绿盟威胁和漏洞管理平台

用户手册

NSFOCUS

https://www.nsfocus.com.cn

版本： V3.0R01F02 (2023-02-17)　　密级： 限制分发级

■ 版权声明

■ 内容声明

您购买的产品、服务或特性等受合同和条款的约束，本文档中描述的部分功能可能不在您的购买或使用范围之内。

本文档仅作为使用指导，实际产品可能会由于版本升级或其他原因，与文档描述有略微差异。

■ 免责声明

在使用产品之前，请详细阅读免责声明，一旦开始使用，即认可和接受本声明的全部内容。在使用过程中，绿盟科技不对以下情况承担任何责任：

- 因系统运维或管理人员未及时处理影响系统稳定性和可用性的告警，而造成的数据损失、系统可用性降低等情况。
- 因业务量超过所规划硬件能力而造成的数据损失、系统可用性降低等情况。
- 因自然灾害（包含但不限于水灾、火灾、地震等）或外部原因（包含但不限于断网、断电等）而造成的数据损失、系统可用性降低或不可用等情况。

■ 格式约定

- **粗体字**：菜单、命令和关键字
- *斜体字*：文档名、变量
-  **说明**：对描述内容的补充和引用信息
-  **提示**：使用设备时的技巧和建议
-  **注意**：需要特别注意的事项和重要信息
-  **警告**：有可能造成人身伤害的警告信息

目录

前言 1
内容简介 1
修订历史 1
获得帮助 2
1 概述 3
1.1 TVM 简介 3
1.2 Web 管理 4
2 典型场景 6
2.1 漏洞管理 6
2.2 资产稽查 7
2.3 脆弱性分析 8
2.4 大屏监控 8
2.5 安全运营 8
3 全景感知 9
3.1 仪表盘 9
3.2 主机态势 11
3.3 网站态势 12
4 资产管理 13
4.1 资产列表 13
4.1.1 新建子组 13
4.1.2 新建主机资产 14
4.1.3 新建网站资产 17
4.1.4 其他操作 19
4.2 资产监控 22
4.3 资产配置 23
4.3.1 属性管理 23
4.3.2 类型管理 24
4.3.3 标签管理 24
4.3.4 异常资产配置 24
4.3.5 重复资产配置 25

5 漏洞管理.....26
5.1 漏洞处置.....26
5.1.1 处置列表.....26
5.1.2 漏洞视角/端口视角/服务视角.....31
5.1.3 漏洞归并修复建议.....32
5.2 漏洞归档.....32
5.3 漏洞配置.....32
6 扫描管理.....34
6.1 新建扫描任务.....34
6.2 扫描任务管理.....34
6.2.1 新建任务.....34
6.2.2 任务管理.....49
6.3 批量任务管理.....51
6.4 扫描设备管理.....51
6.4.1 设备管理.....51
6.4.2 引擎实例.....55
6.5 任务配置.....55
7 流程处置.....57
7.1 工单管理.....57
7.2 流程管理.....60
7.3 通知策略.....62
8 报表管理.....64
8.1 统计分析.....64
8.1.1 任务对比.....64
8.1.2 分组统计.....65
8.1.3 时间维度对比.....66
8.2 报表任务.....67
8.3 报表配置.....68
9 知识建设.....69
9.1 知识概览.....69
9.2 知识库.....70
9.2.1 产品漏洞库.....70
9.2.2 口令字典库.....72
9.2.3 配置模板.....72
9.2.4 情报管理.....73
9.2.5 漏洞指纹插件库.....77
9.2.6 资产标记库.....78
9.2.7 知识库升级.....81

9.3 模板管理 81
9.3.1 产品漏洞模板 81
9.3.2 口令字典模板 82
9.3.3 资产探测模板 84
9.4 运营经验库 84
9.4.1 修复方案库 84
9.4.2 漏洞误报库 85
9.5 知识配置 85
10 系统配置 87
10.1 主题配置 87
10.2 安全防护 88
10.3 数据外发 88
10.4 二次接口 90
10.5 工具管理 90
A 出厂设置 91
B 支持的设备及版本 92
C 安全等级保护 93

前言

本文主要介绍绿盟威胁和漏洞安全管理平台（NSFOCUS Threat and Vulnerability Security Management Platform，以下简称 TVM）的 Web 管理界面的各模块的功能点及使用方法。

本手册仅作为使用指导，实际产品可能会由于版本升级或其他原因，与手册描述有略微差异。

内容简介

章节	概述
1 概述	介绍 TVM 的产品特点和 Web 管理。
2 典型场景	介绍常见的 TVM 的使用场景。
3 全景感知	介绍如何查看各类综合统计数据。
4 资产管理	介绍如何管理资产。
5 漏洞管理	介绍如何管理和处置漏洞。
6 扫描管理	介绍如何管理各类扫描任务。
7 流程处置	介绍如何管理工单。
8 报表管理	介绍如何查看各类报表。
9 知识建设	介绍如何管理知识库。
10 系统配置	介绍如何维护 TVM、用户帐号等。
A 出厂设置	介绍 TVM 的出厂默认配置。
B 支持的设备及版本	介绍 TVM 可以管理的安全设备及其版本。
C 安全等级保护	介绍国家等保级别的前四级。

修订历史

版本	说明
V3.0R01F02	首次发布。

获得帮助

文档意见反馈

可以通过以下方式反馈在文档使用过程中遇到的任何问题和对文档的建议和意见。

邮箱：info-support@nsfocus.com

软件升级

用户在了解安全设备的基础操作后，可以帮助用户自助进行安全设备的升级操作。

网站：http://update.nsfocus.com/

售后服务

提供全国范围内的服务热线，可以帮助用户解决在使用安全设备和服务过程中遇到的各种问题和困难。

- 服务热线

  网站：https://www.nsfocus.com.cn/html/6/61/169/

业务类型	支持热线	E-mail	服务时间
安全产品与平台售后服务	400-818-6868 转接 0 13321167330	support@nsfocus.com	周一至周日 7×24 小时全天服务
云安全服务	400-818-6868 转接 2	rs@nsfocus.com	
购买咨询	400-818-6868 转接 1	csc@nsfocus.com	

- 盟管家服务
  - 网站：https://user.nsfocus.com/hm_es/nsfocus/nsfocus_c/index.html
  - 微信公众号：搜索并关注“绿盟科技技术服务”，单击“盟管家”
  - 二维码：

1 概述

本章主要包含以下内容：

功能	描述
TVM 简介	介绍 TVM 的功能。
Web 管理	介绍如何通过 Web 端访问 TVM。

1.1 TVM 简介

近两年，漏洞的披露和漏洞的利用方式逐步发生了改变，借助各大社区、社交平台，漏洞的传播速度惊人，上午披露漏洞，下午可能出现利用代码，晚上可能已经发生很多攻击。

安全厂商已经开始积极应对这种变化，领先的厂商已经建立了完善的系统的安全情报体系，并且已经打通厂商和用户通道，帮助用户建立安全漏洞的应急响应机制，第一时间知道漏洞爆发，随着漏洞出现时间跟踪漏洞的利用过程，随时调整漏洞的响应级别。

针对现在安全漏洞在互联网传播迅速、被利用时间短、对网络爆发式影响的特点，结合多年的安全研究和服务经验，绿盟科技提出了绿盟威胁和漏洞管理（TVM）方案。

绿盟科技认为，对互联网中安全漏洞威胁的跟踪应该作为漏洞管理的一个重要环节，而只有安全厂商才有跟踪到这些威胁情报的能力，安全厂商应该积极参与到用户的漏洞管理流程中。

绿盟科技 TVM 提出：

- 威胁是外部因素，新漏洞的披露，漏洞是否被关注，是否已经存在利用该漏洞的攻击代码，是否被用于恶意软件进行传播，这些因素表明了漏洞的外部威胁的强弱。
- 漏洞是内部因素，是在具体网络资产上客观存在的。漏洞的利用难度、利用方式、被利用的后果，资产和资产上数据的重要性，以及安全防护是否到位，这些因素表明了网络自身的健壮程度。
- 通过适合的管理流程，把内外部安全因素统一度量、分析和管理，才能有效应对目前安全漏洞的变化趋势。

1.2 Web 管理

Web 管理为管理员提供了直观的人机交互方式，管理员通过 Web 管理页面可以直接对系统进行管理和配置。

支持的浏览器

浏览器	版本	其他要求
Firefox	最新版本	• 请检查浏览器是否设置了禁止弹出窗口属性或者禁止 javascript；如果是，请撤销此设置。 • 取消增强保护模式。
Chrome	最新版本	

推荐屏幕分辨率

屏幕分辨率最好设置为 1280*1024 及以上。

Web 登录

登录 Web 管理页面之前，需要保证网络连接正常。

打开浏览器，使用 HTTPS 方式访问管理口的 IP 地址（例 https://192.168.1.1）；接受正常风险后，进入 Web 登录页面；输入已启用的用户名和密码，单击【登录】按钮即可。

- 初始用户名和密码、浏览器和屏幕分辨率要求请参见 出厂设置。
- 初次登录时，需要配置新的密码后重新登录。

Web 页面布局

各功能模块的页面布局相同，示例如图 1-1 所示。

说明	页面布局中的菜单和工作区会因用户权限的不同而不同，具体情况请以页面展示为准。

图1-1 页面布局

编号	区域	描述
1	菜单栏/导航栏	• TVM 的一级功能菜单栏。将鼠标悬停在菜单上，出现对应的二级和三级功能菜单。 • 单击展示 TVM 的全部菜单导航，单击直接进入对应的页面。当前所在页面的菜单名，在导航栏中显示为绿色。
2	BSA 通用菜单/快捷工具栏	绿盟大数据安全平台（简称 BSA），从左至右的具体说明如下： • ：选择并进入具体的解决方案。 • ：管理系统告警信息。红色数字表示当前的告警信息数量。 • ：查看关于信息和在线帮助。 • ：返回当前系统的首页。 • ：BSA 的通用菜单栏。具体功能说明请查阅 BSA 产品手册。 • ：当前用户退出系统。
3	工作区	各类功能的配置、操作、浏览都在此区域进行。

2 典型场景

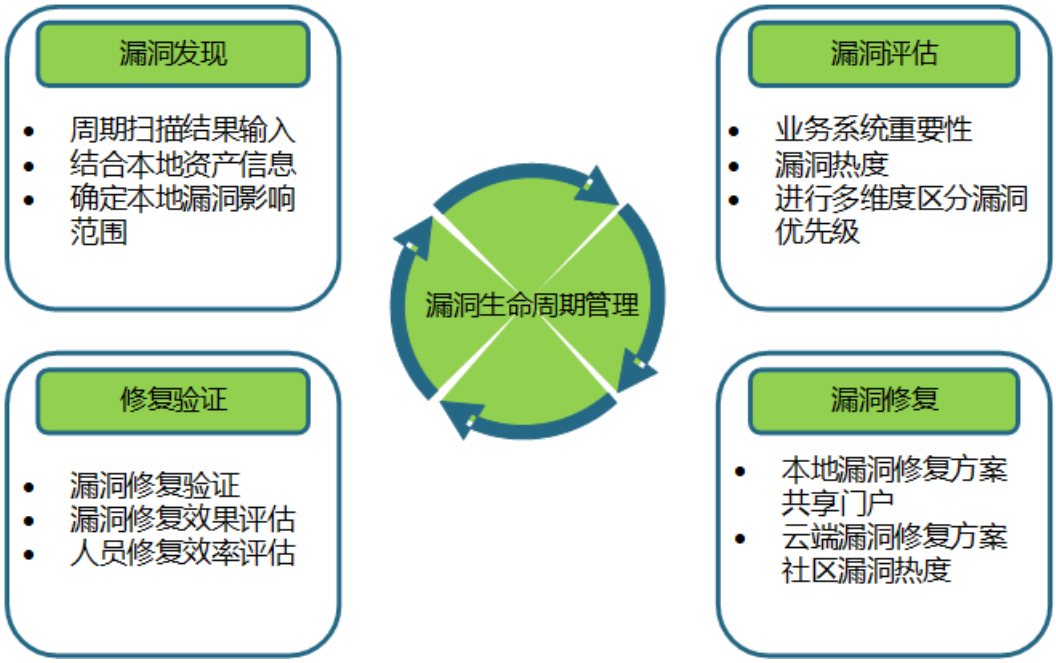
本章主要包含以下内容：

功能	描述
漏洞管理	介绍漏洞管理场景及使用流程。
资产稽查	介绍资产稽查场景及使用流程。
脆弱性分析	介绍脆弱性分析场景及使用流程。
大屏监控	介绍大屏监控场景及使用流程。
安全运营	介绍安全运营场景。

2.1 漏洞管理

漏洞管理能够全方位检测 IT 系统存在的漏洞，发现信息系统存在的漏洞和 Web 安全事件等。通过对安全漏洞全生命周期的过程监控，可以快速发现问题，并对安全加固过程全程跟踪，最终形成整体安全风险报告，如图 2-1 所示。

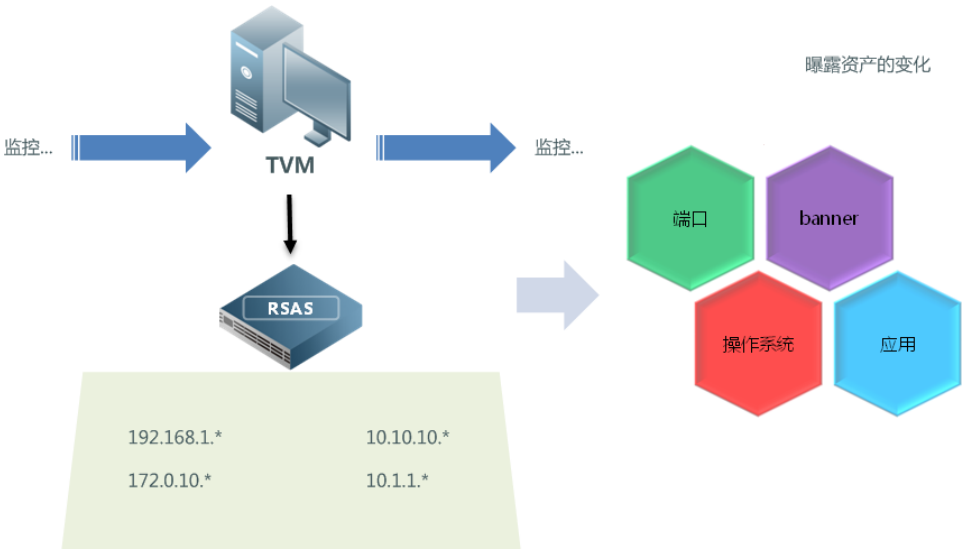
图2-1 漏洞管理场景



2.2 资产稽查

基于 TVM 可以建立资产库，通过持续监控的手段，可以实时了解资产的变化情况，从而实现对新增资产和变更资产的有效稽查，如图 2-2 所示。

图2-2 资产稽查场景



2.3 脆弱性分析

为了对资产进行实时或者定期的脆弱性识别，TVM 利用威胁情报、漏洞扫描、网站监测、人工渗透、第三方扫描数据和配置核查等收集资产的脆弱性信息，通过周期性趋势对比和分析、态势呈现和总体分值等可视化技术直观展现资产的脆弱性情况。

脆弱性分析场景如图 2-3 所示。

图2-3 脆弱性分析场景

2.4 大屏监控

大屏监控是将收集到的各种安全数据，利用大数据技术结合威胁情报进行集中处理、关联分析，再利用可视化技术，将各种安全事件进行可视化呈现，为安全运营提供可靠的信息数据支撑。

大屏监控既可以对全网的安全态势进行呈现；又可以覆盖各种安全运营场景，从系统漏洞、网站安全进行安全态势感知。

2.5 安全运营

TVM 能够统一管理安全组织、安全策略、安全技术、安全风险、安全事件、安全操作等，并能够保证其有效（Effective and Efficiency）运转（Operations）。

TVM 提供综合管理与安全运营的能力，而不仅仅是一个综合的安全设备管理技术或管理工具。

安全运营涵盖了上述所有场景，在完成上述使用流程后，可以查看当前网络的脆弱性情况。

3 全景感知

本章主要包含以下内容：

功能	描述
仪表盘	介绍如何查看当前的统计数据。
主机态势	介绍如何查看主机漏洞的统计数据。
网站态势	介绍如何查看 Web 漏洞的统计数据。

3.1 仪表盘

进入 **全景感知 > 仪表盘** 页面，可以查看知识库、工单、资产、漏洞和扫描任务等统计数据。页面展示内容说明如图 3-1 和表 3-1 所示。

图3-1 仪表盘

表3-1 仪表盘

展示项	描述
主机漏洞总数/网站漏洞总数	• 展示当前发现的主机漏洞总数/网站漏洞总数。 • 展示今日新增主机漏洞总数/网站漏洞总数。 • 展示当前发现的各风险等级的主机漏洞总数/网站漏洞总数。 • 单击漏洞数据，进入 产品漏洞库 页面，可以对筛选后的漏洞进行管理。
风险资产数/资产总数	• 展示当前的风险资产总数/资产总数。 • 展示当前的风险主机资产总数/主机资产总数。 • 展示当前的风险网站资产总数/网站资产总数。 • 单击资产数据，进入 资产列表 页面，可以对筛选后的资产进行管理。
扫描任务数	• 展示当前不同执行状态的扫描任务数。 • 单击扫描任务数据，进入 扫描任务管理 页面，可以对筛选后的扫描任务进行管理。
工单待办/我的申请	• 展示当前我的待办工单总数/我申请的工单总数。 • 展示今日新增我的待办工单总数/我申请的工单总数。 • 展示当前不同状态工单的数量。 • 单击工单数据，进入 工单管理 页面，可以对筛选后的工单进行管理。
漏洞统计	• 展示当前不同处置状态的漏洞数量。 • 单击漏洞数据，进入 漏洞处置 页面，可以对筛选后的漏洞进行管理。
分组风险 TOP	• 以柱状图方式展示当前风险值最高的 TOP5/10 资产子组的风险情况。 • 将鼠标悬停在图中，可以查看对应子组的风险值。
整体风险值趋势(周)	• 以柱状图方式展示近一周内所有资产的风险情况。 • 将鼠标悬停在图中，可以查看对应时间的风险值。
风险统计	• 展示各风险等级的资产数量。 • 单击资产数据，进入 资产列表 页面，可以对筛选后的资产进行管理。
资产脆弱性	• 以列表方式展示当前脆弱性值最高的 TOP5/10 资产的情况。 • 支持脆弱性值、漏洞数、配置符合度和弱口令数的排序展示。 • 单击资产名称，进入 资产列表 页面，可以对筛选后的资产进行管理。 • 单击【查看全部】，进入 资产列表 页面，可以对所有资产进行管理。
工单待办	• 以列表方式展示指派给当前登录用户优先级最高的 5 个待办工单。 • 单击【查看全部】，进入 工单管理 页面，可以对筛选工单进行管理。
扫描统计	展示当前扫描设备的不可用设备数、可用设备数、在线设备数和其他设备数。
资产发现统计	• 展示当前各资产发现状态资产的数量。 • 单击图例可以取消/显示对应状态在图中的统计。 • 将鼠标悬停在图中，可以查看对应状态的具体数据。
知识库统计	• 展示当前各知识库的知识数量。 • 单击知识库数据，进入对应 知识库 页面，可以对筛选后的知识进行管理。

3.2 主机态势

进入 **全景感知 > 主机态势** 页面，可以查看的内容如图 3-2 和表 3-2 所示。单击图例可以取消/显示对应类别在图中的统计。将鼠标悬停在图中，可以查看对应类别的具体数据。

