嵌入式安全审计平台

快速入门

腾讯云

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

快速入门
创建分析

最近更新时间：2024-05-15 17:19:32

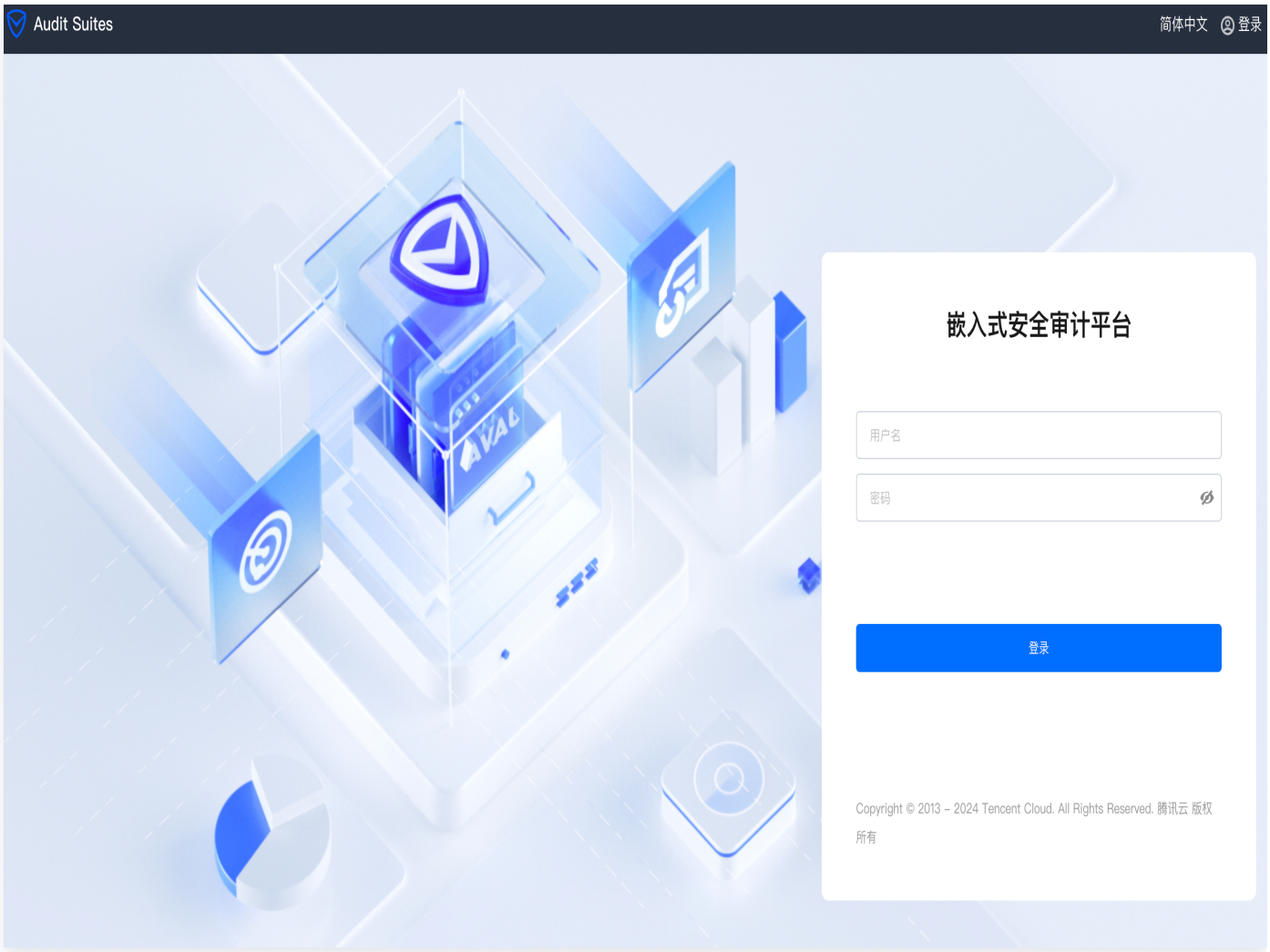
上传待检测文件，发现待检测文件中第三方组件所带来的安全、敏感信息、投毒组件以及许可证合规性等方面的问题，避免组件带来的风险。

前提条件

已安装嵌入式安全审计平台并可正常登录。

步骤1：登录平台

1. 输入用户名和密码，单击**登录**进入嵌入式安全审计平台，创建用户请联系管理员。



2. 登录成功后进入系统概览页面，用户权限分为管理员（Admin）和普通用户（User）。
   - 管理员（Admin）：可查看概览、项目管理、审计策略、KnowledgeBase（开源软件资产知识库）、报

告管理、用户管理、任务中心、系统设置页面。

- 普通用户（User）：可查看概览、项目管理、审计策略、KnowledgeBase（开源软件资产知识库）、报告管理页面。

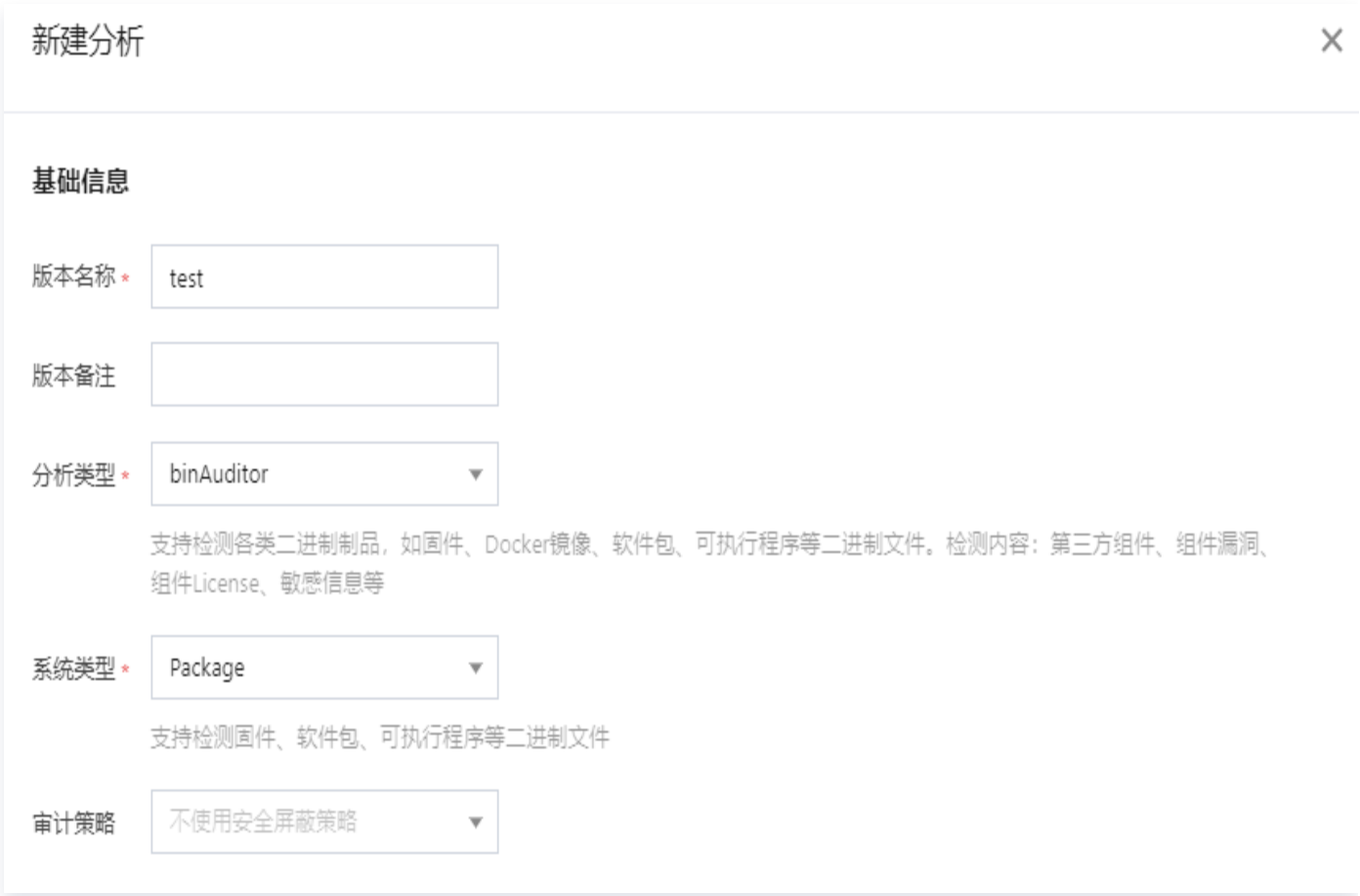
步骤2：创建项目

1. 在概览页面，单击页面上方的**项目管理**。
2. 在项目管理页面，选择所需团队，单击右上角的**新建项目**。
3. 在新建项目页面，输入项目名称和备注，单击**新建**。

