# Stealthwatch 6.8（第 1.1 版）— 猎捕邪恶！

最后更新日期：2017 年 2 月 13 日

## 关于此演示

“Stealthwatch 6.8（第 1.1 版）猎捕邪恶！”演示指南包括以下内容：

# 关于此解决方案

思科 StealthWatch 通过收集并分析网络数据，为您的网络提供全面的可视性和保护，即使是规模最大、变动最频繁的网络，也尽在其掌握之中。Stealthwatch 分析来自思科和其他供应商的路由器、交换机、防火墙和其他网络设备的行业标准 NetFlow 数据，以检测高级长期安全威胁，如内部传播的恶意软件、数据泄露、僵尸网络命令和控制流量和网络侦察。

作为对抗隐秘、复杂网络攻击的关键组成部分，Stealthwatch 通过分析网络内部（局域网和边界）的流量模式提供行为见解。思科身份服务引擎 (ISE) 解决方案使用情景信息（如用户身份、用户权限级别、设备类型和状态）补充 Stealthwatch 基于 NetFlow 的威胁行为检测数据。同时，StealthWatch 和思科 ISE 可为网络安全分析师提供一个集成用户、设备信息和网络流量数据的建议，使安全分析师能够以及时、高效且具成本效益的方式检测和辩明潜在威胁的严重程度。

此演示旨在让您熟悉思科 Stealthwatch 解决方案的用法。您将在模拟的企业环境中与先前配置和部署的解决方案进行交互。

Stealthwatch 包括若干核心和可选组成部分。核心组成部分包括：

- StealthWatch 管理控制台
- 流量收集器

系统可选组成部分可让您更灵活地部署和查看网络的各区域，它包括以下内容：

- 流量传感器
- UDP Director
- 云授权
- 代理授权
- 威胁源授权

**图 1.** 统一视图


本演示包含 13 个不同场景。

场景 1 至 6 包括 Stealthwatch 产品、Web 接口以及 Swing 客户端界面：

- 网络客户端 (WebUI) 可视为整体网络安全状态/视图的快照，以便您深入挖掘围绕事件的上下文。
- 高级运行控制台（Swing 客户端）是一种完全可定制的控制台 UI，可用于产品安装和设置、高级调查、深度分析和数据可视化。

此外，这些场景向您介绍 Stealthwatch 如何处理主机和策略以进行分析。

场景 7 至 13 涵盖围绕 Stealthwatch 系统用户在使用该软件时可能遇到的使用案例而展开的一系列活动。您将会调查在模拟网络环境中发生的警报和事件。

在每个场景结束时，将呈现与此活动相关的问题。请花点时间，根据您所学的知识回答这些问题。在会话结束时，将会复习这些问题。

# 要求

**表 1.** 要求

| 必备 | 可选 |
| --- | --- |
| • 一台装有远程桌面客户端的计算机<br>• 连接到 dCloud 环境 | • 不适用 |

注意：Stealthwatch Swing 客户端是一款 Java 应用程序。此客户端不在网络浏览器中运行，因此，不会存在“在网络浏览器中启用 Java”的安全问题。

# 拓扑

**图 2.** 拓扑

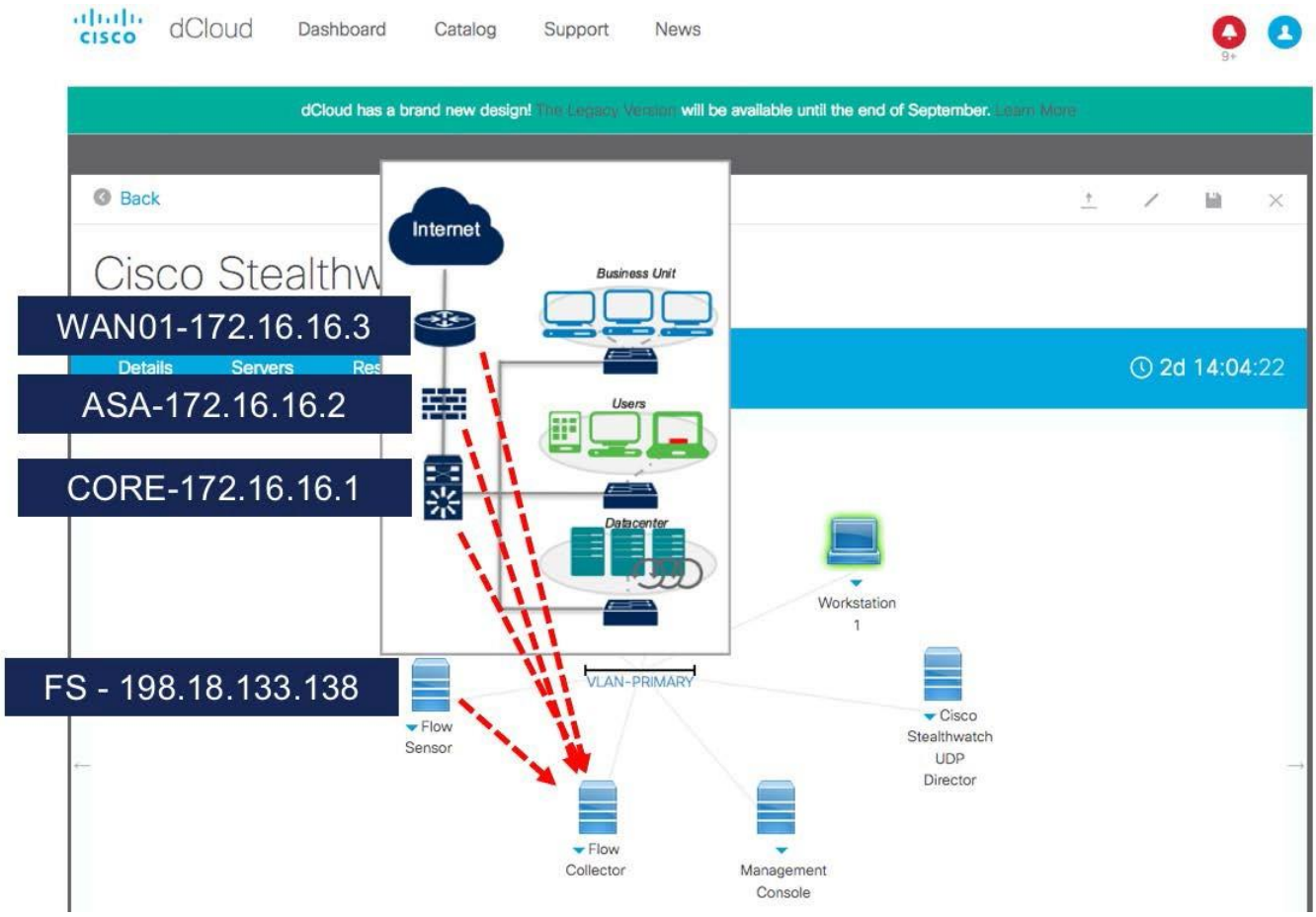



**表 2.** 设备详细信息

| 设备 | 功能 | 必备或可选 |
|---|---|---|
| 管理控制台 | Stealthwatch 解决方案的中央管理控制台 | 必备 |
| 流量收集器 | 收集流量（NetFlow 和 IPFIX 以及其他供应商流量协议），处理数据并将其存储于板载数据库中。 | 必备 |
| 流量传感器 | 基于已连接网络流量的数据包捕获创建流量。通过 SPAN 端口或网络分流器连接至网络。 | 可选 |
| UDP Director | UDP 管理中继器。根据需要，UDP Director 还用于通过中继数据至多个流量收集器实现高可用性。 | 可选 |
| 流量生成器 | 在 dCloud 环境中使用的模拟 NetFlow 数据 | |

# 入门指南

**演示前**

Cisco dCloud 强烈建议您先用活动会话执行本文档中的任务，然后再给现场观众演示。这样您将熟悉文档和内容的结构。

遵循本指南后，有必要安排一个新会话，以将环境重置为其原始配置。

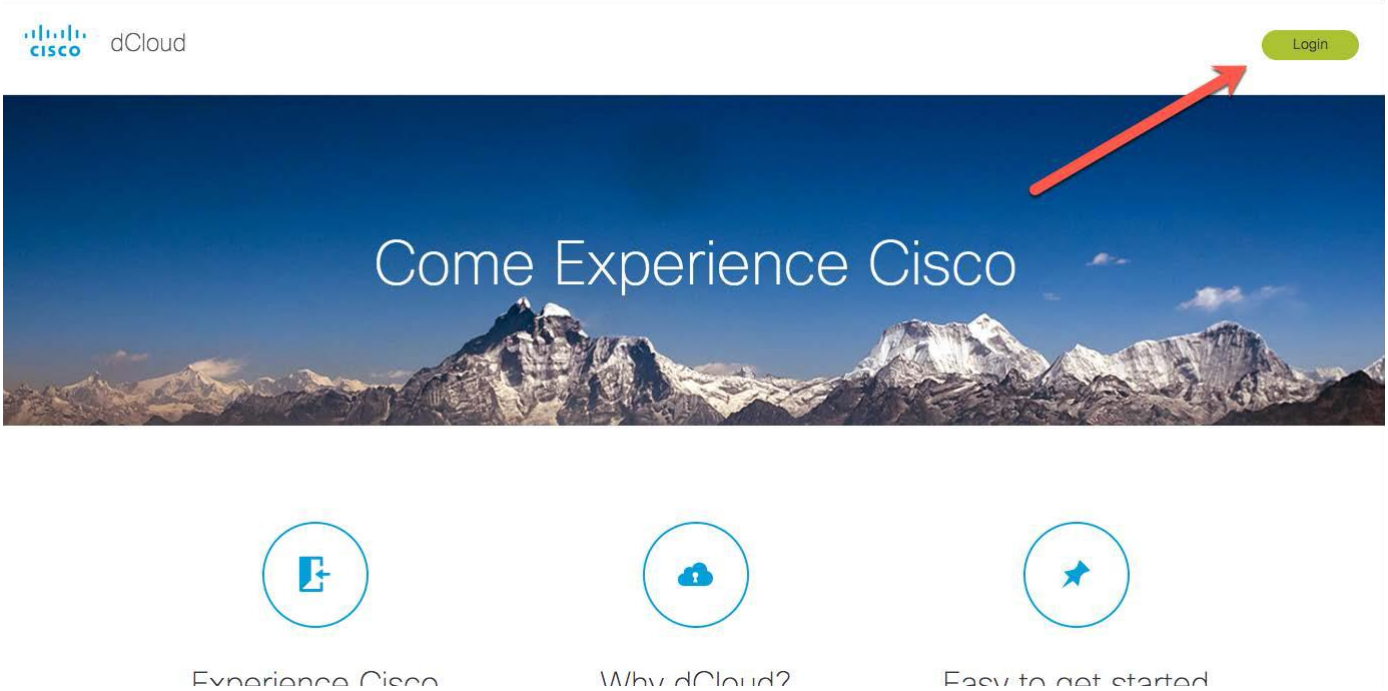
**细致的准备对于一场成功的演示至关重要。**

每位学生均有一个专用的远程访问工作站，可用于执行场景。

使用网络浏览器输入 URL：

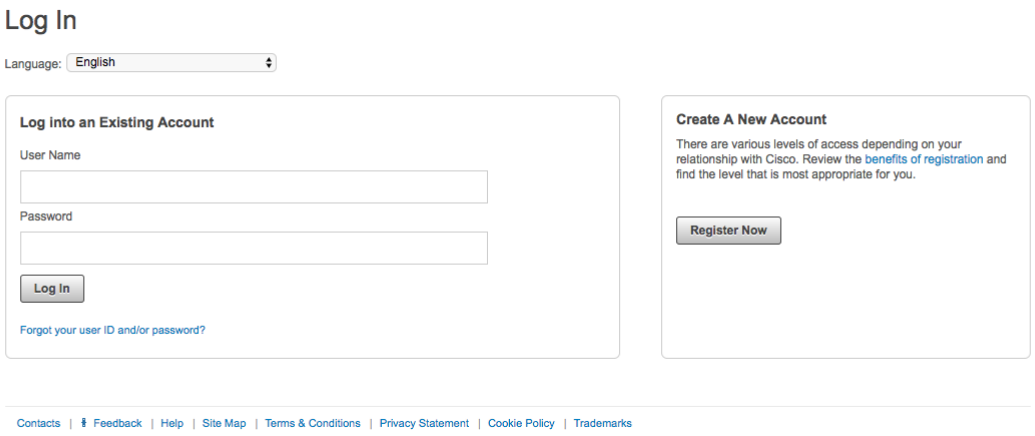
https://dcloud.cisco.com/

**图 3.** dCloud 登录



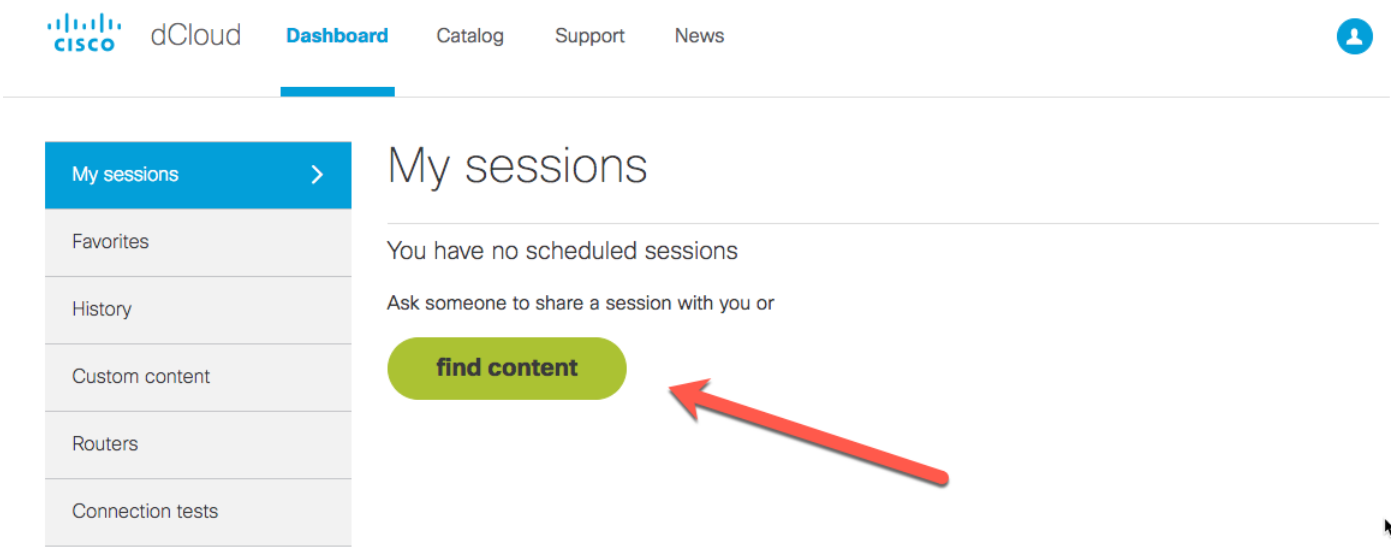

如果您尚未登录，请输入您的 CEC 凭证，然后点击登录。

**图 4.** CEC 登录屏幕



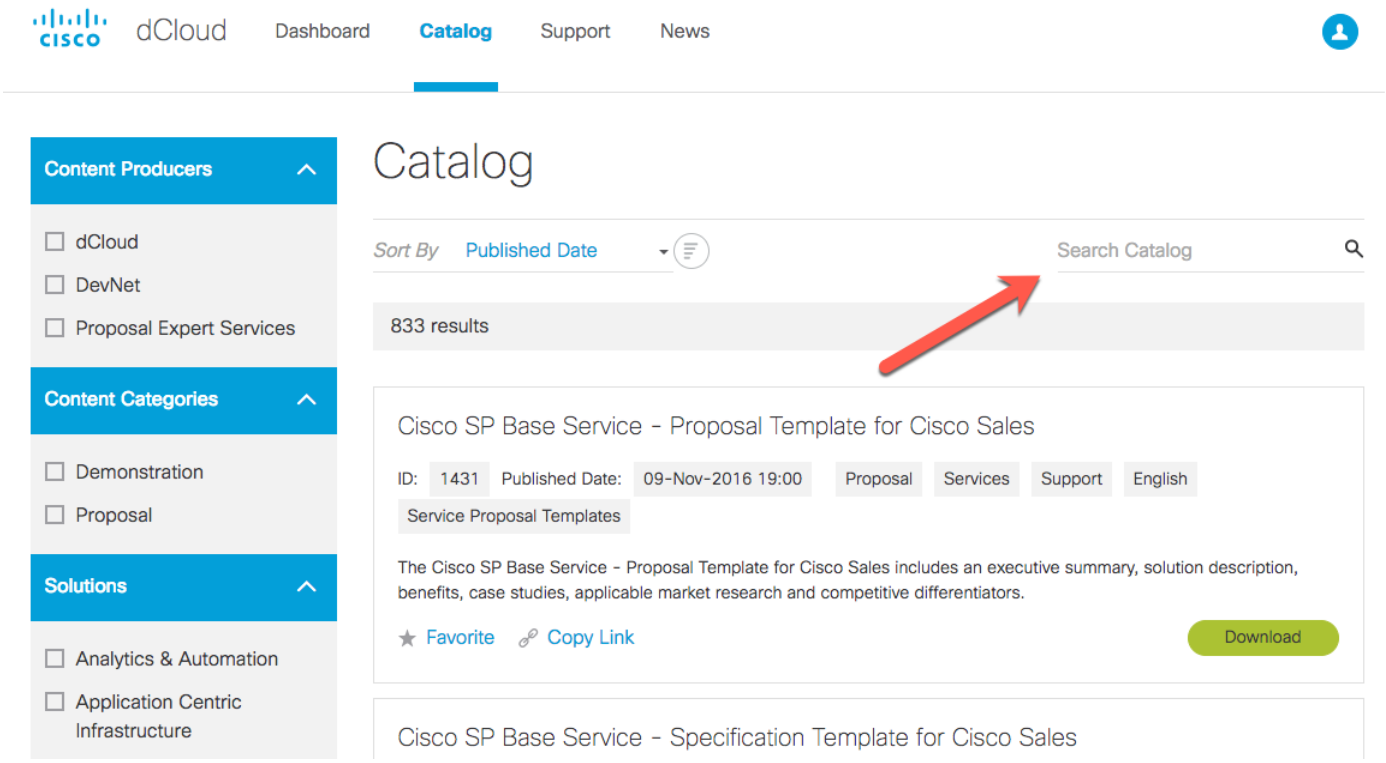

以下屏幕将会打开：

**图 5.** dCloud 我的会话 - 查找内容



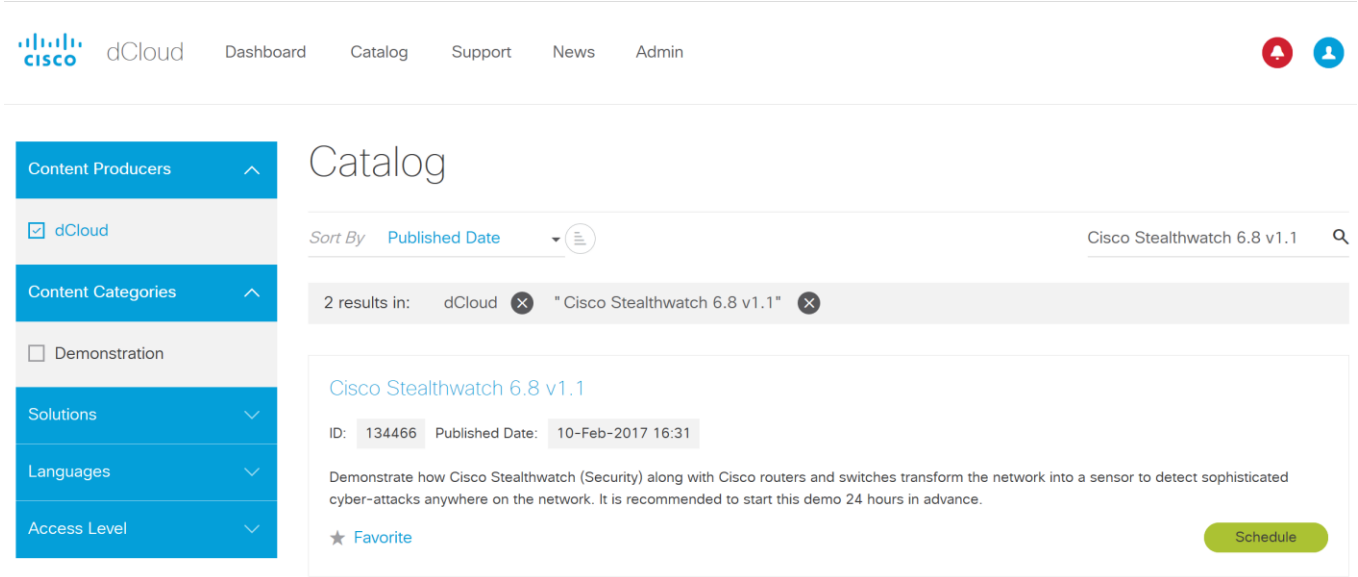

点击**查找内容 (find content)** 按钮，启动该屏幕：

**图 6.** dCloud 搜索目录




在**搜索目录 (Search Catalog)** 框中输入“思科 Stealthwatch 6.8”，系统随即显示以下屏幕：

**图 7.** dCloud 搜索思科 Stealthwatch 6.8（第 2 版）



在 dCloud 中安排您的会话。

要连接到您的 dCloud 会话，使用您的 CCO ID 登录到 dCloud，然后依次选择**控制面板 (Dashboard) > 我的会话 (My sessions)** 查看安排的会话。选择**详细信息 (Details)**，并向下滚动查看您的会话详细信息。现在使用此信息，建立一个 **AnyConnect** 连接，一旦连接上，使用本地计算机上的 **RDP 客户端**连接到 **WKST1** 计算机 (**198.18.133.36**)。

