管理适用于IBM QRadar的云安全应用

目录

简介

本文档介绍如何管理适用于IBM QRadar的思科云安全应用。

概述

IBM的QRadar是常用的日志分析SIEM。它提供强大的接口来分析大数据块，例如Cisco Umbrella为您的组织的DNS流量提供的日志。适用于IBM QRadar的思科云安全应用中显示的信息来自Cisco Umbrella、CloudLock、Investigate和Enforcement的API。

当您为QRadar设置思科云安全应用时，它集成了思科云安全平台的所有数据，并允许您在QRadar控制台中以图形形式查看数据。从应用中，分析师可以：

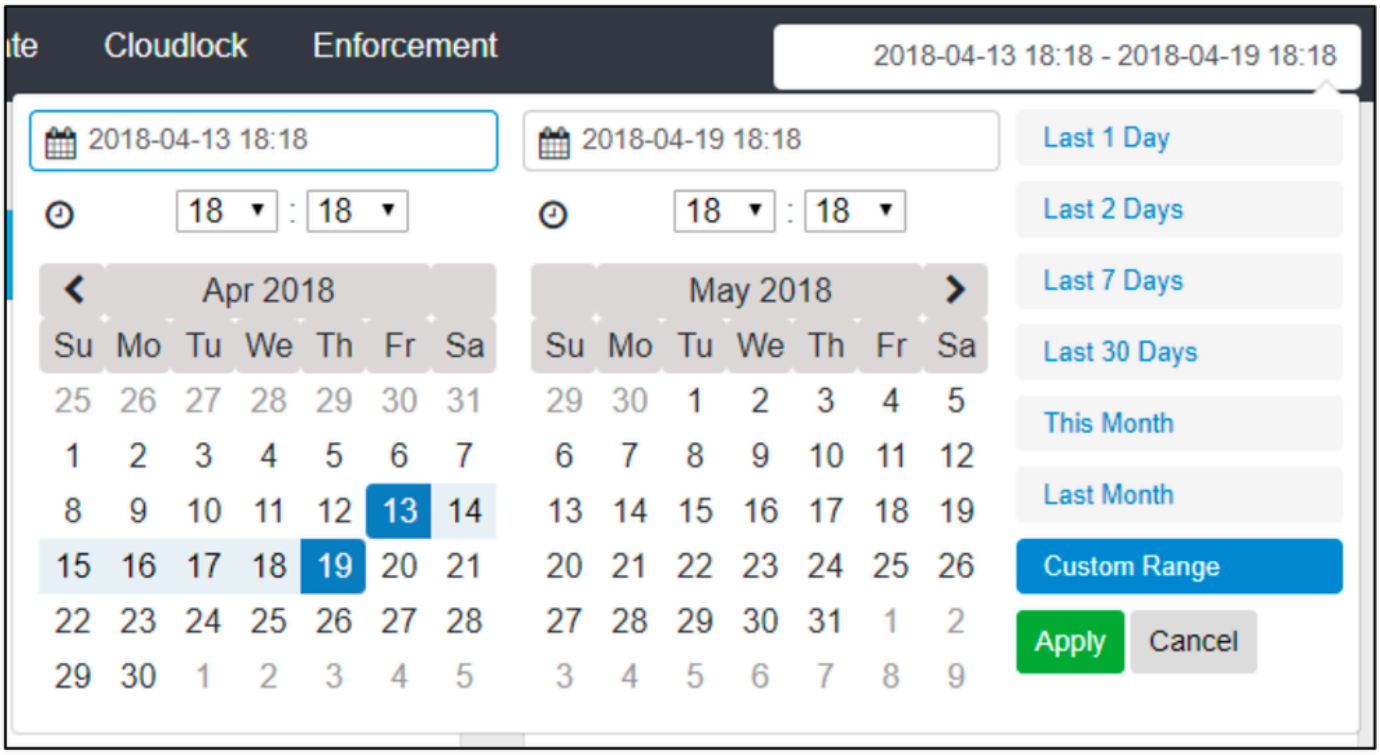
- 调查域、IP地址、邮件地址
- 阻止和取消阻止域（实施）
- 查看网络所有事件的信息。

本文将向您介绍如何导航思科云安全应用。有关如何设置应用的说明，请访问以下网址：为IBM QRadar配置思科云安全应用

访问思科云安全应用

要导航到IBM QRadar中的思科云安全应用，请转至主页并点击Cisco Cloud Security选项卡。系统将显示Cloud Overview选项卡和控制面板。然后，您可以访问Umbrella、Investigate、CloudLock和Enforcement选项卡以查看日志。