步骤3：新建分析

1. 在项目管理页面，单击目标**项目名称**，进入详情页单击**新建分析**。

2. 在新建分析页面，填写基础信息。



参数名称	说明
版本名称	分析包版本名称。
版本备注	该版本备注信息。
分析类型	支持 sysAuditor、binAuditor、srcAuditor与 apkAuditor，详细分析可参见 分析类型概览 。
系统类型	支持不同类型二进制文件，包括但不限于固件、软件包、可执行程序、Docker 镜像、bin、hex、s19格式的 RTOS 固件等。
审计策略	应用于不同分析，用于屏蔽/突出特定的漏洞，License，审计规则以及组件信息，可以方便使用策略快速排查问题

3. 在新建分析页面，单击**新增分析文件**，选择**文件类型**，单击**点击上传**，上传目标文件。

4. 在新建分析页面，配置分析参数。

参数名称	说明

屏蔽路径	大小写敏感，支持通配符*匹配，如： • 屏蔽指定目录下的所有文件和子目录：/skipped/path/* • 屏蔽所有目录下的pom.xml文件：*/pom.xml • 屏蔽所有以_test结尾的go文件：*/*_test.go
分析文件	分析的文件类型，会对安全审计结果及分析时间产生影响
分析超时	文件分析响应时间，若某文件未在响应时间内分析成功，则触发超时机制
开启 C/C++组件SCA	默认启用，禁用后跳过 C/C++组件 SCA 分析
开启 C/C++组件 SC A深度扫描	开启后扫描精确度提升，扫描耗时也将增加
解包递归深度	0 表示递归深度自动调整

5. 完成上述配置后，单击**新建**，即可创建成功。

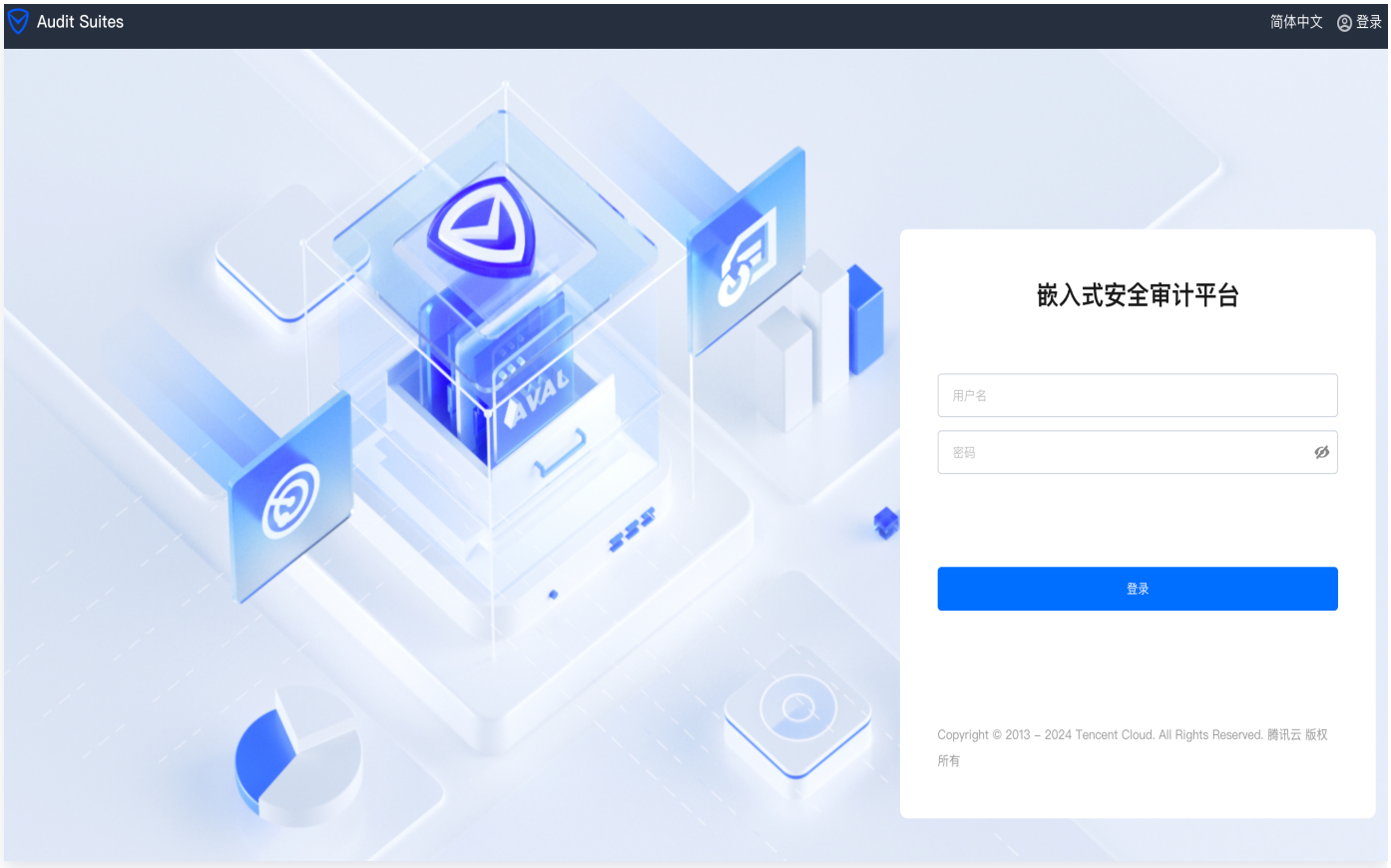
分析类型概览

产品类型名称		描述
sysAuditor	系统基线安全审计	集信息采集、结果分析和检测报告于一体的自动化安全审计平台。
binAuditor	制品安全审计	聚焦于完整的系统的二进制分析，帮助用户分析出制品中的种种安全问题。
srcAuditor	源码安全审计	以源码为核心的软件成分分析平台，帮助用户检测开源组件、敏感信息、license 合规、Copyright、病毒文件风险，建立 SBOM，解决供应链安全及开源合规问题。
apkAuditor	安卓应用安全审计	对用户提供的安卓应用进行安全漏洞、隐私合规检测，检测权限、组件、网络等 App 基础安全漏洞，并提供详细的漏洞信息及修复建议。

