

嵌入式安全审计平台 操作指南



腾讯云

【 版权声明 】

©2013–2024 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 商标声明 】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【 联系我们 】

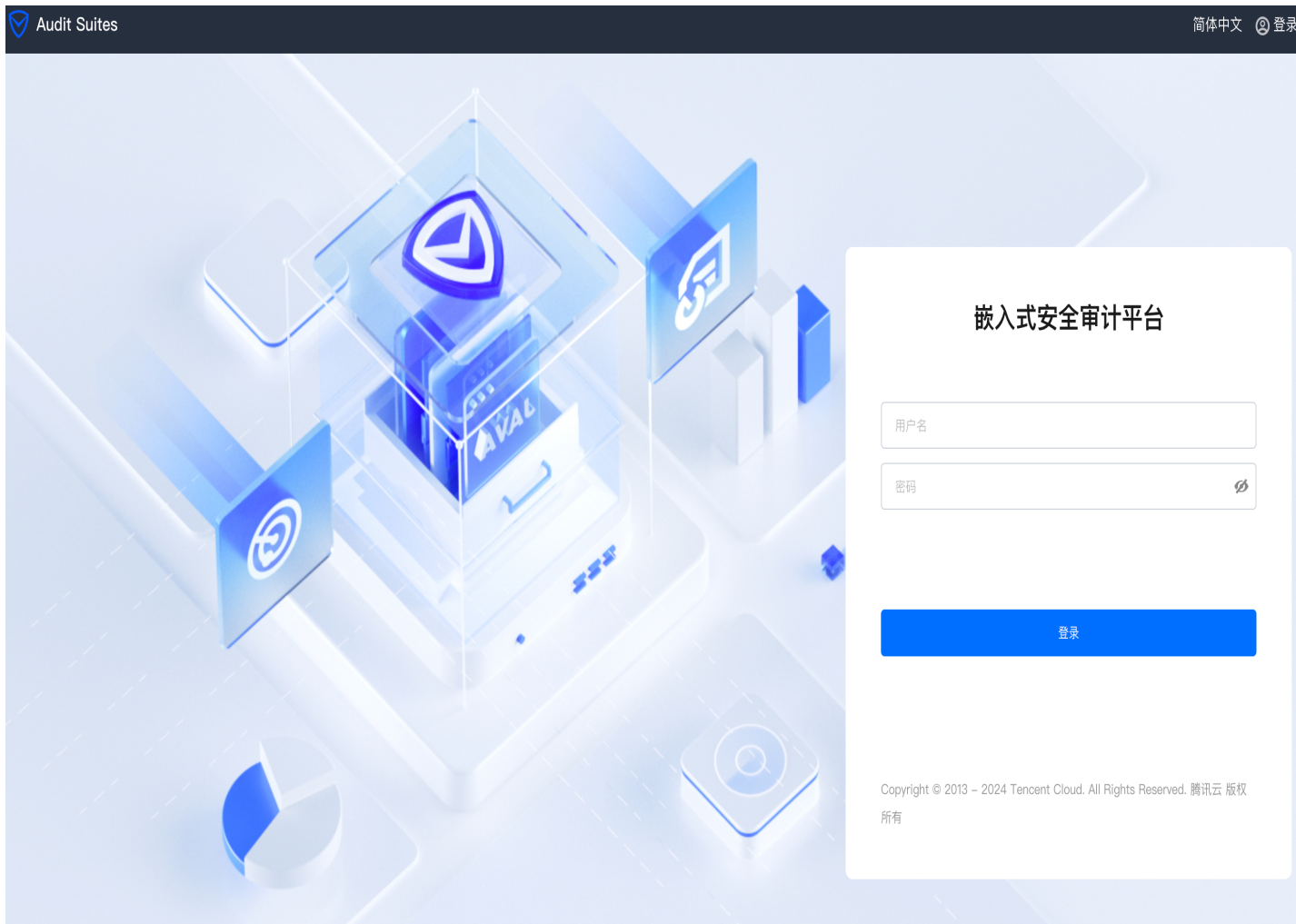
我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或 95716。