默认情况下，云安全应用设置为显示最近7天的数据。您可以通过点击右上角的日期范围来更改时间范围：

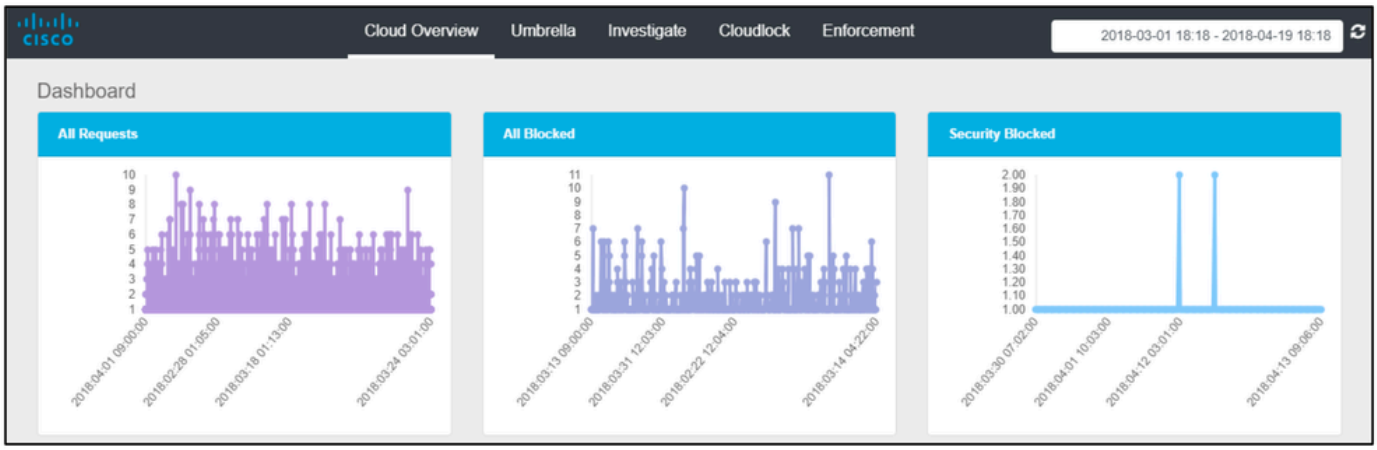


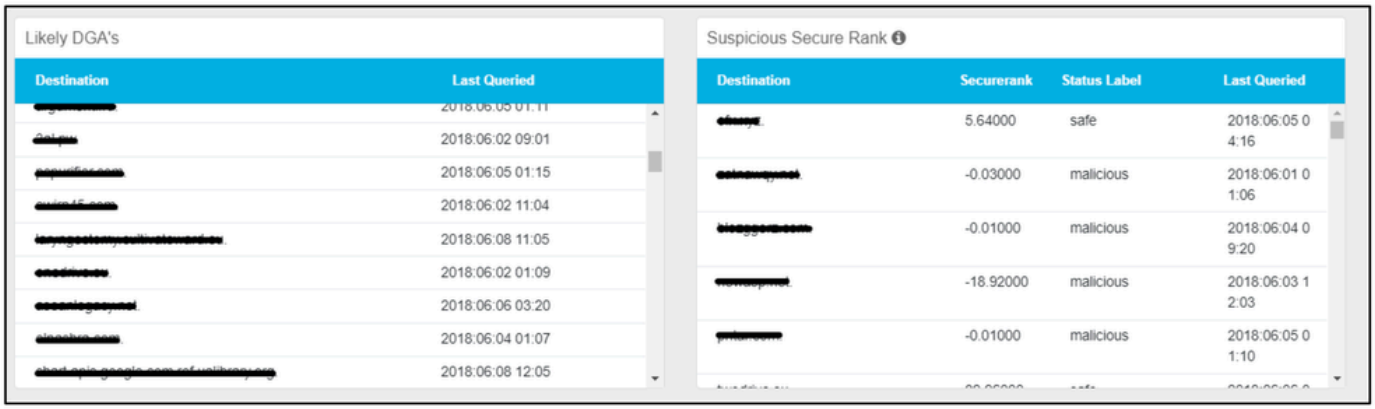
360072030052

思科云安全应用组件

