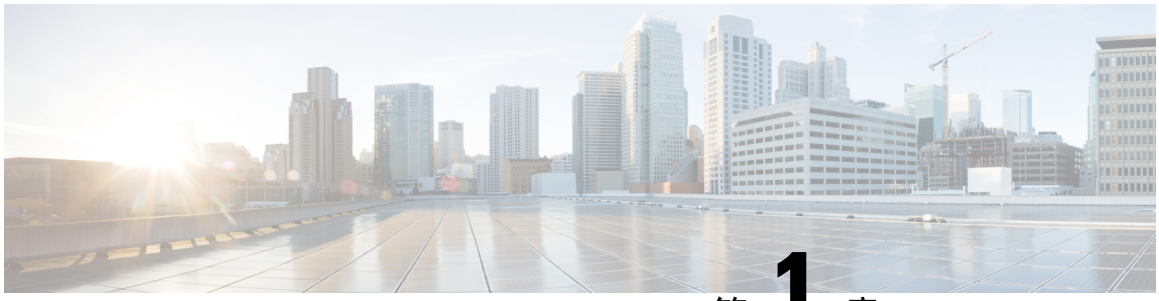
Secure Network Analytics 中的全局威胁警报

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

目录



第 1 章

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。

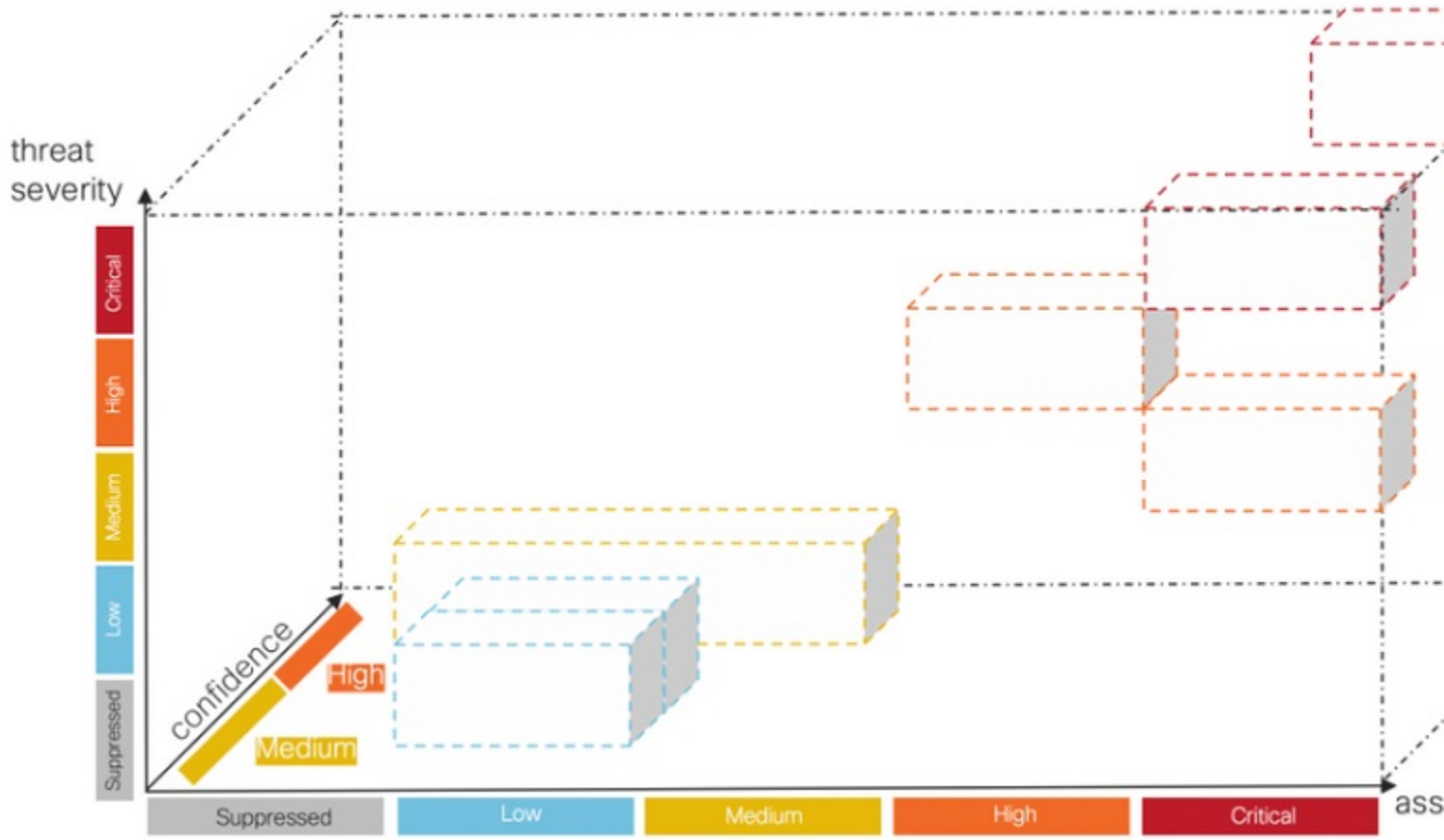
使用机器学习和网络统计模型，全局威胁警报创建正常活动的基准并识别网络中发生的异常流量。它分析设备行为和网络流量以查明命令和控制通信和以及数据泄渗露。

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。

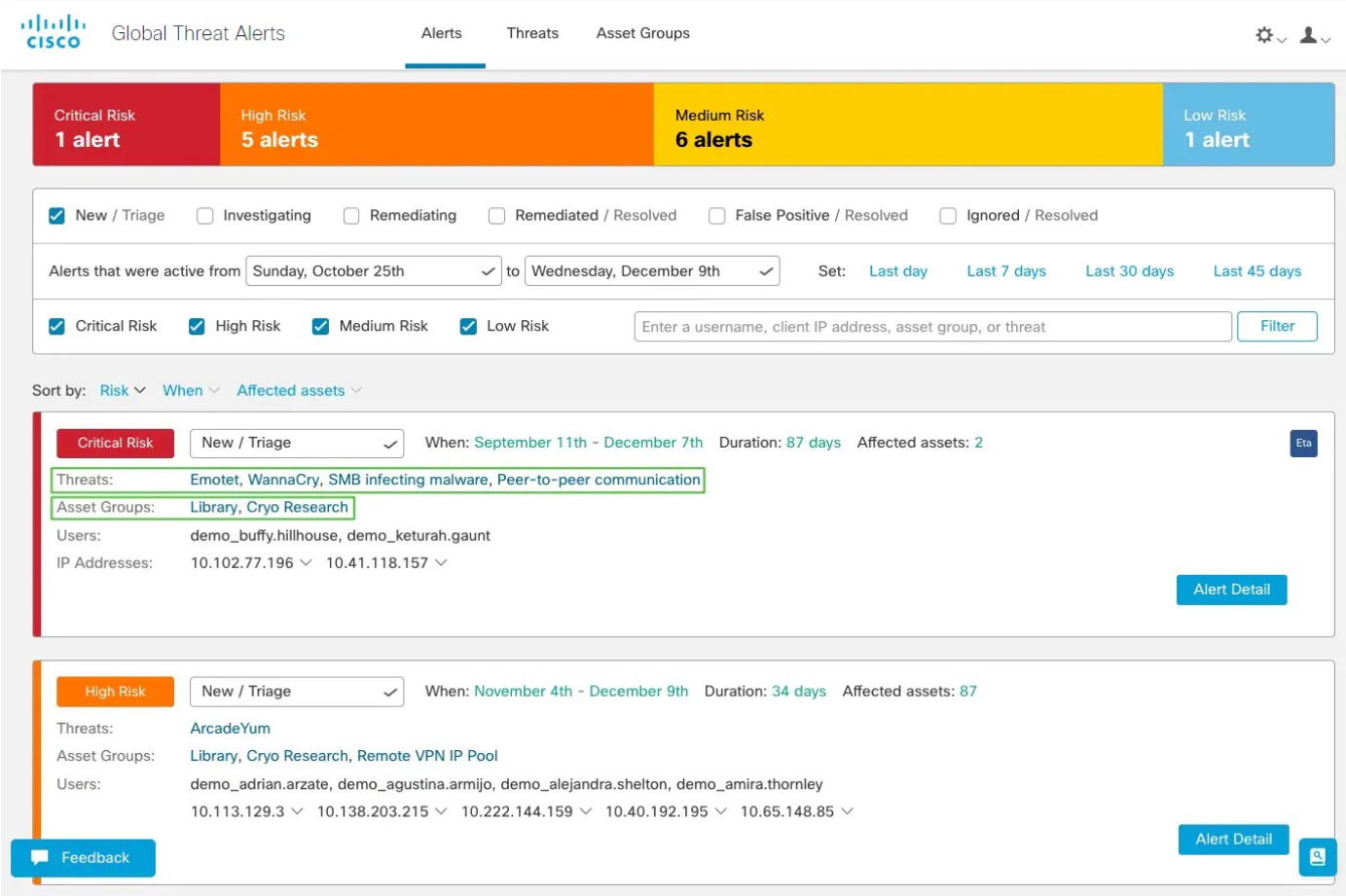
我们的融合算法使用这些检测来识别具有相似威胁及预测的集群，以计算其风险级别。然后，我们的Web门户会将这些作为安全警报显示在按风险级别划分的优先级列表中。每个警报都指向您的网络上受到的威胁，代表调查和后续补救的自然工作单元。