您现已成功连接到用于执行场景的工作站。

# 帐户和密码

下表包含您的会话中预配置用户的可用详细信息。

**表 3.** 用户详细信息

| 用户名 | 密码 | 终端设备 | IP 地址 |
|---|---|---|---|
| wkst1\管理员 | C1sco12345 | 工作站 1 | 198.18.133.36 |
| admin | C1sco12345 | 管理控制台 | 198.18.133.136 |
| admin | C1sco12345 | 流量收集器 | 198.18.133.137 |
| admin | C1sco12345 | 流量传感器 | 198.18.133.138 |
| admin | C1sco12345 | UDP Director | 198.18.133.139 |

# 场景 1　　WebUI

## 场景描述

既然您已连接到该环境，下一步是访问 Stealthwatch 管理控制台 (SMC) 的接口。

## 场景目标

了解 Stealthwatch WebUI 控制面板中的布局和可用工具。

## 步骤

1. 使用您的网络浏览器，通过 HTTPS 连接到 Stealthwatch 管理控制台 (SMC)。
    - IP 地址：198.18.133.136
    - 用户名：admin，密码：C1sco12345
2. 如果系统显示“证书错误”页面，请忽略并继续进入网站。
3. 使用本文档开头所列的凭证登录到您的 Stealthwatch 管理控制台。
4. 当您登录后，系统将显示 SMC 的 WebUI 控制面板。注意前面和中间提供的以下有关网络环境的信息：

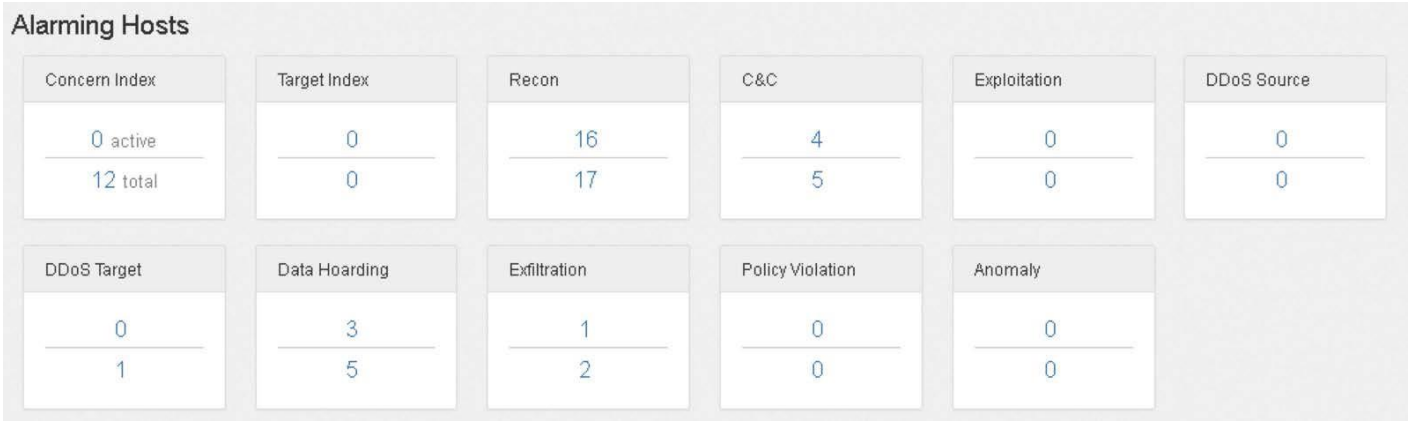



**图 9.**　警报主机

5. 在顶部，**报警主机 (Alarming Hosts)** 显示当前有效警报（当前正在发生的事件）数量，以及特定日期出现的**总**警报数量。

点击数字，将显示相关警报类型的详细信息：

a) **关注指数 (Concern Index)** — 可能是恶意软件的异常行为的汇总信息。

b) **数据收集 (Data Hoarding)** — 观测到的、在内部移动大量数据的用户/主机

c) **外泄 (Exfiltration)** — 将数据发送到网络外部的用户/主机

d) 围绕针对性攻击进行的**侦察**和**漏洞攻击**

e) **命令和控制 (C&C)** — 在网络中检测到的僵尸网络通信活动

f) **DDoS 源（DDoS Source）** — 内部主机可能涉及 DDoS 活动的警报

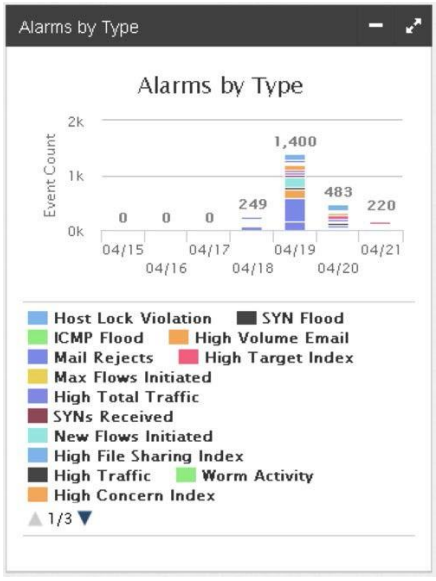
g) **DDoS 目标 (DDoS Target)** — 内部主机可能被 DDoS 活动利用的警报

h) **策略违规 (Policy Violation)** — 由 Stealthwatch 系统管理员定义的策略和自定义事件触发的警报

i) **异常 (Anomaly)** — 其他检测到的异常行为。

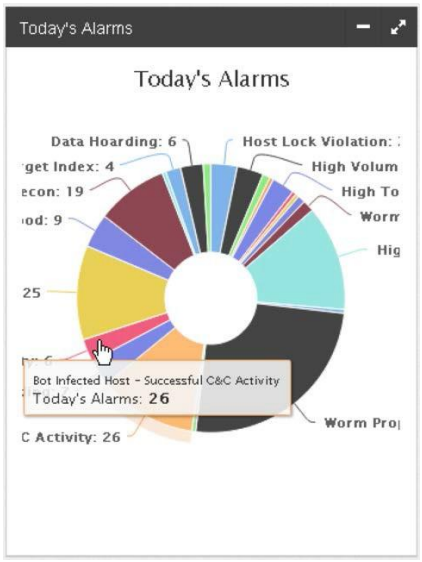
6. **按类型分类警报 (Alarms by Type)：**描述过去一周的警报趋势的条形图（按照天和警报类型分类）。您可以点击显示的各种日条形图中任意报警类型，查看该日相关的警报详细信息。您可以点击框右上角的箭头，将图表布满整个屏幕，以便于阅读。

**图 10.** 按类型分类警报



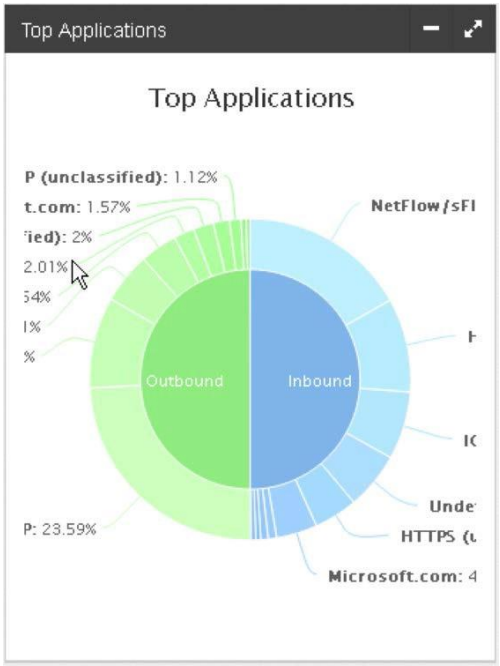
7. **当天警报 (Today's Alarms)：**此饼形图提供当天已经发生的所有警报概览。您可以点击图表中的任意警报类型，查看当天相关警报的详情。您可以点击框右上角的箭头，将图表布满整个屏幕，以便于阅读。

**图 11.** 当天警报



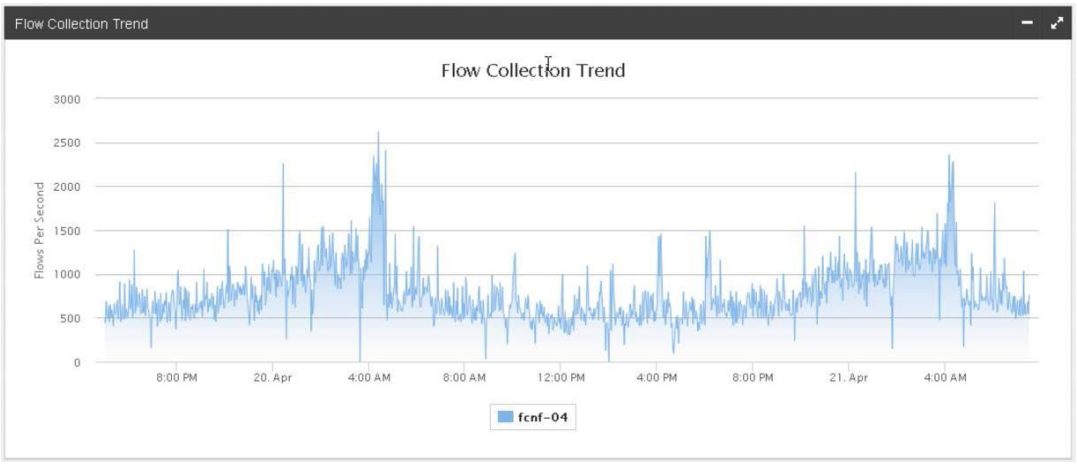

8. **热门应用（Top Applications）：**此饼形图显示在您的网络中检测的热门应用传入和传出流量类型。

**图 12.** 热门应用




9. **流量收集趋势 (Flow Collection Trend）：**此图表显示收集的 NetFlow 活动在过去 48 小时内的起伏。

**图 13.** 流收集趋势




10. WebUI 左侧有多种选项可供您深入了解企业的其他信息。点击各项旁边的 [+]，会出现一个下拉列表，显示可供选择的选项。

    1) **监控 (Monitor)** 下方的内容：

        i. **主机 (Host）** — 此视图显示您的网络中所有观察到的主机以及相关的警报。

        ii. **用户 (User)** — 此视图显示您的网络中所有观察到的主机以及相关的警报。

    2) **分析 (Analyze）**下方的内容：

        i. **流量查询 (Flow Query)** — 弹出分析屏幕，以便您通过Stealthwatch 收集的 NetFlow 数据库构建和执行查询。

        ii. **已保存的查询 (Saved Queries)** — 已保存的流量搜索列表，可由 StealthWatch 用户定义，用以快速查询常搜索的参数。

        iii. **已保存的结果 (Saved Results)** — 当您通过流量搜索接口完成查询时，系统可将其保存并显示在此屏幕上。

        iv. **主机搜索 (Host Search)** — 弹出主机搜索屏幕，以便您快速查询有关观测到的主机的信息，其中包括在网络上首次和最后一次观测到该主机的时间、其参与的数据传输量和其他信息，如与其通信最多的对等设备。

        v. **版权侵犯 (Copyright Infringement)** — 弹出一个控制板，以便用户快速调查网络上可能已经发生的已报告版权侵犯事件。

    3) **工作 (Jobs)** 下方的内容（如果您不是使用管理员帐户登录，则此处可能不会显示全部选项）：

        i. **工作管理 (Job Management)** — 在 SMC 上执行的已保存和正在进行的流量查询列表。

    4) 在**配置 (Configure)** 下方的内容：

        i. **网络分类 (Network Classification)** — 该选项定位参与扫描活动但不在扫描仪主机组中或未采用扫描仪策略的主机。

ii. **应用 (Applications)** — 借助该项，Stealthwatch 管理员可以根据在网络中所观察到的属性配置自定义应用定义。

iii. **自定义安全事件 (Custom Security Events)** — 弹出“自定义安全事件”屏幕，以便您根据用户定义的标准，定义将以报警形式出现的自定义警报。

iv. **外部查找配置 (External Lookup Configuration)** — 配置 Stealthwatch 外部查找功能，借助该功能，它可以查询外部设备和服务，以获得围绕相关主机的其他上下文。

5) **部署 (Deploy)** 下方的内容(除非您使用的是管理员帐户，否则您不会看到这些选项)：

i. **思科® ISE 配置 (Cisco® ISE Configuration)** — 您可以通过该选项为思科 ISE 集群输入配置信息，这样 Stealthwatch 能够获取用户和设备信息，并将该上下文添加到观察到的网络事件中。

ii. **Active Directory** — 您可以通过该选项配置 Stealthwatch，与您的 Active Directory 服务器通信，这样 Stealthwatch 能够获取用户信息，并将该上下文添加观察到的网络事件中。

11. 您可以随时查看 WebUI 控制面板的功能。我们将在接下来的场景中，探讨该面板的许多功能。
12. 完成后，点击左侧的**控制面板 (Dashboard)** 返回到 **控制面板 (Dashboard)** 主页。

## 问题

1. 用户查看哪些主机牵涉到数据泄露活动的两种方式是什么？
2. “报警主机”(Alarming Hosts) 下方各分类的顶部和底部数字间的差是多少？

# 场景 2　　Swing 客户端

## 场景描述

StealthWatch 管理控制台 (SMC) 提供贵组织整个安全基础设施的完整图形视图。从具备 NetFlow、ISE 和 NBAR 功能的路由器收集的所有信息会合并到一个视图中。

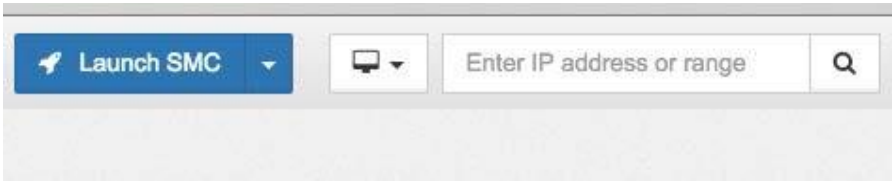
## 场景目标

了解 Stealthwatch Swing 客户端的布局和即时可用的工具。

## 步骤

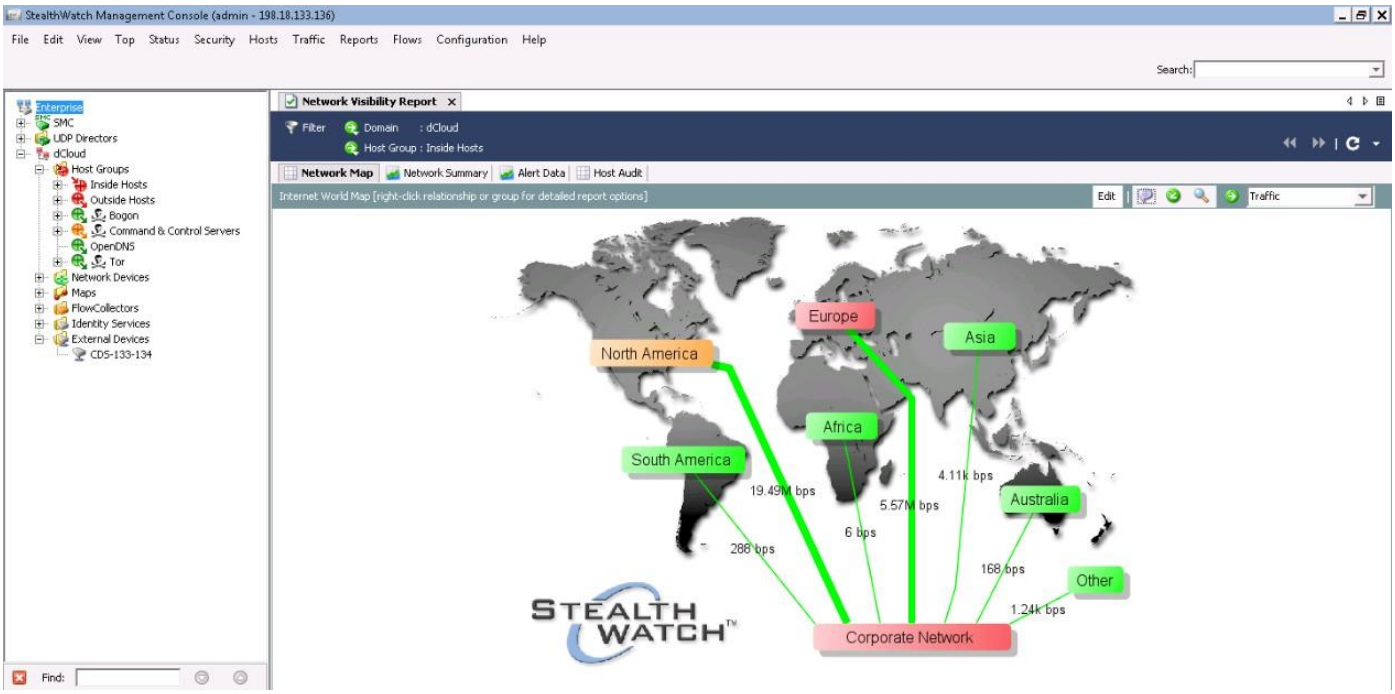
1. 从您的工作站，点击 WebUI 上的**启动 SMC (Launch SMC)** 按钮，启动 **Stealthwatch 管理控制台** Swing 客户端。

