自定义工作流程

以下主题介绍如何使用自定义工作流程：

自定义工作流程简介

如果预定义工作流程和思科提供的自定义工作流无法满足需求，则可以创建并管理自定义工作流程。

自定义工作流程是为满足贵组织的特有需求而创建的工作流程。创建自定义工作流程时，请选择工作流程所基于的事件（或数据库表）类型。在 防火墙管理中心中，可以将自定义工作流程基于自定义表。还可以选择自定义工作流程包含的页面；自定义工作流程可以包含向下展开页面、表视图页面和主机页面或数据包视图页面。

如果事件评估过程更改，则可以编辑自定义工作流程来满足新的需求。请注意，不能编辑任何预定义工作流程。

提示 可以将自定义工作流程设置为任何事件类型的默认工作流程。

已保存的自定义工作流程

除无法修改的预定义工作流程以外，防火墙管理中心还包含若干已保存的自定义工作流程。其中每个工作流程基于自定义表，并且可以修改。

在多域部署中，这些已保存的工作流程属于全球域，并且不能在较低的域中进行修改。

表 *1:* 已保存的自定义工作流程

工作流程名称	说明
按照优先级和分类显示事件	此工作流程按事件优先级列出事件及其类型，随之还列出一个表明每个事件已发生的次数的计数。 此工作流程基于 Intrusion Events 自定义表。
具有服务器的主机默认工作流程	可以使用此工作流程快速查看“具有服务器的主机”自定义表中的基本信息。 此工作流程基于 Hosts with Servers 自定义表。
服务器和主机详细信息	可以使用此工作流程确定哪些服务器在网络上使用最频繁以及哪些主机在运行这些服务器。 此工作流程基于 Hosts with Servers 自定义表。

自定义工作流程的创建

如果预定义工作流程和思科提供的自定义工作流程无法满足需求，则您可以创建自定义工作流程。

提示 可以从其他设备导出自定义工作流程，然后将其导入到设备上，而不是创建新的自定义工作流程。然后，可以编辑导入的工作流程来满足需求。

创建自定义工作流程时，请执行以下操作：

- 选择要作为工作流程源的表
- 提供工作流程名称
- 向工作流程中添加向下钻取页面和表视图页面

对于工作流程中的各向下钻取页面，可以：

- 提供显示在 Web 界面中页面顶部的名称
- 每页包含最多五列
- 指定默认排序顺序（升序或降序）

可以在一系列工作流程页面的任何位置添加表视图页面。它们不具有任何可编辑属性，如页面名称、排序顺序或用户可定义的列位置。

注释 必须向自定义工作流程中添加至少一个向下钻取页面或事件表视图。

注释 如果您选择**漏洞 (Vulnerabilities)** 作为表类型，然后添加 **IP 地址 (IP Address)** 作为表列，则除非使用搜索功能限制工作流程以查看特定 IP 地址或地址块，否则在使用自定义工作流程查看漏洞时不会显示 IP 地址列。

自定义工作流程的最终页面取决于工作流程所基于的表，如下表所述。创建工作流程时，系统会默认添加这些最终页面。

表 *2:* 自定义工作流程最终页面

事件/资产类型	最终页面
发现事件	主机数
漏洞	漏洞详细信息
第三方漏洞	主机数
用户	用户
危害表现	主机或用户
入侵事件	数据包

系统不是根据其他种类的事件（例如，审核日志或恶意软件事件）向自定义工作流程中添加最终页面。

基于连接数据的自定义工作流程与其他自定义工作流程类似，不同之处在于其中可包括具备连接摘要数据的向下钻取页面、连接数据图形页面、具备单独连接数据的向下钻取页面和表视图页面。

根据非连接数据创建自定义工作流程

您必须具有管理员或安全分析师权限，才能根据非连接数据创建自定义工作流程。

过程

步骤 1 选择**分析** > **高级** > **自定义工作流程**。

步骤 2 点击**创建自定义工作流程 (Create Custom Workflow)**。

步骤 3 在**名称 (Name)** 字段中输入工作流程的名称。

步骤 4 输入**说明 (Description)**（可选）。

步骤 5 从**表 (Table)** 下拉列表中选择要包含的表。

步骤 6 如果要向工作流程中添加一个或多个向下展开页面，请点击**添加页面 (Add Page)**。

步骤 7 在**页面名称 (Page Name)** 字段中输入页面的名称。

步骤 8 在“列 1”(Column 1) 下，选择排序优先级和表列。此列将显示在页面最左侧的列中。

示例：

例如，要创建显示所针对的目标端口的页面，并要按计数对页面进行排序，请从**排序优先级**下拉列表中选择 **2**，并从**字段** 下拉列表中选择**目标端口/ICMP 代码**。

步骤 9 继续选择要包含的字段并设置其排序优先级，直至指定要在页面上显示的所有字段。

步骤 10 如果要向工作流程中添加表视图页面，请点击**添加表视图**。

步骤 11 点击**保存**。

创建自定义连接数据工作流程

基于连接数据的自定义工作流程与其他自定义工作流程类似，不同在于可以包含连接数据图形页面以及向下展开页面和表视图页面。可以按任意顺序在工作流程中包含尽可能多的各类型的页面。每个连接数据图形页面包含单个图形，可以是曲线图、条形图或饼形图。在曲线图和条形图中，可以包含多个数据集。

