [關鍵變化](#)
- [立即行動和關鍵日期](#)
- [停用、更改或不可用的內容](#)
- [客戶就緒性核對表](#)
- [在新的XDR體驗中尋找自己的方式](#)
- [檢測、事件和觀察使用案例](#)
- [通知、匯出、網路掛接和自動化](#)
- [遙測源和逐源切除](#)
- [設定、調整、監視清單和資產上下文](#)
- [感測器、雲整合和運行狀況](#)
- [歷史資料、報告和管理](#)
- [API和自定義整合](#)
- [已完成過渡專案](#)

關鍵變化

2026年10月24日將不再提供安全雲分析使用者體驗。Cisco XDR成為SCA派生的檢測、調查、資產情景、通知、匯出和相關工作流的操作介面。



注意：專用的SCA到XDR客戶過渡計畫定於9月30日結束，而2026年10月24日仍是計畫棄用SCA使用者介面的目標日期。立即啟用Cisco XDR，以便您的團隊可以完成下面所述的就緒操作。

立即行動和關鍵日期

發生什麼事了，我現在該怎麼辦？

狀態	需採取的行動
詳細資料	思科正在停用SCA使用者體驗，並將SCA衍生的功能遷移到Cisco XDR。遙測和分析成為活動、檢測、事件、調查、資產環境、響應和自動化的更廣泛的XDR工作流程的一部分。
客戶操作	啟用XDR、連線SCA租戶、驗證訪問、使用XDR檢測和事件進行日常操作、使用

	Activities進行源遙測切換、測試XDR工作流程以及在2026年10月24日之前匯出歷史資訊。
--	--

我應該計畫在哪個日期？

日期	里程碑	這意味著什麼
2026年9月15日	針對所選客戶的AWS和Azure配置設定	受影響的美國和EMEA客戶轉向推薦的XDR配置方法。
2026年9月30日	專用的SCA到XDR客戶過渡計畫結束	在計畫結束前完成授權、調配和就緒操作。
2026年10月7日	AWS CloudTrail、Azure Activity Log和GCP稽核日誌檢測已切換	在XDR中操作這些源
2026年10月14日	自定義事件檢測被切斷；XDR中提供了事件調節、監視清單和實體組配置	將相關工作流程和配置移至XDR
2026年10月21日	NetFlow檢測被切斷	在XDR中運行NetFlow檢測
2026年10月24日	SCA使用者體驗不再可用	在此日期之前完成向XDR的遷移並匯出歷史資料。

如果無所作為或未調配XDR，會出現什麼情況？

狀態	不推薦
詳細資料	如果在刪除SCA使用者體驗之前不啟用並連線Cisco XDR，您將失去對SCA的訪問許可權，並且無法為您的SCA衍生工作流、檢測、調查、整合或歷史資料提供替代XDR體驗。等待還會將啟用、使用者設定、工作流驗證和操作更改壓縮到轉換的最後部分。
客戶操作	立即啟用並連線XDR，以便您的團隊能夠在2026年9月30日之前完成使用者設定、工作流驗證和匯出準備。SCA介面仍定於2026年10月24日棄用；如果沒有連線的XDR租戶，在SCA訪問結束時沒有替代的XDR體驗。

停用、更改或不可用的內容

哪些SCA概念顯然不能以相同形式繼續使用？

狀態	更改或報廢
詳細資料	- SCA使用者體驗：於2026年10月24日移除。 - 舊版SCA Webhook行為：替換為XDR工作流。 - SCA觀察體驗：不是一對一XDR功能。 - 子網敏感性：被資產價值優先概念所取代。 - 實體組：替換為資產標籤、資產組和價值評分。 - 暫停檢測設定：未遷移；使用事件調整（如果可用）。 - 客戶控制的警報優先順序行為：未保留。

	一些報告、使用率較低的頁面和功能：已停用，或者由XDR本機體驗取代。
--	--

哪些報告或整合專案應被棄用或移動？

狀態	預期更改
詳細資料	示例包括cloud posture watchlist、Kubernetes monitoring、AWS視覺化/dashboard/session-search/IP-search experience、Meraki和Umbrella情景整合、基於電子郵件的月度報告和每日警報摘要。此清單不保證每個舊版頁面都有一對一的替換。

