安全玻璃盒

让安全更简单更智能

自适应防护系统

产品手册

杭州孝道科技有限公司

目录

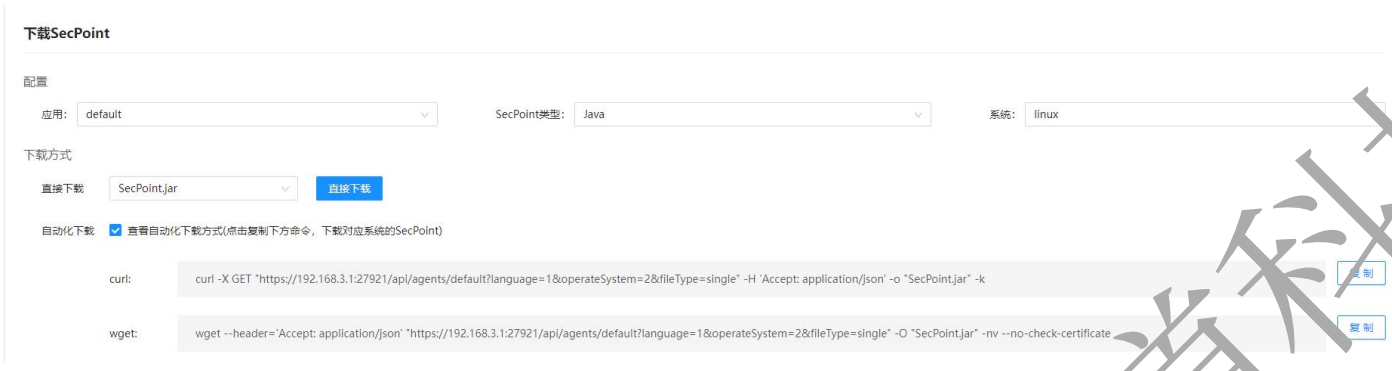
1 系统登录

输入登录页面地址，打开登录页面，输入管理员分配的用户名及密码，即可登录成功，进入系统主页。如果忘记密码，可通过忘记密码功能设置新密码（忘记密码功能需要管理员在系统管理-系统配置-邮件设置中配置邮件服务器且需要用户账号绑定有效的邮箱）

2 添加 secpoint

点击右上角的添加 secpoint 按钮,进入 agent 安装引导界面，可根据提示进行 agent 的下载与安装。

1） RASP 平台提供了 Java SecPoint 类型，您可以根据自己的应用选择相应类型的 SecPoint 及操作系统环境进行下载。



2）创建应用的时候需要输入应用的唯一标识 key，SecPoint 通过 key 与应用进行绑定。SecPoint 启动时需要在启动脚本中添加字段 -DappKey = 应用 key(在下载 SecPoint 页面选择需要绑定的应用，此处的应用 key 会相应变化)。

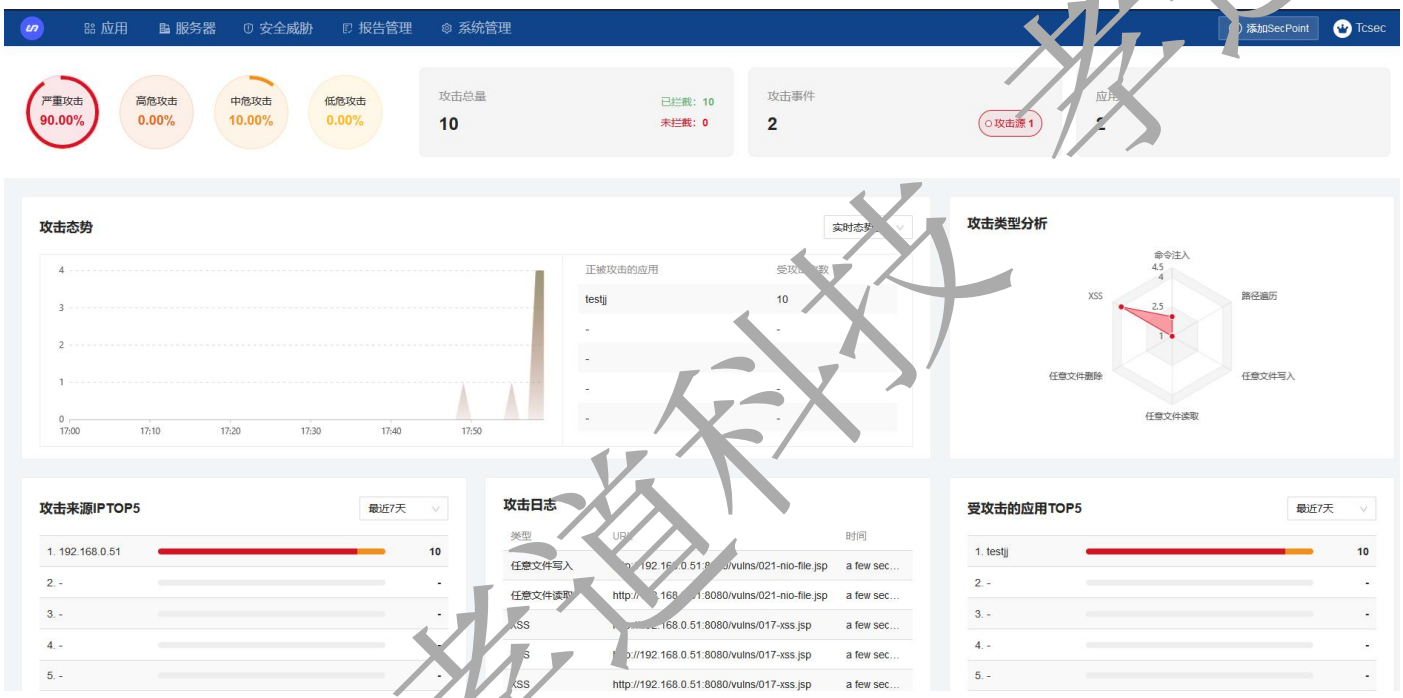
3 主页

RASP 主页是对所有应用防护数据的统计，在主页我们可以查看到应用受到的攻击危害等级占比、已拦截及未拦截的攻击总量，通过攻击态势图我们可以实时地查看到正在受攻击的应用及该应用受攻击的次数。此外，您也可以通过蛛网图查看攻击类型分析，通过攻击来源 IP-TOP5 发现对应用攻击次数较多的 IP 等。

4 应用

4.1 总览

RASP 总览是对当前应用防护数据的统计，您可以查看到应用受到的攻击危害等级占比、已拦截及未拦截的攻击总量，通过攻击态势图我们可以查看近 7 天该应用受攻击的次数，同时该页面还记录了最近新增的攻击事件且根据攻击来源和受攻击 URL 的频繁程度分别进行统计。



4.2 攻击日志

系统中的任意应用受到攻击时，都会记录攻击日志，一次攻击请求就记一条攻击日志。通过攻击流量图，您可以实时的查看当前应用的受攻击情况，同时您也可以根据不同的条件筛选查看攻击日志。

