天翼云网站安全监测
产品使用指南

中 国 电 信 天 翼 云 科 技 有 限 公 司

目录

1 产品介绍

1.1 产品定义

天翼云网站安全监测服务依托全球部署的分布式监测集群，对目标系统提供 7*24 小时安全监测服务，通过对网站可用性、安全事件、内容安全、OWASP Top 10 Web 漏洞以及 DNS 解析的实时监测，协助客户及时发现目标系统风险，并解决安全隐患，为网站安全保驾护航。

本产品实现一站式全托管服务，SaaS 产品性质远程直接交付，应用更快捷。

网站安全监测基本架构：

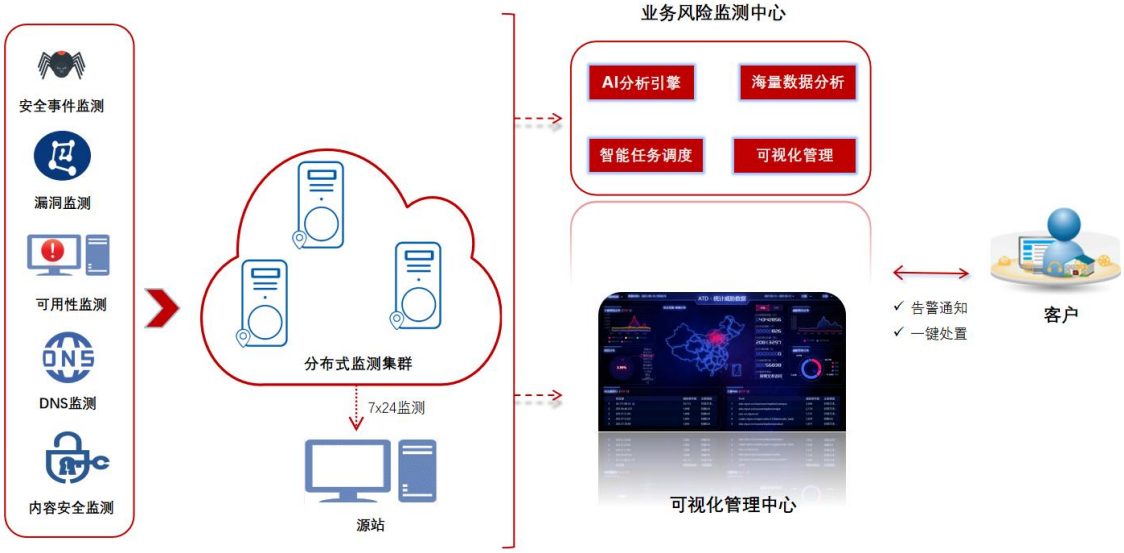


图 1-1 产品架构

1.2 术语解释

1.2.1 DNS

DNS 即 Domain Name System，是域名解析服务的意思。它在互联网的作用是：把域名转换成为网络可以识别的 ip 地址。人们习惯记忆域名，但机器间互相只认 IP 地址，域名与 IP 地址之间是一一对应的，它们之间的转换工作称为域名解析，域名解析需要由专门的域名解析服务器来完成，整个过程是自动进行的。比如：上网时输入的 www.baidu.com 会自动转换成为 220.181.112.143。

1.2.2 安全边缘节点

在天翼云所有文档中，边缘节点、CDN 节点、Cache 节点、缓存节点、加速节点、天翼云节点等都是指天翼云边缘节点。边缘节点是相对于网络的复杂结构而提出的一个概念，指距离最终用户接入具有较少的中间环节的网络节点,对最终接入用户有较好的响应能力和连接速度。其作用是将访问量较大的网页内容和对象保存在服务器前端的专用 Cache 设备上，以此来提高网站访问的速度和质量。