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。

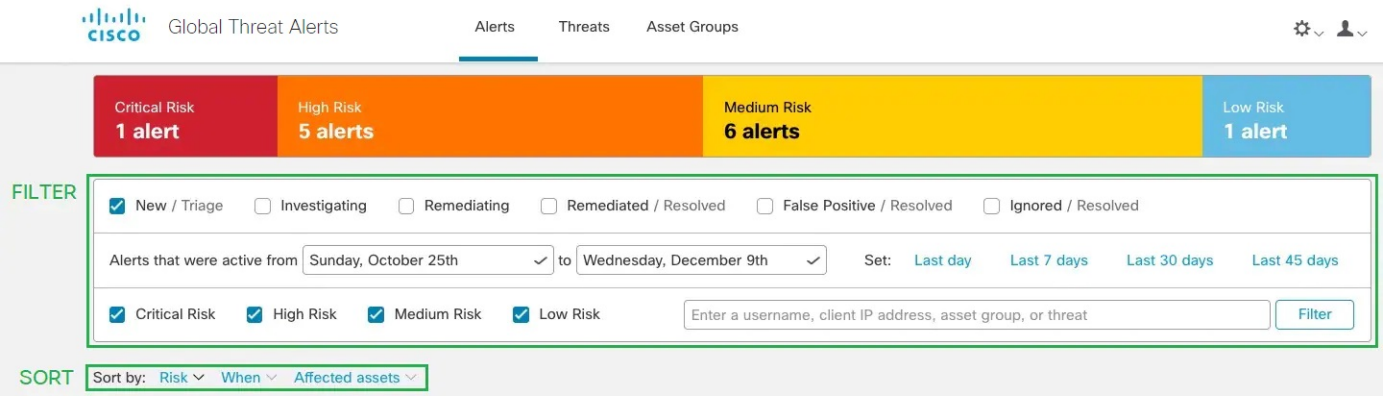
- 严重

- 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。

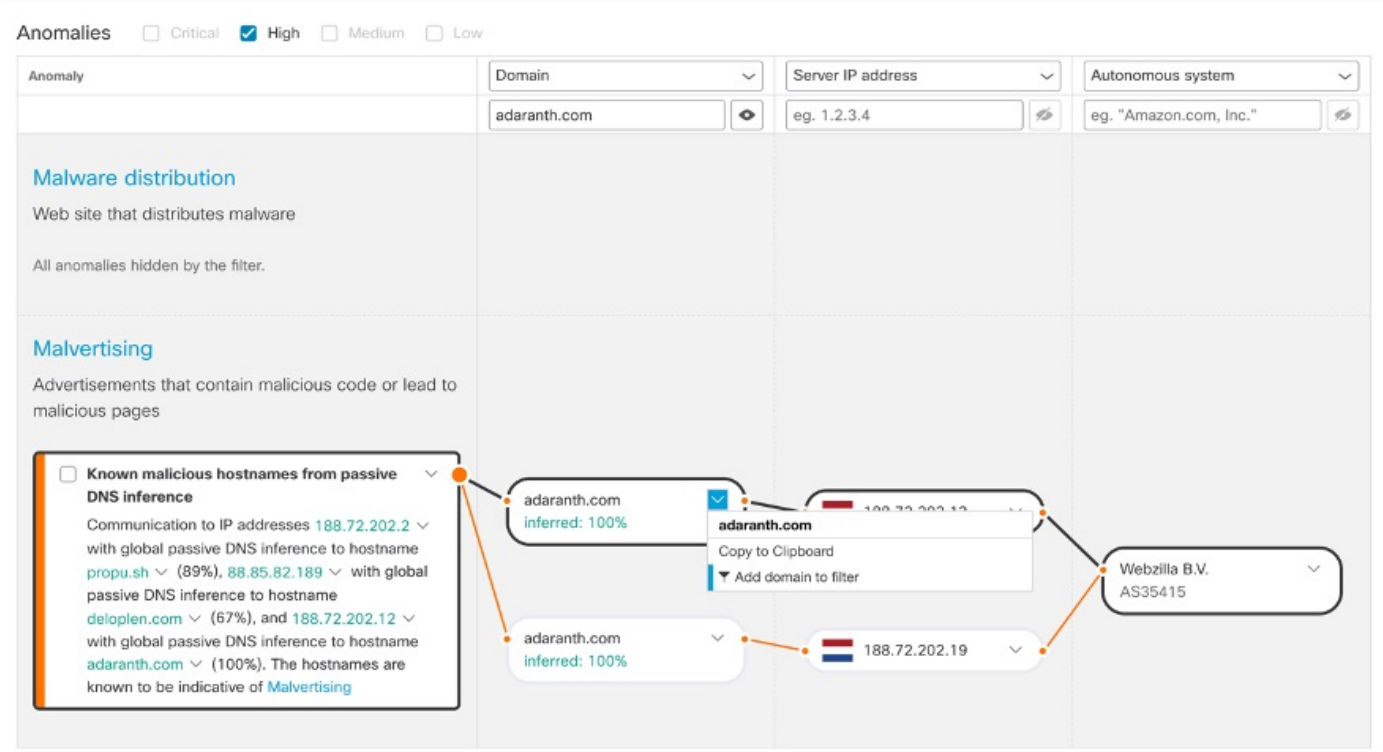
注释　当其状态不再为**新建/分类**时，警报卡将保持不变且稳定，以便于调查。

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:*

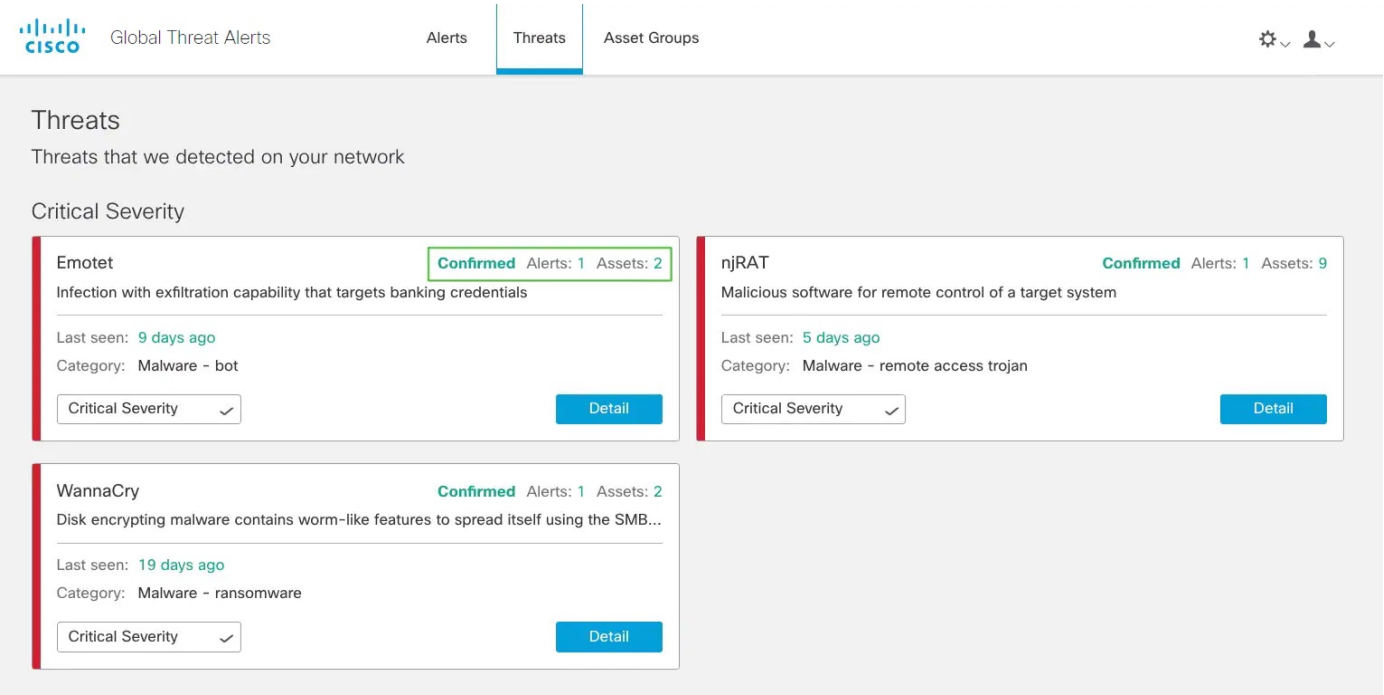


提示 点击下拉箭头，并将此 IoC 复制到剪贴板，以简化后续调查步骤。

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:*



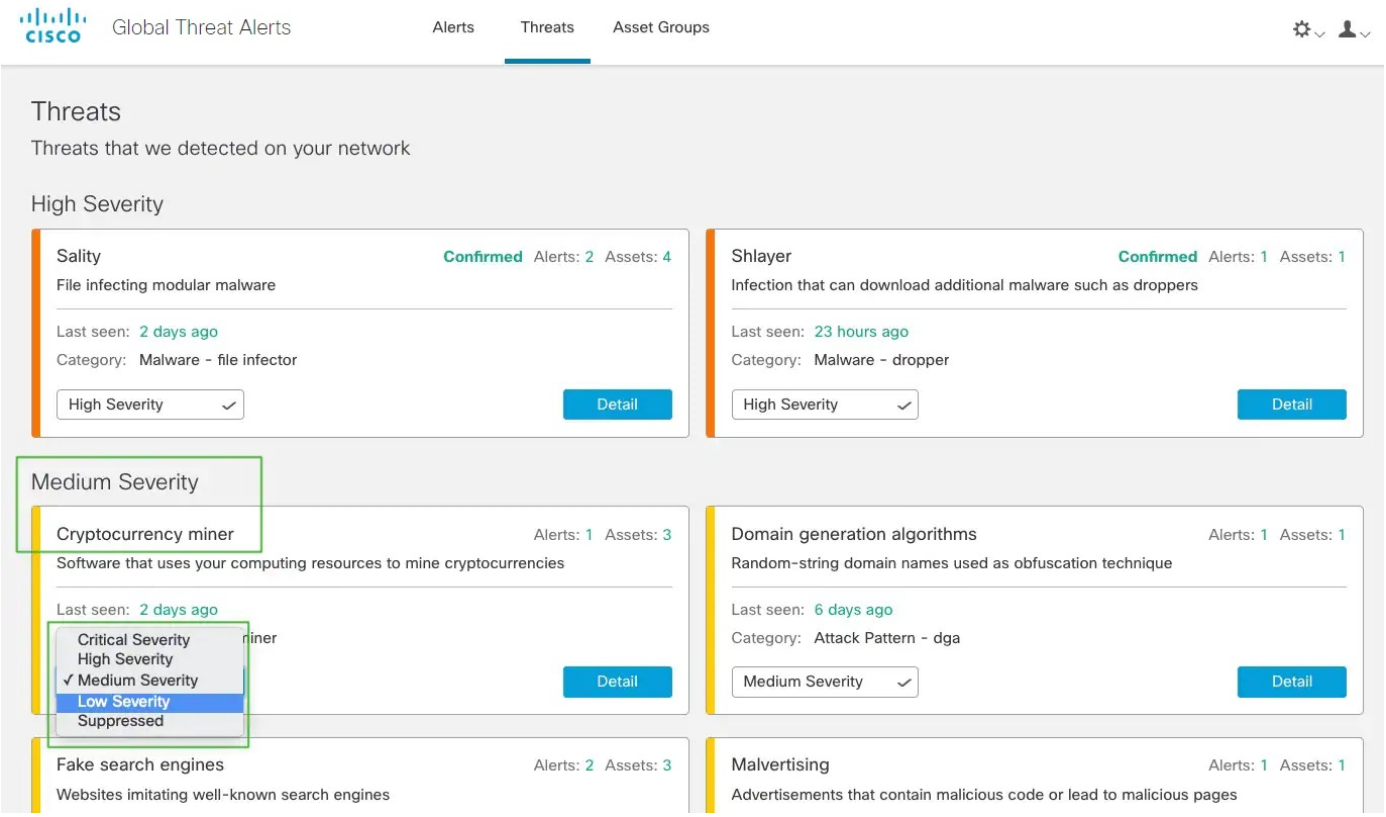
步骤 2 一种特定类型的威胁可能涉及多个警报。卡上有一个计数器，用于指示此特定类型威胁涉及的警报数量以及受此威胁影响的资产数量。

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。

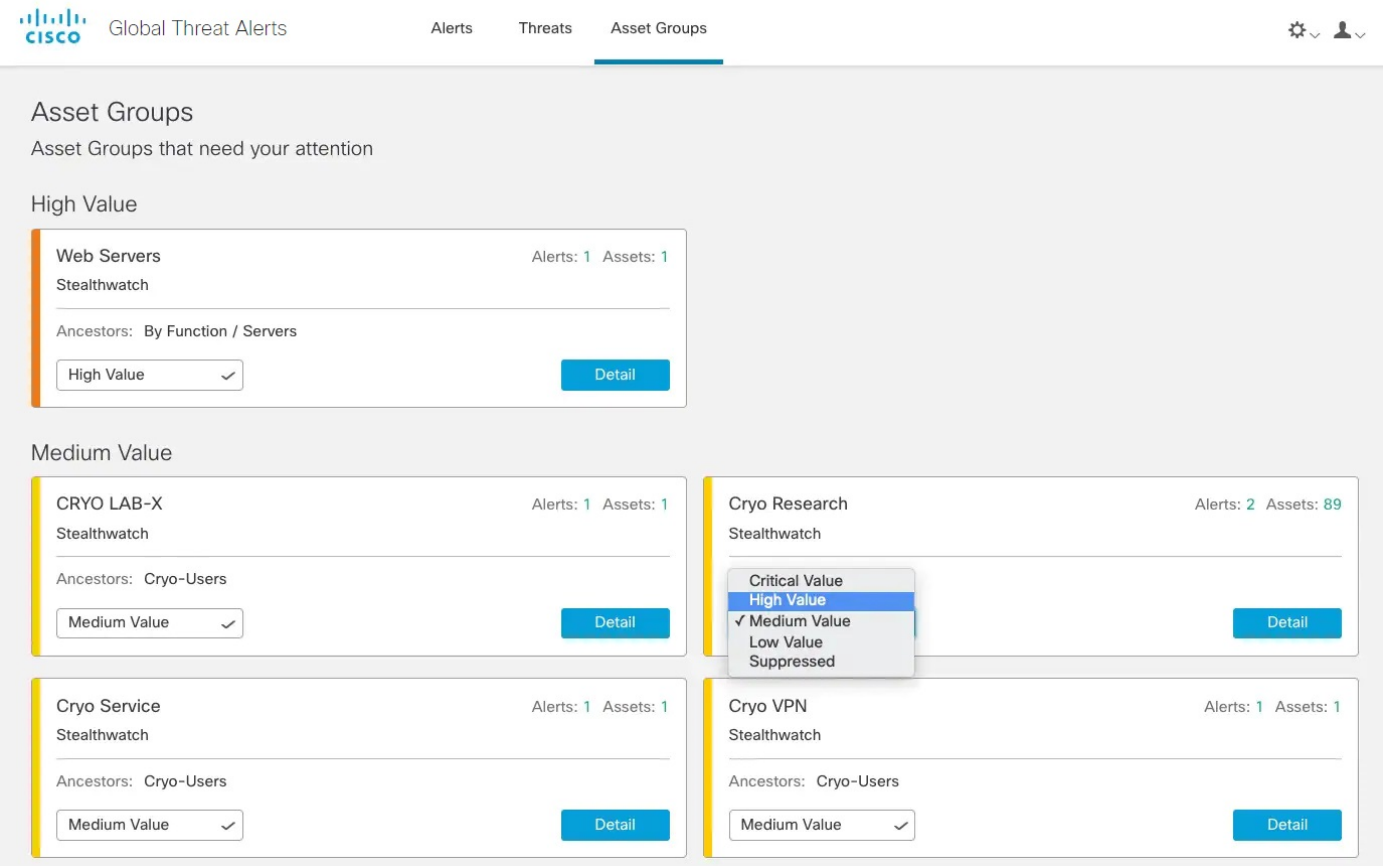
资产组

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:*

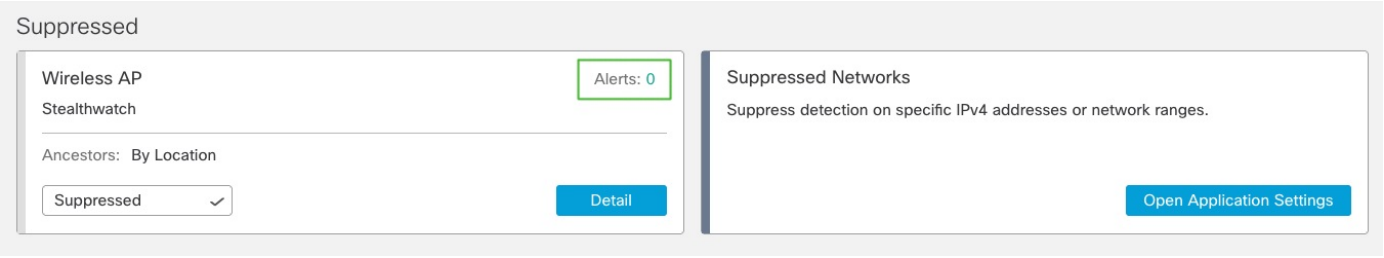


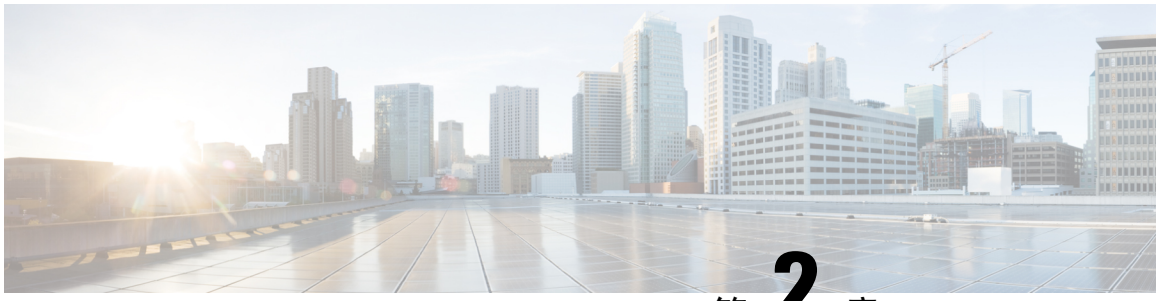
注释　　不再处于**新建/分类**状态的所有其他警报不受威胁严重性变化的影响；它们保持不变和稳定，以便于调查。