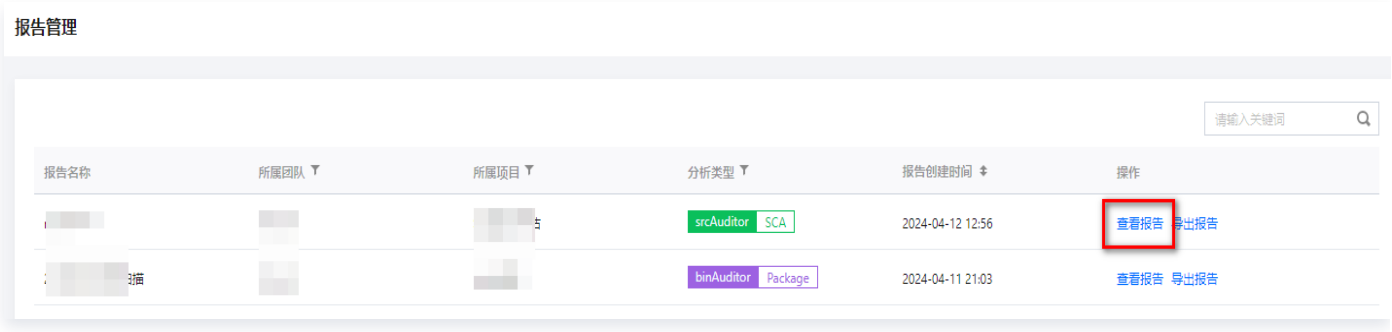
查看报告

最近更新时间：2024-05-15 17:19:32

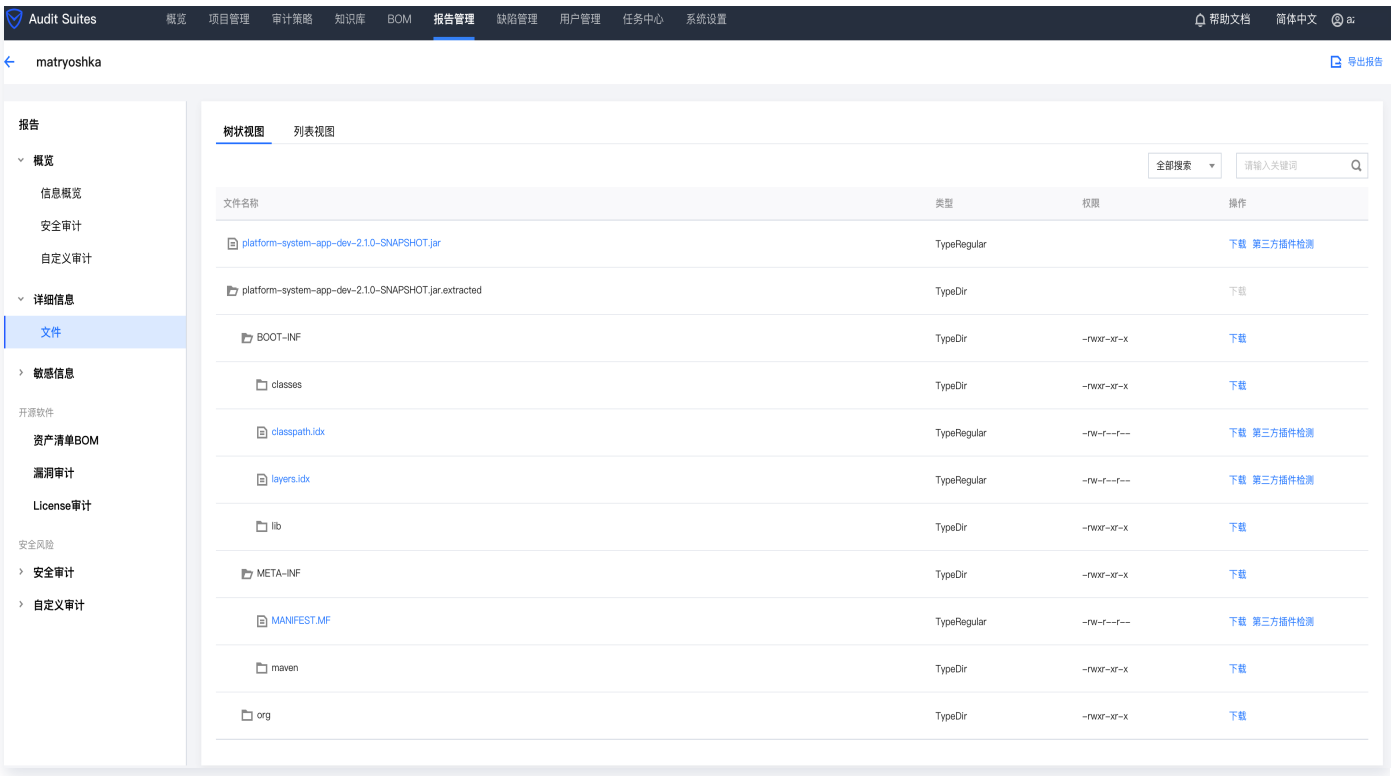
1. 输入用户名和密码，单击**登录**进入嵌入式安全审计平台，创建用户请联系管理员。



2. 在报告管理页面，选择所需报告，单击**查看详情**。



3. 在报告页面，分为概览、详细信息、敏感信息、潜在风险、漏洞审计、资产清单 BOM、漏洞审计、License 审计、安全审计和自定义审计9个部分。单击不同菜单即可查看详细内容。

