Übergang von sicheren Cloud-Analysen zu Cisco XDR

Inhalt

Die wichtigsten Änderungen

Secure Cloud Analytics ist ab dem 24. Oktober 2026 nicht mehr verfügbar. Cisco XDR wird zur Bedienoberfläche für SCA-abgeleitete Erkennungen, Untersuchungen, Ressourcenkontext, Benachrichtigungen, Exporte und zugehörige Workflows.

⚠ Vorsicht: Das dedizierte SCA-to-XDR-Kundenübergangsprogramm soll am 30. September abgeschlossen werden, während der 24. Oktober 2026 das Zieldatum für die geplante Abwertung der SCA-Benutzeroberfläche bleibt. Aktivieren Sie jetzt Cisco XDR, damit Ihr Team die unten beschriebenen Vorbereitungsaktionen durchführen kann.

Sofortmaßnahmen und kritische Termine

Was passiert, und was sollte ich jetzt tun?

Status	Maßnahme erforderlich

Details	Cisco stellt die SCA-Benutzerumgebung ein und überträgt von SCA abgeleitete Funktionen auf Cisco XDR. Telemetrie und Analysen werden Teil umfassenderer XDR-Workflows für Aktivitäten, Erkennungen, Vorfälle, Untersuchungen, Ressourcenkontext, Reaktion und Automatisierung.
Kundenaktion	Aktivieren Sie XDR, schließen Sie den SCA-Tenant an, validieren Sie den Zugriff, verwenden Sie XDR-Erkennungen und -Vorfälle für den täglichen Betrieb, verwenden Sie Aktivitäten für die Übernahme der Quelltelemetrie, testen Sie XDR-Workflows, und exportieren Sie historische Informationen bis zum 24. Oktober 2026.

An welchen Terminen sollte ich mich orientieren?

Datum	Meilenstein	Was bedeutet das?
15. September 2026	AWS- und Azure-Konfiguration für ausgewählte Kunden	Betroffene Kunden in den USA und EMEA wechseln zur empfohlenen XDR-Konfigurationsmethode.
30. September 2026	Abschluss des dedizierten SCA-zu-XDR-Programms für den Kundenwechsel	Führen Sie Berechtigungen, Bereitstellung und Vorbereitungsmaßnahmen durch, bevor das Programm endet.
7. Oktober 2026	Erkennung von AWS CloudTrail, Azure Activity Log und GCP Audit Log gekürzt	Nutzen Sie diese Quellen in XDR.
14. Oktober 2026	Benutzerdefinierte Ereigniserkennung umgeschaltet; Konfiguration von Incident Tuning, Watchlists und Entity Groups in XDR verfügbar	Verschieben verwandter Workflows und Konfigurationen auf XDR
21. Oktober 2026	NetFlow-Erkennungsfunktion unterbrochen	Betrieb von NetFlow-Erkennungen in XDR
24. Oktober 2026	SCA-Benutzerumgebung nicht mehr verfügbar	Schließen Sie den Wechsel zu XDR ab, und exportieren Sie historische Daten vor diesem Datum.

Was passiert, wenn ich nichts tue oder XDR nicht bereitgestellt habe?

Status	Nicht empfohlen
Details	Wenn Sie Cisco XDR nicht aktivieren und verbinden, bevor die SCA-Benutzererfahrung entfernt wird, verlieren Sie den Zugriff auf SCA und verfügen nicht über die XDR-Ersatzerfahrung für Ihre SCA-abgeleiteten Workflows, Erkennungen, Untersuchungen, Integrationen oder Verlaufsdaten. Waiting komprimiert außerdem die Aktivierung, die Benutzereinrichtung, die Validierung der Workflows und die betrieblichen Änderungen im letzten Teil der Umstellung.
Kundenaktion	Aktivieren und verbinden Sie XDR jetzt, damit Ihr Team vor dem 30. September 2026 die Benutzereinrichtung, die Workflow-Validierung und die Exportvorbereitung abschließen kann. Die SCA-Schnittstelle wird weiterhin am 24. Oktober 2026 als veraltet eingestuft. ohne angeschlossenen XDR-Tenant ist nach Beendigung des

	SCA-Zugriffs kein Ersatz-XDR-Erlebnis verfügbar.