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





第 2 章

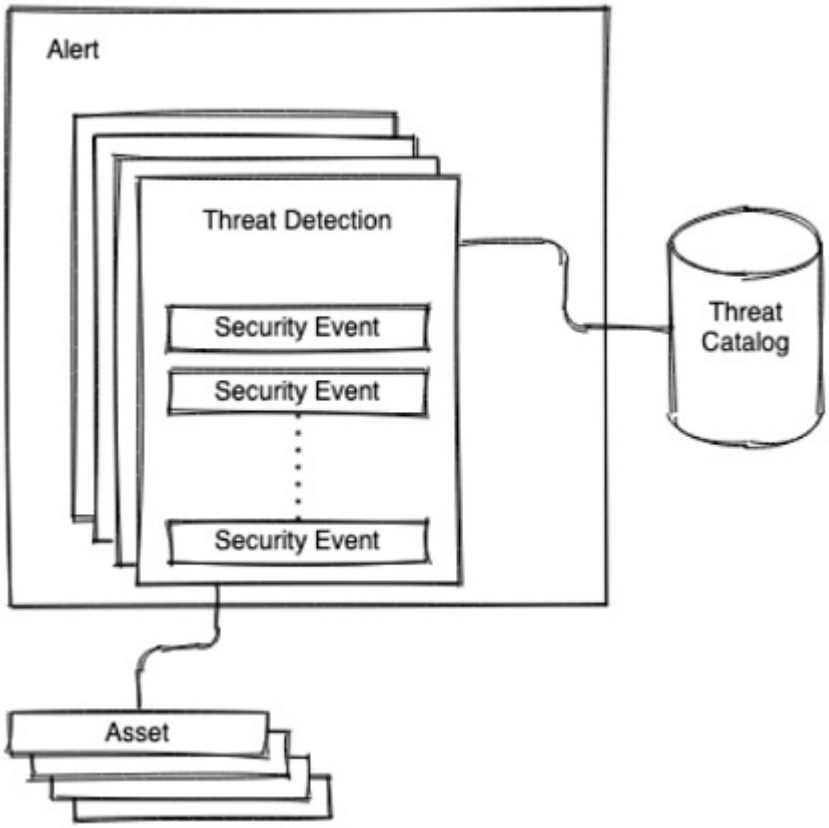
术语表

警报

警报是提示您调查威胁检测的通知。

在全局威胁警报中，警报侧重于一个或多个威胁检测。这些威胁检测发生在一个或多个资产上。我们的融合算法使用这些检测来识别具有相似威胁及其预测的集群，以计算风险级别。然后，我们的 Web 门户会将它们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。

图 *9:*



安全事件

安全事件是可能表示恶意或可疑行为的重要安全事件。威胁检测引擎用于处理安全事件。对检测可疑或恶意行为至关重要的安全事件称为判定。在威胁检测时为受影响资产观察到的安全事件称为情景。每个安全事件都包含其重要性的说明。此说明称为安全注释。

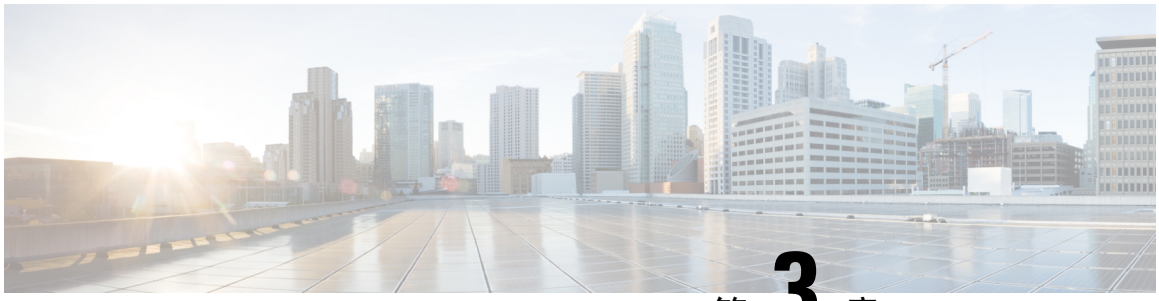
威胁目录

威胁目录组织了可能的威胁检测，并按三个基本类别进行排序：恶意软件、工具和攻击模式。它还包括到 MITRE 的映射（如果存在）。

威胁检测

威胁检测是指检测影响资产的可疑或恶意行为。在全局威胁警报威胁目录中，它可识别多种类型的威胁检测。

威胁检测引擎可处理各种来源，例如安全事件。它会将它们关联起来，以揭示异常模式和趋势，其可能以一定的置信水平揭示或分析性地证实存在威胁。



第 3 章

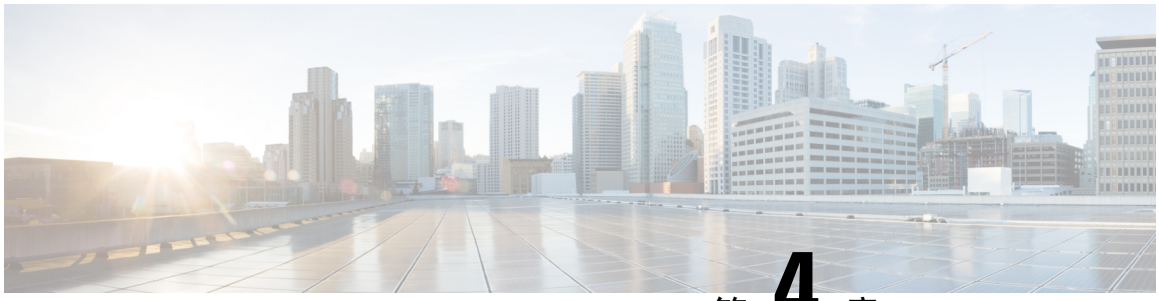
设置

设置

要配置全局设置，请点击页面右上角的齿轮图标下拉菜单：

- **电子邮件通知**—输入电子邮件地址，以每 24 小时向其发送一次新威胁和已更新威胁的摘要。
- **CTA STIX/TAXII API**—使用 CTA STIX/TAXII API 将全局威胁警报检测到的事件的信息提取到您的 SIEM 客户端，以供进一步分析、事件响应和数据存档。请参阅 STIX/TAXII 服务。
- 设备帐户-将日志文件中的遥测数据从一个或多个源代理设备上传到全局威胁警报系统进行分析。要访问此服务，必须为贵公司启用并调配外部遥测功能。如果您不具备外部遥测功能，请联系您的思科安全客户团队。请参阅代理设备上传。
- **应用设置**
  - **受抑制网络**—通过列出要忽略的 IPv4 地址和网络范围来隐藏警报。这对于过滤和抑制不必要的警报（例如来自访客网络或网络中其他不太重要的部分的警报）非常有用。输入要从事件列表中隐藏的主机、子网或 IPv4 地址范围的 IPv4 地址（例如：10.100.10.1、10.100.10.0/24、10.100.10.1-10.100.10.254）。
  - **思科SecureX 集成**—通过选择 SecureX 帐户的区域，点击**授权**并登录到 SecureX 帐户，启用与 SecureX 的集成。
- **发行说明**—汇总功能更新、更改和修复（如本指南后面部分所示）。

设置



第 4 章

STIX/TAXII 服务

概述

全局威胁警报允许您将检测到的事件的相关信息提取到客户端，以进行进一步的关联分析和存档。该服务支持 MITRE 的指标信息的可信自动化交换 (TAXII) 标准，用于与安全信息和事件管理 (SIEM) 系统集成。TAXII 标准指定用于在系统之间共享网络威胁信息的传输机制。

有关 TAXII 的详细信息，请参阅：

TAXII MITRE 组织

TAXII 项目 GitHub

使用结构化威胁信息表示式 (STIX) 语言格式表示每个事件中的信息。STIX 是一种结构化语言，用于描述网络威胁信息，以便以一致的方式共享、存储和分析这些信息。STIX 格式允许全局威胁警报以分层格式表示其漏洞检测结果。TAXII 服务使用 STIX 语言的子集描述全局威胁警报检测到的事件。目前，支持的对象包括：

- 活动—已确认威胁类别（如果可用）
- 事件—异常活动
- TTP—策略、技术和流程
- 可观察条件—Web 请求
- 指示器—识别可观察条件的模式

有关 STIX 的详细信息，请参阅：

https://stix.mitre.org/

轮询服务

轮询服务使用标准化 TAXII 传输机制，以将事件信息从全局威胁警报发送到支持 TAXII 标准的客户端。要提取事件信息，TAXII 客户端需向 TAXII 轮询服务发送轮询请求。HTTP 基本身份验证仅用于限制授权用户的访问权限。然后，TAXII 轮询服务通过将来自全局威胁警报的事件信息发送到 TAXII 客户端进行响应。HTTPS 协议用于保护所有数据传输的安全性。

您的 SIEM 或其他安全工作流程系统必须能够本地支持 STIX/TAXII。将第三方 TAXII 客户端配置为定期轮询 TAXII 轮询服务。

- 要获取您的帐户信息，请求 STIX/TAXII 服务。
  - 点击右上角的全局设置齿轮图标。
  - 点击 **CTA STIX/TAXII API**。
  - 点击**添加帐户**按钮。
  - 输入名称以标识您的帐户，然后点击**添加帐户**按钮。
- 完成配置过程后，系统将显示您的帐户信息。在关闭窗口之前，请将此帐户信息复制到安全位置。

注释 出于安全原因，加密密码仅显示一次。如果丢失加密密码，则必须撤销现有加密密码并生成新的加密密码。

- 将唯一属性复制到第三方 TAXII 客户端中：
  - pollEndpoint 或源服务 URL=`https://taxii.cloudsec.sco.cisco.com/skym-taxii-ws/PollService`
  - 用户名
  - 密码
  - 集合名称或源名称

注释 2018 年 8 月，感知智能（以前称为感知威胁分析或 CTA）开始迁移到 Amazon Web Services 中的新位置，从而产生新的IP地址和访问和使用该服务的额外URL。要保持对服务的访问，可能需要更新出站防火墙规则。在 2018 年 11 月切换后，您将无法再将数据成功发送到旧的数据注入服务 IP 地址。有关所需更改和其他重要信息的具体详细信息，请参阅现场通知。

注释 我们不为配置第三方产品或SIEM设备提供技术支持。如果出现问题，请咨询特定供应商支持团队。

或者，您可以从思科下载并使用示例 TAXII 客户端。如果您的 SIEM 或其他安全系统本地不支持 STIX/TAXII，思科会提供一个轻量级 Java TAXII 日志适配器，您可以将其部署到 SIEM 旁边的 Linux 或 Windows VM 环境。点击提供的链接以查看设置说明。适配器使用 TAXII API 对任何新情报执行定期轮询，并在 STIX 消息中传送数据。然后，适配器将 STIX 消息转换为常见 SIEM 系统接受的其他格式。

要实现轮询服务的稳定性、性能和可用性，请执行以下操作：

- 每 10 分钟内仅允许来自任何单个 TAXII 客户端的一个轮询请求。否则，将返回指示此错误的状态消息。
- 每个轮询请求可以检索长达三天的事件信息。
- 存储的事件信息最多可检索 30 天。

轮询请求

以下是从您的 TAXII 客户端到 TAXII 轮询服务的轮询请求示例。

方式为 POST。

HTTP 请求信头：

```
x-taxii-content-type: urn:taxii.mitre.org:message:xml:1.1
x-taxii-protocol: urn:taxii.mitre.org:protocol:http:1.1
x-taxii-services: urn:taxii.mitre.org:services:1.1
x-taxii-accept: urn:taxii.mitre.org:message:xml:1.1
content-type: application/xml
accept: application/xml
authorization: Basic ...
```

请求正文：

```
<taxii_11:Poll_Request xmlns:taxii_11="http://taxii.mitre.org/messages/taxii_xml_binding-1.1"

                           message_id=" " collection_name=" ">

<taxii_11:Exclusive_Begin_Timestamp>2015-01-16T00:00:00+00:00</taxii_11:Exclusive_Begin_Timestamp>


<taxii_11:Inclusive_End_Timestamp>2015-01-17T00:00:00+00:00</taxii_11:Inclusive_End_Timestamp>

 <taxii_11:Poll_Parameters allow_asynch="false"/>
  <taxii_11:Response_Type>FULL</taxii_11:Response_Type>
 </taxii_11:Poll_Parameters>
</taxii_11:Poll_Request>
```

支持的请求参数	说明
Poll_Request	
message_id	根据 TAXII 规范为每个请求随机生成的字符串。重新生成每个请求的唯一字符串。

支持的请求参数	说明
collection_name	要从全局威胁警报服务提取的集合的名称。此属性将在调配过程完成后由思科提供给您。
Exclusive_Begin_Timestamp	根据您的时间范围调整此值。
Inclusive_End_Timestamp	根据您的时间范围调整此值。
Poll_Parameters	
allow_asynch	始终将此属性设置为 false。

注释 **Exclusive_Begin_Timestamp** 和 **Inclusive_End_Timestamp** 之间支持的最大差值为三天。如果差值较大，则返回的结果限于 **Inclusive_End_Timestamp** 之前的最后三天。

轮询响应

以下是从 TAXII 轮询服务到 TAXII 客户端的轮询响应示例。

HTTP 响应信头：

```
x-taxii-content-type: urn:taxii.mitre.org:message:xml:1.1
x-taxii-protocol: urn:taxii.mitre.org:protocol:http:1.1
x-taxii-services: urn:taxii.mitre.org:services:1.1
```

响应正文：

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<t:Poll_Response xmlns:t="http://taxii.mitre.org/messages/taxii_xml_binding-1.1"
                 xmlns:c="http://cybox.mitre.org/cybox-2"
                 xmlns:cc="http://cybox.mitre.org/common-2"
                 xmlns:co="http://cybox.mitre.org/objects#CustomObject-1"
                 xmlns:coa="http://stix.mitre.org/CourseOfAction-1"
                 xmlns:sc="http://stix.mitre.org/common-1"
                 xmlns:ind="http://stix.mitre.org/Indicator-2"
                 xmlns:ttp="http://stix.mitre.org/TTP-1"
                 xmlns:inc="http://stix.mitre.org/Incident-1"
                 xmlns:s="http://stix.mitre.org/stix-1"
                 collection_name=" " more="true"
                  result_id=" " result_part_number="1"
                  in_response_to="generatedMessageID" message_id="responseMessageID">
    <t:Exclusive_Begin_Timestamp>2015-01-17T15:11:00.648Z</t:Exclusive_Begin_Timestamp>
    <t:Inclusive_End_Timestamp>2015-01-20T15:11:00.649Z</t:Inclusive_End_Timestamp>
    <t:Content_Block>
      <t:Content_Binding binding_id="STIX_XML_1.1"/>
      <t:Content>
        <s:STIX_Package xmlns:cta="http://cisco.com/td/cta"
               id="cta:package-1412045744-66911c07-c9b8-4389-8888-00e438f58c2e"
               timestamp="2015-01-20T15:11:02.766Z" version="1.1.1">
          <s:STIX_Header>
            <s:Package_Intent>Incident</s:Package_Intent>
              <s:Information_Source>
                <sc:Identity id="cta:customer-1234567890"/>
```

