

从安全云分析过渡到思科XDR

目录

- [关键变化](#)
- [立即行动和关键日期](#)
- [什么即将停用、更改或不可用](#)
- [客户就绪性核对表](#)
- [在新的XDR体验中寻找自己的方法](#)
- [检测、事件和观察使用案例](#)
- [通知、导出、网络挂接和自动化](#)
- [遥测源和逐源转换](#)
- [设置、调整、监视列表和资产情景](#)
- [传感器、云集成和运行状况](#)
- [历史数据、报告和管理](#)
- [API和自定义集成](#)
- [已完成的过渡项目](#)

关键变化

2026年10月24日将不再提供安全云分析用户体验。Cisco XDR成为SCA派生的检测、调查、资产情景、通知、导出和相关工作流的操作界面。



警告：专门的SCA到XDR客户过渡计划定于9月30日结束，而2026年10月24日仍是计划弃用SCA用户界面的目标日期。立即激活Cisco XDR，以便您的团队完成下面所述的就绪操作。

立即行动和关键日期

发生了什么情况，我现在应该做什么？

状态	所需操作
详细信息	思科正在淘汰SCA用户体验，并将SCA衍生的功能迁移到Cisco XDR。遥测和分析成为活动、检测、事故、调查、资产情景、响应和自动化的更广泛的XDR工作流程的一部分。
客户操作	激活XDR、连接SCA租户、验证访问、使用XDR检测和事件进行日常操作、使用“活

	动”进行源遥测转换、测试XDR工作流程，并在2026年10月24日之前导出历史信息。
--	--

我应该计划什么日期？

日期	里程碑	这意味着什么
2026年9月15日	针对所选客户的AWS和Azure配置设置	受影响的美国和EMEA客户转向推荐的XDR配置方法。
2026年9月30日	专用的SCA到XDR客户过渡计划结束	在计划结束前完成授权、调配和就绪操作。
2026年10月7日	AWS CloudTrail、Azure Activity Log和GCP审核日志检测被转换	在XDR中操作这些源
2026年10月14日	自定义事件检测切换；XDR中提供的事件调整、监视列表和实体组配置	将相关工作流程和配置移至XDR
2026年10月21日	NetFlow检测被切断	在XDR中运行NetFlow检测
2026年10月24日	SCA用户体验不再可用	在此日期之前完成向XDR的迁移并导出历史数据。

如果无所作为或未调配XDR，会发生什么情况？

状态	不推荐
详细信息	如果您在删除SCA用户体验之前没有激活和连接Cisco XDR，您将失去对SCA的访问权限，并且没有适用于SCA衍生的工作流程、检测、调查、集成或历史数据的替代XDR体验。Waiting还会将激活、用户设置、工作流验证和操作更改压缩到过渡的最后部分。
客户操作	立即激活并连接XDR，以便您的团队能够在2026年9月30日之前完成用户设置、工作流验证和导出准备。SCA接口仍定于2026年10月24日弃用；如果没有连接的XDR租户，在SCA访问结束时无法提供替代XDR体验。

什么即将停用、更改或不可用

哪些SCA概念显然不能以相同形式继续下去？

状态	更改或报废
详细信息	- SCA用户体验：于2026年10月24日移除。 - 传统SCA Webhook行为：替换为XDR工作流程。 - SCA观察体验：不是一对一XDR功能。 - 子网敏感性：被资产价值优先级概念取代。 - 实体组：替换为资产标签、资产组和价值评分。 - 暂停检测设置：未迁移；使用事件调整（如果可用）。 - 客户控制的警报优先级行为：未保留。 - 一些报告、使用率较低的页面和功能：已停用或替换为XDR原生体验。

哪些报告或集成项目预计将被弃用或移动？

状态	预期更改
详细信息	示例包括云状态监视列表、Kubernetes监控、AWS可视化/控制面板/会话搜索/IP搜索体验、Meraki和Umbrella情景集成，以及基于电子邮件的月度报告和每日警报摘要。此列表不保证每个旧版页面都有一对一的替换。

