了解WBNP和SBNP

目录

简介

背景信息

- WSA - WebBase网络参与
- ESA - SenderBase网络参与

一般安全问题常见问题解答

操作

- SenderBase（邮件）网络参与
  - 每个邮件设备共享的统计信息
  - 每个IP地址共享的统计信息
  - 每个SDS客户端共享的统计信息
  - AMP SBNP遥测数据
- WebBase(Web)网络参与
  - 每个Web请求共享的统计信息
  - 每个Web请求的高级恶意软件统计信息
  - 最终用户反馈统计信息源
  - 提供的示例数据 — 标准参与
  - 提供的示例数据 — 参与受限
  - 完整WBNP解码
  - 每个Web请求共享的统计信息
  - 每个Web请求的高级恶意软件统计信息
  - 最终用户反馈统计信息源

Talos检测内容

专注于威胁

相关信息

简介

本文档介绍遥测数据到Cisco和Talos的后向路径。

背景信息

思科Web和邮件内容安全产品可以向思科和Talos提供遥测数据，以提高网络安全设备(WSA)中网络分类以及连接邮件安全设备(ESA)的IP信誉的有效性。

遥感勘测数据在选择的基础上提供给WSA和ESA。

数据通过二进制编码SSL加密数据包传输。随附的附件提供了对数据、特定格式和传输数据的说明的深入信息。

无法以直接日志或文件格式查看WebBase网络参与(WBNP)和SenderBase网络参与(SBNP)数据。该数据以加密形式传输。此数据在任何时候都不是“静态”。

WSA - WebBase网络参与

思科认识到维护隐私的重要性，不会收集或使用个人或机密信息，如用户名和密码。此外，主机名中包含的文件名和URL属性会被模糊处理，以确保机密性。

当涉及解密HTTPS事务时，SensorBase网络仅接收证书中服务器名称的IP地址、Web信誉分数和URL类别。

有关完整信息，请查看WSA用户指南，了解设备上当前运行的AsyncOS for Web Security的版本。

请参阅ESA用户指南中的Cisco SensorBase网络。

ESA - SenderBase网络参与

如果您参与SenderBase网络，则允许思科收集有关您组织的汇总电子邮件流量统计信息，从而增加面向所有用户的服务实用程序。参与是自愿的。思科仅收集有关邮件属性的摘要数据，以及有关思科设备如何处理不同类型邮件的信息。例如，思科不收集邮件正文或邮件主题。个人身份信息和标识组织的信息将保密。

有关完整信息，请查看ESA用户指南，了解设备上当前运行的AsyncOS for ESA Security的版本。

请参阅《用户指南》中的SenderBase网络参与章节。

一般安全问题常见问题解答

收集的数据存储在哪里？

设备遥测存储在思科美国数据中心。

谁有权访问收集和存储的数据？

仅限分析/使用数据以创建可操作情报的Cisco SBG人员访问。

所收集数据的保留时间是多久？

没有与设备遥测相关的数据保留/过期策略。数据可以无限期保留，也可以出于各种原因删除，包括但不限于缩减采样/聚合、存储管理、使用期限、与当前/未来威胁的相关性等。

客户序列号或公有IP地址是否存储在Talos分类数据库中？

否，仅保留URL和类别。WBNP数据包不包含源IP信息。

操作

本节详细介绍操作、数据类型（按说明）和示例数据，以演示要传输的信息：

- SBNP — 与邮件安全相关的特定数据类型（字段）和示例数据
- WBNP — 与网络安全相关的特定数据类型（字段）和示例数据
- 威胁检测操作 — 从操作角度概述威胁检测

SenderBase（邮件）网络参与

每个邮件设备共享的统计信息

项目	示例数据
MGA标识符	MGA设10012
时间戳	数据从2005年7月1日上午8点至下午8点05分
软件版本号	MGA版本4.7.0
规则集版本号	反垃圾邮件规则集102
防病毒更新间隔	每10分钟更新一次
隔离区大小	500 MB
隔离邮件计数	隔离区当前有50封邮件
病毒分数阈值	将邮件发送到威胁级别为3或更高的隔离区
进入隔离区的邮件的病毒分数总和	120
进入隔离区的邮件计数	30（平均得分为4）
最长隔离时间	12 小时
按进入和退出隔离区的原因划分的爆发隔离区邮件的计数，与防病毒结果关联	50个由于.exe规则进入隔离区30个由于手动释放而离开隔离区，所有30个均为病毒阳性
按离开隔离区后采取的操作划分的爆发隔离区邮件计数	10封邮件在离开隔离区后附件被删除