在此遷移過程中，您不需要我做什麼？

狀態	沒有此型別的操作
詳細資料	思科並不要求客戶重新部署現有網路感測器、重新配置雲日誌接收僅用於UX遷移、手動重新建立支援的標準檢測配置對象或將SCA保留為長期並行控制檯。

客戶就緒性核對表

1. 啟用Cisco XDR並在2026年9月30日之前連線現有的SCA租戶，因此您的團隊可以在過渡計畫關閉之前完成就緒操作。
2. 在XDR中建立使用者、驗證登入並確認適當的訪問許可權。
3. 檢視檢測、事件、活動、調查和資產洞察/裝置洞察。
4. 將每個SCA webhook、匯出、通知、SIEM/SOAR切換和自定義自動化對映到XDR工作流或其他XDR操作介面。
5. 在每個源可用時驗證「活動」中所需的源遙測。
6. 在每個源轉換之前驗證所需的檢測和響應行動手冊。
7. 檢視子網敏感性、實體組、暫停、警報優先順序、監視清單、掃描程式規則、受信任網路和資產價值優先順序。
8. 資產舊報告、僅SCA頁面和API依賴關係；確定替代品或出口要求。
9. 在2026年10月24日之前匯出所需的警報、觀察、原始日誌、配置記錄和報告。

在新的XDR體驗中尋找自己的方式

SCA客戶是否有權使用Cisco XDR？

狀態	作為過渡的一部分提供
詳細資料	作為過渡的一部分，現有SCA客戶有權使用Cisco XDR。目標結果是在核心工作流程進入XDR的同時，繼續實現SCA價值。
客戶操作	啟用Cisco XDR，連線現有的SCA租戶，並在需要幫助時使用Cisco XDR啟用過程。

我的SCA功能在Cisco XDR中處於什麼位置？

SCA函式	XDR目標
警報和警報工作流程	XDR檢測和事件
觀察與事件導向	XDR活動和XDR調查
事件檢視器	XDR調查和活動
裝置上下文	資產洞察/裝置洞察
Webhook、通知、匯出和下游傳送	XDR工作流程
檢測配置	XDR配置體驗隨著每個設定達到其里程碑

SCA是否仍作為並行日常使用控制檯可用？

狀態	否
詳細資料	SCA使用者體驗計畫於2026年10月24日刪除。使用重疊時段來實踐XDR操作模型、驗證工作流和更新Runbook。

檢測、事件和觀察使用案例

檢測是否只是一對一地移動？

狀態	模型更改
詳細資料	不。思科正在改進檢測內容和操作模式，而不是將每個傳統SCA警報作為未更改的XDR對象進行複製。名稱、邏輯、證據、關聯和結果可能會發生變化。
客戶操作	根據您需要操作的安全方案評估XDR檢測結果、證據和事件關聯；不要將名稱匹配單獨用作接受。

我是否應該將XDR事件或檢測用於我的警報工作流？

狀態	按結果選擇
詳細資料	使用突發事件進行人工響應、分析師通知、分類、上報、案例管理以及協調響應。將檢測用於單個結果、檢測級別匯出和機器到機器自動化。活動是遙測面。
客戶操作	更新Runbook，以便在適當情況下從突發事件觸發人工通知和響應流程；使用檢測功能實現詳細的分析、匯出和查詢級別自動化。

基於觀察的使用案例是否繼續？

狀態	不是一對一
詳細資料	不要假定舊觀察名稱、UI對象或觸發條件將保留。目標通過活動、檢測、事件和更廣泛的關聯實現同等或改進的覆蓋範圍。
客戶操作	在2026年10月24日之前確定並更新Runbook、控制板和自動化中的依賴項。

如果我主要依賴NetFlow且無法部署EDR，該怎麼辦？

狀態	仍在範圍內
詳細資料	現有的網路感測器和接收功能仍可正常工作，並且無需部署EDR即可繼續使用遷移的

	網路檢測。
客戶操作	使用XDR檢測、發現、事件、事件調整和可用資產上下文。如果終端可視性受到高度限制，則請求部署特定指南。

通知、匯出、網路掛接和自動化

SCA webhooks會發生什麼情況？

狀態	遷移和測試
詳細資料	XDR自動化工作流是通知、匯出和下游自動化的長期控制點。目標匯出路徑與OCSF一致，可提供比傳統SCA警報和觀察模型更完整的情景檢測詳細資訊。
客戶操作	如果Webhook將檢測資訊傳送給人員、SIEM、SOAR或其他系統，請在XDR工作流中重新建立並測試該行為。