**图 14.** 启动 SMC




2. 接受任何安全警报并继续。忽略和/或取消所有浏览器或 Java 更新请求。
3. 当系统显示提示时，请用 **admin/C1sco12345** 登录。
4. 当您成功通过身份验证后，您将登录到 StealthWatch Swing 客户端中。

**图 15.** Stealthwatch Swing 客户端




5. Swing 客户端接口的左侧导航窗格中的项目列表通常称为**企业树** (**Enterprise Tree**)。该树显示监控网络的结构。

    a. 点击“企业树”(Enterprise Tree) 中的加减符号即可了解 **dCloud 域**树的各分支。企业树包括：

        i. **主机组 (Host Groups)** — 包含 IP 地址块的逻辑组。

        ii. **网络设备 (Network Devices)** — 包含导出器、防火墙等向系统报告的网络设备。如果导出器为防火墙或其他流阻止设备，则显示相应图标。

        iii. **示意图 (Maps)** — 包含关系流图、多主机组状态图形视图及其之间的任何通信。

        iv. **流量收集器 (Flow Collectors)** — 包含与域关联的所有 Stealthwatch 流量收集器。

        v. **身份服务 (Identity Services)** — 包含识别与域相关联的用户信息的设备，例如思科 ISE。思科 ISE 设备存在于集群内，用文件夹来表示。

        vi. **外部设备 (External Devices)** — 包含与域相关联的所有外部设备，例如 Snort 测试设备。

**注意：**项目最高层的颜色表示该项目下所有分支的最高警报级别。例如，如果“Inside Hosts”（内部主机）分支（位于“Host Groups”（主机组）下）下方的所有分支都为橙色，则“Inside Hosts”（内部主机）级别显示橙色。这可作为视觉指示器，指示该分支在其层次结构内具有警报。

**图 16.** 严重性级别

| 严重级别 | 关联颜色 |
| --- | --- |
| 严重 | 红色 |
| 重大 | 橙色 |
| 次要 | 黄色 |
| 轻微 | 蓝色 |
| 信息性 | 淡蓝色 |
| 警报不存在 | 绿色 |

6. 在企业树的域分支下为“Host Groups”（主机组）。“主机组”(Host Groups) 是 IP 地址逻辑组。“Host Groups”（主机组）结构为分层结构，被分为两大主要段- 内部和外部。“Host Groups”（主机组）是流量和行为监控的中心。对各主机和主机组进行行为监控，并与该组的基准行为进行比较。

    a. 点击**主机组 (Host Groups)** 标题上的加号。

    b. 点击**内部主机 (Inside Hosts)** 和**外部主机 (Outside Hosts)** 组中的加号即可查看这些主机的组织方式。

    c. 默认情况下，“Inside Hosts”（内部主机）文件夹包含名为 **Catch All（捕获全部）**的文件夹，其中包含对应于目标网络的大 IP 范围。无法重命名、移动或删除“Catch All”（捕获全部）文件夹。您可编辑“捕获全部”(Catch All) 主机组属性以定义要添加至该文件夹的 IP 范围。

**注意：**您可将鼠标悬停于 SMC 客户端接口中的各元素上，显示该元素的摘要信息。

    d. 展开树查看“主机组”(Host Groups) >“主机内部”(Inside Hosts) >“业务单元”(Business Units) >“工程”(Engineering)。

    e. 右键点击“工程”(Engineering) 组，然后依次选择“配置”(Configuration) >“主机组属性”(Host Group Properties)。

**注意：**如果系统提示您重新输入管理员凭证，请使用用户名：**admin** 和密码：**C1sco12345!** 登录以继续操作。

    f. “编辑主机组”(Edit Host Group) 窗口打开并显示 IP 地址在定义网络范围内的主机。

    g. 点击“关闭”(Close) 返回到 SMC 界面。

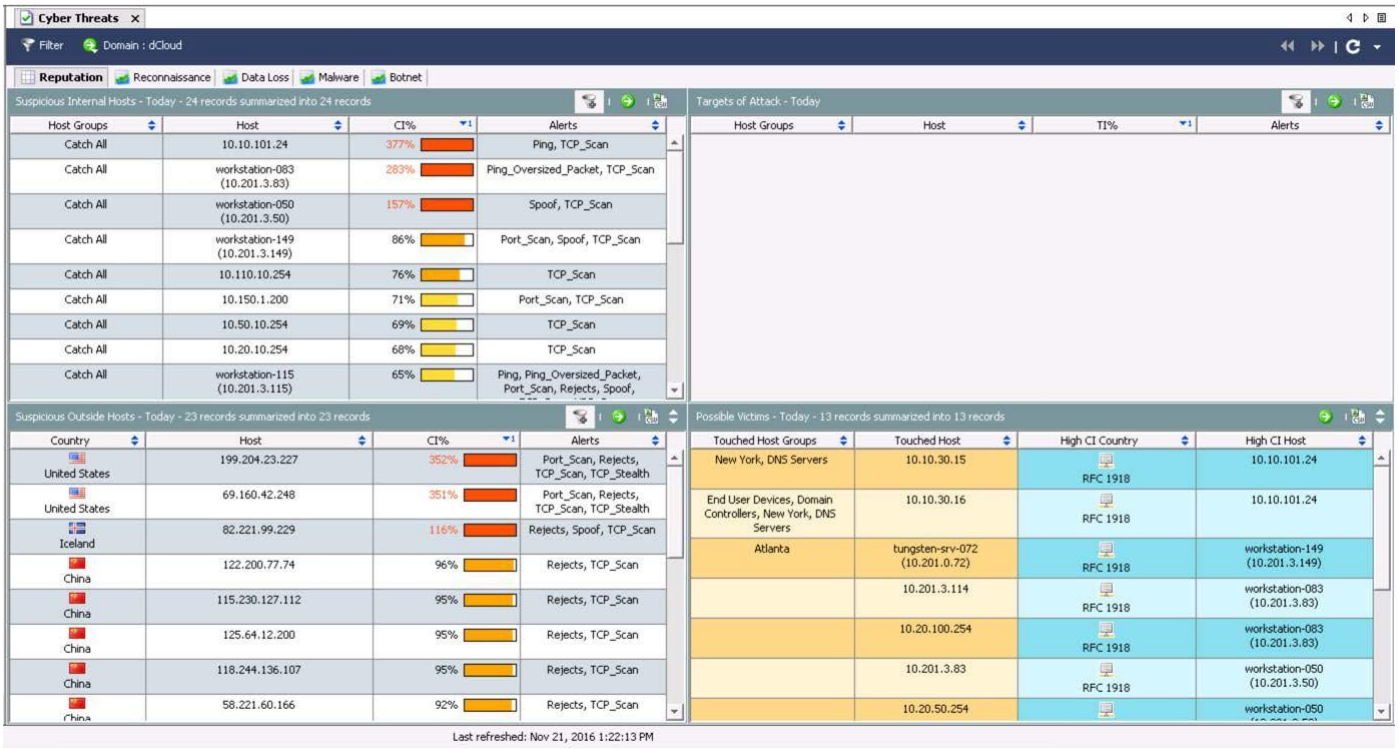
7. 企业树右边是显示控制面板和文档的选项卡式界面。SMC 显示表格和图表，其中，系统数据以文档形式显示在 SMC GUI 中间。活动文档即您当前正在查看的文档。

    a. 活动文档会自动刷新，而不活动文档不会。

    b. 用户应管理打开的文档数，因这些文档不会超时或自动关闭。

8. 默认情况下，双击域“dCloud”，网络威胁控制面板将显示在文档窗口中。

**图 17.** 网络威胁控制面板




9. 网络威胁控制面板旨在跟踪以下几项：

   a. **信誉 (Reputation)** — 有关可疑内外部主机的高级信息。

   b. **侦察 (Reconnaissance)** — 探测网络，发现可用于自定义攻击的攻击载体。

   c. **数据丢失 (Data Loss)** — 通常通过命令和控制通信将敏感信息导回给攻击者。

   d. **恶意软件 (Malware)** — 在整个内部网络中的主机上传播恶意软件，收集安全侦察信息、窃取数据或创建用于入侵网络的后门。

   e. **僵尸网络 (Botnet)** — 攻击者和网络内受侵害主机间的命令和控制通信。

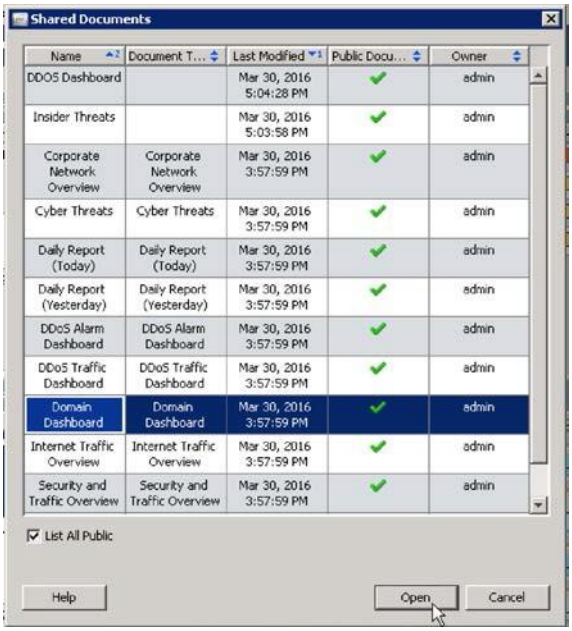
10. 域控制面板提供网络上的潜在威胁活动的高级视图。

    a. 高亮显示企业树中的 **dcloud** 域。

    b. 从菜单选项中，依次选择**文件(File) > 打开 (Open)**，然后从**共享文档 (Shared Documents)** 列表中选择**域控制面板 (Domain Dashboard)**。务必选中**列出所有公开文档 (List All Public)**。

    c. 点击**打开 (Open)** 显示**域控制面板 (Domain Dashboard)**。系统会显示**网络地图 (Network Map)** 选项卡。

**图 18.** 共享文档




d. 选择**摘要 (Summary)** 选项卡。

**注意：**将“摘要”(Summary) 选项卡上的“高度关注内部主机”(High Concern Inside Hosts) 表设置为将结果过滤为仅显示高度关注主机。如果此表为空，则表明此时网络中不存在高度关注主机。

取消选中过滤器 (  )，查看未表现出高度关注行为的主机。

i. 此处面板提供表现出大部分关注和警报迹象且可能需要调查的主机的概览。此处直观地显示过去24小时的流量模式，以供查看所有异常活动。

e. 选择**警报 (Alarms)** 选项卡。

i. 此处显示会所有当前有效警报以及过去两周的警报趋势。

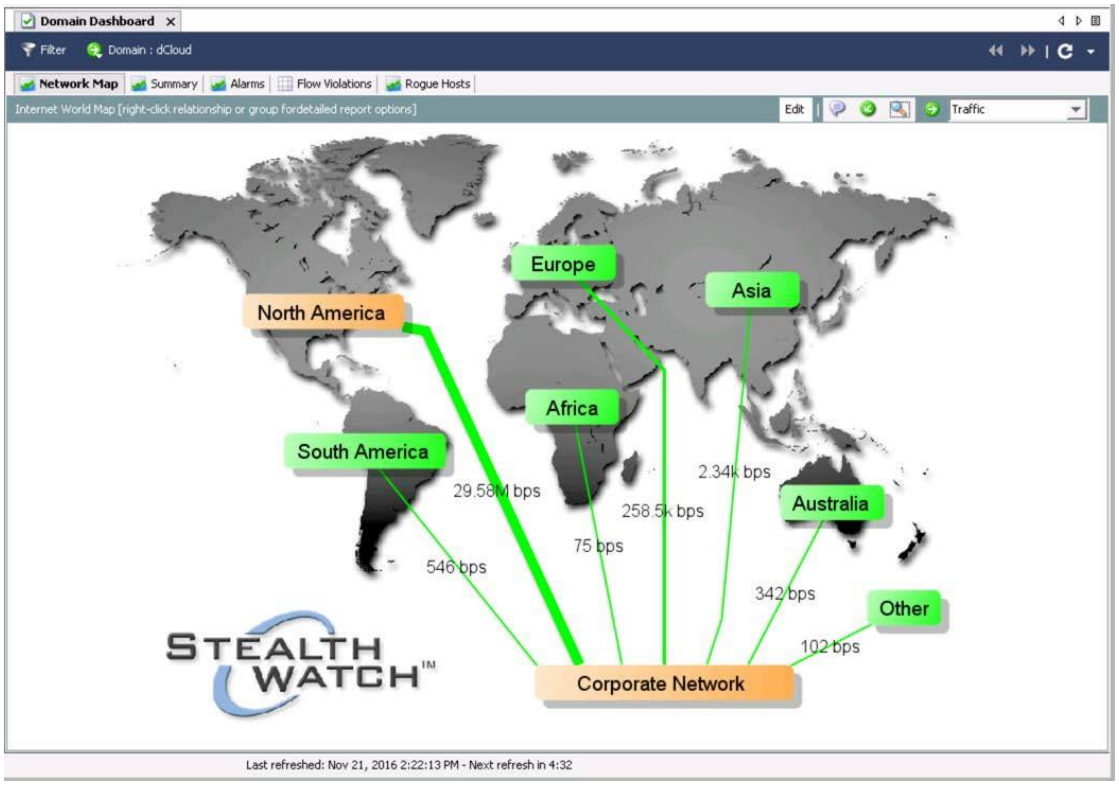
f. 选择**流量违规行为 (Flow Violations)** 选项卡。

i. 此处详细显示所有当前定义的主机锁定规则，以及当天违反规则的次数。

g. 选择**欺诈主机 (Rogue Hosts)** 选项卡。

i. 此选项卡显示所有观察到的、未分配到主机组的内部主机。

**图 19.** 域控制面板




11. 您极有可能已经在您的 SMC 显示屏中打开了大量的选项卡。要快速关闭这些选项卡，请按 ctrl + shift + W 同时关闭所有打开的选项卡。然后依次选择**文件 (File) > 打开 (Open) > 网络可视性报告 (Network Visibility Report)**，返回到场景开始时的初始状态。

## 问题

1. 在可视化Stealthwatch 部署中的数据时，您如何访问供您使用的文档？
2. 哪些严重性级别属于黄色警报指标？

# 场景 3　　检查主机组设置

## 场景描述

**主机组 (Host Groups)** 是 Stealthwatch 如何组织信息，将流量和行为模式进行分类的一个重要部分。使用主机组预配置部署，以反映 dCloud 公司的 IP 地址空间，包括内置主机组和用于该部署的客户定义的主机组。

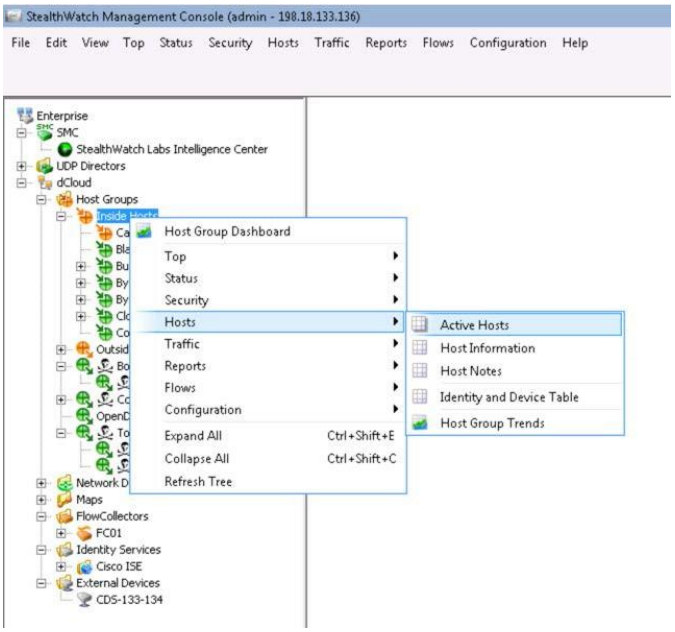
## 场景目标

此场景的目标是简要了解现有主机组配置，以及了解如何将主机与主机组分类。将主机与主机组进行分类，有助于简化和增强监控和策略分配。

## 步骤

1. 此场景在 Swing 客户端上进行。确保在前台中已装有该客户端。
2. 查看内置主机组
    a. 从企业树中，展开 **dCloud** 域旁边的加号
    b. 展开“主机组”旁边的加号，因此两个默认主机组显示：**内部 (Inside)** 和**外部 (Outside)。**
    c. 右键点击**内部主机（Inside Hosts），**然后依次选择**主机 (Hosts) 虚拟主机 (Active Hosts)。**系统会显示“活跃主机”文档，其中列出所有归类为**内部**的活跃主机。

