TAC产品使用分析培训

2019护网专项培训

NSFOCUS

CONTENTS 目 录

01

产品简介

TAC是什么？

- TAC: Threat Analysis Center
- 威胁分析系统
- 针对高级威胁，具备多种检测能力的分析系统
- 针对APT、勒索软件、特种木马等高级威胁的，具备信誉、病毒检测、静态、动态检测技术的威胁分析系统
- TAC可以作为传统安全设备检测能力的扩展组件：与IPS/FW/SEG联动，组成NGTP解决方案，通过联动，建立针对高级威胁的检测与防御能力

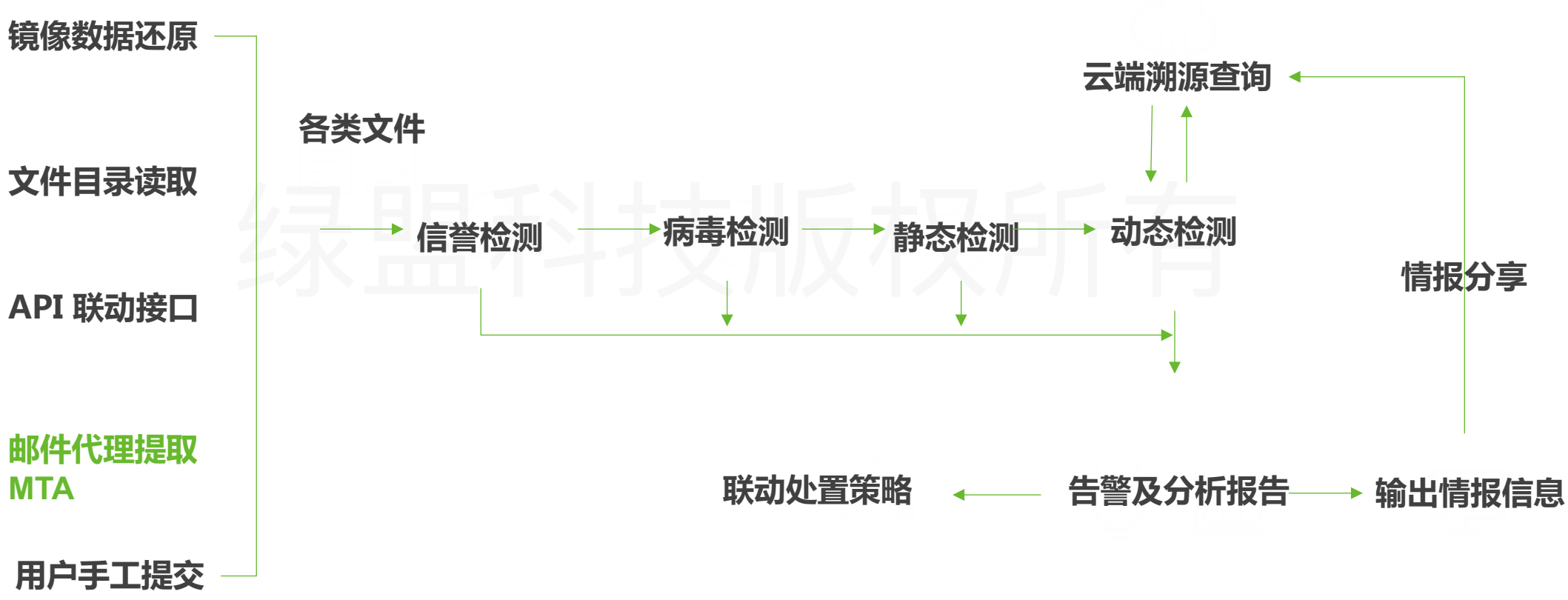
三种系列

- D系列：绿盟威胁分析系统D系列（NSFOCUS Threat Analysis Center D-series），网络高级威胁检测系统
- E系列：绿盟威胁分析系统E系列（NSFOCUS Threat Analysis Center E-series），邮件高级威胁防御系统
- V系列：绿盟威胁分析系统V系列（NSFOCUS Threat Analysis Center V-series），虚拟化部署

TAC检测

- 信誉检测：基于黑白IP/URL/域名/MD5等情报信息检测可疑链接与文件
- 病毒检测：基于专业的Bitdefender与火绒引擎检测已知病毒
- 静态检测：基于静态特征检测隐藏在文件中的可疑SHELLCODE与可执行脚本
- 动态检测：俗称沙箱，利用虚拟化技术，模拟用户操作环境运行可疑文件，通过文件行为检测威胁