图3-2 主机态势

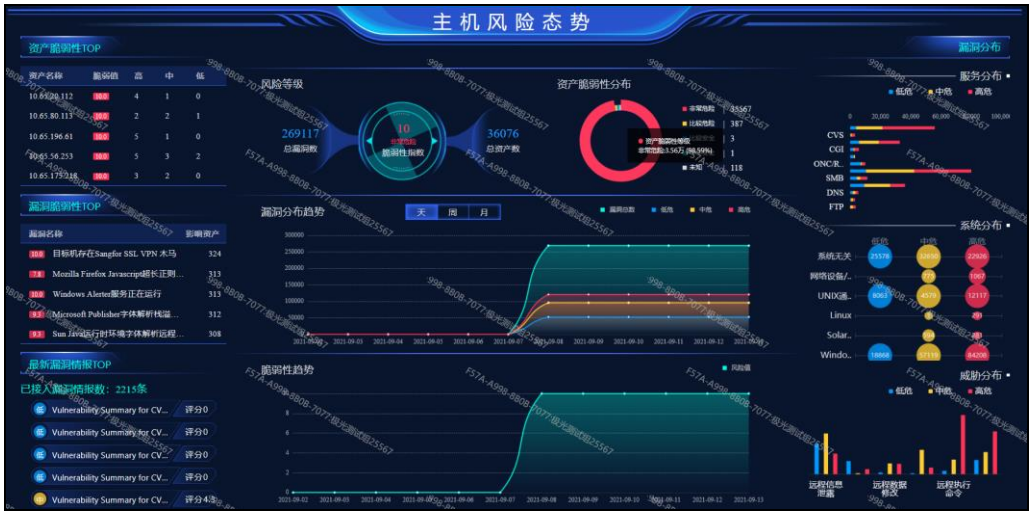


表3-2 主机态势

区域名称	描述
风险等级	通过统计、分析网络中的主机资产总数、存在的漏洞总数，给出主机资产的脆弱性指数和风险等级评分。
资产脆弱性分布	以饼图方式展示主机资产中存在的漏洞等级分布。
漏洞分布趋势	按天/周/月展示最近 12 天/周/月里主机资产中的各个威胁等级的漏洞分布趋势。
脆弱性趋势	按天/周/月展示最近 12 天/周/月里主机资产的脆弱性趋势。
资产脆弱性 TOP	按脆弱值由高至低，以列表方式展示 TOP 的脆弱主机资产，脆弱主机资产信息包括：资产名称、脆弱值、高/中/低漏洞数目。
漏洞脆弱性 TOP	以列表方式展示对主机资产的脆弱性影响最大的漏洞 TOP。
最新漏洞情报 TOP	以列表方式展示主机资产中已接入的落地情报数、最新漏洞 TOP。
漏洞分布-服务分布	以柱状图方式展示高/中/低危漏洞在服务中的数量分布。
漏洞分布-系统分布	以柱状图方式展示高/中/低危漏洞在操作系统中的数量分布。
漏洞分布-威胁分布	以柱状图方式展示高/中/低危漏洞在漏洞威胁方式中的数量分布。

3.3 网站态势

进入 **全景感知 > 网站态势** 页面，可以查看的内容如图 3-3 和表 3-3 所示。

图3-3 网站态势

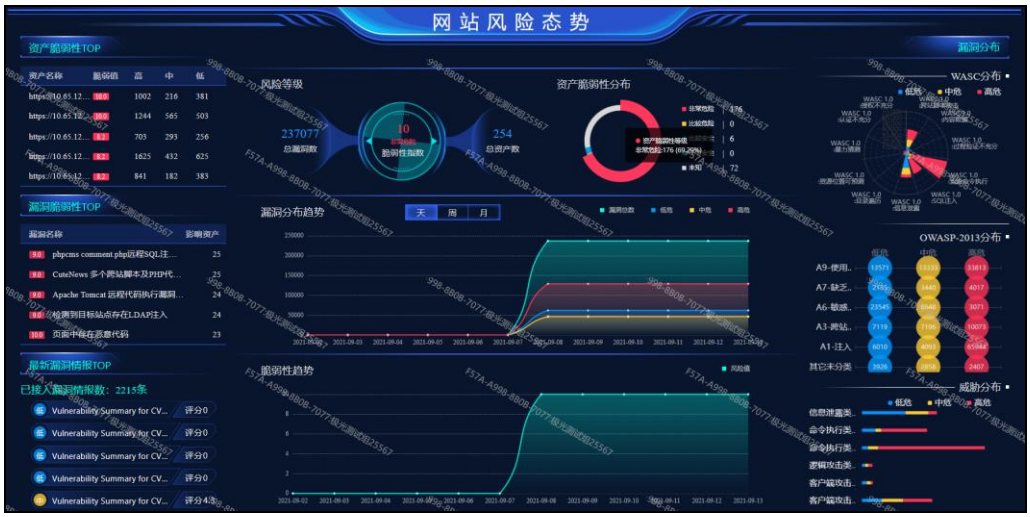


表3-3 网站态势

区域名称	描述
风险等级	通过统计、分析网络中的网站资产总数、存在的漏洞总数，给出网站资产的脆弱性指数和风险等级评分。
资产脆弱性分布	以饼图方式展示网站资产中存在的漏洞等级分布。
漏洞分布趋势	按天/周/月展示最近 12 天/周/月里网站资产中的各个威胁等级的漏洞分布趋势。
脆弱性趋势	按天/周/月展示最近 12 天/周/月里网站资产的脆弱性趋势。
资产脆弱性 TOP	按脆弱值由高至低，以列表方式展示 TOP 的脆弱网站资产，脆弱网站资产信息包括：资产名称、脆弱值、高/中/低漏洞数目。
漏洞脆弱性 TOP	以列表方式展示对网站资产的脆弱性影响最大的漏洞 TOP。
最新漏洞情报 TOP	以列表方式展示网站资产中已接入的落地情报数、最新漏洞 TOP。
漏洞分布-WASC 分布	展示漏洞在标准分类中的分布情况。
漏洞分布-OWASP-2013 分布	展示漏洞在 OWASP（2013）标准分类中的分布情况。
漏洞分布-威胁分布	以柱状图方式展示高/中/低危漏洞在漏洞威胁方式中的数量分布。

4 资产管理

具有 资产配置 权限的帐号才可以进行资产的属性管理；具有资产管理权限的帐号才可以进行资产操作。

本章主要包含以下内容：

功能	描述
资产列表	介绍如何管理资产。
资产监控	介绍如何管理发现的资产。
资产配置	介绍如何管理资产的公共属性。

4.1 资产列表

TVM 可以管理所有已经入库的正式资产。

- TVM 管理的资产数量受证书控制，最多可管理 100 万个，即手动添加资产、手动导入资产和自动发现资产的总数不允许超过 100 万个。
- 若待添加资产数量超过 100 万个，TVM 将提示用户超过上限。

4.1.1 新建子组

在每个视图下，可以新建子组，方便用户进行分组管理资产。

进入 **资产管理 > 资产列表** 页面，切换视图、单击左树中视图名称旁的，配置子组参数即可。子组参数如表 4-1 所示。

表4-1 子组参数

配置项	描述
节点名称	子组的名称，取值范围为 1~30 个字符。 不允许包含特殊字符，特殊字符的范围请以界面展示为准。
是否隐藏	隐藏后，该子组仅对其所有人可见，对其他帐号不可见。
联系人	子组的联系人，取值范围为 0~30 个字符。

配置项	描述
	不允许包含特殊字符，特殊字符的范围请以界面展示为准。
联系人邮箱	子组联系人的 Email 地址，只能填写 1 个邮箱，取值范围 0~64 个字符。 配置邮箱前，请先配置邮件服务器，有关邮件配置的详细介绍，请参见 BSA 用户手册中的邮件配置。
联系人手机号	子组联系人的手机号码，只能填写 1 个手机号码。
地理位置	选择子组所在的地理位置。 从下拉列表中选择，选项数据来源于新建的地理视图子组。
经纬度	子组所在的经度和纬度。
价值	子组的重要性。
描述	子组的说明信息。
自动入库范围配置	主要用于资产发现自动入库时的 IP 匹配，对本组内资产无强制性约束。入库时，当资产 IP 匹配到多个资产组、且匹配到资产组存在父子关系时，TVM 根据 入库配置，将资产发现结果入库在最外层“父资产组”或最内层“子资产组”。
选择设备	该资产组绑定的扫描设备。 设备可扫描 IP 范围的配置请参见 管理设备。

4.1.2 新建主机资产

单个新增

进入 **资产管理 > 资产列表** 页面，单击左树中视图名称旁的 ＋ **> 主机资产**，默认进入“单个新增”页面，配置主机资产参数即可。单个新增资产时配置的参数如表 4-2、表 4-3、表 4-4 和表 4-5 所示。

表4-2 单个主机资产基本信息

配置项		描述
基础属性	IP 必填项	选择主机资产 IP 地址的类型。
	IPv4/IPv6/IPv4&IPv6	根据“IP 必填项”，配置资产的 IPv4/IPv6 地址。
	资产名称	资产的名称，取值范围为 1~30 个字符。 不允许包含特殊字符，特殊字符的范围请以界面展示为准。
	资产组	资产所属的资产组。 从下拉列表中选择，选项数据来源于资产组。
高级属性	资产重要性	资产的重要性。
	等保级别	资产的等保级别。
	资产标签	资产关联的标签，可以根据需要【添加标签】。
	地理位置	选择资产所在的地理位置。

配置项		描述
		从下拉列表中选择，选项数据来源于新建的地理视图子组。
	经纬度	资产所在的经度和纬度。
	MAC 地址	资产的 MAC 地址。 最多支持输入 10 组不重复的 Mac 地址，多个 MAC 地址间使用英文逗号、分号、空格或者回车分隔。
	资产描述	资产的说明信息。
自定义属性（可在中 属性管理 进行管理）	业务视图	资产所属的业务系统。 从下拉列表中选择，选项数据来源于新建的业务视图子组。
	组织架构	资产所在的组织。 从下拉列表中选择，选项数据来源于新建的组织架构子组。
	行业	资产所属的行业。 从下拉列表中选择，选项数据来源于新建的行业子组。
	资产防护情况	对资产的防护情况。 从下拉列表中选择，选项数据来源于新建的资产防护情况子组。
	资产位置	资产所属的网络位置情况，外网/专网/内网等。
	介质类型	资产的介质类型。
	自定义视图属性	资产所属的自定义视图属性。
联系人信息	联系人	资产的联系人，取值范围为 0~30 个字符。 不允许包含特殊字符，特殊字符的范围请以界面展示为准。
	联系人手机	资产联系人的手机号码，只能填写 1 个手机号码。
	联系人邮箱	资产联系人的 Email 地址，只能填写 1 个邮箱，取值范围 0~64 个字符。 配置邮箱前，请先配置邮件服务器，有关邮件配置的详细介绍，请参见 BSA 用户手册中的邮件配置。

表4-3 单个主机资产主机信息

配置项		描述
系统信息	操作系统	资产的操作系统类型。
	操作系统版本	资产的操作系统版本。
设备信息	设备类型	资产所属的设备类型。取值从设备类型属性选择。
	设备厂商	资产所属的厂商。取值范围为最多 30 个字数。
	设备型号	资产的型号。取值范围为最多 30 个字数。
登录信息	登录 IP 地址	资产的登录 IP 地址。
	登录协议/登录端口	资产的登录协议/登录端口。

配置项		描述
	主机认证方式	资产的登录认证方式。
	登录帐号/登录密码	资产的登录帐号/登录密码。
跳板机登录信息	跳板机 IP 地址	跳转机的 IP 地址。 在 TVM 不能直接登录目标主机时，可以使用跳转主机进行扫描，需要保证跳转主机能够连接到目标主机。
	跳板机免密登录	是否通过用户名和密码登录。
	跳板机登录端口	TVM 登录跳板机的登录端口。
	跳板机登录账号/跳板机登录密码	TVM 登录跳板机的登录用户名和密码。
关联地址	地址	资产的域名信息。 单击【添加地址】添加，内容不允许为空。

表4-4 单个主机资产服务信息

配置项	描述
端口号	取值范围为 1~65535 的整数。
协议	端口运行的协议类型。
服务名称	由英文字母、数字或-字符组成，区分大小写。取值范围为最多 30 个字数。
更新时间	选择服务的更新时间。
备注（banner）	服务的备注信息。取值范围为为最多 1 万个字数。
【添加服务信息】	将服务信息添加到页面下方服务信息列表中。服务信息支持删除。

表4-5 单个主机资产应用信息

配置项	描述
应用名称	资产中应用的名称。
应用版本	应用的版本信息。
厂商	应用所属的厂商。
备注	应用的备注信息。取值范围为最多 1 万个字数。
【添加应用信息】	将应用信息添加到页面下方应用信息列表中。应用信息支持删除。

批量新增

批量新增只能添加 IPv4 资产的基本信息，无法设置主机信息、服务信息和应用信息。

进入 **资产管理 > 资产列表** 页面，单击左树中视图名称旁的 ＋ **> 主机资产**，单击【批量新增】按钮，配置主机资产参数即可。批量新增资产时配置的参数如表 4-6 所示。

表4-6 批量主机资产基本信息

配置项		描述
基本属性	IPv4 范围	主机资产的 IPv4 地址范围。IPv4 支持的格式：192.168.1.1、192.168.1.1/24 或 192.168.1.1-192.168.1.100 的 IPv4 网段。
	资产组	资产所属的资产组。 从下拉列表中选择，选项数据来源于资产组。
高级属性	资产重要性	资产的重要性。
	等保级别	资产的等保级别。
	资产标签	资产关联的标签，可以根据需要【添加标签】。
	地理位置	选择资产所在的地理位置。 从下拉列表中选择，选项数据来源于新建的地理视图子组。
	经纬度	资产所在的经度和纬度。
	资产描述	资产的说明信息。
自定义属性	业务视图	资产所属的业务系统。 从下拉列表中选择，选项数据来源于新建的业务视图子组。
	组织架构	资产所在的组织。 从下拉列表中选择，选项数据来源于新建的组织架构子组。
	行业	资产所属的行业。 从下拉列表中选择，选项数据来源于新建的行业子组。
	介质类型	选择资产的介质类型。
联系人	联系人	资产的联系人，取值范围为 0~30 个字符。 不允许包含特殊字符，特殊字符的范围请以界面展示为准。
	联系人手机	资产联系人的手机号码，只能填写 1 个手机号码。
	联系人邮箱	资产联系人的 Email 地址，只能填写 1 个邮箱，取值范围 0~64 个字符。 配置邮箱前，请先配置邮件服务器，有关邮件配置的详细介绍，请参见 BSA 用户手册中的邮件配置。

4.1.3 新建网站资产

进入 **资产管理 > 资产列表** 页面，单击左树中视图名称旁的 ＋ **> 网站资产**，配置网站资产参数即可。网站资产参数如表 4-7、表 4-8 和表 4-9 所示。

表4-7 网站资产基本信息

配置项		描述
基础属性	URL	网站资产的 URL 域名。 URL 格式：协议://域名/路径。其中协议和域名必须小写，域名不可以 / 为开头，域名和路径不可以包含空字符，例 https://nsfocus.com,ftp://192.168.1.1，请勿输入超过 128 个字符。
	资产名称	资产的名称，取值范围为 1~30 个字符。 不允许包含特殊字符，特殊字符的范围请以界面展示为准。
	资产组	资产所属的资产组。 从下拉列表中选择，选项数据来源于资产组。
高级属性	资产重要性	资产的重要性。
	等保级别	资产的等保级别。
	资产标签	资产关联的标签，可以根据需要【添加标签】。
	地理位置	选择资产所在的地理位置。 从下拉列表中选择，选项数据来源于新建的地理视图子组。
	经纬度	资产所在的经度和纬度。
	资产描述	资产的说明信息。
自定义属性	业务视图	资产所属的业务系统。 从下拉列表中选择，选项数据来源于新建的业务视图子组。
	组织架构	资产所在的组织。 从下拉列表中选择，选项数据来源于新建的组织架构子组。
	行业	资产所属的行业。 从下拉列表中选择，选项数据来源于新建的行业子组。
联系人信息	联系人	资产的联系人，取值范围为 0~30 个字符。 不允许包含特殊字符，特殊字符的范围请以界面展示为准。
	联系人手机	资产联系人的手机号码，只能填写 1 个手机号码。
	联系人邮箱	资产联系人的 Email 地址，只能填写 1 个邮箱，取值范围 0~64 个字符。 配置邮箱前，请先配置邮件服务器，有关邮件配置的详细介绍，请参见 BSA 用户手册中的邮件配置。

表4-8 网站资产网站信息

配置项		描述
语言备案	开发语言	网站使用的开发语言。
	语言版本	开发语言的版本。
	ICP 备案	ICP 备案信息。取值范围为最多 1 万个字数。

配置项		描述
	服务器类型	资产所属的服务器类型。
	服务器版本	资产所属的服务器版本号。
登录信息	登录帐号/登录密码	资产的登录帐号/登录密码。
	登录 URL 地址	资产的登录 URL 地址。
子域名		资产的子域名信息。 单击【添加子域名】，内容不允许为空。
关联 IP		关联主机资产的 IP 地址。 单击【关联 IP】，内容不允许为空。

表4-9 网站资产网站组件

配置项	描述
服务名称	由英文字母、数字或-字符组成，区分大小写。取值范围为最多 30 个字数。
版本	网站组件的版本信息。
备注	网站组件的备注信息。
【添加服务信息】	将网站服务添加到页面下方网站服务列表中。网站服务支持删除。

4.1.4 其他操作

新建资产后，可以对已入库资产进行编辑、删除等操作；此外还可以根据需要导出/导入资产等其他操作。

导出资产

进入 **资产管理 > 资产列表** 页面，在资产列表页面中，勾选资产

- 普通导出：单击【导出】按钮，可以将勾选的资产导出至本地保存。
- 单击多格式批量导出：以 EXCEL 格式，批量导出资产信息至本地保存。

导入资产

TVM 平台支持通过资产文件导入资产

- 资产文件要求：支持导入扩展名为.xlsx 的资产文件，软件版本要求 WPS 2016 及以上、Office 2019 和 office 365。
- 批量导入资产时，TVM 允许的最大资产数为 100 万。

进入 **资产管理 > 资产列表** 页面；单击【导入】按钮，进入导入资产文件页面。【下载导入模板】后进行编辑，在虚线框区域，单击资产文件或将资产文件拖拽到该区域；配置入库策略即可。入库策略如表 4-10 所示。

表4-10 入库策略

资产状态	策略	描述
变更资产：以 IP 为唯一标识，文件中存在的资产，也在资产库中存在。	【覆盖】	以文件中的数据为准，覆盖资产库中相同资产的数据。
	【忽略】	保持现有资产库中的数据不变。
	【合并文件优先】	合并文件中与资产库中相同资产的数据，如有属性冲突，以文件中的数据为准。
	【合并资产库优先】	合并文件中与资产库中相同资产的数据，如有属性冲突，以资产库中的数据为准。
新增资产：以 IP 为唯一标识，文件中存在的资产，不在资产库中存在。	【插入】	以文件中的数据为准，在资产库中创建资产。
	【忽略】	保持现有资产库中的数据不变。
减少资产：以 IP 为唯一标识，文件中不存在的资产，在资产库中存在。	【忽略】	保持现有资产库中的数据不变。
	【删除】	以文件中的数据为准，删除资产库中的减少资产。

批量转移资产

进入 **资产管理 > 资产列表** 页面；在资产列表页面中，勾选资产，单击批量转移资产；配置“用户组”和“帐号”后，该帐号和当前帐号将同时拥有管理相应资产的权限。

查询资产

进入 **资产管理 > 资产列表** 页面，可以查询资产如图 4-1 和表 4-11 所示。

图4-1 查询资产

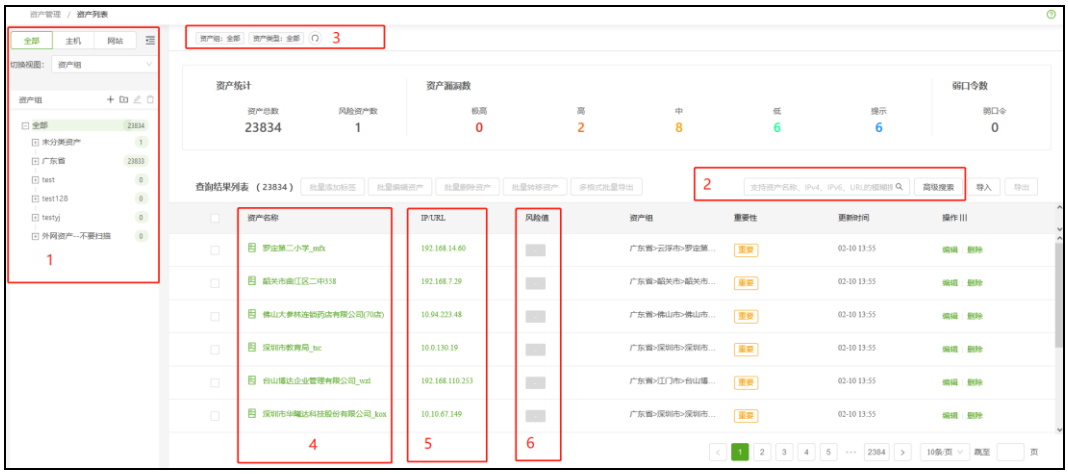


表4-11 查询资产

方式	描述
1	按照选择的视图及其组，在页面右侧展示查询到的资产。
2	可以配置更多的查询条件，搜索指定资产。
3	重置搜索条件。
4	查看资产详情，可以查看资产的基本信息、主机信息、服务信息、应用信息和对该资产执行过的历史任务。
5	跳转到 漏洞处置 的相应的查询页面。
6	跳转到 单资产风险 页面。可以查看 主机单资产风险。