**图 20.**　“主机”(Hosts) >“活跃主机”(Active Hosts)

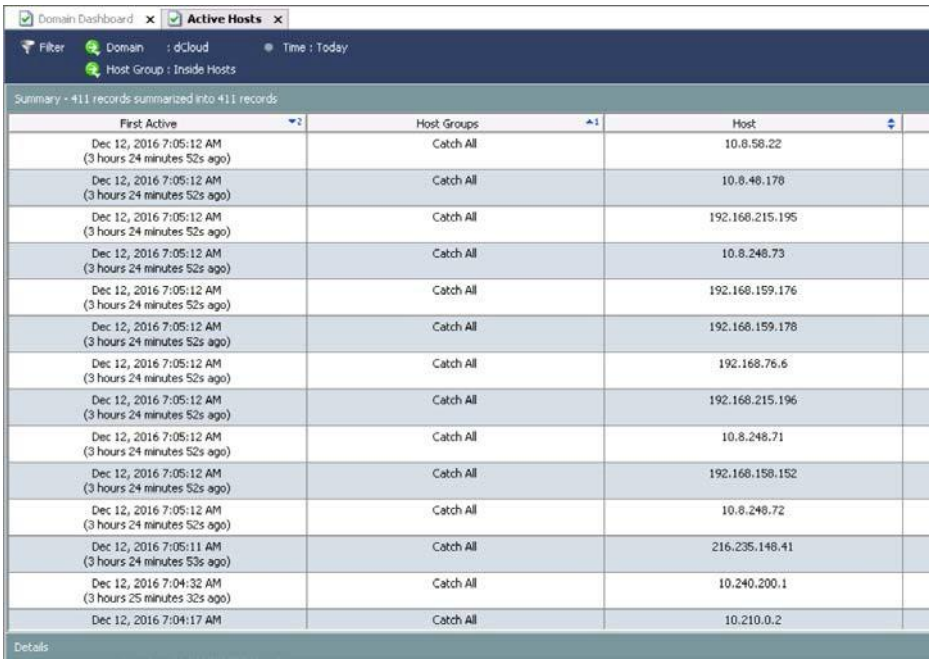


d. 点击**主机组** (**Host Groups**) 列标题，按照**主机组 (Host Group)** 分类排序。向下滚动并注意大量 IP 属于**捕获全部 (Catch All)** 主机组。

i. **捕获全部 (Catch All)** 主机组默认配置为将所有私网 IP 范围 (RFC 1918) 作为其成员包括在内。

ii. 建议您将**捕获全部 (Catch All)** 组下分配给企业**的所有公网 IP 范围包括在内（例如：– DMZ、NAT'd IP's 等）。**

**图 21.** **活跃**主机




3. 要查看**捕获全部** (**Catch All**) 主机组，请按以下步骤操作：

a. 右键点击**捕获全部** (**Catch All**) 主机组，然后依次选择**配置 (Configuration) > 管理主机组 (Manage Host Groups)。**

b. 系统将显示编辑主机组对话框，注意**范围(Ranges)** 下已配置的私网 IP范围。

c. 点击**关闭 (Close)** 以退出。

4. 使用右上角的**搜索 (Search)** 字段：

**图 22.** 搜索框

a. 在 Swing 客户端 GUI 右上角的**搜索字段 中**输入 IP 地址 10.10.30.16，然后点击 **Enter**。

b. 系统将显示搜索结果窗口，并在列表中显示 **IP 地址**。

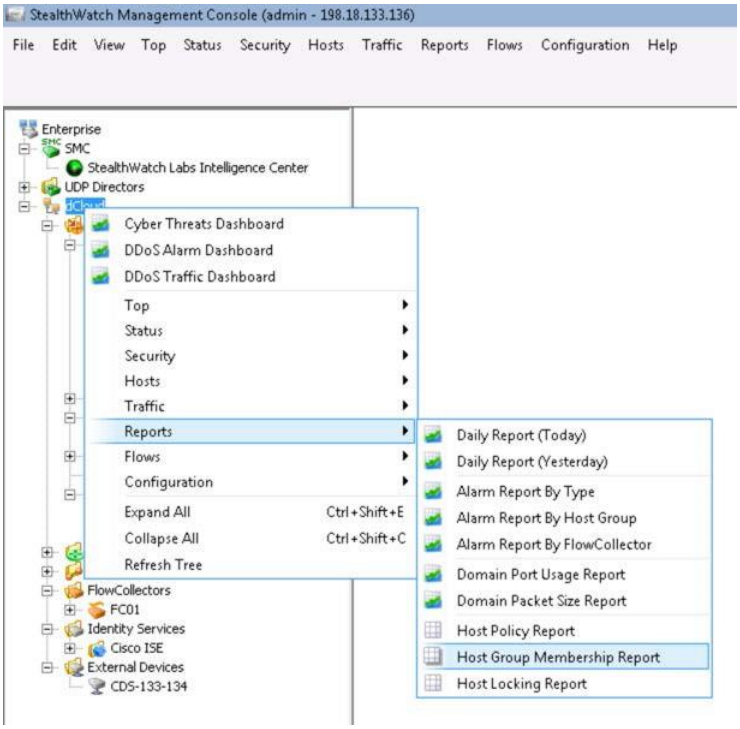
c. 右键点击结果窗口中的 IP 地址条目，然后依次选择**配置 (Configuration) > 管理主机组 (Manage Host Groups)。**注意 IP 地址所属的主机组。

d. 关闭主机组窗口。

5. 使用主机组成员报告：

a. 右键点击 **dCloud** 域，然后选择**报告 (Reports) > 主机组成员报告 (Host Group Membership Report)**。

**图 23.** 报告 (Reports) > 主机组成员报告 (Host Group Membership Report)




b. 系统会打开主机组成员报告

c. 您可以对报告视图进行自定义：

i. 右键点击任意列标题。这样您可以选中及取消选中报告选项，以显示或隐藏列（注意：该操作对 Stealthwatch 中的所有报告均有效）。

d. 点击列标题，按升序或降序对字段中的结果进行排列（注意：该操作对 Stealthwatch 中的所有报告均有效）。

e. 检查结果。定义的内部和外部主机组有多少？

f. 右键点击“内部主机”(Inside Hosts) 下方的“按功能分类主机”(By Function Host Group)，选择“展开全部”(Expand All)。注意：并非所有在企业树中显示的主机组也会出现在“主机组成员报告”(Host Group Membership Report) 选项卡中。

g. 当您完成该场景时，请关闭“主机组成员报告”(Host Group Membership Report) 选项卡清除以关闭所有窗口，右键点击企业树中“按功能分类”(By Function) 并选择“全部收起”(Collapse All)，以减少视觉混乱。

## 问题

1. “捕获全部”(Catch All) 主机组默认包含哪些内容？
2. **10.10.30.16** 属于哪个主机组?

# 场景 4　　执行流量查询

## 场景描述

对于此场景，我们要演示如何搜索网络中的特定设备。让我们看一个简单场景，在该场景中，我们可以使用流量数据确定该信息。

## 场景目标

了解如何在 Swing 客户端和 WebUI 中进行流量查询。

## 步骤

1. 首先让我们了解流量表的基本信息，以及如何获取该文档。场景的这部分在 Swing 客户端上进行。确保在前台中已装有该客户端。

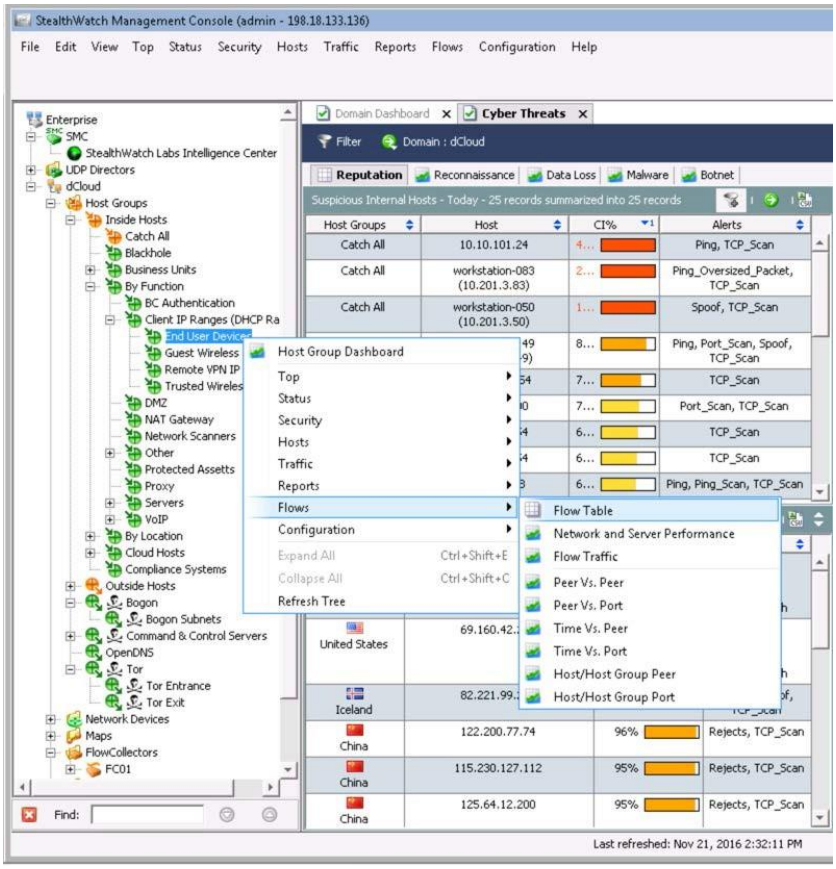
**注意：**记住虽然您可以同时访问大量流量数据，但这通常并非高效的做法；最佳做法是从高级数据开始，然后仅关注相关流量，这点至关重要。

2. 点击企业树中的 **dCloud。**
3. 在企业树窗格底部的**查找** (**Find**) 字段中，输入 **End**，然后按 **Enter**。

**注意：**右上角的**搜索 (Search)** 字段可搜索全部实际流数据；**查找 (Find)** 字段可搜索企业树中的命名对象。

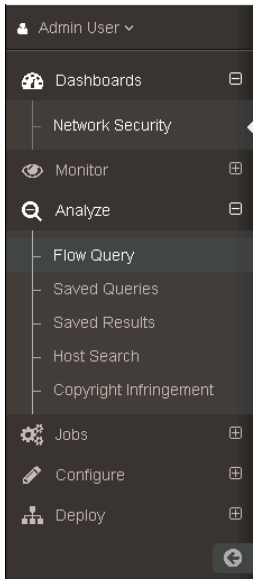
4. 您的搜索应返回“内部主机”(Inside Hosts) >“按照功能分类”(By Function) >“客户端 IP范围（DHCP 范围）”(Client IP Ranges [DHCP Range]) >“最终用户设备主机组”(End User Devices Host Group)。
5. 右键点击“最终用户设备主机组”(End User Devices Host Group)，然后依次选择“流量”(Flows) >“流量表”(Flow Table)。系统返回多少条记录？

**图 24.** “流量”(Flows) >“流量表”(Flow Table)



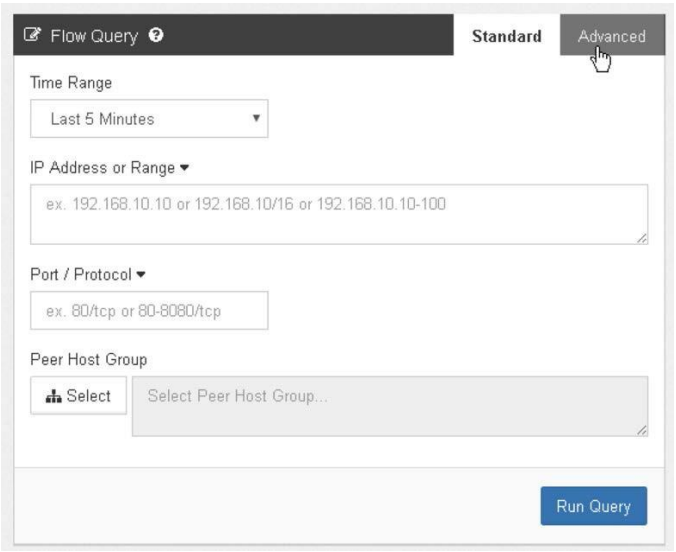

6. 在完成该部分场景后，关闭SMC 中的所有流量表文档，以清理混乱因素。
7. 此场景的第二部分在SMC WebUI上进行。最小化 Swing 客户端，这样打开控制面板的网络浏览器位于靠前位置。
8. 选择左侧导航面板的**分析 (Analyze) > 流量查询 (Flow Query)**。

**图 25.** “分析”(Analyze) >“流量查询”(Flow Query)。



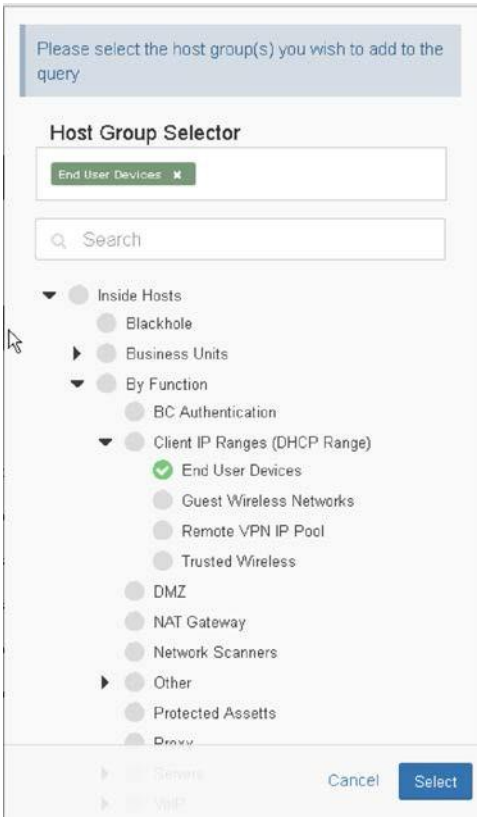

9. 选择**高级** (**Advanced**) 搜索选项卡

**图 26.** 高级搜索选项卡




10. 设置以下过滤条件：
    a. **范围：**5 分钟
    b. 搜索对象：
        i. 对于主机，选择：包括，主机组
            1. 在主机组下方，点击**选择 (Select)**
            2. 在打开的主机组选择器窗格中，浏览到：**内部主机 (Inside Hosts) > 按照功能分类(By Function) > 客户端 IP 范围（DHCP 范围）(Client IP Ranges [DHCP Range]) > 最终用户设备(End User Devices)，然后勾选旁边的复选框。**

**图 27.** 主机组选择器



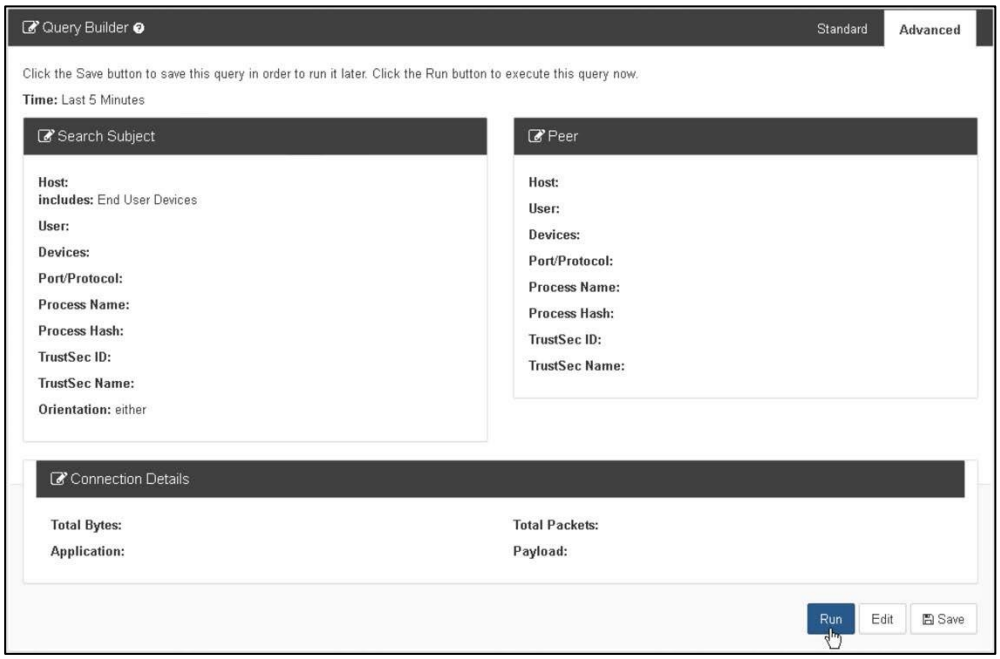

**注意：**在该窗格中，您还可以通过在搜索 (Search) 字段中输入完整或部分名称搜索主机组。

3. 点击**选择 (Select)**。

ii. 不理会剩余的设置，但是注意可用于调整查询条件的选项。

11. 点击屏幕底部的**查看查询 (Review Query)**。
12. 查看您的查询设置，然后在准备就绪时点击运行 (**Run**)。

**图 28.** 查询生成器




13. 系统返回多少条记录？

**注意：**由于执行时间不同，此处返回的结果可能与 Swing 客户端所显示的内容不同。

14. 当查询完成时，注意**操作 (Actions)** 面板中的可用选项：

    c. **保存结果 (Save Results)** — 保存当前所执行查询的结果，以供随后查看。您可通过左侧导航面板的**流量 (Flows) > 保存结果 (Saved Results)** 查看保存的结果。

    d. **保存查询(Save Query)** —保存当前的查询参数，以供随后使用。您可通过左侧导航面板的**流量 (Flows) > 保存的查询 (Saved Queries)** 中查看已保存的查询。

    e. **克隆查询 (Clone Query)** —将当前查询的参数复制到选项中，执行新的流量查询。

    f. **导出为 .CSV (Export as .CSV)** —将当前结果导出为可下载到您的本地设备的 .csv 格式文件，以供外部使用和分析。

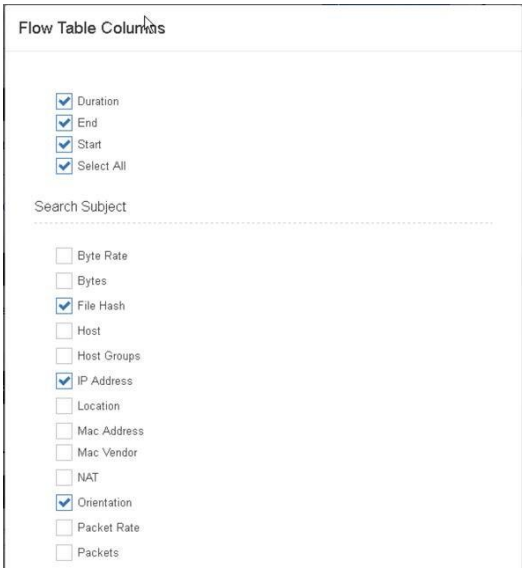
**图 29.** dCloud **流量**


15. 在流量查询结果面板右上角，请注意网格图标。点击该图标会切换到**表状**视图。

**图 30.** “流量查询结果”(Flow Query Results)


16. 在**活动 (Actions)** 面板中，请注意您有一个新的可用选项：**管理列**。点击它。
17. 注意各种可添加到流量查询结果的其他信息列，这些列可为您提供围绕活动的其他上下文。
    g. 要添加额外的信息列，勾选在数据属性旁边的复选框。您可以进行添加和删除，以便根据需要自定义显示的结果。
    h. 现在，点击**取消 (Cancel)**。

**图 31.** 流量表列




18. 注意流量查询结果表格左侧的选项，以优化您的结果。
19. 点击**网络安全 (Network Security)**，以返回到 WebUI 的控制面板屏幕。您已经完成该场景。

## 问题

1. 多少个不同的设备客户端主机 IP 与用户 **ethel 相关**？
2. 在 WebUI 流量查询结果中，向您提供的任意三个与**连接 (Connection)** 相关的其他信息列**是什么？**

# 场景 5　　使用文档

## 场景描述

Stealthwatch 能够以多种方式显示流量和统计信息。每当请求查询或报告时，如流量查询和热门报告，文档会在右侧面板中打开并显示。除了启动 Swing 客户端时打开的文档外，SMC 还有许多其他文档和预定义的控制面板。此场景检查一些可能与许多客户相关的文档。