TAC工作原理



TAC的检测对象

常见文件载体

例如office文档、pdf、exe、zip、rar等可在windows 平台执行的文件

企业自建邮件系统：

包括邮件正文中的域名、url地址、邮件附件

安卓移动应用：

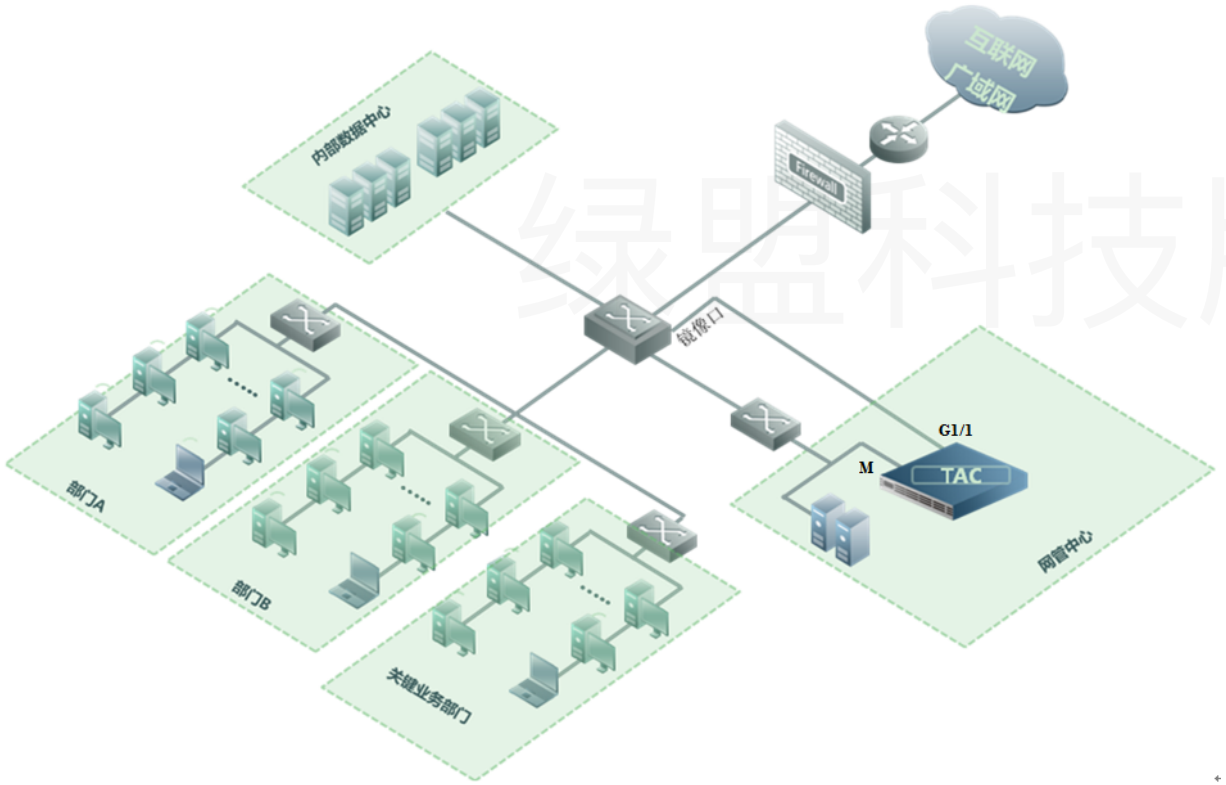
apk安装文件

02

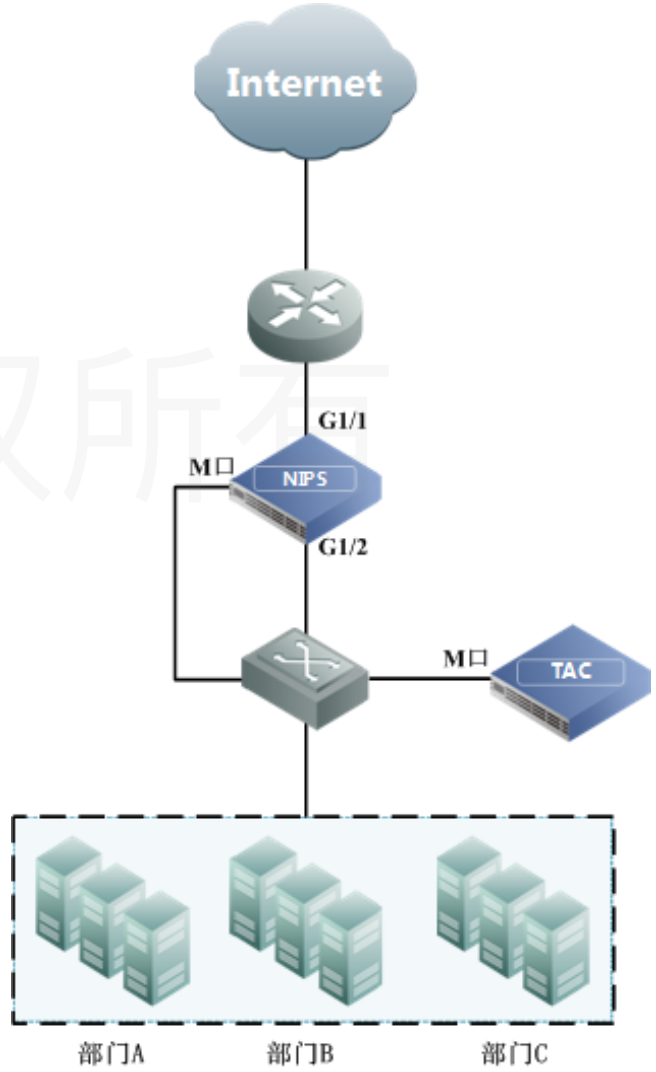
部署方式

TAC-D部署方式

监听部署：

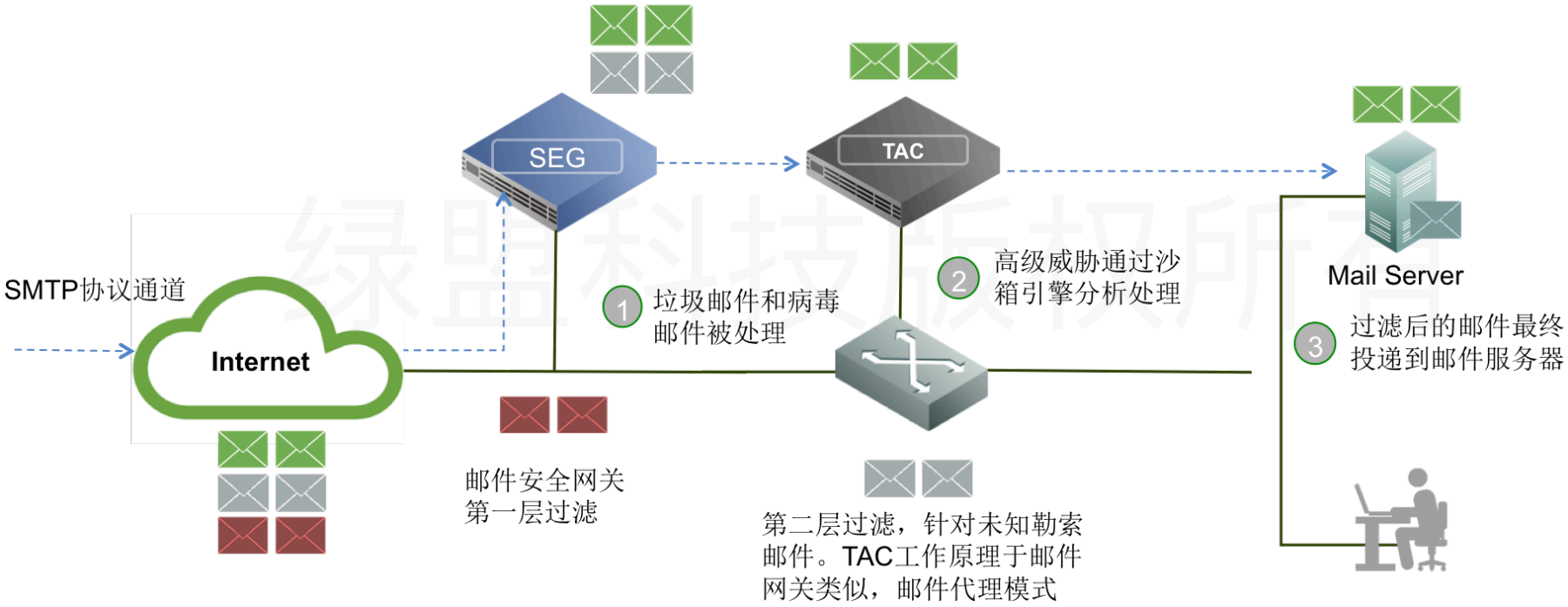


联动部署：



TAC-E部署方式

邮件网关部署：



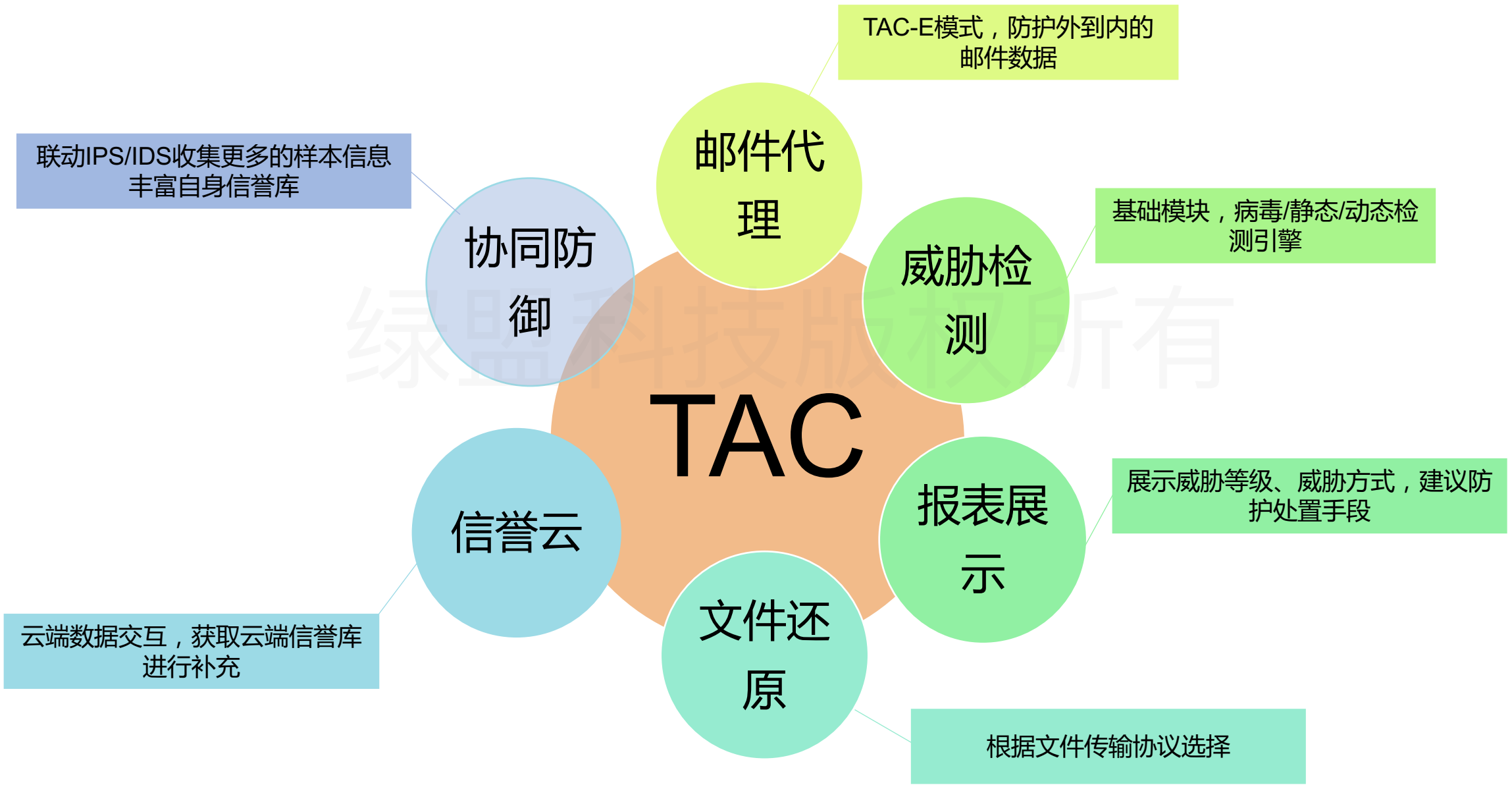
03

TAC的使用和配置

初始web账户

	Web操作员	Web审计员	Console口管理员
用户名	admin	auditor	conadmin
密码		无	

主要功能



TAC-D威胁检测

威胁检测

- 静态检测：静态检测引擎新增复合格式检测、JS样本检测、office宏检测，新增内置yara规则。复合格式检测即针对PE类修改后缀为图片格式的样本检测告警，告警摘要如下：

威胁检测

- 压缩包检测：

新增压缩包检测引擎，处理压缩包样本，进行解压和检测恶意压缩包样本，压缩包检测引擎在web界面没有展示。

- 动态检测：

动态引擎新增自定义规则、网络访问控制、沙箱逃逸检测，另外告警日志的展示相对201也有很大的改变，增加了威胁行为、危害和处理建议，整个页面的展示风格也跟以前有所不同。