1.2.3 分布式监测集群

分布式结构就是将一个完整的系统，按照业务功能，拆分成一个个独立的子系统，在分布式结构中，每个子系统就被称为“服务”。这些子系统能够独立运行在 web 容器中，它们之间通过 RPC 方式通信。因此按照微服务的思想，网站安全监测产品的功能模块可拆分成多个独立的服务，即：安全事件监测、漏洞监测、可用性监测、DNS 监测、内容安全监测。每个服务都是独立的项目，可以独立运行。如果服务之间有依赖关系，那么通过 RPC 方式调用。

单机处理到达瓶颈的时候，就把单机复制几份，这样就构成了一个“集群”。集群中每台服务器就叫做这个集群的一个“节点”，所有节点构成了一个集群。每个节点都提供相同的服务，那么这样系统的处理能力就相当于提升了好几倍（有几个节点就相当于提升了这么多倍）。

分布式监测集群可以在实现网站安全监测产品完整、系统化的同时，能够解决访问速度和质量的问题。

1.2.4 Web 漏洞

WEB 漏洞通常是指网站程序上的漏洞，可能是由于代码编写者在编写代码时考虑不周全等原因而造成的漏洞，常见的 WEB 漏洞有 Sql 注入、Xss 漏洞、上传漏洞等。

如果网站存在 WEB 漏洞并被黑客攻击者利用，攻击者可以轻易控制整个网站，并可进一步提权获取网站服务器权限，控制整个服务器。主要有以下几种攻击方法：SQL 注入、XSS 跨站点脚本、跨目录访问、缓冲区溢出、cookies 修改、Http 方法篡改、CSRF、CRLF、命令行注入。

1.2.5 Web 安全

相关 Web 应用层面的安全问题与事件,包括各种 Web 组件、协议、应用等。

1.2.6 网站白名单

通过设置网站白名单，可以让满足条件的请求不经过任何网站安全监测防护模块的检测，直接访问源站服务器。

1.2.7 IP 黑名单

支持一键阻断来自指定 IP 地址、IP 地址段以及指定地理区域的 IP 地址的访问请求。

1.2.8 网页挂马

网页挂马指的是把一个木马程序上传到一个网站里面然后用木马生成器生一个网马，再上到空间里面，而后加代码使得木马在打开网页时运行。

1.2.9 暗链攻击

暗链就是看不见的网站链接，其在网站中做得非常隐蔽，短时间内不易被搜索引擎察觉。暗链攻击，是指黑客通过隐形篡改技术在被攻击网站的网页植入暗链，这些暗链往往被非法链接到色情、诈骗、甚至反动信息。

1.3 产品功能

1.3.1 漏洞扫描及验证

- 通过网站安全监测系统平台，在无需用户采购任何 Web 应用扫描产品前提下，即可通过报告形式获得网站的漏洞态势，以及每个漏洞的详情介绍和修补建议；统计分析看板直观获取不同等级漏洞类型、易受攻击目标等数据，漏洞趋势分析摸底网站漏洞发展情况，同时兼具实时大屏态势感知功能方便跟踪漏洞发生大盘状态，方便及时作出处置。
- 服务支持远程扫描 Web 漏洞和按照国际权威安全机构 WASC 分类的 25 种 Web 应用漏洞，全面覆盖 OWASP Top 10 Web 应用风险。
- 如采购漏洞专家验证服务，还会提供针对中高危漏洞提供专家验证，确保漏洞真实存在，并协助客户完成漏洞复验，更好的完成漏洞生命周期管理。

1.3.2 安全事件监测

- 使用静态分析和动态解析相结合的主动挂马监测技术，通过解析引擎模拟环境监控记录 URL 页面运行行为，生成日志；通过后端引擎根据预定义规则高效、准确识别网站页面中的恶意代码，以及黄赌毒私服等词汇的恶意链接，使网站管理员能够及时清除网页木马及黑链，避免给访问者带来安全威胁，影响网站信誉。
- 使用前后页面对比的方式，辅以恶意文本核查分析，实时监测目标网站页面的篡改情况，支持监测静态文本内容的变化以及 DOM 树结构的变化；发现页面被篡改情况，第一时间通知用户，避免篡改事件影响扩散，给自身带来声誉和法律风险。
- 实时监测目标站点的页面内容，如出现个人敏感信息（包含手机号、银行卡号、身份证号码）泄露问题，第一时间告警通知客户。

