控制面板

全局威胁警报（以前称为认知情报）功能可帮助您对进行中或试图在您的网络中运行的复杂隐秘攻击进行快速检测和做出响应。此功能自动识别和调查可疑或有恶意的基于 Web 的流量。它可以识别已确认的威胁和潜在的威胁，使您能够快速补救感染并缩小攻击的范围和减少损害，无论是已知的威胁活动已在多个组织中传播，还是您从未见过的独特威胁。

作为基于云的服务，全局威胁警报分析现有网络安全解决方案生成的信息，无需额外的硬件或软件。它归零绕过安全控制的恶意活动。

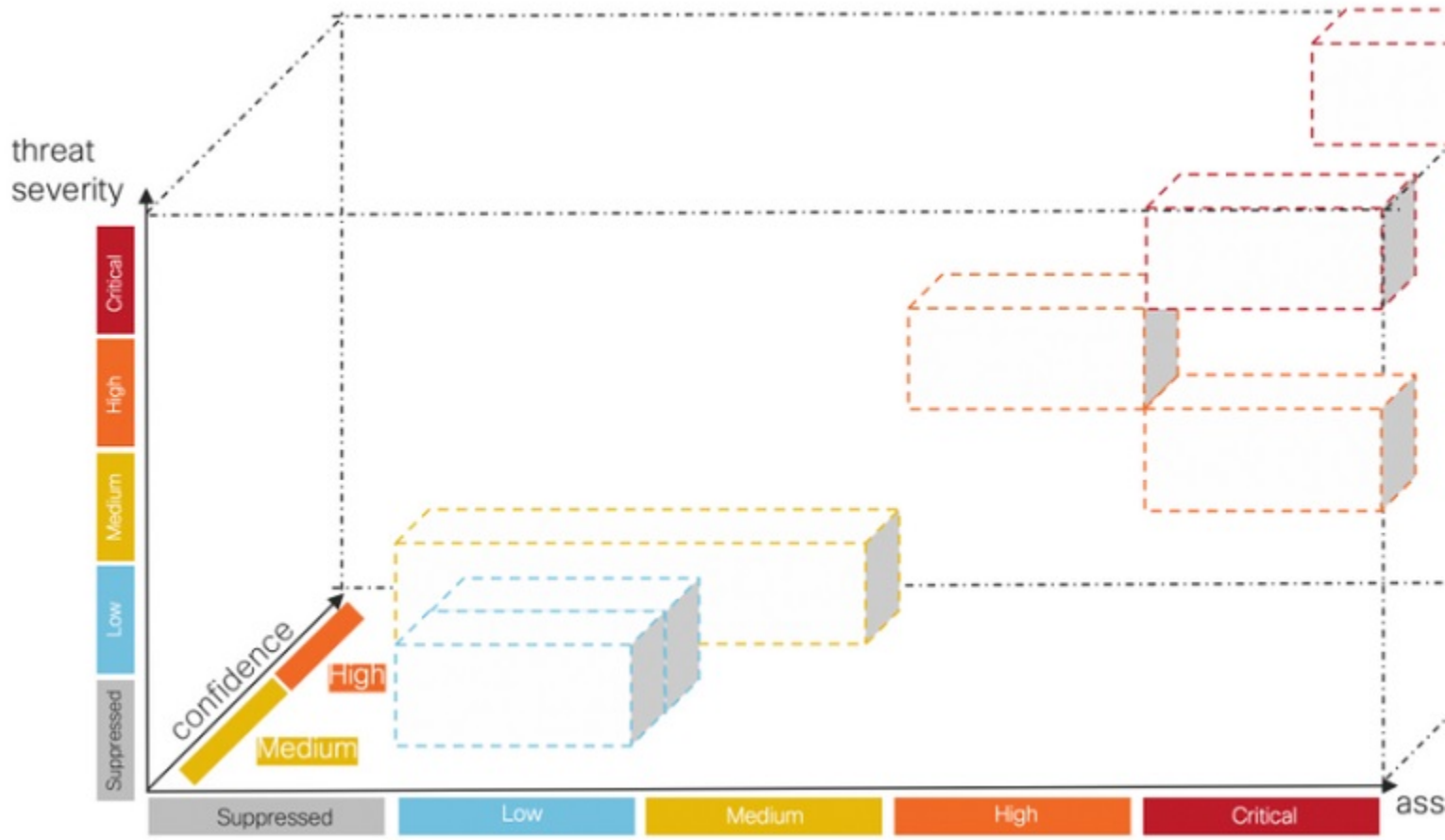
使用机器学习和网络统计模型，全局威胁警报创建正常活动的基准并识别网络中发生的异常流量。它分析设备行为和网络流量以查明命令和控制通信和以及数据泄渗露。