威胁检测

- 自定义规则可以支持用户自定义动态规则，可以通过备份恢复中的恢复功能导入用户自定义的规则，规则导入后重启引擎生效。

- 网络访问控制分为三种，默认配置为限制部分访问，即限制虚拟机访问私有网络地址；限制网络访问即限制虚拟机网络访问，不能访问任何地址；开放网络访问即不做任何限制。

- 沙箱逃逸检测默认支持，web上不能配置，TAC检测到沙箱逃逸的样本后再文件分析报告中会有具体展示。下面是导出的一份动态检测样本的分析报告：

Adobe Acrobat Document

TAC-E

- 邮件代理配置步骤：
- 1、选择菜单 **策略** > **邮件代理** > **邮件代理**，进入邮件代理配置页面

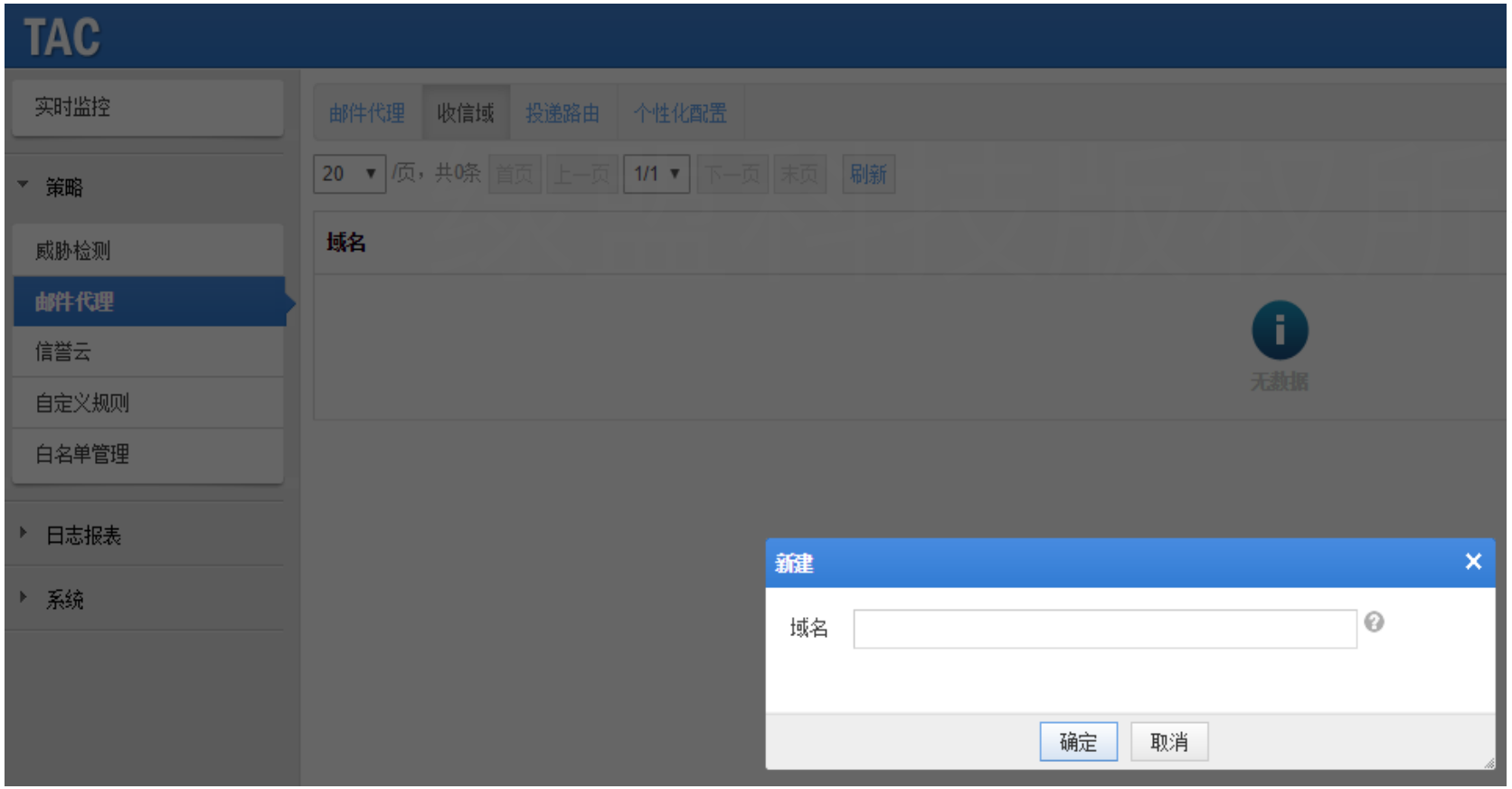
主域：内部邮件系统的主域名称
主机名：TAC对外发送smtp helo/echo 的名称

隔离：检测到异常邮件进行隔离。
监控：检测到异常邮件进行告警。

延迟发送：邮件最大延迟发送时间

TAC-E

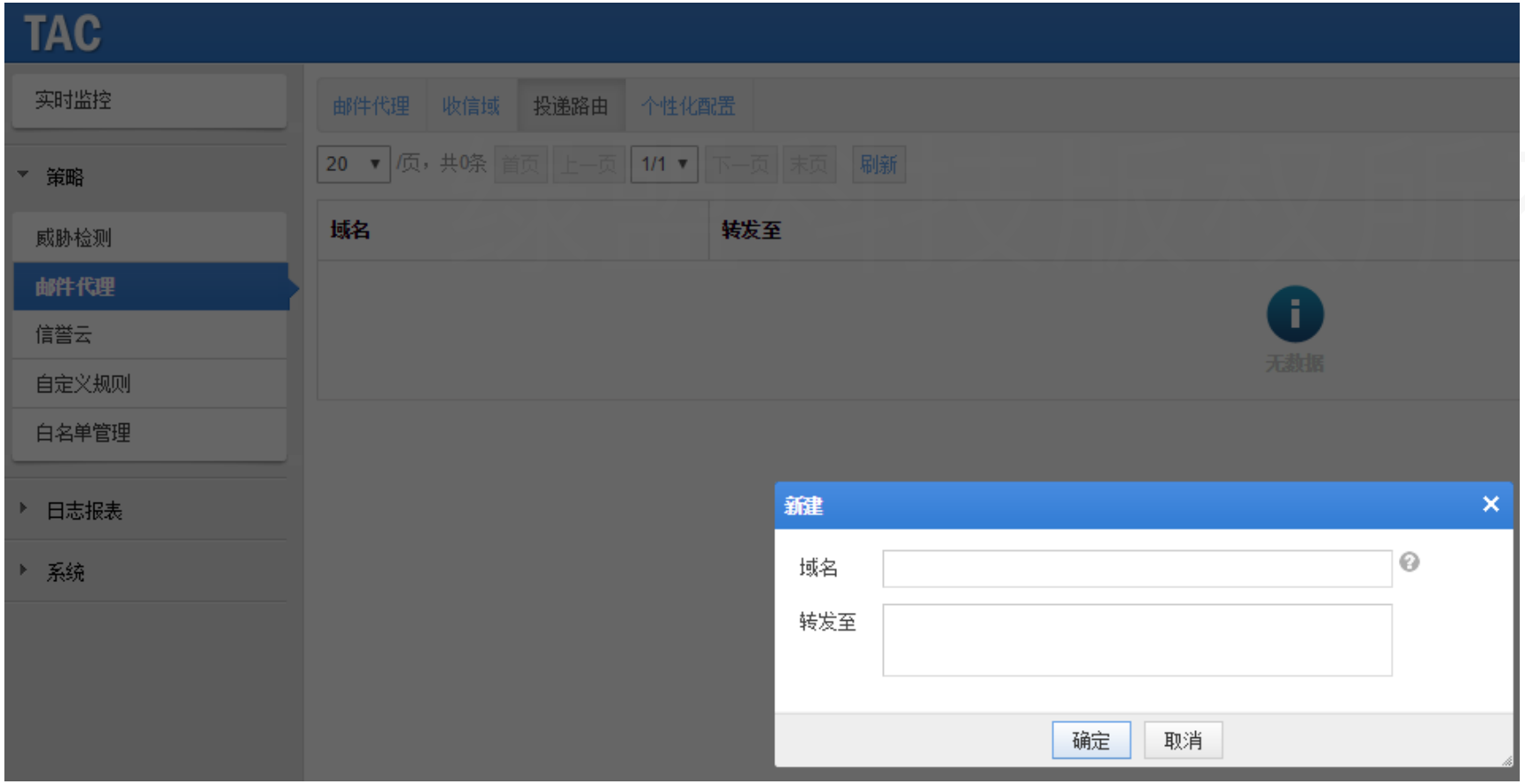
- 邮件代理配置步骤：
- 2、选择菜单 **策略** > **邮件代理** > **收信域**，进入收信域防护配置页面