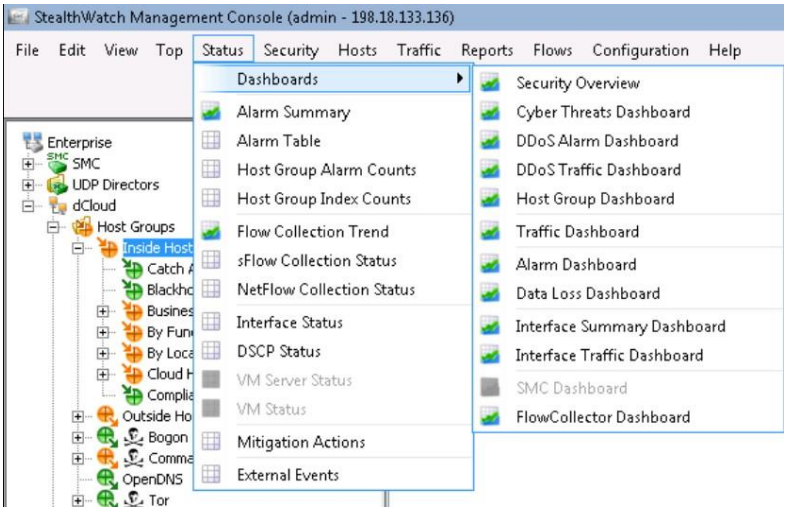
## 场景目标

了解文档及其在故障排除和调查时的使用。

## 步骤

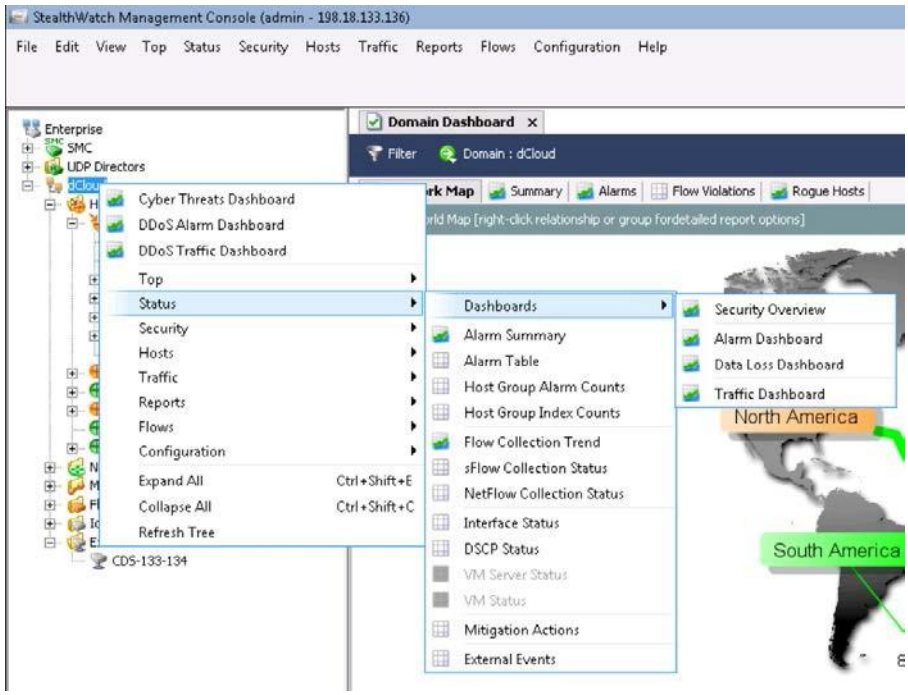
1. 此场景在 Swing 客户端上进行。确保在前台中已装有该客户端。
2. 要在您的 SMC 上显示可用的控制面板选项，点击顶部菜单栏的**状态 (Status)**，然后点击**控制面板 (Dashboards)**，以查看可用的控制面板列表。

**图 32.**　SMC 控制面板




3. 注意：根据左侧企业树中的所选内容，可用控制面板和文档列表是否会发生变化？例如：
    i. 选择然后右键点击企业树中的 **dCloud**，接着依次点击**状态 (Status) > 控制面板** (**Dashboards**)。

**图 33.** “状态”(Status) >“控制面板”(Dashboards)




j. 选择然后右键点击企业树中的 **SMC**，接着依次点击**状态 (Status) > 控制**面板 (**Dashboards**)。

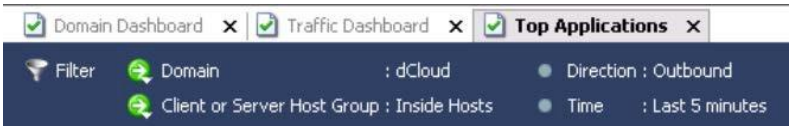
k. 哪些项目在这两种情况下均可用？哪些只适用于一种情况？

4. 依次点击菜单栏中的**状态 (Status) > 控制面板 (Dashboards) > 流量控制面板 (Traffic Dashboard)**，查看由内部和外部主机引发的当前流量情况。依次选择**帮助 (Help) > 帮助 (Help)**，访问适用于此控制面板的上下文相关帮助。（注意：如果系统提示您进行身份验证，请输入您的登录信息，返回并再次选择“帮助”(Help) >“帮助”(Help)，以打开上下文相关帮助。）在阅读控制面板内容后，请切换回Stealthwatch 管理控制台窗口。

5. 文档和控制面板可以通过企业树层次的各个级别直接显示。例如，右键点击 **dCloud** 域，然后依次选择**热门 (Top) > 应用 (Applications) > 出站 (Outbound)**。注意本文档顶部深蓝横幅栏中显示的过滤条件。已选择哪个主机组？显示信息的时间范围是多久？哪些应用显示在顶部？

6. 点击横幅条中的**过滤 (Filter)** 图标。选择**日期/时间** (**Date/Time**)，将当前值从 0 天、0 小时、5 分钟更改为 1 天、0 小时、0 分钟，并点击**确定**。热门应用是否已更改？

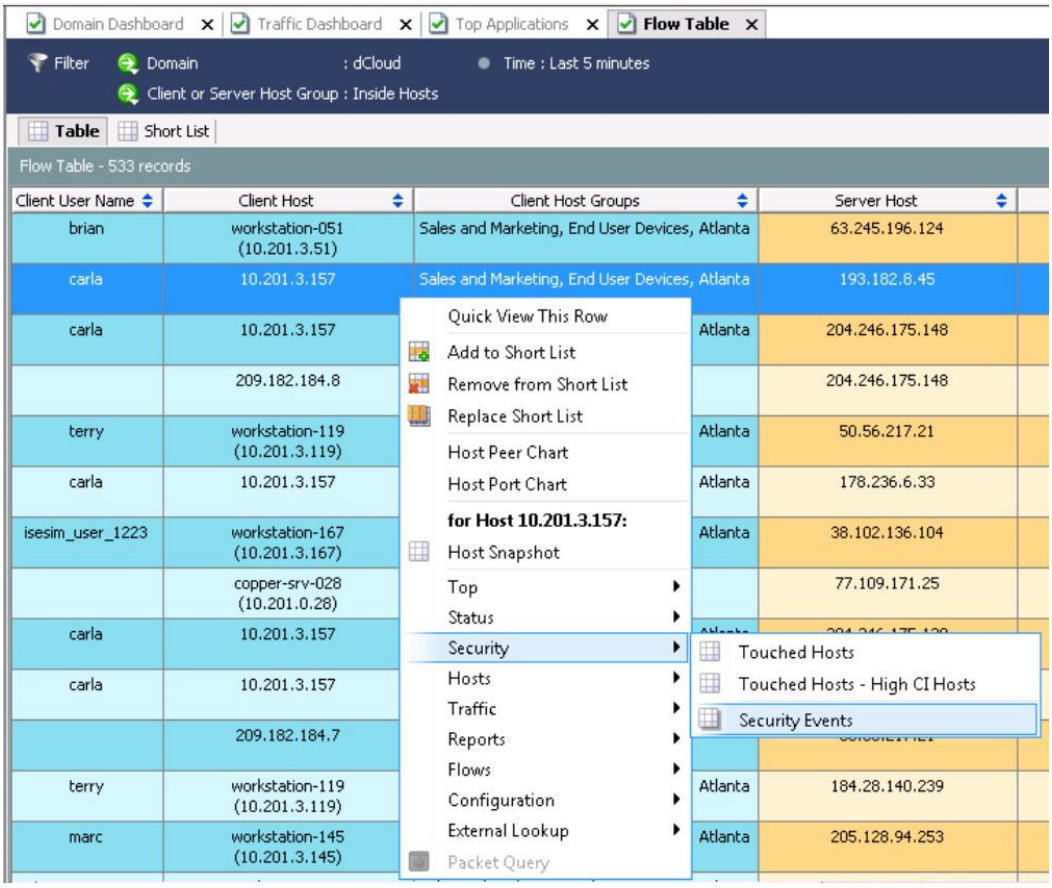
**图 34.** 热门应用




7. 右键点击列表中的热门应用，然后选择**流量 (Flows) > 流量表(Flow Table)**。这时会显示组成热门应用文件中所示流量的实际流量。

8. 从列表中选择一个看起来怪异的 IP 地址（服务器或客户端），右键点击该字段，然后依次选择**安全性 (Security) > 安全事件 (Security Events)**。这时系统会显示与该 IP 地址关联的关注指数 (CI) 事件。注意：在横幅栏中，过滤器现在设定为只选择您已选定的 IP 地址。

**图 35.** 流量表




9. 如时间允许，请随时查看其他文件、主机和其他信息元素。类似地，您可以按照先前场景中访问域控制面板的方式访问文档：依次点击顶部菜单上的**文件 (File) > 打开 (Open)**，选择一个共享文档，然后点击**打开 (Open)**。

10. 在此场景中结束时，您可能已经在SMC 中打开了大量的选项。
要快速关闭这些选项卡，请按 ctrl + shift + W 同时关闭所有打开的选项卡。然后选择**文件 (File) > 打开 (Open) > 网络可视性报告 (Network Visibility Report)**，返回到场景开始时的初始状态。

## 问题

1. 哪些控制面板通过右键点击 **dCloud** 直接打开？

# 场景 6　　确认规则/策略参数

## 场景描述

默认情况下，在正常 Stealthwatch 操作中，新 IP 会分配给**捕获全部 (Catch All)** 主机组。管理员随后将这些 IP 分配到相应的主机组。根据主机属的组，向网络上检测到的主机分配主机策略。如果未向主机或其所属的主机组分配特定策略，则该主机将继承默认的**内部**或**外部主机策略。**

通过自定义安全事件，您可以创建主机与/或主机组之间的数据流规则。自定义安全事件有助于审计安全策略和改善合规性。

## 场景目标

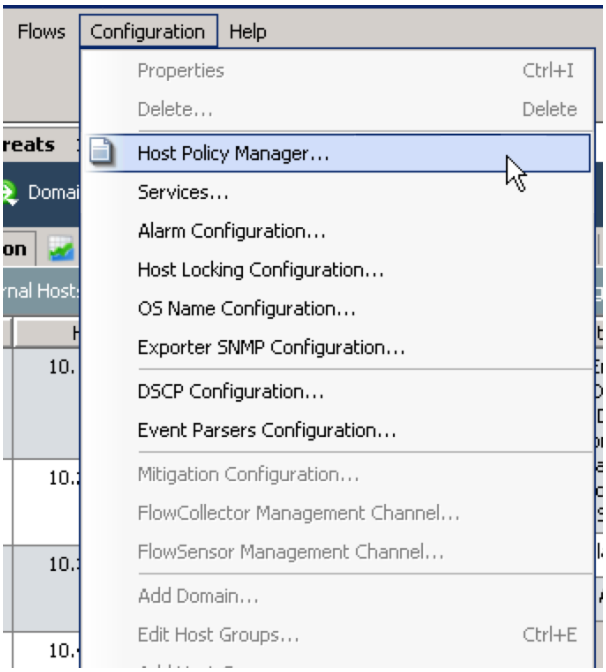
学习主机策略和自定义安全事件

## 步骤

查看内置**主机策略 (Host Policies)：**

1. 从顶部菜单中，依次选择**配置 (Configuration) > 主机策略管理器** (**Host Policy Manager**)。（注意：系统可能会提示您进行身份验证。如果出现提示，请输入密码，然后再次依次选择**配置 (Configuration) > 主机策略管理器** (**Host Policy Manager**)）

**图 36.**　“配置”(Configuration) >“主机策略管理器”(Host Policy Manager)

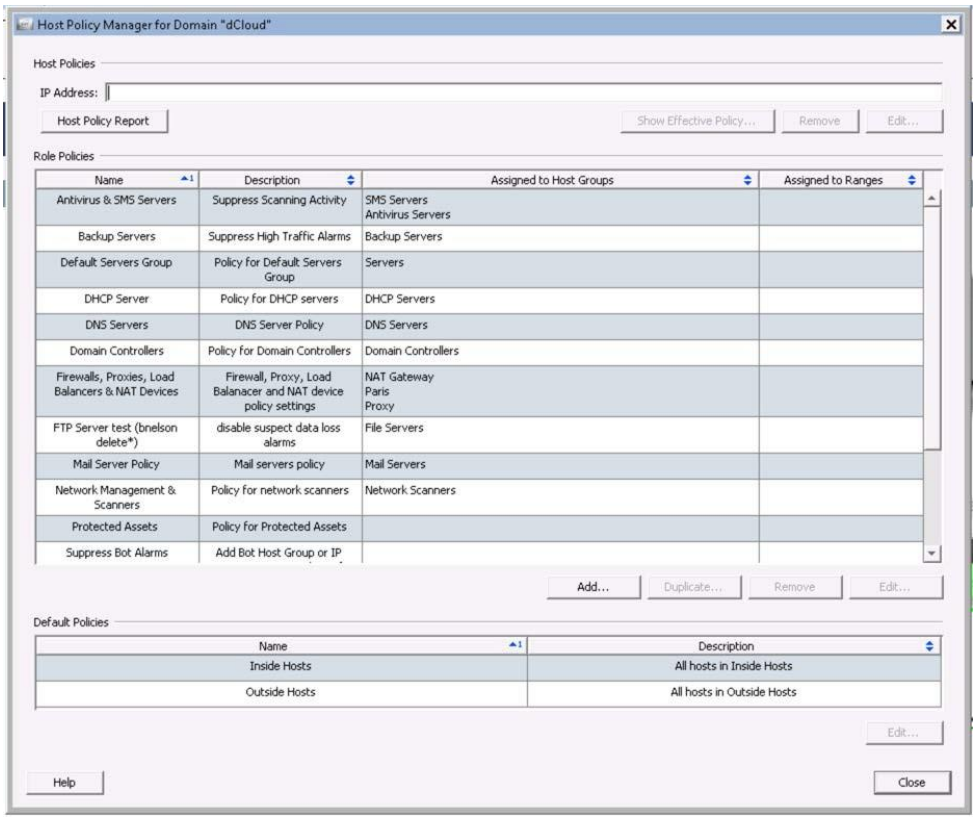



2. 系统会显示**主机策略管理器** (**Host Policy Manager**)。注意角色策略部分。

a. 多少个**主机组**分配了角色策略？

b. 有多少默认策略？

**图 37.** “dCloud”的主机策略管理器




3. 双击其中一项默认策略，系统会显示**编辑默认策略** (**Edit Default Policy**) 对话框。注意由此策略管理的警报类别和安全事件。

   a. 有多少警报类别已禁用？

4. 点击“关闭”(Close)，以关闭**编辑默认策略 (Edit Default Policy)** 窗口

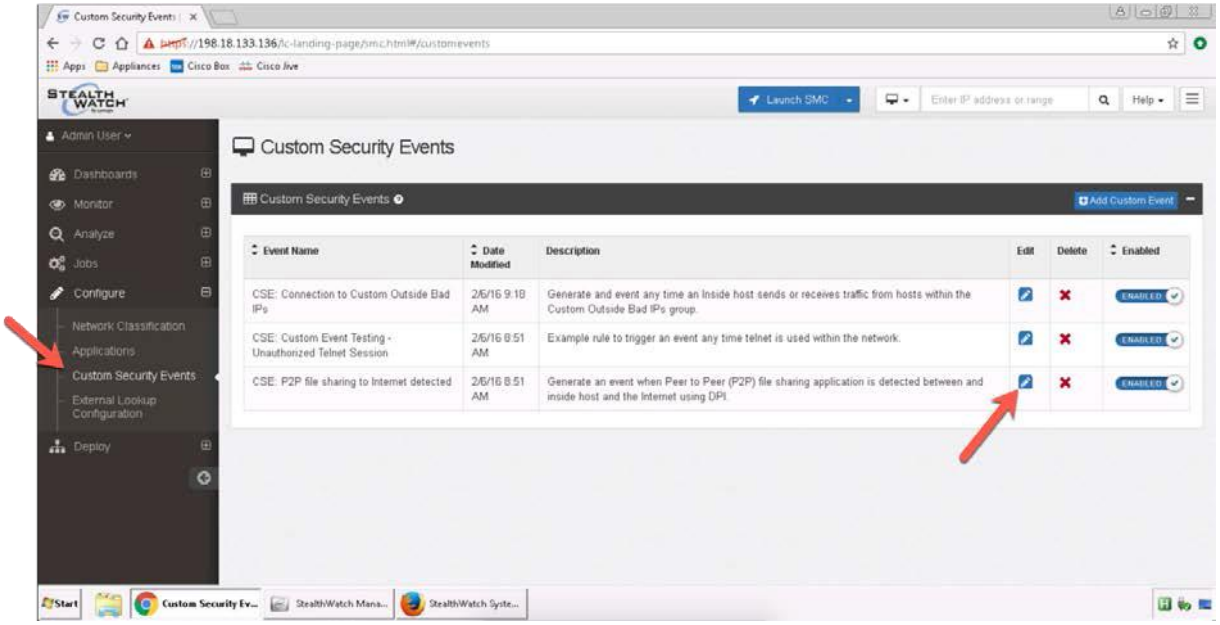
5. 点击“关闭”(Close)，以关闭**主机策略管理器 (Host Policy Manager)** 窗口

查看**自定义安全事件 (Custom Security Events)：**

6. 在 SMC Web 界面中，导航至**配置 (Configure) > 自定义安全事件 (Custom Security Events)。**

7. 选择规则**检测到 CSE: P2P 文件共享到互联网(CSE: P2P file sharing to Internet detected)** 的**编辑** (Edit) **按钮**

**图 38.** 自定义安全事件配置




8. 查看自定义安全事件参数
9. 选择**取消 (Cancel)**，以取消对该 CSE 进行的任何更改。

## 问题

1. 内部主机默认策略的数据收集警报设置是什么？
2. 客户安全事件寻求什么应用，在哪些组之间进行寻求？

# 场景 7　　调查警报

## 场景描述

Stealthwatch 利用大量行为和基于策略的算法，将在网络上观察到的行为警告其用户。最常见的警报是提醒 Stealthwatch 用户调查关注指数 (CI) 值高的主机。我们现在将执行此任务，尝试确定它是否属于正常行为，以及是否可以进行校正。

## 场景目标

在该场景中，您的目标是了解如何在 Stealthwatch 中调查警报，以及导出相关数据提交给 IT。

## 步骤

1. 场景的这部分在 Swing 客户端上进行。确保在前台中已装有该客户端。
2. 如需要，您可以从**状态 (Status) > 控制面板 (Dashboards)** 菜单中重新打开**网络威胁控制面板 (Cyber Threats Dashboard)**，然后点击该控制面板的**信誉 (Reputation)** 选项卡。
3. 在左上角象限中，查看**可疑内部主机(Suspicious Internal Hosts) 中的CI 值高的内部主机列表。**

**注意：**如果空间过窄，无法完整显示 CI% 列，可将鼠标光标悬停在各条上查看相关值。

4. 为更好地查看这个高 CI 主机，使用绿色的**前往文件 (Go To Document)** 控件，打开新的**关注指数 (Concern Index)** 文档选项卡。

**图 39.**　内部主机 - 当天


5. 切换回**关注指数** (**Concern Index**) 文档，然后选择与扫描（如 TCP_Scan）活动相关的一行。右键点击该行，然后依次选择**安全 (Security) > 安全事件 (Security Events)**。
6. 正在扫描哪些端口和网络范围？切换到**目标主机摘要** (**Summary of Target Hosts**) 选项卡。正被扫描的主机是否看起来有针对性，还是均匀分布？