檢測工作流程與突發事件工作流程有何區別？

狀態	使用匹配觸發器
詳細資料	使用面向檢測的工作流程進行資料移動、匯出和機器消耗。使用面向事件的工作流程進行更廣泛的操作活動和人工通知，例如電子郵件、Slack或Webex。兩者都可以支援出口。

SIEM、SOAR或自定義下游整合有哪些變化？

狀態	需要稽核
詳細資料	請勿假設特定於SCA的webhook、負載、警報名稱或匯出將保持不變。目標匯出路徑與OCSF一致，可提供更完整的情景檢測詳細資訊。
客戶操作	將依賴項遷移到XDR工作流和XDR資料模型，然後測試下游接收和Runbook行為。

是否需要更改NVM通知和匯出？

狀態	NVM轉換已完成
詳細資料	NVM檢測於2026年5月移至XDR。依賴傳統NVM webhook模式的客戶需要在2026年5月15日轉換之前移動通知並匯出到XDR工作流。
客戶操作	繼續使用和驗證NVM的XDR工作流模式。

在源轉換之前應該測試什麼？

狀態	必需的就緒檢查
客戶操作	對於每個源，測試檢測或事件觸發器、通知或匯出負載、下游接收、過濾或路由規則以及更新的Runbook響應。在源離開SCA體驗之前進行測試。

遙測源和逐源切除

XDR活動何時提供遙測功能？

日期	遙測里程碑	客戶操作
2026年8月19日	活動中的ONA資料遙測	開始複查ONA遙測。
2026年8月26日	活動中的CTB資料遙測	開始複查CTB遙測。
2026年9月16日	活動中的AWS VPC流日誌、Azure流日誌和GCP VPC流日誌	開始檢視雲流遙測。
2026年9月23日	XDR中的AWS源配置	如果適用，請使用XDR配置體驗。
2026年9月30日	活動中的AWS CloudTrail、Azure活動日誌和GCP稽核日誌	開始檢視稽核日誌遙測。

我是否需要重新部署網路感測器或重新配置雲日誌接收？

狀態	不，不僅僅適用於UX遷移
詳細資料	現有網路感測器和雲日誌接收在此階段保持正常運行，並且無需重新部署或重新配置，因為使用者體驗和檢測將遷移到XDR。
重要例外	感測器和整合使用的公共IP地址或端點可能會發生變化。檢查防火牆規則、代理允許清單和其他網路控制；在需要更改配置之前，思科將提供所需的XDR終端詳細資訊。

源檢測何時切斷？

狀態	源特定計畫
詳細資料	在轉換時，該源的遙測和檢測無法再通過SCA使用者體驗使用。 • 2026年10月7日：檢測到AWS CloudTrail、Azure Activity Log和GCP稽核日誌。 • 2026年10月14日：自定義事件檢測。 • 2026年10月21日：NetFlow檢測。

設定、調整、監視清單和資產上下文

是否遷移我的檢測配置？

狀態	分階段遷移
詳細資料	支援的標準配置對象預期會作為更廣泛的檢測引擎轉換的一部分進行遷移。NVM檢測設定於2026年5月移至XDR;其他設定在其功能可用時進行轉換。
客戶操作	除非思科針對您的部署發佈特定說明，否則不要只為遷移手動重新建立標準設定。

什麼可以取代子網敏感性、實體組和暫停？

狀態	概念更改
詳細資料	- 子網敏感性：由資產洞察/裝置洞察中的裝置價值優先順序評分取代；計畫在2026年9月30日前在XDR裝置洞察中發佈。 - 實體組：2026年10月14日在XDR Device Insights中計畫的配置；現有組將遷移至標籤，資產標籤和值評分用於劃分優先順序。 - 暫停：暫停的設定不會遷移；事件調整計畫於2026年10月14日推出。

監視清單何時移動？

狀態	計畫於2026年10月14日
詳細資料	監視清單配置計畫於2026年10月14日在XDR中提供。將遷移現有的監視清單，但保留邏輯後，術語和規則表示可能會發生變化。
客戶操作	在轉換期間驗證與監視清單相關的規則、抑制和工作流。