此迁移过程中没有要求我做什么？

状态	没有此类型的操作
详细信息	思科不要求客户重新部署现有网络传感器、重新配置云日志接收仅用于UX迁移、手动重新创建支持的标准检测配置对象或将SCA保留为长期并行控制台。

客户就绪性核对表

- 1. 激活思科XDR并在2026年9月30日之前连接现有的SCA租户，因此您的团队可以在过渡计划关闭之前完成就绪操作。
- 2. 在XDR中创建用户、验证登录和确认适当的访问权限。
- 3. 查看检测、事件、活动、调查和资产见解/设备见解。
- 4. 将每个SCA Webhook、导出、通知、SIEM/SOAR切换和自定义自动化映射到XDR工作流程或其他XDR操作界面。
- 5. 在每个源可用时验证“活动”中所需的源遥测。
- 6. 在每次源切换之前验证所需的检测和响应行动手册。
- 7. 查看子网敏感性、实体组、暂停、警报优先级、监视列表、扫描程序规则、受信任网络和资产价值优先级。
- 8. 资产传统报告、仅SCA页面和API依赖关系；确定替代方案或出口要求。
- 9. 在2026年10月24日之前导出所需的警报、观察、原始日志、配置记录和报告。

在新的XDR体验中寻找自己的方法

SCA客户是否有权使用Cisco XDR？

状态	作为过渡的一部分提供
详细信息	作为过渡的一部分，现有SCA客户有权使用Cisco XDR。当核心工作流程进入XDR时，预期结果为continued SCA value。
客户操作	激活Cisco XDR，连接现有SCA租户，并在需要帮助时使用Cisco XDR激活流程。

我的SCA功能在Cisco XDR中处于什么位置？

SCA函数	XDR目标
警报和警报工作流程	XDR检测和事件
观察和事件导向的调查	XDR活动和XDR调查

事件查看器	XDR调查和活动
设备环境	资产洞察/设备洞察
Webhook、通知、导出和下游传送	XDR工作流程
检测配置	XDR配置体验随着每个设置达到其里程碑

SCA是否仍可作为并行日常控制台使用？

状态	无
详细信息	SCA用户体验计划于2026年10月24日删除。使用重叠时段来实践XDR运营模型、验证工作流并更新操作手册。

检测、事件和观察使用案例

检测是否只是一对一的移动？

状态	模型更改
详细信息	不会。思科正在改进检测内容和操作模式，而不是将每个传统SCA警报都复制为未更改的XDR对象。名称、逻辑、证据、关联和结果可能会发生变化。
客户操作	根据您需要操作的安全场景评估XDR检测结果、证据和事件关联；不要将名称匹配单独用作接受。

是否应该将XDR事件或检测用于我的警报工作流程？

状态	按结果选择
详细信息	使用突发事件进行人工响应、分析师通知、分类、上报、案例管理以及协调响应。将检测用于单个发现、检测级别导出和机器到机器自动化。活动是遥测平面。
客户操作	更新Runbook，以便在适当情况下从突发事件触发人工通知和响应流程；使用检测进行详细分析、导出和查找级别自动化。

基于观察的使用案例是否继续？

状态	不是一对一
详细信息	请勿假定旧观察名称、UI对象或触发器条件将保留。通过活动、检测、事件和更广泛的关联，目标相当于或改善了覆盖范围。
客户操作	在2026年10月24日之前确定并更新Runbook、控制面板和自动化中的依赖项。

如果我主要依赖NetFlow而无法部署EDR，该怎么办？

状态	仍在范围内
详细信息	现有网络传感器和接收功能仍可正常工作，并且无需部署EDR即可继续使用迁移的网络检测。
客户操作	使用XDR检测、发现、事件、事件调整和可用资产情景。如果终端可视性受到高度限制，则请求部署特定指南。

通知、导出、网络挂接和自动化

SCA webhooks会发生什么情况？

状态	迁移和测试
详细信息	XDR自动化工作流程是通知、导出和下游自动化的长期控制点。目标导出路径与OCSF一致，可提供比传统SCA警报和观察模型更完整的情景检测详细信息。
客户操作	如果Webhook将检测信息发送给人员、SIEM、SOAR或其他系统，请在XDR工作流程中重新创建并测试该行为。