邮件在隔离区中保留的时间总和	20 小时

每个IP地址共享的统计信息

项目	示例数据	标准参与	有限参与
设备内不同阶段的邮件计数	被防病毒引擎发现：100 被反垃圾邮件引擎看到：80		
反垃圾邮件和防病毒分数与判定的总和	2,000（所有查看邮件的反垃圾邮件分数总和）		
命中不同反垃圾邮件和防病毒规则组合的邮件数	100条消息命中规则A和B 仅50封邮件命中规则A		
连接的数量	20个SMTP连接		
收件人总数和无效收件人数	共50个收件人 10个无效收件人		
散列文件名：(a)	在名为<one-way-hash>.zip的存档附件中找到文件<one-way-hash>.pif。	未模糊的文件名	散列文件名
模糊文件名：(b)	在文件aaaaaa.zip中找到文件aaaaaa0.aaa.pif。	未模糊的文件名	模糊文件名
URL主机名(c)	在发往www的消息中找到一个链接。domain.com	未模糊的URL主机名	模糊的URL主机名
模糊的URL路径(d)	在发往主机名www的消息中找到一个链接。domain.com，路径为aaa000aa/aa00aaa。	未模糊的URL路径	模糊的URL路径
按垃圾邮件和病毒扫描结果统计的邮件数	10个垃圾邮件 10个垃圾邮件 5可疑垃圾邮件 4病毒阳性 16病毒阴性 5病毒无法扫描		

按不同的反垃圾邮件和防病毒判定结果统计的邮件数	500个垃圾邮件、300个火腿		
大小范围内的邮件计数	30K-35K范围内有125个		
不同分机类型的计数	300个“.exe”附件		
附件类型、实际文件类型和容器类型的关联	100个附件具有“.doc”扩展名但实际为“.exe” 50个附件是zip中的“.exe”扩展名		
扩展名和实际文件类型与附件大小的关联	50-55K范围内有30个附件为“.exe”		
按随机抽样结果统计的消息数	14条消息跳过采样 25条消息排队等待采样 通过采样扫描50封邮件		
DMARC验证失败的邮件数	有34封邮件未通过DMARC验证		

注意：

(a)文件名以1次散列(MD5)编码。

(b)文件名以模糊形式发送，所有小写ASCII字母([a-z])替换为"a"，所有大写ASCII字母([A-Z])替换为"A"，任何多字节UTF-8字符替换为"x"（为其他字符集提供隐私），所有ASCII数字([0-9])替换为。

(c)与IP地址一样，URL主机名指向提供内容的Web服务器。不包括用户名和密码等机密信息。

(d)主机名中包含的URL信息会被模糊处理，以确保不泄露用户的任何个人信息。

每个SDS客户端共享的统计信息

项目	示例数据
时间戳	

客户机版本	
向客户端发出的请求数	
从SDS客户端发出的请求数	
DNS查找的时间结果	
服务器响应时间结果	
建立与服务器的连接所需的时间	
已建立的连接数	
到服务器的并发打开连接数	
到WBRS的服务请求数	
到达本地WBRS缓存的请求数	
本地WBRS缓存的大小	
远程WBRS的响应时间结果	

AMP SBNP遥测数据

Format	示例数据
amp_verdicts' :{ (“裁决”、“间谍名称”、“分数”、“已上传”、“文件名”)	
("verdict"、"spyname"、"score"、"uploaded"、"file_name"),	
("verdict"、"spyname"、"score"、"uploaded"、"file_name"),	
.....	