Was wird eingestellt, geändert oder ist nicht verfügbar?

Welche SCA-Konzepte setzen sich explizit nicht in der gleichen Form fort?

Status	Änderung oder Außerbetriebnahme
Details	• SCA-Benutzererfahrung: am 24. Oktober 2026 entfernt. • Verhalten des älteren SCA-Webhooks: ersetzt durch XDR-Workflows. • SCA-Beobachtungserfahrung: keine 1:1-XDR-Funktion. • Subnetzempfindlichkeit: durch Konzepte zur Priorisierung der Vermögenswerte ersetzt. • Entitätsgruppen: durch Anlagenbeschriftungen, Anlagengruppen und Wertbewertung ersetzt. • Einstellungen für die Erkennungsfunktion für Erstickungen: nicht migriert; Falls verfügbar, verwenden Sie Incident Tuning. • Vom Kunden gesteuerte Warnungspriorität: nicht beibehalten. • Einige Berichte, Seiten mit geringerer Auslastung und Funktionen: in den Ruhestand versetzt oder durch XDR-native Funktionen ersetzt.

Welche Berichts- oder Integrationselemente werden voraussichtlich veraltet oder verschoben?

Status	Erwartete Änderung
Details	Beispiele hierfür sind Cloud-Statusüberwachungslisten, Kubernetes-Monitoring, AWS-Visualisierung/Dashboard/Sitzungssuche/IP-Suche, Meraki- und Umbrella-Kontextintegrationen sowie E-Mail-basierte Monatsberichte und tägliche Warnzusammenfassungen. Diese Liste verspricht keinen 1:1-Ersatz für jede Legacy-Seite.

Was wird in dieser Migration nicht von mir verlangt?

Status	Keine Aktion dieses Typs
Details	Cisco fordert seine Kunden nicht auf, vorhandene Netzwerksensoren neu bereitzustellen, die Erfassung von Cloud-Protokollen nur für die UX-Migration neu zu konfigurieren, unterstützte Standarderkennungskonfigurationsobjekte manuell neu zu erstellen oder SCA als langfristige parallele Konsole beizubehalten.

Checkliste zur Kundenbereitschaft

1. Aktivieren Sie Cisco XDR, und verbinden Sie den vorhandenen SCA-Tenant vor dem 30. September 2026. So kann Ihr Team die Bereitschaftsaktionen abschließen, bevor das

Übergangsprogramm endet.
2. Erstellen Sie Benutzer, validieren Sie die Anmeldung, und bestätigen Sie den entsprechenden Zugriff in XDR.
3. Überprüfung von Erkennungen, Vorfällen, Aktivitäten, Untersuchungen und Einblicken in Ressourcen/Geräte
4. Ordnen Sie jeden SCA-Webhook, -Export, -Benachrichtigung, SIEM/SOAR-Übergabe und jede benutzerdefinierte Automatisierung XDR-Workflows oder einer anderen XDR-Bedienoberfläche zu.
5. Validieren Sie die erforderliche Quelltelemetrie in "Activities" (Aktivitäten), sobald die Quellen verfügbar sind.
6. Validieren Sie die erforderlichen Erkennungen und strategischen Leitfäden für die Reaktion vor der Umstellung auf die neue Quelle.
7. Überprüfen Sie die Subnetz-Empfindlichkeit, Entitätsgruppen, Snooze, Alert-Priorität, Watchlists, Scanner-Regeln, vertrauenswürdige Netzwerke und die Priorisierung von Ressourcen.
8. Bestandsaufnahme älterer Berichte, nur SCA-Seiten und API-Abhängigkeiten Alternativen oder Exportanforderungen zu ermitteln.
9. Exportieren erforderlicher Warnmeldungen, Beobachtungen, Rohprotokolle, Konfigurationsdatensätze und Berichte vor dem 24. Oktober 2026

Die neue XDR-Erfahrung

Haben SCA-Kunden Anspruch auf Cisco XDR?