检测工作流程与突发事件工作流程有何区别？

状态	使用匹配的触发器
详细信息	使用面向检测的工作流程进行数据移动、导出和机器消耗。使用面向事件的工作流程进行更广泛的操作活动和人工通知，例如电子邮件、Slack或Webex。两者都可以支持出口。

SIEM、SOAR或自定义下游集成有哪些变化？

状态	需要审核
详细信息	请勿假设特定于SCA的Webhook、负载、警报名称或导出将保持不变。目标导出路径与OCSF一致，可提供更完整的情景检测详细信息。
客户操作	将依赖项迁移到XDR工作流和XDR数据模型，然后测试下游接收和运行手册行为。

是否需要更改NVM通知和导出？

状态	NVM转换已完成
详细信息	NVM检测在2026年5月移至XDR。依赖传统NVM Webhook模式的客户需要在2026年5月15日转换之前移动通知并导出到XDR工作流程。
客户操作	继续使用和验证NVM的XDR工作流模式。

在源转换之前应该测试什么？

状态	所需的就绪性检查
客户操作	对于每个源，测试检测或事件触发器、通知或导出负载、下游接收、过滤或路由规则以及更新的Runbook响应。在源设备离开SCA体验之前进行测试。

遥测源和逐源转换

XDR活动何时提供遥感勘测？

日期	遥测里程碑	客户操作
----	-------	------

2026年8月19日	活动中的ONA数据遥测	开始检查ONA遥感勘测。
2026年8月26日	活动中的CTB数据遥测	开始审查CTB遥感勘测。
2026年9月16日	活动中的AWS VPC流日志、Azure流日志和GCP VPC流日志	开始审核云流遥感勘测。
2026年9月23日	XDR中的AWS源配置	如果适用，请使用XDR配置体验。
2026年9月30日	活动中的AWS CloudTrail、Azure活动日志和GCP审核日志	开始审核审核审核日志遥测。

是否需要重新部署网络传感器或重新配置云日志接收？

状态	不，不仅仅适用于UX迁移
详细信息	现有网络传感器和云日志接收在此阶段保持正常运行，无需重新部署或重新配置，仅因为用户体验和检测将迁移到XDR。
重要例外	传感器和集成使用的公有IP地址或终端可能会发生变化。审查防火墙规则、代理许可列表和其他网络控制；在需要更改配置之前，思科将提供所需的XDR终端详细信息。

源检测何时切断？

状态	源特定计划
详细信息	在转换时，该源的遥测和检测不再通过SCA用户体验使用。 • 2026年10月7日：AWS CloudTrail、Azure活动日志和GCP审核日志检测。 • 2026年10月14日自定义事件检测。 • 2026年10月21日：NetFlow检测。

设置、调整、监视列表和资产情景

我的检测配置是否会被迁移？

状态	分阶段迁移
详细信息	支持的标准配置对象预计会在更广泛的检测引擎过渡过程中进行迁移。NVM检测设置在2026年5月移至XDR;其他设置在其功能可用时进行转换。
客户操作	除非思科针对您的部署发布特定说明，否则不要仅为迁移手动重新创建标准设置。

下列哪项可取代子网敏感度、实体组和暂停？

状态	概念更改
详细信息	• 子网敏感性：由Asset Insights/Device Insights中的设备价值优先级评分取代；在2026年9月30日之前安排在XDR设备见解中。

	• 实体组：在2026年10月14日XDR设备见解中安排的配置；现有组将迁移到标签，资产标签和价值评分用于划分优先级。 • 暂停：暂停设置未迁移；事件调整计划于2026年10月14日推出。
--	--

监视列表何时移动？

状态	定于2026年10月14日
详细信息	监视列表配置计划于2026年10月14日在XDR中提供。将迁移现有的监视列表，但保留逻辑后，术语和规则表示可能会发生变化。
客户操作	在过渡期间验证与监视列表相关的规则、抑制和工作流。