("verdict"、"spyname"、"score"、"uploaded"、"file_name"),	
}	
描述	
裁决 — AMP信誉查询	恶意/干净/未知
Spyname — 检测到的恶意软件的名称	[特洛伊木马测试]
分数 — AMP分配的信誉分数	[1-100]
上传 — 指示上传文件的AMP云	1
File Name — 文件附件的名称	abcd.pdf

WebBase(Web)网络参与

每个Web请求共享的统计信息

项目	示例数据	标准参与	有限参与
version	coeus 7.7.0-608		
Serial Number			
SBNP采样系数（体积）			
SBNP采样系数（速率）	1		
目标IP和端口		未模糊的URL路径段	散列URL路径段
反间谍软件选择的恶意软件类别	已跳过		

WBRS得分	4.7		
McAfee恶意软件类别判定			
引用方URL		未模糊的URL路径段	散列URL路径段
内容类型ID			
ACL决策标记	0		
传统Web分类			
CIWUC Web类别和决策来源	{'src':'req', 'cat':“1026”}		
AVC应用名称	广告和跟踪		
AVC应用类型	广告网络		
AVC应用行为	不安全		
内部AVC结果跟踪	[0,1,1,1]		
通过索引数据结构跟踪用户代理	3		

每个Web请求的高级恶意软件统计信息

AMP统计信息	
裁决 — AMP信誉查询	恶意/干净/未知
Spyname — 检测到的恶意软件的名称	[特洛伊木马测试]
分数 — AMP分配的信誉分数	[1-100]

上传 — 指示上传文件的AMP云	1
File Name — 文件附件的名称	abcd.pdf

最终用户反馈统计信息源

按最终用户共享的统计信息分类错误反馈	
项目	示例数据
引擎ID（数字）	0
传统Web分类代码	
CIWUC Web分类源	'响应' / '请求'
CIWUC Web类别	1026

提供的示例数据 — 标准参与

```
# categorized
"http://google.com/": {    "wbrs": "5.8",
    "fs": {
          "src": "req",
          "cat": "1020"
    },
}

# uncategorized
"http://fake.example.com": {    "fs": {
      "cat": "-"
    },}
```

提供的示例数据 — 参与受限

- 来自客户端的原始请求：www.example.com/Sample-Web-Request-Path
- 记录的消息（在遥测服务器中）：http://www.example.com/76bd845388e0

完整WBNP解码

每个思科设备共享的统计信息：

项目	示例数据
version	coeus 7.7.0-608
序列号	0022190B6ED5-XYZ1YZ2
型号	S660
Webroot已启用	1
已启用AVC	1
已启用Sophos	0
响应端分类已启用	1
已启用反间谍软件引擎	default-2001005008
反间谍软件SSE版本	default-2001005008
反间谍软件Spycat定义版本	default-8640
反间谍软件URL阻止列表DAT版本	
反间谍软件URL网络钓鱼DAT版本	
反间谍软件Cookie DAT版本	
已启用反间谍软件域阻止	0
反间谍软件威胁风险阈值	90

已启用McAfee	0
McAfee引擎版本	
McAfee DAT版本	default-5688
WBNP详细级别	2
WBRS引擎版本	freebsd6-i386-300036
WBRS组件版本	categories=v2-1337979188,ip=default-1379460997,keyword=v2-1312487822,prefixcat=v2-1379460670,rule=default-1358979215
WBRS阻止列表阈值	-6
WBRS允许列表阈值	6
已启用WBRS	1

支持安全移动	0
L4流量监控器已启用	0
L4通信监控阻止列表版本	default-0
L4流量监控管理阻止列表	
L4通信监控管理阻止列表端口	
L4通信监控允许列表	
L4通信监控允许列表端口	
SBNP采样系数	0.25

SBNP采样系数（体积）	0.1
SurfControl SDK版本（旧版）	default-0
SurfControl完整数据库版本（旧版）	default-0
SurfControl本地增量累积文件版本（旧版）	default-0
Firestone引擎版本	default-210016
Firestone DAT版本	v2-310003
AVC引擎版本	default-110076
AVC DAT版本	default-1377556980
Sophos引擎版本	default-1310963572
Sophos DAT版本	default-0
已启用自适应扫描	0
自适应扫描风险评分阈值	[10、6 和 3]
自适应扫描负载系数阈值	[5、3 和 2]
已启用SOCKS	0
事务总数	

事务总数	
允许的事务总数	
检测到的恶意软件事务总数	

被管理员策略阻止的事务总数	
被WBRS得分阻止的事务总数	
高风险事务总数	
流量监控器检测到的事务总数	
与IPv6客户端的交易总数	
与IPv6服务器的事务总数	
使用SOCKS代理的事务总数	
来自远程用户的事务总数	
来自本地用户的事务总数	
使用SOCKS代理允许的总事务数	
允许使用SOCKS代理的本地用户事务总数	
允许使用SOCKS代理的远程用户事务总数	
使用SOCKS代理阻止的事务总数	
使用SOCKS代理阻止的本地用户的事务总数	
使用SOCKS代理阻止的远程用户事务总数	