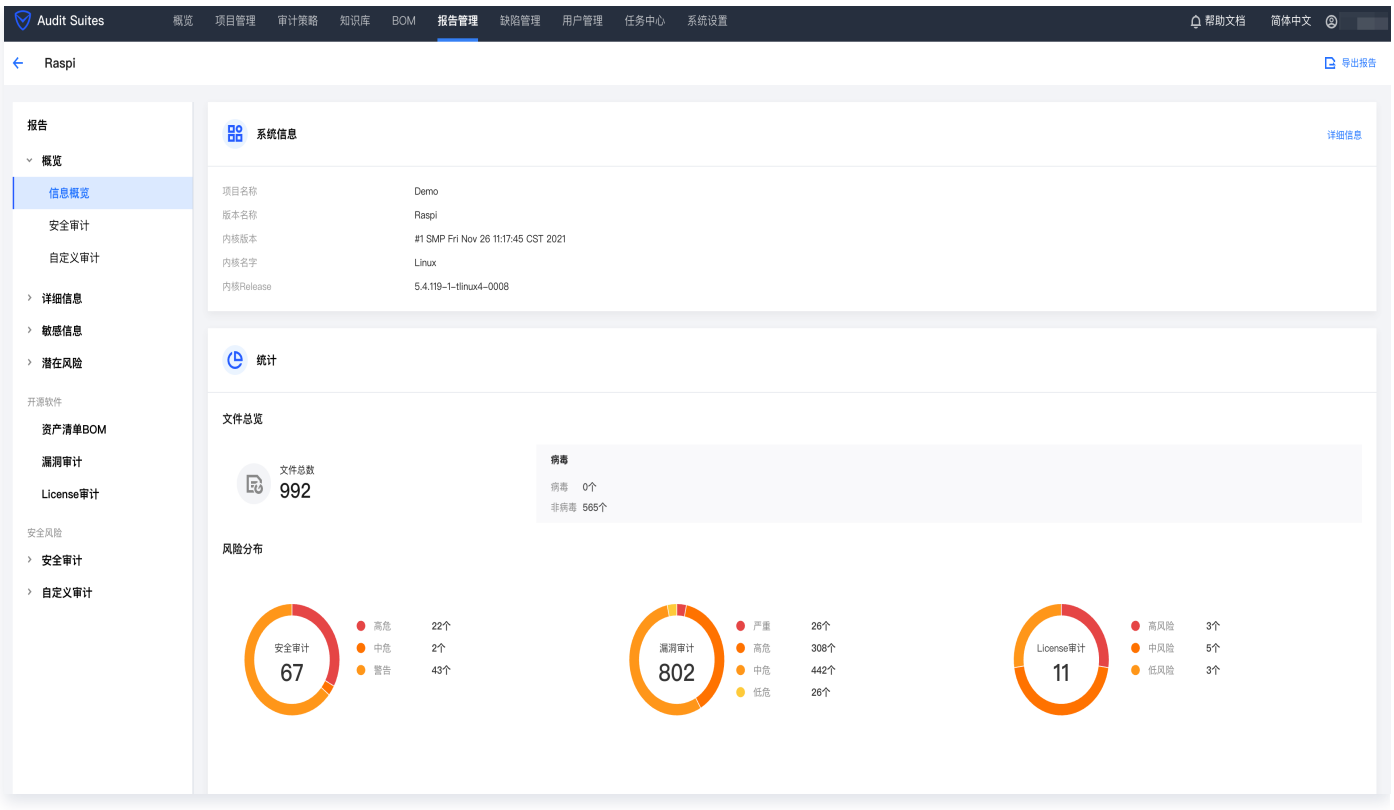


报告内容

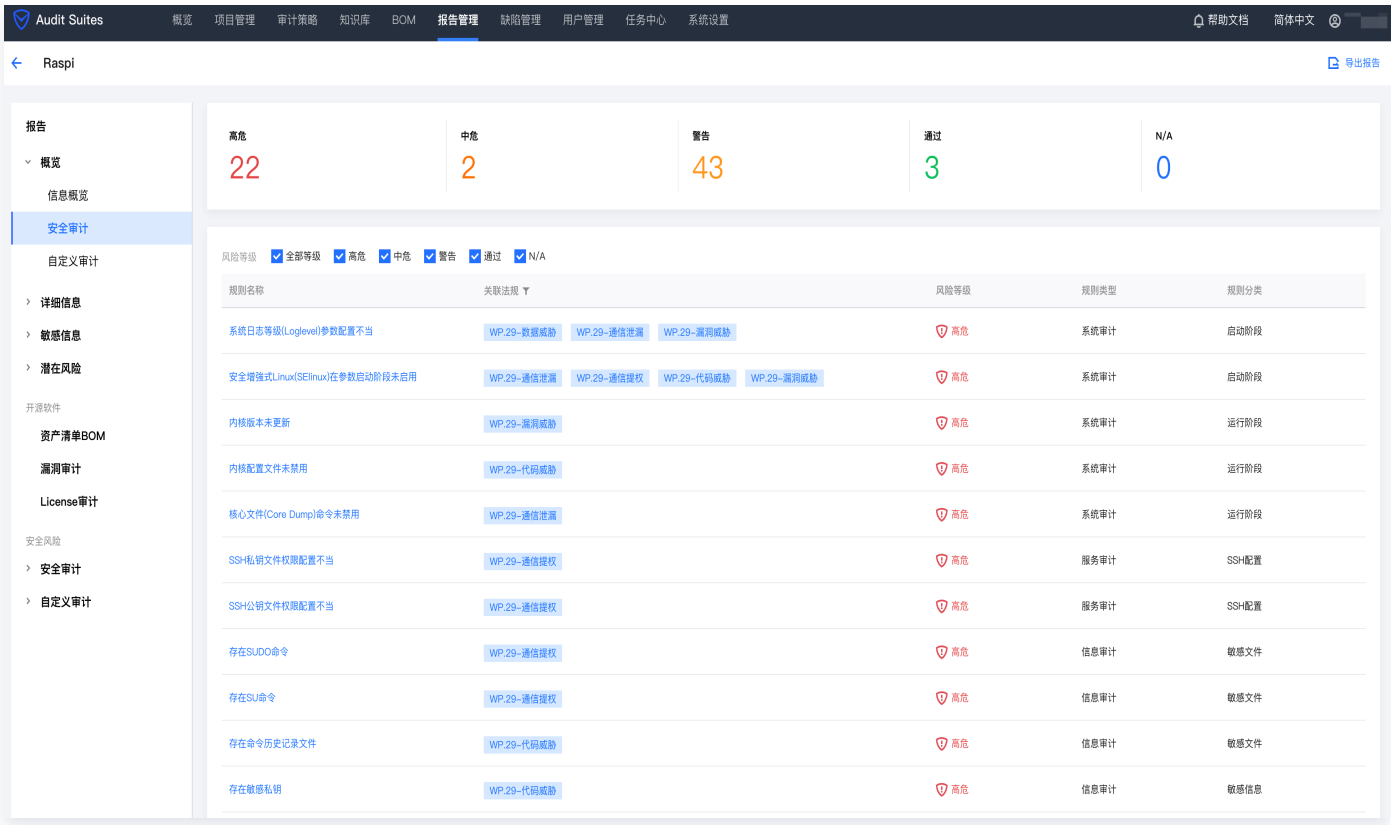
报告页共包含概览、详细信息、敏感信息、潜在风险、漏洞审计、资产清单 BOM、漏洞审计、License 审计、安全审计和自定义审计9个部分。

概览

- 信息概览：包含系统信息和风险统计。单击**风险内容**可跳转至对应详情页。



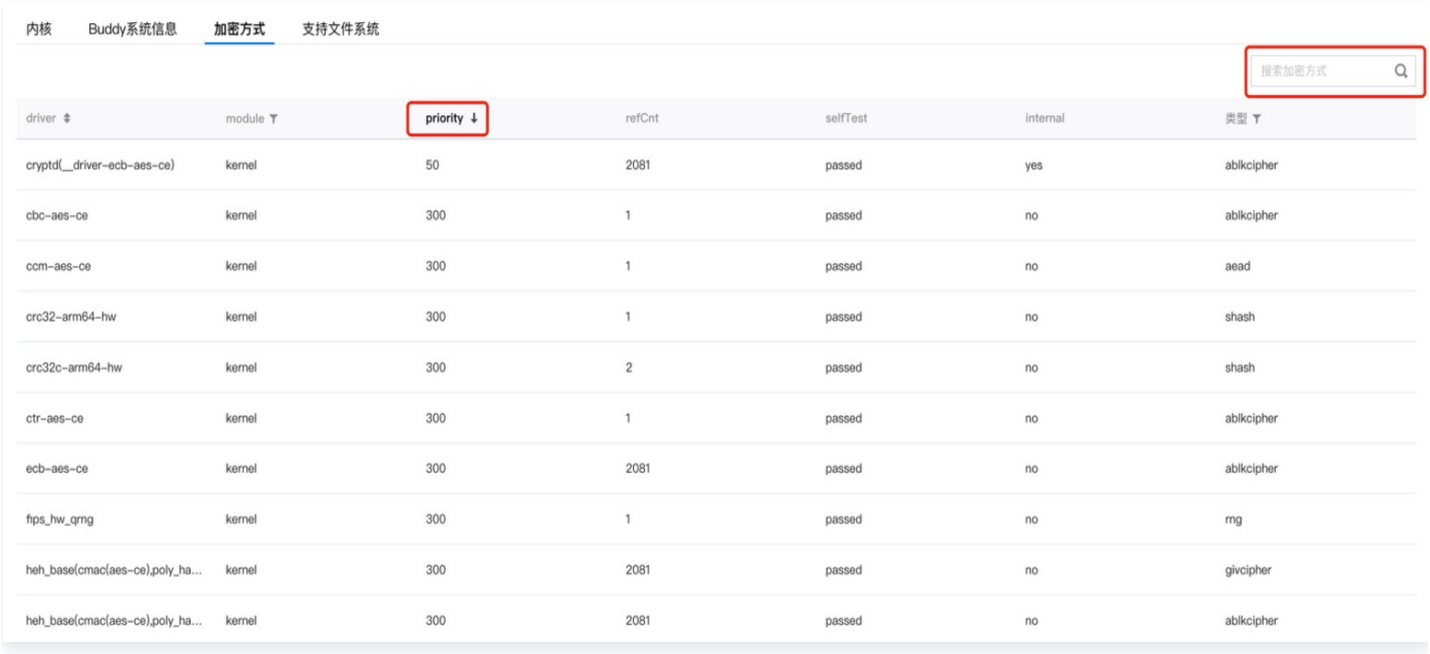
- 安全审计（自定义审计）：显示审计统计结果和检查规则结果。并给出WP.29法规对应风险类型。