主机单资产风险

网站资产的脆弱性统计和主机资产的类似，区别在于网站资产统计的为 Web 漏洞的信息，这里以主机资产为例进行介绍，网站资产的不再赘述。主机资产脆弱性统计的信息如表 4-12 所示。

说明	将鼠标置于页面图中颜色处，可以查看具体的数据。

表4-12 主机资产脆弱性统计

资产分析	资产属性	可以查看主机资产 IP 地址、名称和资产属性。单击资产名称，弹出资产详细信息页面，可以查看资产详情。
	分布汇总	【漏洞】：可以查看当前主机资产存在的漏洞总数和各风险级别漏洞分布情况（总数和百分比）。 【脆弱性】：可以查看当前主机资产脆弱性值。 【配置核查】：可以查看当前主机配置核查信息。 【弱口令】：可以查看当前主机弱口令信息。
	趋势分析	可以查看最近十天/最近十周/最近十个月内各级别漏洞个数或脆弱性值的变化趋势。
	漏洞分布	可以查看当前主机资产存在的不同漏洞分类中各级别漏洞的分布情况。 单击下拉列表，可以选择展示的漏洞分类。如何管理漏洞分类，具体请参见 管理分类。
	漏洞 TOP5	可以查看当前主机资产的风险等级最高的漏洞 TOP5，单击待查看的漏洞名称，可以查看漏洞详情。

	配置风险分布	可以查看当前主机资产的配置合规分布数据。
	配置风险类别	可以查看当前主机资产的配置风险类别分布数据。
漏洞统计	漏洞统计	可以查看当前资产中存在的漏洞的统计信息。 单击“漏洞名称”，弹出漏洞详情对话框，可以查看漏洞详情。 单击“出现次数”，弹出漏洞出现次数列表对话框，可以查看受该漏洞影响的端口清单。
配置合规	配置合规	可以查看当前资产中存在的配置合规的统计信息。
弱口令统计	弱口令统计	可以查看当前资产中存在的弱口令的统计信息。

4.2 资产监控

管理通过扫描发现的资产。目前扫描发现结果的来源有 RSAS 扫描发现、NTI 扫描发现、NESSUS 扫描发现和启明扫描发现。

入库配置

根据入库配置，TVM 每小时自动对扫描发现结果进行处置，并将处置结果记录至审计日志中。

进入 **资产管理 > 资产监控** 页面，单击【入库配置】按钮，启用“自动入库”、配置入库配置参数即可。入库配置参数如表 4-13 所示。

表4-13 入库配置

配置项	描述
处理状态	TVM 自动匹配“发现状态”的扫描发现结果，根据“优先入库”规则匹配资产组后、进行注册/变更/退网/处理操作。
优先入库	当资产 IP（目前仅支持 IPv4）匹配到多个资产组、且匹配到资产组存在父子关系时，TVM 自动将扫描发现结果入库在最外层“父资产组”或最内层“子资产组”。

管理扫描发现结果

进入 **资产管理 > 资产监控** 页面，可以对发现的资产进行操作，如表 4-14 所示。

表4-14 可对发现的资产进行操作

操作	说明
【查询】	配置查询条件或选择发现状态，单击【查询】按钮。
【忽略】/批量忽略扫描发现结果	忽略扫描发现结果中的资产，不可恢复。

操作	说明
导出扫描发现结果	导出扫描发现结果到本地。
批量下发任务	跳转到 扫描任务管理 页面。
【注册】/批量入库扫描发现结果	对于“新增”状态的资产，可以手动入库资产。 入库参数的说明请参见 新建主机资产。
【变更】	对于“变更”状态的资产，若所选资产属性值的来源均为资产库时，单击【变更】后，忽略该扫描发现信息，不可恢复。
【退网】	对于“离线”状态的资产，可以手动退网，退网操作会注销资产库中对应的资产，注销后不可恢复，只能重新添加。
【处理】	对于“错误”状态的资产，可以处理该资产，确认为错误的资产信息。

4.3 资产配置

资产属性用于分组管理资产，资产属性的类型分为树属性和文本属性，只有树属性可以“设置为视图属性”，进行 类型管理 后，展示在 资产列表 页面的左树中对资产进行管理。

4.3.1 属性管理

TVM 可以管理 50 个资产属性，视图属性不允许超过 7 个。

- 默认提供 5 个系统属性（树属性），分别为资产组、地理视图、业务视图、组织架构、行业。
- 用户也可以根据需要自定义资产的属性。
- 仅在新增/编辑树属性时支持添加子组。

进入 **资产管理 > 资产配置 > 属性管理** 页面，单击【新增属性】按钮，配置属性参数后即可新建属性。属性参数的说明如表 4-15 所示。新增属性后，还可以进行编辑、删除和排序操作。

表4-15 属性参数

属性类型	配置项	描述
文本	文本	文本类型的属性，在页面上以文本的形式展现。
	属性名称	属性的名称，具体请参见界面要求。
树	树	树类型的属性，在页面上以列表的形式进行展示。 只有树属性可以“设置为视图属性”，展示在 资产列表 页面的左树中对资产进行管理。仅树属性支持添加子组。
	属性名称	属性的名称，具体请参见界面要求。
	添加子组	新增属性/编辑属性时单击 **+添加子节点**，配置“节点名称”即可。添加子组后，还可以进行编辑和删除操作。

属性类型	配置项	描述
		在资产管理页面，也可以进行子组的新建、编辑和删除操作，具体请参见 新建子组。
	设置为视图属性	启用并进行类型管理后，属性展示在 资产列表 的左树中，可以对资产进行管理。

4.3.2 类型管理

类型管理，即将资产属性与主机资产或网站资产进行绑定，只有绑定后的资产属性才能在资产中使用。与资产绑定的树属性、且已“设置为视图属性”的，将显示在 资产列表 的左树中，可以对资产进行管理。

进入 **资产管理 > 资产配置 > 类型管理** 页面，单击【主机资产】/【网站资产】 >  ，选择需要绑定的“树属性”和“文本属性”即可。

4.3.3 标签管理

标签是用户为资产关联的除属性外的其他资产特性。

进入 **资产管理 > 资产配置 > 标签管理** 页面，单击【+添加标签】，编辑标签名称即可添加一个新的标签。可以批量删除所有标签。

4.3.4 异常资产配置

启动异常资产规则后，下发扫描任务时，设备将触发异常资产规则的资产直接判定为异常。

规则

进入 **资产管理 > 资产配置 > 异常资产配置 > 规则** 页面，单击【新建规则】，配置异常资产规则参数，批量启动异常资产规则 即可。异常资产规则参数如表 4-16 所示。新建规则后，还可以进行查看、编辑、删除和批量停用异常资产规则 的操作。

表4-16 异常资产规则参数

配置项	描述
规则名称	异常资产规则的名称，具体请参见界面要求。
规则对象	若资产匹配规则对象，则判定为异常。
规则描述	异常资产规则的说明信息，具体请参见界面要求。
异常条件	若资产匹配异常资产规则中的异常属性条件，则判定为异常。

白名单

异常资产分析时，若资产 IP 匹配异常资产白名单，则不进行分析。

进入 **资产管理 > 资产配置 > 异常资产配置 > 白名单** 页面，配置资产的 IPv4 地址即可。

4.3.5 重复资产配置

进入 **资产管理 > 资产配置 > 重复资产配置** 页面，配置是否允许存在重复资产。

- 选择否：系统全局资产不支持存在重复资产。
- 选择是：系统全局支持存在重复资产，但是同一资产组内不支持存在重复资产。

5 漏洞管理

本章主要包含以下内容：

功能	描述
漏洞处置	介绍如何处置管理资产中的漏洞。
漏洞归档	介绍如何管理归档后的漏洞。
漏洞配置	介绍如何管理脆弱性值计算方法和漏洞处置优先级等。

5.1 漏洞处置

在漏洞处置模块，统计资产中存在的漏洞情况，并进行不同维度的数据分析。

5.1.1 处置列表

处置列表从漏洞处置情况维度分析漏洞。

进入 **漏洞管理 > 漏洞处置 > 处置列表** 页面，可以管理当前资产中存在的漏洞。TVM 从脆弱性维度和资产维度来进行数据统计和展示，两者展示的内容和操作类似，这里以脆弱性维度为例进行介绍。

- 脆弱性维度

  从漏洞的维度进行统计，分析对资产的影响情况。选择左树中的漏洞类型和进行分类切换后，可以查看相应漏洞或漏洞分类的统计数据。

- 资产维度

  从资产的维度进行统计，分析资产中存在的漏洞情况。选择左树中的资产类型和切换视图后，可以查看相应资产或资产组的漏洞统计数据。

新建漏洞/弱口令

单击【新建】按钮，即可新建一条漏洞信息或弱口令信息。新建漏洞后，平台将漏洞的状态置为初始发现。新建漏洞的参数说明如表 5-1 所示，新建弱口令的参数说明如表 5-2 所示。

表5-1 新建漏洞参数

配置项		描述
数据类型		选择“漏洞”。
漏洞类型		可选项有主机、网站。
主机漏洞	端口	漏洞影响的主机端口。取值范围为 1~65535。
	协议	漏洞影响的主机访问协议。最多支持 128 个字符。
	影响服务	漏洞影响的主机访问服务。最多支持 128 个字符。
网站漏洞	请求方式	漏洞影响的网站访问请求方式。最多支持 32 个字符。
	关键 URL	漏洞影响的网站 URL。支持填写多个 URL，用英文逗号分隔。最多支持 1000 个字符。
	问题参数	漏洞影响的网站问题参数。最多支持 1000 个字符。
其他信息		漏洞的其他信息。最多支持 1000 个字符。
漏洞列表		单击【添加漏洞】按钮，可以从漏洞情报库中选择添加。添加后，支持删除操作。
资产列表		根据所选的漏洞类型，选择存在漏洞的主机资产/网站资产。

表5-2 新建弱口令参数

配置项	描述
数据类型	选择“弱口令”。
其他信息	漏洞的其他信息。最多支持 1000 个字符。
用户名/密码	弱口令的用户名和密码。其中，用户名最多支持 100 个字符，密码最多支持 32 个字符。
端口	漏洞影响的主机/网站端口。取值范围为 1~65535。
协议	可选项有 UDP、TCP、ICMP。
服务类型	漏洞影响的远程服务类型。
漏洞列表	单击【添加漏洞】按钮，可以从漏洞情报库中选择添加。添加后，支持删除操作。
资产列表	根据所选的漏洞类型，选择存在漏洞的主机资产/网站资产。

漏洞编辑

可以对主机漏洞进行处置，漏洞处置参数说明如表 5-3 所示。

- 单个处置：单击操作栏的【编辑】，配置漏洞处置参数即可。
- 批量处置：勾选需要处置的漏洞，单击【批量编辑】按钮，配置漏洞处置参数即可。

表5-3 漏洞处置参数

配置项	描述
数据类型	可选项有漏洞、弱口令。
处置状态	请参见 漏洞处置状态 进行配置。
处置方式	对漏洞的建议处置方式。
处置人	将漏洞指派给其他责任人进行处理。
协议/影响服务	漏洞影响的协议/服务。
资产防护	勾选后，表示资产已经防护该漏洞，平台会降低漏洞处置单的默认优先级。
优先级更新方式	在关闭“资产防护”时，可以配置“优先级更新方式”。 • 自动：TVM 自动调整漏洞的“处置优先级”。 • 手动：TVM 根据“优先值”来确定漏洞的“处置优先级”。
时间忽略	在该时间段内，不对该漏洞计算脆弱性值。
处置评论	对漏洞的处置建议。
其他信息	漏洞的其他信息。

漏洞处置状态

漏洞处置状态如图 5-1 和表 5-4 所示。

图5-1 处置状态

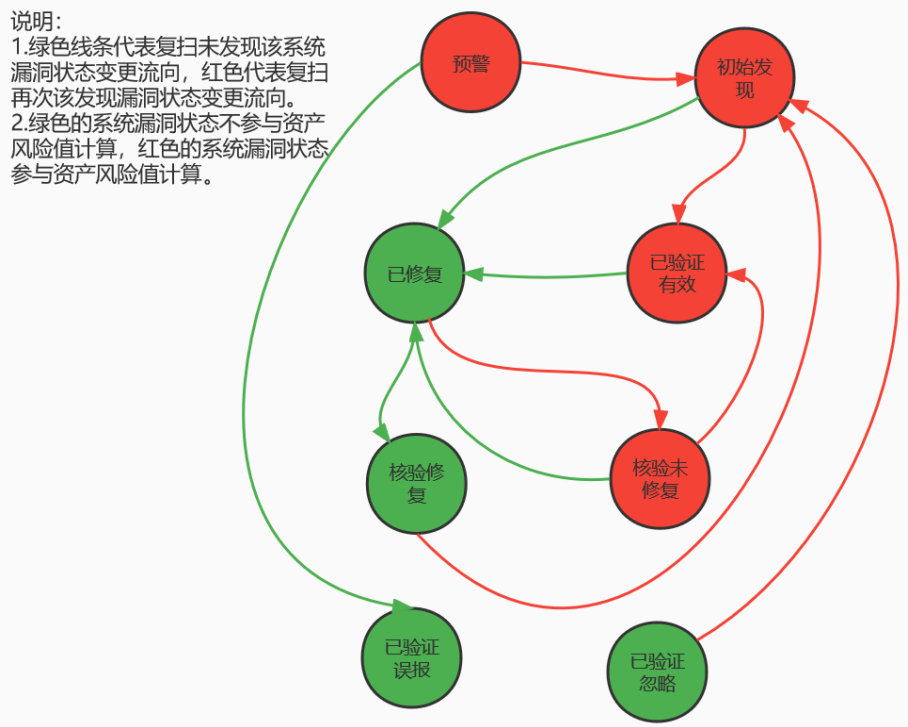


表5-4 处置状态

处置状态		描述
未处理状态	初始发现	• 新建漏洞 后，平台将漏洞的状态置为初始发现。 • 第一次发现漏洞时，平台将漏洞的状态置为初始发现。 • 对于预警状态的漏洞，若执行 预警扫描验证 后发现该漏洞，则平台将处置状态置为初始发现。
	已验证有效	对于状态为初始发现的系统漏洞，若执行 漏洞复扫 后该漏洞仍被发现，漏洞状态变更为已验证有效。
	预警	通过 新建产品漏洞预警任务 发现的漏洞，平台将处置状态置为预警。
已处理状态	已验证误报	确认为误报，不参与资产风险值的计算。
	已验证忽略	已验证忽略后，本次不计算该漏洞的风险值，再次扫描时如果又发现该漏洞，则平台将处置状态置为初始发现。
	已修复	对于所有状态的漏洞，若执行 漏洞复扫 后该漏洞不存在，则平台将处置状态置为已修复。
	核验修复	对于状态被置为已修复的漏洞，若再次扫描时该漏洞不存在，则平台将处置状态置为核验修复。
	核验未修复	对于状态被置为已修复的漏洞，再次扫描时如果又发现该漏洞，则平台将处置状态置为核验未修复。

漏洞管理

新建/发现漏洞后，还可以进行如表 5-5 所示的管理操作。

表5-5 脆弱性维度

统计维度/操作	描述
查询	按照如下分类，在漏洞列表中展示相应漏洞数据 • 漏洞处置优先级：单击 5 高优先级 13 中优先级 11 低优先级 • 漏洞处置状态：单击 0 预警 29 初始发现 0 已验证有效 0 已验证误报 0 已验证忽略 0 已修复 0 核验修复 0 核验未修复 • 漏洞查询：支持漏洞名称的模糊查询。单击【高级查询】按钮，可以设置更多查询条件。系统漏洞的高级查询条件说明如表 5-6 所示。 单击操作栏的【详情】，查看漏洞的详细信息。
漏洞统计概览	• 漏洞状态统计：以饼图的方式，展示“时间周期”内，不同状态漏洞的数量和占比。 • 处置优先级统计：以柱状图的方式，展示“时间周期”内，不同处置优先级漏洞的数量。
漏洞归档	单击操作栏的【归档】/【批量归档】按钮，可以对处置状态为“核验修复”且不再关注的漏洞进行归档，归档后，该漏洞移至 漏洞归档 模块、不再出现在系统漏洞列表中且不再上报。
漏洞复扫	单击【批量复扫】按钮/在漏洞详情页单击【漏洞复扫】按钮，重新执行扫描任务。
批量新建漏洞误报	请参见 漏洞误报库。
预警扫描验证	单击【预警扫描验证】按钮，对预警匹配的漏洞执行扫描任务。若执行预警扫描验证后发现该漏洞，则平台将处置状态置为初始发现。
查看关联任务	单击关联任务，可以查看发现该漏洞的扫描任务的报表。
查看漏洞详情	单击操作栏的【详情】，可以查看漏洞详情。
查看影响资产	单击影响资产数下的数字，可以查看该漏洞的影响资产清单。

表5-6 系统漏洞高级查询条件

查询项		描述
漏洞查询条件	数据类型	可选项有漏洞、弱口令。
	漏洞名称	漏洞的名称。
	漏洞编号	漏洞的编号。
	生命周期序号	漏洞的生命周期序号。取值范围为大于 0 的整数。 说明 生命周期，是指漏洞从初始发现到核验修复，是第一轮生命周期；

查询项		描述
		再次被发现，就进入到第二次生命周期。
	漏洞分值	拖动鼠标设置漏洞的分值。取值范围为 0~10 的整数。
	脆弱性等级	可选项有极高、高、中、低、提示。支持多选。
	处置优先级	可选项有高、中、低。支持多选。
	处置单状态	可选项有预警、初始发现、已验证有效、已验证误报、已验证忽略、已修复、检验修复、检验未修复。支持多选。
	漏洞模板	漏洞模板的查看与配置方法，请参见 产品漏洞模板。
	来源厂商	目前支持的漏洞来源厂商包括绿盟科技、启明、安恒、奇安信、自定义。支持多选。
	影响端口	取值范围为 1~65535。
	空端口	是否为空端口。
	更新时间	漏洞更新的时间范围。
	服务类型	漏洞影响的远程服务类型。支持多选。
	空服务	是否为空服务。
	是否可验证	是否验证漏洞已存在。
工单查询条件	工单编号	工单编号的查询方法，请参见 工单管理。
	是否关联工单	是否关联 工单管理 中的工单进行查询。
	流程状态	可选项有初始化、处理中、审核中、完成。
资产查询条件	资产 IP	支持资产 IP 的模糊查询和精确查询。仅支持单个 IPv4 地址。
	资产名称	支持资产名称的模糊查询和精确查询。最多支持 100 个字符。
	资产联系人	支持资产联系人的模糊查询和精确查询。最多支持 100 个字符。
任务查询条件	任务名称	支持关联任务名称的模糊查询和精确查询。

5.1.2 漏洞视角/端口视角/服务视角

进入 **漏洞管理 > 漏洞处置 > 漏洞视角/端口视角/服务视角** 页面，可以从相应维度管理当前资产中存在的漏洞。

- 漏洞视角：对单个漏洞进行统计分析，单击“影响资产数”可以下钻查询关联的资产情况，单击“详情”可以查看漏洞的详细信息。
- 端口视角：从开放端口维度进行统计分析，单击“影响资产数”可以下钻查询关联的资产情况，单击“影响漏洞数/POC 漏洞数”可以下钻查询关联的漏洞情况，单击“详情”可以查看关联的处置单情况。
- 服务视角：从应用服务维度进行统计分析，单击“影响资产数”可以下钻查询关联的资产情况，单击“影响漏洞数/POC 漏洞数”可以下钻查询关联的漏洞情况，单击“详情”可以查看关联的处置单情况。

5.1.3 漏洞归并修复建议

进入 **漏洞管理 > 漏洞处置 > 漏洞归并修复建议** 页面，可以对系统中部分受当前软件版本影响的漏洞进行统计管理和处置操作，如表 5-7 所示。

表5-7 漏洞归并修复建议

区域	描述
统计概览	• 类型统计：以柱状图的方式，不同类型漏洞的数量。 • 升级状态统计：以饼图的方式，不同升级状态漏洞的数量和占比。
漏洞修复升级列表	修复方案：受影响漏洞的修复方案，可以参考方案进行漏洞修复。
	升级状态：随跟软件关联的漏洞处置单状态的变化而变化。 • 当跟软件关联的漏洞处置单状态为新增、待修复、修复失败、再次发现时，软件升级状态为“待升级”。 • 当跟软件关联处置单状态为单次忽略、永久忽略、已修复、已验证时，软件升级状态为“已升级”。
	影响资产数：单击后，可以下钻查询关联的资产情况。
	影响漏洞数：单击后，可以下钻查询关联的漏洞情况。
	详情：单击后，可以查看受该软件影响的漏洞处置列表以及统计信息。
	处置：可以处置漏洞，具体请参见 漏洞处置。