Status	Verfügbar als Teil der Umstellung
Details	Bestehende SCA-Kunden haben im Rahmen der Umstellung Anspruch auf Cisco XDR. Das angestrebte Ergebnis ist ein kontinuierlicher SCA-Wert, während die Core-Workflows in XDR migriert werden.
Kundenaktion	Aktivieren Sie Cisco XDR, schließen Sie den vorhandenen SCA-Tenant an, und verwenden Sie den Cisco XDR-Aktivierungsprozess, wenn Sie Hilfe benötigen.

Wo befinden sich meine SCA-Funktionen in Cisco XDR?

SCA-Funktion	XDR-Ziel
Warnungen und Warn-Workflows	XDR-Erkennungen und -Vorfälle
Beobachtungen und ereignisorientierte Untersuchungen	XDR-Aktivitäten und XDR-Untersuchung
Ereignisanzeige	XDR-Untersuchung und -Aktivitäten
Gerätekontext	Ressourceneinblicke/Geräteeinblicke
Webhooks, Benachrichtigungen, Exporte und nachgelagerte Bereitstellung	XDR-Workflows
Erkennungskonfiguration	Die XDR-Konfiguration wird wahrgenommen, wenn jede

	Einstellung ihren Meilenstein erreicht.

Wird SCA als parallele Konsole für den täglichen Gebrauch verfügbar bleiben?

Status	Nein
Details	Die SCA-Benutzererfahrung soll am 24. Oktober 2026 entfernt werden. Verwenden Sie die Überlappungsperiode, um das XDR-Betriebsmodell zu üben, Workflows zu validieren und Runbooks zu aktualisieren.

Erkennung, Vorfälle und Anwendungsfälle zur Beobachtung

Werden Erkennungen einfach "One-to-One"-Angriffe erkannt?

Status	Modelländerung
Details	Nein. Cisco entwickelt Erkennungsinhalte und das Betriebsmodell weiter, anstatt jede ältere SCA-Warnung als unverändertes XDR-Objekt zu kopieren. Namen, Logik, Beweise, Korrelation und Ergebnisse können sich ändern.
Kundenaktion	Bewerten Sie das Ergebnis, den Nachweis und die Korrelation von Vorfällen mit der XDR-Erkennung anhand des Sicherheitsszenarios, das Sie benötigen. Verwenden Sie nicht nur die Namenszuordnung als Annahme.

Soll ich XDR-Vorfälle oder -Erkennungen für meinen Warn-Workflow verwenden?

Status	Nach Ergebnis auswählen
Details	Einsatz von Vorfällen für die Reaktion durch Mitarbeiter, Analystenbenachrichtigungen, Triage, Eskalation, Fallmanagement und koordinierte Reaktion Verwenden Sie Erkennungen für individuelle Ergebnisse, den Export auf Erkennungsebene und die Automation von Maschine zu Maschine. Aktivitäten ist die Telemetrieoberfläche.
Kundenaktion	Aktualisierung von Runbooks, damit bei Zwischenfällen ggf. menschliche Benachrichtigungen und Reaktionsprozesse ausgelöst werden; Verwenden Sie Erkennungen für detaillierte Analysen, Exporte und Automatisierung auf Suchebene.

Werden die beobachtungsbasierten Anwendungsfälle fortgesetzt?