1.3.3 内容安全监测

- 网站文本、图片内容的合规性监测，监测类别包含涉黄、涉毒、涉政、赌博、暴恐、邪教；支持监测的图像格式包括但不限于 JPEG、GIF、PNG、BMP、TIFF、JPEG2000；支持监测的文本格式包括但不限于 Big5、UTF-8、GBK、GB2312，内容类型至少支持 txt、html、wmlc、wml、xhtml、mht。
- 基于大量数据训练的深度学习模型，对待监测页面进行文本、图片元素的敏感内容监测，输出相关敏感信息和类别。
- 发现页面出现敏感信息后，第一时间通知用户。用户可参考天翼云提供的安全建议及时删除敏感内容，避免事件影响扩散，给自身带来声誉和法律风险。用户也可以自定义所关心的敏感关键词。

1.3.4 可用性监测

- 多线路远程实时监测目标站点在多种网络协议下的响应速度、可访问性等反映网站性能状况的内容，一旦发现网站无法访问，或访问出现延迟。根据事先定义好的网站通断级别，第一时间通知用户。风险日志详细展示存在的访问性问题，问题时长以及各监测点的诊断信息。用户也可以视情况选择合适的网站响应时间告警阈值。

1.3.5 DNS 监测

- 从各省运营商网络线路远程实时监测各地主流 ISP 的 DNS 缓存服务器和用户 DNS 授权服务器的解析过程及结果。一旦发现用户域名无法解析或解析不正确，第一时间通知用户。避免出现由于 DNS 解析失败产生的网站无法访问，以及域名劫持等安全风险。

1.3.6 业务管理能力

- 提供态势感知大屏服务，满足客户大屏监控场景需求，以一站式全局视角，实时跟踪目标系统的风险情况，及时定位问题。
- 提供在线统计分析看板服务，态势感知帮助用户进行业务指标跟踪，能够多维度展示监测数据情况，数据统计分析能力赋能用户分析聚焦漏洞问题。
- 提供网站安全评估报告和漏洞扫描报告生成和下载服务，聚合任务监测的风险结果，让您整体掌握网站的风险状况及安全趋势。

1.4 产品优势

1.4.1 应用快，免安装

- 纯 SaaS 服务，无需安装任何软硬件，成本低
- 7*24 小时全天候服务，按需购买，即买即用，无部署无需改变网络结构，无需占用机房或办公空间
- 使用公网可访问的域名即可自助开启服务

1.4.2 资源广布，专业服务

- 支持多点监测，覆盖全国多地区、三大运营商线路
- 支持监测挂马、篡改、敏感内容、平稳度、域名解析、黑链等事件，并可以在用户门户上做可视化呈现
- 支持扫描 WASC 25 种 Web 应用漏洞，全面覆盖 OWASP Top 10 Web 应用风险

1.4.3 全流程管理，用户友好

- 多功能体系化产品，发现风险一键处置，联动 WAF 访问控制能力操作封禁
- 无需处理软硬件故障、升级等问题，完全托管，无需亲自运维
- 可视化看板、报表和态势跟踪全方位辅助业务数据跟踪，更好地进行业务管理

1.4.4 高效率，高专业度

- 分钟级实时监测能力，最高监测频率可达 2min/次
- 漏洞扫描结果经安全专家验证，进一步保证结果可信

1.5 应用场景

1.5.1 政企行业监测场景

网站被挂马、恶意篡改后对政府形象造成不利影响，安全事件监测根据规则精准识别违规信息，及时同步客户，保障网站安全，维护网站名誉不受影响。

1.5.2 媒体行业监测场景

网站暴露面广且要求网站内容输出的准确性，网站内容监测基于深度学习模型，对敏感内容检测，输出相关敏感信息和类别，及时同步客户，保障网站稳定安全的运行。

1.5.3 金融、证券行业监测场景

网站对业务可用性要求非常高，产生网站安全和性能风险后，将造成用户流失、在线交易失败等经济损失。网站可用性监测，多维度监测目标网站在多种网络协议下的响应速度、可访问性等，保障网站性能，满足客户业务需求。