5.2 漏洞归档

进入 **漏洞管理 > 漏洞归档** 页面，可以管理 漏洞归档 后的漏洞。

- 可以查询漏洞、查看漏洞详情。
- 单击【批量清除】按钮，批量删除漏洞后，相应漏洞不再出现在归档列表和 漏洞处置 的系统漏洞列表、且不再上报。
- 单击【清除配置】按钮，可以配置自动删除归档漏洞的频度和范围。

5.3 漏洞配置

在漏洞配置模块，可以管理脆弱性值计算方法和漏洞处置优先级等。

风险评估模型

TVM 根据模型计算资产或资产组的脆弱性值。

进入 **漏洞管理 > 漏洞配置 > 风险评估模型** 页面，可以自定义资产风险评估模型的“脆弱性因子权重”和“资产因子权重”。

处置优先级模型

进入 **漏洞管理 > 漏洞配置 > 处置优先级模型** 页面，可以配置资产因子、脆弱性因子、漏洞威胁因子和漏洞运维因子对漏洞处置优先级的影响程度。

- 开启：将相应因子作为处置漏洞的优先级条件。关闭：相应因子不会影响处置漏洞的优先级。
- 权重：对处置漏洞优先级影响程度。
- 级别：级别越高，影响越大。

6 扫描管理

本章主要包含以下内容：

功能	描述
新建扫描任务	介绍如何快捷创建扫描任务。
扫描任务管理	介绍如何管理新建的任务。
批量任务管理	介绍如何管理导入的任务
扫描设备管理	介绍如何管理执行扫描任务的设备和引擎实例。
任务配置	介绍如何管理扫描任务的部分执行策略。

6.1 新建扫描任务

该模块作为配置各类扫描任务的快捷入口。

进入 **扫描管理 > 新建扫描任务** 页面，选择扫描任务类型后，即可配置新的扫描任务。具体详情请参见 6.2.1 新建任务。

6.2 扫描任务管理

在扫描任务管理模块，可以管理所有扫描任务。

6.2.1 新建任务

介绍如何新建各类扫描任务。

6.2.1.1 新建主机扫描任务

主机扫描任务可以对主机资产进行系统漏洞扫描，能够发现资产中存在的系统漏洞。

进入 **扫描管理 > 扫描任务管理** 页面，单击【新建任务】按钮，选择【主机扫描】，配置主机扫描任务的基本信息、登录配置、系统配置和端口及存活配置参数即可新建一个主机扫描

任务。其中，登录配置、系统配置和端口及存活配置为可选，可以保持默认值。各参数如表 6-1、表 6-2、表 6-3 和表 6-4 所示。

表6-1 主机扫描任务-基本信息

配置项	描述
任务名称	该扫描任务的名称，不允许为空和重名。 • 取值范围为 1~60 个字符。 • 不允许包含特殊字符，特殊字符的范围请以界面展示为准。
执行方式	• 立即执行：设备将执行即时扫描任务。 • 定时执行：设备将执行定时扫描任务。 • 周期执行：设备将执行周期扫描任务。
目标类型	扫描目标的 IP 地址的格式。
漏洞验证	启用后，任务结束时，TVM 自动新建漏洞验证任务，检测是否存在扫描到的漏洞。
引擎类型	执行任务的扫描引擎。 • 绿盟科技：需要配置“扫描设备”和“漏洞模板”。 • 第三方扫描引擎：需要配置 引擎版本。
目标方式	• 选择资产：选择待扫描的主机资产或主机资产组。 • 手动输入：手动配置待扫描的主机资产，格式要求请参见界面提示。
目标白名单	不执行扫描的目标，如何管理白名单请参见 扫描白名单管理。 全局级的目标白名单默认对所有任务生效。
端口修正	将扫描到的端口替换为自定义端口，用于修正扫描结果中端口的准确性。
选择设备	• 自动分发：根据扫描目标，TVM 自动分配扫描设备。 • 手动指派：手动选择扫描设备。
漏洞模板	• 自动匹配：根据扫描目标，TVM 自动分配扫描漏洞模板。 • 手动指派：手动选择漏洞模板。
登录检查	开启后，会对目标主机进行预登录。 此时，需要配置“登录配置”参数，如表 6-2 所示。
日期白名单	不执行扫描任务的时间段，如何管理白名单请参见 扫描白名单管理。 全局级的日期白名单默认对所有任务生效。
自动生成报表	启用后，自动各生成报表类型支持的报表格式的离线报表。
扫描时间段	执行扫描任务的时间范围。

表6-2 主机扫描任务-登录配置

配置项	描述
当前节点	选择需要进行登录配置的资产所在的节点。

配置项		描述
基本信息	用户名/密码	预登录扫描目标的用户名和密码。
	登录协议/端口	登录扫描目标使用的登录协议和端口信息。 RDP 协议仅支持进行配置核查，不支持进行漏洞扫描。
	主机跳转	• 在设备不能直接登录目标主机时，可以使用跳转主机进行扫描，需要预先配置跳转主机的认证信息。 • 需要保证跳转主机能够连接到目标主机。 • 只有在通过 SSH、Telnet 方式登录目标主机时，才能配置主机跳转功能。 • 跳转机 IP/用户名/密码：跳转机的 IP 地址、登录的用户名和密码。 • 登录协议和端口：登录跳转机使用的登录协议和端口信息。
漏扫策略	ORACLE	• 不开启：设备只上报 ORACLE 相关服务识别和原理扫描漏洞。 • 开启：设备上报所有漏洞，除上报上述漏洞外、还上报本地 ORACLE 漏洞，此时需要配置登录 ORACLE 的用户名和密码、端口和 SID 信息。
WEBLOGIC	WEBLOGIC	开启后，通过搭建 WEBLOGIC 服务的设备后台来访问 WEBLOGIC。 此时需要配置 WEBLOGIC 服务所在主机的操作系统类型、Weblogic 的版本、Weblogic 的用户名和 Weblogic 的 Wls 的安装路径。

表6-3 主机扫描任务-系统配置

配置项	描述
调度优先级	设备将根据调度优先级数值和后台算法判断扫描任务的执行顺序。
调试模式	开启后，设备将记录扫描任务的执行信息，当扫描任务执行异常时，可以导出异常信息并发送给绿盟科技的技术支持人员进行错误分析。
扫描深度	数值越大，设备获取的信息可能就越多，扫描时间越长。 建议使用缺省配置。
危险插件扫描	此类插件可能导致资产的系统崩溃或服务中断。 通常情况下不建议使用，只有在特定情况下启用（如：产品评测）。
oracle 漏洞深度扫描	• 不开启：设备只上报 ORACLE 相关服务识别和原理扫描漏洞。 • 开启：设备上报所有漏洞，除上报上述漏洞外、还上报本地 ORACLE 漏洞。
深度扫描重要网络设备	启用此功能可能导致某些特定型号的网络设备在扫描中出现故障，请谨慎启用。
插件超时限制（秒）	单个插件在插件超时限制的时间内如果未正常结束，将会被强行终止。
socket 超时限制（秒）	从网络层获取扫描数据时，等待的最大超时时间。 • 此选项对扫描速度和准确度有较大影响，局域网建议 5 秒，ADSL 建议 15 秒。

配置项	描述
	• 可以根据网络速度的情况，配置 Socket 超时限制；若网速慢，则 Socket 超时限制需要配置的大一些。

表6-4 主机扫描任务-端口及存活配置

配置项	描述
扫描范围	• 标准端口扫描：只扫描常用服务对应的端口。 • 快速端口扫描：只扫描 1~1024 端口。 • 指定端口范围：只扫描指定范围内的端口。
扫描速度	扫描速度越慢，获取的端口开放信息将会越准确，同时花费的时间可能会越长。
TCP 端口扫描方式	• CONNECT：通过直接建立完整的 TCP 连接来判断端口的开放情况，此方法快而准确。 • SYN：向目标端口发送 SYN 包，依据对方是否回复 ACK 报文来判断端口的开放情况。
主机存活测试	主机存活测试，向目标主机发送数据报文，根据目标主机的反应以判断其是否存活。只有存活的主机才可以执行扫描任务。 启用后，需要选择使用的测试方法 ICMP Ping、UDP Ping 或 TCP Ping，若选择 TCP Ping 方式，还需要配置测试端口。
UDP 扫描	开启后，才会扫描 UDP 端口。 启用 UDP 扫描将会大大增加扫描时间，因此不建议选择此项。

6.2.1.2 新建配置核查任务

配置核查任务能够发现扫描目标中存在安全配置不合规信息。

进入 **扫描管理 > 扫描任务管理** 页面，单击【新建任务】按钮，选择【配置核查】，配置任务的基本信息和登录配置参数即可新建一个配置核查任务。各参数如表 6-5 和表 6-6 所示。

表6-5 配置核查任务-基本信息

配置项	描述
任务名称	该扫描任务的名称，不允许为空和重名。 • 取值范围为 1~60 个字符。 • 不允许包含特殊字符，特殊字符的范围请以界面展示为准。
执行方式	• 立即执行：设备将执行即时扫描任务。 • 定时执行：设备将执行定时扫描任务。 • 周期执行：设备将执行周期扫描任务。
目标类型	扫描目标的 IP 地址的格式。

配置项	描述
目标方式	• 选择资产：选择待扫描的主机资产或主机资产组。 • 手动输入：手动配置待扫描的主机资产，格式要求请参见界面提示。
目标白名单	不执行扫描的目标，如何管理白名单请参见扫描白名单管理。 全局级的目标白名单默认对所有任务生效。
选择设备	• 自动分发：根据扫描目标，TVM 自动分配扫描设备。 • 手动指派：手动选择扫描设备。
登录检查	需要配置“登录配置”参数，如表 6-6 所示。
日期白名单	不执行扫描任务的时间段，如何管理白名单请参见扫描白名单管理。 全局级的日期白名单默认对所有任务生效。
自动生成报表	启用后，自动各生成报表类型支持的报表格式的离线报表。
扫描时间段	执行扫描任务的时间范围。

表6-6 配置核查任务-登录配置

配置项		描述
当前节点		选择需要进行登录配置的资产所在的节点。
基本信息	用户名/密码	预登录扫描目标的用户名和密码。
	登录协议/端口	登录扫描目标使用的登录协议和端口信息。 RDP 协议仅支持进行配置核查，不支持进行漏洞扫描。
	主机跳转	• 在设备不能直接登录目标主机时，可以使用跳转主机进行扫描，需要预先配置跳转主机的认证信息。 • 需要保证跳转主机能够连接到目标主机。 • 只有在通过 SSH、Telnet 方式登录目标主机时，才能配置主机跳转功能。 • 跳转机 IP/用户名/密码：跳转机的 IP 地址、登录的用户名和密码。 • 登录协议和端口：登录跳转机使用的登录协议和端口信息。
配置模板	等级保护/等保级别	扫描目标是否启用等级保护功能。 • 勾选启用后，选择安全等级保护级别，然后可以为其选用相应等保级别的等保模板。 • 安全等级保护级别的详细说明请参见安全等级保护。
	设备类型	主机指安装了操作系统的计算机。单击模板项进行选择，配置模板参数即可。 • 操作系统模板：需要匹配操作系统类型。 • 虚拟化设备模板：需要匹配虚拟化设备类型。 • 应用程序模板：需要匹配已经安装的应用程序类型。 • 数据库模板：需要匹配已经安装的数据库类型。

配置项		描述
		• 大数据模板：需要匹配已经安装的大数据软件或平台类型。
		网络设备指除主机外连接到网络中的物理实体，如交换机、路由器等。 • 单击模板项进行选择，配置模板参数即可。 • 需要匹配网络设备的类型。

6.2.1.3 新建口令猜测任务

TVM 可以通过口令字典中的用户名和密码尝试登录目标主机，若登录成功说明目标主机中存在脆弱帐号。

进入 **扫描管理 > 扫描任务管理** 页面，单击【新建任务】按钮，选择【口令猜测】，配置口令猜测任务的基本信息、系统配置、主机存活配置和口令猜测参数即可新建一个口令猜测任务。各参数如表 6-7、表 6-8、表 6-9 和表 6-10 所示。

表6-7 口令猜测任务-基本信息

配置项	描述
任务名称	该扫描任务的名称，不允许为空和重名。 • 取值范围为 1~60 个字符。 • 不允许包含特殊字符，特殊字符的范围请以界面展示为准。
执行方式	• 立即执行：设备将执行即时扫描任务。 • 定时执行：设备将执行定时扫描任务。 • 周期执行：设备将执行周期扫描任务。
目标类型	扫描目标的 IP 地址的格式。
目标方式	• 选择资产：选择待扫描的主机资产或主机资产组。 • 手动输入：手动配置待扫描的主机资产，格式要求请参见界面提示。
目标白名单	不执行扫描的目标，如何管理白名单请参见扫描白名单管理。 全局级的目标白名单默认对所有任务生效。
选择设备	• 自动分发：根据扫描目标，TVM 自动分配扫描设备。 • 手动指派：手动选择扫描设备。
日期白名单	不执行扫描任务的时间段，如何管理白名单请参见扫描白名单管理。 全局级的日期白名单默认对所有任务生效。
自动生成报表	启用后，自动各生成报表类型支持的报表格式的离线报表。
扫描时间段	执行扫描任务的时间范围。

表6-8 口令猜测任务-系统配置

配置项	描述
调度优先级	设备将根据调度优先级数值和后台算法判断扫描任务的执行顺序。
调试模式	开启后，设备将记录扫描任务的执行信息，当扫描任务执行异常时，可以导出异常信息并发送给绿盟科技的技术支持人员进行错误分析。

表6-9 口令猜测任务-主机存活配置

配置项	描述
主机存活测试	主机存活测试，向目标主机发送数据报文，根据目标主机的反应以判断其是否存活。只有存活的主机才可以执行扫描任务。 启用后，需要选择使用的测试方法 ICMP Ping、UDP Ping 或 TCP Ping，若选择 TCP Ping 方式，还需要配置测试端口。
UDP 扫描	开启后，才会扫描 UDP 端口。 启用 UDP 扫描将会大大增加扫描时间，因此不建议选择此项。

表6-10 口令猜测任务-口令猜测

配置项	描述
猜测次数	对单个主机的猜测次数，0 表示不受次数限制。
最大并发线程数	对单个主机的单个服务进行口令猜测时的并发线程数目。 范围：1~10，值越大，探测速度越快。
口令猜测频率（秒）	对某个被扫描目标进行两次相同协议口令猜测的时间间隔。范围：0~600 秒。
口令猜测时间（分钟）	一个口令猜测插件的最长运行时间，达到设定时间该插件终止运行。时间范围：1~10080。
口令字典模板	选择不同分组下的口令猜测模板。

6.2.1.4 新建网站扫描任务

网站扫描任务可以根据用户需要对目标站点进行不间断的页面爬取、分析、匹配，从而发现目标站点中存在的 Web 漏洞。

进入 **扫描管理 > 扫描任务管理** 页面，单击【新建任务】按钮，选择【网站扫描】，配置网站扫描任务的基本信息、网站认证、网站访问、网站检测和网站爬行参数即可新建一个网站扫描任务。其中，网站访问、网站检测和网站爬行为可选，可以保持默认值。各参数如表 6-11、表 6-12、表 6-13、表 6-14 和表 6-15 所示。

表6-11 网站扫描任务-基本信息

配置项	描述
任务名称	该扫描任务的名称，不允许为空和重名。 • 取值范围为 1~60 个字符。 • 不允许包含特殊字符，特殊字符的范围请以界面展示为准。
执行方式	• 立即执行：设备将执行即时扫描任务。 • 定时执行：设备将执行定时扫描任务。 • 周期执行：设备将执行周期扫描任务。
漏洞验证	启用后，任务结束时，TVM 自动新建漏洞验证任务，检测是否存在扫描到的漏洞。
引擎类型	执行任务的扫描引擎。 • 绿盟科技：需要配置“扫描设备”和“漏洞模板”。 • 第三方扫描引擎：需要配置 引擎版本。
目标方式	• 选择资产：选择待扫描的网站资产或网站资产组。 • 手动输入：手动配置待扫描的网站资产，格式要求请参见界面提示。
扫描范围	爬虫并扫描的范围。 • 整站扫描：扫描父域名及子域名下的所有 URL。 • 扫描子域名：只扫描父域名及此处配置的子域名下的所有 URL，不扫描其他子域名。 • 跳过子域名：不扫描此处配置的子域名，只扫描父域名及其他子域名下的所有 URL。 • 当前目录及其子目录：只扫描“扫描目标”及所有子目录中的 URL。 • 当前链接：只扫描“扫描目标”中的 URL。
目标白名单	不执行扫描的目标，如何管理白名单请参见扫描白名单管理。 全局级的目标白名单默认对所有任务生效。
选择设备	• 自动分发：根据扫描目标，TVM 自动分配扫描设备。 • 手动指派：手动选择扫描设备。
漏洞模板	• 自动匹配：根据扫描目标，TVM 自动分配扫描漏洞模板。 • 手动指派：手动选择漏洞模板。
日期白名单	不执行扫描任务的时间段，如何管理白名单请参见扫描白名单管理。 全局级的日期白名单默认对所有任务生效。
自动生成报表	启用后，自动各生成报表类型支持的报表格式的离线报表。

表6-12 网站扫描任务-网站认证

配置项	描述
协议认证	扫描目标使用的认证协议。
协议认证用户名/密码	扫描目标使用的认证协议的用户名/密码。

配置项	描述
登录扫描	启用后，TVM 会使用配置的登录信息来登录扫描目标进行扫描。 需要配置用来记录登录会话标识的 Cookie。例：action=login&username=admin&password=admin88
认证代理配置	是否需要通过代理服务器才可以连接待扫描目标。 • 代理类型：代理服务器的类型。 • 认证协议：代理服务器使用的认证协议。 • 服务器地址/端口：代理服务器 IP 地址/端口号，服务器地址可以是 IP 地址或域名。 • 用户名/密码：代理服务器的登录用户名和密码。必须同时配置用户名和密码。

表6-13 网站扫描任务-网站访问

配置项	描述
并发线程数	进行网站扫描时，扫描插件的并发扫描线程数，数值越大，扫描速度越快。 • 默认值为 100；取值范围为 1~100。 • 配置时，需要考虑网络带宽以及服务器的处理能力，过大的数值会影响目标服务器的正常运行。
超时限制（秒）	扫描一个页面的最长时间限制。 默认值为 30 秒；取值范围为 1~300 秒。
请求失败重试次数	网站访问请求失败后，允许重新请求的最大次数。
网页编码方式	为了能够正常访问扫描目标，需要正确匹配扫描目标中网页的编码方式。 • 自动检测：自动匹配网页的编码方式。 • 手动检测：手动指定扫描目标的网页编码方式。
自定义 User-Agent	执行 Web 应用扫描任务时，使用指定的浏览器或搜索引擎访问扫描目标。

表6-14 网站扫描任务-网站检测

配置项	描述
目录猜测范围	每个目录下常见敏感目录、敏感文件的猜测范围。 • 默认值为 1；取值范围为 0~3，0 表示不猜测。 • 数值越大，猜测的范围越广，可能猜测出的目录、文件越多，但是扫描时间会更长。
目录猜测深度	敏感目录、敏感文件的猜测层次深度。 该数值不能大于 Web 爬行参数中“目录深度”的数值。 默认值为 3；取值范围为 0~30。
备份文件检查类型	需要检查哪些类型的文件中存在备份文件，多个类型之间用“,”分隔。