Status	Nicht One-to-One
Details	Gehen Sie nicht davon aus, dass der Name der älteren Beobachtung, das UI-Objekt oder die Triggerbedingung erhalten bleiben. Das Ziel ist eine gleichwertige oder verbesserte Abdeckung durch Aktivitäten, Erkennungen, Vorfälle und eine umfassendere Korrelation.
Kundenaktion	Identifizieren und Aktualisieren von Abhängigkeiten in Runbooks, Dashboards und Automatisierungsprozessen vor dem 24. Oktober 2026

Was wäre, wenn ich mich hauptsächlich auf NetFlow verlasse und EDR nicht bereitstellen könnte?

Status	Noch im Geltungsbereich
Details	Vorhandene Netzwerksensoren und die Erfassung bleiben funktionsfähig, und die EDR-Bereitstellung ist nicht erforderlich, um migrierte Netzwerkerkennungen weiterhin verwenden zu können.
Kundenaktion	Nutzung von XDR-Erkennungen, -Erkennungen, -Vorfällen, -Tuning und des Kontexts der verfügbaren Ressourcen Wenn die Transparenz von Endgeräten stark eingeschränkt ist, können Sie um bereitstellungsspezifische Unterstützung bitten.

Benachrichtigungen, Exporte, Webhooks und Automatisierung

Was passiert mit SCA Webhooks?

Status	Migration und Tests
Details	XDR-Automatisierungs-Workflows sind der langfristige Kontrollpunkt für Benachrichtigungen, Exporte und nachgeschaltete Automatisierung. Der Zielexportpfad ist OCSF-orientiert und bietet umfassendere kontextbezogene Erkennungsdetails als das ältere SCA-Warnungs- und Beobachtungsmodell.
Kundenaktion	Wenn ein Webhook Erkennungsinformationen an Personen, SIEM, SOAR oder ein anderes System sendet, erstellen Sie dieses Verhalten neu und testen es in XDR-Workflows.

Worin besteht der Unterschied zwischen Erkennungs- und Incident-Workflows?

Status	Den passenden Auslöser verwenden
Details	Verwenden Sie erkennungsorientierte Workflows für Datenbewegungen, Exporte und den Maschinenverbrauch. Einsatz vorfallsorientierter Workflows für breitere betriebliche Aktivitäten und menschliche Benachrichtigungen wie E-Mail, Slack oder WebEx. Beide können den Export unterstützen.

Welche Änderungen ergeben sich bei SIEM, SOAR oder benutzerdefinierten Downstream-Integrationen?

Status	Prüfung erforderlich
Details	Gehen Sie nicht davon aus, dass ein SCA-spezifischer Webhook, eine Nutzlast, ein Warnungsname oder ein Export unverändert fortgeführt werden. Der Zielexportpfad ist OCSF-ausgerichtet und bietet umfassendere kontextbezogene Erkennungsdetails.
Kundenaktion	Migrieren Sie Abhängigkeiten zu XDR-Workflows und dem XDR-Datenmodell, und testen Sie dann das Downstream-Empfangsverhalten und das Runbook-Verhalten.

Muss ich die NVM-Benachrichtigungen und -Exporte ändern?

Status	NVM-Umstellung abgeschlossen
Details	Die NVM-Erkennung wurde im Mai 2026 auf XDR verschoben. Kunden, die sich auf das ältere NVM-Webhook-Muster verlassen, mussten bis zur Umstellung am 15. Mai 2026 Benachrichtigungen und Exporte in XDR-Workflows verschieben.
Kundenaktion	Verwenden und validieren Sie weiterhin das XDR-Workflow-Muster für NVM.

Was sollte ich vor der Umstellung auf eine neue Bezugsquelle testen?

Status	Erforderliche Bereitschaftsprüfung
Kundenaktion	Testen Sie für jede Quelle die Erkennungs- oder Incident-Trigger-, Benachrichtigungs- oder Export-Payload, die Downstream-Empfangs-, Filter- oder Routing-Regeln und die aktualisierte Runbook-Antwort. Führen Sie einen Test durch, bevor die Quelle den SCA verlässt.