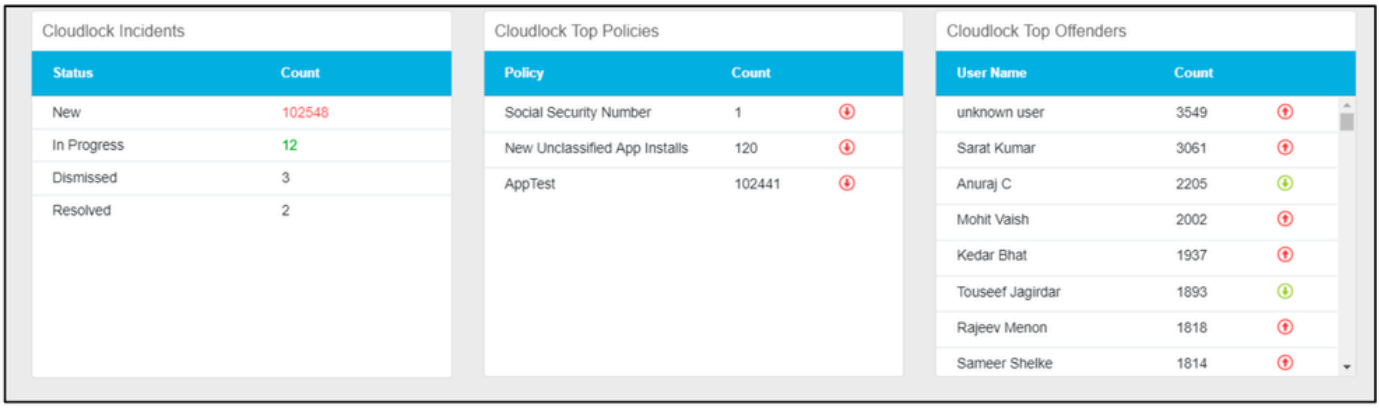
云概述

Cloud Overview（云概述）选项卡以基于图表的直观形式显示所有请求、所有已阻止、安全已阻止、可能的DGA、可疑安全排名、云锁定事件、CloudLock Overall（总体云锁定）、排名靠前的策略和排名靠前的违规者等信息。