自上次重新启动以来的秒数	2843349
CPU利用率(%)	9.9
RAM利用率(%)	55.6

硬盘使用率(%)	57.5
带宽利用率（/秒）	15307
开放式TCP连接	2721
每秒事务数	264
客户端延迟	163
缓存命中率	21
代理CPU利用率	17
WBRS WUC CPU利用率	2.5
记录CPU利用率	3.4
报告CPU利用率	3.9
Webroot CPU利用率	0
Sophos CPU利用率	0
McAfee CPU利用率	0
vmstat实用程序输出(vmstat -z， vmstat -m)	
配置的访问策略数量	32
已配置的自定义Web类别的数量	32
身份验证提供程序	基本，NTLMSSP
身份验证领域	身份验证提供程序主机名、协议和其他配置

	元素

每个Web请求共享的统计信息

项目	示例数据	标准参与	有限参与
version	coeus 7.7.0-608		
Serial Number			
SBNP采样系数（体积）			
SBNP采样系数（速率）	1		
目标IP和端口		未模糊的URL路径段	散列URL路径段
反间谍软件选择的恶意软件类别	已跳过		
WBRS得分	4.7		
McAfee恶意软件类别判定			
引用方URL		未模糊的URL路径段	散列URL路径段
内容类型ID			
ACL决策标记	0		
传统Web分类			
CIWUC Web类别和决策来源	{'src':'req', 'cat':“1026”}		

AVC应用名称	广告和跟踪		
AVC应用类型	广告网络		
AVC应用行为	不安全		
内部AVC结果跟踪	[0,1,1,1]		
通过索引数据结构跟踪用户代理	3		

每个Web请求的高级恶意软件统计信息

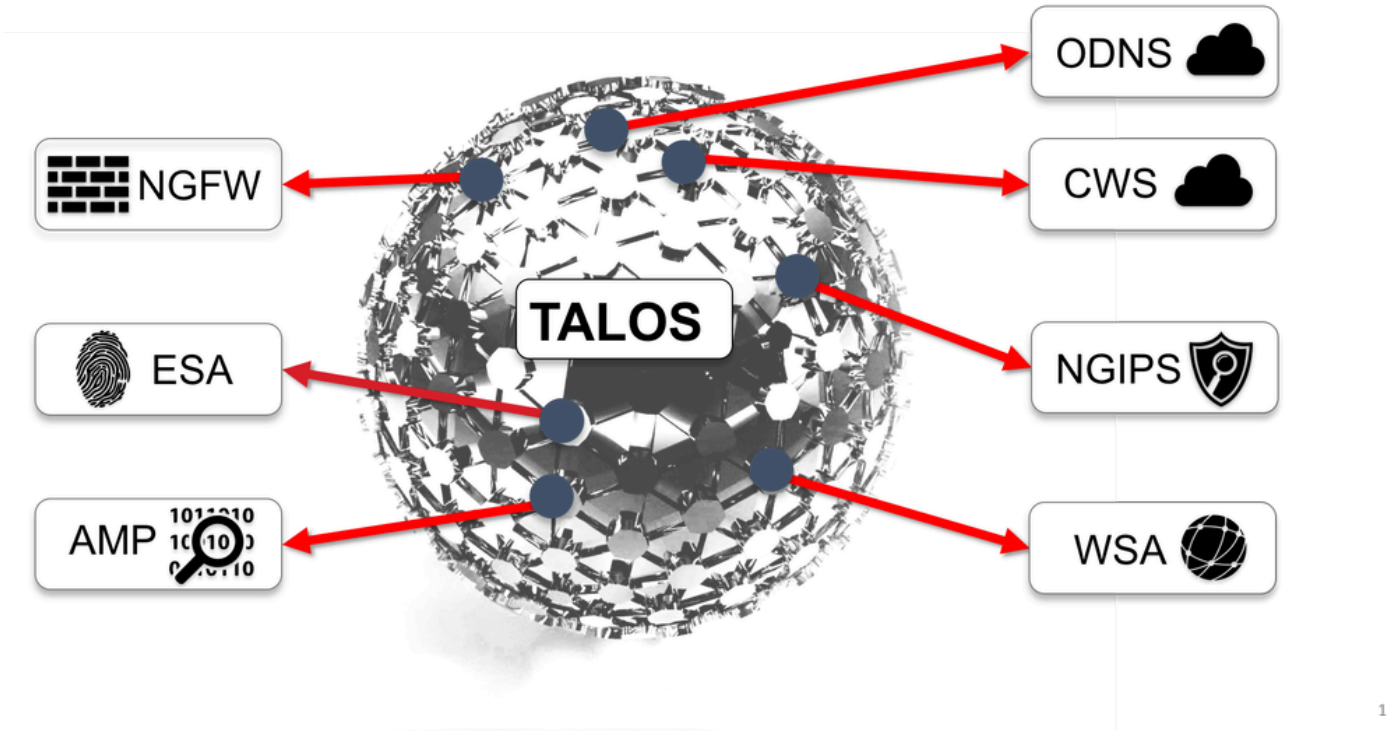
AMP统计信息	
裁决 — AMP信誉查询	恶意/干净/未知
Spyname — 检测到的恶意软件的名称	[特洛伊木马测试]
分数 — AMP分配的信誉分数	[1-100]
上传 — 指示上传文件的AMP云	1
File Name — 文件附件的名称	abcd.pdf