您必须具有管理员权限，才能根据连接数据创建自定义工作流程。

过程

步骤 1 选择**分析** > **高级** > **自定义工作流程**。

步骤 2 点击**创建自定义工作流程 (Create Custom Workflow)**。

步骤 3 在**名称 (Name)** 字段中输入工作流程的名称。

步骤 4 输入**说明 (Description)**（可选）。

步骤 5 从**表 (Table)** 下拉列表中，选择**连接事件 (Connection Events)**。

步骤 6 如果要向工作流程中添加一个或多个向下钻取页面，您有两个选择：

- 点击**添加页面 (Add Page)** 以添加包含有关个别连接的数据的向下钻取页面。
- 点击**添加摘要页面 (Add Summary Page)** 以添加包含连接摘要数据的向下钻取页面。

步骤 7 在**页面名称 (Page Name)** 字段中输入页面的名称。

步骤 8 在**列 1 (Column 1)** 下，选择排序优先级和表列。此列将显示在页面最左侧的列中。

步骤 9 继续选择要包含的字段并设置其排序优先级，直至指定要在页面上显示的所有字段。

示例：

例如，要创建显示通过受监控网络传输的流量的页面，并要按传输最多流量的响应方对页面进行排序，请从**排序优先级 (Sort Priority)** 下拉列表中选择 **1**，并从**字段 (Field)** 下拉列表中选择**响应方字节数 (Responder Bytes)**。

步骤 10 如果要向工作流程中添加一个或多个图形页面，请点击**添加图形 (Add Graph)**。

步骤 11 在**图形名称 (Graph Name)** 字段中输入页面的名称。

步骤 12 选择要包含在页面上的图形的类型：

- 曲线图 (**折线图**（  ）)
- 条形图 (**条形图**（  ）)
- 饼形图 (**饼图** （  ）)

步骤 13 通过选择图形的 x 轴和 y 轴指定要图形化的数据种类。

在饼图中，x 轴表示独立变量，y 轴表示因变量。

步骤 14 选择要包含在图形中的数据集。

请注意，饼形图只能包含一个数据集。

步骤 15 如果要添加连接数据的表视图，请点击**添加表视图 (Add Table View)**。

表视图不可配置。

步骤 16 点击**保存**。

自定义工作流程使用和管理

用于查看工作流程的方法取决于工作流程是基于其中一个预定义事件表还是基于自定义表。

如果自定义工作流程基于预定义事件表，请以与访问设备随附的工作流程相同的方式对其进行访问。例如，要根据“主机”表访问自定义工作流程，请选择**分析** > **主机标题为** > **主机**。另一方面，如果自定义工作流程基于自定义表，则必须从 Custom Tables 页面对其进行访问。

如果事件评估过程更改，则可以编辑自定义工作流程来满足新的需求。请注意，不能编辑任何预定义工作流程。

提示 可以将自定义工作流程设置为任何事件类型的默认工作流程。

根据预定义表查看自定义工作流程

您必须具有管理员、维护或安全分析师权限才能查看自定义工作流程。

过程

步骤 1 为自定义工作流程所基于的表选择适当的菜单路径和选项，如工作流程选择中所述。

步骤 2 要使用其他工作流程，包括自定义工作流程，请点击当前工作流程标题旁边的**切换工作流程 (switch workflow)**。

步骤 3 如果未显示事件并且可按时间限制工作流程，则可能需要调整时间范围；请参阅事件时间限制。

根据自定义表查看自定义工作流程

您必须具有管理员或安全分析师权限，才能查看基于自定义表的自定义工作流程。

在多域部署中，系统会显示在当前域中创建的自定义工作流程，您可以对其进行编辑。系统还会显示在祖先域中创建的自定义工作流程，您不可以对其进行编辑。要查看和编辑较低域中的自定义工作流程，请切换至该域。

过程

步骤 1 选择**分析** > **高级** > **自定义表**。

步骤 2 点击要查看的自定义表旁边的 **视图** ( ) ，或者点击自定义表的名称。

步骤 3 要使用其他工作流程，包括自定义工作流程，请点击当前工作流程标题旁边的 **(switch workflow)**。

步骤 4 如果未显示事件并且可按时间限制工作流程，则可能需要调整时间范围；请参阅事件时间限制。

编辑自定义工作流程

您必须具有管理员或安全分析师权限才能编辑自定义工作流程。

在多域部署中，系统会显示在当前域中创建的自定义工作流程，您可以对其进行编辑。系统还会显示在祖先域中创建的自定义工作流程，您不可以对其进行编辑。要查看和编辑较低域中的自定义工作流程，请切换至该域。

过程

步骤 1 选择**分析** > **高级** > **自定义工作流程**。

步骤 2 点击要编辑的工作流程名称旁边的 **编辑** ( ) 。

如果显示**视图** ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 对工作流程进行所需的任何更改。

步骤 4 点击**保存**。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。