全局威胁警报根据观察吸取教训，以适应持续的漏洞识别，降低重复攻击或持续感染的风险。它通过与多个思科安全产品集成的基于 Web 的直观门户提供信息，以便您可以评估入侵的严重性和范围，了解威胁的任务及其工作原理，并立即采取行动。

概述

我们的分析引擎将机器学习应用于传入数据流，并将检测结果投放到 3D 空间中：

图 *1:*



- **威胁严重性维度**。威胁的严重性如何？已确认的威胁及其严重性。为了更好地与贵组织针对单个威胁类型的风险状况保持一致，您可以选择调整单个威胁的预定义严重性。
- **资产值维度**。资产的价值如何？如果连接到网络的所有设备并非同等重要，您可以选择调整单个资产组的商业价值，以优先检测更重要的设备。
- **置信度维度**。我们对裁决是否有信心？我们对我们的算法对客户环境中观察到的单个威胁做出的裁决充满信心。在某些情况下，我们观察到的行为表现足以确定我们的裁决。在其他一些情况下，尽管症状类似，但实际证据可能是粗略的。因此，误差容限会增加。

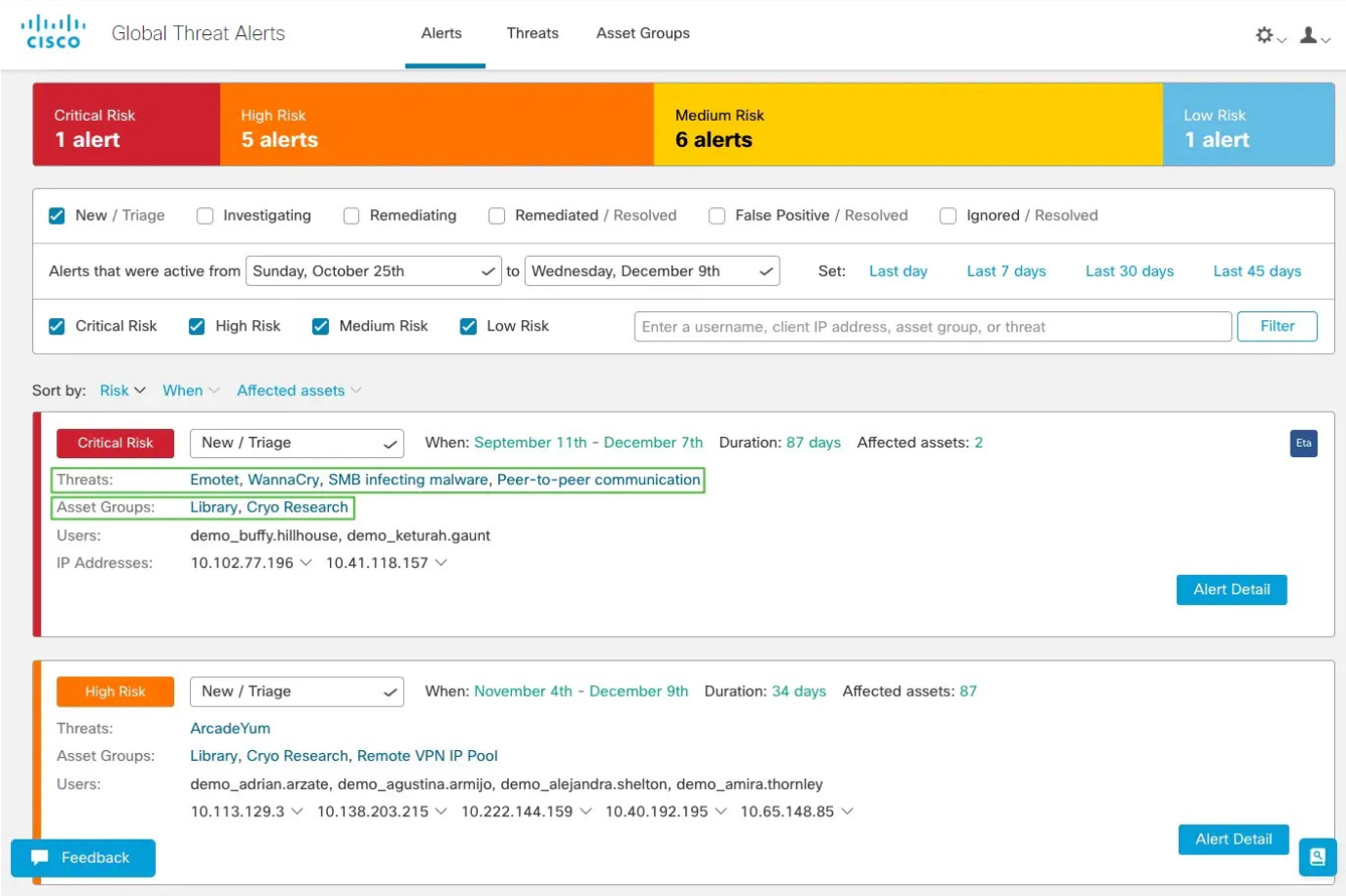
我们的融合算法使用这些检测来识别具有相似威胁及预测的集群，以计算其风险级别。然后，我们的Web门户会将这些作为安全警报显示在按风险级别划分的优先级列表中。每个警报都指向您的网络上受到的威胁，代表调查和后续补救的自然工作单元。