1.5.4 医疗、卫健行业监测场景

涉及到市民的重要隐私数据，需要保证大量的个人信息数据安全，同时医院门户网站及各类线上信息输送渠道访问量大，其访问安全性需要被满足。网站安全监测集合内容安全、可用性及漏洞扫描能力，全方位为网站安全保驾护航。

2 购买指南

2.1 价格

【计费项】
套餐包：预付费，可根据业务选择不同规格
扩展服务-大屏：预付费
扩展服务-图片审核：按需付费，根据实际使用量产生费用

2.1.1 套餐计费

表 2-1 套餐标准资费

网站安全监测				
套餐内容		体验版	专业版	旗舰版
监测服务内容		1、可用性监测 2、安全事件监测：篡改、暗链、挂马、敏感信息检测 3、内容安全：文本敏感词检测	1、可用性监测 2、DNS 监测 3、安全事件监测：篡改、暗链、挂马、敏感信息检测 4、内容安全：文本敏感词检测 5、内容安全：支持图片审核扩展	1、可用性监测 2、DNS 监测 3、安全事件监测：篡改、暗链、挂马、敏感信息检测 4、内容安全：文本敏感词检测 5、内容安全：支持图片审核扩展 6、支持自定义引擎配置、人工配置审核
漏洞检测		1 次/月	1 次/月 提供漏洞验证	1 次/周 提供漏洞验证
标准资费	域名数量	标准资费	标准资费	标准资费
	[1,10)	560 元/个/月	1260 元/个/月	2160 元/个/月
	[10,30)	336 元/个/月	756 元/个/月	1296 元/个/月
	[30,50)	280 元/个/月	630 元/个/月	1080 元/个/月