收信域是指TAC作为邮件网关，TAC只对收信域列表中的邮件进行检测。

TAC-E

- 邮件代理配置步骤：
- 3、选择菜单 **策略** > **邮件代理** > **投递路由**，进入投递路由配置页面



投递路由为收信域指明了邮件的转发路径。当邮件到达TAC并经安全检测后，按照投递路由的设置，将检测后未发现异常的邮件转发至目的地。

信誉云

- 如果设备能够正常上网，且证书中包含信誉云模块，则设备每天早上七点从云端拉取信誉（文件信誉和url信誉），一天更新一次，初始状态这两个信誉文件都是空的。若证书中不包含信誉云模块，TAC虽然可以连上云，但是无法拉取信誉。

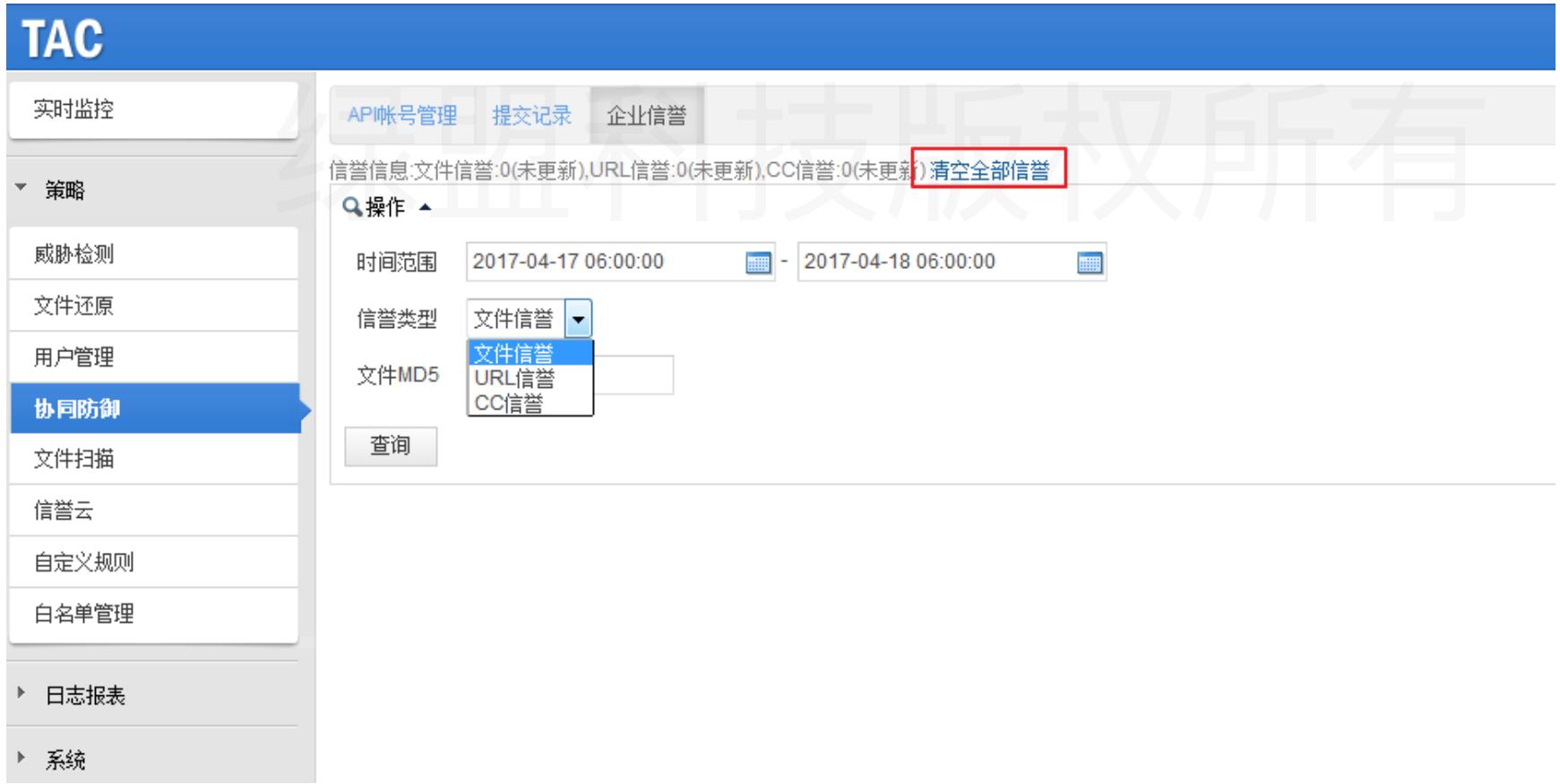
设备上的开关控制信誉检测的时候过不过云信誉文件，若选择启用信誉检测，则设备在信誉检测的时候会过从云端更新到的两个信誉文件；若选择否，则设备在信誉检测的时候不过从云端更新到的信誉文件。