调查警报

步骤 1 点击**警报**选项卡以查看网络上的所有活动警报。每个警报都显示在自己的卡上。

a) 每个警报卡汇聚了一个或多个威胁，这些威胁同时影响网络上具有类似商业价值的一组资产。

图 *2:*



- **威胁**。一起出现的不同威胁。
- **资产组**。这些威胁发生在属于具有类似商业价值的这些资产组的终端上。

b) 风险级别基于威胁的严重性级别和资产组的商业价值。风险级别越高，表示威胁严重影响网络上的宝贵资产的风险越高。

步骤 2 风险级别较高的警报卡其排列顺序更接近列表顶部。通过根据警报的风险级别响应警报并首先调查风险较高的警报，以确定分析的优先级。

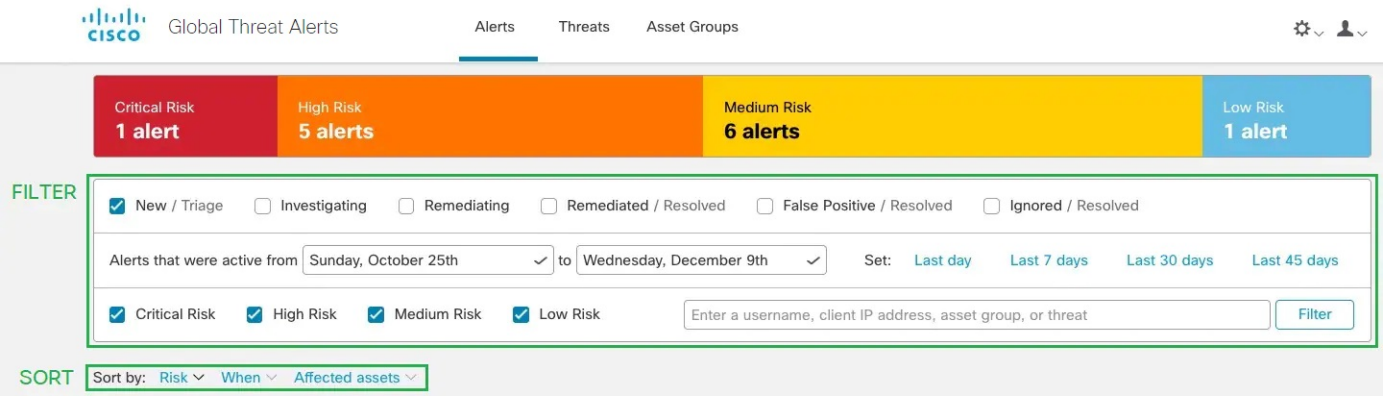
- 严重

- 高
- 中
- 低

注释　　警报卡可以动态更改，例如当新威胁添加到组或资产组商业价值，或者威胁严重性发生更改时。

步骤 3 您可以通过选择状态、期限、风险级别、用户名、IP 地址、资产组和/或威胁来**筛选**显示特定警报。您还可以选择按期限、风险级别或受影响资产的数量**排序**。