	[50,+∞)	224 元/个/月	504 元/个/月	864 元/个/月

2.1.2 扩展服务计费

表 2-2 图片审核计费标准

计费项	价格
图片审核-不确定	0 元/千张/日
图片审核-确定	1.3 元/千张/日

注：图片审核功能中不确定审核的图片，当前为免费，不收取费用。

表 2-3 大屏服务计费标准

计费项	价格
大屏服务	1500 元/月

2.2 购买

开通天翼云网站安全监测服务，须注册天翼云账户并确保已实名认证。

1、天翼云账号注册指导文档：https://www.ctyun.cn/document/10000036/10464864

2、实名认证说明文档：https://www.ctyun.cn/document/10000036/10013537

也可参考开通步骤如下：

【步骤 1】注册并登录天翼云 http://www.ctyun.cn

图 2-2 天翼云官网登录页面

热门产品分类

【步骤 2】未实名认证的用户请按提示完成实名认证才能开通网站安全监测服务

图 2-3 实名认证提醒

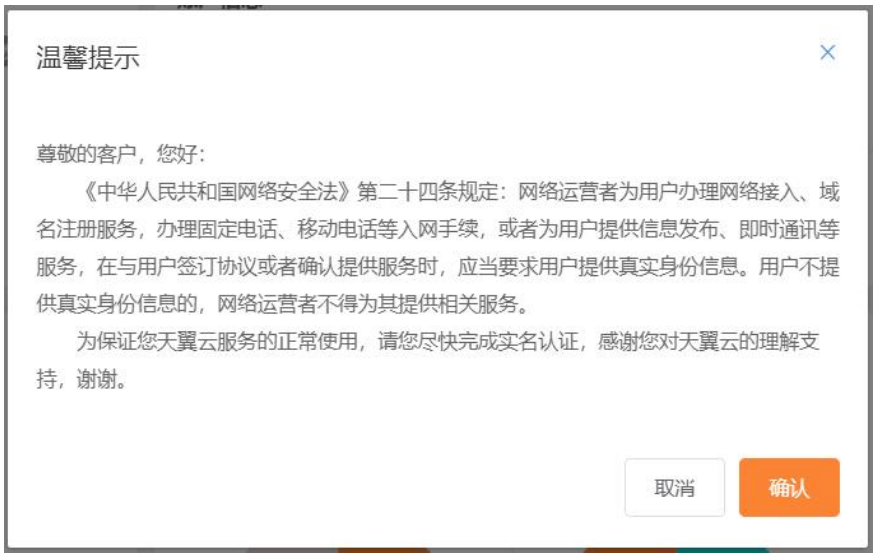


图 2-4 完成实名认证

【步骤 3】实名认证后进入网站安全监测产品详情页快速了解产品，之后单击“立即开通”；

图 2-5 产品详情页

【步骤 4】在购买页面选择适合的版本和所需功能，勾选并阅读服务协议，确认无误后点击“立即开通”，网站安全监测服务即开通；

图 2-6 产品开通页

【步骤 5】网站安全监测服务开通后，便可以根据操作手册去控制台开始接入您要监测的域名（天翼云网站安全监测控制台 https://cdn.ctyun.cn/h5/ctbrm）；

2.3 变更

您如果有变更计费的需求，可以联系客户经理或天翼云客服，提供您的变更需求。也可以登录官网，在订单管理-产品中找到您要变更的订单，点击“订购”进行产品变更，提交您的变更需求。目前套餐变更只支持升级套餐，不支持降级套餐的操作。

2.4 续费

续费步骤如下：

【步骤 1】在天翼云官网，点击用户菜单下的“基本信息“；

图 2-7 登录页

【步骤 2】进入“总览”页面，选择“账户充值”；

图 2-8 充值页面

【步骤 3】进入现金充值页面，在充值金额中输入充值金额，点击“充值”；

图 2-9 输入金额页面

【步骤 4】进入超级收银台页面，选择合适的支付方式完成付款；

图 2-10 付款方式页

2.5 续订服务

支持续订操作，登录官网订单管理-产品-产品视图-产品续订，提交您的续订需求，续订规则详见如下链接：https://www.ctyun.cn/document/10000038/10303747