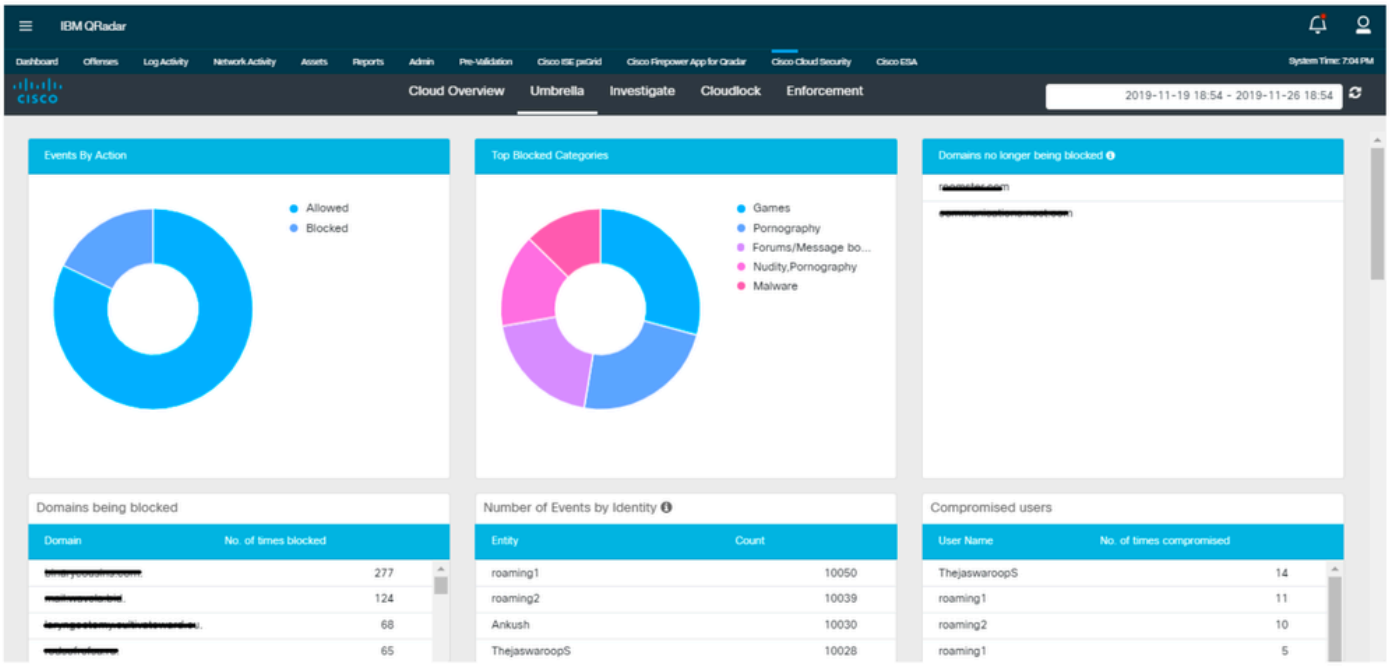
360072257631



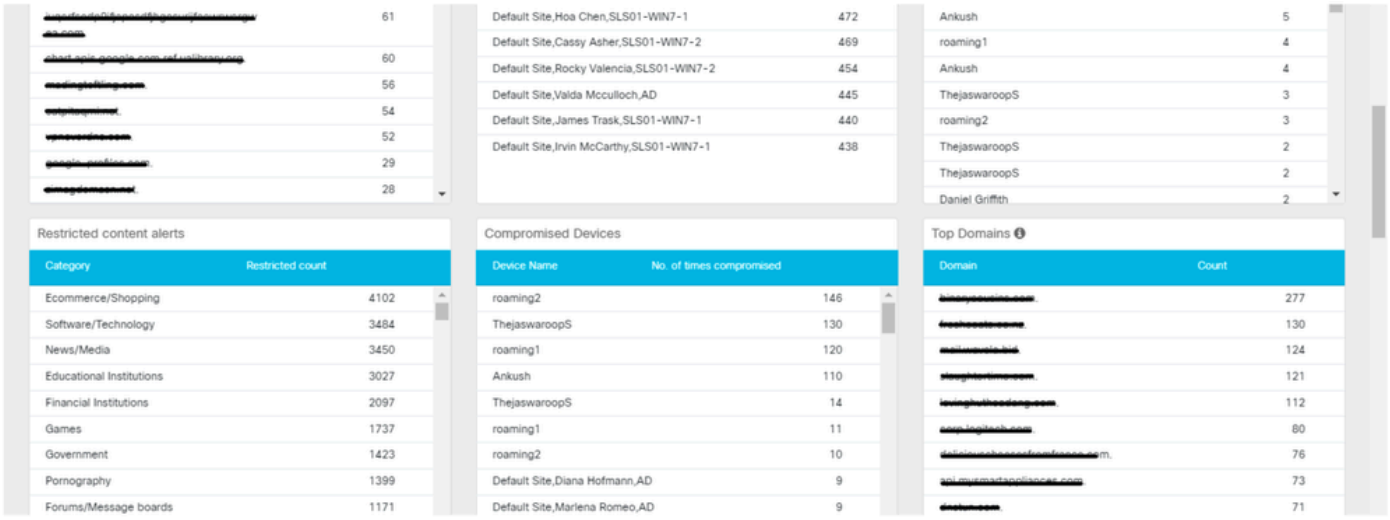
360072257611

Umbrella

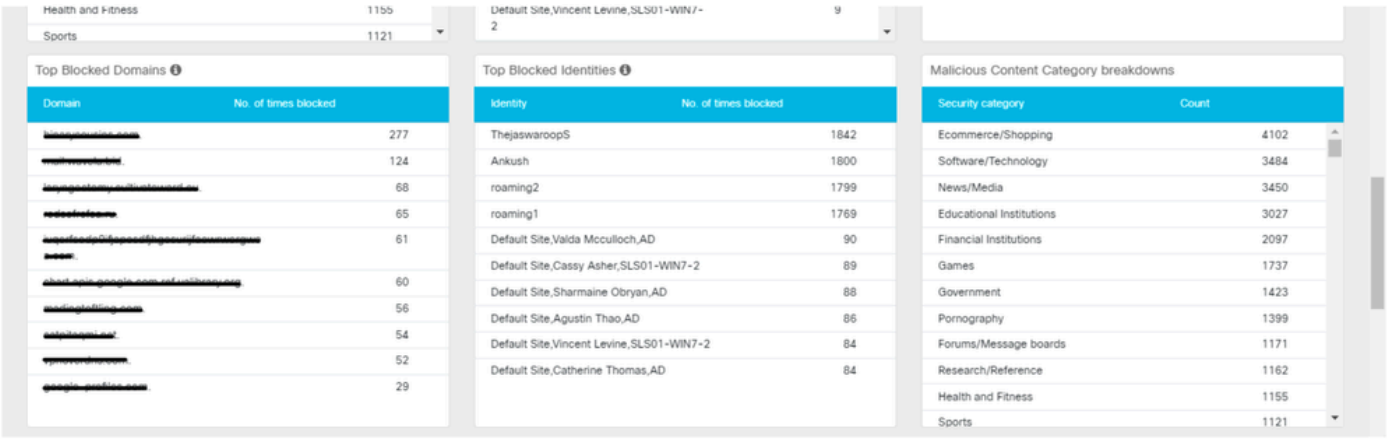
Umbrella选项卡以基于图表的视觉表示形式显示按操作显示的事件、排名靠前的阻止类别、按标识显示的事件的数量、被阻止的域、不再被阻止的域、被入侵的用户、受限制的内容警报、被入侵的设备、排名靠前的域、排名靠前的阻止的域、排名靠前的阻止的身份、恶意内容类别细分、排名靠前的类别、活动和用户访问趋势。