配置项	描述
备份文件检查扩展名	需要检查的备份文件的扩展名，与“备份文件检查类型”配合使用，多个扩展名之间用“,”分隔。

表6-15 网站扫描任务-网站爬行

配置项	描述
爬行顺序	扫描过程中采取的 URL 获取方式。
单目录文件数	当启用“链接消重策略”时，每个目录下被扫描的文件个数的最大值。 取值范围为大于等于-1 的整数，“-1”表示不限制。
目录深度	扫描时，爬虫获取的目录层次深度。 • 默认值为 15；取值范围为-1~30，“-1”表示不限制。 • 目录层次深度是指从根目录开始，在 URL 中第几个“/”就是第几层。目录层次深度的数值越大，扫描越深入，消耗的时间越长，因此需要适当限制目录层次深度。
链接总数	获取到的 URL 总个数的最大值。 取值范围为大于等于-1 的整数，“-1”表示不限制。
是否大小写敏感	在扫描过程中是否区分 URL 中的大小写字母。
自定义链接	必须扫描的 URL，可以是外部链接。 多个 URL 之间使用“,”、回车分隔。
排除链接	不需要爬取的 URL。
自定义目录	爬虫分析的目录范围。 多个目录之间使用“,”、回车分隔。 不允许包含特殊字符，特殊字符的范围请以界面展示为准。
排除目录	不需要爬取的目录。 多个目录之间使用“,”、回车分隔。 不允许包含特殊字符，特殊字符的范围请以界面展示为准。
排除文件名	不需要爬取哪些名称的文件。 多个文件名之间使用“,”分隔。
排除后缀	不需要爬取哪些后缀的文件。 多个后缀之间使用“,”分隔。
是否解析 Flash 文件	是否开启 Flash 相关扫描，目前只支持解析 Flash 10 以下的版本。
是否执行 JavaScript	爬取页面时，是否执行页面中的 JavaScript 脚本代码以获取 URL。 • 是：表示需要执行 javascript 代码，并且模拟触发各类事件。 • 否：表示禁止执行 javascript 代码，这样会提高扫描速度，但是会有部分 URL 不被爬取。
链接消重策略	指定 URL 消重策略的等级，可选值 0、1、2、3、4，默认值为 2。 一般来说，一个 URL 地址由一个五元组（page，method，query-name，

配置项	描述
	query-value，post-data）组成，消重策略的等级指定了对 URL 地址五元组中的哪些元素敏感，从而区分不同 URL 地址。 以 http://www.nsfocus.com/test.php?login=admin 为例： • page=http://www.nsfocus.com/test.php（page=协议+域名+路径文件） • method=GET • query-name=login • query-value=admin • post-data=NULL 那么对于消重等级来说： • 0：对 page 敏感 • 1：对 page，method 敏感 • 2：对 page，method，query-name 敏感 • 3：对 page，method，query-name 和 query-value 敏感 • 4：对 page，method，query-name，query-value 和 post-data 敏感 消重等级越高，则 URL 地址的相同因素就要越多，当设定等级为 0 时，只要两个 URL 的 page 相同，就认定这两个 URL 是同一个 URL，无需再考虑后续的参数值。
表单扫描	当页面中存在表单时，是否对表单进行扫描，从而发现更多的漏洞信息。
添加表单	当页面中存在表单时，是否对表单进行填充，以获取更多的 URL，从而发现更多的漏洞信息。 启用后，需要配置填充项信息；单击【添加表单】，可以添加填充项。

6.2.1.5 新建资产发现任务

资产发现任务用来发现内网和外网的资产，包括主机资产和网站资产。

进入 **扫描管理 > 扫描任务管理** 页面，单击【新建任务】按钮，选择【资产发现】，配置资产发现任务的基本信息和端口及存活配置参数即可新建一个资产发现任务。各参数如表 6-16 和表 6-17 所示。

表6-16 资产发现任务-基本信息

配置项	描述
任务名称	该扫描任务的名称，不允许为空和重名。 • 取值范围为 1~60 个字符。 • 不允许包含特殊字符，特殊字符的范围请以界面展示为准。
执行方式	• 立即执行：设备将执行即时扫描任务。 • 定时执行：设备将执行定时扫描任务。 • 周期执行：设备将执行周期扫描任务。
目标类型	主机目标的 IP 地址的格式或网站目标的 URL。
目标方式	• 选择资产：目标类型为“IPv4”或“IPv6”时，选择待扫描的主机资产或主机

配置项	描述
	资产组。 • 手动输入：目标类型为“IPv4”、“IPv6”或“域名”时，手动配置待扫描的主机 IP、主机 IP 范围或 URL 信息，格式要求请参见界面提示。 • 资产组 IP 范围：目标类型为“IPv4”时，选择待扫描的资产组。
目标白名单	不执行扫描的目标，如何管理白名单请参见扫描白名单管理。 全局级的目标白名单默认对所有任务生效。
选择设备	• 自动分发：根据扫描目标，TVM 自动分配扫描设备。 • 手动指派：手动选择扫描设备。 • 绿盟威胁情报中心：通过 NTI 执行扫描任务。
日期白名单	不执行扫描任务的时间段，如何管理白名单请参见扫描白名单管理。 全局级的日期白名单默认对所有任务生效。
自动生成报表	启用后，自动各生成报表类型支持的报表格式的离线报表。
扫描时间段	执行扫描任务的时间范围。

表6-17 资产发现任务-端口及存活配置

配置项	描述
扫描范围	• 标准端口扫描：只扫描常用服务对应的端口。 • 快速端口扫描：只扫描 1~1024 端口。 • 指定端口范围：只扫描指定范围内的端口。
扫描速度	扫描速度越慢，获取的端口开放信息将会越准确，同时花费的时间可能会越长。
TCP 端口扫描方式	• CONNECT：通过直接建立完整的 TCP 连接来判断端口的开放情况，此方法快而准确。 • SYN：向目标端口发送 SYN 包，依据对方是否回复 ACK 报文来判断端口的开放情况。
主机存活测试	主机存活测试，向目标主机发送数据报文，根据目标主机的反应以判断其是否存活。只有存活的主机才可以执行扫描任务。 启用后，需要选择使用的测试方法 ICMP Ping、UDP Ping 或 TCP Ping，若选择 TCP Ping 方式，还需要配置测试端口。
UDP 扫描	开启后，才会扫描 UDP 端口。 启用 UDP 扫描将会大大增加扫描时间，因此不建议选择此项。

6.2.1.6 新建渗透测试任务

渗透测试任务可以模拟检验网络中的安全隐患。

进入 **扫描管理 > 扫描任务管理** 页面，单击【新建任务】按钮，选择【渗透测试】，配置渗透测试任务的任务信息和漏洞信息参数即可新建一个渗透测试任务。各参数如表 6-18 和表 6-19 所示。

表6-18 渗透测试任务-任务信息

配置项	描述
任务名称	该扫描任务的名称，不允许为空和重名。 • 取值范围为 1~60 个字符。 • 不允许包含特殊字符，特殊字符的范围请以界面展示为准。
目标类型	主机目标的 IP 地址的格式或网站目标的 URL。
目标方式	• 手动输入：手动配置待扫描的主机资产或网站资产，格式要求请参见界面提示。 • 选择目标：选择待扫描的主机资产、主机资产组或网站资产、网站资产组。
测试时间	选择渗透任务的开始时间。
测试人员姓名	测试人员的姓名。
测试人员联系方式	测试人员的联系方式。
风险等级	拖动鼠标，选择该任务的风险等级。
【保存】	创建相应的渗透测试任务。

表6-19 渗透测试任务-漏洞信息

漏洞类型	配置项	描述
系统漏洞/Web 漏洞	【导入漏洞】/【添加漏洞】	选择漏洞的添加方式。 • 导入漏洞：仅支持上传一个 1~20MB 的扩展名为.xlsx 的漏洞文件。 • 添加：手动配置漏洞参数。
	漏洞名称	进行渗透测试使用的漏洞名称。
	发现时间	漏洞的发现时间。
	漏洞评分	鼠标拖动漏洞的评分。
	CVE_ID	漏洞的 CVI ID。
	漏洞描述	漏洞的备注信息。
	解决方案	对漏洞的解决方案。
	附件上传	对漏洞的说明附件。
	【完成】	完成所有参数配置后，单击【完成】按钮，提交渗透测试任务。
系统漏洞	端口	漏洞影响的端口。

漏洞类型	配置项	描述
	协议	漏洞影响的协议。
	服务	漏洞影响的服务信息。
	操作系统/操作系统版本	漏洞影响的操作系统/操作系统版本。
	应用名称/应用版本	漏洞影响的应用名称/应用版本。
	漏洞详情	漏洞的详细信息。
Web 漏洞	请求方式	HTTP 的请求方式。
	URL	漏洞影响的 URL。
	问题参数	漏洞使用的请求参数。

6.2.1.7 新建网站信息收集任务

网站信息收集任务可以爬取网站的页面信息。

进入 **扫描管理 > 扫描任务管理** 页面，单击【新建任务】按钮，选择【网站信息收集】，配置网站信息收集任务参数即可。参数如表 6-20、表 6-11 和表 6-15 所示。

表6-20 网站信息收集任务

配置项	描述
预先探测目标可达	执行扫描任务前，先测试与目标的连通性。

6.2.1.8 新建产品漏洞预警任务

当情报的 CVE ID 和漏洞库某一个漏洞的 CVE ID 匹配时，TVM 以该情报的 CVE ID 关联的漏洞为模板对扫描目标进行情报验证，若匹配到系统和软件则该资产存在该情报漏洞。

进入 **扫描管理 > 扫描任务管理** 页面，单击【新建任务】按钮，选择【产品漏洞预警】，即可新建一个产品漏洞预警任务。产品漏洞预警任务参数如表 6-21 所示。

表6-21 产品漏洞预警任务

配置项	描述
任务名称	该扫描任务的名称，不允许为空和重名。 • 取值范围为 1~60 个字符。 • 不允许包含特殊字符，特殊字符的范围请以界面展示为准。
执行方式	• 立即执行：设备将执行即时扫描任务。 • 定时执行：设备将执行定时扫描任务。 • 周期执行：设备将执行周期扫描任务。
目标类型	扫描目标的 IP 地址的格式。

配置项	描述
资产列表	选择待扫描的主机资产或主机资产组。
漏洞列表	选择待进行情报验证的漏洞。
目标白名单	不执行扫描的目标，如何管理白名单请参见 扫描白名单管理。 全局级的目标白名单默认对所有任务生效。

6.2.1.9 新建漏洞验证任务

漏洞验证是指 TVM 针对漏洞下发一个主机/网站扫描任务，检测是否还存在该脆弱性。

进入 **扫描管理 > 扫描任务管理** 页面，单击【新建任务】按钮，选择【漏洞验证】，即可新建一个漏洞验证任务。漏洞验证任务参数如表 6-22 所示。

表6-22 漏洞验证任务

配置项	描述
任务名称	该扫描任务的名称，不允许为空和重名。 • 取值范围为 1~60 个字符。 • 不允许包含特殊字符，特殊字符的范围请以界面展示为准。
执行方式	• 立即执行：设备将执行即时扫描任务。 • 定时执行：设备将执行定时扫描任务。 • 周期执行：设备将执行周期扫描任务。
任务类型	待验证漏洞对应的扫描任务类型。
选择目标任务	选择需要进行漏洞验证的扫描任务及其扫描目标。

6.2.1.10 新建 POC 扫描任务

进入 **扫描管理 > 扫描任务管理** 页面，单击【新建任务】按钮，选择【POC 扫描】，即可新建一个 POC 扫描任务。POC 扫描任务参数如表 6-23、表 6-11、表 6-12、表 6-13、表 6-14 和表 6-15 所示。

表6-23 POC 扫描任务

配置项	描述
选择产品漏洞	需要验证的 POC 漏洞。如何管理 POC 请参见 POC 管理。
选择引擎	TVM 自动适配引擎或手动选择引擎。 手动选择引擎时，需要“选择引擎实例”，即执行 POC 扫描的引擎实例。如何管理引擎实例请参见 引擎实例。
预先探测目标可达	执行扫描任务前，先测试与目标的连通性。

6.2.1.11 新建资产探测任务

资产探测任务分为主机资产探测和网站资产探测，RSAS 探测到资产信息将自动记录至已有资产的信息中。

- 主机资产探测支持探测主机的存活、开放端口、服务应用等相关信息。
- 网站资产探测支持探测 Web 站点的组件框架、title、logo 等信息。

进入 **扫描管理 > 扫描任务管理** 页面，单击【新建任务】按钮，选择【资产探测】，即可新建一个资产探测任务。

- 主机资产探测任务参数的说明如表 6-1、表 6-3、表 6-4 和表 6-24 所示。

表6-24 主机资产探测任务

页面	配置项	描述
基本信息	扫描模板	在下拉列表框中，选择用于扫描的资产标记模板。
	关联网站探测资产	若主机开放 Web 端口（即存在 Web 应用），则 RSAS 会同时探测并记录 Web 资产（站点设备）的相关信息。
系统配置	关键页面总数	仅支持配置为“1”，表示仅对主机资产已开放的 Web 端口对应的 URL 进行探测。

- 网站资产探测任务参数的说明如表 6-11、表 6-3 和表 6-25 所示。

表6-25 网站资产探测任务

页面	配置项	描述
基本信息	关联主机探测资产	启用后，会将探测到的 Web 资产（站点设备）所在主机的 IP、系统、开放端口和服务应用等信息更新至资产管理模块。不启用则不更新。
系统配置	关键页面总数	仅支持配置为“1”，表示仅对 Web 资产对应的 URL 进行探测。
	插件超时限制	单个插件在指定时间内如果未正常结束，将会被调入引擎终止。 单位为秒，取值范围为 1～300 秒。
	调试模式	预防出现扫描任务异常时，可以配置该参数。记录扫描任务的执行信息，当任务执行异常，导出异常信息并发送给绿盟科技的技术支持人员进行错误分析。

6.2.2 任务管理

新建任务后，可以进行查询、编辑、删除、查看任务统计数据和其他管理操作。

任务统计数据

进入 **扫描管理 > 扫描任务管理** 页面，TVM 从不同维度统计当前扫描任务的数量。

- 状态监控：展示任务总数和不同状态扫描任务的数量。

- 任务类型分布：展示任务总数和不同类型扫描任务的数量。
- 任务量趋势：展示最近 7 天内，每天扫描任务数量的变化趋势。

其他管理操作

进入 **扫描管理 > 扫描任务管理** 页面，在任务列表区域，可以执行其他的扫描任务的管理操作，如表 6-26 所示。

表6-26 其他管理操作

操作	描述
单击“任务名称”	查看在线报表 可以查看扫描任务的在线报表，不同任务的报表内容不同，具体请以界面展示为准。
	查看审计日志、下载任务故障诊断日志 进入 **审计日志** 页签，可以查看审计日志 • 对于“异常”状态的任务，还可以查看异常原因。 • 若扫描任务的 **综述信息** 页签中失败数不为零，单击【下载任务故障诊断日志】，可以下载扫描失败目标的最近一次的任务信息。
	【同步风险】/【批量同步风险】至资产组 进入 **主机信息** 或 **站点列表** 页签；单击【同步风险】，将任务中所选资产的漏洞信息同步至所选资产组中相应的已有资产。若所选资产组中无匹配资产，请先在 资产列表 中新建相应资产。
	【同步产品漏洞】 进入 **漏洞列表** 页签；单击【同步产品漏洞】，将任务中所选资产的漏洞信息同步至 产品漏洞库。
	获取脆弱帐号的密码 进入 口令猜测任务的 **脆弱帐号** 页签，单击【获取密码】，输入当前 TVM 的登录帐号的密码，页面可以展示脆弱帐号用户名相应的登录密码。
单击“百分比”的当前状态	可以查看任务进度的详情。
单击“执行次数”	可以查看任务的主要信息和历史执行情况。
【展开】/【收起】	可以展开/收起“完成”状态的配置核查任务。展开后，可以在“执行结果”中查看其他的任务结果的统计信息。
【停止】/批量停止任务	可以停止“百分比”状态的扫描任务，终止相应任务；停止后，任务状态变更为“已停止”。
【重扫】/批量重扫任务	可以再次扫描“完成”、“已暂停”、“已停止”和“异常”状态的非导入扫描任务。重扫后，任务状态变更为“等待”。
【暂停】/批量暂停任务	可以暂停“百分比”状态的扫描任务；暂停后，任务状态变更为“已暂停”。 可以续扫“已暂停”状态的扫描任务。

6.3 批量任务管理

TVM 支持在本地编辑扫描任务策略模板后，将扫描任务策略批量导入 TVM，提高新建扫描任务的效率。可以先下载导入模板，按照模板要求编写后、批量导入任务。

进入 **扫描管理 > 批量任务管理** 页面，单击【导入】按钮，在虚线框中单击选择扫描任务策略文件或鼠标拖拽扫描任务策略文件至虚线框中即可导入任务。

- 导入扫描任务策略后，单击【执行】即可新建相应任务，后续可以进行 任务管理。
- 导入扫描任务策略后，还可以进行删除的操作。

6.4 扫描设备管理

在扫描设备管理模块，可以对安全设备和引擎实例进行管理。

说明	对于不同版本的不同设备，对设备管理各功能支持的情况不同，具体的支持情况请以页面展示为准。

6.4.1 设备管理

设备是指绿盟科技的安全设备（如 RSAS）和第三方的扫描设备，用于向 TVM 上报数据。TVM 可以管理 RSAS、BVS、WVSS 设备。

6.4.1.1 设备接入

通过 TVM 添加设备

进入 **扫描管理 > 扫描设备管理** 页面，单击【添加设备 > 添加绿盟设备/添加三方设备】按钮，即可接入一台安全设备。添加安全设备的参数说明如表 6-27 所示。

表6-27 添加设备

设备类型	配置项	描述
绿盟设备&三方设备	设备名称	安全设备的名称。
	设备 IP/设备接口地址	安全设备的 IP 地址。
	设备组	安全设备所属的设备组。
	描述	安全设备的说明信息。
第三方设备	设备厂商	第三方设备所属的厂商。
	设备版本	第三方设备的版本。
	扫描类型	支持扫描任务的类型。

设备类型	配置项	描述
	最大任务并发数	同一时间内，第三方设备支持执行扫描任务的最大数目。
	用户名&密码	登录第三方设备的用户名和密码。

通过设备端向 TVM 注册

以 RSAS 为例，登录 RSAS，进入 **联动管理 > 安全中心** 页面，联动配置如图 6-1 和表 6-28 所示。

图6-1 RSAS 与 TVM 联动配置

表6-28 RSAS 与 TVM 联动配置

配置项	描述
本地 IP 地址	与 TVM 联动的 RSAS 的 IP 地址。
企业安全中心地址	TVM 的管理口的 IP 地址。
端口	与 TVM 通信的端口号，目前仅支持 443。
版本	目前仅支持 TVM/ISOP。
启动	勾选。

6.4.1.2 设备组

为方便分类管理设备，TVM 提供设备组功能。

进入 **扫描管理 > 扫描设备管理 > 设备管理** 页面，在“设备组”区域，选中父设备组后，单击添加设备组 ＋，配置“设备组名称”即可新建子设备组，具体请参见界面要求。新建子设备组后，可以进行编辑和删除操作。

6.4.1.3 管理设备

进入 **扫描管理 > 扫描设备管理 > 设备管理** 页面，可以对与 TVM 进行联动的安全设备进行管理，如表 6-29 所示。

表6-29 管理设备

操作	描述
筛选设备	单击“设备组”、“设备状态”、“设备类型”，在设备列表中筛选设备。
查询设备	配置查询条件，可以查看指定设备。
单击“设备名称”	• 查看设备的详细信息。 • 配置“设备名称”、“NAT IP”、“首选/备选 DNS 服务器”、“备注”。 • 选择设备的“所属组”。 • 配置“设备权限”：公开后，所有帐号可以查看和使用该设备；私有后，只有被选择的帐号可以查看和使用该设备。 • 配置允许设备执行扫描任务的“可扫描范围”，即扫描目标的范围。 • 配置设备并发扫描时的“最大并发扫描任务数”、“最大并发扫描主机数”和“最大任务并发插件数”。
【监控】	可以查看设备的性能趋势。 • 单击【今天/7 天/30 天/90 天】，可以查看相应时间范围内的性能指标的变化趋势图。 • 将鼠标置于图中节点处，可以查看具体的占用率和流量数据。
删除/批量删除设备	取消与设备的联动。
【更多 > 设备配置】	可以查看设备的网络配置信息。
【更多 > 同步设备】/批量同步设备	可以同步设备信息至 TVM。
【更多 > 启用/禁用设备】	可以启用/禁用设备。
【更多 > 登录设备】	跳转至设备的登录界面，登录后可以对设备进行管理。
【更多 > 查看证书】	可以查看设备证书详情。
【更多 > 重启设备】	立即重启相应设备。
批量配置 DNS 接口	批量配置设备的“首选/备选 DNS 服务器”。