操作指南

最近更新时间：2024-05-15 17:19:32

1.1 登录

输入用户名和密码登录进入嵌入式安全审计平台，创建用户请联系管理员。



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）。

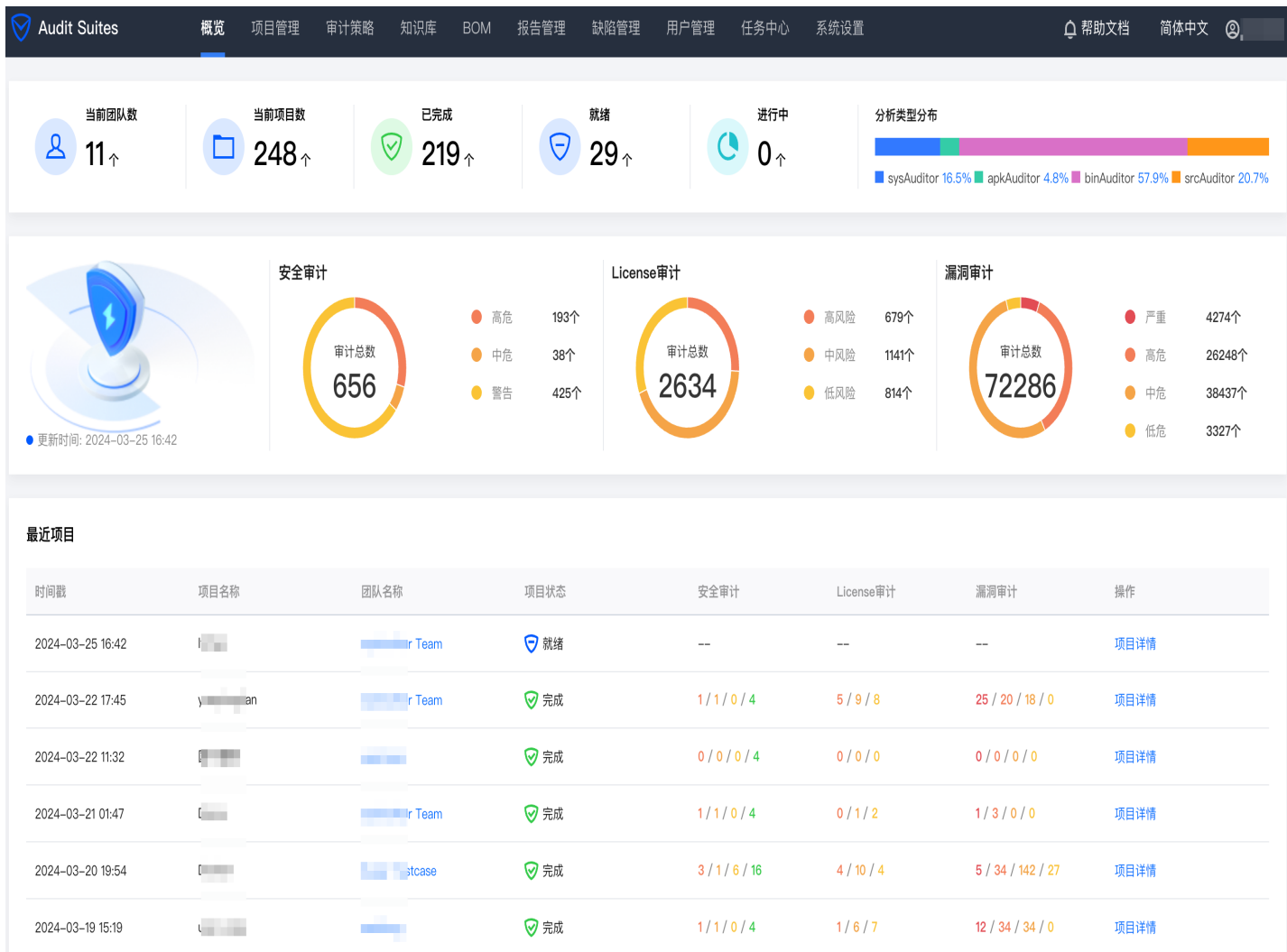
- 管理员（Admin）：可查看概览、项目管理、审计策略、KnowledgeBase（开源软件资产知识库）、报告管理、用户管理、任务中心、系统设置页面。
- 普通用户（User）：可查看概览、项目管理、审计策略、KnowledgeBase（开源软件资产知识库）、报告管理页面。