4.3 策略管理

4.3.1 防护

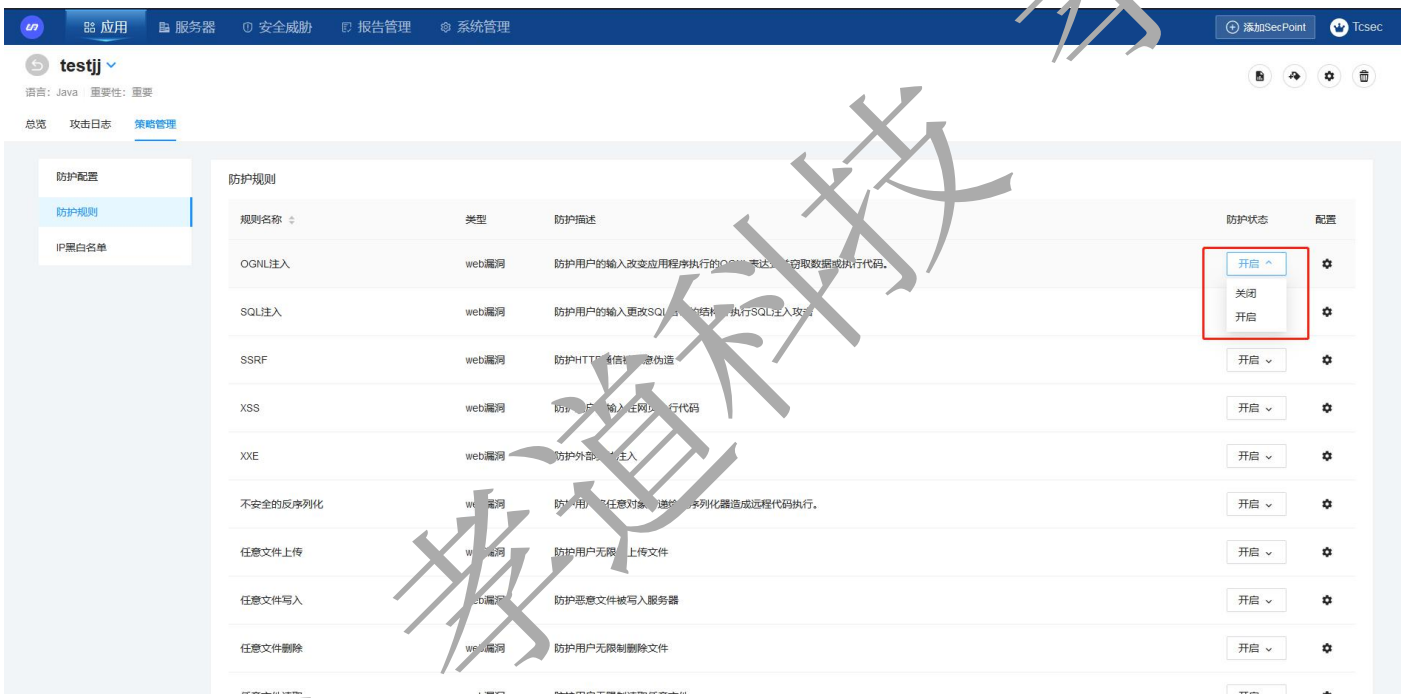
1 防护规则

1） Web 漏洞

Web 漏洞防护规则有开启、关闭两种种状态。

A．开启：防护功能开启后，对该规则的攻击进行监控及防护

B．关闭：不对该规则的攻击进行监控及防护



2） 您也可以点击配置按钮来对 RASP 规则算法进行编辑，一共有三种状态：记录日志、拦截攻击、完全忽略。

2 IP 黑白名单

1）黑名单：加入黑名单的主机/范围/网段，禁止访问应用。

2）白名单：加入白名单的主机/范围/网段，为信任主机，不做任何防护。

3）在攻击日志中，点击操作可以快捷的将 IP 添加进黑白名单

5 服务器

服务器列表展示了部署了 SecPoint 的应用所对应的信息，一个 SecPoint 对应一个服务器。

列表中展示了服务器基本信息，包括 SecPoint 版本、开发语言、所属应用、防护状态等。您可以通过所属应用、升级状态、在线状态、所属小组、搜索框来筛选对应的服务器。

5.1 SecPoint 升级

ASTP 升级完成之后，SecPoint 版本可能会有变更。当前服务器绑定的 SecPoint 不是最新版本时，会提示 SecPoint 可升级，点击升级图标，可选择在线热升级进行 SecPoint 升级。在线热升级无需重启服务器。

勾选服务器可以进行批量升级

5.2 服务器设置

5.2.1 添加标签

您可以为服务器添加标签来标记该服务器。

5.2.2 设置服务器

在操作中点击设置，进入设置服务器页面，您可以修改服务器名，根据自己的需求进行 Secpoint 日志配置，包括日志空间配置、日志等级及存储位置配置。

6 安全威胁

6.1 攻击事件

一个攻击事件是多个攻击日志的集合。同一攻击来源的攻击请求如果与前一次的攻击请求之间的间隔不超过半小时，则记入同一个攻击事件，此攻击事件为活跃状态；超过半小时，则此攻击事件结

束（不再活跃），之后的攻击请求记入另一个新的攻击事件，新的攻击事件为活跃状态。

1、攻击日志的删除不影响攻击事件，例如某个攻击事件的最后一次攻击日志时间为 10:00，然后将 10:00 的攻击日志删除了，则 10：30 之前的攻击请求仍是计入此次攻击事件。

2、攻击日志的删除不影响攻击事件的攻击次数统计，也不会影响对应攻击事件的其他数据显示（只是该条攻击日志的信息没有了）。

如下图所示，点击右下角图标可展开设置列表，您可以根据具体情况将 IP 加入黑白名单，切记当选择所有应用时，之后新增的应用也会受此处添加的黑白名单的影响。

1）IP 加入黑名单->受攻击应用：系统禁止此攻击 IP 访问该条攻击日志中的被攻击应用

2）IP 加入黑名单→所有应用：系统禁止此攻击 IP 访问所有应用

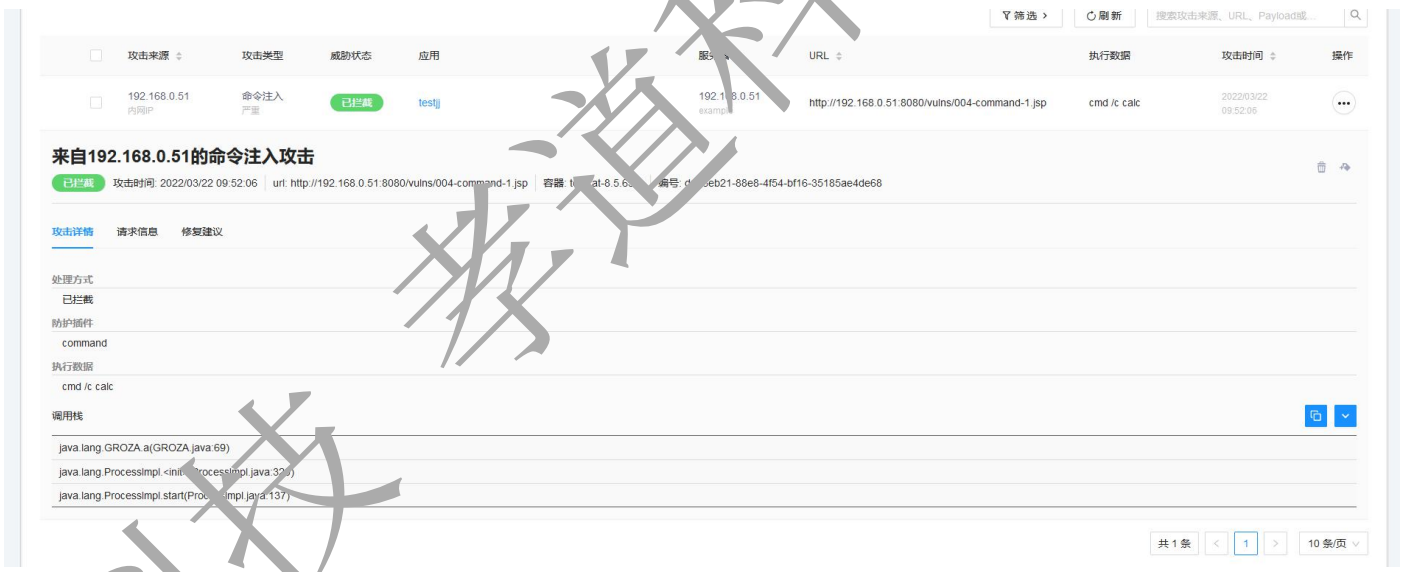
3）IP 加入白名单→受攻击应用：系统不再监控或防护此 IP 对该条攻击日志中被攻击应用的访问。