详细信息

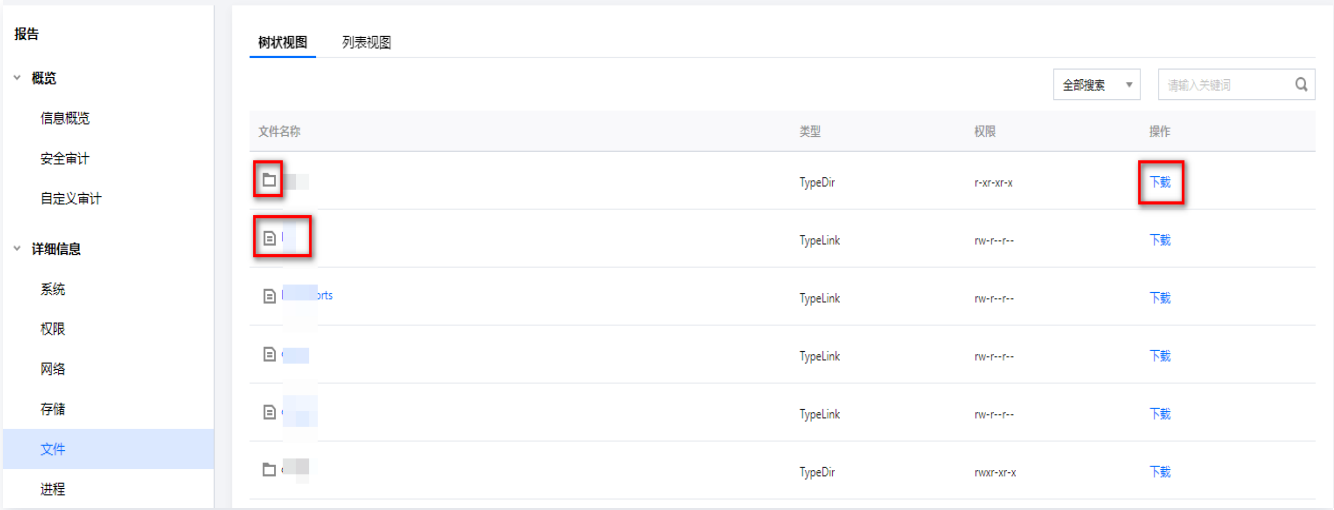
详细信息包含系统、权限、网络、存储、文件、进程、命令和外设。

- 以系统为例：部分列可做排序筛选，部分页面可模糊搜索。

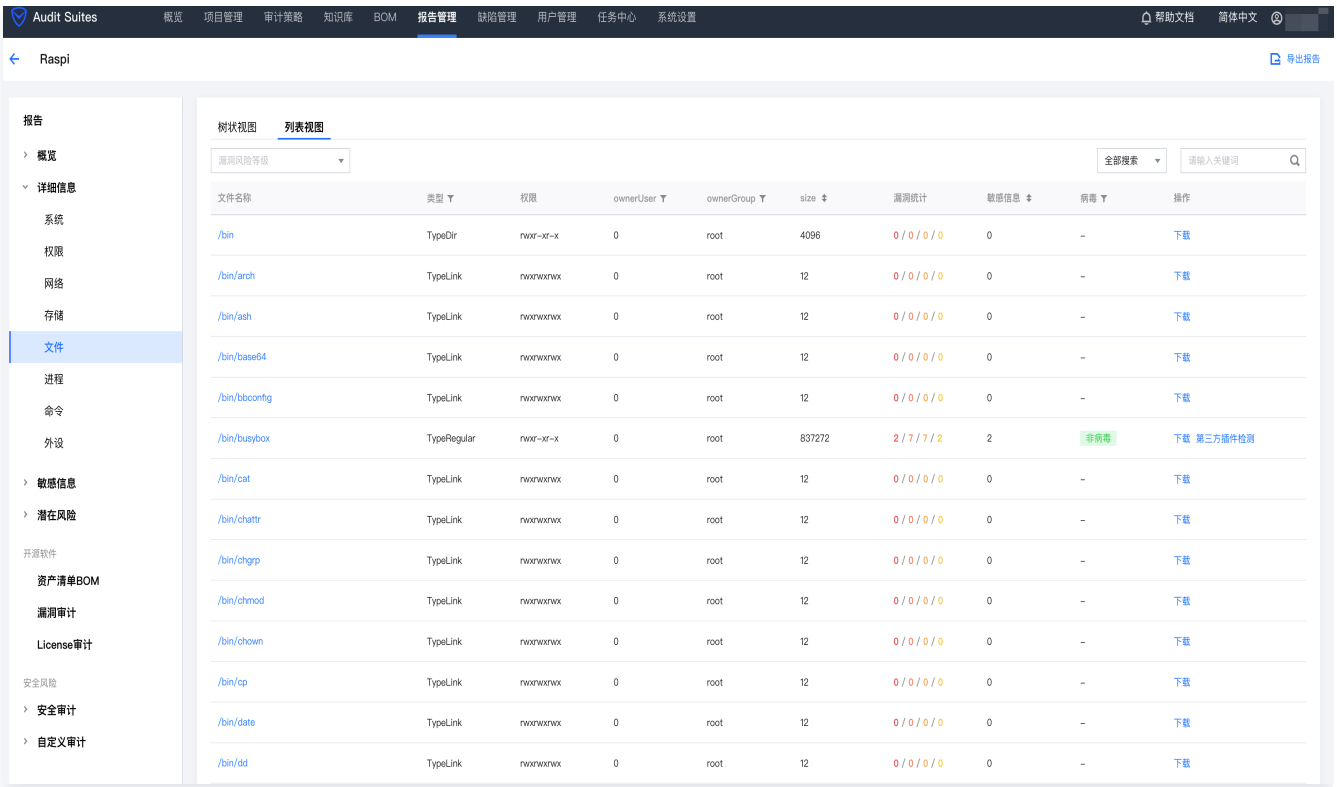


driver	module	priority	refCnt	selfTest	internal	类型
cryptd(__driver-ecb-aes-ce)	kernel	50	2081	passed	yes	ablkcipher
cbc-aes-ce	kernel	300	1	passed	no	ablkcipher
ccm-aes-ce	kernel	300	1	passed	no	aead
crc32-arm64-hw	kernel	300	1	passed	no	shash
crc32c-arm64-hw	kernel	300	2	passed	no	shash
ctr-aes-ce	kernel	300	1	passed	no	ablkcipher
ecb-aes-ce	kernel	300	2081	passed	no	ablkcipher
fips_hw_qrng	kernel	300	1	passed	no	rng
heh_base(cmac(aes-ce),poly_ha...	kernel	300	2081	passed	no	givcipher
heh_base(cmac(aes-ce),poly_ha...	kernel	300	2081	passed	no	ablkcipher

- 文件和进程具有树状视图和列表视图。
  - 树状视图可单击展开和收缩；单击**下载**可下载单个文件或文件夹；单击**蓝色文件名称**查看文件完整信息；搜索区可选择目标列模糊搜索。