7. 点击**安全事件 (Security Events)** 文档中的**表格**选项卡，然后检查**安全事件(Security Events)** 列信息。是否有任何具备超高安全相关性的端口成为攻击目标？
8. 右键点击其中一行，然后选择**快速查看此行** (**Quick View This Row**)。留意点击计数。在检查数据后，关闭快速视图窗口。
9. 右键点击其中一行中的**源主机 (Source Host) IP**，然后选择**主机快照** (**Host Snapshot**)，查看正在执行扫描的主机的详细信息。
10. 选择主机快照文档的**导出器接口** (**Exporter Interfaces**) 选项卡。您看到哪些 NetFlow 源？
11. 切换到**身份、DHCP 和主机说明** (**Identity, DHCP & Host Notes**) 选项卡。检查思科 ISE 集成提供的信息。关于用户和设备，您有什么想法？
12. 切换至**安全性** (**Security**) 选项卡。此扫描主机是否已经“联系”另一台主机？

**注意：**如果当天的搜索选项中未显示内容，尝试更改**过滤器**，将昨天的数据包含在内。

“联系”表示扫描主机已经与联系的主机建立连接，并交换数据。

13. 在**安全性** (**Security**) 选项卡的**联系信息** (**Touch Information**) 部分，右键点击**已经联系另一台主机 (Has Touched Another)** 或**已被联系 (Has Been Touched)** 列的**！确定 (!Yes)** 字段，然后根据可用情况，选择**联系的主机 (Touched Hosts)** 或**被联系的主机 (Hosts Touched By)**。此扫描主机已联系多少台其他主机？
14. 要将主机快照打印到文件上，以便将其转发到IT 安全部门，用以调查和补救该设备，请按以下步骤操作：
    a. 选择**主机快照** (**Host Snapshot**) 文档。
    b. 在主菜单栏，依次选择**文件 (File) > 打印文件 (Print to File)**，将文件命名为 **malware-host.pdf**，然后将主机快照保存到您的**桌面**文件夹中。
15. 作为在此场景中的最后一步，返回到**网络威胁** (**Cyber Threats**) 控制面板，右键点击该选项卡，然后选择**关闭其他 (Close Others)** 以清理界面。切换到**网络威胁 (Cyber Threats)** 控制面板上的**侦察 (Reconnaissance)** 选项卡，查看右下角的**排名靠前的外部发起的扫描事件 (Top Scans from Outside)** 面板。我们是否报告外部发起的扫描事件？如果是，从何处发起扫描？他们在寻找什么？
16. 在您完成调查后，除“网络威胁”控制面板之外，关闭所有打开的文档。

此场景的第二部分在SMC WebUI上进行。最小化 Swing 客户端，这样打开控制面板的网络浏览器位于靠前位置。我们将使用 WebUI 中的可用信息调查高 CI 警报。

17. 有效警报首行是**关注指数** (**Concern Index**)。
    c. 点击警报框中的底部编号（在**总计**行中）。
    d. 或者，您可以展开**当天警报** (**Today's Alarms**) 面板，并点击**高度关注指数** (**High Concern Index**) 的扇形图或文本。
18. 系统将会打开带有警报表的页面，显示所有正在参与可疑活动的所有源主机。

19. 在**详细信息** (**Details**) 列，设有观测活动量的摘要，以及触发警报的阈值。点击该文本，查看主机相关信息。
20. 系统会加载**安全事件详细信息** (**Security Event Details**) 页面，显示触发警报的安全事件的相关信息，包括源 IP、目标 IP、事件关注指数评分和事件类型。
21. 审核围绕警报的安全事件。主机参与何种行为？是否有活动看起来似乎在针对特定相关端口？
22. 在**源主机 (Source Host)** 字段中点击主机 IP 地址。这将打开主机的**主机报告** (**Host Report**)。
23. 查看**按类型分类警报（过去 7 天）(Alarms by Type [last 7 days])** 面板。在过去一周中，此主机是否涉及任何其他可疑行为？
24. 点击**按类型分类警报（过去 7 天）(Alarms by Type [last 7 days])** 中的警报栏，以获得围绕活动的额外详细信息。
25. 点击左侧导航面板上的**控制面板** (**Dashboard**) 链接，返回到 WebUI 控制面板屏幕。您已经完成该场景。

## 问题

1. 在第 16 步中，我们询问“我们是否报告外部发起的扫描事件？如果是，从何处发起扫描？”排名靠前的外部扫描仪主机的 IP 和原产地是什么？
2. 排名靠前的扫描仪特别关注什么范围的端口？

# 场景 8　　版权侵犯事件

## 场景描述

您今天上午收到以下信息：

尊敬的先生/女士：

此通知仅面向主要互联网服务帐户的持有者。有人使用此帐户参与受版权保护音乐的非法复制和/或传播。

pyright Enforcement Group, LLC,（“我们”）代表该艺术家。艺术家对如下所列的注册版权，拥有所有权利、所有权和权益。

证据：

侵权标题：TAYLOR SWIFT - 1989 年

侵权文件名：Taylor Swift - 1989 (Deluxe Edition) [Full Album] 320kbps [n00b].rar

侵权散列：6D0313EZ9F8A0XX1F6A3300FE53DD0CE8459CA24

侵权文件大小：214 MB 侵权协议：BitTorrent

侵权时间戳：2016-10-07 08:59:00 北美东部时间

侵权者 IP 地址：209.182.184.7 侵权者端口：14001

根据《美国版权法》(17 U.S.C. 106) 特此通知您未经授权的复制和/或传播行为违反艺术家的注册版权。鉴于此，特此要求您及所有使用该帐户的人员立即并永久停止未经授权的复制和/或传播本通知所列的注册版权或艺术家以其他方式拥有的版权。

顺祝商祺！

Copyright Enforcement Agent

Copyright Enforcement Group, LLC

版权侵犯报告利用 StealthWatch 的能力，可以读取来自 NetFlow 的 NAT 转换数据信息，并将观察到的网络活动返回到您的网络中的初始主机上；为用户提供一个快速执行操作的界面。

注意：Stealthwatch 无法检测正在发生的违规行为。它可以为您提供历史数据和调查事件报告的方法，以进行补救和确保准确性。

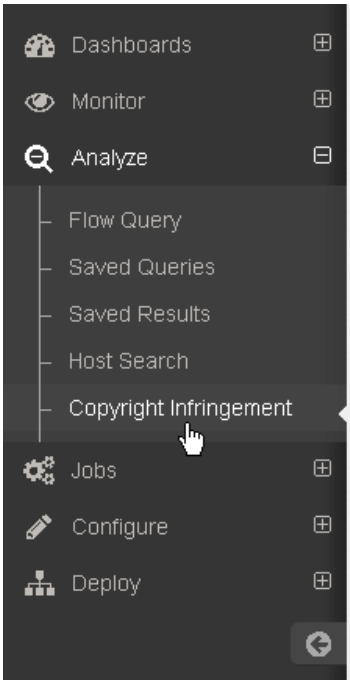
# 场景目标

使用 Stealthwatch 版权侵犯报告，查看您的网络中负责所报告的版权侵犯活动的人员。

# 场景步骤

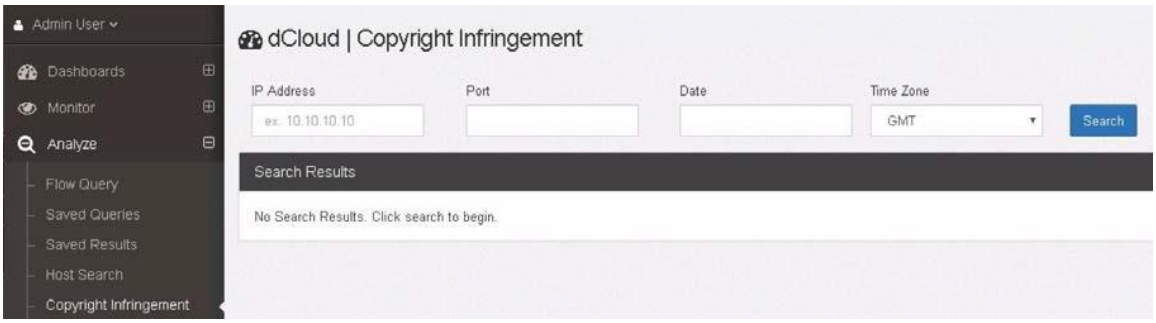
1. 此场景在 SMC WebUI 上进行。如有必要，最小化 Swing 客户端，这样打开控制面板的网络浏览器位于靠前位置。
2. 选择左侧导航面板的**分析 (Analyze) > 版权侵犯 (Copyright Infringement)**。

**图 40.** “分析”(Analyze) >“版权侵犯”(Copyright Infringement)




3. 系统将显示**版权侵犯控制面板 (Copyright Infringement dashboard)**。

**图 41.** 版权侵犯控制面板



4. 输入受举报涉及版权侵犯活动的主机信息。

    a. **IP 地址：**209.182.184.7

    b. **端口：**14001

    c. **选择日期和时间 (Select the Date and Time)：**<当天日期> 08:59:00

    d. **选择时区 (Select the Time Zone)：**东部

5. 点击**搜索 (Search)**。如果发现匹配，将显示结果窗格。

6. 由于这是一个实验，所以会存在匹配。点击**选择 (Select)**，选择定位的连接，以供进一步查看。

7. 点击**内部主机 (Inside Host)** 的 IP 地址，以便在负责文件传输活动的内部主机上弹出**主机报告 (Host Report)** 屏幕。

8. 注意向您提供的主机及其活动的其他信息，并考虑下面的问题。

## 问题

1. 对所报告活动负责的内部主机 IP 地址是什么？

2. 对所报告活动负责的用户名称是什么？

# 场景 9　　验证 思科 TrustSec 实施

## 场景描述

思科 TrustSec 技术可简化网络访问的调配，加快与安全相关的操作速度，并确保整个网络的策略实施保持一致。此类可扩展和敏捷分段技术嵌入到超过 40 种的交换机、路由器、无线设备和其他思科产品中。借助支持思科 TrustSec 结构的设备，通过 NetFlow，Stealthwatch 可以使用思科安全组标记 (SGT) ID 和命名数据。

您的企业开始采用此技术，现在是测试阶段。

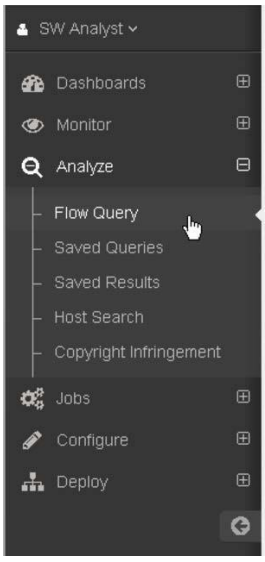
## 场景目标

了解如何使用 Stealthwatch 检验 TrustSec 在您企业中是否成功配置。

## 步骤

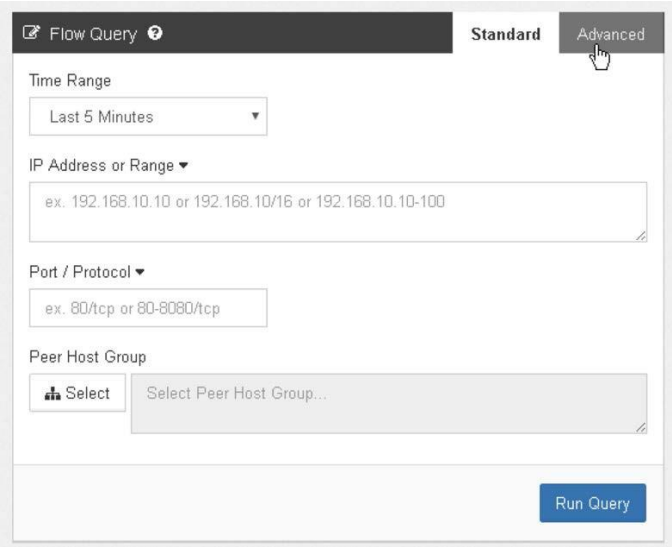
1. 此场景在 SMC WebUI 上进行。如有必要，最小化 Swing 客户端，这样打开控制面板的网络浏览器位于靠前位置。
2. 选择左侧导航面板的**分析 (Analyze) > 流量查询 (Flow Query)**。

**图 42.**　“分析”(Analyze) >“流量查询”(Flow Query)。




3. 选择**高级 (Advanced)** 搜索选项卡。

**图 43.** “流量查询”(Flow Query) >“高级”(Advanced)




4. 根据您的工程师的意见，SGT ID 8 目前在网络上活跃，并已经分配到多台主机。在高级流量查询面板上，请设置以下过滤器：

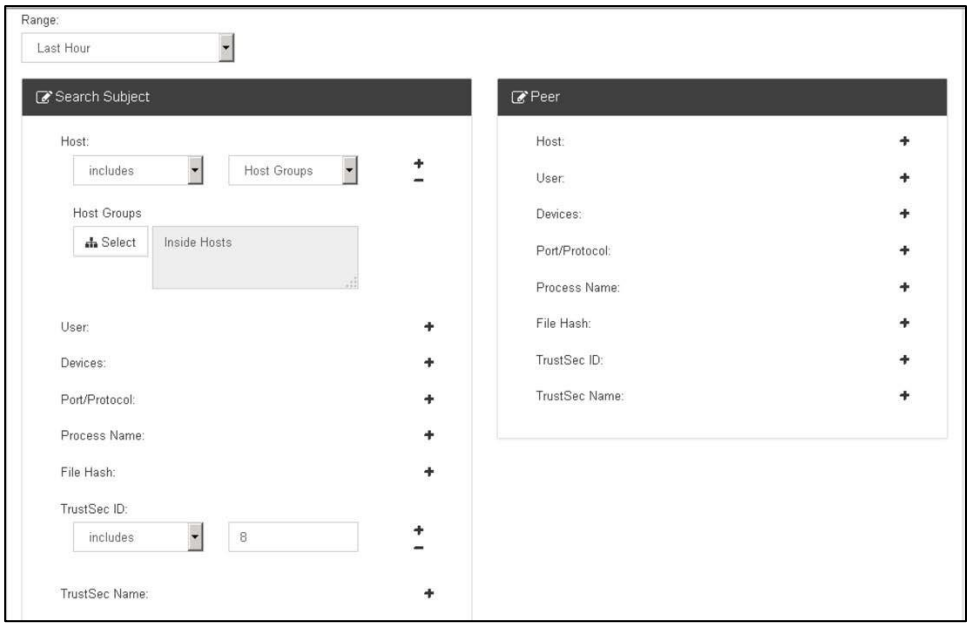
    a. **范围**：最后一小时

    b. **搜索对象**：

        i. **主机：(Host:)**> **包括** (**Includes**) > **主机分组 (Host Groups)** > **内部主机** (**Inside Hosts**)（如果尚未选择）

        ii. **TrustSec ID**: > **包括 (Includes)** > **8**

**图 44.** 高级搜索框



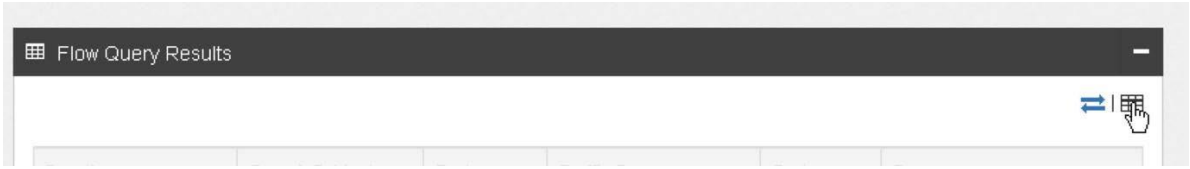

5. 点击**审核查询 (Review Query)**。

6. 验证是否正确设置参数，然后点击**运行 (Run)**。
7. 将显示搜索结果。在**流量查询结果 (Flow Query Results)** 面板中，从“搜索对象”(Search Subject) 列选择主机，然后点击 IP 地址旁边的省略号(**…**)。

**图 45.** “省略号”(Ellipsis) 对话框


8. 从随即显示的菜单上选择**查看详细信息 (View Details)**。
9. 验证 **TrustSec ID** 和**名称 (Name)** 是否出现在主机中**。**
10. 点击**关闭 (Close)**，以关闭**详细摘要窗口 (Detailed Summary Window)**。
11. 在“流量查询”(Flow Query) 结果面板的右上角，请点击网格图标，切换到**表格 (Tabular)** 视图。

**图 46.** 表格视图




12. 在**操作 (Action)** 面板，点击**管理列 (Manage Columns)**。
13. 在“流量表格列”(Flow Table Columns) 面板的**搜索对象**部分，勾选 **TrustSec ID** 和 **TrustSec 名称 (TrustSec Name)** 的复选框。

**图 47.** TrustSec 复选框


14. 点击**设置 (Set)**，将这些列添加到**流量查询结果 (Flow Query Results)** 面板。
15. 查看显示的信息，并考虑以下问题。

## 问题

1. TrustSec ID 8 组的 TrustSec 名称是什么？

# 场景 10　恶意软件调查

## 场景描述

在Swing 客户端存在一个“蠕虫跟踪”(Worm Tracker) 文档，可有助于确定和可视化呈现蠕虫样活动的系统。我们现在将对此进行检查。

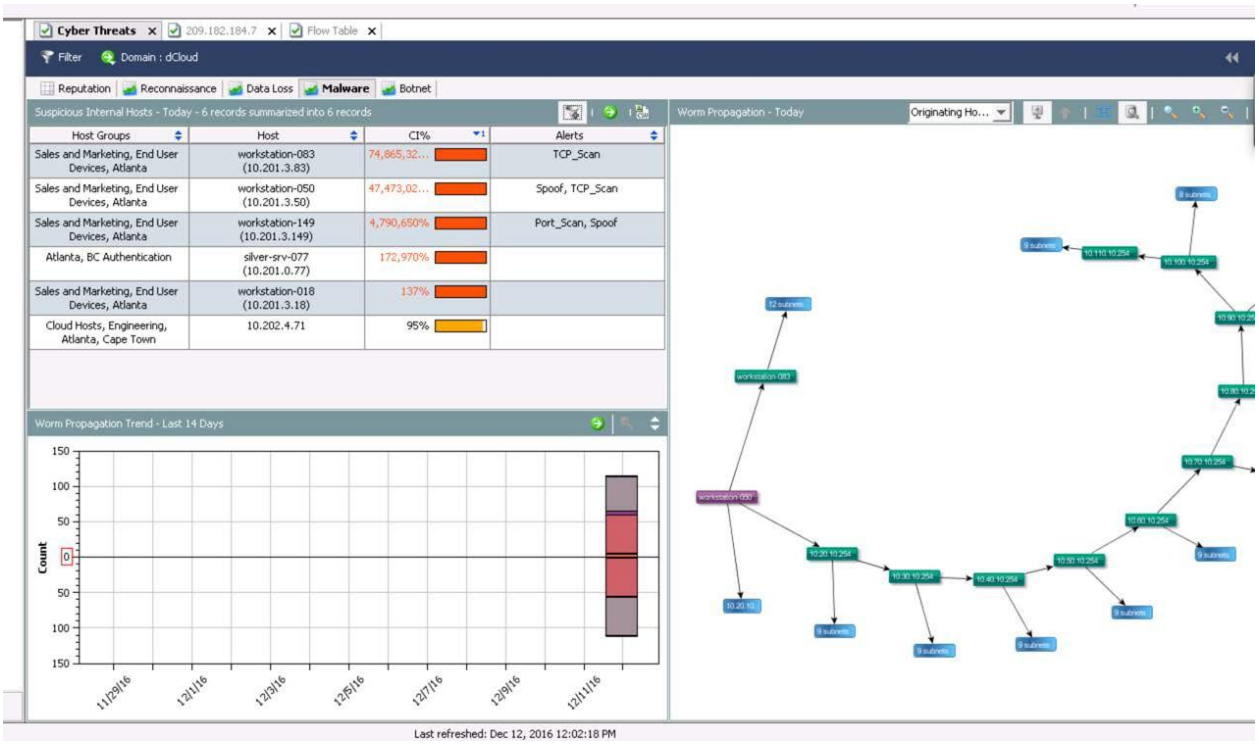
## 场景目标

在该场景中，您的目标是检查 Stealthwatch 对蠕虫在您的网络上进行信息传播的可视化能力。

## 步骤

1. 返回到Swing 客户端 Stealthwatch 管理控制台 (SMC) 界面。
2. 如有必要，请从**状态 (Status) > 控制面板 (Dashboards)** 菜单中重新打开**网络威胁控制面板 (Cyber Threats Dashboard)**，并查看该控制面板的**恶意软件 (Malware)** 选项卡。