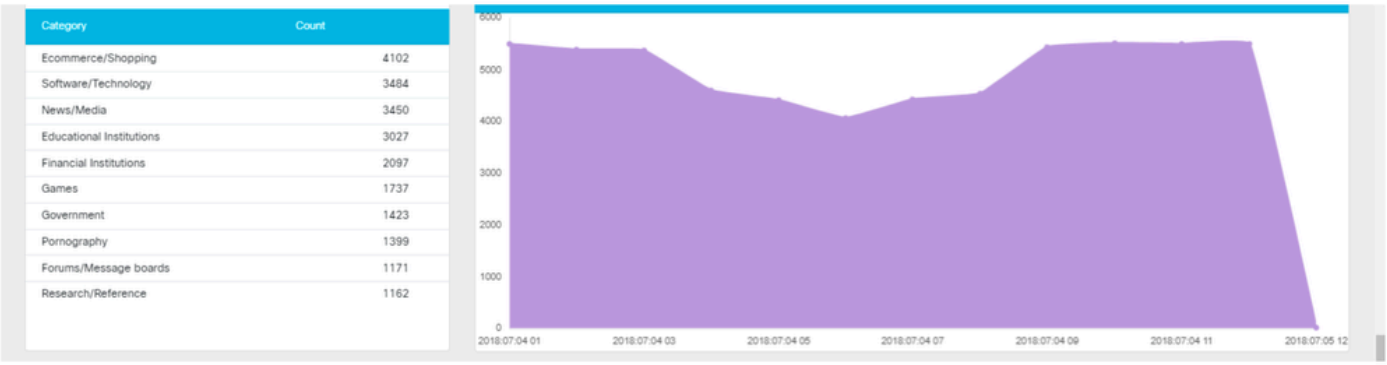
360072263411



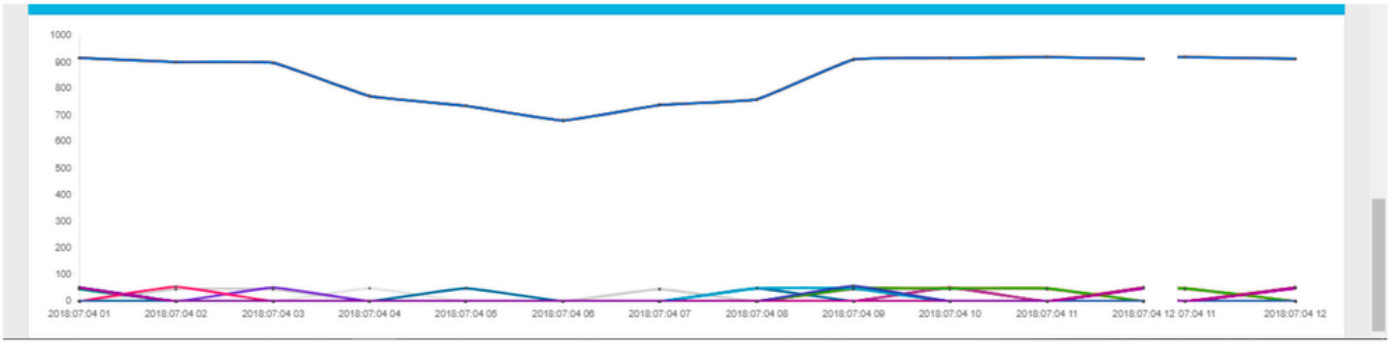
360072263391



360072037372



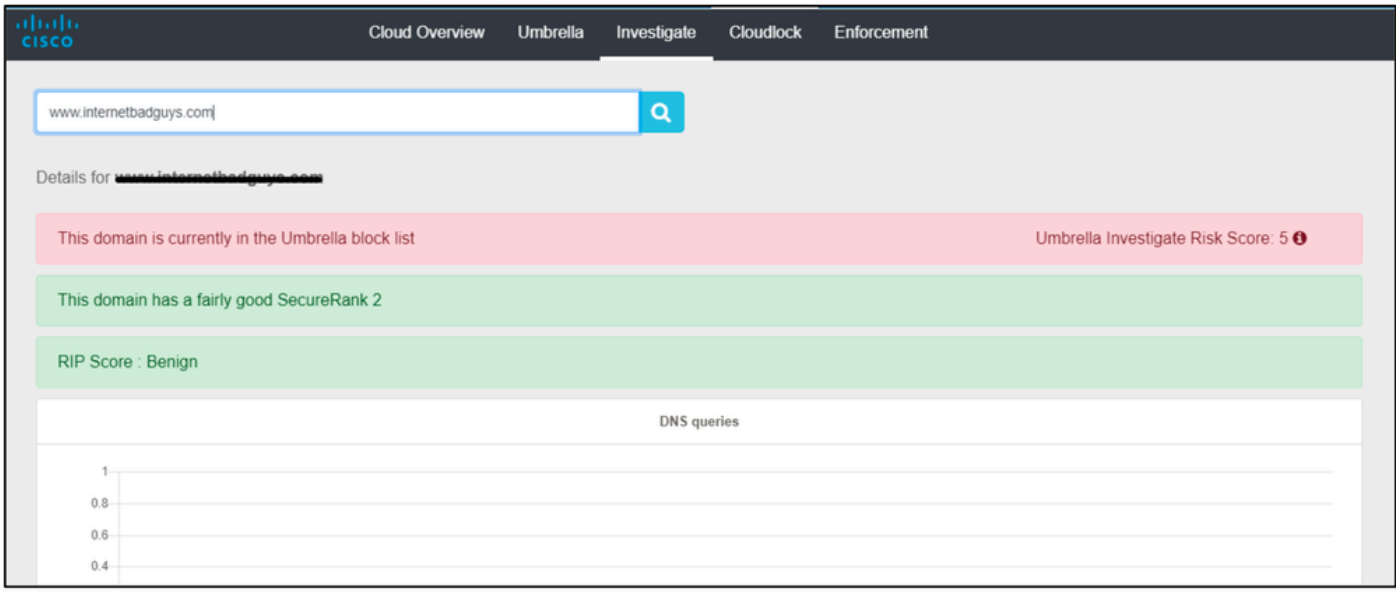
360072263331