6.4.1.4 设备升级

可以升级的设备及版本如表 6-30 所示。

表6-30 可以升级的设备及版本

设备	版本
BVS	V6.0R01F03SP13 以上版本
RSAS	V6.0R02F03SP13 以上版本
RSAS(XC)	V6.0R02F01.2101 及以上版本

设备	版本
WVSS	V6.0R03F01SP19 以上版本

升级管理

进入 **扫描管理 > 扫描设备管理 > 设备管理** 页面，单击【设备升级】按钮，选择页签 **升级管理**，进入升级管理页面。

- 可以查看支持升级的设备的状态、版本和可用升级包信息，如图 6-2 所示。

图6-2 升级管理

- 可以升级在线设备，如表 6-31 所示。TVM 会周期性执行所有（可选）操作，用户可以根据需要立即执行相应操作。

表6-31 升级设备

步骤	操作	描述
1	升级站点/ 配置升级站点	设备获取升级包的方式。 • 在线升级：通过绿盟科技的升级站点获取升级包。 • 平台托管：通过 TVM 获取升级包。
2	（可选）【同步设备】	同步设备信息至 TVM。
3	（可选）【更新升级文件】	适用于“平台托管”场景，手动更新 TVM 中升级包描述文件，即 XML 文件。
4	（可选）在线更新设备升级包	适用于“平台托管”场景，从绿盟科技的升级站点更新设备升级包至 TVM。
5	【升级】	手动升级设备。

升级包管理

进入 **扫描管理 > 扫描设备管理 > 设备管理** 页面，单击【设备升级】按钮，选择页签 **升级包管理**，可以查看在 TVM 中已存在的设备升级包的统计数据、升级包清单和升级包详情。

6.4.2 引擎实例

引擎实例将引擎和设备进行关联，用于执行 POC 扫描任务。

进入 **扫描管理 > 扫描设备管理 > 引擎实例** 页面，单击【新增】按钮，即可新建一个引擎实例。引擎实例参数如表 6-32 所示。新建引擎实例后，可以进行查询、查看、编辑和删除的操作。

表6-32 引擎实例

配置项	描述
引擎实例名称	引擎实例的名称。
引擎名称	引擎的名称。如何管理引擎请参见 引擎管理。
引擎版本	引擎的版本。如何管理引擎请参见 引擎管理。
实例名称	引擎关联的设备。如何管理设备请参见 设备管理。
引擎实例描述	引擎实例的说明信息。

6.5 任务配置

任务配置用于管理扫描任务的部分执行策略。

漏洞智能分析配置

漏洞处置 模块根据漏洞智能分析配置对扫描结果中的漏洞自动进行误报消除。

基于资产库

开启后，TVM 会以选中资产组中资产的端口和服务信息为标准，对扫描结果中的漏洞进行误报消除。

进入 **扫描管理 > 任务配置 > 漏洞智能分析配置 > 基于资产库** 页面，“启用”并指定“资产组”即可。

基于黑名单规则

配置后，TVM 以配置的规则为标准，对扫描结果中的漏洞进行误报消除。

进入 **扫描管理 > 任务配置 > 漏洞智能分析配置 > 基于黑名单规则** 页面，配置“软件名称”和“软件版本”，选择“协议”即可。新建规则后，可以进行删除操作。

- 【单条新建】：新建一条规则。
- 【批量新建】：最多可以新建十条规则。

扫描白名单管理

若扫描任务中的扫描对象包含扫描白名单中的信息，则不对其进行扫描。

进入 **扫描管理 > 任务配置 > 扫描白名单管理** 页面，单击【新建】按钮，配置扫描白名单参数即可新建扫描白名单。扫描白名单参数如表 6-33 所示。新建扫描白名单后，可以进行编辑和删除操作。

表6-33 扫描白名单参数

配置项		描述
白名单名称		扫描白名单的名称，具体请参见界面要求。
生效类型		• 全局级：admin 可以管理所有的资产和扫描任务。其他帐号可以使用全局的白名单执行扫描任务。 • 用户级：所有帐号仅可以管理权限内的资产和扫描任务。
类型		白名单内容所属类型。
资产	资产类型	资产的类型。
	目标类型	目标资产的地址格式。
	目标方式	必须扫描的资产。 • 选择资产：适用于全局级和用户级。 • 手动输入：适用于全局级。
日期	目标时间	必须扫描的时间段。
描述		对扫描白名单的说明信息。

端口修正配置

进入 **扫描管理 > 任务配置 > 端口修正配置** 页面，单击【新建】按钮，配置端口修正参数，即可新建端口修正信息。端口修正参数说明如表 6-34 所示。新建端口修正信息后，可以进行编辑和删除操作。

表6-34 端口修正参数

配置项	描述
名称	填写端口修正的名称。最多支持 30 个字符。
生效类型	• 全局级：仅支持 admin 创建，对整个系统默认生效。 • 用户级：下发任务时，用户只能选择自己创建的端口配置。
端口配置	填写要修正的端口号及服务名称。端口取值范围为 1~65535。
描述	填写端口修正的描述信息。

7 流程处置

本章主要包含以下内容：

功能	描述
工单管理	介绍如何管理各类工单。
流程管理	介绍如何管理各类流程。
通知策略	介绍如何管理各类通知策略。

7.1 工单管理

统计维度

TVM 按照不同维度呈现工单的统计数据，具体如表 7-1 所示。

表7-1 工单管理页签

页签	统计维度
待办工单	需要当前帐号处置的工单。
已办工单	当前帐号已经处置的工单。
已完结工单	当前帐号新建且“流程状态”为完成的工单。
我的申请	当前帐号新建的所有工单。
草稿箱	新建的工单，尚未启动。启动后，移至“待办工单”页签。

工单处置流程

工单处置流程如表 7-2 所示。

表7-2 工单处置流程

步骤	页签	动作
1	我的申请/待办工单/已办工单/草稿箱	新建工单
2	草稿箱	生效工单 单击操作栏的【启动】，下发工单。
3	待办工单	处理工单 3.1 接收工单：单击操作栏的【处理】，对漏洞进行排查修复处置、确认工单流转记录后，给出工单意见，【提交】工单即可。
	已办工单	可选 3.2 撤办工单：单击操作栏的【撤办】，撤回已处理工单，重新【处理】。 3.3 催办工单：单击操作栏的【催办】，提醒下一环节跟进工单。
4	已完结工单	查看工单 单击操作栏的【详情】，查看工单处置详情。

新建工单

进入 **流程处置 > 工单管理** 页面，单击【新增】按钮，即可新建一个工单。工单参数如表7-3 所示。新建工单后，进入 **草稿箱** 页签，单击操作栏的【启动】，即可下发工单；还可以进行查询、查看详情、编辑和删除的操作。

表7-3 工单参数

配置类别	配置项	描述
基本信息	工单名称	工单的名称。
	优先级	工单的处置优先级。
	流程类型	工单适用的流程所属的类型。可选项有预置、自定义。
	流程名称	根据所选的流程类型，选择一个对应的流程。流程类型为“预置”的工单如下： • 产品漏洞验证：验证产品漏洞是否真实有效。 • 漏洞专项排查：对资产是否受某些漏洞进行排查。 • 漏洞处置修复：对资产上的漏洞修复工作进行指派。 • 产品漏洞核验：对产品漏洞状态进行核验。 • 漏洞排查验证：对资产已排查发现的漏洞进行再次漏洞验证。 • 漏洞修复核验：对资产上的漏洞是否修复进行核验。 • 产品漏洞插件开发：对产品漏洞插件进行开发。 • 漏洞排查闭环：对资产预警漏洞及未知漏洞进行排查修复闭环。 • 漏洞跟踪闭环：对资产已知漏洞进行跟踪修复闭环。 关于预置流程和自定义流程的管理方法，请参见 流程管理。

配置类别	配置项		描述
	数据来源		• 漏洞：勾选后，流程配置中可添加漏洞处置列表中的漏洞，用于已知漏洞跟踪修复闭环。 • 产品漏洞+资产：勾选后，流程配置中可添加平台已有资产与产品漏洞，用于排查已知资产的未知漏洞。 • 口令字典模板+资产：勾选后，流程配置中可添加平台已有资产与口令字典模板，用于排查已知资产的弱口令漏洞。
	附件		工单关联的附件。
	说明		工单的描述信息。
流程配置	资产列表		对于上一步选择的部分流程，需要选择本工单要处置的主机资产或网站资产。
	漏洞列表		选择本工单需要处置的主机漏洞或网站漏洞。
规则配置	工单要求完成时间		工单处置的截止时间。
	通知设置		完成工单处置每个环节后的通知方式。可选项有到期通知、延期通知。
	执行次数		到期通知和延期通知的执行方式： • 只执行一次 • 重复执行
	只执行一次	到期前	通知设置为“到期通知”时，需要配置提前多久发送通知。单位可选项有天、小时、分钟。
		延期后	通知设置为“延期通知”时，需要配置延期多久后发送通知。单位可选项有天、小时、分钟。
	重复执行	延期后	通知设置为“延期通知”时，需要配置初次执行延期多久后发送通知。单位可选项有天、小时、分钟。
		到期前每隔	通知设置为“到期通知”时，需要配置到期前多久发送通知。单位可选项有天、小时、分钟。
		延期后每隔	通知设置为“延期通知”时，需要配置延期后每隔多久发送通知。单位可选项有天、小时、分钟。
		最多执行	延期后，发送通知的次数上限。
	执行时间		选择具体的通知时间。
	通知对象		支持以下三类通知对象： • 当前环节处理人：通知流程当前环节的处理人。 • 流程环节选择：选择流程的其他环节处理人作为通知对象。 • 组织架构选择：选择用户组及组内用户作为通知对象。
	通知方式		支持以下两种通知方式： • 待办提醒：通过待办工单来通知。

配置类别	配置项	描述
		• 邮件通知：通过邮件来通知，需要配置邮件模板和邮件通知内容。关于邮件模板的配置方法，请参见 BSA 用户手册中的邮件配置。
预览	-	在线预览工单所有配置信息。

7.2 流程管理

进入 **流程处置 > 流程管理** 页面，初始状态下，默认显示预置的漏洞处置流程，如图 7-1 所示。用户也可以自定义漏洞处置流程，同时支持流程启用/禁用、查看详情、导入流程、导出流程、修改和删除等操作。

图7-1 漏洞处置流程管理

说明	预置的漏洞处理流程，不支持修改和删除。

新建流程

新建漏洞处理流程的方法包括两种：流程复制新建、手动新建流程。

流程复制新建

在漏洞处置流程列表中，单击操作栏的【复制新建】，即可在对应流程的基础上进行修改，另存为新的漏洞处置流程。

手动新建流程

单击【新增】按钮，绘制漏洞处置流程，配置流程参数；单击【保存】按钮，即可新建自定义漏洞处置流程。漏洞处置流程参数说明如表 7-4 所示。

漏洞处置流程绘制时，从工具栏中拖拽节点图标至画布后，单击节点图标，即可使用浮现的工具图标进行连线等操作。工具图标说明如表 7-5 所示。

表7-4 漏洞处置流程参数

配置项		描述
名称		• 流程名称：在绘制图中不选中组件的状态下，自定义当前流程名称。 • 组件名称：在绘制图中单击某个组件，自定义当前节点/分支/用户任务名称。
流程描述		填写当前流程的描述信息。
关联表单		选择当前流程关联的流程表单。可选项有通用、产品漏洞处置、产品漏洞插件开发、系统漏洞处置。
用户任务	环节参与者	• 办理人：工单直接流转到对应人员。 • 候选组：组内的所有人员均会收到工单，谁签收谁办理。 • 允许转办/允许催办：勾选后，将允许所选的环节参与者转办/催办工单。
	环节操作	环节参与者有权进行的操作。

表7-5 漏洞处置流程绘制的工具图标

图标	描述
	当前节点后添加结束节点。本图标不适用于结束节点。
	当前节点后添加用户任务节点。本图标不适用于结束节点。
	当前节点后添加分支节点。本图标不适用于结束节点。
	修改当前节点的类型。不同的节点，可以修改的节点类型也有所不同。
	从画布中移除当前节点。
	连接线，将当前节点与关联节点连接起来。

发布流程

本功能仅支持自定义流程。

自定义流程新建成功后，单击操作栏的【发布】，即可发布对应的自定义流程。发布后，不支持删除。

导入流程

单击【导入】按钮，选择流程文件后，进入流程的绘制页；定义流程名称、流程描述和关联表单；单击【保存】按钮，完成漏洞处置流程的导入。

导出流程

单击操作栏的【导出】，即可将对应的漏洞处理流程导出为 bpmn 文件。

流程启用/禁用

单击操作栏的【禁用】或【启用】，即可控制对应漏洞处置流程的状态。

新建工单时，不支持选择禁用状态的漏洞处置流程。

7.3 通知策略

用户可以自定义不同流程的通知策略和通知内容。

通知策略

进入 **流程处置 > 通知策略 > 通知策略** 页面，单击【新建策略】按钮，配置通知策略参数，即可针对所选流程新建一个通知策略。通知策略参数说明如表 7-6 所示。

通知策略新建后，可以进行启用/批量启用、停用/批量停用、查看详情、编辑、删除和查询等操作。

表7-6 通知策略参数

配置项		描述
通知策略名称		填写通知策略的名称。
选择流程名		选择一个使用该通知策略的预置流程或已发布的自定义流程。 关于预置流程和自定义流程的管理方法，请参见 流程管理。
通知设置		选中该流程的通知方式。可选项有到期通知、延期通知。
执行次数		到期通知和延期通知的执行方式： • 只执行一次 • 重复执行
只执行一次	到期前	通知设置为“到期通知”时，需要配置提前多久发送通知。单位可选项有天、小时、分钟。
	延期后	通知设置为“延期通知”时，需要配置延期多久后发送通知。单位可选项有天、小时、分钟。
重复执行	到期前	通知设置为“到期通知”时，需要配置到期前多久发送通知。单位可选项有天、小时、分钟。
	延期后	通知设置为“延期通知”时，需要配置延期后每隔多久发送通知。单位可选项有天、小时、分钟。

配置项	描述
执行时间	选择具体的通知时间。
通知对象	支持以下三类通知对象： • 当前环节处理人：通知流程当前环节的处理人。 • 流程环节选择：选择流程的其他环节处理人作为通知对象。 • 用户选择：选择用户组及组内用户作为通知对象。
通知方式	支持以下三种通知方式： • 待办提醒：通过待办工单来通知。 • 邮件通知：通过邮件来通知。关于邮件内容的配置方法，请参见 通知内容。 • 站内消息：通过站内消息来通知。关于站内消息的配置方法，请参见 通知内容。
通知策略描述	设置自动发送的通知内容，支持以下两种方式： • 勾选“自动生成”：根据通知设置自动生成通知内容。 • 不勾选“自动生成”：自定义通知内容。

通知内容

进入 **流程处置 > 通知策略 > 通知内容** 页面，单击【新建内容】按钮，配置通知内容参数，即可新建一个邮件通知或站内消息通知内容。通知内容参数说明如表 7-7 所示。

通知内容新建后，可以进行编辑、删除、查询和查看详情操作。

表7-7 通知内容参数

配置项	描述
通知消息类型	选择通知消息的发送方式。可选项是邮件。
通知内容标题	根据所选的通知消息类型，填写通知标题。
通知内容	根据所选的通知消息类型，填写通知内容。可将“示例”内容复制粘贴过来进行修改，作为通知内容。

8 报表管理

本章主要包含以下内容：

功能	描述
统计分析	介绍如何进行数据的统计分析。
报表任务	介绍如何管理报表任务。
报表配置	介绍如何管理报表模板。

8.1 统计分析

TVM 支持通过任务维度、资产分组维度、时间维度，进行资产风险数据的统计分析。

8.1.1 任务对比

任务对比指将两个“系统扫描”、“网站扫描”或“资产发现”任务进行对比，分析任务参数和结果数据间的差异。

新建任务对比分析任务

进入 **报表管理 > 统计分析 > 任务对比** 页面，单击【创建对比】按钮，配置任务对比分析任务参数即可新建一个对比任务。对比任务参数如表 8-1 所示。

表8-1 对比任务参数

配置项	描述
对比任务名称	该对比任务的名称，具体请参见界面要求。
对比任务类型	支持对“系统扫描”、“网站扫描”或“资产发现”任务进行对比分析。
基线任务	被对比的任务。以此任务为基线，分析“对比任务”相较于“基线任务”的差异。
对比任务	与“基线任务”进行差异分析的任务。 • 可以添加多个任务，无个数限制。

配置项	描述
	• 每个“对比任务”分别与“基线任务”进行对比。
报表类型	目前仅支持.html 格式的在线报表和离线报表。
描述	对比任务的说明信息。

管理对比任务

新建对比任务后，还可以执行除删除外的其他管理操作，如表 8-2 所示。

表8-2 管理对比任务

操作	描述
【预览】	查看在线报表。 报表中的对比结果是以“对比任务”相对于“基线任务”的差异进行统计的。
【下载】	下载离线报表。 报表中的对比结果是以“对比任务”相对于“基线任务”的差异进行统计的。
【更多 > 重新执行】	重新执行对比任务。

8.1.2 分组统计

分组统计指将 1 个资产属性（视图属性）中的多个子组进行对比，分析多个子组间资产脆弱性、漏洞情况和不合规情况的统计信息。

新建分组统计分析任务

进入 **报表管理 > 统计分析 > 分组统计** 页面，单击【创建分析】按钮，配置分组统计分析任务参数即可新建一个分析任务。分析任务参数如表 8-3 所示。

表8-3 分析任务参数

配置项	描述
分析任务名称	该分析任务的名称，具体请参见界面要求。
执行方式	选择任务的执行方式。
资产类型	被对比的资产类型。
资产视图	在视图属性下，选择一个拥有子组的父节点。 如何管理视图属性请参见属性管理。
视图节点	选择进行统计分析的多个子组，不限制子组个数。 以当前子组情况进行统计分析。
描述	分析任务的说明信息。

管理分析任务

新建分析任务后，还可以进行除删除外的其他管理操作，如表 8-4 所示。

表8-4 管理分析任务

操作	描述
单击“分析任务名称”	查看在线报表。 报表中的分析结果是以当前每个子组的情况进行统计的。
【展开】/【收起】	可以在“视图节点”中查看参与统计分析的子组。
【重新执行】	重新执行分析任务。

8.1.3 时间维度对比

时间维度对比用于分析不同时间点同一资产属性（视图属性）的资产脆弱性、漏洞情况和不合规情况的统计信息。

新建时间对比分析任务

进入 **报表管理 > 统计分析 > 时间维度对比** 页面，单击【创建对比】按钮，配置时间对比任务参数即可新建一个任务。时间对比任务参数如表 8-5 所示。

表8-5 时间对比任务参数

配置项	描述
对比任务名称	该时间对比任务的名称，具体请参见界面要求。
资产范围	进行时间对比的资产对象。
基线日期	被对比的日期。以此时间为基线，分析“对比日期”相较于“基线日期”的差异。
对比日期	与“基线日期”进行差异分析。
描述	对比任务的说明信息。

管理对比任务

新建时间对比任务后，还可以进行除删除外的其他管理操作，如表 8-6 所示。

表8-6 管理分析任务

操作	描述
单击“对比任务名称”	查看在线对比分析报表，如环比修复率、资产和漏洞的变化情况等。

操作	描述
【重新执行】	重新执行分析任务。

8.2 报表任务

进入 **报表管理 > 报表任务** 页面，单击【新建】按钮，配置报表任务参数即可。报表任务参数如表 8-7 所示。新建报表任务后，还可以对其进行删除和如表 8-8 所示的操作。

表8-7 报表任务参数

报表类型	配置项	描述
资产风险报表	资产范围	单击后，选择需要对其生成报表的资产/资产属性。
	报表内容	综述信息默认必选，可以选择是否包括详细信息。
	报表格式	默认 HTML 格式，还可选择生成 EXCEL 格式报表。
主机扫描综合报表	任务选择	单击后，选择需要对其生成报表的任务。
	报表格式	默认 HTML 格式，还可选择生成 EXCEL 格式报表。
配置核查报表	任务选择	单击后，选择需要对其生成报表的任务。
	报表格式	默认 HTML 格式，还可选择生成 EXCEL 格式报表。
漏洞处置报表	处置单状态	对相应处置单状态的工单内容生成报表。 单击后，选择需要对其生成报表的处置单状态。
	资产范围	单击后，选择需要对其生成报表的资产/资产属性。
	起止时间	对相应时间内的工单内容生成报表。 单击后，选择需要对其生成报表的时间范围。
	报表格式	默认 EXCEL 格式。
口令猜测报表	任务选择	单击后，选择需要对其生成报表的任务。
	报表格式	默认 HTML 格式，还可选择生成 EXCEL 格式报表。
网站扫描报表	任务选择	单击后，选择需要对其生成报表的任务。
	报表格式	默认 HTML 格式，还可选择生成 EXCEL 格式报表。
资产发现报表	任务选择	单击后，选择需要对其生成报表的任务。
	报表格式	默认 HTML 格式，还可选择生成 EXCEL 格式报表。
预警任务报表	任务选择	单击后，选择需要对其生成报表的任务。
	报表格式	默认 EXCEL 格式。
POC 扫描报表	任务选择	单击后，选择需要对其生成报表的任务。
	报表格式	默认 HTML 格式，还可选择生成 EXCEL 格式报表。