最终用户反馈统计信息源

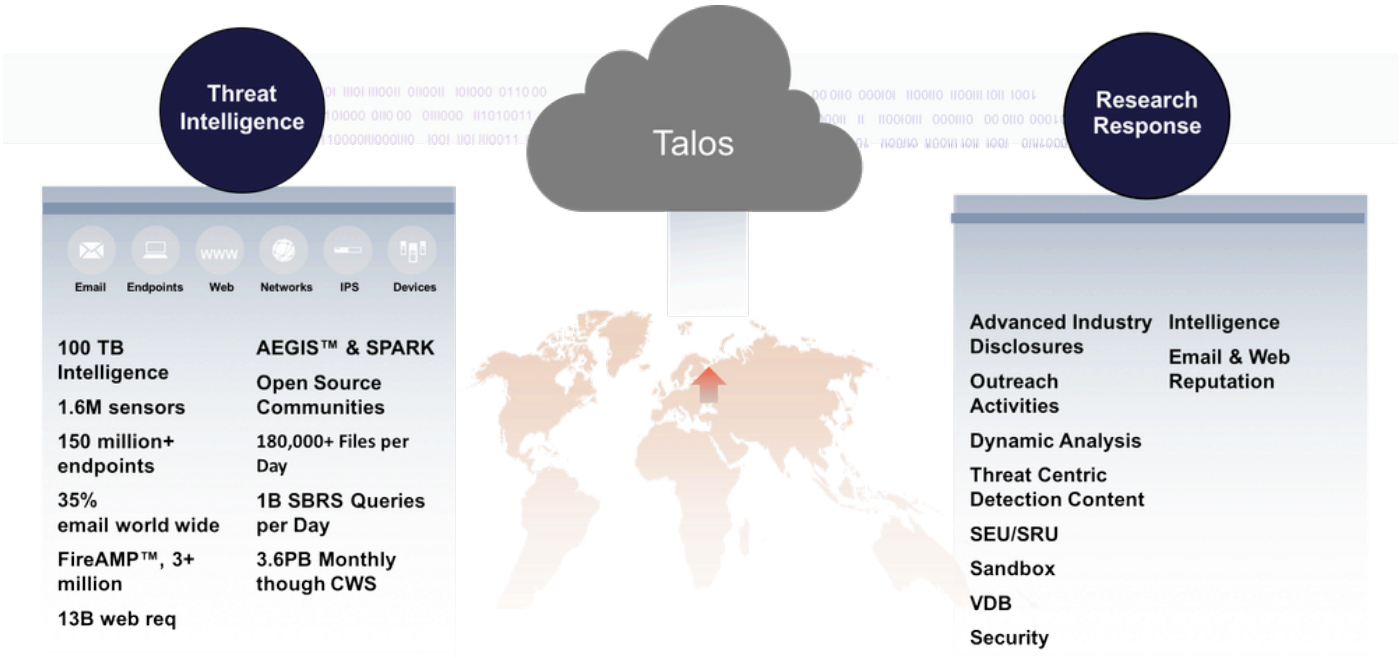
按最终用户共享的统计信息分类错误反馈	
项目	示例数据
引擎ID（数字）	0
传统Web分类代码	