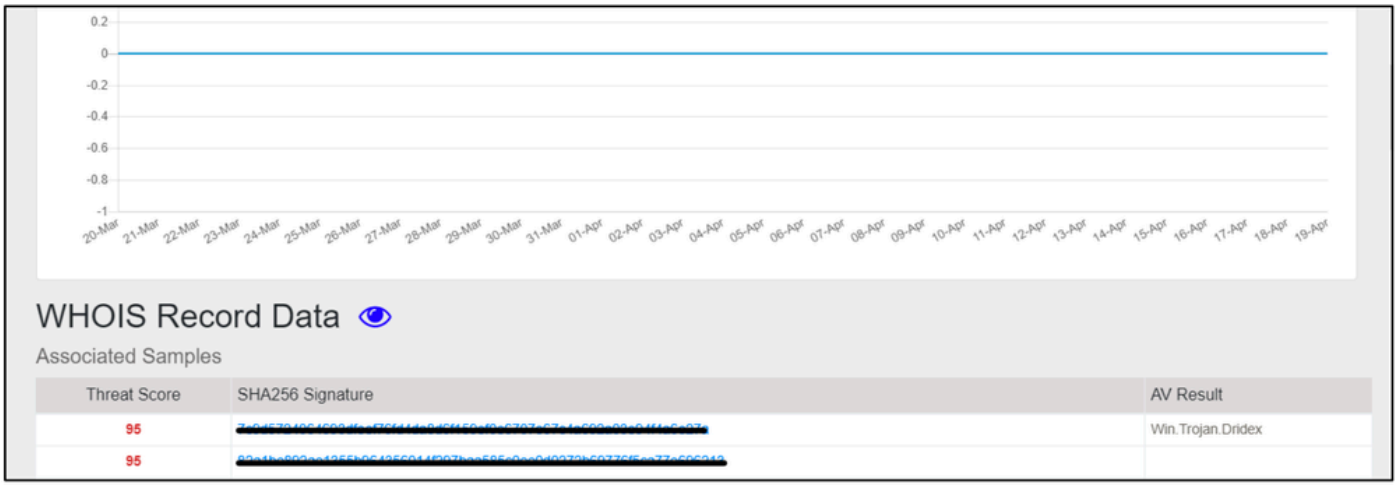
360072263351

调查

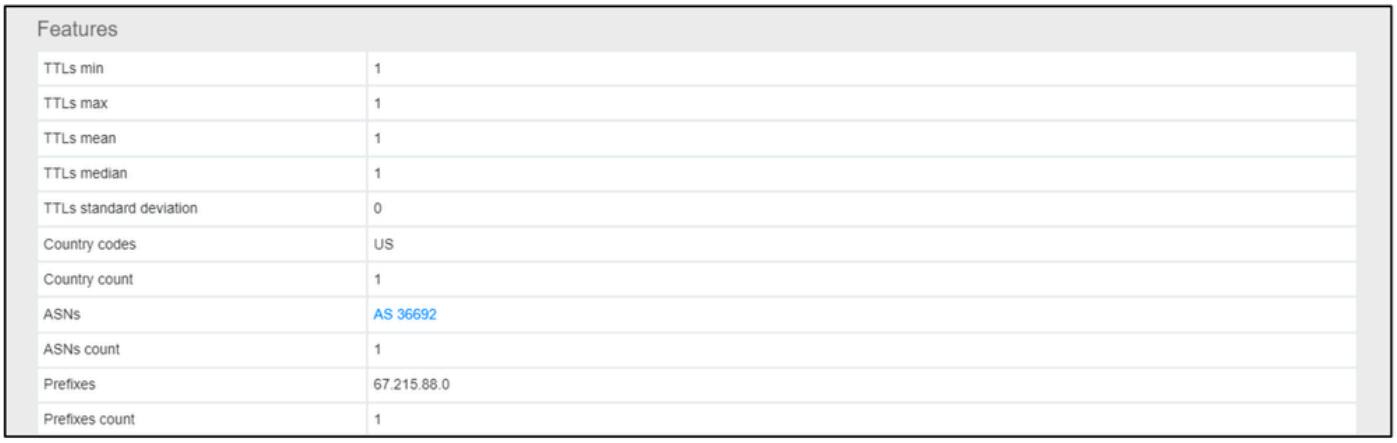
Investigate选项卡使用户能够搜索与主机名、URL、ASN、IP、散列或电子邮件地址相关的信息。它还具有WHOIS记录、DGA信息等信息。