```
      <sc:Tools>
         <cc:Tool id="cta:tool-cta">
             <cc:Name>Cognitive Threat Analytics</cc:Name>
             <cc:Vendor>Cisco</cc:Vendor>
         </cc:Tool>
         <cc:Tool id="cta:tool-amp">
             <cc:Name>Advanced Malware Protection</cc:Name>
             <cc:Vendor>Cisco</cc:Vendor>
         </cc:Tool>
      </sc:Tools>
   </s:Information_Source>
</s:STIX_Header>
<s:Incidents>
  <s:Incident xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xsi:type="inc:IncidentType"
          id="cta:incident-1412045744_f8bae03fb2ff7d6185907ae3240d_ITMAL1">
   <inc:Title>malware|using automatically generated domain (DGA)</inc:Title>
   <inc:Victim>
       <sc:Name>JohnDoe</sc:Name>
   </inc:Victim>
    <inc:Related_Indicators>
     <inc:Related_Indicator>
      <sc:Indicator xsi:type="ind:IndicatorType"
     id="cta:indicator-1412045744_1421623800000_f8bae03fb2ff7d6185907ae3240d_0">

       <ind:Observable>
        <c:Observable_Composition operator="AND">
          <c:Observable>
           <c:Object>
            <c:Properties xsi:type="co:CustomObjectType">
             <cc:Custom_Properties>
              <cc:Property name="timestamp">1421623882432</cc:Property>
              <cc:Property name="xElapsedTime">1810</cc:Property>
              <cc:Property name="scHttpStatus">0</cc:Property>
              <cc:Property name="csContentBytes">622</cc:Property>
              <cc:Property name="scContentBytes">907</cc:Property>
              <cc:Property name="csUrl"></cc:Property>
              <cc:Property name="sIP">195.22.26.231</cc:Property>
              <cc:Property name="cIP">33.196.39.11</cc:Property>
              <cc:Property name="cUsername">JohnDoe</cc:Property>
              <cc:Property name="sReputation">-580</cc:Property>
              <cc:Property name="sCategory">unclassified</cc:Property>
             </cc:Custom_Properties>
            </c:Properties>
           </c:Object>
          </c:Observable>
          <c:Observable>
           <c:Object>
            <c:Properties xsi:type="co:CustomObjectType">
             <cc:Custom_Properties>
              <cc:Property name="timestamp">1421623896635</cc:Property>
              <cc:Property name="xElapsedTime">1942</cc:Property>
              <cc:Property name="scHttpStatus">0</cc:Property>
              <cc:Property name="csContentBytes">361</cc:Property>
              <cc:Property name="scContentBytes">582</cc:Property>
              <cc:Property name="csUrl"></cc:Property>
              <cc:Property name="sIP">195.22.26.231</cc:Property>
              <cc:Property name="cIP">33.196.39.11</cc:Property>
              <cc:Property name="cUsername">JohnDoe</cc:Property>
              <cc:Property name="sReputation">-580</cc:Property>
              <cc:Property name="sCategory">unclassified</cc:Property>
             </cc:Custom_Properties>
            </c:Properties>
           </c:Object>
```

```
                    </c:Observable>
                   </c:Observable_Composition>
                  </ind:Observable>
                  <ind:Indicated_TTP>
                   <sc:TTP xsi:type="ttp:TTPType">
                    <ttp:Title>communication to automatically generated domain
(DGA)</ttp:Title>
                   </sc:TTP>
                  </ind:Indicated_TTP>
                 </sc:Indicator>
                </inc:Related_Indicator>
               </inc:Related_Indicators>
               <inc:Discovery_Method>Log Review</inc:Discovery_Method>
               <inc:COA_Requested>
                <inc:Course_Of_Actionxsi:type="coa:CourseOfActionType">
                 <coa:Stage>Remedy</coa:Stage>
                 <coa:Type>Eradication</coa:Type>
                 <coa:Parameter_Observablescybox_major_version="2"cybox_minor_version="1">
                  <c:Observable_Package_Source>
                   <cc:Time>
                    <cc:Produced_Time>2016-08-15T17:02:02.616Z</cc:Produced_Time>
                   </cc:Time>
                  </c:Observable_Package_Source>
                  <c:Observable>
                   <c:Object>
                    <c:Propertiesxsi:type="user:UserAccountObjectType">
                     <user:Username>JohnDoe</user:Username>
                    </c:Properties>
                   </c:Object>
                  </c:Observable>
                  <c:Observable>
                   <c:Object>
                    <c:Propertiesxsi:type="addr:AddressObjectType"category="ipv4-addr">
                     <addr:Address_Value>33.196.39.11</addr:Address_Value>
                    </c:Properties>
                   </c:Object>
                  </c:Observable>
                 </coa:Parameter_Observables>
                </inc:Course_Of_Action>
               </inc:COA_Requested>
               <inc:Confidence>
                <sc:Value>Low</sc:Value>
               </inc:Confidence>
               <inc:Information_Source>
                   <sc:Tools>
                       <cc:Tool idref="cta:tool-cta"/>
                   </sc:Tools>
               </inc:Information_Source>
           </s:Incident>
          </s:Incidents>
         </s:STIX_Package>
        </t:Content>
    </t:Content_Block>
</t:Poll_Response>
```

注释 在 `Poll_Reponse` 中，如果没有更多威胁项目，则 `more` 和 `result_id` 这两个属性不存在。当 `more=true` 存在时，您可以使用 `Poll_Fulfillment` 请求响应的下一页。

支持的响应对象	字段说明
Poll_Response	
collection_name	要从全局威胁警报服务提取的集合的名称。此属性将在调配过程完成后由思科提供给您。
result_id	将此值复制到轮询执行请求。
Exclusive_Begin_Timestamp	此轮询响应涵盖的时间范围的排他性起点。缺少此字段表示轮询响应涵盖此 TAXII 数据源的最早时间。
Inclusive_End_Timestamp	此轮询响应覆盖的时间范围的包含端。
Content_Block	返回的内容。
Content_Binding	
内容	
STIX_Package	有关 STIX 语言的信息。
STIX_Header	有关 STIX 内容包的信息。
突发事件	一个或多个事件。
事故	有关单个事件的信息。
标题	描述此事件的标题。
受害者	有关此事件的受害者的信息。
Related_Indicators	标识与此事件相关的指示器。
Related_Indicator	标识与此事件相关的单个指示器。
指标	指示器由识别特定可观察条件的模式以及有关模式含义、应如何实施和何时执行操作等的情景信息组成。
可观察	此指示器的相关可观察对象。
Observable_Composition	允许通过组合其他可观察对象的逻辑组合，来指定更高层次的复合可观察对象。
可观察	表示单个可观察对象。
对象	识别特定对象（例如文件、注册表密钥、流程）的特征
属性	对对象执行操作时枚举的属性。

支持的响应对象	字段说明
Custom_Properties	启用指定一组可能在现有属性架构中未定义的自定义对象属性。
属性	对对象执行操作时枚举的单个属性。
Indicated_TTP	指定此指示器指示的相关战术、技术和程序 (TTP)。
Discovery_Method	有关用于发现代码的方法和/或工具的信息。
COA_Requested	针对此事件的建议操作步骤。
置信	有关表征此事件的置信度的信息。
Information_Source	有关此事件来源的信息。
工具	
工具	哪个工具（CTA 或 AMP）检测到此事件。

如果出现错误，则将返回错误消息。例如：

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<t:Status_Message
          xmlns:t="http://taxii.mitre.org/messages/taxii_xml_binding-1"
          xmlns:c="http://cybox.mitre.org/cybox-2"
          xmlns:cc="http://cybox.mitre.org/common-2"
          xmlns:co="http://cybox.mitre.org/objects#CustomObject-1"
          xmlns:sc="http://stix.mitre.org/common-1"
          xmlns:ind="http://stix.mitre.org/Indicator-2"
          xmlns:ttp="http://stix.mitre.org/TTP-1"
          xmlns:inc="http://stix.mitre.org/Incident-1"
          xmlns:s="http://stix.mitre.org/stix-1"
                status_type="FAILURE" in_response_to="23537"
                message_id="16ed0b75-2af6-4537-b71c-da00e0a0c419">
   <t:Message>An error occurred during request processing.</t:Message>
</t:Status_Message>
```

TAXII status_type	错误说明
	用户未通过身份验证，HTTP 响应状态代码为 404
DENIED	用户未通过授权，HTTP 响应状态代码为 401
BAD_MESSAGE	请求消息无效，请参阅消息参数
失败	未指定错误，请参阅消息参数

轮询执行

以下是从您的 TAXII 客户端到 TAXII 轮询服务的轮询执行请求示例。

方式为 POST。

HTTP 请求信头：

```
x-taxii-content-type: urn:taxii.mitre.org:message:xml:1.1
x-taxii-protocol: urn:taxii.mitre.org:protocol:http:1.1
x-taxii-services: urn:taxii.mitre.org:services:1.1
x-taxii-accept: urn:taxii.mitre.org:message:xml:1.1
content-type: application/xml
accept: application/xml
authorization: Basic ...
```

请求正文：

```
<taxii_11:Poll_Fulfillment
xmlns:taxii_11="http://taxii.mitre.org/messages/taxii_xml_binding-1.1"
                           message_id=" " collection_name=" "
                           result_id=" " result_part_number="2" />

<taxii_11:Exclusive_Begin_Timestamp>2015-01-16T00:00:00+00:00</taxii_11:Exclusive_Begin_Timestamp>


<taxii_11:Inclusive_End_Timestamp>2015-01-17T00:00:00+00:00</taxii_11:Inclusive_End_Timestamp>

 <taxii_11:Poll_Parameters allow_asynch="false"/>
  <taxii_11:Response_Type>FULL</taxii_11:Response_Type>
 </taxii_11:Poll_Parameters>
</taxii_11:Poll_Request>
```

支持的请求参数	说明
Poll_Request	
message_id	根据 TAXII 规范为每个请求随机生成的字符串。重新生成每个请求的唯一字符串。
collection_name	要从全局威胁警报服务提取的集合的名称。此属性将在调配过程完成后由思科提供给您。
result_id	从轮询响应中粘贴此值。
result_part_number	将此值从轮询响应中的值增加 1。
Exclusive_Begin_Timestamp	根据您的时间范围调整此值。
Inclusive_End_Timestamp	根据您的时间范围调整此值。
Poll_Parameters	
allow_asynch	始终将此属性设置为 false。

注释 **Exclusive_Begin_Timestamp** 和 **Inclusive_End_Timestamp** 之间支持的最大差值为三天。如果差值较大，则返回的结果限于 **Inclusive_End_Timestamp** 之前的最后三天。

常规查询

本节介绍思科 STIX/TAXII API 中使用的一些常见查询，以帮助确定调查结果的优先顺序，以便进一步调查。示例查询中使用的语法基于 SPLUNK 集成并，为符号。特定字段和值可能因本地集成而异，但查询的含义广泛适用于 SIEM 系统和集成。

提示 如果您正在收集 SPLUNK 中的其他数据，请在主机名、索引或源名称前添加查询，以仅搜索全局威胁警报数据。

受到已确认威胁影响的用户

此查询将返回带有已确认威胁的所有用户，并且可能会报告给事件响应团队进行桌面补救。如果这些事件也具有高风险，请考虑重新映像受影响的设备。此查询将生成一个表格，其中包含受其影响的用户名和活动名称。搜索非空活动名称，然后删除重复的用户名+活动对：

```
campaign!="" | table cUsername campaign | dedup cUsername campaign | sort + cUsername
```

或者，使用活动名称的多值字段：

```
campaign!="" | transaction cUsername | table cUsername campaign | sort + cUsername
```

在一个时间段内受到已确认威胁影响的用户

此查询还包括“首次发现”和“最后发现”列。搜索非空活动，按用户名+活动对进行汇总，并计算网络流时间戳的最小值和最大值。结果以纪元毫秒为单位，如果需要，可以转换为日历时间。

```
campaign!="" | stats min(timestamp) max(timestamp) by cUsername campaign
```

或者，使用 strftime 函数包含纪元转换。此示例将时间戳除以 1000 以删除毫秒：

```
campaign!="" | stats min(timestamp) as oldest max(timestamp) as newest by cUsername campaign
 |
  eval oldest_time=strftime(oldest/1000,"%m/%d/%y %H:%M:%S") |
  eval newest_time=strftime(newest/1000,"%m/%d/%y %H:%M:%S") |
  table cUsername, campaign, oldest_time, newest_time
```

受高风险和高置信度事件影响的用户

此查询生成高风险和高置信度用户的优先级列表，无论他们是否有已确认的活动。搜索高风险、高置信度和重复数据删除的用户名。由于所有这些事件都具有高风险和高置信度，因此请考虑重新映像受影响的设备。

```
confidence="High" risk="High" | dedup cUsername | table cUsername campaign
```

受活动影响的用户

此查询将生成一个图表，显示一段时间内受感染用户的数量，并按活动细分。搜索非空活动，按一天的时间间隔归纳数据，并计算该收集器中的不同用户名计数。

```
campaign!="" | timechart dc(cUsername) span=1d by campaign
```

注释 在 SPLUNK 中，可以使用时间表快捷方式。

命令和控制服务器

此查询生成“已确认”类别中所有检测到的命令和控制 (C&C) 服务器的列表。搜索非空活动，同时显示服务器 IP 地址和活动，然后对服务器 IP 地址进行重复数据删除。此结果列出了受感染设备的 C&C IP 目标地址以用于维护 C&C 通信。对于每个 C&C IP 地址，您还可以查看其涉及的威胁活动。可用于查询其他系统以获取更多情报，提供感染指标 (IOC) 以及识别受感染终端上的恶意进程和应用。

```
campaign!="" | table sIP campaign | dedup sIP
```

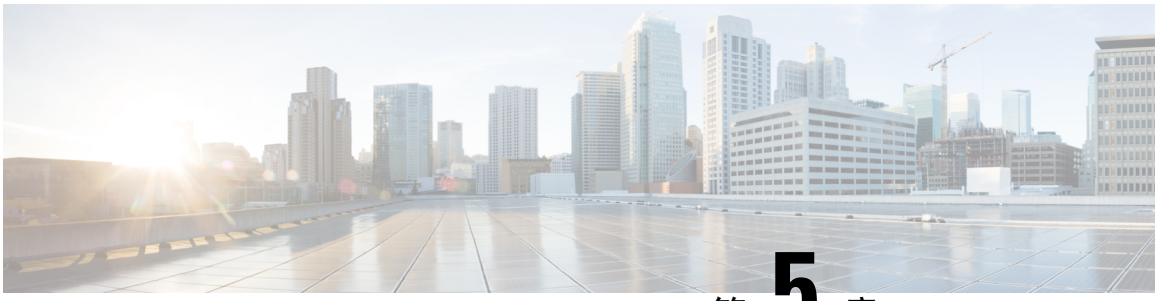
与思科 ISE 的集成

思科身份服务引擎 (ISE) 是一种可用于安全地访问网络资源的安全策略管理平台。思科 ISE 是一个策略决策点，可帮助企业确保合规，加强基础设施安全以及简化服务操作。通过思科 ISE，企业可以从网络、用户和设备收集实时情境信息。然后，您可以通过将身份绑定到网络中的各种元素，使用该信息做出前瞻性的管理决策。