4）IP 加入白名单→所有应用：系统不再监控或防护此 IP 对所有应用的访问。

5）点击导出攻击事件报告，则下载此次攻击事件包含的所有攻击日志的信息列表

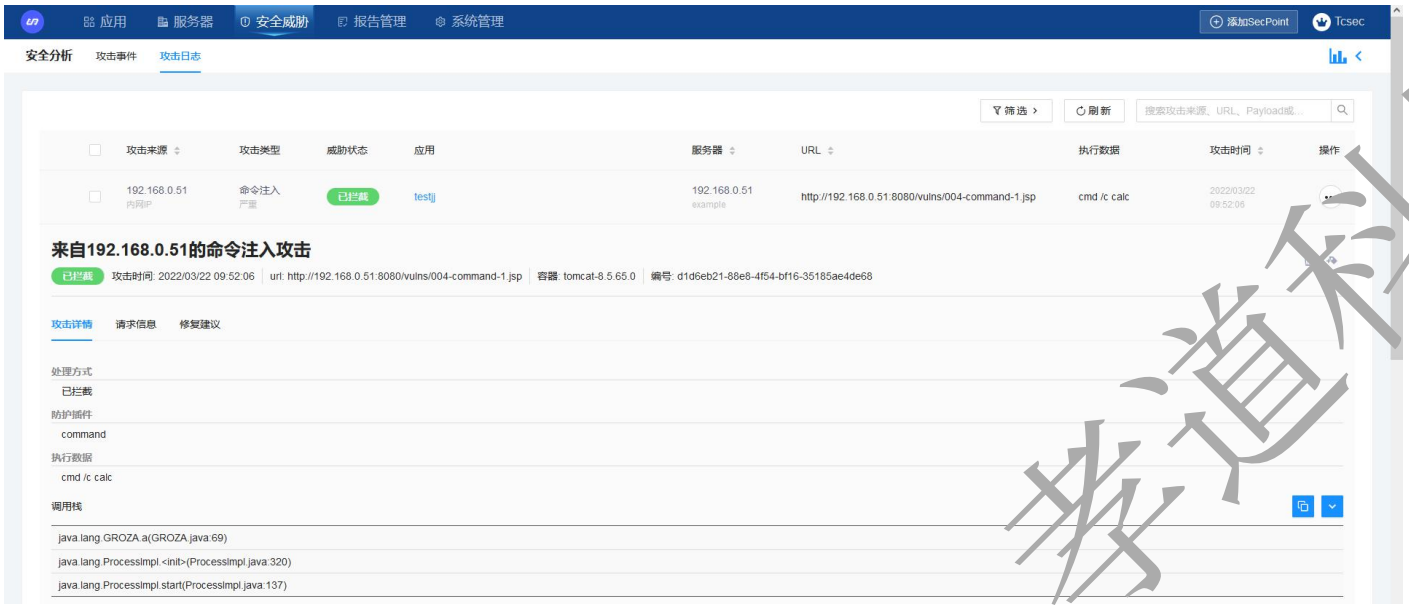
点击攻击来源下的 IP，可进入该攻击事件的详情页面，详情页面展示出了该攻击事件中受攻击的应用、服务器以及该攻击持续的时间和攻击日志列表，通过攻击流量图，您可以实时的查看当前应用的受攻击情况。

选择点击一条攻击日志后，可展开查看该条攻击日志的详情。攻击日志详情中您可以查看该次攻击的攻击详情、请求信息以及针对该次攻击请求的修复建议。



6.2 攻击日志

系统中的任意应用受到攻击时，都会记录攻击日志，一次攻击请求就记一条攻击日志。您可以实时的查看当前应用的受攻击情况，选择点击一条攻击日志后，可展开查看该条攻击日志的详情，同时您也可以根据不同的条件筛选查看攻击日志。



7 报告管理

报告管理主要提供了用户使用系统模板或者自定义模板生成报告的功能，您可以在报告模板页面中创建自定义的模板，在报告列表中您可以通过系统默认模板或者自定义添加模板进行报告生成、下载以及管理。