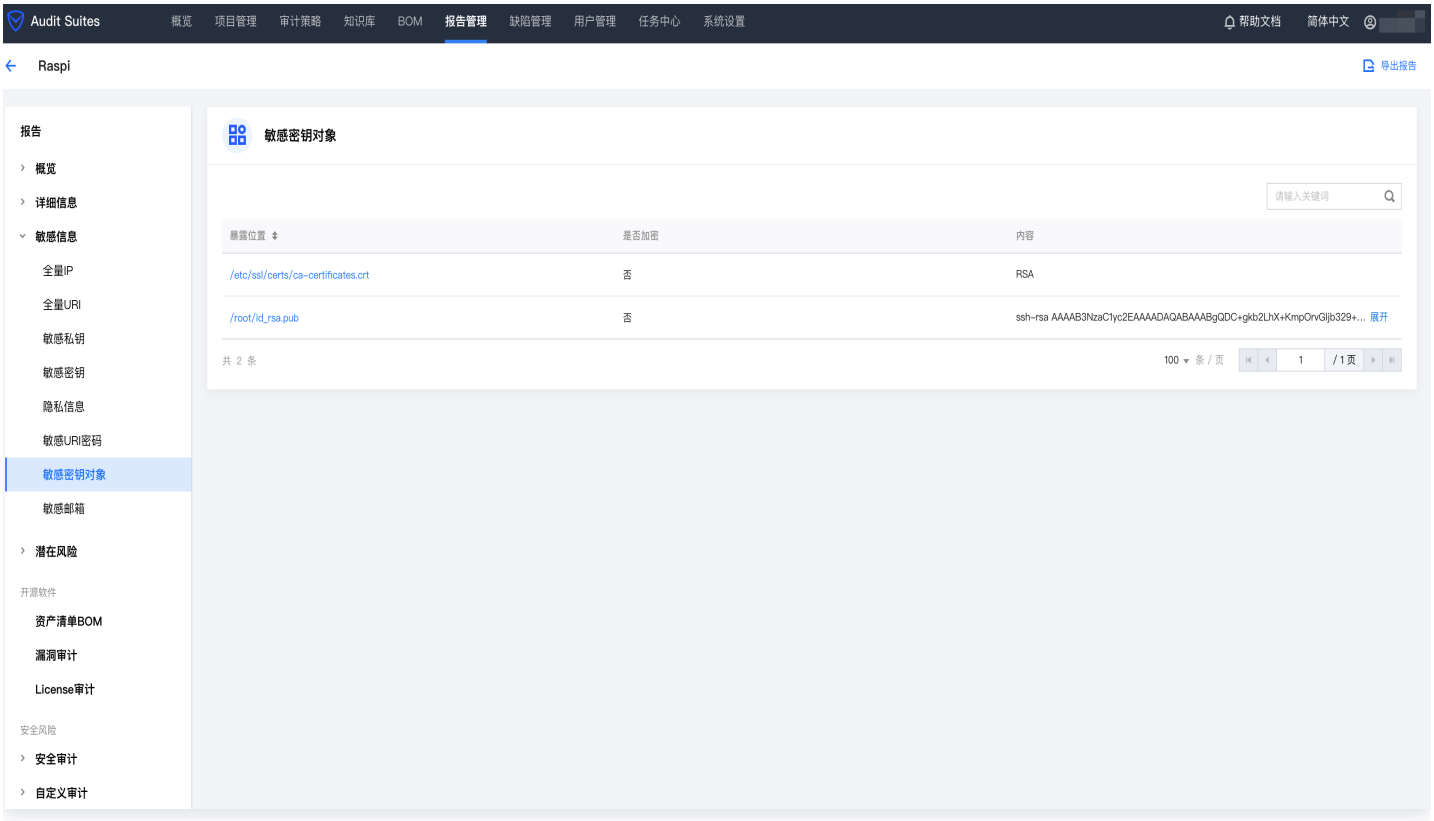
  - 列表视图，可根据类型、权限、ownerUser 等子项进行排序，针对单独的文件可以进行下载，部分文件可以进行第三方插件病毒检测；搜索区域可选择关键词模糊搜索。



敏感信息

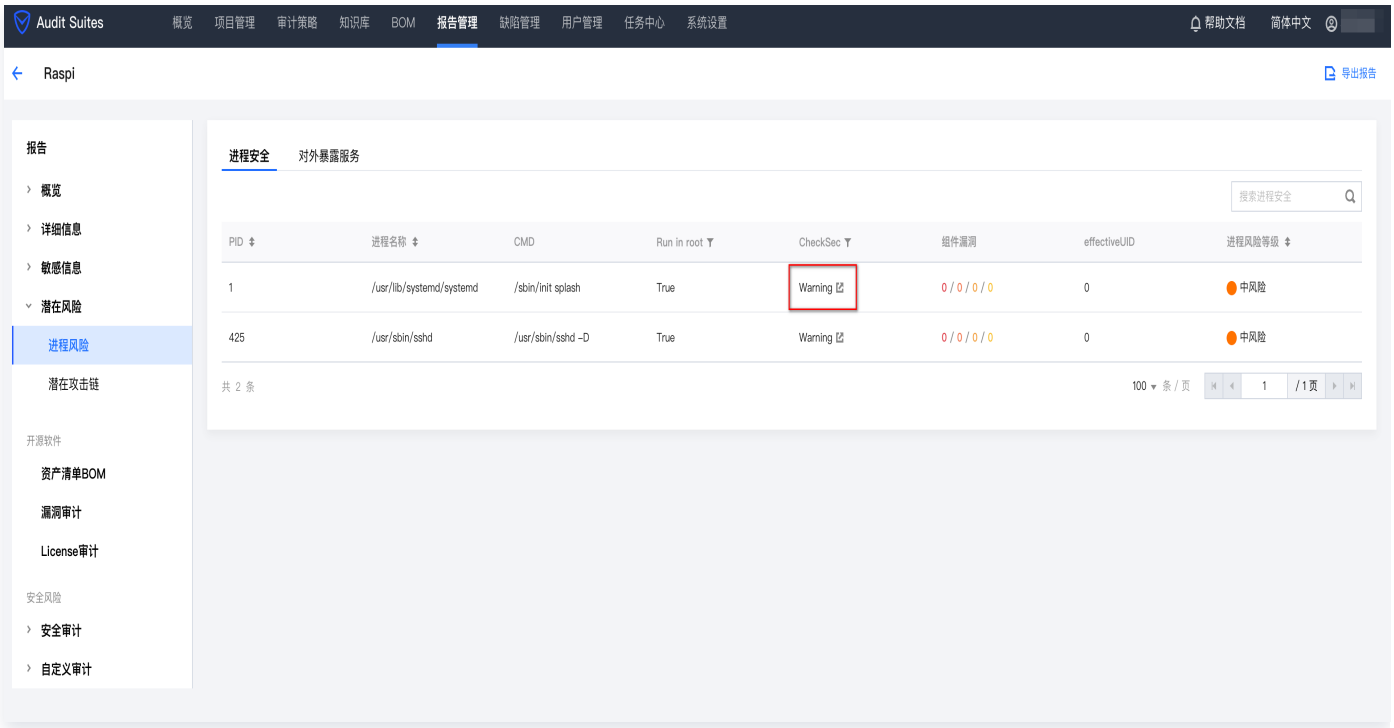
敏感信息包含敏感 URI、IP、邮箱、私钥、密钥、隐私信息、密钥对象和 URI 密码。

以敏感 URI 为例，以根域名视角，查看分析项中包含的敏感 URI。URI 数量为该域名下检测到的不同 URI 数量。暴露数量为该 URI 涉及的文件个数。单击**文件列表**，展示所有涉及文件，且单击**文件**可以跳转**详细信息 >文件列表**，查看文件详细信息。