1.2 概览

在概览页面，主要包含团队项目统计、状态统计、风险统计、最近项目等。

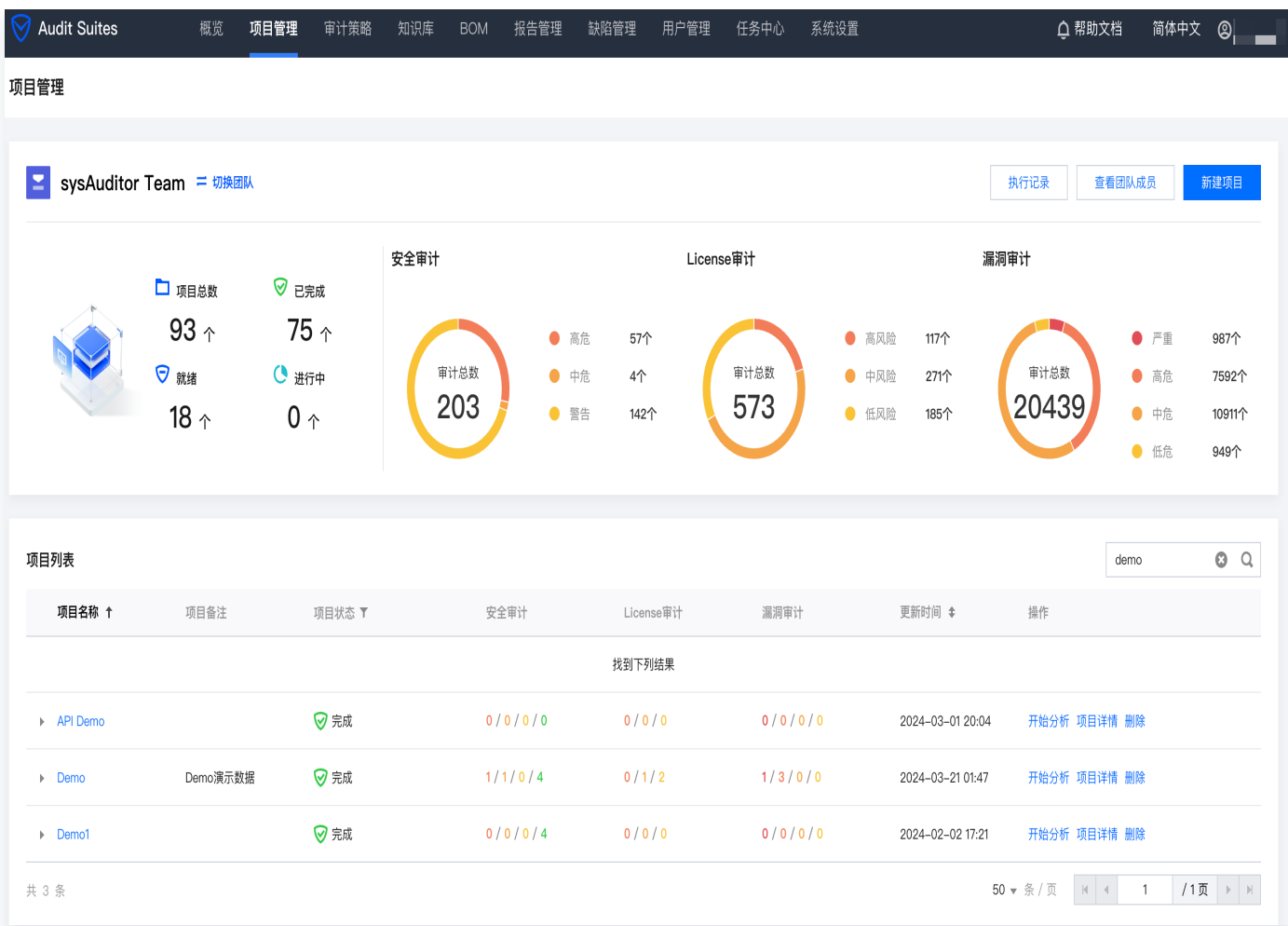
- 团队项目统计：统计用户加入的团队和项目个数。
- 状态统计：统计用户项目分析状态信息。