全局威胁警报与思科ISE集成以提供网络级隔离，该功能具有从网络中删除受感染设备的功能，这样就无法进一步泄露敏感数据。全局威胁警报与思科 ISE 之间的集成使用 STIX/TAXII。对于系统能够将感染归因于单个用户的关键级别风险发现，思科 ISE 会收到请求的操作过程，该过程建议威胁中心网络访问控制 (TC-NAC) 隔离，这隶属于思科快速威胁遏制框架。根据与感染相关的风险，请求的操作过程可以是监控、根除、内部阻止或组合。内部阻止是要在 TC-NAC 中的阻止策略中使用的操作过程。有关详细信息，请参阅思科快速威胁遏制。

您可以使用思科 ISE 和全局威胁警报 STIX/TAXII 服务提供的数据源来开发自己的解决方案。数据源包含有关识别受感染设备和要执行的操作的信息。您可以根据全局威胁警报STIX / TAXII源中的建议在思科ISE中定义隔离策略。有关如何在思科ISE中配置全局威胁警报适配器的信息，请参阅《思科ISE管理员指南，版本2.2》。http://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22.html

注释 全局威胁警报使用 Web 代理日志中作为客户端 IP 或用户名列出的用户身份。具体而言，在使用 IP 地址的情况下，通过代理日志可用的 IP 地址可能是与内部企业网络上另一个 IP 地址（用于另一台设备）冲突的 IP 地址。例如，通过 AnyConnect 和分割隧道直接连接到互联网的漫游用户可以在家中获取本地 IP 地址（例如，10.0.0.x 地址），该地址可能与内部企业网络中使用的重叠私用范围中的 IP 地址冲突。当您定义快速遏制威胁策略时，请考虑您的逻辑网络架构，以避免将隔离操作应用于不匹配的设备。



第 5 章

代理设备上传

代理设备上传

将日志文件中的遥测数据从思科网络安全设备 (WSA) 和 Blue Coat ProxySG 等代理设备上传到全局威胁警报系统以进行分析。

步骤 1 点击页面右上角的齿轮图标，然后选择**设备帐户**以打开设置向导。

注释 如果已有至少一个现有设备帐户，则跳过设置并显示设备帐户页面。

步骤 2 当您准备启动安装向导以添加设备帐户时，请点击**让我们开始吧**。

步骤 3 通过从下拉列表中选择自动或手动上传，选择如何从设备上传遥测数据。全局威胁警报系统一次仅支持一种上传方法；不能一起使用这两种方法。

注释 要从自动上传切换到手动上传，必须先从自动上传配置中删除所有代理设备。

步骤 4 如果选择了自动上传方法，请通过选择 **SCP** 或 **HTTPS** 选择用于传输日志文件的协议。

a) 输入此设备的名称，然后点击**添加帐户**。

b) 如果选择了 SCP：

- 复制信息（主机、端口、目录、用户名），以粘贴到您的思科 WSA 配置中。出于安全原因，信息仅显示一次。
- 有关如何配置思科 WSA 的详细信息，请参阅其配置指南。
- 思科 WSA 管理控制台返回公钥 SSH 后，请将公钥 SSH 复制并粘贴到设备帐户中。
- 点击**完成**。
- 或者，您可以稍后通过导航到设备帐户页面并点击该设备来输入公共 SSH 密钥。

c) 如果选择了 HTTPS：

代理设备上传

- 复制信息（主机、端口、路径、用户名、密码）以粘贴到 Blue Coat ProxySG 配置中。
- 有关如何配置 Blue Coat ProxySG 的详细信息，请参阅其配置指南。
- 点击**完成**。

步骤 5 如果您选择手动上传方法：

a) 验证日志文件的格式。遵循这些准备指南：

- 支持由思科 WSA 和 Blue Coat 代理创建的 W3C 日志文件。
- 所有日志文件必须以 GZip (*.gz) 格式压缩。
- 每个日志文件必须小于 1 GB。大于 1 GB 的日志文件应分为多个较小的文件。确保单独的时间间隔不重叠，并且每个文件都包含相同的正确信头。
- 日志文件涵盖的总时间间隔应大于两天。
- 每个日志文件必须具有特定的非重叠时间间隔。
- 每个日志文件必须按升序包含日志条目；较早的条目在较新的条目之前。
- 日志文件应按字母/数字排序，并根据时间顺序上传；较旧的文件应在较新的文件之前上传。在单次上传中，上传组件会自动对文件进行排序。如果上传多次，请确保始终上传比以前更新的数据。如果保留代理日志文件中默认使用的命名约定，则文件名已正确排序。
- 将不会处理早于之前上传的数据的数据。
- 日志文件的内容必须与某些条件匹配才能有效上传。
  - 我们为您提供日志验证工具，用于在上传之前检查您的日志文件。
  - 将日志文件的前 20 行复制并粘贴到日志验证工具中，以检查是否存在错误。
  - 系统会显示任何错误，并且在您纠正错误后，该工具将自动继续检查是否存在错误。

b) 点击**添加文件**以选择要上传的日志文件，或将日志文件拖放到上传框中。

注释 点击**清除文件**以清除添加到上传框中的所有文件。

c) 点击**开始上传**会将所选日志文件上传到全局威胁警报系统以进行分析。允许全局威胁警报系统在查看到结果之前等待一段时间。

注释 为了最大限度地降低数据丢失的风险，全局威胁警报系统会在 5 小时后开始处理上传的数据。这使您有时间完成所有上传操作，并确保在数据处理开始之前一切就绪且顺序正确。

注意 尝试从手动上传切换到自动上传会立即中止所有上传并停止处理已上传的数据。所有上传的数据都将被丢弃。

注释 关闭页面或导航离开页面将停止任何当前文件上传。

注释 除非先停止所有手动上传，否则您无法使用自动上传。如果在处理完所有数据之前便进行切换，则转换过程中可能会丢失一些分析数据。为确保系统不丢失任何数据，请在上次手动上传 24 小时后执行切换。

下一步做什么

“设备帐户”页面列出代理设备及其信息。“状态”列显示每个设备的状态：

- 新建—SCP 的配置不完整，可能缺少公共 SSH 密钥
- 调配—正在调配的帐户，尚未准备就绪
- 就绪—已成功创建帐户
- 错误—将光标悬停在状态上以显示解释错误的弹出消息

在此概述页面中，您可以添加更多设备帐户，或者点击任意设备将其删除，输入公共 SSH 密钥或进行故障排除。

虽然可以在多个设备或上传流程之间共享帐户，但我们建议您为每个设备使用单独的帐户，以最大程度地减少文件名冲突的可能性，并简化上传问题的故障排除。

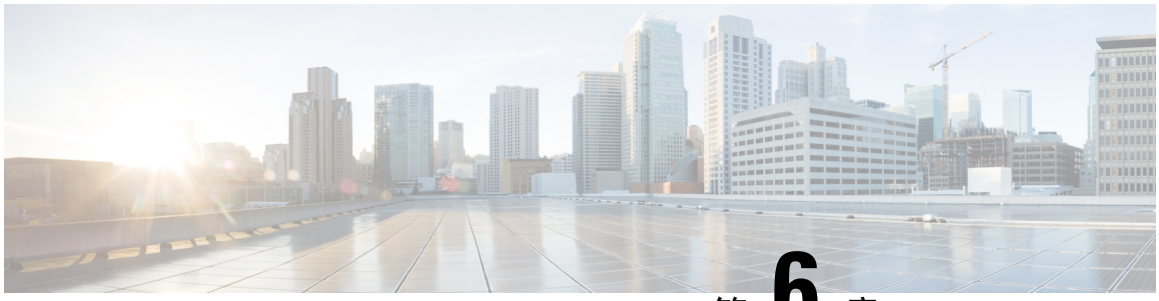
一旦您的设备帐户准备就绪，点击以查看**已确认**或**已检测**页面，以了解网络中的任何可疑活动。

注释 数据通常在调配完成后两到三天内可用。

代理设备上传

第 I 部分

发行说明



第 6 章

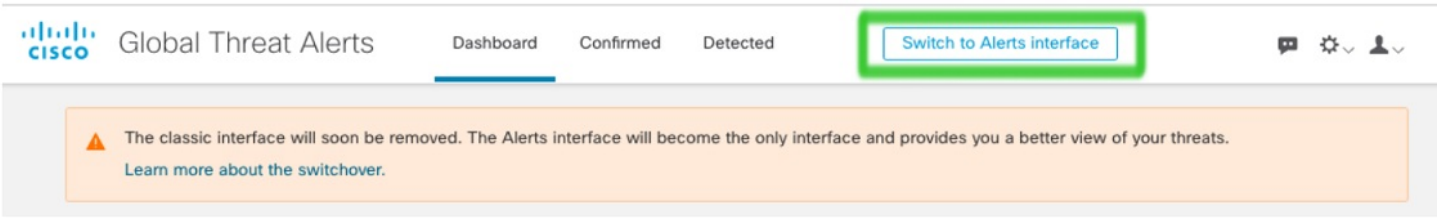
2021 年 8 月

2021 年 8 月发布的思科基于云的机器学习全局威胁警报更新。

已停用传统接口

早在 6 月，我们便建议您从传统接口切换到警报接口。

图 *10:*



较旧的经典接口现已停用，而较新的警报接口已成为唯一接口，为您提供网络威胁的增强视图。

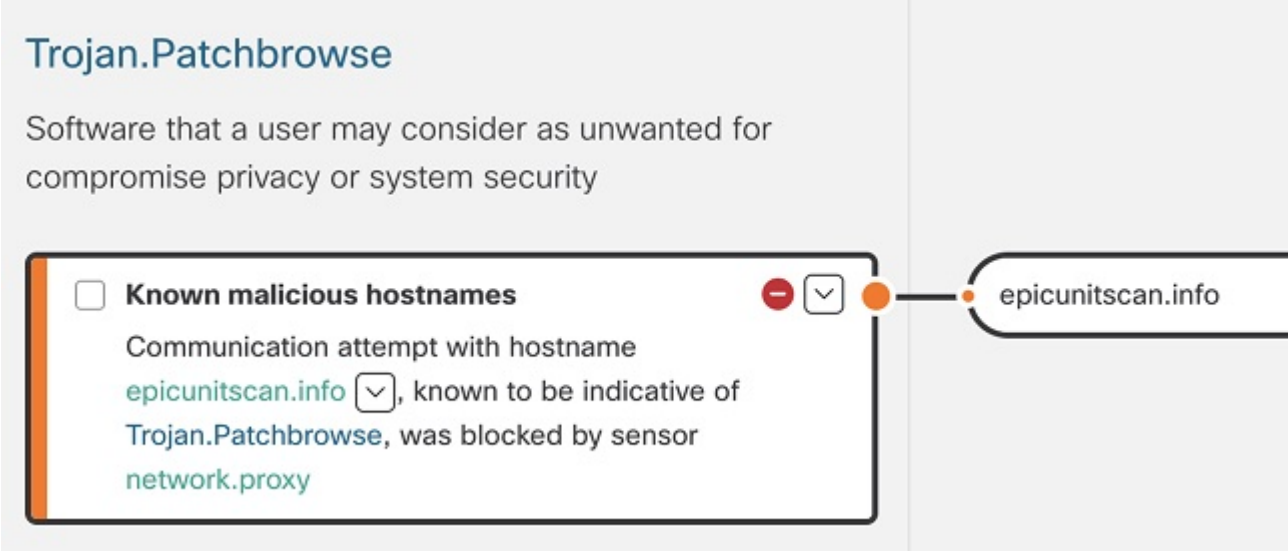
改进了对扫描和受阻通信的处理

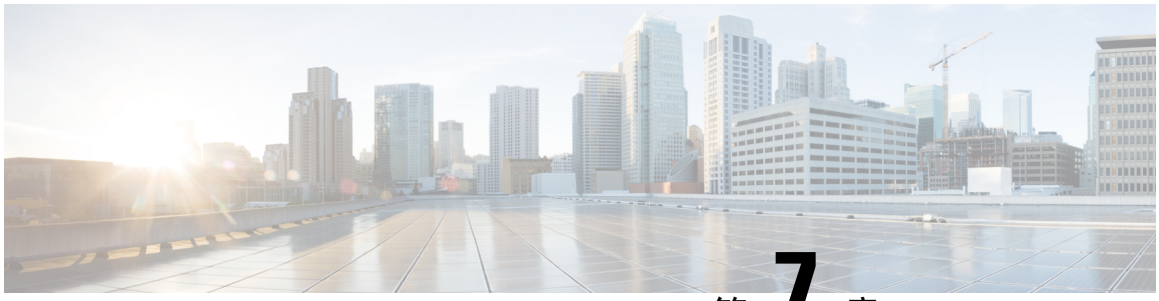
为了减少误报的数量，全局威胁警报现在可以抑制由水平扫描通信触发的威胁检测。它现在还可以在感染的初始阶段抑制对代理阻止的通信的威胁检测。

为了提高案例的可视化效果，当感染持续存在于终端，并且部分出站通信被代理（或其他出站控制进程）阻止时，全局威胁警报将描述作为一部分呈现的特定安全事件威胁检测。

在本例中，代理传感器阻止了与主机（已知为特洛伊木马）通信的尝试。安全事件通知您此软件被视为不需要，因为它可能会危害您的隐私或系统安全。

图 *11:* 示例：通知您通信尝试已被代理阻止的安全事件





第 7 章

2021 年 6 月

2021 年 6 月发布的思科基于云的机器学习全局威胁警报更新。

用于自动化支持的新 REST API

现在，您可以通过新的 REST API 使用全局威胁警报控制面板中的所有可见数据。您可以使用它下载单个警报的内容，甚至通过将所有警报流式传输到网络中的第三方 SIEM，以自动化整个数据收集过程。