**图 48.**　“网络威胁控制面板”(Cyber Threats Dashboard) >“恶意软件选项卡”(Malware Tab)




3. 将鼠标悬停在**蠕虫传播趋势 (Worm Propagation Trend)** 图的一些项目上。随着时间推移，是否可观察到趋势？大多数活动发生在何处？

4. 注意窗口右侧**蠕虫跟踪器 (Worm Tracker)** 显示的恶意软件传播的图形表示。**紫色矩形**是识别为传播恶意软件感染的源主机。**绿色矩形**是识别为与起源主机表现出相同行为的主机，因此表明存在感染的传播。**蓝色矩形**总结所扫描的子网和主机数量。
5. 显示的项目可能因太小而无法轻易辨认；点击**启用放大器 (Turn On Magnifier)** 图标，并将鼠标光标在图表上移动。再次点击该图标，以关闭放大器。
6. 将鼠标光标移到一个**紫色**矩形上，代表网络中的一个主要感染源。注意关于主机活动的更多信息弹出显示。
7. 右键点击紫色矩形，然后选择**主机快照** (**Host Snapshot**)。查看**身份、DHCP 和主机说明 (Identity, DHCP & Host Notes)** 选项卡中的信息，并思考如何将其用于事件响应。
8. 检测**安全事件 (Security Events)** 选项卡。从该主机上可以看到哪种扫描和其他行为？
9. 除网络威胁控制面板之外，关闭所有打开的选项卡，以在该场景结束时进行清理界面。

## 问题

1. 在恶意软件传播链条中倒数第二台主机的 IP地址是什么？
2. 它扫描的子网和主机有多少？

# 场景 11.　调查代理连接

## 场景描述

代理许可证功能便于 Stealthwatch 与思科的 WSA、McAfee、Bluecoat 和基于 Squid 的代理设备集成，有助于消除因代理产生的盲点。代理许可证功能通过使用从代理发送的 syslog 信息进行工作，并将其集成到 StealthWatch 的流量可视性中。该代理提供遭拦截的网络流量信息，并将其发送至 StealthWatch 系统。Stealthwatch 随后将收到的系统日志相互关联，并将其关联到代理前后通过网络设备收集的流量。

在此场景中，我们将使用代理许可证获取有关连接的其他信息，并且此类信息会流经具有可视化能力的代理 Stealthwatch。

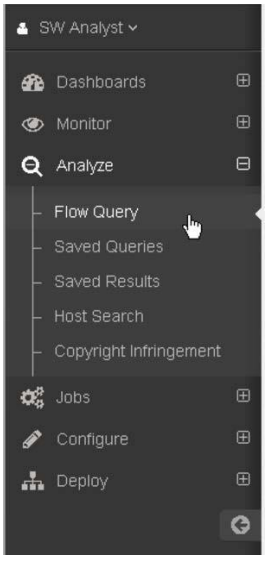
## 场景目标

围绕流经代理设备的网络连接，展开详细调查。

## 步骤

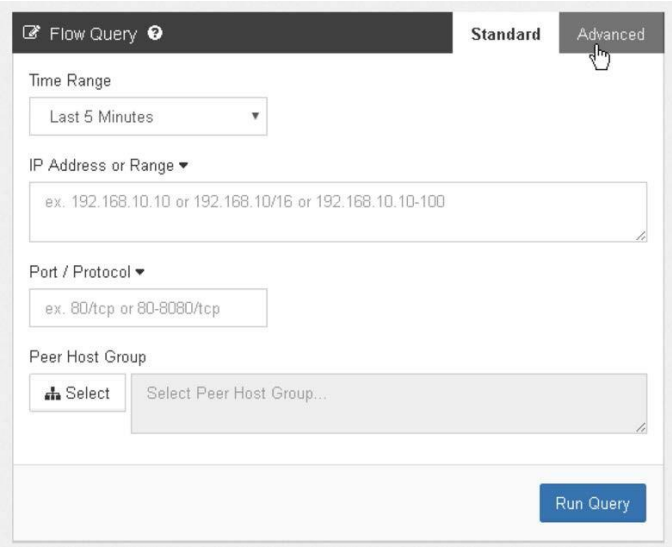
1. 此场景在 SMC WebUI 上进行。如有必要，最小化 Swing 客户端，因此打开控制面板的网络浏览器可以位于靠前位置。
2. 选择左侧导航面板的**分析 (Analyze) > 流量查询 (Flow Query)**。

**图 49.**　“分析”(Analyze) >“流量查询”(Flow Query)。




3. 选择**高级 (Advanced)** 搜索选项卡

**图 50.** 高级 (Advanced) 搜索选项卡




4. 设置以下过滤条件：

    a. **范围：**过去 8 小时

    b. 对于**搜索对象 (Search Subject)**

        i. 对于主机，选择：**包括，IP 地址/列表 (includes, IP Address/List)**

        ii. 在提供的复选框中输入 **10.20.30.40** 中。

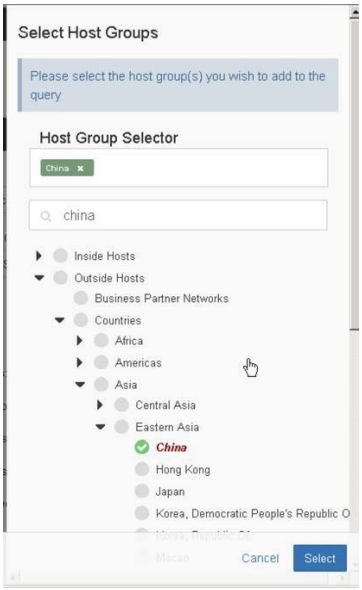
    c. **对等点:**

        i. 对于**主机 (Host)**，选择：**包括，主机组 (includes, Host Groups)**

            1. 在主机组下方，点击**选择 (Select)**

            2. 在打开的主机组选择窗格中，依次浏览并勾选复选框：**外部主机 (Outside Hosts) > 国家 (Countries) > 亚洲 (Asia) > 东亚 (Eastern Asia) > 中国 (China)。**

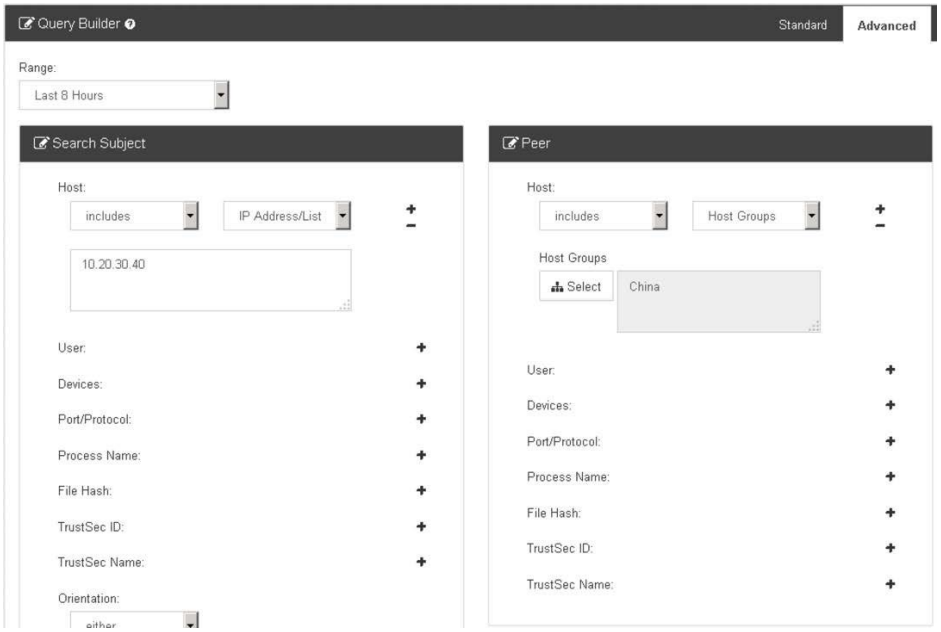
**图 51.** “外部主机”(Outside Hosts) >“国家”(Countries) >“亚洲”(Asia) >“东亚”(Eastern Asia) >“中国”(China)




**注意：**通过在该面板的**搜索 (Search)** 字段输入全部或部分名称，您可以搜索**中国 (China)** 拟主机组。

3. 点击**选择 (Select)**。

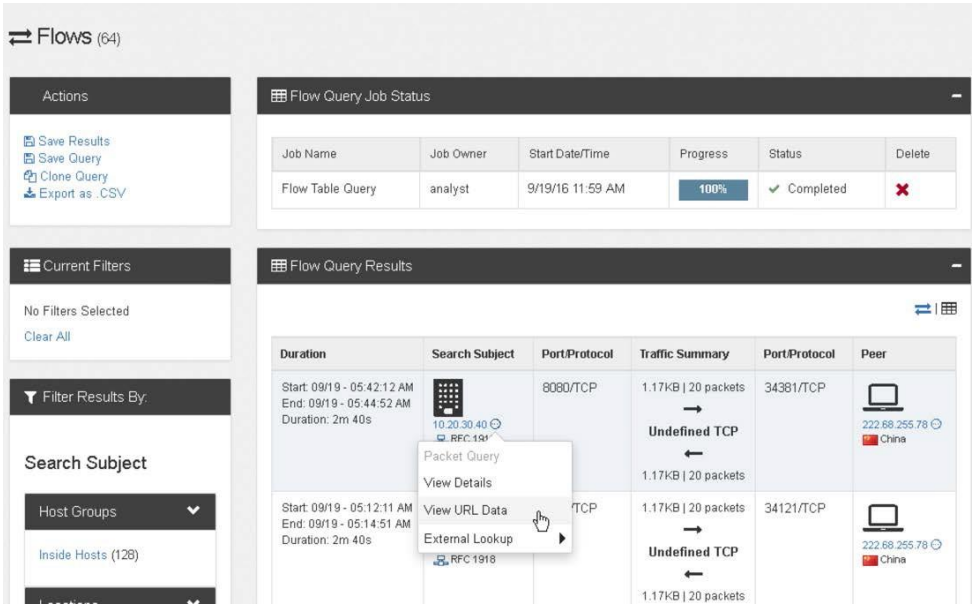
**图 52.** “高级查询生成器”(Advanced Query Builder)




4. 不理会其余部分的设置。
5. 点击**审核查询 (Review Query)**。
6. 验证您的查询设置，然后点击**运行 (Run)**。

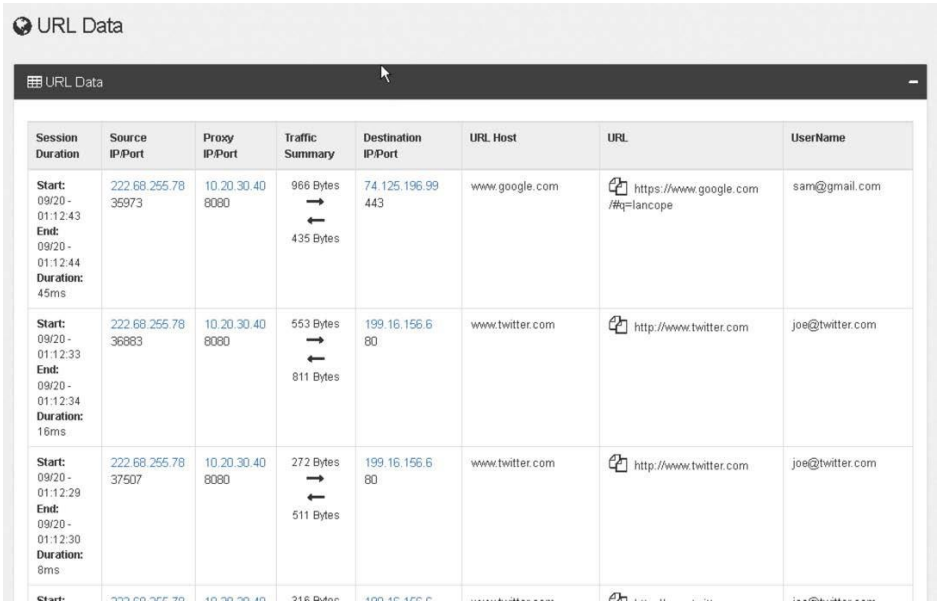
7. 在**流量查询结果 (Flow Query Results)** 面板中，将显示所有地理定位 IP 地址位于中国，在代理和主机之间的观测流量列表。

**图 53.** “流量查询结果”(Flow Query Results)




8. 在**流量查询结果 (Flow Query Results)** 面板中，点击代理 (**10.20.30.40**) IP 地址旁边的省略号(**…**)。
9. 在出现的下拉菜单中，点击**查看 URL 数据 (View URL Data)**。这方便您查看在该流量持续时间内该行所列**代理 (Proxy)** 和**对等点 (Peer)** 之间各连接的相关代理记录。
10. 将会显示 **URL 数据 (URL Data)** 页面，显示相关连接详细信息。

**图 54.** URL 数据




11. 查看各连接的详细信息，并考虑如下问题。

## 问题

1. “Mary”通过代理访问的是哪个网站？

# 场景 12　内部威胁检测

## 场景描述

当网络活动偏离常态，和当主机在网络上的行为异于平常时，这可能表明遭受攻击。除旨在通过网络进行扰乱活动的攻击外，越来越多的攻击，其目的在于访问并盗取目标网络所存储的信息。该信息可能是信用卡信息、个人记录、社会保险号、机密文件等。

## 场景目标

测试 StealthWatch 识别网络内部威胁的能力。

## 步骤

1. 此场景的第一部分在 SMC WebUI 上进行。最小化 Swing 客户端，这样打开 WebUI **控制面板 (Dashboard)** 的网络浏览器可以位于靠前位置。
2. 在控制面板顶部的警报类别，主要包含与内部威胁检测相关的两个类别：**数据收集 (Data Hoarding)**（用户窃取数据）和**泄露 (Exfiltration)**（用户向外发送数据）。
3. 在“控制面板”(Dashboard) 中，您可以点击警报下方的数字，深入了解任意一种警报，查看当前有效的警报。您也可将 WebUI 用于深入了解所有在网络上观测到的主机活动，以及哪些主机触发多个类别的警报。

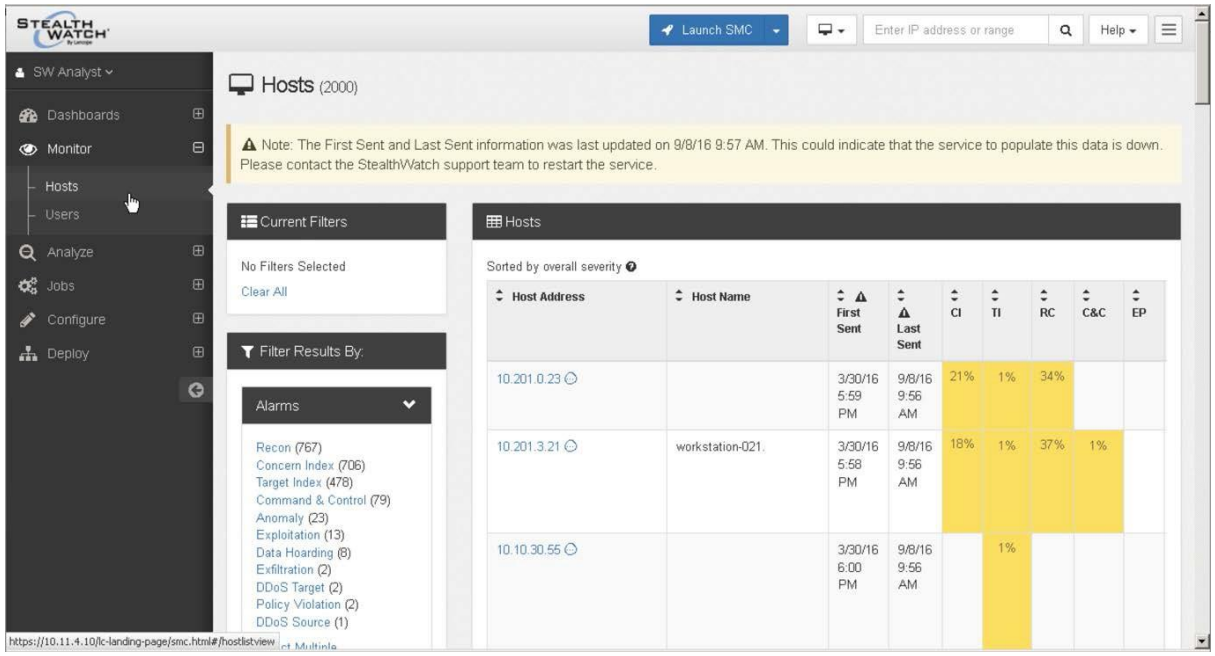
**图 55.** WebUI 显示示例


4. 点击左侧导航面板的**监控 (Monitor) > 主机 (Hosts)**。
5. 列表中设有显示 IP 地址和主机名的列。此外，也有与**控制面板 (Dashboard)** 所显示的警报类别相对应的列。

**注意：**您可能需要水平滚动表格，以查看所有列。

6. 鼠标悬停在列标题上，以显示警报名称和说明。

**图 56.** 主机列表示例

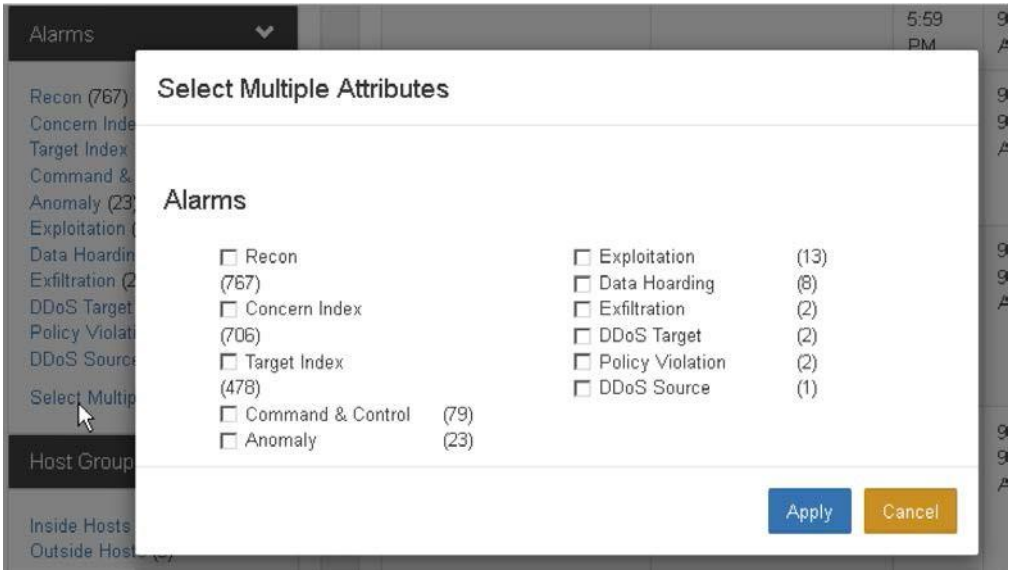



7. 默认情况下，列表按警报类别的严重性进行排序，因此警报最严重的主机会位于列表顶部。排序取决于每台主机的警报类别的汇总（组合）情况。
8. 要更改排序顺序，点击任意列标题的箭头。