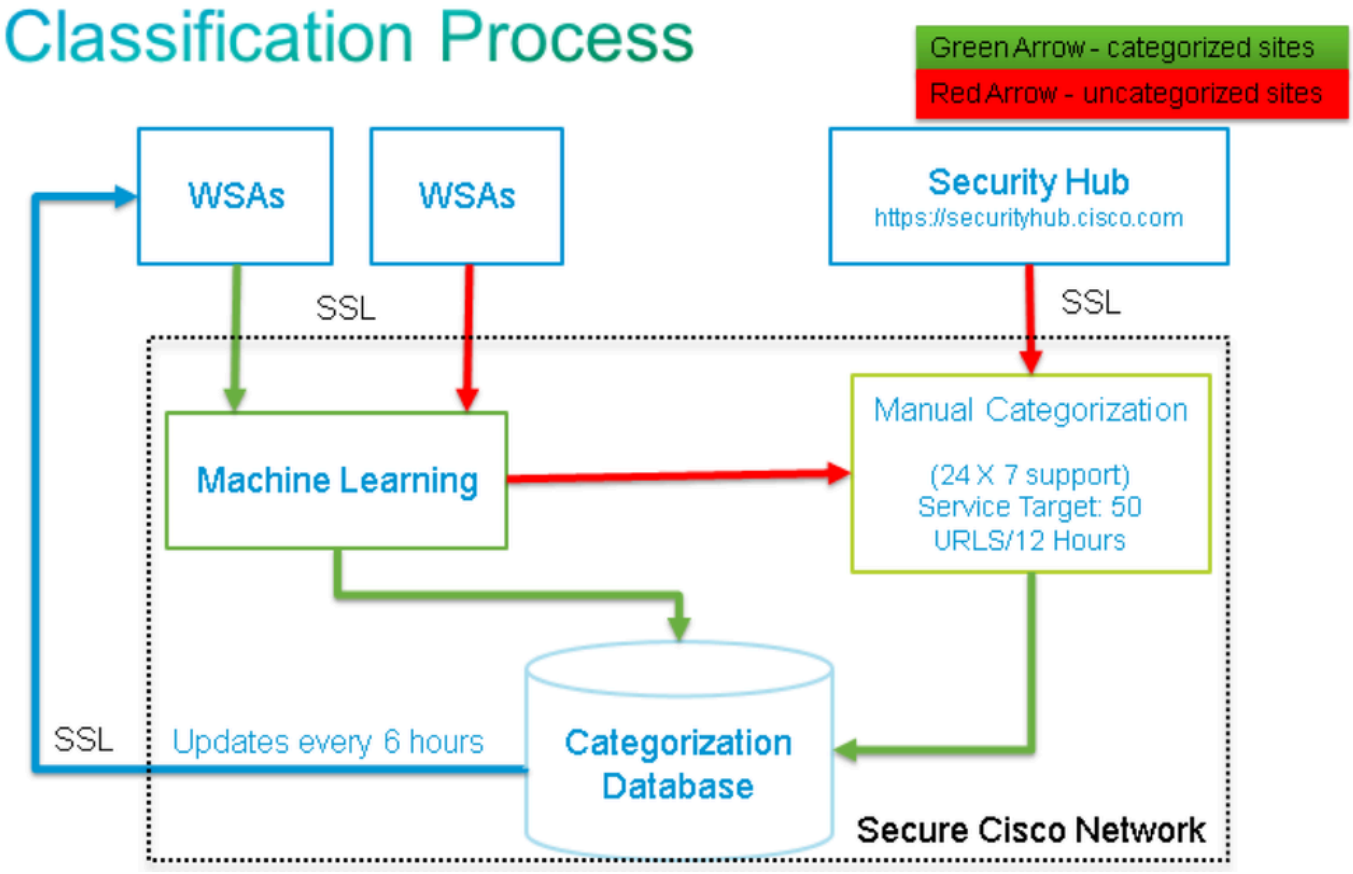
CIWUC Web分类源	'响应' / '请求'
CIWUC Web类别	1026

Talos检测内容



专注于威胁





相关信息

- 思科网络安全设备 — 产品页面
- 思科邮件安全设备 — 产品页面
- 技术支持和文档

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）。