Telemetriequellen und Source-by-Source-Umstellung

Wann wird Telemetrie in XDR-Aktivitäten verfügbar sein?

Datum	Telemetrie-Meilenstein	Kundenaktion
19. August 2026	ONA-Datentelemetrie in Aktivitäten	Beginnen Sie mit der Prüfung der ONA-Telemetrie.
26. August 2026	CTB-Datentelemetrie in Aktivitäten	Beginnen Sie mit der Prüfung der CTB-Telemetrie.
16. September 2026	AWS VPC-Flow-Protokolle, Azure-Flow-Protokolle und GCP-VPC-Flow-Protokolle in Aktivitäten	Beginnen Sie mit der Überprüfung der Cloud-Flow-Telemetrie.
23. September 2026	AWS-Quellkonfiguration in XDR	Nutzen Sie ggf. die XDR-Konfigurationserfahrung.
30. September 2026	AWS CloudTrail, Azure-Aktivitätsprotokolle und GCP-Überwachungsprotokolle in Aktivitäten	Beginnen Sie mit der Überprüfung der Telemetrie des Prüfprotokolls.

Müssen Netzwerksensoren neu bereitgestellt oder die Erfassung von Cloud-Protokollen neu konfiguriert werden?

Status	Nein, nicht nur für UX-Migration
Details	Vorhandene Netzwerksensoren und die Erfassung von Cloud-Protokollen bleiben in dieser Phase funktionsfähig und müssen nicht neu bereitgestellt oder neu konfiguriert werden, nur weil die Benutzerumgebung und die Erkennungsfunktionen auf XDR umgestellt werden.
Wichtige	Öffentliche IP-Adressen oder Endpunkte, die von Sensoren und Integrationen

Ausnahme	verwendet werden, können sich ändern. Überprüfung von Firewall-Regeln, Proxy-Zulassungslisten und anderen Netzwerkkontrollen; Bevor eine Konfigurationsänderung erforderlich ist, stellt Cisco die erforderlichen Details für das XDR-Endgerät bereit.

Wann wird die Quellenerkennung unterbrochen?

Status	Quellspezifischer Zeitplan
Details	Nach der Umstellung können Telemetrie und Erkennungsfunktionen für diese Quelle nicht mehr über die SCA-Benutzerumgebung genutzt werden. • 7. Oktober 2026: Erkennung von AWS CloudTrail, Azure-Aktivitätsprotokoll und GCP-Überwachungsprotokoll. • 14. Oktober 2026: Benutzerdefinierte Ereigniserkennungen. • 21. Oktober 2026: NetFlow wird erkannt.

Einstellungen, Tuning, Watchlisten und Ressourcenkontext

Werden meine Erkennungskonfigurationen migriert?

Status	Phasenweise Migration
Details	Es wird erwartet, dass die unterstützten Standardkonfigurationsobjekte im Rahmen des umfassenderen Übergangs zur Erkennungs-Engine migriert werden. NVM-Erkennungseinstellungen wurden im Mai 2026 auf XDR verschoben; Die anderen Einstellungen werden angepasst, sobald sie verfügbar sind.
Kundenaktion	Erstellen Sie die Standardeinstellungen nur für die Migration manuell neu, es sei denn, Cisco veröffentlicht eine spezielle Anweisung für Ihre Bereitstellung.

Was ersetzt Subnetz-Empfindlichkeit, Entitätsgruppen und Snooze?

Status	Konzepte ändern sich
Details	• Subnetzempfindlichkeit: in Asset Insights/Device Insights durch eine Bewertung der Gerätewerte ersetzt. geplant für XDR Device Insights bis zum 30. September 2026. • Entitätsgruppen: Konfiguration geplant für XDR Device Insights am 14. Oktober 2026; Bestehende Gruppen werden zu Labels migriert, wobei die Labels der Ressourcen und die Wertebewertung für die Priorisierung verwendet werden. • Schlummern: nicht migrierte Einstellungen; Incident Tuning soll am 14. Oktober 2026 verfügbar sein.