协同防御

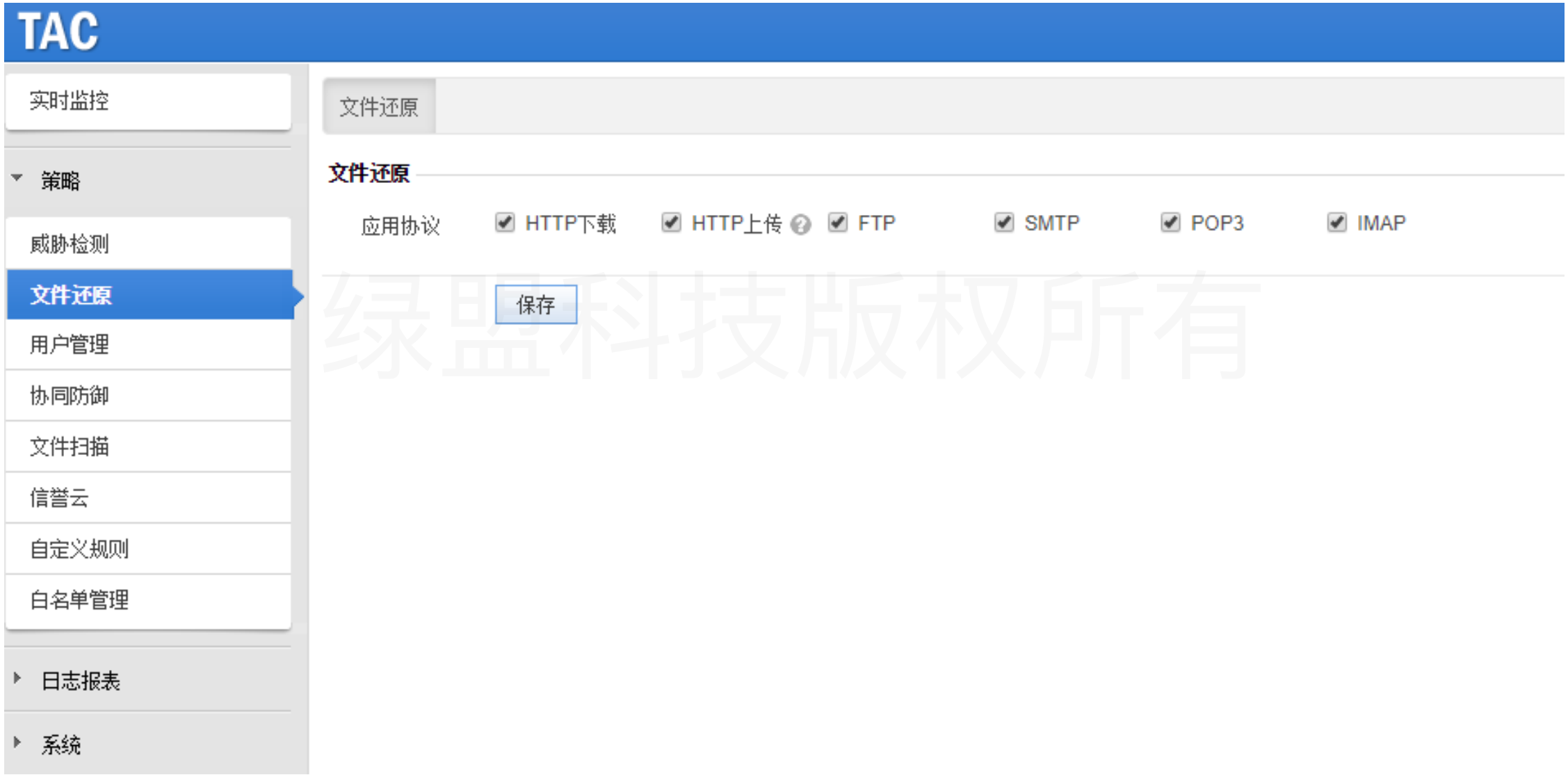
- 原有的API管理模块现在放在协同防御标签页下，新增了提交记录和企业信誉两个功能。
- 提交记录中记录了第三方如IPS、NF或其他使用API账号通过API接口提交文件进行检测的提交信息，包括提交IP、提交文件总数、和最近提交时间。

协同防御

- 企业信誉中记录了TAC自身产生的信誉信息，包括文件信誉、URL信誉和CC信誉，以及这些信誉的最后更新时间（TAC需开启专业参数中generate_credit参数才能产生信誉）。