- **风险统计**：统计用户项目的不同等级风险信息。
- **最近项目**：显示最近操作的10个项目信息。

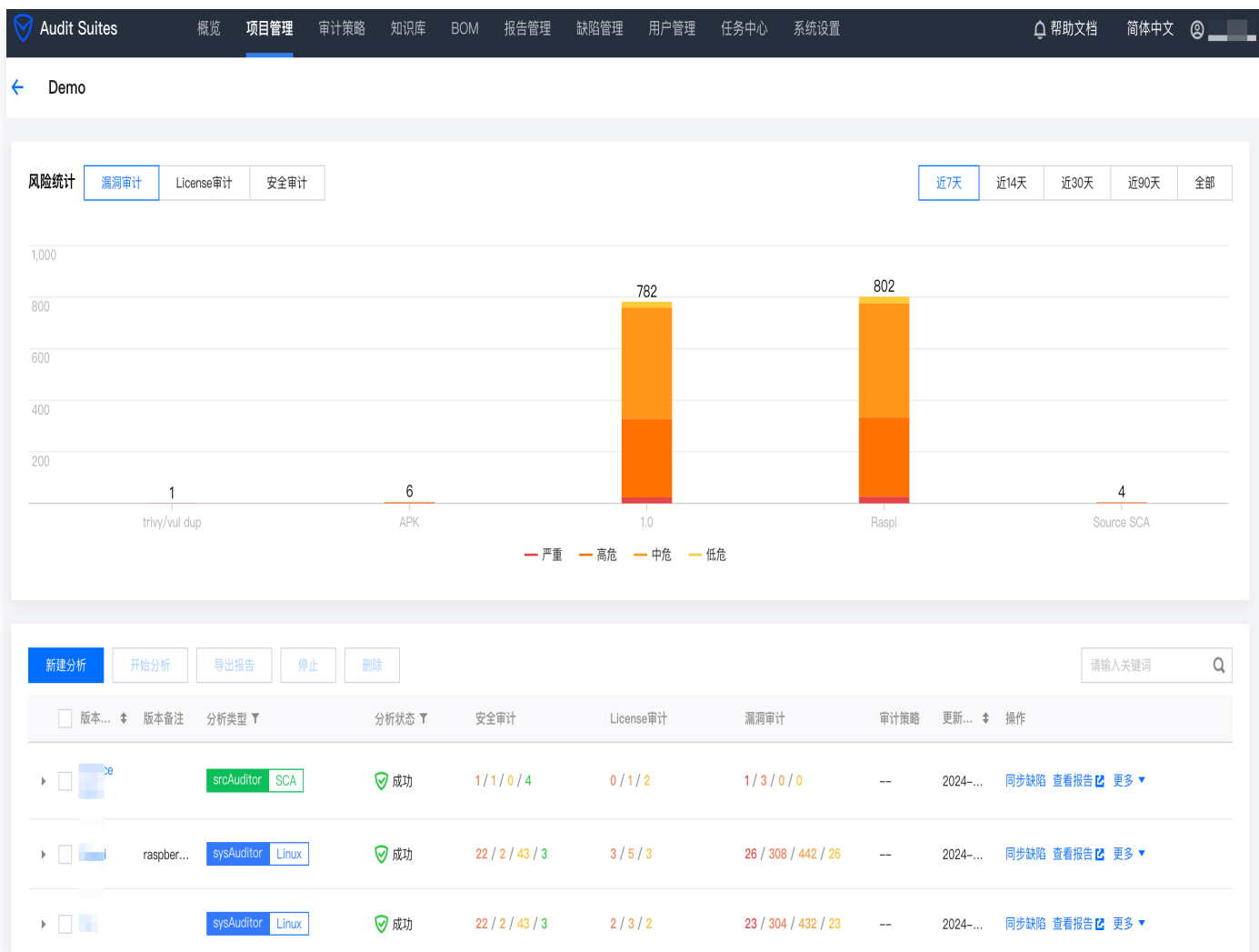


1.3 项目管理

- 在项目管理页面，可以查看当前团队下项目列表和相关统计信息。
 - 新建项目：创建新项目。详情请参见 [创建分析](#)。
 - 开始分析：可触发项目下所有分析。
 - 删除：可以软删除当前项目，系统管理员可在任务中心恢复软删除的项目。
 - 项目详情：可以进入项目查看详细分析版本列表。
 - 执行记录：仅团队管理员可见，可以查看项目的历史执行记录。
 - 查看团队成员：仅团队管理员可见，可以管理团队成员，包含添加成员、删除成员、显示所有成员。