我是否仍可以像在SCA中那樣設定警報優先順序？

狀態	否
詳細資料	警報優先順序使用思科威脅研究進行硬設定，不是客戶管理的誤報抑制控制。

感測器、雲整合和運行狀況

FTD、ISE、AWS、Azure或GCP整合是否保持不變？

狀態	驗證業務關鍵路徑
詳細資料	不要假定每個整合都保留相同的UI、工作流或配置方法。GCP配置已在XDR中；AWS和Azure將緊隨其後；與感測器相關的本地遷移專案將在10月遷移。
客戶操作	根據特定於產品的指導，驗證FTD、ISE隔離、豐富、與SAL連線的工作流程和其他關鍵業務整合。

我可以用同樣的方法監控感測器的健康狀況、活性、流量傳輸和容量嗎？

狀態	就緒性稽核
詳細資料	思科在過渡期間會維護感測器和接收操作，但並非每個SCA監控頁面或工作流程都承諾進行一對一遷移。
客戶操作	清查您所依賴的運行狀況、協定、流量和交付情況檢查，並驗證其XDR操作路徑。

ONA或CTB映像的分佈、目標URL、服務金鑰或公共IP地址是否會更改？

狀態	檢視網路相關性
詳細資料	在此階段，思科不要求重新部署感測器，但遙測目標可能會隨著源過渡到XDR而更改。
客戶操作	在相關源轉換之前，檢查防火牆規則、代理允許清單、目標URL和服務金鑰依賴關係

	。如果沒有發佈遷移說明，請勿進行預防性感測器更改。
--	---------------------------

歷史資料、報告和管理

當SCA使用者體驗關閉時，歷史SCA資料會發生什麼情況？

狀態	2026年10月24日之前出口
詳細資料	通過SCA介面訪問歷史資料將在使用者體驗被移除時結束。原始遙測在檢測遷移路徑之前和通過檢測遷移路徑接收到XDR中，但SCA不是用於歷史檢索的長期位置。 - 警報和觀察結果可以從SCA控制檯匯出為CSV。 - 如果需要，原始日誌（包括網路流量和雲日誌）可以匯出為CSV。 - 在匯出之前定義稽核、調查分析和保留證據要求。

是否所有SCA報告功能都將移至XDR？

狀態	某些已報廢或已更換
詳細資料	某些報告功能、使用率較低的頁面和舊版功能預計會停用，或由XDR本機檢測、調查、活動和資產洞察體驗取代。
客戶操作	立即清點操作所需的報告並確定XDR體驗、匯出或更換工作流程。

如何演示遷移的完整性？

狀態	定義證明工件
客戶操作	定義所需的記錄和證據，在2026年10月24日之前匯出所需的SCA歷史記錄，並驗證每個所需來源的XDR可見性。該過渡不是客戶管理的批次重新匯入到單獨的系統中。

儲存在SCA端的管理員資訊會發生什麼情況？

狀態	在停用前提供文檔
詳細資料	請勿假設SCA中儲存的客戶可見的配置、管理資訊或歷史記錄在2026年10月24日之後仍然可用。
客戶操作	匯出或記錄管理、稽核或歷史參考所需的任何內容，並使用XDR作為目標操作介面。

API和自定義整合

以下哪一項可取代獲取觀察API、SCA裝置API或其他特定於SCA的API？

狀態	庫存相關性
詳細資料	思科尚未針對每個SCA API發佈最終一對一API替換矩陣。圍繞活動、檢測、事件、工作流、資產洞察/裝置洞察和XDR調查進行規劃。
客戶操作	現在庫存直接依賴項，並且不假定舊式終端名稱在2026年10月24日之後仍然可用。

傳統的事件建立方法和自定義自動化會發生什麼情況？

狀態	視為過渡狀態
詳細資料	FAQ沒有為每個舊式事件建立方法或API建立已提交的公共棄用日期。目標方向是XDR自定義安全事件和檢測、XDR模型中的事件生成以及用於結果管理的事件調整。
客戶操作	將每個使用SCA觀察、警報名稱、裝置、網路掛接、匯出或報告的自動化對映到XDR工作流、檢測、事件、活動或資產洞察使用案例。在相關源轉換之前測試端到端行為。

已完成過渡專案

NVM檢測遷移

狀態	◆◆成
解析	NVM檢測和相關檢測設定於2026年5月移入XDR。依賴傳統NVM通知和匯出的客戶應使用XDR工作流並驗證工作流模式。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。