API 不是只读的；您可以更改全局威胁警报环境的配置。例如，您可以增加关键资产组的特定商业价值或更改分配给威胁的严重性。

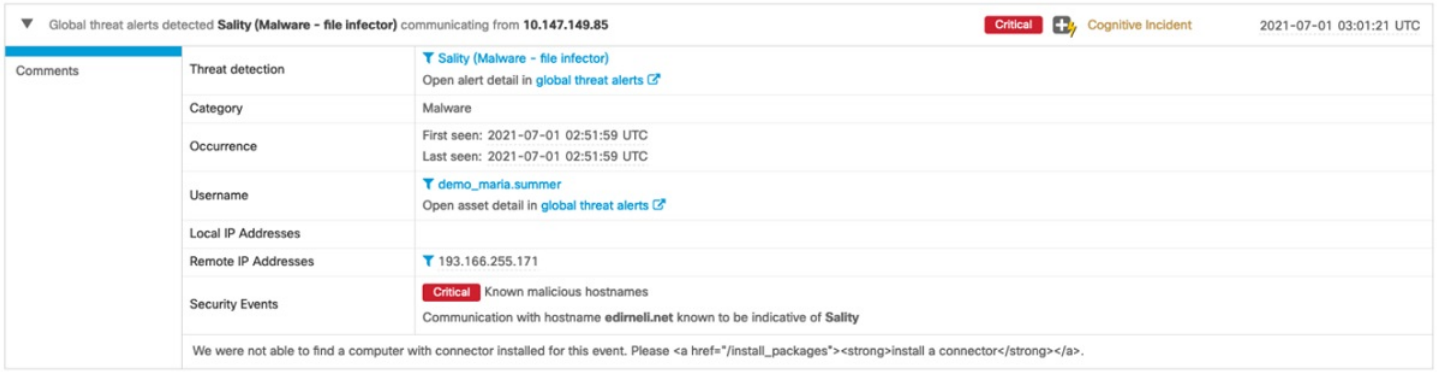
要查看 API 可能性，请参阅https://api.cta.eu.amp.cisco.com。在那里，您可以找到更详细地描述 API 可能性的规范和使用案例，以及用于额外集成的示例脚本。

要了解有关新 REST API 的更多信息，请参阅全局威胁警报 REST API 现已发布！

Secure Endpoint 集成更新

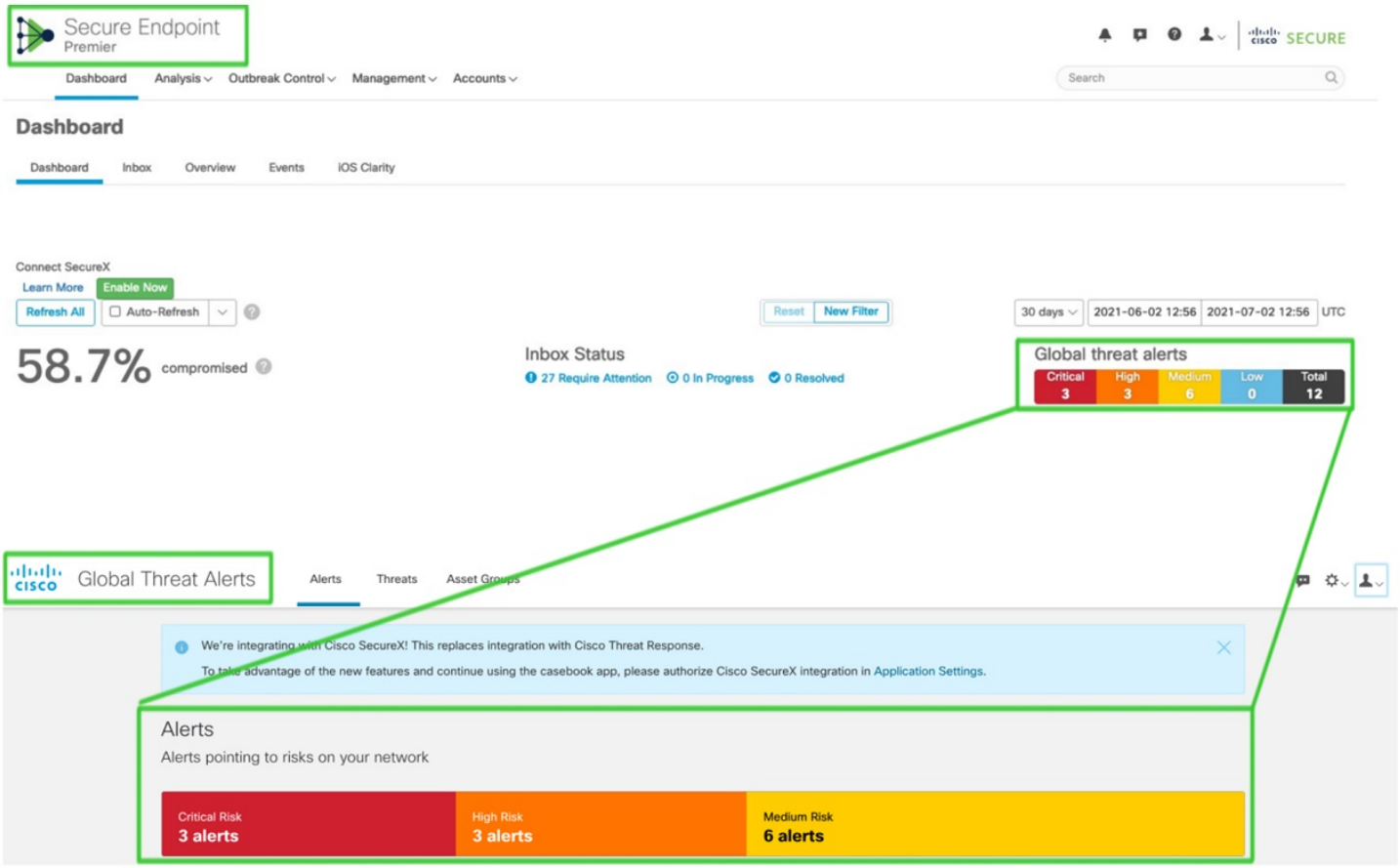
我们更新了在安全终端中显示全局威胁警报的检测方式。现在，检测在控制台中显示为事件，并且与警报接口直接关联。因此，警报接口中的威胁严重性变化会反映在这些事件中。

图 *12:* 全局威胁警报检测现在在安全终端控制台中显示为事件



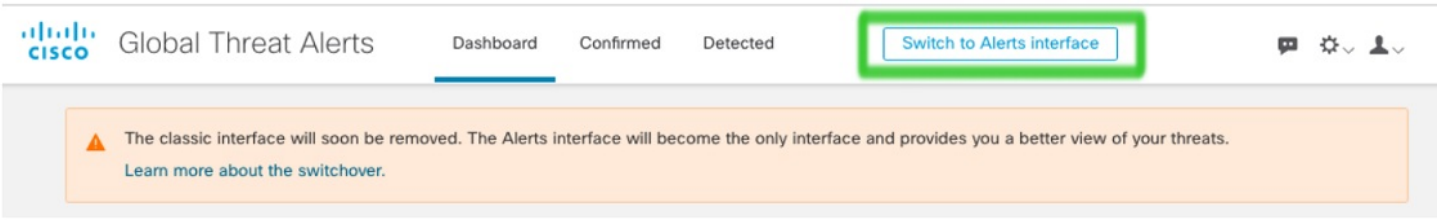
当全局威胁警报界面中的警报状态或风险发生变化时，它会反映在安全终端控制台的警报概述中：

图 *13:*



为避免出现兼容性问题，传统接口将很快停用，因此我们建议您从传统接口切换到警报接口。在全局威胁警报控制面板上，点击切换到警报接口按钮：

图 *14:*



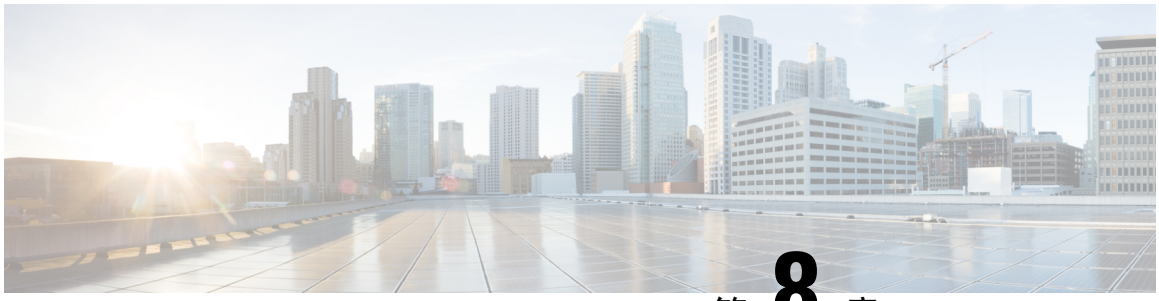
STIX/TAXII API 更新

STIX/TAXII API 源提供的检测链接和威胁词汇现在与全局威胁警报控制面板中的警报接口兼容。

图 *15:*

```
<s:Incident xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
            xsi:type="inc:IncidentType"
            URL="https://cta.eu.amp.cisco.com/ui/assets/demo_3399f455c51cf4879ce08796f0dee9613832f2bd165127f4f7e5fabcc825979c"
            id="cta:incident-demo_a304ea5e63d526a9077406ada15697554bbb1d3ea7d2b49f1773c0ee104ede1d">
   <inc:Title>njRAT</inc:Title>
   <inc:Victim>
      <sc:Name>demo_sook.putnam</sc:Name>
   </inc:Victim>
   <inc:Impact_Assessment>
      <inc:Impact_Qualification>Catastrophic</inc:Impact_Qualification>
   </inc:Impact_Assessment>
   <inc:Related_Indicators>
      <inc:Related_Indicator>
         <sc:Indicator xsi:type="ind:IndicatorType"
                       id="cta:indicator-demo_6a0d469ac3f4383b00f6b221fe4c7d88fa70161089a75fa8b6c8058985dc981e">
            <ind:Observable>
               <c:Observable_Composition operator="AND">
                  <c:Observable>
                     <c:Object>
```

由于威胁措辞和分类发生了变化，我们建议您检查 STIX / TAXII API 提供的工具和 SIEM 中是否存在不兼容问题以及依赖关系是否中断。



第 8 章

2021 年 5 月

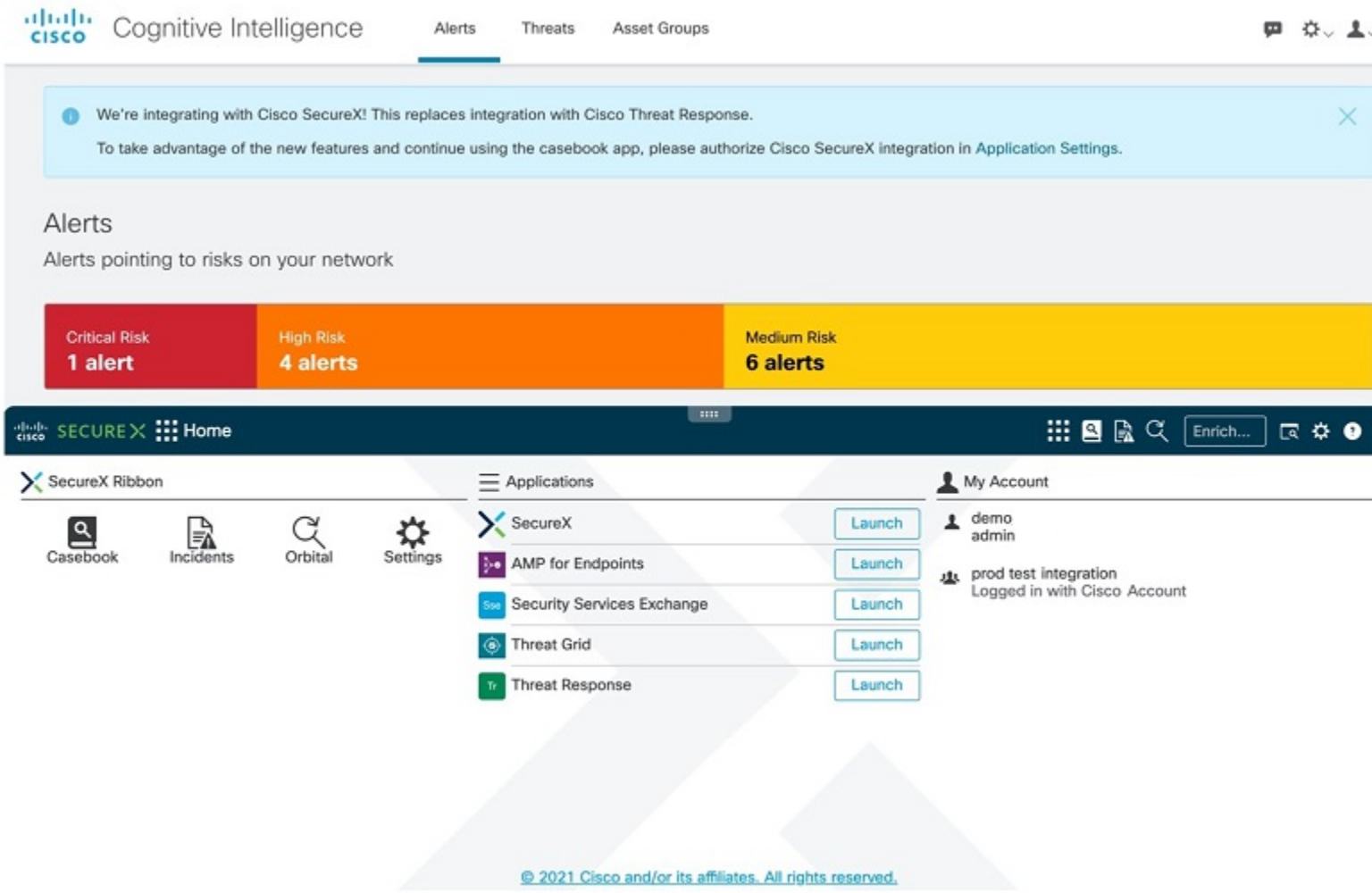
2021 年 5 月发布的思科基于云的机器学习全局威胁警报更新。

SecureX Ribbon 支持

SecureX 是集中式控制台和分布式功能集，可统一可视性，实现自动化，加速事件响应工作流程并改善威胁搜索。这些分布式功能以 SecureX 功能区中的应用和工具的形式呈现。