图 *3:*



步骤 4 通过更改警报的状态**新建/分类**，开始警报调查。

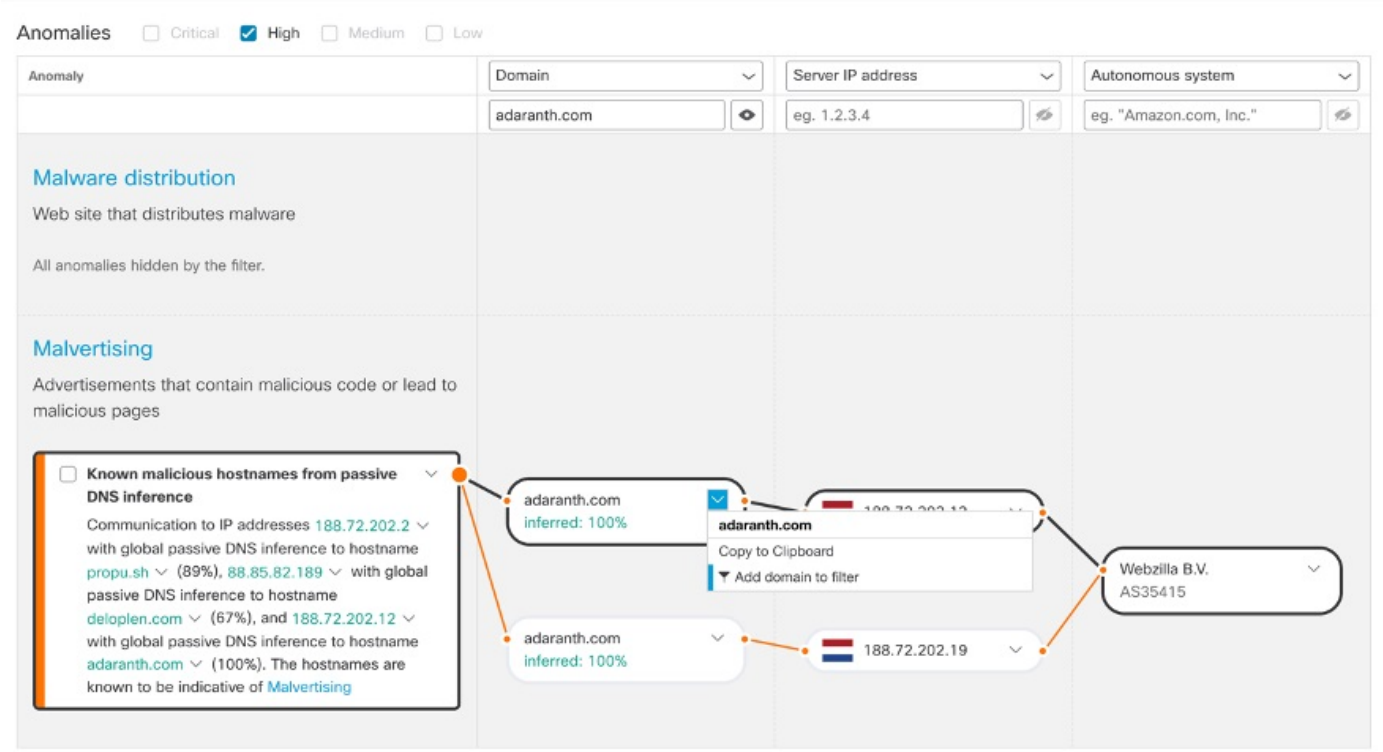
注释　　当其状态不再为**新建/分类**时，警报卡将保持不变且稳定，以便于调查。