360072263511



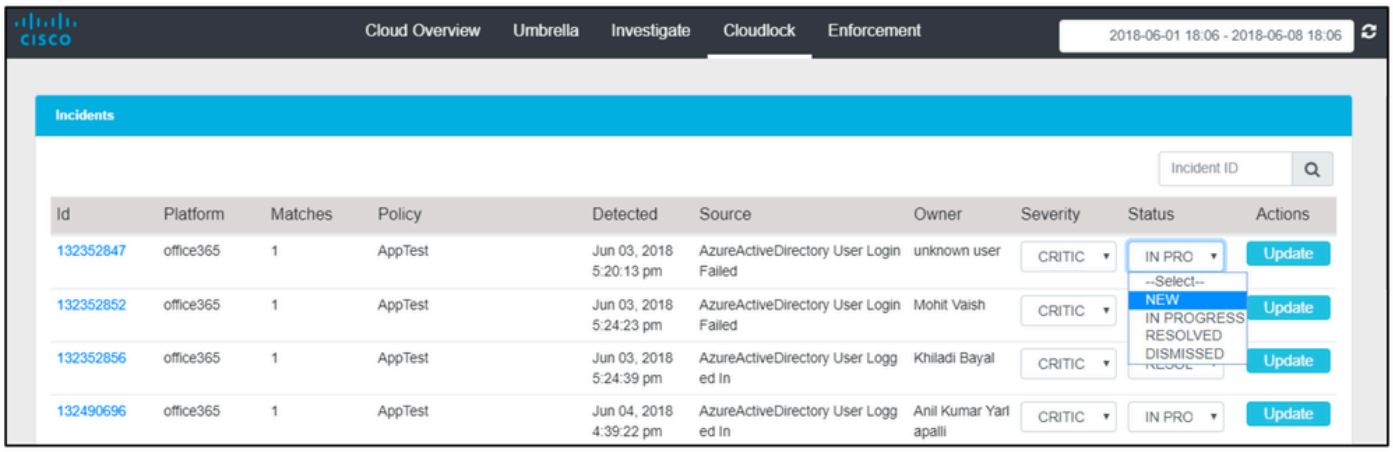
360072037472



360072037452

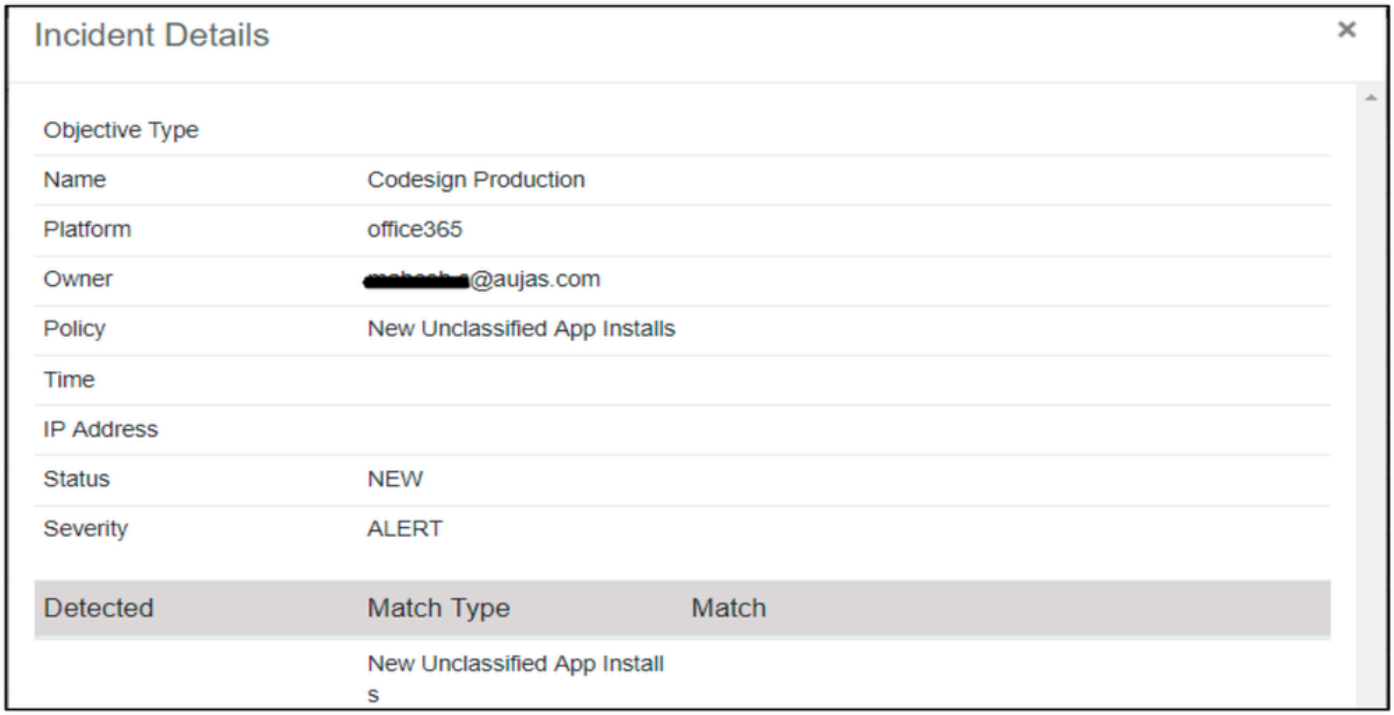
CloudLock

通过CloudLock选项卡，用户可以查看有关检测到的所有事件的信息。用户还可以通过从下拉菜单中选择值并点击“更新”来更新事件的严重性和状态。



360072268311

用户可以锁定任何事件，以查看有关该事件的更多详细信息。



360072042332

“实施”选项卡

Enforcement选项卡显示有关哪些域被阻止的信息。用户还可以选择阻止的域并从此界面中取消阻止它们。

360072038472

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

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

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