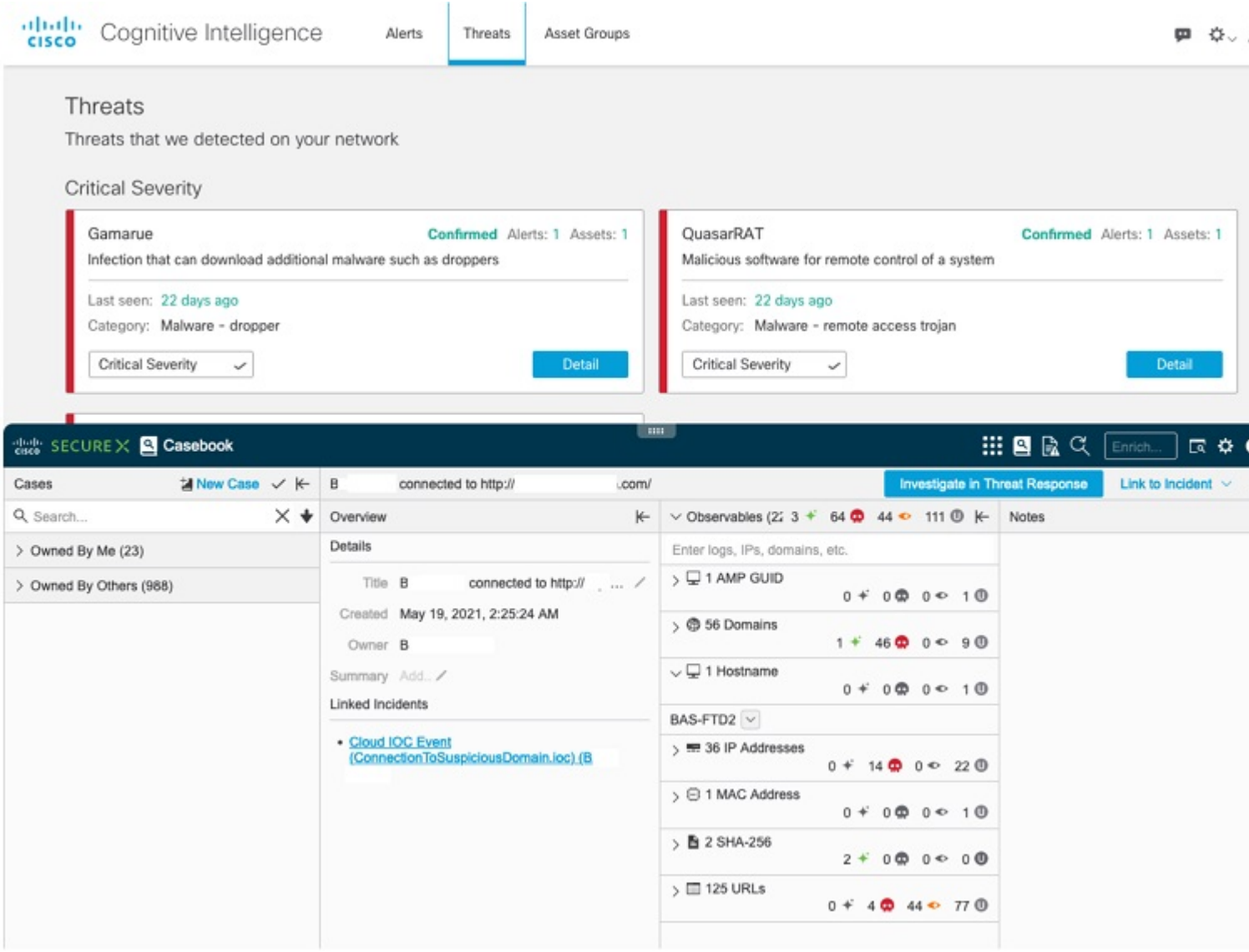
SecureX 功能区现在也存在于全局威胁警报中，位于页面下方，当您在控制面板和环境中的其他安全产品之间移动时，此功能仍然存在。这有助于您将调查结果与案例集和事件相关联。

图 *16:* 位于页面下方的 ***SecureX*** 功能区



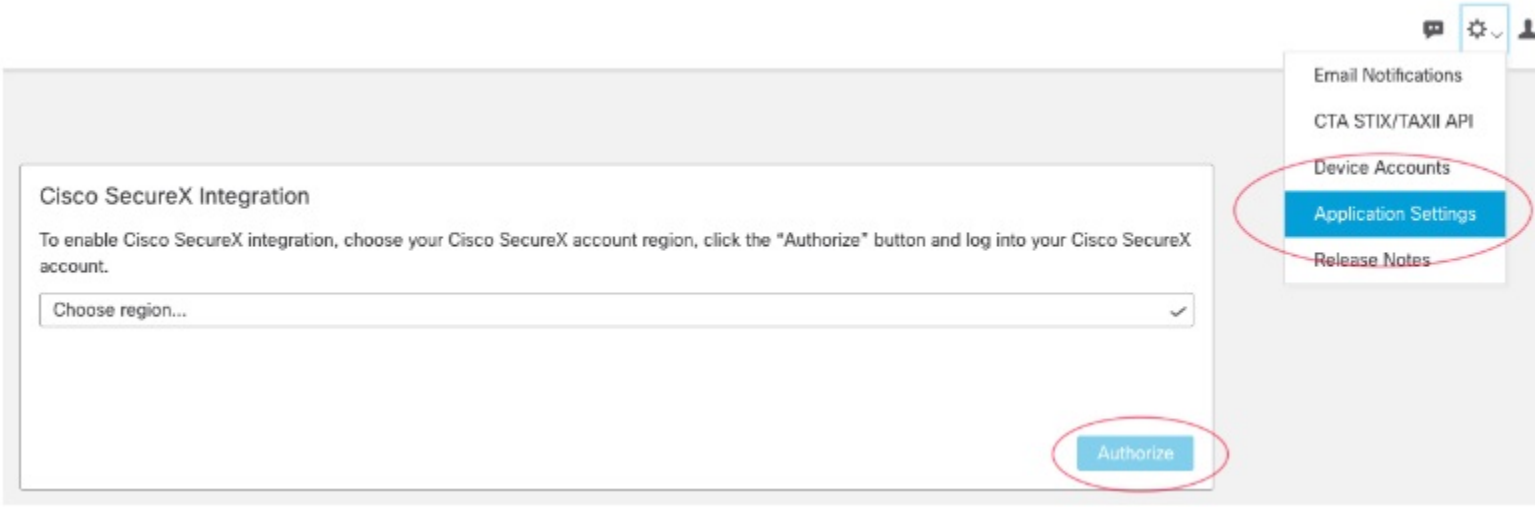
您可以使用此功能区访问案例集、设置和其他应用。您还可以查看事件和搜索可观察对象以进行扩充。

图 *17:* 示例：使用 ***SecureX*** 功能区访问您的案例集



要启用此功能，用户必须拥有 SecureX 帐户并授权“应用设置”中的集成。

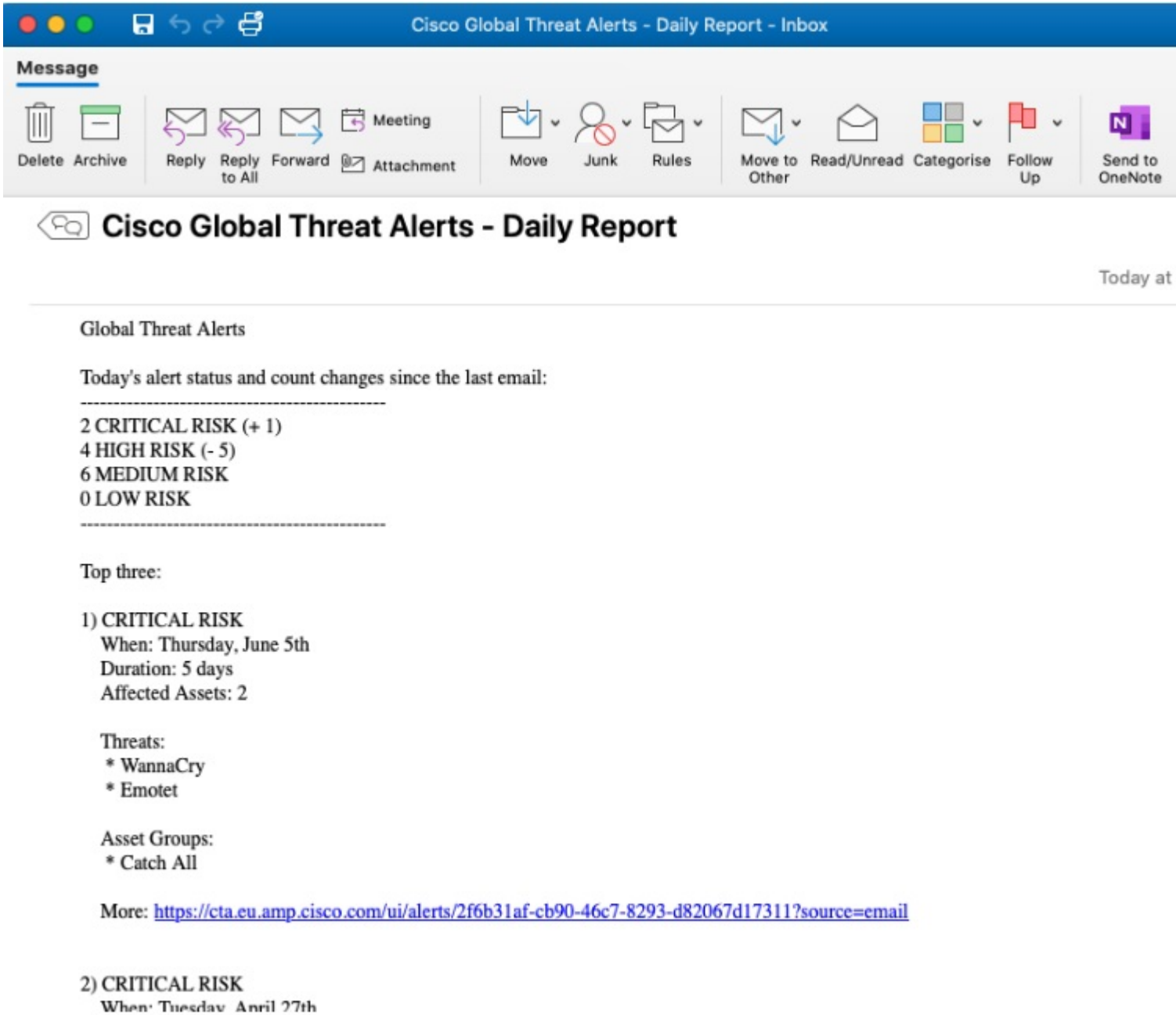
图 *18:* 导航至“应用设置”并授权与 ***SecureX*** 的集成



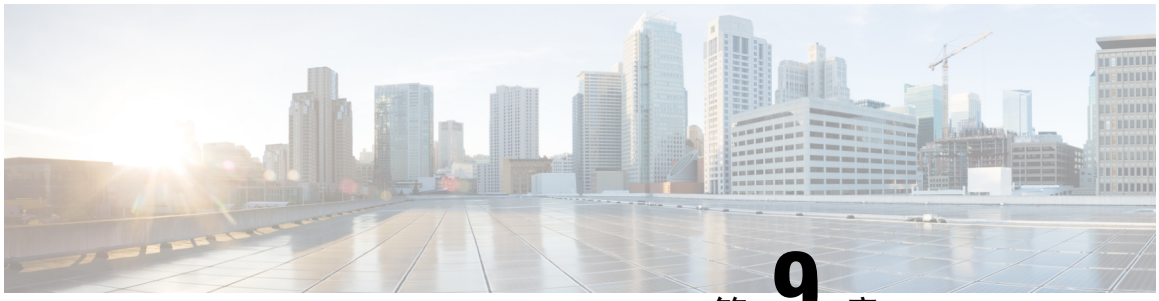
更新的每日报告电子邮件

电子邮件通知服务已更新为通过邮件向您发送与警报控制面板兼容的内容。“每日报告”电子邮件会通知您警报的当前状态以及报告的警报数量的最近变化。

图 *19:* 示例：更新的每日报告电子邮件



要启用此服务，请从全局设置菜单中选择电子邮件通知，然后输入将接收每日报告的电子邮件地址。



第 9 章

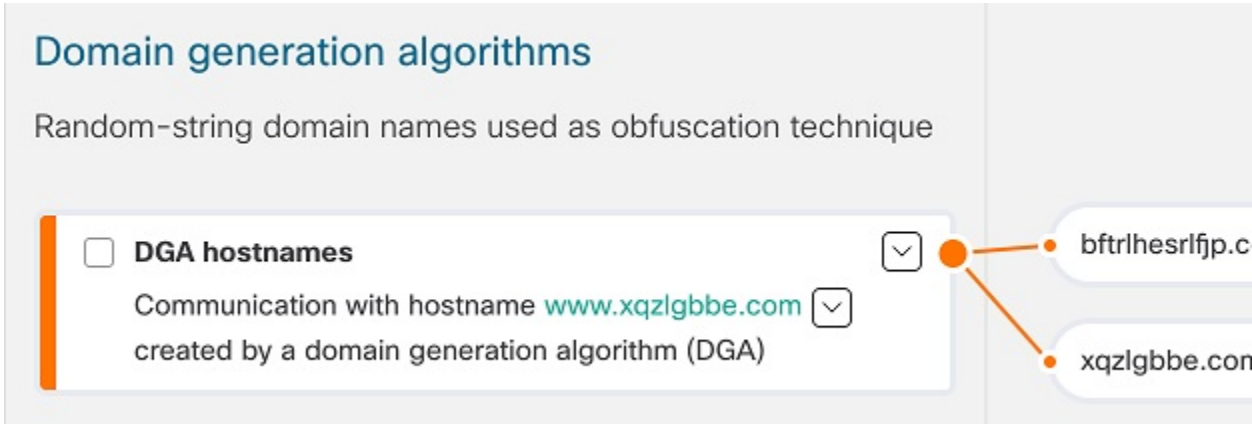
2021 年 4 月

2021 年 4 月发布的思科基于云的机器学习全局威胁警报更新。

新 DGA 2.0 分类器

攻击者使用域生成算法 (DGA) 随机生成主机名，以绕过具有阻止功能的安全产品。这些算法通常用于在僵尸网络和广告软件中进行通信。由于它们是动态生成的，因此可以成功绕过依赖静态、基于签名的监视列表的安全产品，否则这些产品会被阻止。