步骤 5 点击**警报详细信息**以获取有关每个检测到的威胁和受影响资产的其他内容。

- 触发并导致识别此威胁的安全事件
- 资产与之通信的 IP 地址和域
- 哪些特定 IoC 表示该恶意行为
- 机器学习算法分配给此检测的置信度级别

步骤 6 为一个用户选择其中一个特定事件会将您转到安全事件视图，您可以在其中查看触发恶意检测的特定事件详细情景。

图 *4:*

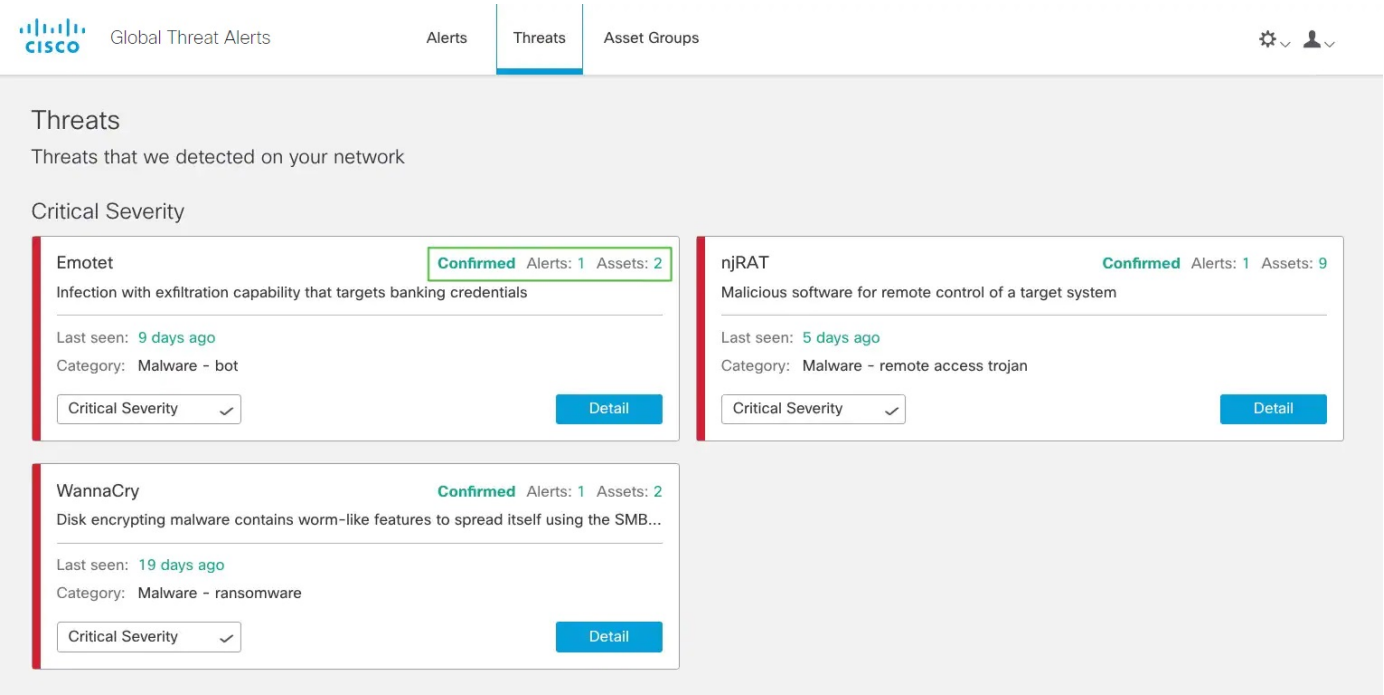


提示 点击下拉箭头，并将此 IoC 复制到剪贴板，以简化后续调查步骤。

调查威胁

步骤 1 点击**威胁**选项卡，查看在网络上报告并按严重性划分优先级的威胁列表。每张卡代表将在警报中分组的不同威胁。

图 *5:*



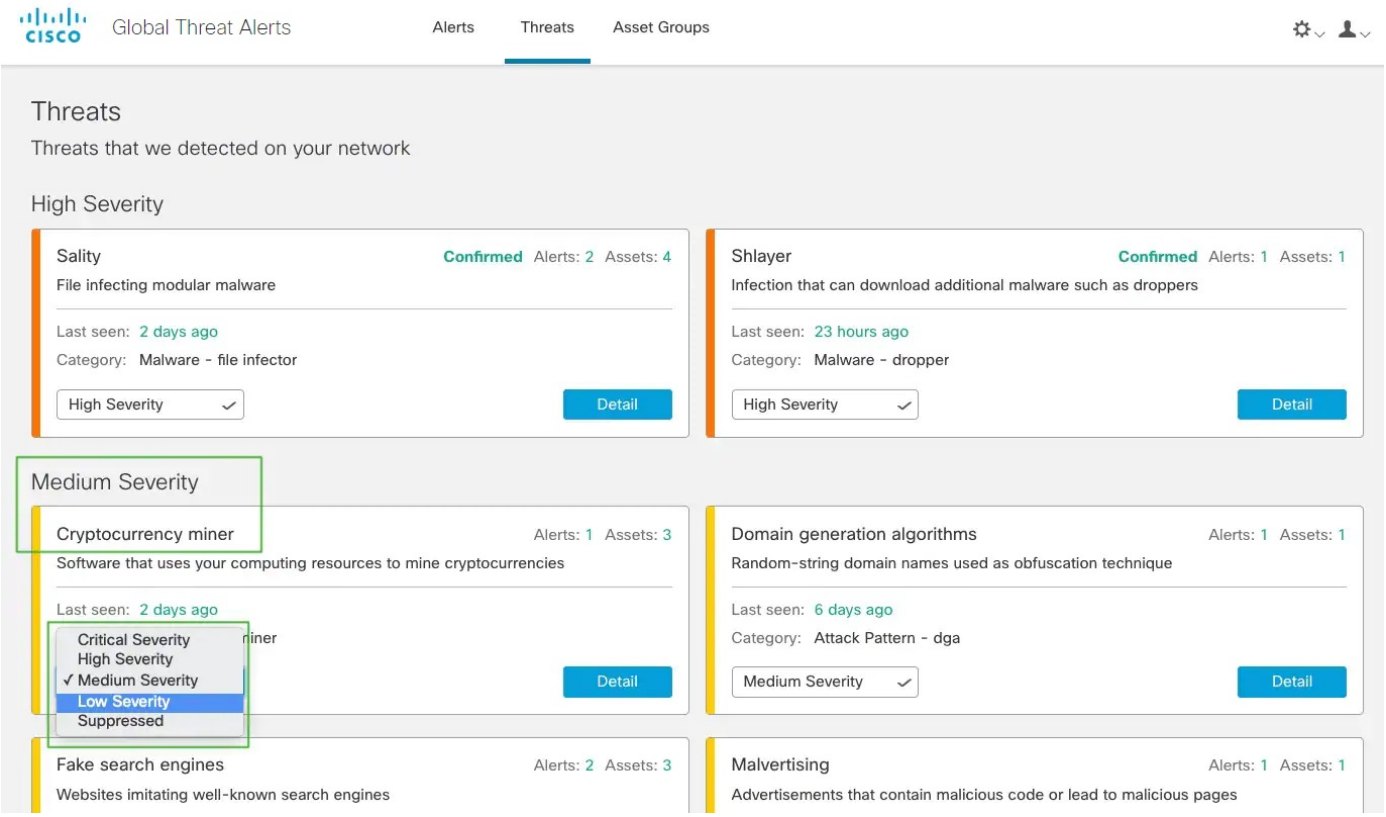
步骤 2 一种特定类型的威胁可能涉及多个警报。卡上有一个计数器，用于指示此特定类型威胁涉及的警报数量以及受此威胁影响的资产数量。

步骤 3 标记为**已确认**的威胁卡表示我们对威胁及其严重性具有高置信度；我们已在流量中看到至少一个与特定恶意行为相关的危害表现 (IoC)。此 IoC 已由一组威胁研究员确认。**已确认**威胁中的说明详细介绍了此警报对您的业务的影响。

步骤 4 您可以根据网络特定条件和业务需求调整威胁的严重性。

- 因此，包含此类威胁的所有**新建/分类**警报将重新计算其风险级别，并使用资产值和置信度对新严重性进行加权。
- 然后，风险级别的任何变更都会影响**新建/分类**警报的相对顺序。
- 例如，如果您降低威胁的严重性，则相关警报风险级别将降低，并且相关警报卡在**警报**选项卡的列表中显示的位置将更低。
- 点击下拉列表以调整威胁的严重性：