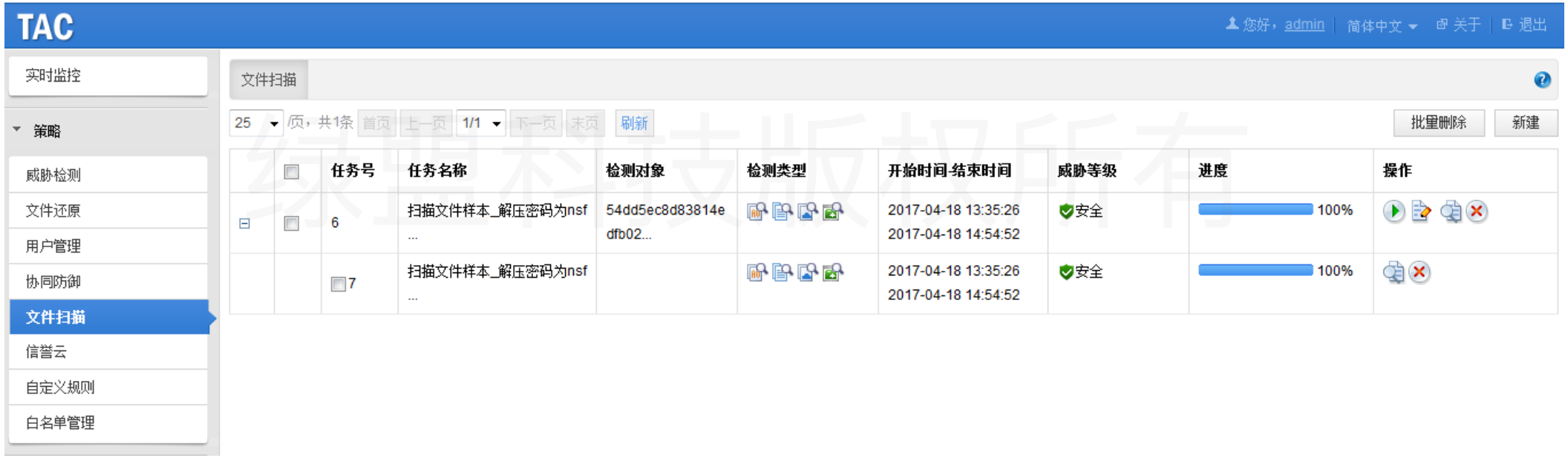


文件还原



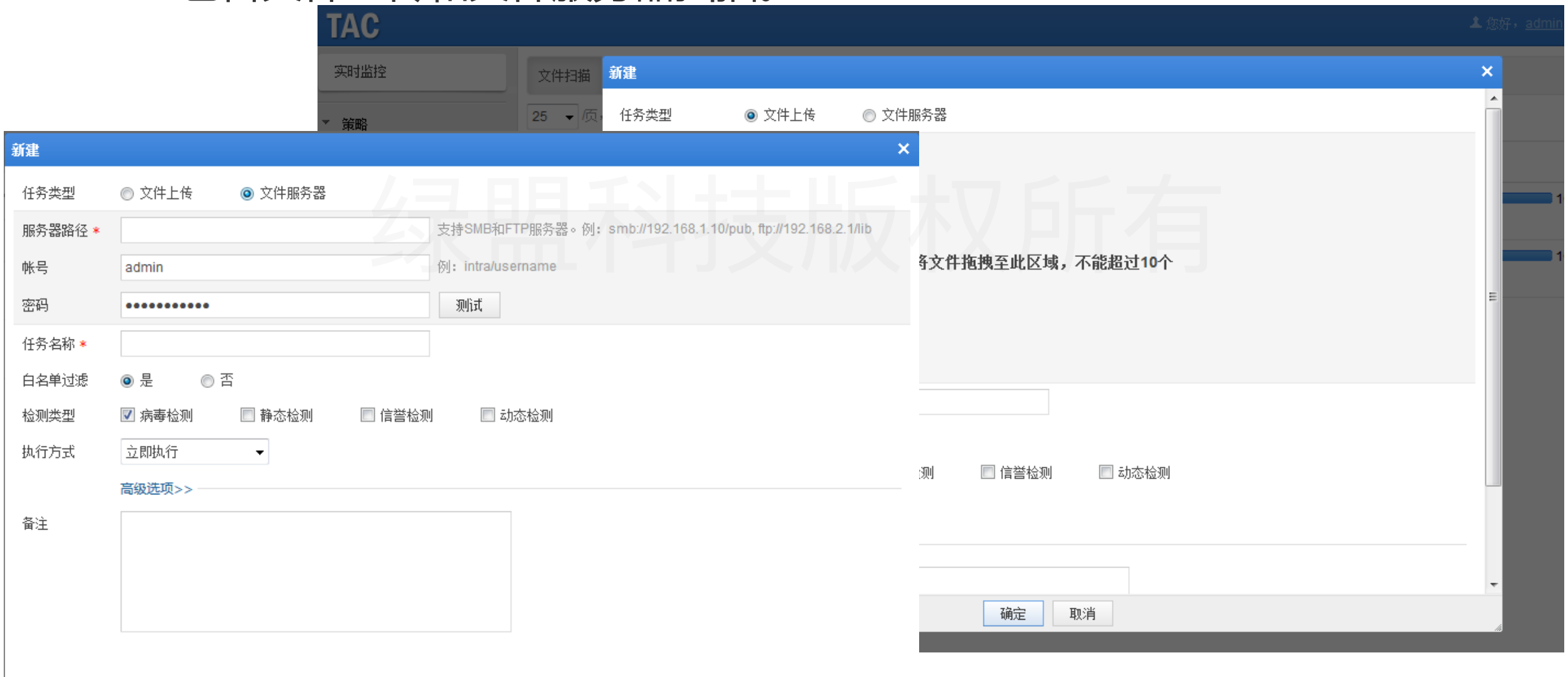
文件扫描

- 202版本中将之前的D、F、P系列三个系列合并，文件扫描的功能添加至策略目录下。文件扫描任务的具体功能与之前离线扫描系列一致。



文件扫描

包含文件上传和文件服务器扫描。



04

FAQ

注意事项

- 虚拟化TAC仅仅支持API上传文件检测，不支持镜像模式传输流量

- TAC各模块检测顺序：用户自定义白名单、用户自定义黑名单、文件白名单、信誉、防病毒、静态、动态

- Q：匹配了黑名单后，是否还会继续检测？
- A：匹配了白名单的不会再检测，匹配了黑名单和信誉的，会继续检测送到后面的检测引擎进行检测

注意事项

- 离线扫描时不能挂载根目录，只能挂载指定的文件夹；
- 推荐使用32G以上FAT32格式U盘对设备或虚拟机进行升级（不支持NTFS及其它格式），移动硬盘分区过多时可能出现加载失败的情况；
- av和静态检测引擎在检测之前都会过一次信誉检测，其中av的信誉检测只过白名单，静态的信誉检测黑白名单都过

注意事项

- 在界面上的文件分析报告处可以把样本加入白名单，在策略-白名单处也可以通过md5将样本加入白名单，这个白名单仅仅是将数据库file_credit表该样本的level值置为0，只是该样本不生成告警了，但是样本进入TAC后依然会进行检测。

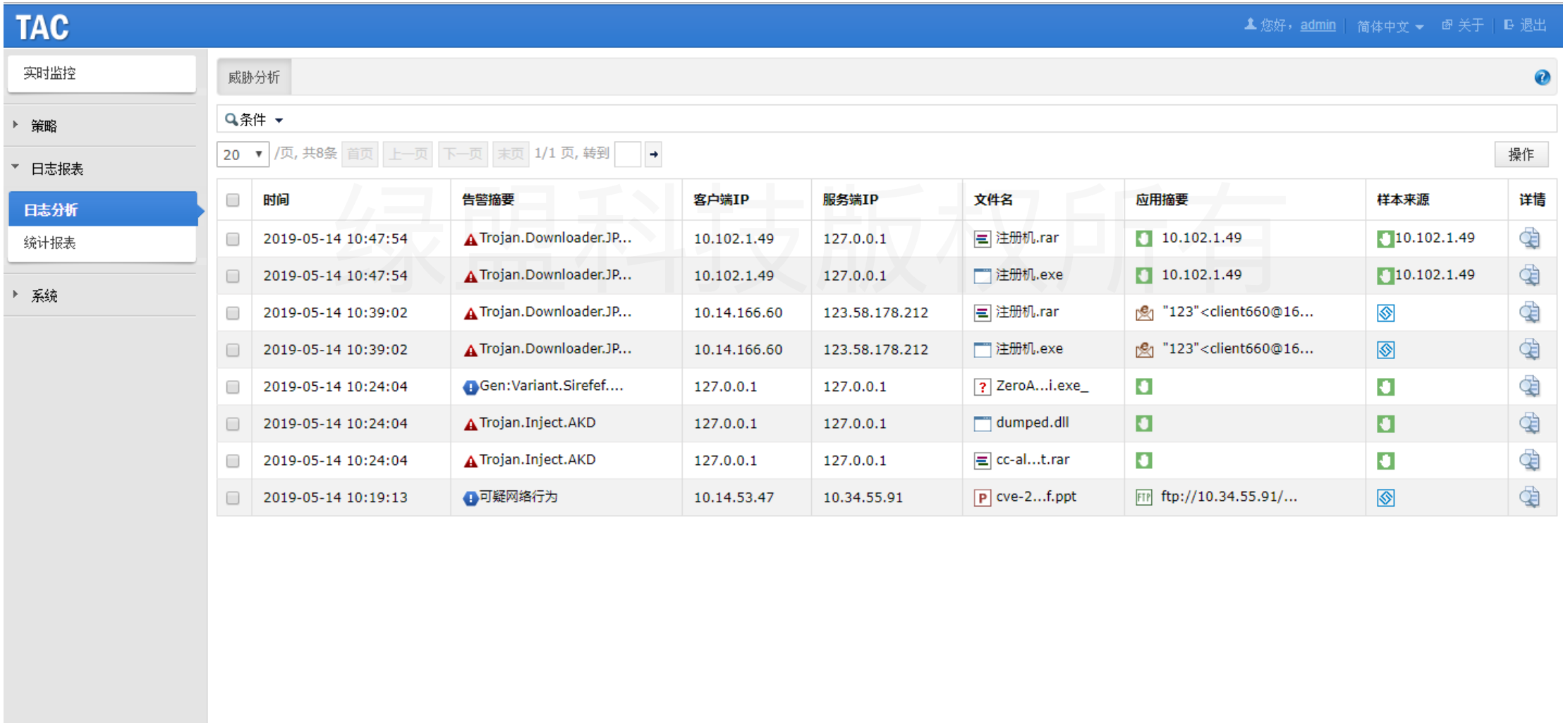
- 设备检测一个白样本3次，会自动把该样本加入白名单，此白名单放在/tmp/remote/db/file.db中，每次重启系统会清空。样本进入tac后会首先对比该白样本，如果匹配到该白名单则会直接放行，不再继续检测。