是否仍可以像在SCA中那样设置警报优先级？

状态	无
详细信息	警报优先级使用思科威胁研究进行硬设置，不是客户管理的误报抑制控制。

传感器、云集成和运行状况

FTD、ISE、AWS、Azure或GCP集成是否保持不变？

状态	验证业务关键路径
详细信息	不要假定每个集成都保留相同的UI、工作流程或配置方法。GCP配置已经在XDR中；AWS和Azure将紧随其后；与传感器相关的内部部署迁移项目将在10月份迁移。
客户操作	根据特定于产品的指南验证FTD、ISE隔离、丰富、与SAL连接的工作流程和其他关键业务集成。

我可以用同样的方法监控传感器的运行状况、活性、流量传输和容量吗？

状态	就绪性审核
详细信息	思科在过渡期间会维护传感器和采集操作，但并非每个SCA监控页面或工作流程都承诺进行一对一迁移。
客户操作	清点您所依赖的运行状况、协议、流量和交付检查，并验证其XDR操作路径。

ONA或CTB映像的分布、目标URL、服务密钥或公共IP地址是否会更改？

状态	检查网络依赖关系
详细信息	在此阶段，思科不要求重新部署传感器，但遥测目标可能会随着源过渡到XDR而更改。
客户操作	在相关源转换之前，检查防火墙规则、代理允许列表、目标URL和服务密钥依赖关系。请勿在未发布迁移说明的情况下进行预防性传感器更改。

历史数据、报告和管理

当SCA用户体验关闭时，历史SCA数据会发生什么情况？

状态	2026年10月24日之前出口
详细信息	用户体验删除后，通过SCA界面访问历史数据即告结束。在检测迁移路径之前和通过检测迁移路径将原始遥感勘测数据输入到XDR中，但SCA不是用于历史检索的长期位置。 - 警报和观察可以从SCA控制台导出为CSV。 - 如果需要，可将原始日志（包括网络流量和云日志）导出为CSV。 - 在导出之前，定义审核、调查分析和保留证据要求。

是否所有SCA报告功能都将转移到XDR？

状态	某些设备已停用或已更换
详细信息	一些报告功能、使用率较低的页面和旧功能预计会停用，或由XDR本机检测、调查、活动和资产洞察体验取代。
客户操作	立即清点运营所需的报告并确定XDR体验、导出或更换工作流程。

如何证明迁移完整性？

状态	定义证明工件
客户操作	定义所需的记录和证据，在2026年10月24日之前导出所需的SCA历史记录，并验证每个所需来源的XDR可视性。此过渡不是客户管理的批量重新导入到单独的系统中。

存储在SCA端的管理员信息会发生什么情况？

状态	在停用前提供文档
详细信息	请勿假设SCA中存储的客户可见的配置、管理信息或历史记录在2026年10月24日后仍然可用。
客户操作	导出或记录管理、审计或历史参考所需的任何内容，并使用XDR作为目标操作界面。

API和自定义集成

什么可以取代获取观察API、SCA设备API或其他SCA特定API？

状态	库存相关项
详细信息	思科尚未针对每个SCA API发布最终的一对一API替换矩阵。围绕活动、检测、事故、工作流程、资产见解/设备见解和XDR调查制定计划。
客户操作	现在库存直接相关项，且假设在2026年10月24日之后传统终端名称仍然可用。

传统的事件创建方法和自定义自动化会发生什么情况？

状态	视为过渡性
详细信息	FAQ没有为每个旧事故创建方法或API确定承诺的公共弃用日期。目标方向是XDR自定义安全事件和检测、XDR模型中的事件生成以及用于结果管理的事件调整。
客户操作	将每个使用SCA观察、警报名称、设备、网络挂接、导出或报告的自动化映射到XDR工作流程、检测、突发事件、活动或资产见解使用案例。在相关源转换之前测试端到端行为。

已完成的过渡项目

NVM检测迁移

状态	◆◆成
分辨率	NVM检测和相关检测设置在2026年5月移至XDR。依赖传统NVM通知和导出的客户应使用XDR工作流程并验证工作流模式。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。