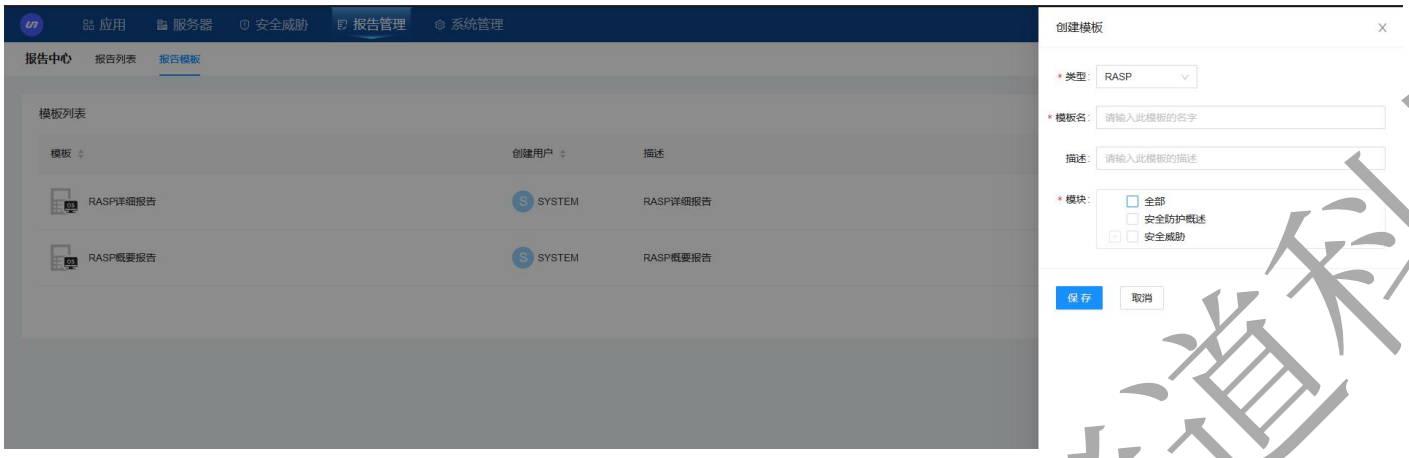
7.1 报告列表

报告列表会展示系统生成的报告记录，将会记录生成的报告名、引用模板、生成用户、生成时间、生成报告的应用、时间等。在列表中也可以进行报告的下载及删除操作。

您也可以在该页面进行报告生成，选择报告类型、模板、应用及报告名后，即可生成相应的报告。

7.2 报告模板

报告模板中提供了两种系统默认模板，包括 RASP 概要报告模板、RASP 详细报告模板。您也可以创建模板，选择您需要的模块进行模板自定义。



8 系统管理

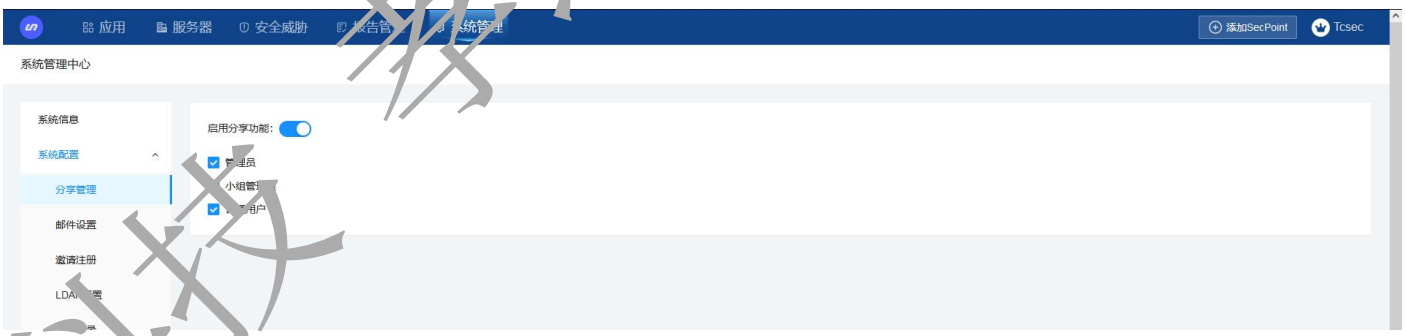
8.1 系统信息

系统状态主要是展示了系统的持续运行时间及版本等信息

8.2 系统配置

1 分享管理

针对检测漏洞分享开关的控制，可以打开或关闭分享功能，或者打开或关闭用户的分享权限。

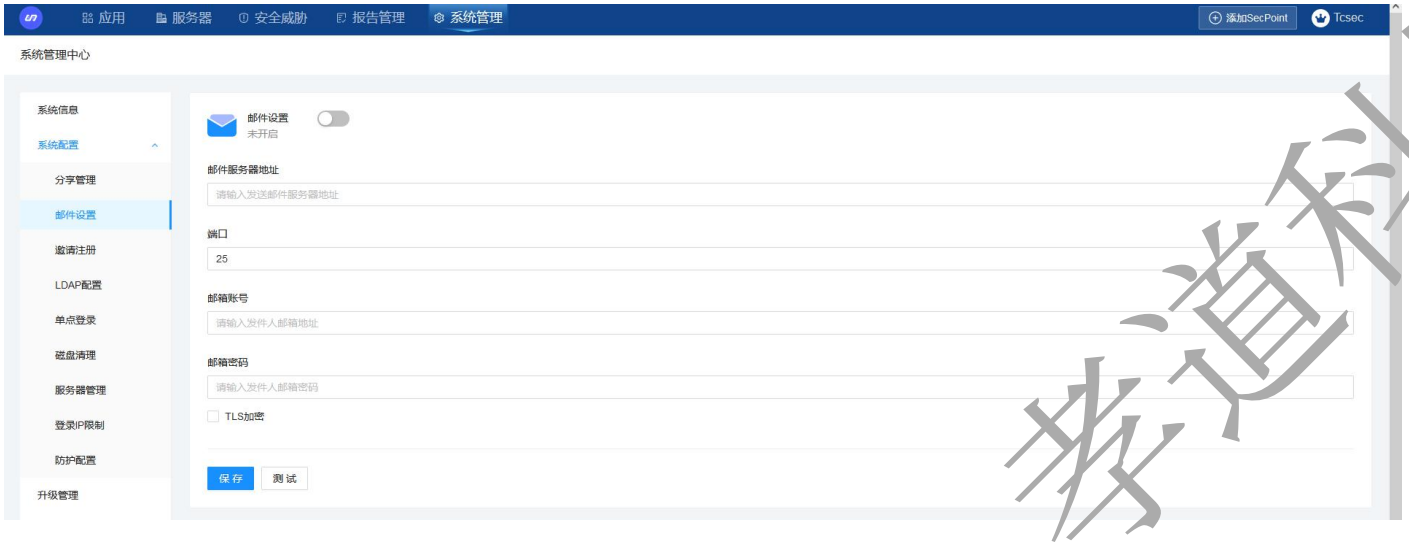


2 邮件设置

邮件设置功能用于配置发送邮件的服务器，配置成功后，忘记密码功能及事件管理中的邮件告警功能才能正常使用。建议 SMTP 服务器及邮箱地址选择企业邮箱，因为个人邮箱的收发会受到一定的限制，相似邮件收发过多可能被判定为垃圾邮件。具体邮件服务器配置方式可根据自己公司使用的企业邮箱自行查询。