报表类型	配置项	描述
漏洞验证报表	任务选择	单击后，选择需要对其生成报表的任务。
	报表格式	默认 EXCEL 格式。
主机资产探测报表/网站资产探测报表	任务选择	单击后，选择需要对其生成报表的任务。
	报表格式	默认 EXCEL 格式。
N/A	任务名称	报表任务的名称，具体请参见界面要求。
N/A	描述	报表任务的说明信息，具体请参见界面要求。
N/A	发送邮件	选择“是”，系统将生成的报表发送到指定邮箱。支持填写多个邮箱地址，用空格符或英文逗号分隔。

表8-8 管理报表任务

操作	描述
单击“任务名称”，查看任务	查看报表任务详情，包括任务基本信息（执行方式、报表类型、任务目标、报表格式、描述）。 查看/删除/下载任务执行记录。
【重新执行任务】	再次执行“执行成功”状态的报表任务。
【下载】/报表批量导出	下载报表任务生成的所有报表下载到本地。

8.3 报表配置

LOGO 配置

进入 **报表管理 > 报表配置 > LOGO 配置** 页面，可以自定义报表的 LOGO。

报表类型配置

进入 **报表管理 > 报表配置 > 报表类型配置** 页面，可以管理是否启动相应的报表模板。

9 知识建设

本章主要包含以下内容：

功能	描述
知识概览	介绍如何查看当前的统计数据。
知识库	介绍如何管理各类脆弱性知识。
模板管理	介绍如何管理各类脆弱性模板。
运营经验库	在运营经验库中，可以管理用户自定义的漏洞修复方案和漏洞误报任务。
知识配置	介绍如何管理知识库的相关配置。

9.1 知识概览

进入 **知识建设 > 知识概览** 页面，可以查看各类知识的统计数据，如表 9-1 所示。

表9-1 知识概览

区域名称	描述
知识大类分布	可以查看 知识库 内各类知识的总数。
产品漏洞近期新增趋势图	可以查看在“时间周期”内，相应漏洞“类型”漏洞的个数及变化趋势。
产品漏洞数近期来源趋势	可以查看在“时间周期”内，相应漏洞“类型”漏洞的来源厂商及其发现漏洞个数。
情报近期新增趋势	可以查看在“时间周期”内，情报的个数及变化趋势。
口令字典近期新增来源分布	可以查看在“时间周期”内，口令字典的来源及其口令字典的个数。
资产标记统计趋势	可以查看在“时间周期”内，资产标记纠偏结果的个数及变化趋势。
插件近期新增来源趋势	可以查看在“时间周期”内，指纹插件的来源及其插件的个数。

9.2 知识库

知识库用于管理扫描任务中用到的脆弱性信息。

9.2.1 产品漏洞库

在产品漏洞库中，可以管理所有主机漏洞和网站漏洞，主机漏洞与网站漏洞的管理方式类似，这里以主机漏洞为例进行介绍。

管理分类

可以按照需要对漏洞进行分类管理。

进入 **知识建设 > 知识库 > 产品漏洞库 > 主机** 页面，单击左侧分类切换旁的 ⋮ > ⊕，即可新建一个漏洞分类。

- 新建漏洞分类后，可以进行删除分类、添加/编辑/删除子分类的操作。
- 删除分类后，漏洞自动归属至父分类中。

添加漏洞

在主机漏洞列表中，可以管理所有主机漏洞。

进入 **知识建设 > 知识库 > 产品漏洞库 > 主机** 页面，可以通过如下方法录入主机漏洞：

- 提取漏洞。
- 单击【导入】按钮，批量导入主机漏洞。
- 单击【新建 > 主机漏洞】按钮，即可新建一个主机漏洞。主机漏洞参数如表 9-2 所示。
- 挖掘（渗透测试任务）：完成渗透测试任务后，同步产品漏洞。
- 报告提取（第三方任务同步）：导入启明天镜设备的扫描任务后，同步产品漏洞。

表9-2 主机漏洞参数

配置项		描述
基本属性	漏洞名称	漏洞的名称，长度不能超过 64 字符。 不能包含\ / < > & " ' ` # * ^ ~ | , : ; ? ( ) [ ] % $特殊字符。
	CWE 分类	漏洞所属的 CWE 分类。
	来源厂商	漏洞的来源厂商。
	脆弱性值	该漏洞的脆弱性值，值越大风险越高。
	描述	对漏洞的说明信息。
高级属性	漏洞分类	该漏洞所属漏洞分类。一个漏洞可以归属于多个漏洞分类。
	检测类型/检测方式	检测该漏洞的方法。
	发布组织	漏洞的发布者。可以多选。
	影响软件	用来 新建产品漏洞预警任务 任务，匹配受该漏洞影响的资产的操作系统和软件。

配置项		描述
	标签	用户自定义的漏洞标签。单击【添加标签】，可以新建标签。
	附件	该漏洞涉及的附件。
	MS/CVE/CNCVE/CNNVD/CNVD 编号	世界知名漏洞知识库中漏洞的编号。
	发现日期/发布日期	漏洞的发现/发布时间。
	修复建议	漏洞的具体解决方案。

管理漏洞

新建漏洞后，可以进行查看详情、编辑、删除和如表 9-3 所示的操作。

表9-3 管理漏洞

配置项	描述
查看统计数据	在 

区域，可以查看各脆弱性等级漏洞的总数。 |
| | 在 

区域，可以查看各产品漏洞状态漏洞的总数，产品漏洞状态如表 9-4 所示。 |
查询设备	在漏洞分类区域，选择漏洞分类，在主机漏洞列表中展示该分类下的主机漏洞。
	单击统计数据区域的各统计项，在主机漏洞列表中展示相应的漏洞。
	配置查询条件，查询指定的漏洞。
标签管理	单击【管理 > 标签管理】按钮，添加或删除漏洞标签。
厂商管理	单击【管理 >厂商管理】按钮，添加或删除厂商标签。
修复建议	单击操作栏的【修复建议】，编辑漏洞的具体解决方案。
上报漏洞	将省侧平台的产品漏洞主动上报到部侧平台。
批量新建漏洞误报	请参见 漏洞误报库。

表9-4 产品漏洞状态

产品漏洞状态	描述
未验证	未对产品漏洞是否真实有效进行验证。
已验证有效	产品漏洞验证有效。
已验证无效	产品漏洞验证无效。
已核验有效	产品漏洞核验有效。

产品漏洞状态	描述
已核验无效	产品漏洞核验无效。

9.2.2 口令字典库

在扫描过程中安全设备将根据密码字典中的内容尝试登录目标设备，若目标设备的登录用户名和密码与密码字典中的内容匹配，则认为目标设备存在脆弱帐号。

密码字典包括系统密码字典（包含一些常见的脆弱帐号，不可编辑和删除）和用户自定义密码字典。

进入 **知识建设 > 知识库 > 口令字典库** 页面，单击【添加】按钮，配置密码字典参数，即可新建自定义密码字典。参数说明如表 9-5 所示。

- 新建密码字典后，还可以进行查看、编辑和删除操作。
- 可以通过勾选/不勾选“类别选择”或“所属”来自定义页面中展示的内容。

表9-5 密码字典参数

配置项	描述
字典名称	由英文字母、数字或中文、-、_字符组成，区分大小写。取值范围为 1~64 个字符。新建字典名称不允许与已有字典名称相同。
类别	• 用户名字典：用于扫描具有风险的弱用户名称。 • 密码字典：用于扫描具有风险的密码。 • 用户名密码组合字典：用于扫描具有风险的用户名称及其密码。
字典内容	• 单击⊕，添加字典内容。最多可输入 100 个字典内容。 • 用户名密码组合字典内容格式为“用户名:密码”。例：administrator:nsfocus。
字典文件	支持导入扩展名为.txt 的字典文件。 在字典文件中，每行一个脆弱帐号，格式和要求与“字典内容”相同。
描述信息	对字典的说明信息。

9.2.3 配置模板

配置模板是配置核查任务的基础，包含完善详细的安全配置检查点及其权重。

新建模板分组

为了方便分类管理配置模板，TVM 支持自定义模板分组。

进入 **知识建设 > 知识库> 配置模板** 页面，单击【管理分组】按钮，单击【新建模板分组】按钮，配置“分组名称”、“描述”、“分组类型”即可，具体请参见界面要求。新建模板分组后，还可以进行编辑和删除操作。

新建配置模板-另存为

进入 **知识建设 > 知识库> 配置模板** 页面，单击某个模板操作栏的【另存为】，配置模板参数即可。配置模板参数说明如表 9-6 所示。新建配置模板后，还可以进行查询、查看详情、编辑和删除操作。

表9-6 配置模板参数

配置项		描述
基本信息	模板名称	配置模板的名称，不允许重名，具体请参见界面要求。
	模板分组	该配置模板所属的分组。
配置检查项	配置检查项	用于检查目标主机是否合规，检查结果将显示在报表中。 TVM 根据配置检查项列表中的先后顺序依次对目标主机进行检查。 可以查看和删除检查项。
附录检查项	附录检查项	附录检查项的目的并不是用来检查目标主机是否合规，而是通过附录检查项获取目标主机的相应信息，然后将其作为“辅助信息”展示在报表中。 可以删除附录检查项。

公开/取消公开模板

默认情况下，每个帐号只能管理自身的自定义配置模板，将自定义模板公开后，其他帐号可以查看和使用该模板。

进入 **知识建设 > 知识库> 配置模板** 页面，单击自定义模板操作栏中的“公开/取消公开”，可以公开/取消公开该自定义模板。

9.2.4 情报管理

随着安全攻防节奏的提升，传统方式的漏洞扫描和网站安全监测已经难以跟上漏洞发掘和 Web 安全事件变化的速度，因此 TVM 提供了以快速发现和响应为目的的情报预警功能。

9.2.4.1 情报

情报用于发布最新的漏洞。

TVM 支持通过绿盟 NTI 获取和手动录入两种方式，实时获取行业的风险情报。

 说明	无法再获取本月以前的情报。

NTI 获取情报

周期性自动获取情报

进入 **知识建设 > 知识库 > 情报管理 > 情报** 页面，单击【配置】按钮，配置参数即可。情报配置参数说明如表 9-7 所示。

表9-7 情报配置参数

配置项	描述
NTI 自动获取	• 是：周期性自动从 NTI 获取情报。 • 否：可以手动从 NTI 获取情报。
自动获取周期	从 NTI 自动获取情报的周期。
NTI 情报 KEY 过期时间	过期后，不支持从 NTI 获取情报。

立即获取情报

进入 **知识建设 > 知识库 > 情报管理 > 情报** 页面，单击【更新】按钮，立即从 NTI 同步漏洞情报至 TVM。

查看情报获取日志

进入 **知识建设 > 知识库 > 情报管理 > 情报** 页面，单击【日志】按钮，查看或删除情报获取日志即可。

手动录入情报

进入 **知识建设 > 知识库 > 情报管理 > 情报** 页面，单击【录入】按钮，配置漏洞情报参数。漏洞情报参数说明如表 9-8 和表 9-9 所示。

表9-8 漏洞情报参数基础信息

配置项	描述
情报名称	情报的名称，具体请参见界面要求。
情报描述	对情报的描述，具体请参见界面要求。
脆弱性等级	该情报的脆弱性等级。
应急情报	是否是目前用户关注度较高的情报。
是否公开	该情报是否对非登录帐号可见。 公开后，非登录帐号也可以看到该情报。

表9-9 漏洞情报参数高级信息

配置项	描述
CVE ID/CWE ID/CNNVD ID/APACHE ID/ BUGTRAP ID/ CISCO ID/X-Force ID	世界知名漏洞知识库中漏洞的编号。
CVSS 评分	漏洞的 CVSS 分数。
发现时间	漏洞的发现时间。
漏洞发布者	漏洞的发布者。
受影响软件	用来匹配受该漏洞影响的资产。 单击【添加】按钮，在弹出的对话框中，配置相关参数，单击【完成】按钮即可。
POC	该情报是否有 POC。
解决方案	漏洞的具体解决方案。
参考网址	漏洞信息的参考链接。

情报导入

TVM 支持导入 NTI 离线情报，可以从绿盟科技的软件升级网站通过 TVM 的证书获取离线情报文件。请联系绿盟科技的技术支持人员获取离线情报文件。

进入 **知识建设 > 知识库 > 情报管理 > 情报** 页面，单击【导入】按钮，在虚线框区域选择情报文件或将情报文件拖拽至虚线框区域即可。

- 支持导入扩展名为.gz 的情报文件，每次仅支持导入 1 个 1~100MB 的情报文件。
- 可以在历史记录中查看情报导入的记录信息。

提取漏洞

提取漏洞用于将情报提取至产品漏洞库，生成漏洞信息并归属至相应漏洞分类和 CWE 分类，也可以应用于新建漏洞验证任务。

进入 **知识建设 > 知识库 > 情报管理 > 情报** 页面，支持手动提取和自动提取情报：

自动提取情报

单击【配置 > 情报自动提取配置】按钮后，选择“是”，启用情报自动提取，即可将情报页面可提取的情报自动提取到产品漏洞库中。

手动提取情报

- 单个提取：单击操作栏中的【提取漏洞】，对相应情报进行提取。
- 批量提取：勾选所需情报，单击【提取漏洞】按钮，对勾选情报进行提取。

预警情报

预警操作后，情报会自动和资产进行匹配，匹配成功后才会生成预警。

进入 **知识建设 > 知识库 > 情报管理 > 情报** 页面，进行预警操作即可。

- 单个预警：单击操作栏中的【预警】，对相应情报进行预警。
- 批量预警：勾选所需情报，单击【预警】按钮，对勾选情报进行预警。

筛选和查看情报

进入 **知识建设 > 知识库 > 情报管理 > 情报** 页面，单击页面上方的情报总数、高/中/低/未知、高级情报数、POC 情报数、应急情报数、配置查询条件，搜索情报后，单击情报名称，查看情报详情即可。

- 在“生命周期”页签中，查看情报的生命周期概览以及情报当前的存疑资产数、已确认资产数、已修复漏洞数、未修复漏洞数。系统每天零点自动更新以上数据，用户可手动单击【更新】按钮，更新以上数据。
- 在“情报详情”页签中，查看情报详情。
- 在“关联预警”页签中，查看受情报影响的资产的发展趋势。将鼠标移至图中节点处，可以查看受影响的资产个数。
- 在“更新历史”页签中，查看情报的更新记录。

9.2.4.2 预警

TVM 根据一定的预警规则进行防护，从而发现防护目标中存在的最新漏洞和威胁事件。

查看预警详情

配置 预警情报 后，TVM 将对匹配成功的情报进行预警，预警成功后，进入 **知识建设 > 知识库 > 情报管理 > 预警** 页面，查询指定预警，单击“情报名称”，查看预警详情即可。

- 在“影响资产”页签中，查看受影响的资产信息，并可查看历史预警、修改预警状态。
- 在“情报详情”页签中，查看情报详情。
- 在“历史预警”页签中，查看历史的预警记录。
- 在“扫描验证”页签中，查看下发的预警扫描验证任务。

预警验证任务

当情报的 CVE ID 和漏洞库某一个漏洞的 CVE ID 匹配时、即“可扫描”时，TVM 可以该情报的 CVE ID 关联的漏洞为模板对预警的关联资产进行漏洞验证。

进入 **知识建设 > 知识库 > 情报管理 > 预警** 页面，单击“情报名称”，选择页签 **影响资产**，勾选需要验证的资产，单击批量验证，配置预警验证任务参数即可。预警验证任务参数如表 9-10 所示。

表9-10 预警验证任务参数

配置项	描述
任务名称	预警验证任务的名称，具体请参见界面要求。

配置项	描述
目标类型	主机资产的 IP 地址类型。
设备选择	执行预警验证任务的设备。

9.2.5 漏洞指纹插件库

漏洞指纹插件库用于管理 POC 扫描任务的 POC、引擎、插件。

9.2.5.1 POC 管理

进入 **知识建设 > 知识库 > 漏洞指纹插件库 > POC 管理** 页面，单击【新增】按钮，可以新建一个 POC 漏洞。POC 参数说明如表 9-11 所示。

- 新建 POC 后，单击操作栏的【发布】，即可应用于 POC 扫描任务。
- 新建 POC 后，单击+展开关联插件详情列表后，可以进行删除关联插件和置为默认插件的操作。
- 发布 POC 后，单击操作栏的【下架】，将不能对该 POC 漏洞进行扫描。下架后，支持重新发布操作。
- 新建 POC 后，可以进行查询、查看、编辑和删除的操作。

表9-11 POC 参数

配置项	描述
POC 名称	该 POC 漏洞的名称。
POC 类型	该 POC 漏洞的类型。可选项有漏洞 POC、漏洞 EXP、漏洞指纹。
公开状态	该 POC 漏洞是否为公开。 • 已公开：公开 POC 为厂商已公布 POC。 • 未公开：未公开 POC 为用户自建 POC。
POC 内容描述	该 POC 漏洞的说明信息。
选择产品漏洞	单击【查询漏洞】按钮，从产品漏洞库中选择与该 POC 关联的网站漏洞（仅支持单选）。支持漏洞名称、漏洞编号的模糊查询和精确查询。 产品漏洞的相关信息请参见 产品漏洞库。 说明 已绑定漏洞将不会在查询列表中展现。
POC 文件/POC 文件描述	上传该 POC 漏洞的文件，填写文件说明信息。
添加插件	该 POC 漏洞的关联插件。支持多选。插件的相关信息请参见 插件管理。

9.2.5.2 引擎管理

进入 **知识建设 > 知识库 > 漏洞指纹插件库 > 引擎管理** 页面，单击【新增】按钮，可以新建一个检测 POC 漏洞的引擎。引擎参数说明如表 9-12 所示。新建引擎后，可以进行查询、查看、编辑、删除和下载文件的操作。

表9-12 引擎参数

配置项	描述
引擎名称	该引擎的名称。
引擎分类	该引擎的所属分类。
引擎类型	该引擎的类型。
引擎来源	该引擎的来源。
引擎描述	该引擎的说明信息。
引擎版本	该引擎的版本。

9.2.5.3 插件管理

进入 **知识建设 > 知识库 > 漏洞指纹插件库 > 插件管理** 页面，单击【新增】按钮，可以新建一个检测 POC 漏洞的插件。插件参数说明如表 9-13 所示。新建插件后，可以进行查询、查看、编辑和删除的操作。

表9-13 插件参数

配置项	描述
插件名称	该插件的名称。
插件版本	该插件的版本。
插件描述	该插件的说明信息。
插件文件	该插件的文件。
引擎名称/引擎版本	该插件的关联引擎及其版本。引擎的相关信息请参见 引擎管理。

9.2.6 资产标记库

TVM 提供标准的资产标记库，支持通过资产纠偏引擎对 资产列表 和 产品漏洞库 的相关信息进行纠偏，并对纠偏结果进行人工确认。

9.2.6.1 标记纠偏任务

进入 **知识建设 > 知识库 > 资产标记库 > 标记纠偏任务** 页面，用户可以根据资产属性和产品漏洞属性执行资产标记纠偏任务；任务执行完成后，可以在纠偏任务列表中查看执行结果，也可以进入纠偏结果列表查看具体信息，请参见 纠偏结果。

新建纠偏任务

单击【新建】按钮，配置资产标记纠偏任务参数，即可创建一个纠偏任务。资产标记纠偏任务参数说明如表 9-14 所示。

表9-14 资产标记纠偏任务参数

配置项	描述
任务名称	填写资产标记纠偏任务的名称，默认为“资产属性处理任务”。最多支持 60 个字符。
执行方式	• 立即执行：任务新建后，立即执行资产标记纠偏任务。 • 定时执行：将按照时间设置定时执行资产标记纠偏任务。 • 周期执行：将按照周期设置执行资产标记纠偏任务。
时间设置	执行方式为“定时执行”或“周期执行”时，需要配置固定时间或每天/周/月的某个时刻执行资产标记纠偏任务。
选择属性	选择资产属性或产品漏洞属性后，再选择具体的目标对象，该任务会影响所选的目标对象的纠偏值。支持多选。 只能选择开启状态的目标对象。关于目标对象状态的启停方法，请参见 目标对象。
单类标记数量	默认为-1，不支持修改。
纠偏阈值	填写纠偏的阈值下限，取值范围为 1~100。建议阈值下限在 90 以上，从而匹配更高的准确率。