Wann werden Watchlists verschoben?

Status	Geplant am 14. Oktober 2026
Details	Die Konfiguration der Watchlist ist für den 14. Oktober 2026 in XDR geplant. Bestehende Watchlists werden migriert, aber Terminologie und Regeldarstellung können sich ändern, solange die Logik erhalten bleibt.
Kundenaktion	Validieren Sie während des Übergangs watchlist-abhängige Regeln, Unterdrückung und Workflows.

Kann ich die Priorität der Warnmeldung weiterhin auf die gleiche Weise festlegen wie in SCA?

Status	Nein
Details	Die Priorität von Warnmeldungen ist mithilfe der Bedrohungsforschung von Cisco sehr streng festgelegt und stellt keine vom Kunden verwaltete Kontrolle zur Unterdrückung von Fehlalarmen dar.

Sensoren, Cloud-Integration und Betriebszustand

Bleiben FTD-, ISE-, AWS-, Azure- oder GCP-Integrationen unverändert?

Status	Validierung geschäftskritischer Pfade
Details	Gehen Sie nicht davon aus, dass bei jeder Integration dieselbe Benutzeroberfläche, derselbe Workflow oder dieselbe Konfigurationsmethode beibehalten wird. Die GCP-Konfiguration befindet sich bereits in XDR.; AWS und Azure werden als Nächstes verschoben. Standortbasierte, sensorbezogene Migrationselemente werden im Oktober verschoben.
Kundenaktion	Validierung von FTD, ISE-Quarantäne, Anreicherung, mit SAL verbundenen Workflows und anderen geschäftskritischen Integrationen unter Berücksichtigung produktspezifischer Richtlinien

Kann ich den Zustand, die Lebensdauer, die Flussabgabe und die Lautstärke der Sensoren auf dieselbe Weise überwachen?

Status	Bereitschafts-Review
Details	Während der Übergangsphase werden die Sensoren und der Aufnahmevorgang von Cisco aufrechterhalten, aber nicht jede SCA-Überwachungsseite oder jeder SCA-Workflow wird einzeln migriert.
Kundenaktion	Bestandsaufnahme der Status-, Protokoll-, Flow-Volume- und Bereitstellungsprüfungen, von denen Sie abhängen, und Validierung des XDR-Betriebspfads

Werden sich die Verteilung von ONA- oder CTB-Bildern, die Ziel-URLs, die Serviceschlüssel oder die öffentlichen IP-Adressen ändern?

Status	Überprüfung der Netzwerkabhängigkeiten

Details	Cisco benötigt in dieser Phase keine erneute Bereitstellung der Sensoren, aber Telemetrieziele können sich ändern, wenn Quellen zu XDR wechseln.
Kundenaktion	Überprüfen Sie Firewall-Regeln, Proxy-Zulassungslisten, Ziel-URLs und Service-Schlüssel-Abhängigkeiten, bevor Sie die relevante Quelle umstellen. Nehmen Sie ohne veröffentlichte Migrationsanweisungen keine präventiven Sensoränderungen vor.

Verlaufsdaten, Berichte und Verwaltung

Was passiert mit historischen SCA-Daten, wenn die SCA-Benutzerumgebung ausgeschaltet wird?

Status	Export vor dem 24. Oktober 2026
Details	Der Zugriff auf Verlaufsdaten über die SCA-Schnittstelle endet, wenn die Benutzererfahrung beendet ist. Rohtelemetrie wird vor und über den Migrationspfad für die Erkennung in XDR aufgenommen. SCA ist jedoch nicht der langfristige Speicherort für Verlaufsabrufe. • Warnungen und Beobachtungen können von der SCA-Konsole als CSV exportiert werden. • Rohprotokolle wie Netzwerk- und Cloud-Datenverkehr können bei Bedarf als CSV-Datei exportiert werden. • Definieren Sie vor dem Export die Anforderungen für Audits, Forensik und Aufbewahrungsnachweise.