邮件配置完成之后，可点击测试发送测试邮件。如果测试邮件发送不成功，请检查配置，如果测

试邮件发送成功、邮箱也接收到，说明邮件配置成功。

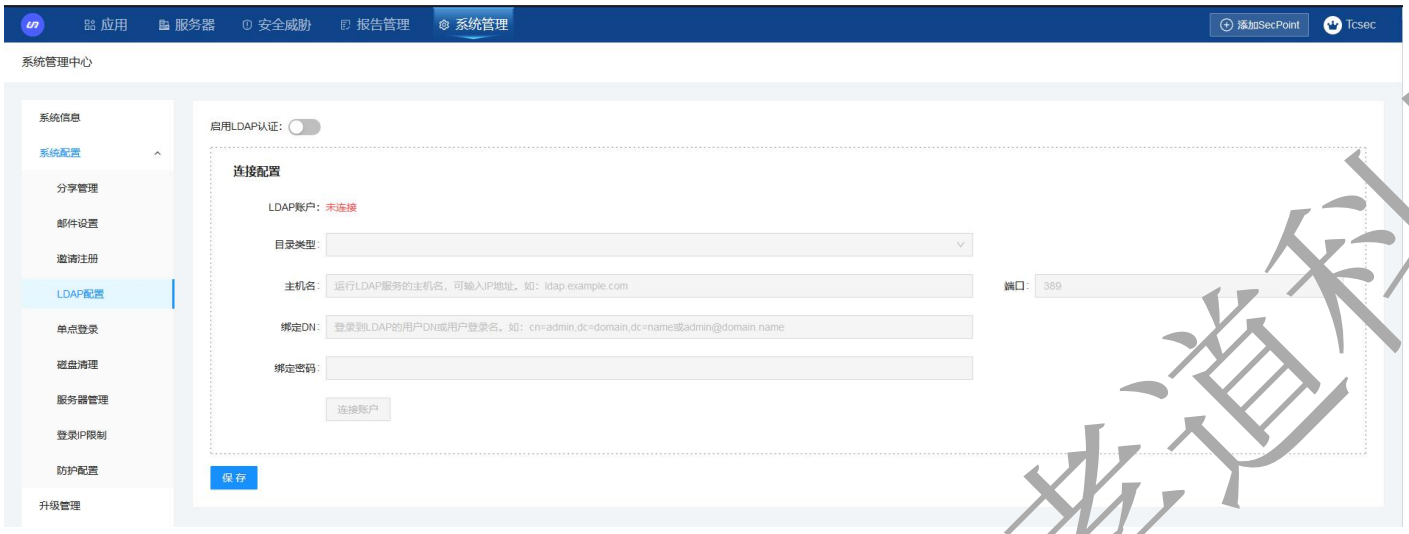


3 邀请注册

邀请注册用于邀请新用户注册 RASP 平台，勾选管理员即只有管理员可以发出邀请注册的链接，勾选管理员、小组管理员即管理员、小组管理员都可以邀请用户注册。

4 LDAP 配置

LDAP 配置完成并启用后，即可同步 LDAP 服务器上的用户信息到 RASP 平台，用户即可以使用 LDAP 账户进行登录。



5 单点登录

通过连接配置，与外部认真平台服务器连接之后，外部服务器的用户在登录后可以连接到 rasp 平台。

6 磁盘清理配置

通过磁盘清理配置，您可以配置定期清理检测日志、攻击日志、系统日志、RASP 平台后台日志、备份数据及操作日志。

立即清理：数据量超过容量阈值时最早产生的超出容量阈值 80%部分的数据会被清理。

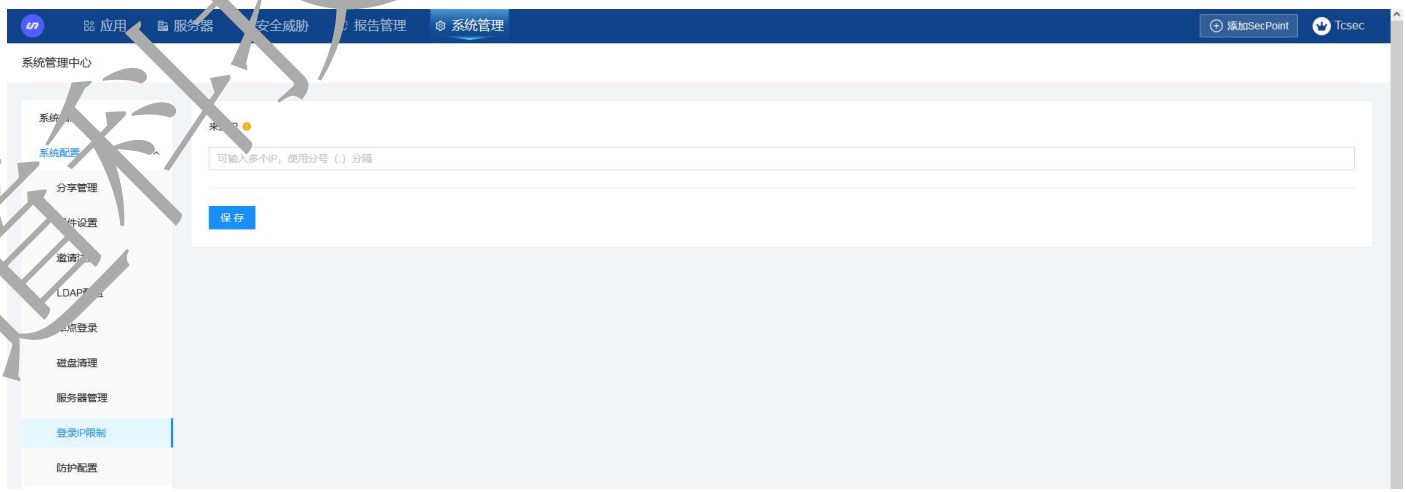
立即清空：清空该项所有数据。

6 服务器管理

打开按钮后，可以保留离线服务器的记录，关闭时将自动清理离线服务器连接纪录

7 登录 IP 限制

通过输入单个或者多个 IP（分号分割）来限制访问平台的来源 IP



8 防护配置

当服务受到攻击时，rasp 会拦截请求，进行防护阻断，返回应答码和拦截信息，在防护配置中可以设置返回的应答码和拦截信息，默认格式如图 1。

防护配置除了返回应答码，还可以选择跳转到制定界面进行防护，在图 2 中输入一个完整的 URL 地址后，当有攻击被防护阻断后，将会跳转到指定界面。

当点击恢复默认按钮后，会恢复到系统默认的配置。

图 1

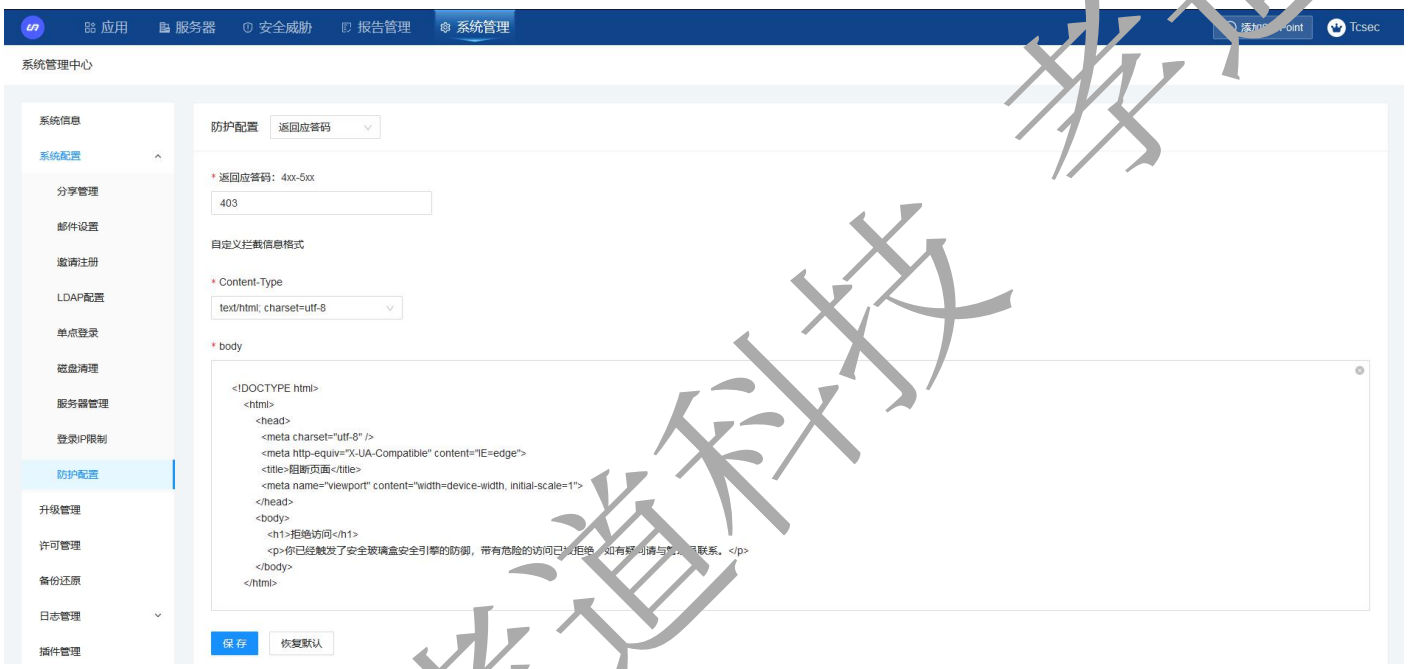
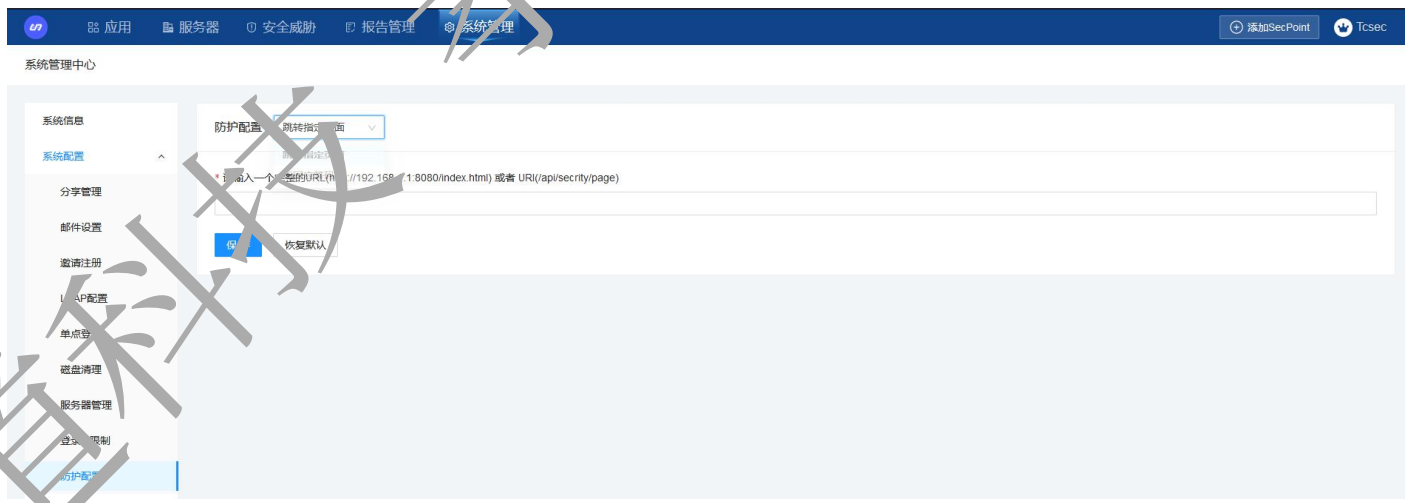


图 2



8.3 升级管理

系统升级

系统升级包主要包含 RASP 平台升级文件、SecPoint 升级文件、三方组件库文件及系统相关补丁，获取升级包后，点击上传升级包，按照提示即可完成升级。

8.4 许可管理

当许可时间到期后或者许可数量不够使用时，可下载许可申请文件，然后联系安全玻璃盒工作人员，获取新的许可文件，导入系统，重新登录即可使用。

8.5 备份恢复

备份恢复功能主要用于对系统数据库信息进行备份，当出现误删或者误操作影响系统的正常使用时，可通过还原操作，将系统还原至之前正常的一个节点。如果系统文件损坏，您也可以重新安装系统，然后将备份数据重新导入平台，之前备份的数据在新的系统中仍能正常使用。