- 可切换团队查看不同团队项目信息，加入团队需联系团队管理员操作，用户在团队中有三种角色。
 - 团队管理员 (Manager)：具有查看、操作项目、管理团队权限，会显示相关团队管理入口。
 - 团队成员 (Member)：具有查看、操作项目相关权限。
 - 团队只读成员 (Viewer)：具有查看项目权限。
- 单击项目详情可查看该项目分析版本列表。



1.4 审计策略

在审计策略页面，可以查看策略列表和相关统计信息，每个团队都有对应的审计策略，审计策略的作用是根据特定的规则过滤分析结果。

说明：

不同的团队角色具有不同的权限。

- 团队管理员 (Manager)：具有查看、创建、编辑审计策略权限。
- 团队普通成员 (Member)：具有查看、创建、编辑审计策略权限。
- 团队只读成员 (Viewer)：具有查看审计策略权限。

- 新建策略：新建团队安全审计策略。
- 设为默认/取消默认：设置/取消当前策略为默认策略，创建分析时将优先显示默认策略。
- 修改策略：修改安全审计策略规则。
- 复制：在当前团队复制出一条相同策略。
- 删除：删除当前策略，若该策略已被分析使用，需先将策略和分析解绑后才可删除。

Audit Suites
帮助文档 简体中文

概览 项目管理 **审计策略** 知识库 BOM 报告管理 缺陷管理 用户管理 任务中心 系统设置

审计策略

sysAuditor Team
切换团队

策略总数 115

sysAuditor数量 33

binAuditor数量 54

apkAuditor数量 17

srcAuditor数量 11

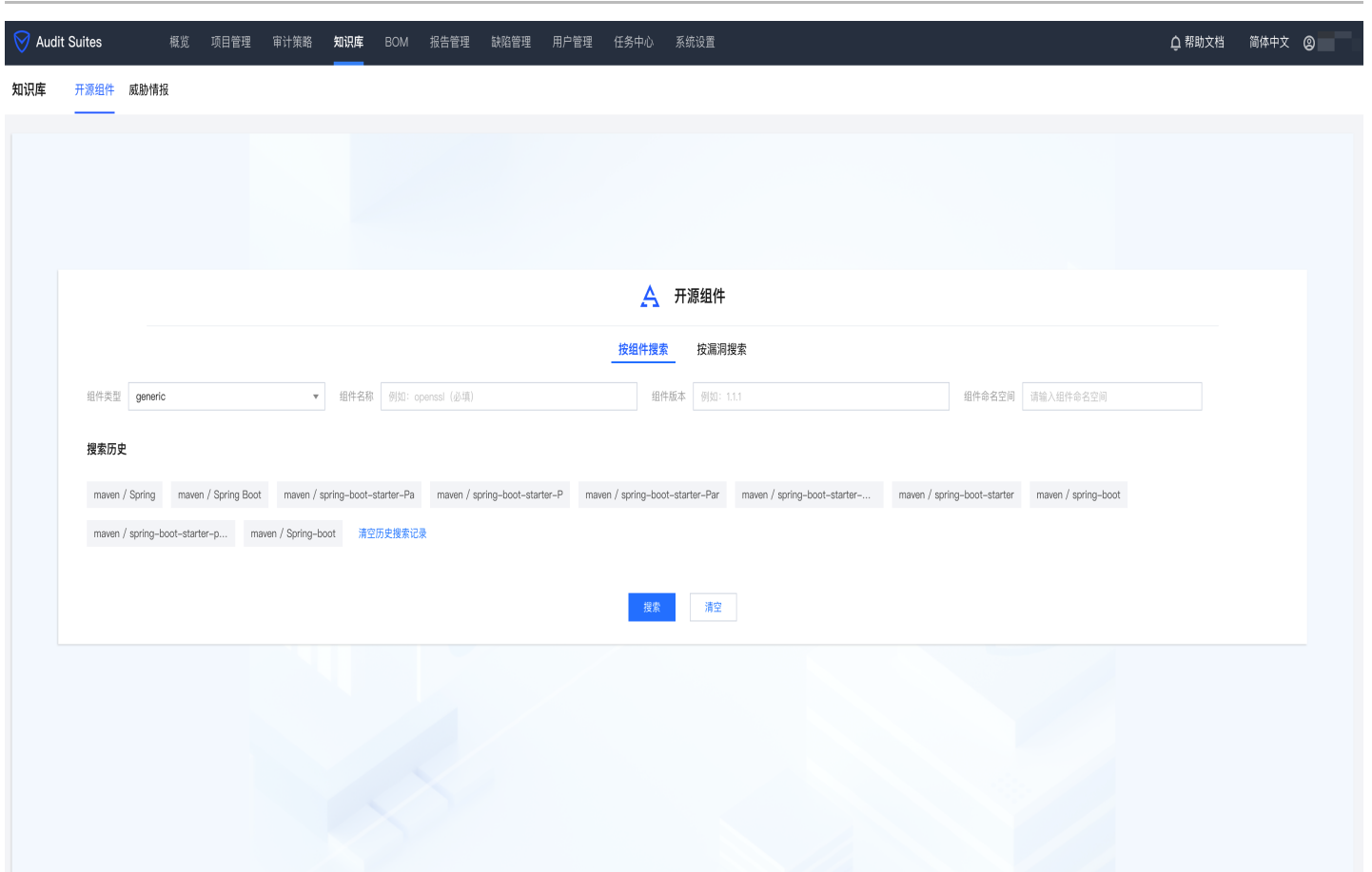
新建策略

策略名称 ↓	策略备注	分析类型 T	关联分析数量	更新时间 ↑	操作
黑名单-特定组件的gpl-2.0		srcAuditor	1	2024-03-11 13:55	设为默认 修改策略 复制 删除
黑名单-去除低license		srcAuditor	1	2024-03-11 13:54	设为默认 修改策略 复制 删除