图 *6:*



注释 不再处于**新建/分类**状态的所有其他警报不受威胁严重性变化的影响；它们保持不变和稳定，以便于调查。

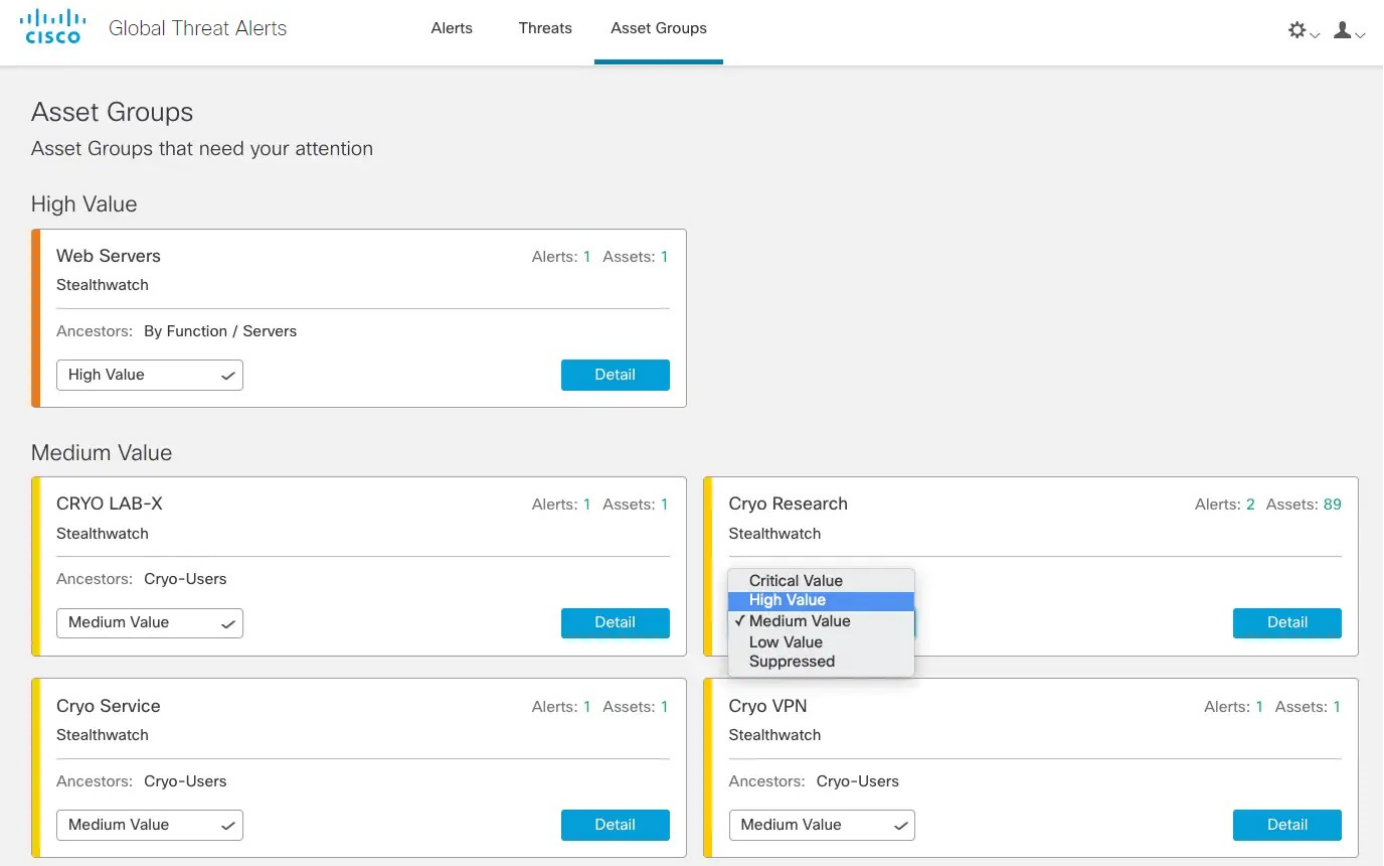
资产组

步骤 1 点击**资产**选项卡以查看将其流量发送到全局威胁警报的所有资产组。每张卡代表一组资产，其全局威胁警报报告至少一个警报。

步骤 2 确定资产组对您的组织的重要性或价值。您可以选择调整资产组的商业价值。

- 因此，影响此资产组的所有**新建/分类**警报将重新计算其风险级别，并使用严重性和置信度对新资产值进行加权。
- 然后，风险级别的任何变更都会影响**新建/分类**警报的相对顺序。
- 例如，如果您增加资产组的商业价值，则相关警报风险级别将提高，并且相关警报卡在**警报**选项卡的列表中显示的位置将更高。
- 点击下拉列表以调整资产组的商业价值：

图 *7:*



注释　　不再处于**新建/分类**状态的所有其他警报不受威胁严重性变化的影响；它们保持不变和稳定，以便于调查。

步骤 3 您可以选择通过将商业价值更改为**已抑制**来抑制资产组。在**已抑制网络**卡上，您可以点击**打开应用设置**以定义要抑制的特定 IPv4 资产或整个子网。

注释　　在属于已抑制组的资产上检测到的威胁将不再发出警报。已抑制资产组在**资产**选项卡中继续可见。

图 *8:* 受抑制网络