您可以手动备份，也可以选择自动备份，设置备份的周期。

8.6 日志管理

8.6.1 系统日志

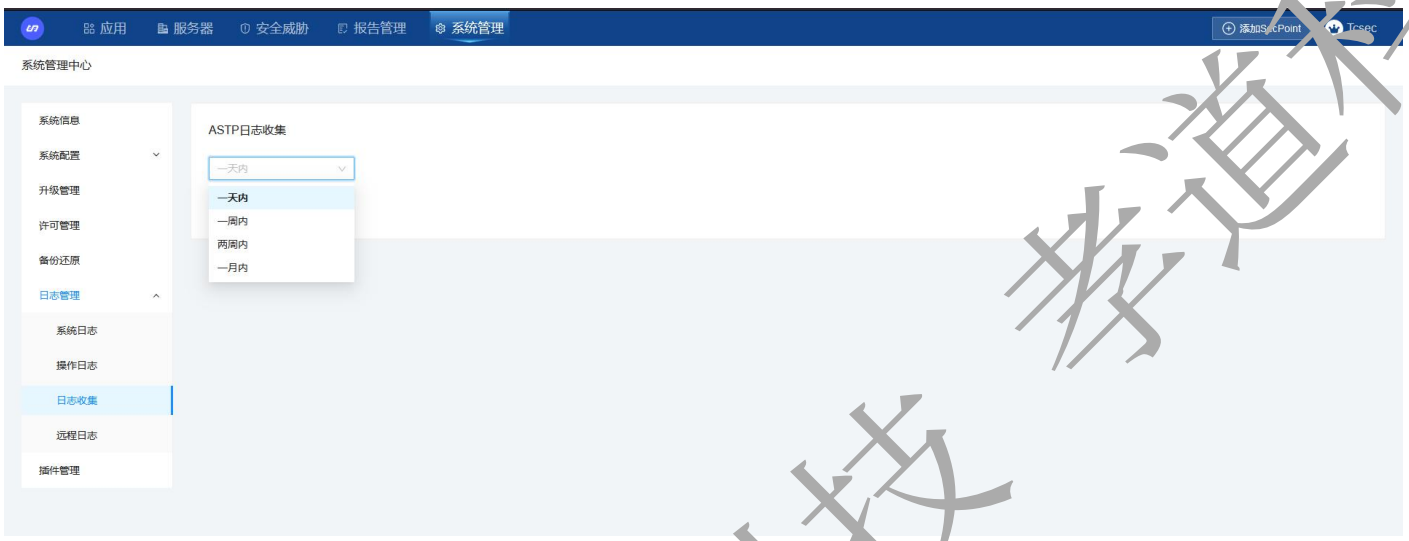
此处可以查看系统的告警日志，当服务器出现状况时，可以及时的得到通知。同时 Agent 升级日志、系统的升级日志都会在此展示。

8.6.2 操作日志

操作日志记录了登录、退出、新增、修改、删除、下载等操作的日志以及相应的搜索，当系统出现异常问题时，可以在此处追踪原因。

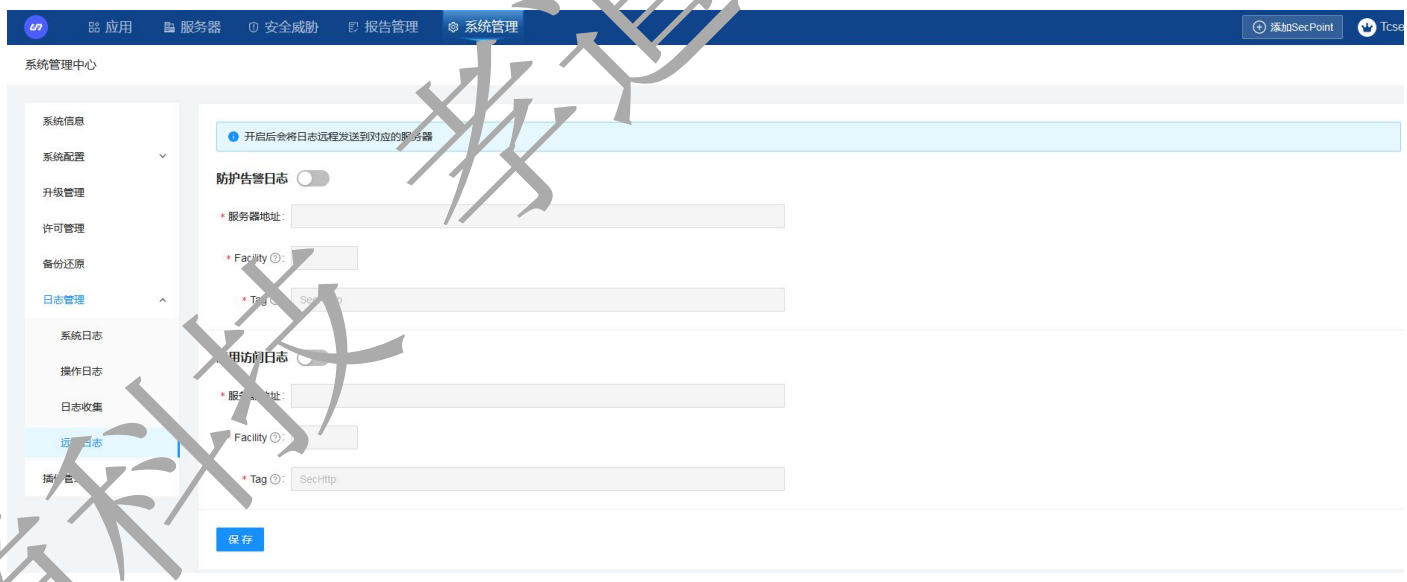
8.6.3 日志收集

您可以通过 astp 日志收集下载 astp 日志，可根据需要选择下载一天内、一周内、两周内、一月内的日志。



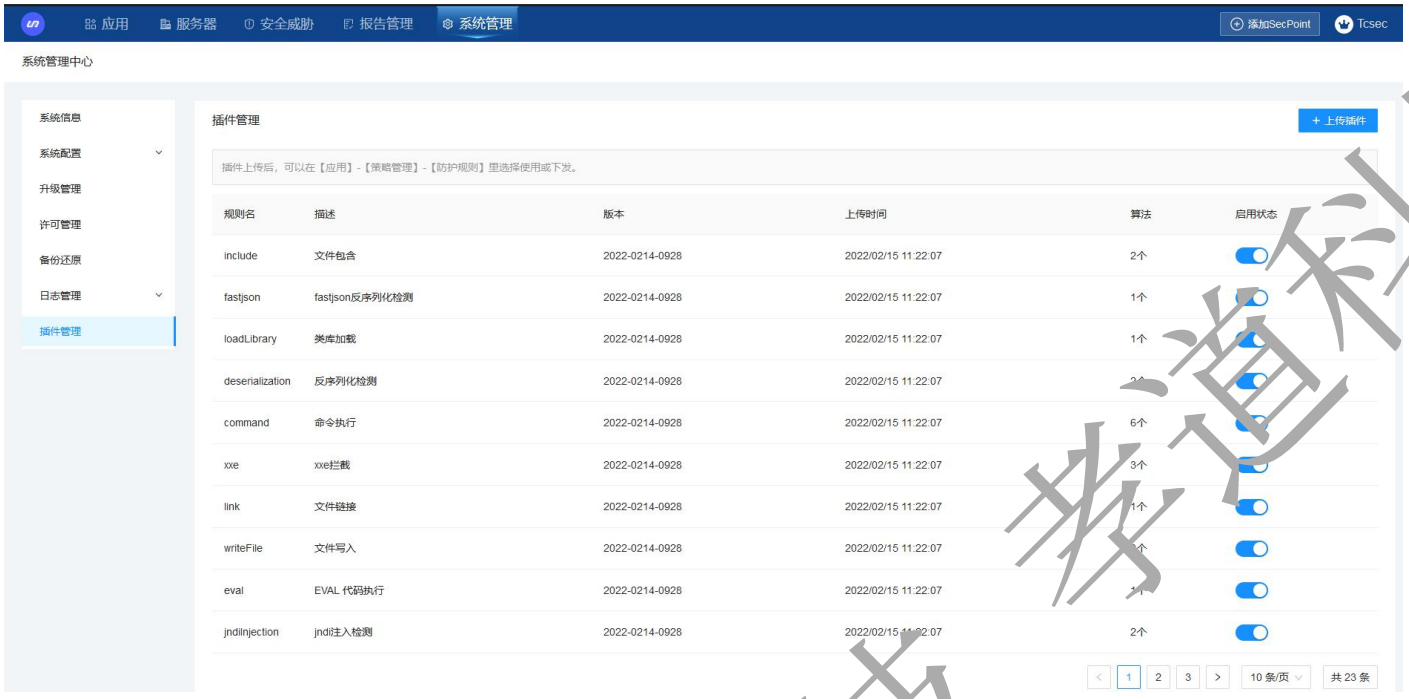
8.6.4 远程日志

填写地址并开启防护告警日志和应用访问日志后，平台会将对应日志远程发送到对应的服务器 。



8.7 插件管理

此处可以对插件进行启用状态的管理，并且可以上传插件，插件上传后，可以在【应用】-【策略管理】-【防护规则】里选择使用或下发。



9 用户中心

点击右上角用户名，进入用户中心，即可进行个人设置、组织设置、策略管理等操作。

9.1 个人设置

您可以在个人设置中修改当前账户的个人信息及密码，如果需要当前账户一直保持在线，您可以在个人信息中将会话超时时间设置为 0，如果不需要一直保持在线，您可以根据自己的需要设置会话超时时间。