图 2-11 产品续订页面

2.6 退订服务

产品支持退订服务，登录官网-订单管理-产品-产品视图-退订管理，找到您要退订的订单，进行退订；客户套餐退订后，扩展服务也会一起退订

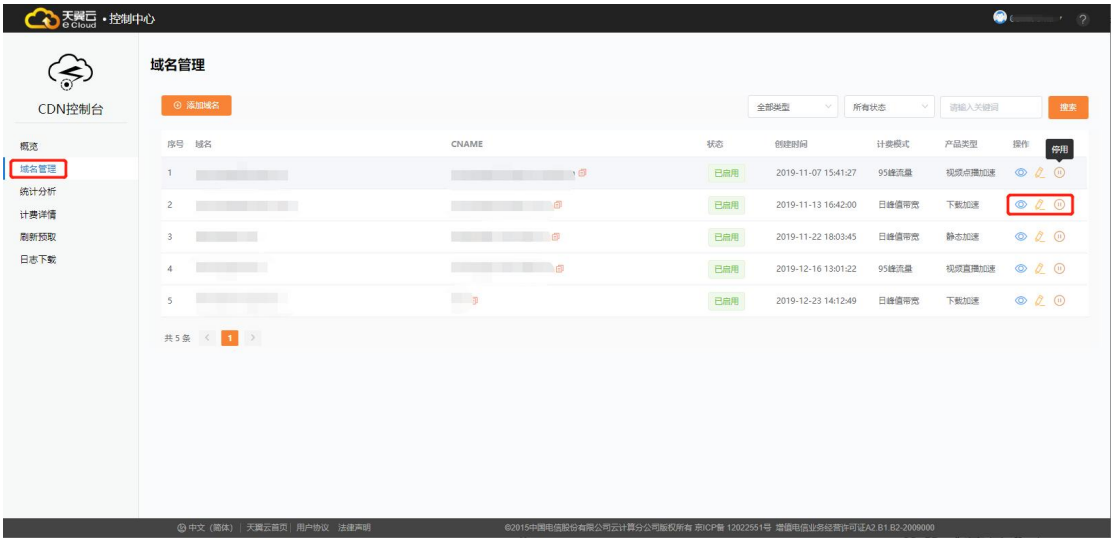
图 2-12 产品退订页面

2.7 关停服务

客户在客户天翼云账户中没有费用并欠款的情况下，通知客户充值，并将关停客户的网站安全监测服务。

客户也可以根据需求，进入客户控制台（https://cdn.ctyun.cn/h5/ctbrm）的“域名管理”页面，操作域名“停用”以及“启用”等操作。

图 2-13 域名管理页面



2.8 增值/定制内容申请