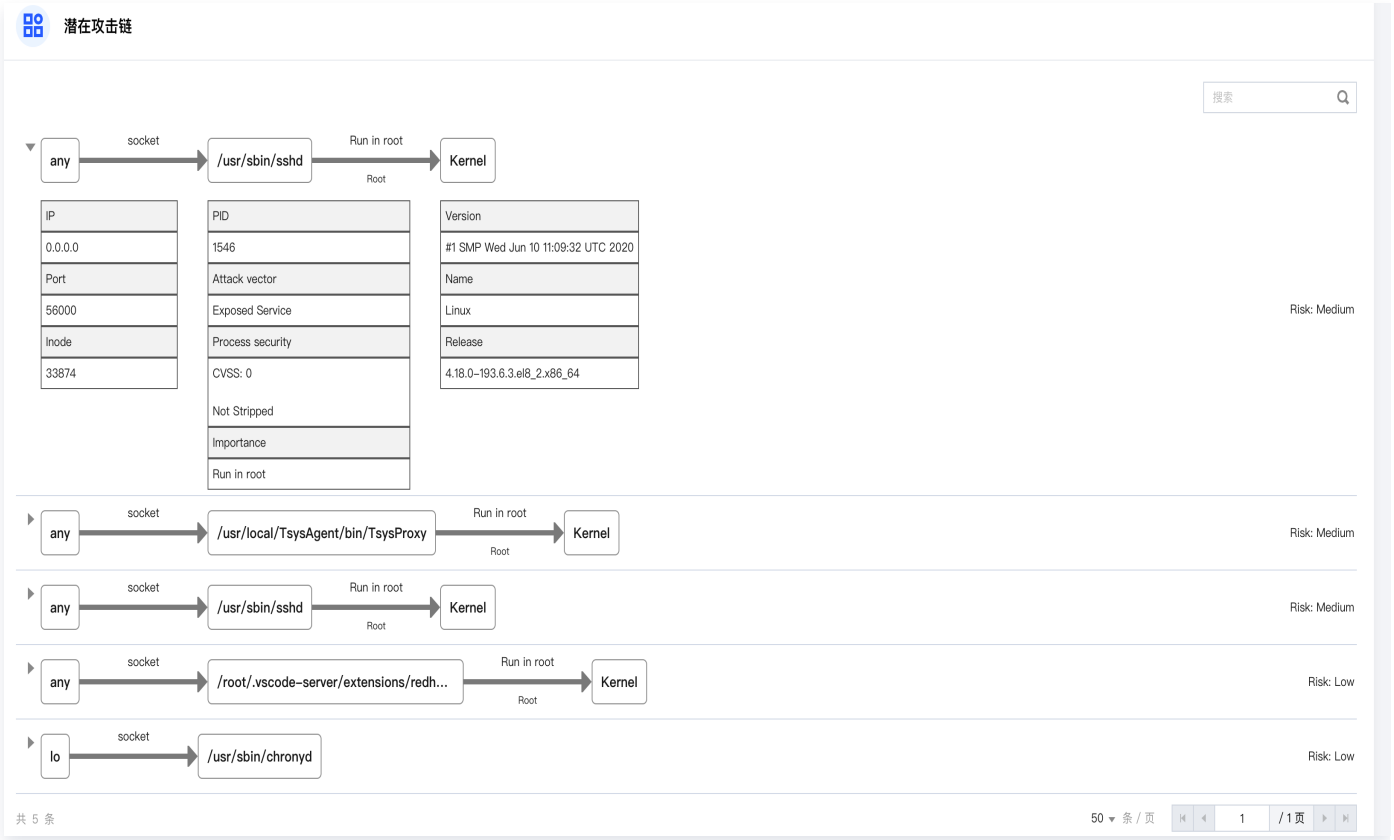


潜在风险

- 进程风险依据运行状态、涉及共享库 CheckSec 结果、漏洞审计结果定义风险等级，CheckSec 和漏洞审计结果单击 Warning 项跳转相关详情页。

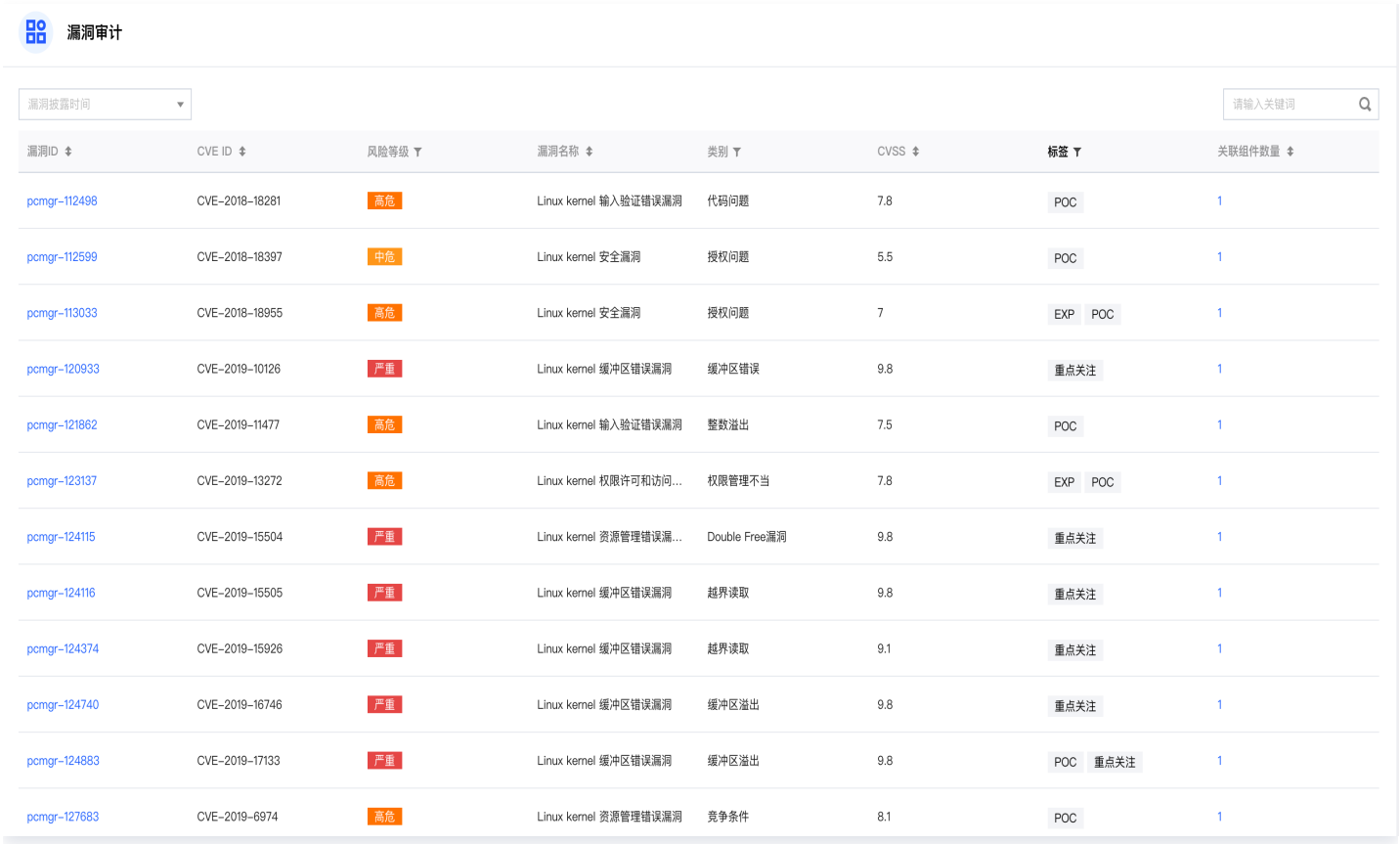


- 潜在攻击链提供攻击端口、进程及影响范围。



漏洞审计

漏洞审计以第三方库或内核版本为视角，统计漏洞信息。
报告提供第三方库信息、漏洞统计、漏洞列表、风险等级、CVSS、漏洞标签（POC、EXP、重点关注）、漏洞状态等详细信息。