Werden alle SCA-Berichtsfunktionen auf XDR verschoben?

Status	Einige eingestellt oder ersetzt
Details	Es wird erwartet, dass einige Berichtsfunktionen, Seiten mit geringerer Nutzung und Legacy-Funktionen eingestellt oder durch XDR-native Erkennungs-, Untersuchungs-, Aktivitäts- und Ressourceneinblicke ersetzt werden.
Kundenaktion	Erfassen Sie jetzt die betriebsnotwendigen Berichte, und identifizieren Sie den XDR-Erfahrungs-, Export- oder Austausch-Workflow.

Wie sollte ich die Vollständigkeit der Migration demonstrieren?

Status	Beweisartefakte definieren
Kundenaktion	Definieren Sie erforderliche Datensätze und Belege, exportieren Sie den benötigten SCA-Verlauf vor dem 24. Oktober 2026, und validieren Sie die XDR-Transparenz für jede erforderliche Quelle. Bei der Umstellung handelt es sich nicht um einen vom Kunden verwalteten Massenimport in ein separates System.

Was geschieht mit den Administratorinformationen, die auf der Seite des SCA

gespeichert sind?

Status	Dokument vor der Stilllegung
Details	Gehen Sie nicht davon aus, dass vom Kunden einsehbare Konfigurationen, administrative Informationen oder der in SCA gespeicherte Verlauf nach dem 24. Oktober 2026 verfügbar bleiben.
Kundenaktion	Exportieren oder dokumentieren Sie alle für Administration, Audit oder Verlaufsdaten erforderlichen Daten, und verwenden Sie XDR als Ziel-Bedienoberfläche.

APIs und kundenspezifische Integrationen

Was ersetzt die Get Observations API, die SCA Devices API oder andere SCA-spezifische APIs?

Status	Bestandsabhängigkeiten
Details	Cisco hat keine endgültige Eins-zu-Eins-API-Ersatzmatrix für jede SCA-API veröffentlicht. Planen Sie Aktivitäten, Erkennungen, Vorfälle, Workflows, Ressourceneinblicke/Geräteeinblicke und XDR Investigate.
Kundenaktion	Suchen Sie jetzt nach direkten Abhängigkeiten, und gehen Sie nicht davon aus, dass nach dem 24. Oktober 2026 weiterhin ältere Endpunktnamen verfügbar sind.

Was geschieht mit den Methoden zur Erstellung älterer Vorfälle und der benutzerdefinierten Automatisierung?

Status	Übergangsbehandlung
Details	In der FAQ wird kein verbindliches Datum für die öffentliche Kündigung aller Methoden oder APIs zur Erstellung von Vorfällen festgelegt. Die Zielrichtung sind benutzerdefinierte XDR-Sicherheitsereignisse und -erkennungen, Vorfallgenerierung im XDR-Modell und Incident-Tuning für das Ergebnismanagement.
Kundenaktion	Ordnen Sie alle automatisierungsintensiven SCA-Beobachtungen, Warnungsnamen, Geräte, Webhooks, Exporte oder Berichte einem XDR-Workflow, einer Erkennung, einem Vorfall, einer Aktivität oder einem Asset Insights-Anwendungsfall zu. Testen Sie das End-to-End-Verhalten vor der entsprechenden Umstellung der Quelle.

Abgeschlossene Übergangselemente

NVM-Erkennungsmigration

Status	✅ Abgeschlossen

Auflösung	NVM-Erkennungen und zugehörige Erkennungseinstellungen wurden im Mai 2026 in XDR verschoben. Kunden, die sich auf ältere NVM-Benachrichtigungen und -Exporte verlassen, sollten XDR-Workflows verwenden und das Workflow-Muster validieren.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.