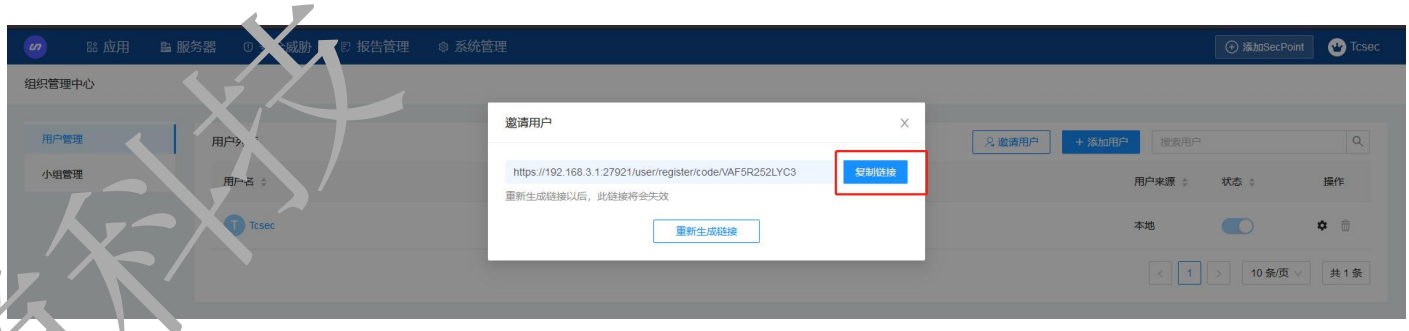
9.2 组织设置

9.2.1 用户管理

RASP 平台可通过邀请注册、平台添加及 LDAP 同步三种方式添加用户

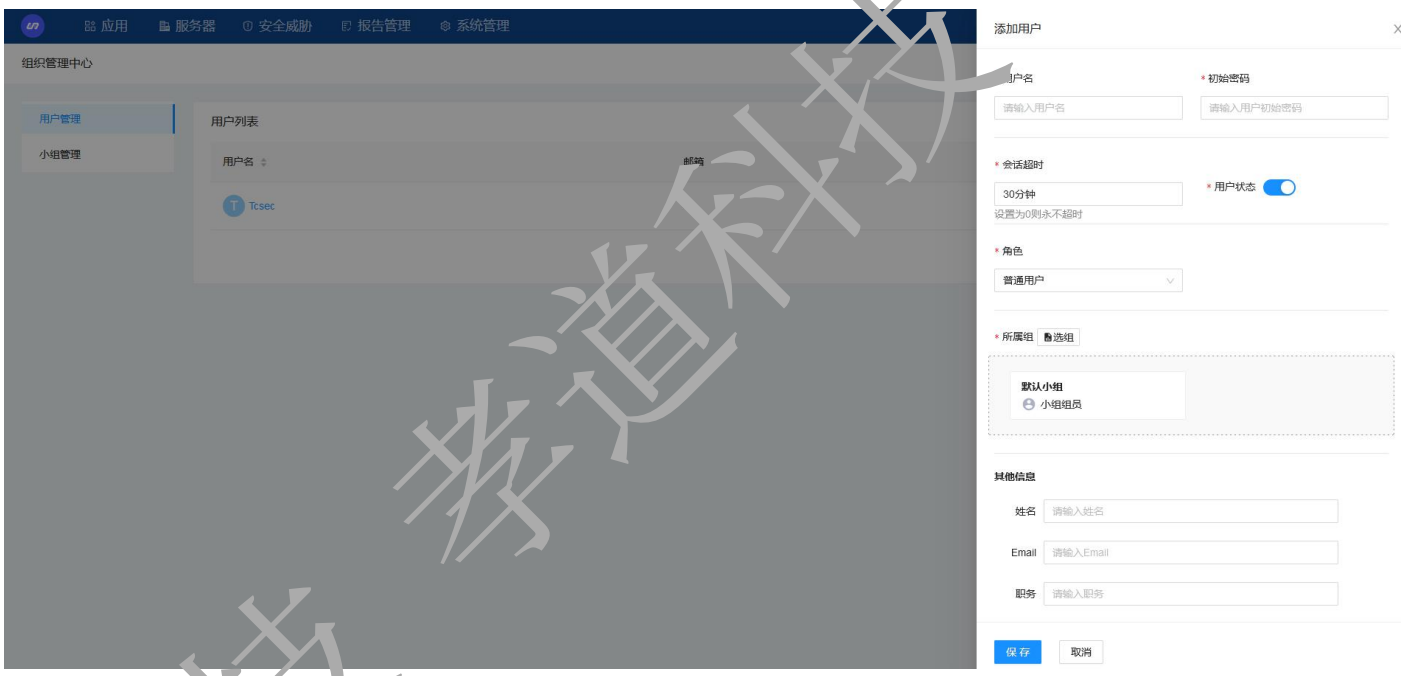
1）使用邀请注册功能需要在系统管理-系统配置-邀请注册页面启用此功能，开启之后即可。

点击邀请用户，复制邀请链接发给需要注册的用户



用户在浏览器打开链接，输入相应的信息点击确认注册即可完成账号的注册，注册完成之后可直接登录。

2）您也可以在 RASP 平台直接添加用户，添加用户的时候可以通过选组功能，直接为用户分配小组。如果添加用户时时未选择小组，用户默认都属于默认小组。



3) 在系统管理-系统配置-LDAP 配置页面完成 LDAP 的配置并保存，即可从 LDAP 服务器同步用户到 RASP 平台。

9.2.2 小组管理

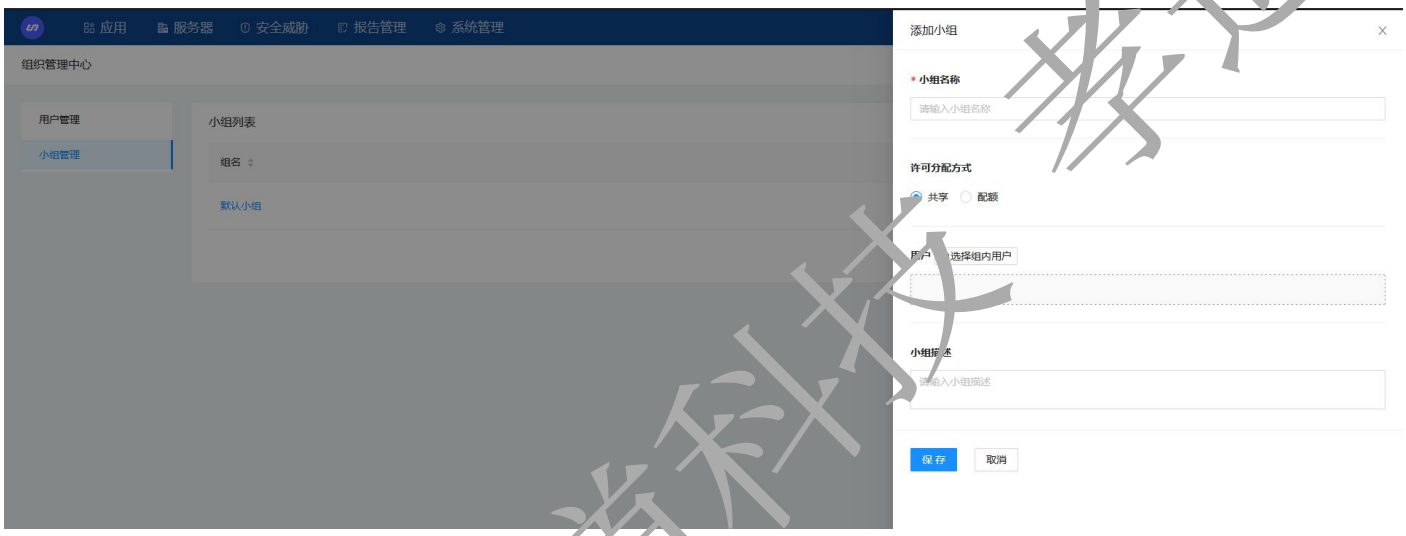
可在小组管理中添加不同的小组，小组许可分配方式有共享和配额两种，默认为共享模式，共享