**注意**：要恢复默认值排序，请点击表格顶部的**按整体严重程度排序 (Sorted by overall severity)**。

9. 页面左侧是筛选此列表的选项，便于您集中关注更为特定的主机。
10. 对于此场景，我们希望侧重于数据收集和泄露活动。通过以下方式，高亮显示这些主机：
    a. 在**按以下方式过滤结果 (Filter Results By)** 面板中，在**警报 (Alarms)** 项下：
        i. 点击**选择多个 (Select Multiple)**。
        ii. 选中**数据收集 (Data Hoarding)** 和**泄露 (Exfiltration)** 框。

**图 57.** 选择多个属性

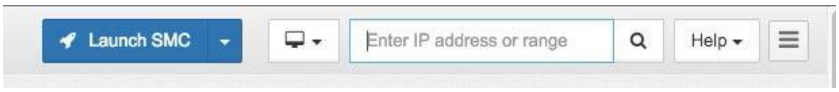



iii. 点击**应用 (Apply)**。

11. 注意触发这些警报的主机。注意有大量**数据收集/泄露**事件的主机。这可能表示存在可疑行为。
12. 点击主机 **10.201.3.149**。

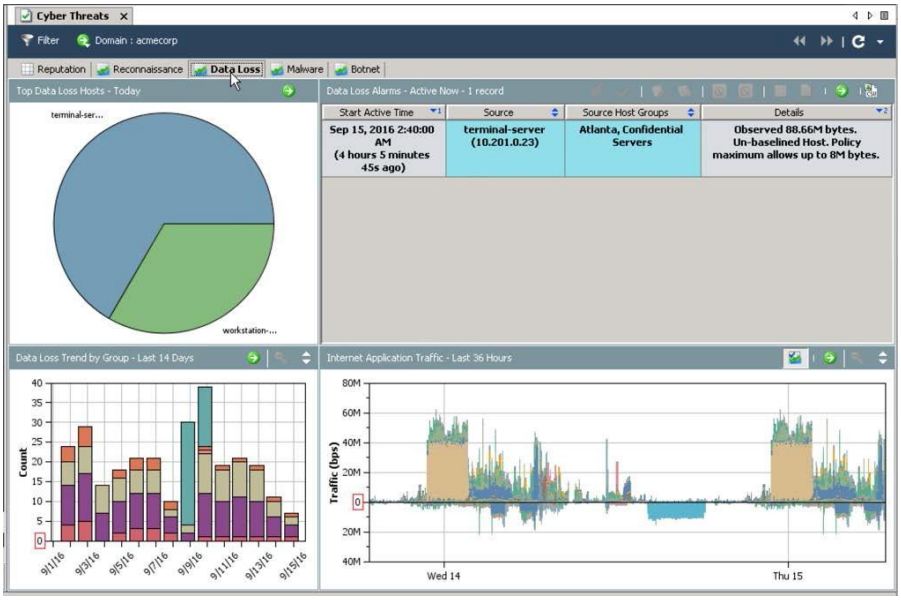
**注意**：如果 **10.201.3.149** 未触发任何数据收集或泄露事件，在此场景中，在页面右上角的搜索字段中输入主机 IP。

**图 58.** IP 地址或范围搜索框




13. **10.201.3.149 主机报告 (Host Report)** 页面打开。
14. 主机报告将围绕在您的网络上所观察到的主机活动，总结大量数据。提供主机所涉及的其他警报类别、主机摘要、用户登录、到其他内外组的流量等方面的信息。
15. 请在主机列表屏幕上随时测试其他触发警报的主机。
16. 当您完成时，点击左侧导航面板上的**控制面板 (Dashboard) > 网络安全 (Network Security)** 链接，以返回到 WebUI 控制面板屏幕。
17. 此场景的第二部分在 Swing 客户端上进行。返回到您的 Stealthwatch 管理控制台 (SMC) 界面。
18. 如有必要，请从**状态 (Status) > 控制面板 (Dashboards)** 菜单中重新打开**网络威胁控制面板 (Cyber Threats Dashboard)**，并查看控制面板中的**数据丢失 (Data Loss)** 选项卡。

**图 59.** “网络威胁控制面板”(Cyber Threat Dashboard) >“数据丢失”(Data Loss)




19. 在**排名靠前的数据丢失主机 (Top Data Loss Hosts)** 或**按组分类的数据丢失趋势 (Data Loss Trend by Group)** 中，选择当前或最近的可疑数据丢失示例。
20. **右键点击**该事件，并选择**警报表 (Alarm Table)**。什么事件触发警报？在事件源中是否存在一致的主题？
21. **右键点击**特定警报，然后选择**流量 (Flows)** > **关联流量表 (Associated Flow Table)**。可疑数据泄露的目的地是什么？
22. **右键点击**数据输出的目的地，针对目的地选择**主机快照 (Host Snapshot)**。在**标识 (Identification)**、**警报 (Alarms)**、**安全 (Security)** 和**安全事件 (Security Events)** 选项卡下方，您发现什么额外信息？
23. 除网络威胁控制面板之外，关闭所有打开的选项卡，以在该场景结束时进行清理界面。

## 问题

1. 用户活动常会造成 Stealthwatch 针对同一个事件产生多个警报。对于数据收集和泄露警报，Stealthwatch 可能会生成其他什么警报？

# 场景 13　创建审核追踪

## 场景描述

使用 WebUI 控制面板，您可以调查警报，例如“数据收集”(Data Hoarding)（可能会从多个来源收集用户数据）和“数据泄露”(Data Exfiltration)（用户在互联网上向一个或多个来源发送数据）。这可能意味着多种情况：

- 心怀不满的员工
- 窃取和销售商业秘密的人员
- 即将离职的员工
- 滥用特权证书的人员，受入侵的用户凭证

一旦确定潜在的内部威胁后，您可以围绕其活动建立审计追踪。

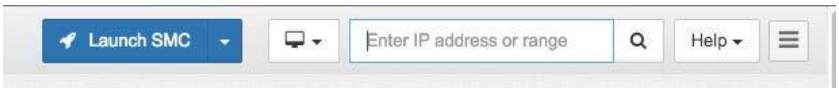
## 场景目标

在此场景中，您的目标是围绕可疑主机活动，建立审计追踪。

## 步骤

1. 此场景在 SMC WebUI 上进行。最小化 Swing 客户端，这样打开控制面板的网络浏览器位于靠前位置。
2. 由于我们之前将主机 **10.201.3.149** 视为可疑主机，因此我们将进行详细检查。
3. 在本例中，在控制面板中高级搜索字段中输入 **10.201.3.149** 地址。

**图 60.** IP 地址或范围搜索框

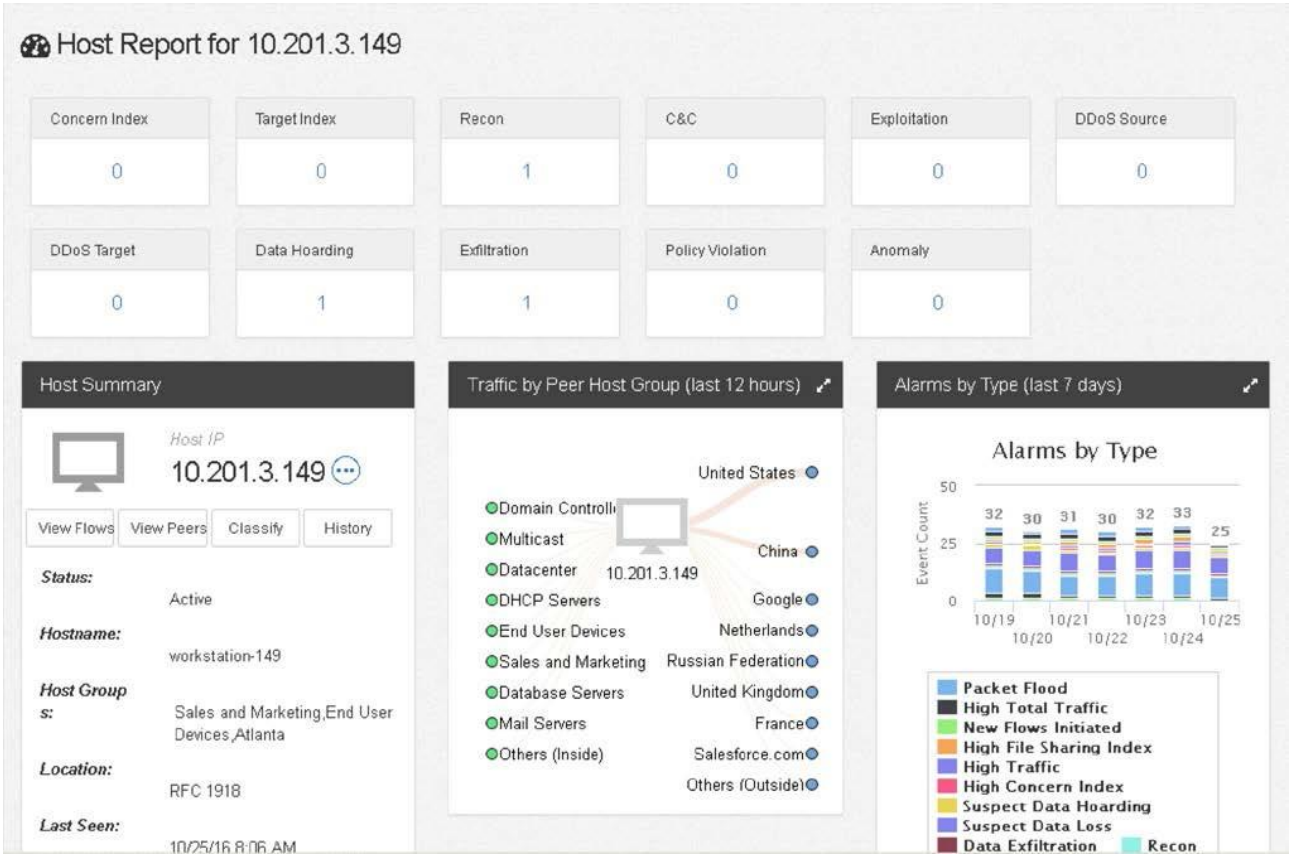



4. 在主机列表的主机地址列中，点击可疑主机的 IP 地址。

**图 61.** 主机列表示例

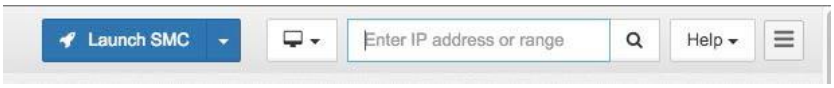

5. 在此，我们看到在主机报告中提供的摘要数据。在此屏幕顶部，是与您正在调查的主机相关的警报。此功能与控制面板中首页的警报列表类似，不同之处在于，它显示当前主机出现警报的详细信息。

**图 62.** 10.201.3.149 的主机报告



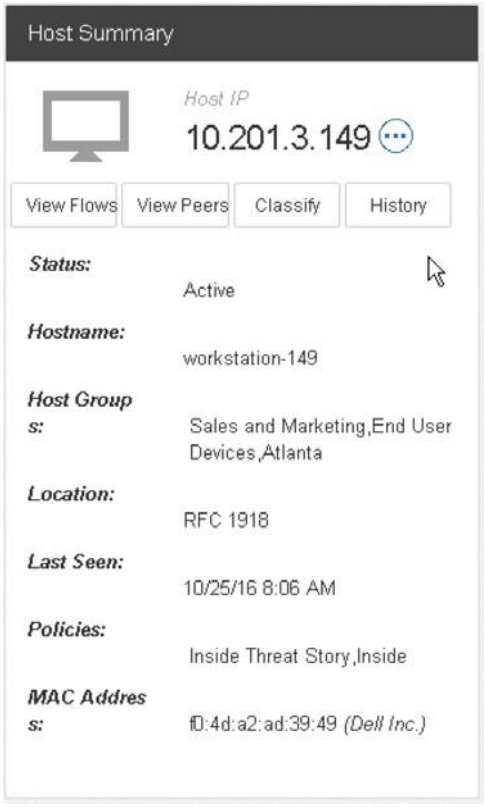
**注意：**仅可在主报告屏幕访问查看主机报告结果。一旦选择一个控制面板选项查看各个结果，其他选项可能就无法再看到。如果您跟随某个链接时偏离正在调查的主机，您可以在屏幕顶端再次搜索原始查询，返回到主机报告。

**图 63.** IP 地址或范围搜索框




6. **主机摘要 (Host Summary)** 面板提供主机名称、位置、最后一次检测到的时间、应用的策略以及主机组。

**图 64.** 主机摘要面板



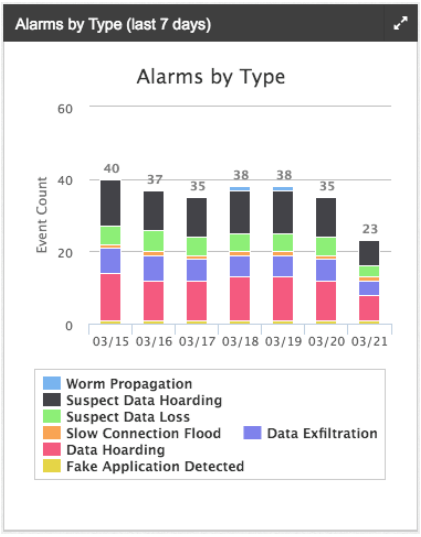

7. 我们还能看到**按对等主机组分类的流量 (Traffic by Peer Host Group)** 面板。这会指示此主机检索和发送流量的位置。在此窗口中，我们可以通过线条的粗细得知与主机进行最多数据转移的主机组对等设备。

**图 65.** 按对等主机组分类的流量


8. 点击列出的“对等主机组”(Peer Host Group)，系统会显示**流量查询 (Flow Query)** 屏幕，在此您可以查看过去 12 小时中主机和组内对等设备进行的所有通信。搜索时间和其他变量可根据需要进行调整。请随时尝试主机已经参与的活动。

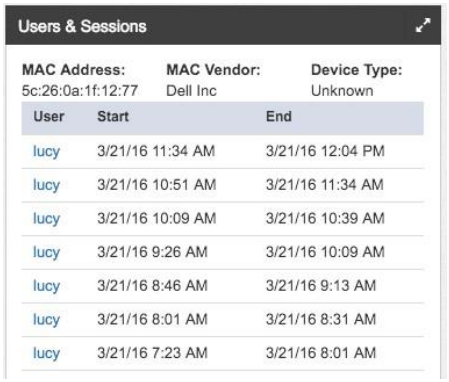
9. **按类型分类警报 (Alarms by Type)** 显示过去一周发生的与主机相关的警报。

**图 66.** 按类型分类警报




10. 在**用户和会话 (Users and Sessions)** 面板中，通过集成 ISE 或 Active Directory 所提供的信息，您可以看到该警报触发时用户登录的内容。

**图 67.** 用户和会话



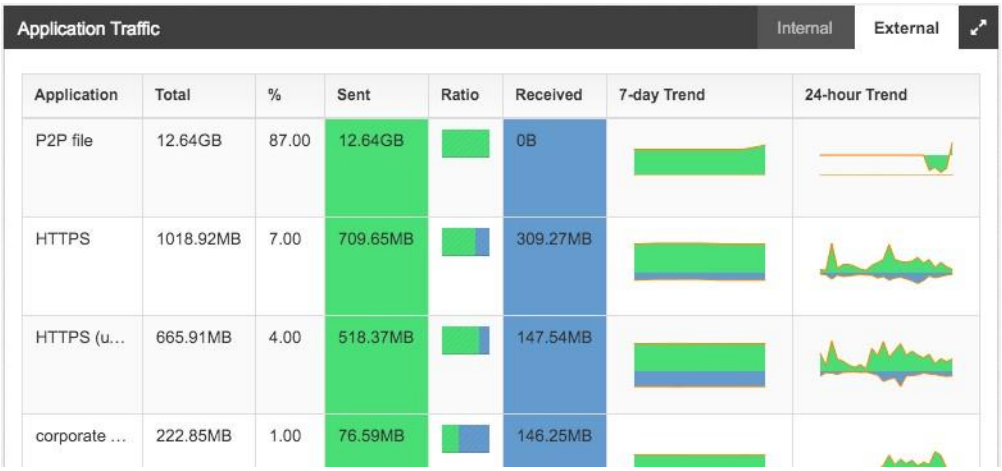

11. **应用流量 (Application Traffic)** 面板显示：

    a. 系统先显示到其他**内部 (Internal)** 主机的应用流量。最高的流量由主机产生，其次由已识别的应用产生。

**图 68.** 内部应用流量


    b. 在应用流量窗口点击**外部 (External)**，以获得由主机产生的流出网络的最高流量摘要，以及由已识别的应用产生的流量摘要。

**图 69.** 外部应用流量




c. **应用流量 (Application Traffic)** 面板包括 **7 天**和 **24 小时**的趋势。您可以将鼠标悬停在各列迷你图表的上，查看额外信息。此外，点击特定应用的 7 天或 24 小时趋势复选框，可以对所选时间段内的观测流量进行流量查询。

12. 注意大量的内部数据转移和大量的数据外流。也注意主机利用的其他应用流量，以及各应用的类型和数量。
13. 返回到**主机摘要 (Host Summary)** 面板，点击**查看流量 (View Flows)** 获取更多信息，并快速回答有关主机最近活动的其他问题。默认情况下，查询搜索前 5 分钟内的所有活动。
14. 要确保显示某些活动，您会希望在**范围** (**Range**) 字段中查询的时间范围更长。将该设置更改为 8 小时。
    a. 点击**查看查询 (Review Query)**，以验证设置。
    b. 点击**运行** (**Run**)，以执行查询。
15. **流量查询结果 (Flow Query Results)** 面板显示该主机在内部和外部参与的所有通信。查看所观察活动的类型和数量。
16. 当您完成后，点击在**搜索对象 (Search Subject)** 列正在调查的主机 IP 地址，返回到主机报告 (Host Report)。
17. 通过使用 Web UI，您可以收集所有必要信息，帮助确定为事件所应采取的适当措施。

## 问题

1. 哪些用户登录到我们的相关主机中？
2. 我们的调查对象从哪台内部主机转移最多的数据？
3. 相关主机与哪两台外部主机组产生最多的流量？
4. 相关主机向哪些外部主机转移最多的数据？

# 附录 A. 其他资源

您可以在以下 URL 中查看与本演示所含主题相关的其他有用信息：

http://www.cisco.com/go/stealthwatch

**美洲总部**
Cisco Systems, Inc.
加州圣何西

**亚太地区总部**
Cisco Systems (USA) Pte.Ltd.
新加坡

**欧洲总部**
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。 地址、电话号码和传真号码均列在思科网站 **www.cisco.com/go/offices** 中。