黑名单 去除apache 2.0		srcAuditor	1	2024-03-11 13:53	设为默认 修改策略 复制 删除
风险等级		binAuditor	0	2023-07-21 20:26	设为默认 修改策略 复制 删除
综合测试-0(1)	各种case	binAuditor	0	2023-02-14 11:55	设为默认 修改策略 复制 删除
综合测试-0	各种case	binAuditor	1	2023-02-15 14:59	设为默认 修改策略 复制 删除
第三方组件规则		binAuditor	4	2022-09-20 16:42	设为默认 修改策略 复制 删除
空		sysAuditor	0	2022-01-21 14:46	设为默认 修改策略 复制 删除
白名单 高中license		srcAuditor	1	2024-03-11 13:52	设为默认 修改策略 复制 删除
白名单 gpl2.0		srcAuditor	1	2024-03-11 13:52	设为默认 修改策略 复制 删除
测试GPL-2.0		binAuditor	1	2022-11-28 13:43	设为默认 修改策略 复制 删除
应急漏洞		binAuditor	1	2023-04-28 15:54	设为默认 修改策略 复制 删除

1.5 开源组件知识库

在开源组件知识库（KnowledgeBase）页面可以查询组件和漏洞相关信息。

- 按组件搜索：根据组件类别、组件名称、组件版本、组件命名空间查询组件详情。
- 按漏洞搜索：根据漏洞ID查询漏洞详情，支持pcmgr ID和CVE ID，如pcmgr-105847，CVE-2018-1000500。



1.6 BOM

在 **BOM > SBOM (Software Bill of Materials)** 页面，可以查看团队下所有分析报告中的组件信息。

- 支持单击**查看组件详情**，查看组件及其关联分析，从而帮助团队确认软件是否受到某些已知风险组件的影响。
- 支持查看组件在知识库中的最新状态，如果最新状态相比分析结果有所更新，则会给出相应的提示，例如“漏洞更新”和“License 更新”，从而展示当前最新的风险情况。