管理纠偏任务

资产标记纠偏任务新建后，根据任务的执行方式，管理操作的具体说明如表 9-15 所示。

表9-15 资产标记纠偏任务管理操作

操作项	描述
编辑任务	• 执行方式为“立即执行”的任务，不支持编辑。 • 执行方式为“定时执行”和“周期执行”的任务，只能编辑任务名称和执行时间。
删除任务	• 已执行完成的任务，被删除后不可恢复。 • 执行中的任务，不支持删除。
任务重扫	重新扫描对应的任务。
任务停止	执行中的任务，支持停止
任务启用/禁用	• 执行方式为“立即执行”的任务，不支持启用/禁用。 • 执行方式为“定时执行”和“周期执行”的任务，默认为启用状态；若暂不需要执行任务，可将其置为禁用状态。
任务查询	支持任务名称的模糊查询。单击【高级查询】按钮，可以按照任务名称、任务 ID、任务属性、状态或执行方式进行查询。

9.2.6.2 纠偏结果

进入 **知识建设 > 知识库 > 资产标记库 > 纠偏结果** 页面，页面左侧是目标对象类型结构，页面右侧默认展示全部类型的资产标记纠偏结果，如图 9-1 所示，纠偏状态说明如表 9-16 所示。支持纠偏结果的查询、删除、批量纠偏和批量恢复等操作。

图9-1 资产标记纠偏结果

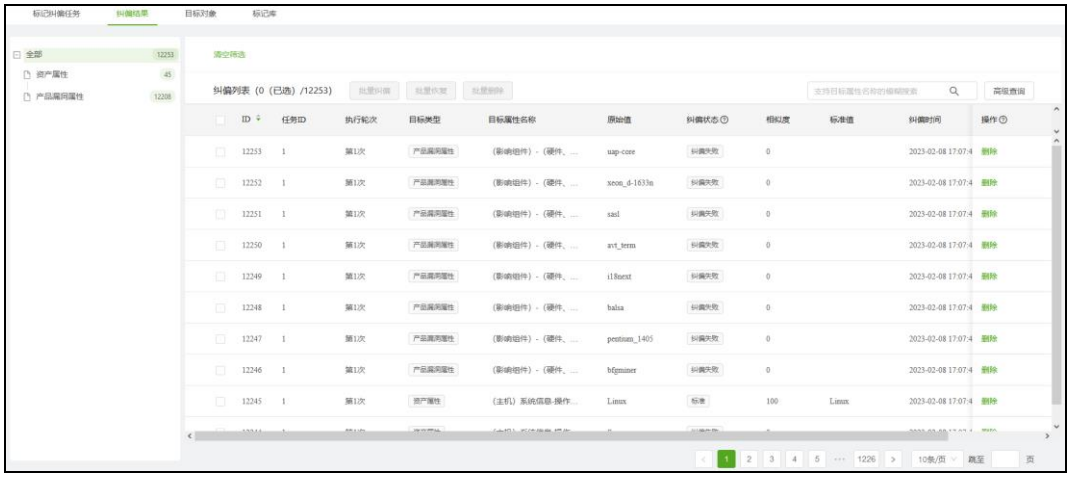


表9-16 资产标记纠偏状态

纠偏状态	描述
已纠偏	在相似度的基础上存在标准值。
纠偏失败	在相似度的基础上不存在标准值，相似度低。
标准	待纠偏属性和标记库中的属性一致。
待纠偏	属性未进行纠偏操作。

批量纠偏

单击纠偏结果列表上方的【批量纠偏】，可将纠偏状态为“待纠偏”的结果批量纠偏。

批量恢复

单击纠偏结果列表上方的【批量恢复】，可将纠偏状态为“已纠偏”的结果批量恢复，恢复后的纠偏状态为“待纠偏”。

9.2.6.3 目标对象

进入 **知识建设 > 知识库 > 资产标记库 > 目标对象** 页面，页面左侧展示资产标记纠偏任务的目标对象属性组，页面右侧展示所选属性组的属性列表，可以进行属性状态的启用/停用。只有启用中的属性，才能应用在标记纠偏任务中。

9.2.6.4 标记库

进入 **知识建设 > 知识库 > 资产标记库 > 标记库** 页面，展示当前互联网上的资产标记库统计信息，页面展示内容说明如表 9-17 所示。

表9-17 资产标记库内容

展示项		描述
漏洞统计概览	产品分类分布 TOP10	以饼图方式展示漏洞最多的软件产品分类 TOP 10。 单击图例可以取消/显示对应类别在图中的统计。将鼠标悬停在图中，可以查看对应类别的具体数据。
	产品族分布 TOP10	以饼图方式展示漏洞最多的介质类型 TOP 10。 单击图例可以取消/显示对应类别在图中的统计。将鼠标悬停在图中，可以查看对应类别的具体数据。
标记数		以列表方式展示互联网上的全部资产标记信息，包括 ID、资产数据来源、产品族、产品名称、产品分类、厂商名称和产品版本。支持产品名称的模糊查询。

9.2.7 知识库升级

目前不支持在线升级知识库，请联系绿盟科技的技术支持人员获取离线知识库升级包。

进入 **知识建设 > 知识库 > 知识库升级** 页面，在虚线框中选择升级文件或拖拽升级文件至虚线框中即可。

9.3 模板管理

模板管理主要用于管理 扫描任务管理 中需要关联的模板。

9.3.1 产品漏洞模板

系统模板和网站模板的管理方法类似，这里以系统模板为例进行介绍。

新建模板分组

进入 **知识建设 > 知识库 > 产品漏洞模板 > 系统模板** 页面，单击【新建模板组】按钮，配置“模板分组名称”即可，具体请参见界面要求。新建模板分组后，还可以进行查看详情、编辑和删除操作。

新建模板

进入 **知识建设 > 知识库 > 产品漏洞模板 > 系统模板** 页面，单击【新建模板】按钮/【另存为】，配置产品漏洞模板参数即可。产品漏洞模板参数如表 9-18 所示。新建产品漏洞模板后，还可以进行查询分组下漏洞、查看详情、编辑、删除、导入/导出的操作。

表9-18 产品漏洞模板参数

配置项	描述
模板名称	漏洞模板的名称，具体请参见界面要求。
详细描述	漏洞模板的说明信息，具体请参见界面要求。
选择分组	漏洞模板所属的模板分组。
添加漏洞	模板包含的漏洞检查项。

公开/取消公开模板

默认情况下，每个帐号只能管理自身的自定义漏洞模板，将自定义模板公开后，其他帐号可以查看和使用该模板。

进入 **知识建设 > 知识库 > 产品漏洞模板 > 系统模板** 页面，单击自定义模板操作栏中的“公开/取消公开”，可以公开/取消公开该自定义模板。

9.3.2 口令字典模板

进入 **知识建设 > 模板管理 > 口令字典模板** 页面，页面左侧展示口令字典模板组（初始状态下，默认展示“绿盟科技模板组”），页面右侧展示所选模板组的口令字典模板列表，如图 9-2 所示。

图9-2 口令字典模板管理

自定义口令字典模板组

初始状态下，系统内置两个口令字典模板组：

- 绿盟科技模板组：包含所有服务默认字典模板和常用服务默认字段模板。不支持在该模板组内新建口令字典模板。
- 未分类：默认为空。新建口令字典模板暂时无法分组时，可将模板暂存在该模板组内。

单击【新建模板组】，可以新建口令字典模板组（目前不支持创建子模板组），支持自定义模板组的删除操作。

自定义口令字典模板

新建口令字典模板的方法包括两种：内置模板另存为、手动新建模板。

口令字典模板新建后，可以进行编辑、删除、查看详情、导出和公开/取消公开等操作。

说明	• 内置的口令字典模板，不支持修改和删除。 • 自定义口令字典模板的公开/取消公开方法，请参见 公开/取消公开模板。

内置模板另存为

在绿盟科技模板组的口令字典模板列表中，单击操作栏的【另存为】，即可在对应内置模板的基础上进行修改，另存为新的自定义口令字典模板。

手动新建模板

单击【新建模板】按钮，配置口令字典模板参数，即可在所选分组中新建口令字典模板。口令字典模板参数说明如表 9-19 所示。

表9-19 口令字典模板参数

配置项		描述
模板名称		填写口令字典模板的名称。
选择分组		选择该模板所属的模板组。关于模板组的配置方法，请参见 自定义口令字典模板组。
模板描述		填写口令字典模板的描述信息。
口令字典列表		单击【新建配置】按钮，可以添加多个口令字典。添加后，支持删除/批量删除。
口令猜测配置	服务类型	选择一个远程服务类型。
	模式	• 标准模式：常见用户名口令的组合字典。 • 组合模式：将用户名字典和密码字典分别配置。
	用户名/密码	模式为“组合模式”时，分别选择用户名字典和密码字典。
	帐号&密码	模式为“标准模式”时，选择一个用户名口令组合字典。
	扩展字段	扩展字段支持两种： • 端口：所选服务类型的端口号。取值范围为 1~65535。 • URL：所选服务类型的 URL。支持多个 URL，填写时请使用英文逗号、分号、空格或者回车符进行分隔。

9.3.3 资产探测模板

进入 **知识建设 > 模板管理 > 资产探测模板** 页面，页面左侧展示资产探测模板组，页面右侧展示所选模板组的资产探测模板列表，如图 9-3 所示。可以查询模板和查看模板详情。

图9-3 资产探测模板

9.4 运营经验库

在运营经验库中，可以管理用户自定义的漏洞修复方案和漏洞误报任务。

9.4.1 修复方案库

进入 **知识建设 > 运营经验库 > 修复方案库** 页面，单击【新建】按钮，可以添加自定义漏洞修复方案，便于用户快速查询解决方案并修复资产存在的脆弱性。漏洞修复方案的参数说明如表 9-20 所示。添加自定义漏洞修复方案后，可以进行查询、编辑、删除和查看详情的操作。

表9-20 漏洞修复方案

配置项	描述
方案名称	漏洞修复方案的名称。
漏洞类型	修复漏洞所属的类型。
选择产品漏洞	修复的漏洞。
公开状态	• 公开：所有用户可见。 • 私有：仅创建用户可见。
修复方案	对漏洞的修复方案。
方案描述	对漏洞修复方案的说明。
详细描述	补充说明。
附件上传	漏洞修复方案的附件。

9.4.2 漏洞误报库

若用户认为某些漏洞属于误报，可以通过漏洞误报任务忽略该漏洞，使其不影响脆弱性值的计算。

批量新建资产漏洞误报（在 漏洞处置 页面创建）和批量新建产品漏洞误报（在 产品漏洞库 页面创建）的操作类似，这里以批量新建产品漏洞误报为例进行介绍。

进入 **知识建设 > 运营经验库 > 漏洞误报库** 页面，单击【新建 > 新建产品漏洞误报】按钮，进入 产品漏洞库 页面，勾选漏洞，单击【批量新建漏洞误报】按钮即可新建一条漏洞误报任务。

- 漏洞误报的参数说明如表 9-21 所示。
- 新建漏洞误报任务后，可以对其进行查询、编辑、删除和查看详情的操作。
- 单击“漏洞名称”，可以查看漏洞详情。

表9-21 漏洞误报参数

配置项	描述
失效时间	漏洞误报任务的有效时间。 在失效时间前，该漏洞不影响脆弱性值；在失效时间后，该漏洞影响脆弱性值。
执行方式	漏洞误报任务的执行频度和时间。
是否关联历史数据	启用后，若历史扫描任务、处置单和资产风险中存在该漏洞，则忽略该漏洞，重新计算脆弱性值，直至超过失效时间。
是否影响未来业务	启用后，在失效时间前，若新的扫描任务、处置单和资产风险中存在该漏洞，则忽略该漏洞，重新计算脆弱性值。
描述	对漏洞误报任务的描述。

9.5 知识配置

漏洞误报库配置

进入 **知识建设 > 知识配置 > 漏洞误报库配置** 页面，可以开启/关闭 漏洞误报库 的操作权限。

- 开启：用户可以对自定义漏洞误报进行编辑、删除，还可以在 产品漏洞库 和 漏洞处置 中批量添加漏洞误报。
- 关闭：不能对漏洞误报进行编辑、删除、添加的操作。

漏洞自动融合配置

进入 **知识建设 > 知识配置 > 漏洞自动融合配置** 页面，可以管理漏洞自动融合的策略，参数说明如表 9-22 所示。

表9-22 漏洞自动融合配置

配置项	描述
启用漏洞自动融合配置	启用后，入库的漏洞在产品漏洞库中匹配到相同 CVE ID 的漏洞，则触发漏洞融合操作。
启用漏洞属性缺失补全	启用后，漏洞自动融合时，自动对补充缺失属性的信息，按照优先级从高到低进行补全。
厂商优先级/来源方式优先级	按照优先级从高到低，对同一属性进行融合和补全。 鼠标拖动厂商/来源方式名称，可以调整优先级排序。

10 系统配置

本章主要包含以下内容：

功能	描述
主题配置	可以对 TVM 的标题和 logo 进行管理。
安全防护	TVM 提供一个安全保护措施来保证系统的安全性。
数据外发	TVM 支持将任务、处置单和预警数据推送至指定服务器或邮箱，方便用户查看。
二次接口	TVM 提供二次接口，方便其他产品调用 TVM 中的用户认证、资产、任务、设备的相关数据。
工具管理	用户可以将 TVM 作为第三方工具存放平台，方便管理工具。

10.1 主题配置

进入 **系统配置 > 主题配置** 页面，如图 10-1 所示，可以对 TVM 的标题和 logo 进行管理，即可以自定义如图 10-2 所示的平台信息。

图10-1 主题配置

图10-2 可以配置的主页面信息

10.2 安全防护

进入 **系统配置 > 安全防护** 页面，TVM 提供一个安全保护措施来保证系统的安全性。

安全证书

用户可以在平台中选择自定义证书，随后上传自定义的安全签证证书，证书校验通过后，将替换系统自带的安全签证证书，系统默认使用系统自带安全签证证书。

完整性保护

系统默认对关键文件数据进行完整性保护措施，以防止恶意篡改和破坏系统。

单击【配置验签周期】按钮，可以配置自定义验签策略。

单击【验签数据列表】按钮，可以查看需要保护的配置文件。

密码保护

对于系统中的弱口令数据，系统提供密码加盐措施，来保证密码数据不被恶意破解和泄露，用户可以在弱口令加密盐值处填写任意的加密盐值。

10.3 数据外发

TVM 支持将任务、处置单和预警数据推送至指定服务器或邮箱，方便用户查看。

配置项

进入 **系统配置 > 数据外发 > 配置项** 页面，启用后，配置数据外发参数即可。数据外发参数如表 10-1 所示。

表10-1 数据外发

发送类型	配置项	描述
任务	发送历史任务	• 开启：会发送历史扫描任务和今后执行的扫描任务的数据。 • 关闭：仅发送今后执行的扫描任务的数据。
	任务类型	若任务类型属于所选类型，则发送任务数据。
处置单	发送周期（分钟）	两次发送处置单数据的时间间隔，具体请参见界面要求。
	过滤条件	单击【添加筛选】，可以添加处置单的过滤条件，过滤条件说明如表 10-2 所示。
预警	发送周期（分钟）	两次发送预警数据的时间间隔，具体请参见界面要求。
发送方式	FTP/SFTP	接收数据的服务器。支持多选。

表10-2 处置单的过滤条件

筛选项	描述
漏洞名称	漏洞的名称。最多支持 100 个字符。
漏洞类型	可选项有全部、主机、资产。
漏洞分值	拖动鼠标选择漏洞分值。取值范围为 0~10。
处置人	工单的处置人。
资产范围	可以切换视图选择资产范围，默认按照资产组进行选择。
资产 IP/URL	最多支持 100 个字符。 • 漏洞类型为“主机”时，支持资产 IP 的模糊查询和精确查询。 • 漏洞类型为“网站”时，支持资产 URL 的模糊查询和精确查询。 • 漏洞类型为“全部”时，支持资产 IP/URL 的模糊查询。
资产名称	支持资产 IP 的模糊查询和精确查询。最多支持 100 个字符。
资产联系人	支持资产 IP 的模糊查询和精确查询。最多支持 100 个字符。
处置优先级	可选项有低优先级、中优先级、高优先级。支持多选。
脆弱性等级	可选项有低危、中危、高危。支持多选。
处置单状态	工单的处置状态。支持多选。
数据来源	处置单的来源设备。支持多选。

外发日志

进入 **系统配置 > 数据外发 > 外发日志** 页面，可以查看数据外发的记录。

10.4 二次接口

TVM 提供二次接口，方便其他产品调用 TVM 中的用户认证、资产、任务、设备的相关数据。

进入 **系统配置 > 二次接口** 页面，显示 TVM 设备的二次接口列表，同时支持以下操作：

- 单击【接口文档】按钮，可以下载二次接口开发文件，获取相关数据。二次开发接口通过 rest 接口会对系统内部数据造成直接影响，请在需要的情况下谨慎使用。
- 单击【测试脚本】按钮，可以下载测试脚本文件，脚本仅支持在有 curl、python 命令的 Linux 系统环境下执行。

10.5 工具管理

用户可以将 TVM 作为第三方工具上存放平台，方便管理工具。

进入 **系统配置 > 工具管理** 页面，单击【新建】按钮，即可导入一个新工具。工具的参数说明如表 10-3 所示。新建工具后，可以对其执行下载 、编辑、删除、查询和查看详情的操作。

表10-3 工具管理

配置项	描述
工具名称	第三方工具的名称。
工具描述	对第三方工具的补充说明。
附件上传	第三方工具的压缩包，仅支持.zip 格式。

A 出厂设置

角色	用户名	密码
系统管理员，审计管理员，业务管理员	admin	admin

B 支持的设备及版本

支持设备	设备引擎版本
BVS	V6.0R01F03SP13
RSAS	V6.0R04F02SP03
WVSS	V6.0R03F01SP17

C 安全等级保护

设备的信息系统安全等级保护功能支持国家等保标准的前四级。

不同安全保护等级的信息系统，其对业务信息的安全性要求和系统服务的连续性要求是有差异的；即使相同安全保护等级的信息系统，其对业务信息的安全性要求和系统服务的连续性要求也有差异。依据国家等级保护标准，第一到第四等级的信息系统应具备的基本安全保护能力如下：

- 第一级安全保护能力

  应能够防护系统免受来自个人的、拥有很少资源的威胁源发起的恶意攻击、一般的自然灾难、以及其他相当危害程度的威胁所造成的关键资源损害，在系统遭到损害后，能够恢复部分功能。

- 第二级安全保护能力

  应能够防护系统免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难、以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和安全事件，在系统遭到损害后，能够在一段时间内恢复部分功能。

- 第三级安全保护能力

  应能够在统一安全策略下防护系统免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难、以及其他相当危害程度的威胁所造成的主要资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够较快恢复绝大部分功能。

- 第四级安全保护能力

  应能够在统一安全策略下防护系统免受来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾难、以及其他相当危害程度的威胁所造成的资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够迅速恢复所有功能。

基本安全要求是针对不同安全保护等级信息系统应该具有的基本安全保护能力提出的安全要求，根据实现方式的不同，基本安全要求分为基本技术要求和基本管理要求两大类。其中基本技术要求根据保护侧重点的不同细分为三类：

- 保护数据在存储、传输、处理过程中不被泄漏、破坏和免受未授权的修改的信息安全类要求（简记为 **S**）；
- 保护系统连续正常的运行，免受对系统的未授权修改、破坏而导致系统不可用的服务保证类要求（简记为 **A**）；
- 通用安全保护类要求（简记为 **G**）。

信息系统定级后，不同安全保护等级的信息系统可能形成的定级结果组合如表 C-1 所示。

表C-1 安全保护等级

安全保护等级	信息系统定级结果的组合
第一级	S1A1G1
第二级	S1A2G2，S2A2G2，S2A1G2
第三级	S1A3G3，S2A3G3，S3A3G3，S3A2G3，S3A1G3
第四级	S1A4G4，S2A4G4，S3A4G4，S4A4G4，S4A3G4，S4A2G4，S4A1G4