即不需要给小组分配许可，所有共享模式的小组都使用系统可分配的许可。

当许可分配方式为配额时，添加小组时需要给小组分配检测、防护许可数量。

示例：系统共有 50 个 RASP 许可，建了三个小组 A、B、C；A 和 B 小组是共享模式，C 是配额模式，分配了 10 个许可。此时 A 和 B 共享使用 40 个，C 独享 10 个同时且 C 不能超过 10 个许可；给小组分配许可额度的时候，可分配数量（检测和防护分别的数量）=许可总数量-已分配给所有小组的额度-共享额度的小组已授权的数量。

添加小组时，可以通过选择组内用户功能为该小组添加用户。



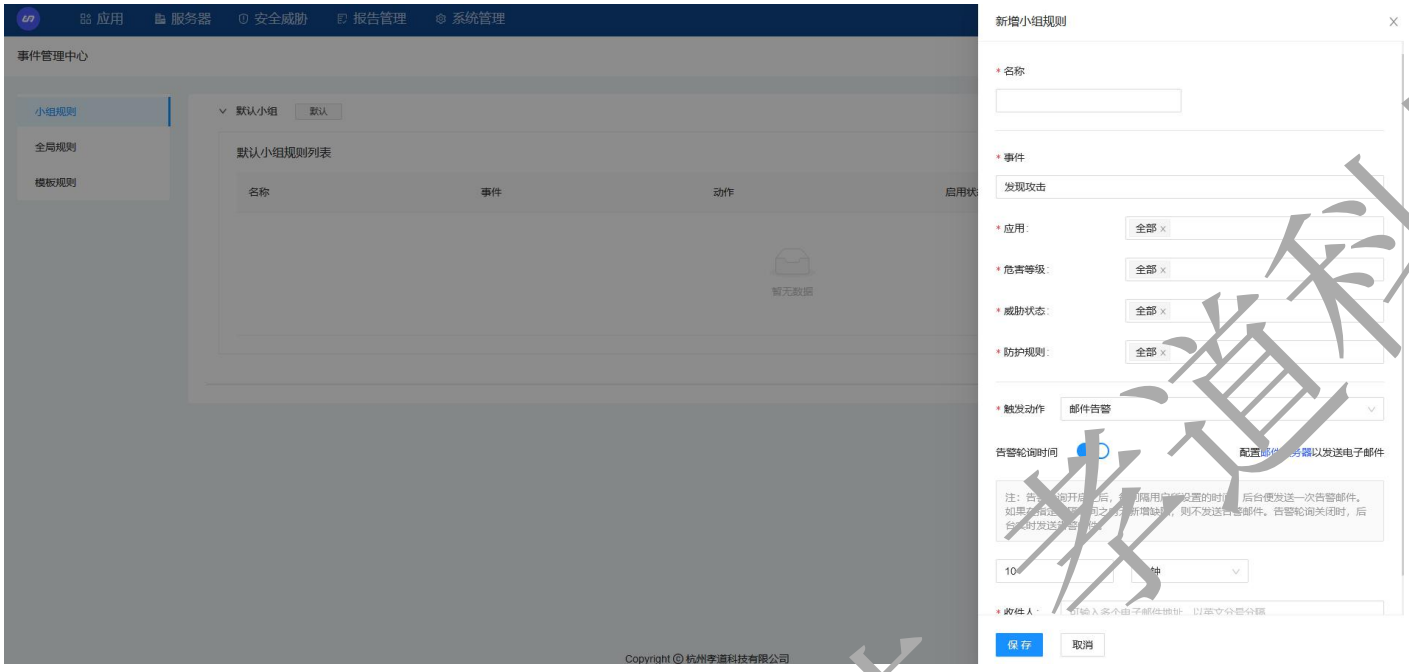
9.3 事件管理

9.3.1 小组规则

小组规则可针对不同的事件建立触发规则，RASP 平台主要有发现攻击、上报系统日志两种事件，每种事件都会触发 RASP 平台主动进行不同的操作。

以发现攻击为例，如下图配置，每当 rasp 应用被恶意攻击时，如果 RASP 平台配置了邮件服务器，就会发邮件到收件人账户。

触发动作选择 IP 加入黑名单，如果 rasp 应用被恶意攻击，那么攻击源 IP 就会被加入黑名单。



9.3.2 全局规则

全局规则是管理员添加的对多个组/多个应用起作用的规则（全局规则添加之后直接生效），只有管理员才能查看编辑全局规则。

9.3.3 模板规则

模板规则本身不触发动作，而是通过将模板规则自动复制到新建小组起作用，非管理员能编辑/删除复制到自己组内的模板规则，若您希望新建小组都有某些规则，则可以添加模板规则。

9.4 大屏展示

1 风险感知大屏

风险感知大屏实时显示了攻击数、拦截数、攻击源、受攻击应用、访问量等数据信息，在风险感知大屏，您可以查看受攻击应用排名-TOP5、攻击危害等级分布、以及攻击类型排名等信息。通过可视化地图，可以直观地查看攻击走向，了解到攻击来源及受攻击应用相关信息。此外，通过右上角的数据筛选，您可以分别查看中国或世界范围的攻击数据信息，或者不同应用所受到的攻击数据信息。

2 安全事件分析大屏

安全事件分析大屏实时展示了攻击态势、攻防日志概览、攻击来源链路-TOP5 等信息。

通过攻击态势，您可以实时查看到严重、高危、中危、低危攻击及访问量的数据量，访问量为正常请求数加上攻击请求数。

通过攻防日志概览，你可以实时查看到时间、攻击源 IP、目标 IP、攻击类型、受攻击应用及攻击链路信息，有助于你及时发现应用的安全风险。

此外，通过右上角的数据筛选，您可以分别查看中国或世界范围的攻击数据信息，或者不同应用所受到的攻击数据信息。

3 攻击关联性分析大屏

通过攻击关联性分析大屏，你可以实时的查看到受攻击应用、攻击来源 IP 的相关信息，同时也可以查看出哪些 IP 是单应用攻击、哪些 IP 是多应用攻击，以便于做出相应的应对措施。

此外，通过右上角的数据筛选，您可以分别查看中国或世界范围的攻击数据信息，或者不同应用所受到的攻击数据信息。

4 攻击来源回溯大屏

通过攻击来源回溯大屏，你可以直观地查看出具体哪些国家、哪些城市、哪些 IP 对应用发起了攻击，有助于你追踪到具体的攻击来源。

此外，通过右上角的数据筛选，您可以分别查看不同颗粒度（国家、省、城市、IP）的攻击来源，或者不同应用的攻击来源。

5 轮播

在设置中可以设置轮播的大屏，以及轮播的播放间隔时间。

9.5 策略管理

9.5.1 防护

1 防护规则

1)开启：防护功能开启后，对该规则的攻击进行监控及防护

2)关闭：不对该规则的攻击进行监控及防护。

2 IP 管理

1）黑名单：加入黑名单的 IP 禁止访问应用。

2）白名单：加入白名单的 IP 为信任主机，不做任何防护。

9.6 使用手册

在此处点击可以下载使用手册。