Audit Suites
概览
项目管理
审计策略
知识库
BOM
报告管理
缺陷管理
用户管理
任务中心
系统设置
帮助文档
简体中文

BOM
SBOM
Services

sysAuditor Team = 切换团队

请输入关键词 Q

组件名	组件类型	组件命名空间	分析报告	状态	关注	操作
Flask	pypi		2	漏洞更新 License更新	☆	查看组件详情
Jinja2	pypi		2	漏洞更新 License更新	☆	查看组件详情
Pygments	pypi		2	漏洞更新 License更新	☆	查看组件详情
Werkzeug	pypi		2	漏洞更新 License更新	☆	查看组件详情
apk-tools	apk	alpine	17	漏洞更新 License更新	☆	查看组件详情
apollo-core	maven	com.ctrip.framework.apollo	1	漏洞更新 License更新	☆	查看组件详情
bash	generic		23	漏洞更新 License更新	☆	查看组件详情
cors	npm	@koa	7	漏洞更新 License更新	☆	查看组件详情
cryptography	pypi		9	漏洞更新 License更新	☆	查看组件详情
dbus	generic	git/dbus	18	漏洞更新 License更新	☆	查看组件详情
electron	npm		4	漏洞更新 License更新	☆	查看组件详情
fastjson	maven	com.alibaba	23	漏洞更新 License更新	☆	查看组件详情

1.7 报告管理

在报告管理页面，可以查看当前用户有权限的分析报告列表，除在线查看报告外，支持导出 PDF、Excel、CSV 报告。更多详情请参见 [查看报告](#)。

报告管理

Q

报告名称	所属团队	所属项目	分析类型	报告创建时间	操作
Source SCA	sysAuditor Team	Demo	srcAuditor SCA	2024-03-21 01:47	查看报告 导出报告
RaspI	sysAuditor Team	Demo	sysAuditor Linux	2024-03-21 01:47	查看报告 导出报告
1.0	sysAuditor Team	Demo	sysAuditor Linux	2024-03-21 01:46	查看报告 导出报告
APK	sysAuditor Team	Demo	apkAuditor APK	2024-03-21 01:41	查看报告 导出报告
trivy/vul dup	sysAuditor Team	Demo	srcAuditor Integration	2024-03-21 01:35	查看报告 导出报告
Firmware	sysAuditor Team	Demo	binAuditor Package	2024-03-18 13:58	查看报告 导出报告
Android 8	sysAuditor Team	Demo	sysAuditor Android 8	2024-03-08 12:50	查看报告 导出报告
python	sysAuditor Team	Demo	binAuditor Docker	2024-02-19 16:55	查看报告 导出报告
Alpine	sysAuditor Team	Demo	binAuditor Docker	2024-02-05 16:00	查看报告 导出报告
RTOS	sysAuditor Team	Demo	binAuditor RTOS	2024-02-05 15:57	查看报告 导出报告
cyclonedx-json	sysAuditor Team	Demo	srcAuditor Integration	2024-02-05 15:56	查看报告 导出报告
dependency-check	sysAuditor Team	Demo	srcAuditor Integration	2024-02-05 15:56	查看报告 导出报告
synopsys-detect	sysAuditor Team	Demo	srcAuditor Integration	2024-02-05 15:56	查看报告 导出报告
spdx	sysAuditor Team	Demo	srcAuditor Integration	2024-02-05 15:56	查看报告 导出报告
Kernel	sysAuditor Team	Demo	binAuditor Package	2024-02-05 15:56	查看报告 导出报告

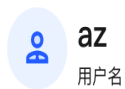
1.8 个人中心

个人资料

1. 在概览页面，单击右上角头像，选择个人资料。
2. 在个人资料页面，支持查看个人信息，单击修改密码。

个人中心 个人资料 令牌管理

基础信息



团队信息

团队名称	团队角色
12333	Member

3. 在修改密码页面，输入新旧密码，单击提交。

修改密码

当前密码 *

新密码 *

重复密码 *

令牌管理

API 令牌可用于 API 调用场景，如通过 API 接口的方式实现1.自动化创建-2.执行-3.查看分析项的场景。

1. 在概览页面，单击右上角头像，选择个人资料。
2. 在个人资料页面，单击令牌管理。
3. 在令牌管理页面，单击新建，输入令牌备注。

创建令牌 ✕

用户名

令牌备注

创建
取消

4. 单击**创建**，即可生成所需令牌。

创建令牌 ✕

令牌 ✔

已复制到剪切版. 请妥善保管令牌

5. 在令牌管理页面，可查看 API 令牌，单击**删除**，经过二次确认后，可删除该令牌。

个人中心 [个人资料](#) [令牌管理](#)

新建
删除

令牌	创建时间	令牌备注	操作
<input type="checkbox"/> eyJ*****23o	2023-12-18 19:18	demo	删除

共 1 条 50 条 / 页 1 / 1 页