图 *20:* 示例：*DGA* 为混淆阻止程序生成的随机字符串域



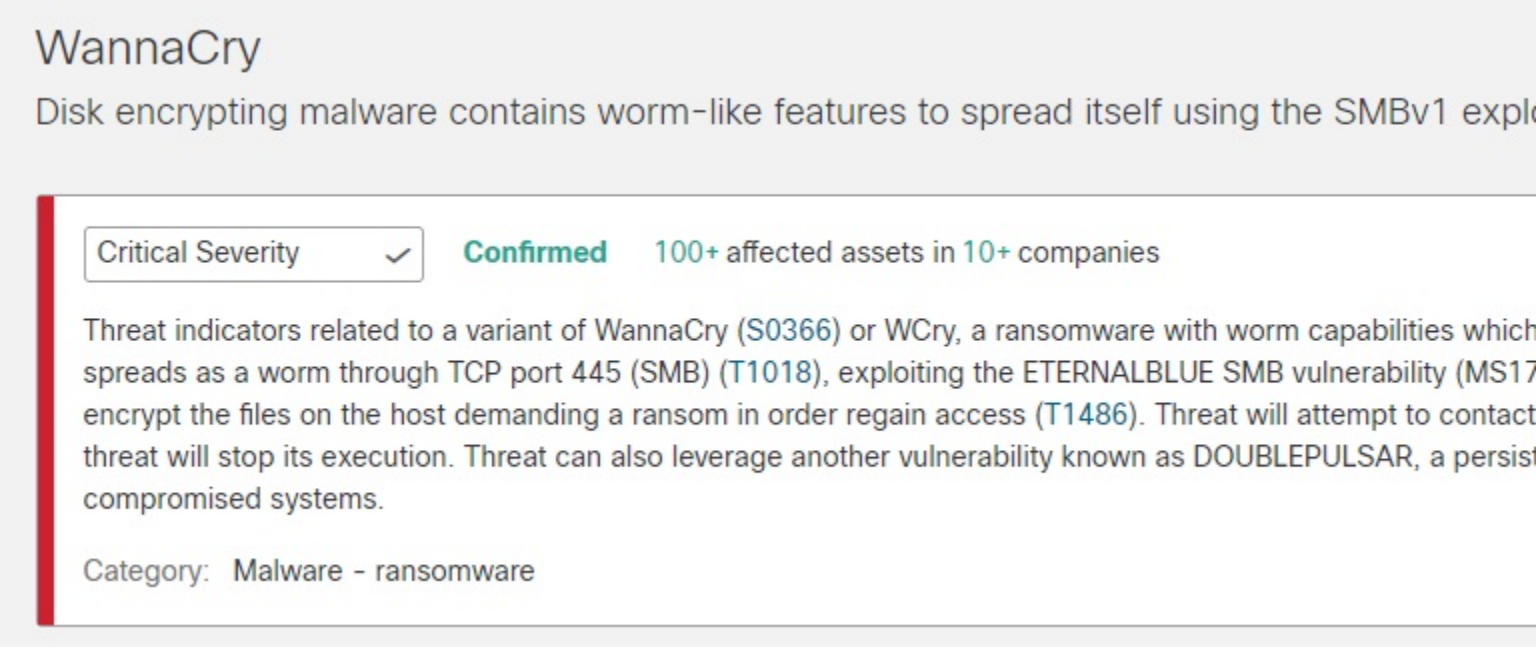
虽然自 2015 年以来，全局威胁警报已支持 DGA 域检测，但 DGA 2.0 分类器是基于神经网络（用于文本处理的最先进解决方案）而不是较旧的随机域林构建的新模型。这种架构更新和新设计的训练集可以使召回率（正确的正误差率数量）翻倍，同时产生更少的错误的正误差率。

这可以在**警报** > **警报详细信息** > **安全事件**中看到。

警报描述中的新 MITRE 参考

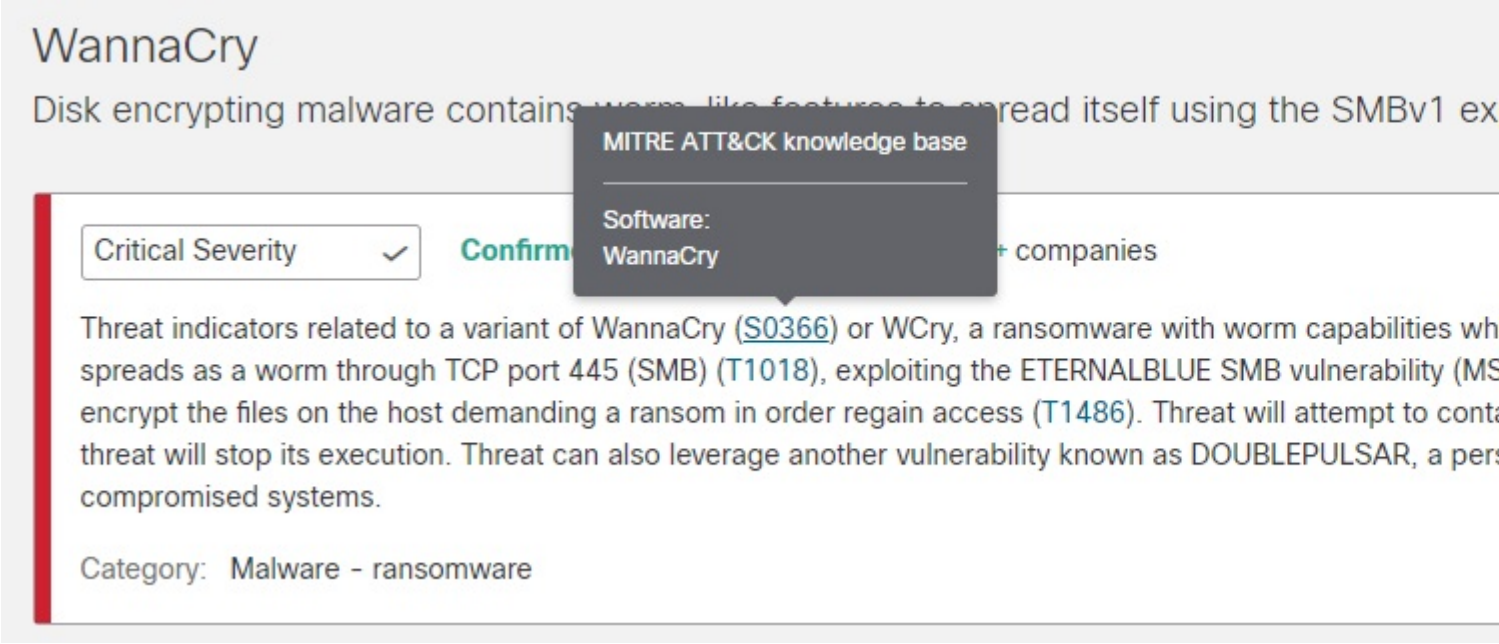
现在，我们已直接在警报的说明中添加 MITRE 引用（如果可用），以便您可以方便地访问补充信息。

图 *21:* 示例：*WannaCry* 说明中的四个 *MITRE* 引用（*S0366*、*T1018*、*T1210*、*T1486*）



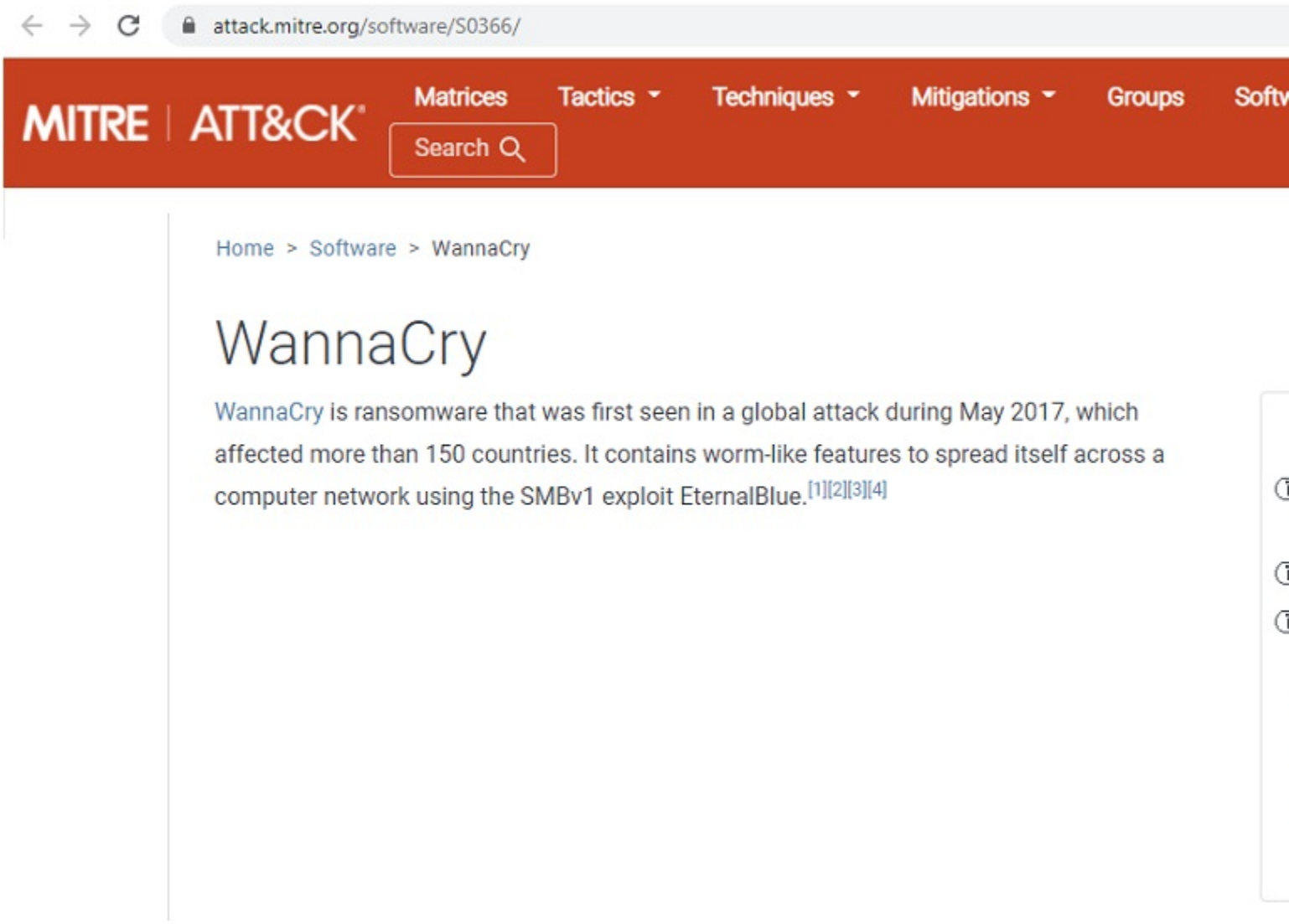
正在查找有关警报及其说明的其他详细信息？点击 ID 号码...

图 *22:* 示例：*S0366* 的 *MITRE ATT&CK* 知识库的嵌入式链接



...打开一个新的浏览器页面，将向您显示 MITRE ATT&CK 知识库，其中包含有关特定威胁的更多信息和详情。

图 *23: MITRE ATT&CK* 页面，包含有关 *S0366* 的更多信息和详情



第 10 章

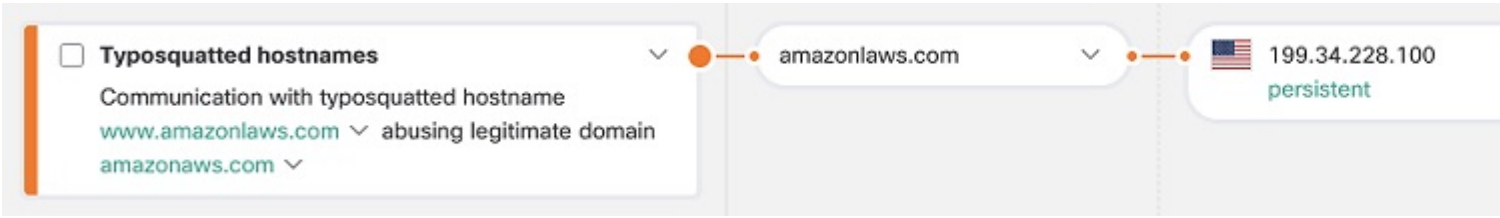
2021 年 3 月

2021 年 3 月发布的思科基于云的机器学习全局威胁警报更新。

新误植域名分类器

误植域名是一种 URL 劫持形式，它依赖于用户在其 Web 浏览器中输入 URL 时出现的印刷错误（打字错误）。这会导致用户被定向到攻击者的替代网站。误植域名 URL 看起来类似于合法 URL，例如：

图 *24:* 示例：添加了其他字母的误植域名主机名



误植域名URL通常导向在线欺诈，例如用于从广告中获利的广告页面或用于窃取用户信息的网络钓鱼页面。

图 *25:* 示例：以有意前往 ***Amazon AWS*** 的用户为目标的广告页面

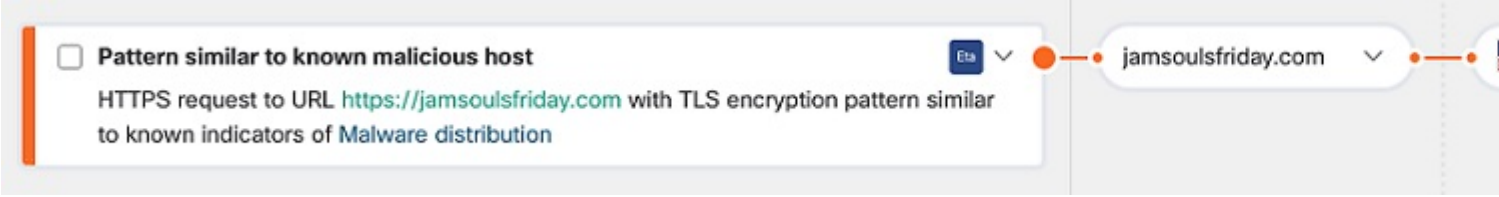
新的分类器旨在保护用户免受针对大多数常用域的误植域名域的攻击。分类器通过计算域的相似性来有效识别与最常用域相似的域。然后，分类器根据其他参数（例如，误植域名域的期限）确定威胁的严重性。

这可以在**警报** > **警报详细信息** > **安全事件**中看到。

新 TLS 模式分类器

新的分类器基于传输层安全 (TLS) 指纹技术构建。考虑到来自加密流量分析 (ETA) 的TLS报头以及其他全局和本地情景功能，分类器根据其TLS足迹检测可疑和恶意应用。通过分析已加密通信，分类器扩展了针对通过 HTTP 通信的威胁的模型的功能。

图 *26:* 示例：类似于已知为恶意的主机的 *TLS* 模式



这可以在**警报** > **警报详细信息** > **安全事件**中看到。

第 11 章

2021 年 3 月前

2021 年 3 月前

2021 年 3 月之前发布的更新将在思科社区安全博客中存档，其中包含**认知情报**标签和**认知发行说明**标签。