05

日志分析

日志分析

- 日志分析——威胁分析



日志分析

威胁分析——详情

NSFOCUS

文件分析报告

生成时间:2019-05-14 13:41:13

分析概述

文件名称	注册机.rar
文件类型	RAR
文件大小	13.3KB (13589 bytes)
会话信息	10.102.1.49:3440 → 127.0.0.1:0
文件来源	nsfocus[10.102.1.49],2019-05-14 10:47:54,手动上传
威胁行为	1)下载器
危害	1)用来从远程服务器下载恶意程序，安装并执行。
处理建议	1)使用杀软进行全盘查杀

威胁等级

高

包含文件

子文件

日志分析

威胁分析——详情

NSFOCUS

文件分析报告

生成时间:2019-05-14 13:41:13

分析概述

文件名称	注册机.rar
文件类型	RAR
文件大小	13.3KB (13589 bytes)
会话信息	10.102.1.49:3440 → 127.0.0.1:0
文件来源	nsfocus[10.102.1.49],2019-05-14 10:47:54,手动上传
威胁行为	1)下载器
危害	1)用来从远程服务器下载恶意程序，安装并执行。
处理建议	1)使用杀软进行全盘查杀

威胁等级

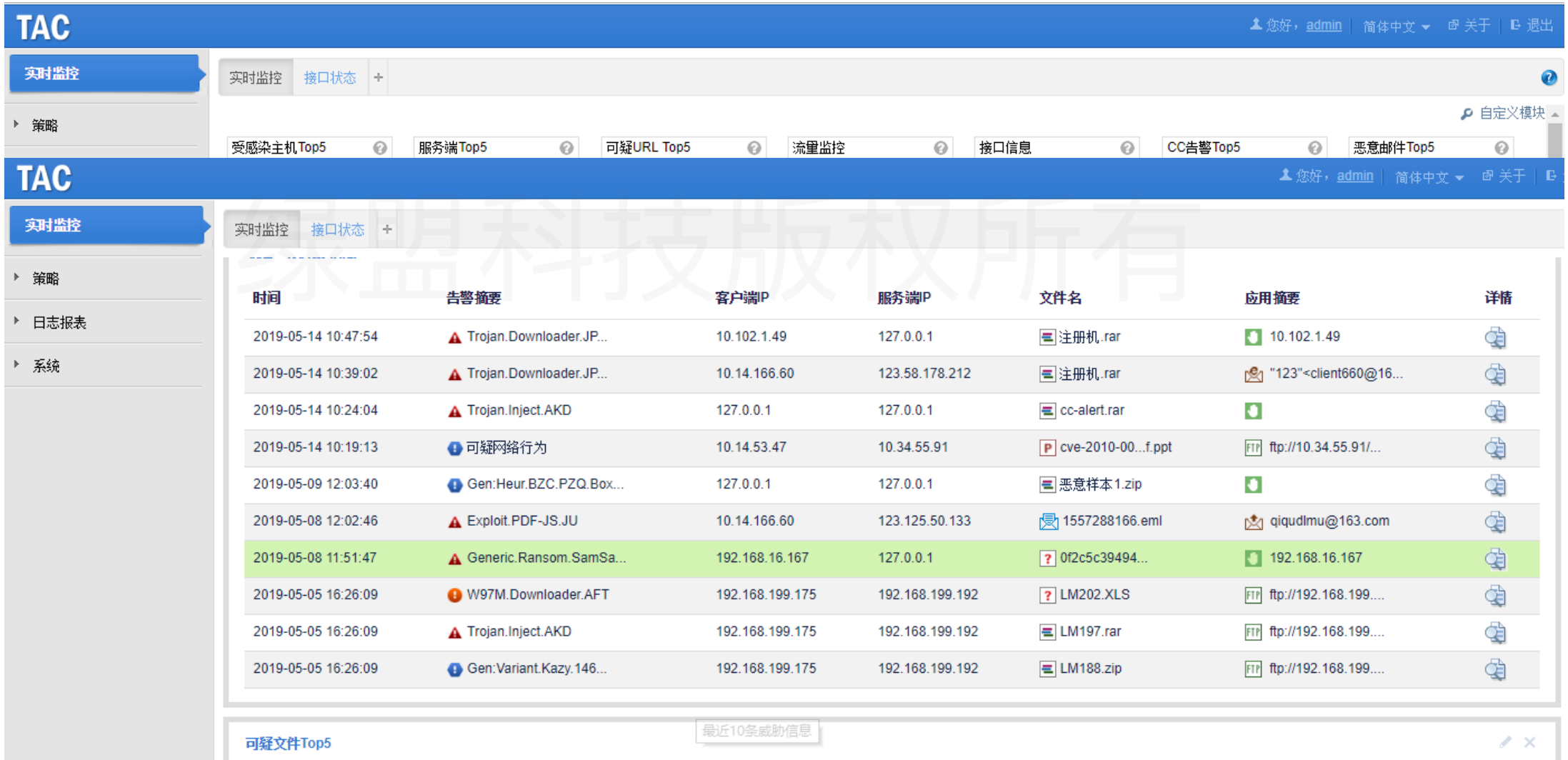
高

包含文件

子文件

首页展示

- 自定义模块展示



谢谢！

NSFOCUS