漏洞ID	CVE ID	风险等级	漏洞名称	类别	CVSS	标签	关联组件数量
pcmgr-112498	CVE-2018-18281	高危	Linux kernel 输入验证错误漏洞	代码问题	7.8	POC	1
pcmgr-112599	CVE-2018-18397	中危	Linux kernel 安全漏洞	授权问题	5.5	POC	1
pcmgr-113033	CVE-2018-18955	高危	Linux kernel 安全漏洞	授权问题	7	EXP POC	1
pcmgr-120933	CVE-2019-10126	严重	Linux kernel 缓冲区错误漏洞	缓冲区错误	9.8	重点关注	1
pcmgr-121862	CVE-2019-11477	高危	Linux kernel 输入验证错误漏洞	整数溢出	7.5	POC	1
pcmgr-123137	CVE-2019-13272	高危	Linux kernel 权限许可和访问...	权限管理不当	7.8	EXP POC	1
pcmgr-124115	CVE-2019-15504	严重	Linux kernel 资源管理错误漏...	Double Free漏洞	9.8	重点关注	1
pcmgr-124116	CVE-2019-15505	严重	Linux kernel 缓冲区错误漏洞	越界读取	9.8	重点关注	1
pcmgr-124374	CVE-2019-15926	严重	Linux kernel 缓冲区错误漏洞	越界读取	9.1	重点关注	1
pcmgr-124740	CVE-2019-16746	严重	Linux kernel 缓冲区错误漏洞	缓冲区溢出	9.8	重点关注	1
pcmgr-124883	CVE-2019-17133	严重	Linux kernel 缓冲区错误漏洞	缓冲区溢出	9.8	POC 重点关注	1
pcmgr-127683	CVE-2019-6974	高危	Linux kernel 资源管理错误漏洞	竞争条件	8.1	POC	1

License 审计

License 审计以第三方库为视角，提供 License 信息，包括 License 名称、要求、来源及声明。

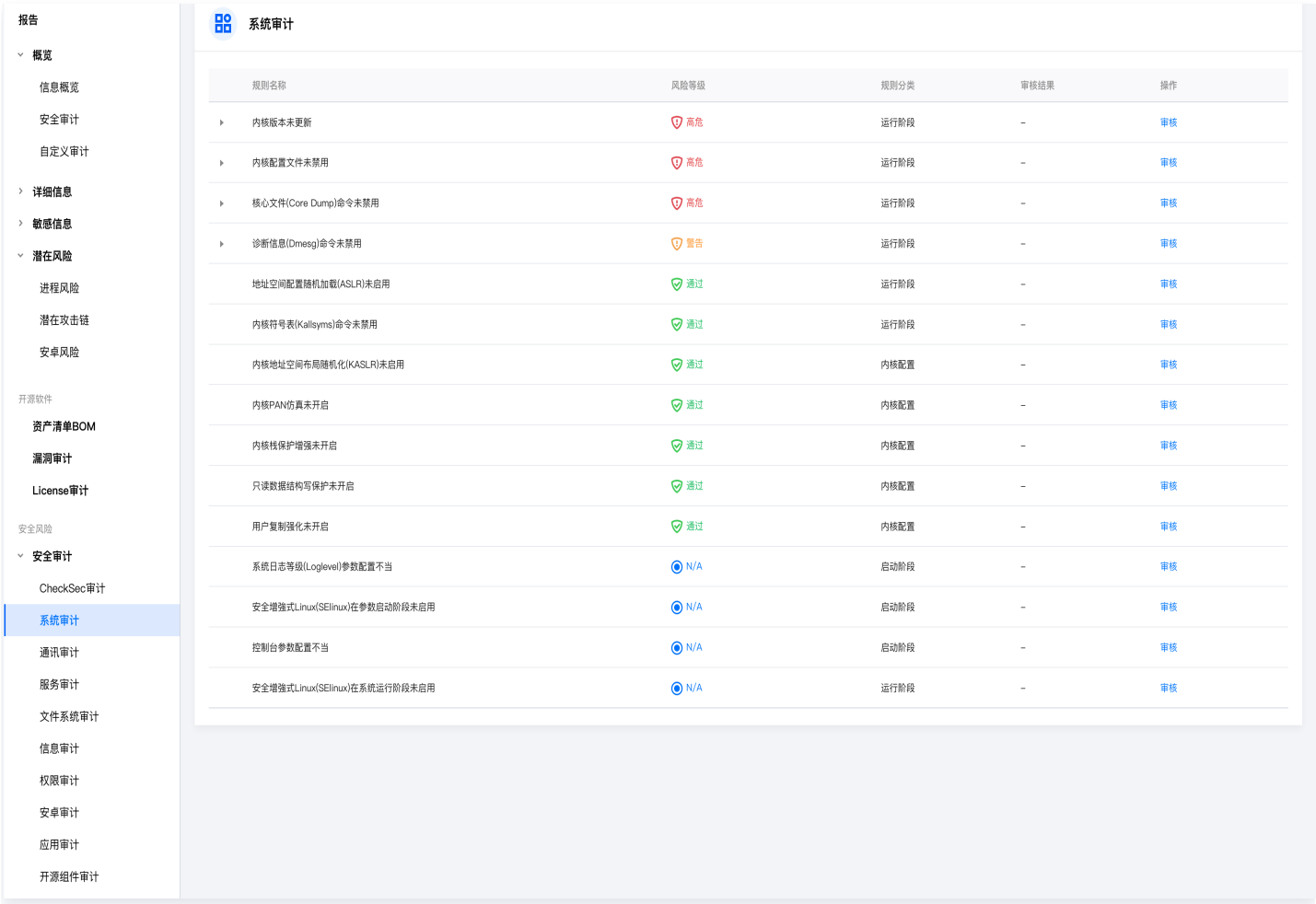
License审计

请输入关键词

License名称	License风险	来源	关联组件数量	关联文件数量
bsd-new	低风险	组件	2	0
gpl-1.0-plus	中风险	组件	2	0
gpl-2.0	高风险	组件	11	0
gpl-2.0-plus	高风险	组件	1	0
gpl-3.0	高风险	组件	2	0
lgpl-2.0	中风险	组件	1	0
lgpl-2.1-plus	中风险	组件	1	0
linux-syscall-exception-gpl	N/A	组件	1	0
mit	低风险	组件	2	0
mit-old-style-no-advert	低风险	组件	1	0
openssl-ssleay	中风险	组件	1	0
other-copyleft	N/A	组件	1	0
other-permissive	N/A	组件	1	0

安全审计

安全审计会以 Checksec 审计、系统审计、通讯审计、服务审计、文件系统审计、信息审计、权限审计、安卓审计、应用审计以及开源组件审计为维度将系统扫描对应的规则详情，做详细的展开。


报告
概览
信息概览
安全审计
自定义审计
详细信息
敏感信息
潜在风险
进程风险
潜在攻击链
安卓风险
开源软件
资产清单BOM
漏洞审计
License审计
安全风险
安全审计
CheckSec审计
系统审计
通讯审计
服务审计
文件系统审计
信息审计
权限审计
安卓审计
应用审计
开源组件审计
系统审计
规则名称
风险等级
规则分类
审核结果
操作
内核版本未更新 高危 运行阶段 - 审核
内核配置文件未禁用 高危 运行阶段 - 审核
核心文件(Core Dump)命令未禁用 高危 运行阶段 - 审核
诊断信息(Dmesg)命令未禁用 警告 运行阶段 - 审核
地址空间配置随机加载(ASLR)未启用 通过 运行阶段 - 审核
内核符号表(Kallsyms)命令未禁用 通过 运行阶段 - 审核
内核地址空间布局随机化(KASLR)未启用 通过 内核配置 - 审核
内核PAN仿真未开启 通过 内核配置 - 审核
内核栈保护增强未开启 通过 内核配置 - 审核
只读数据结构写保护未开启 通过 内核配置 - 审核
用户复制强化未开启 通过 内核配置 - 审核
系统日志等级(Loglevel)参数配置不当 N/A 启动阶段 - 审核
安全增强式Linux(SElinux)在参数启动阶段未启用 N/A 启动阶段 - 审核
控制台参数配置不当 N/A 启动阶段 - 审核
安全增强式Linux(SElinux)在系统运行阶段未启用 N/A 运行阶段 - 审核