如果您有增值/定制的需求，您可以联系客户经理或天翼云客服，提交您的需求。也可以进入官网以工单的形式提交您的需求。

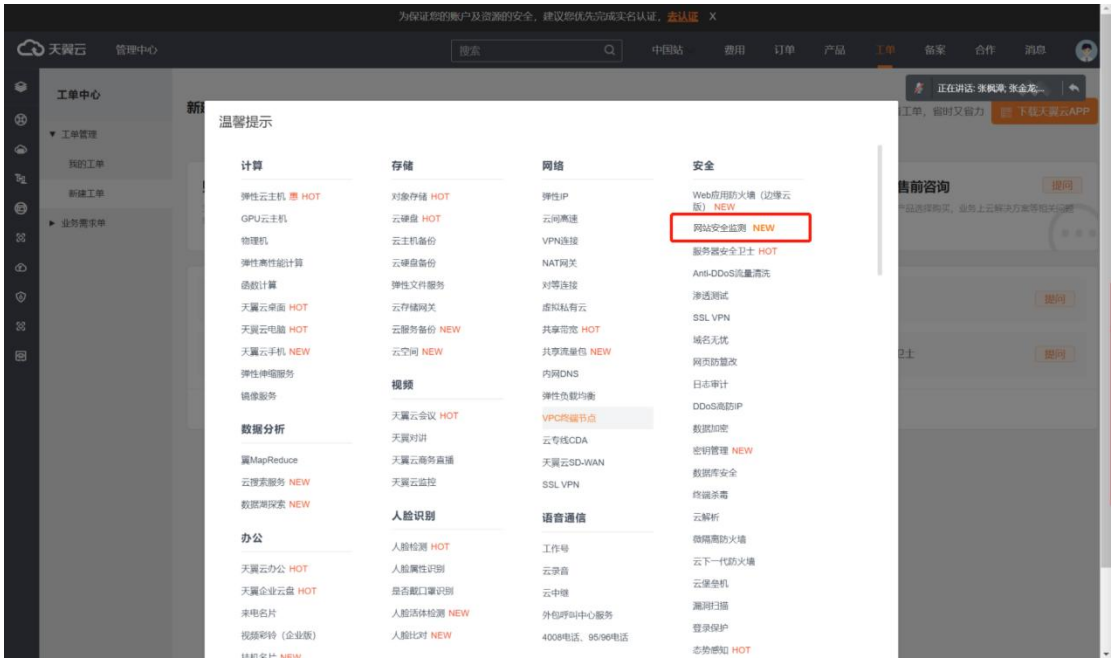
工单提交流程：

【第 1 步】登陆天翼云官网，点击用户菜单下的“工单管理“；

图 2-14 工单管理页面

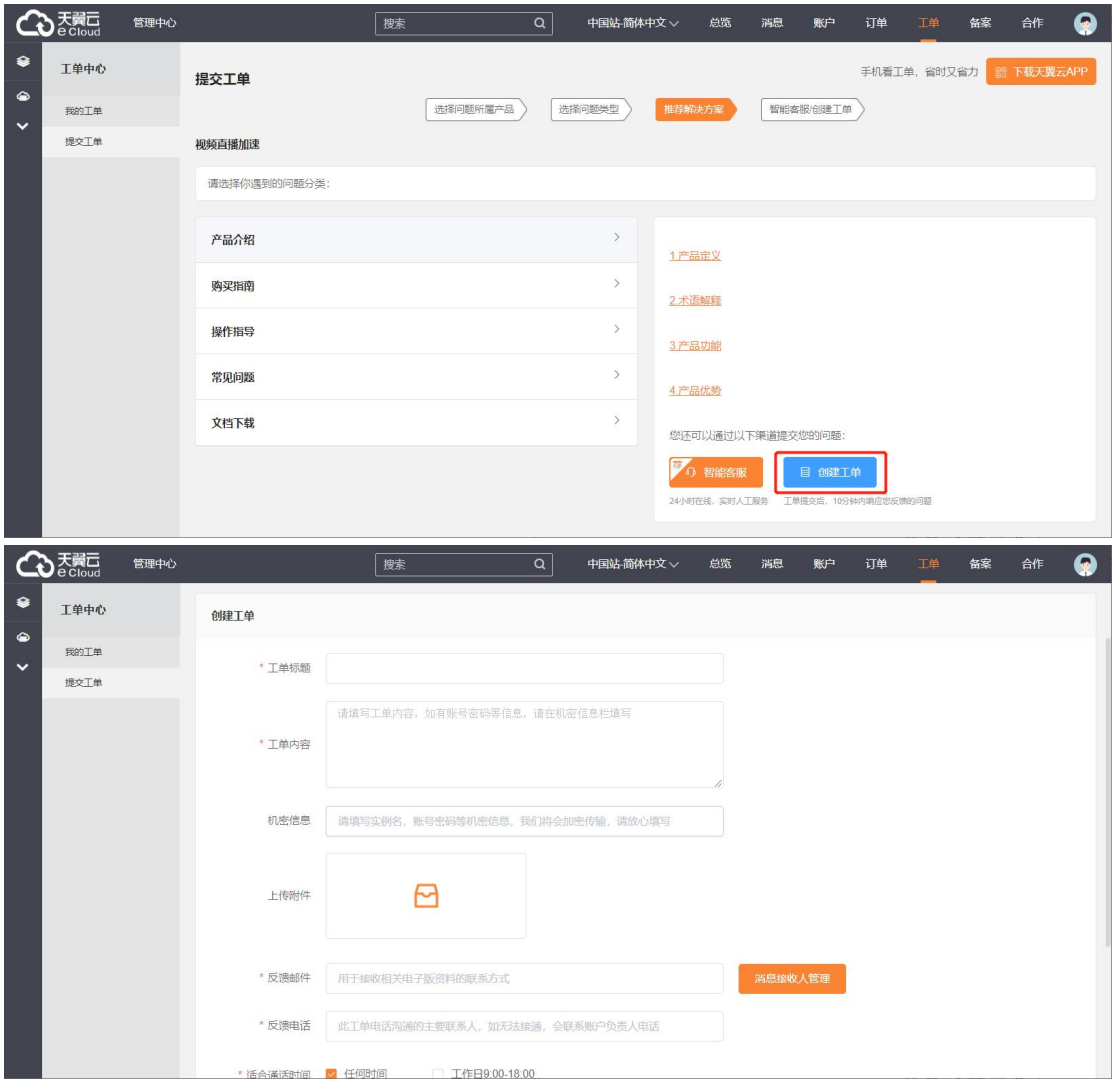
【第 2 步】进入“提交工单”页面，在网站安全监测业务处点击“提问”；

图 2-15 提交工单页面



【第 3 步】根据您的需求，选择“问题分类”，或“创建工单”

图 2-16 问题分类和创建工单页面

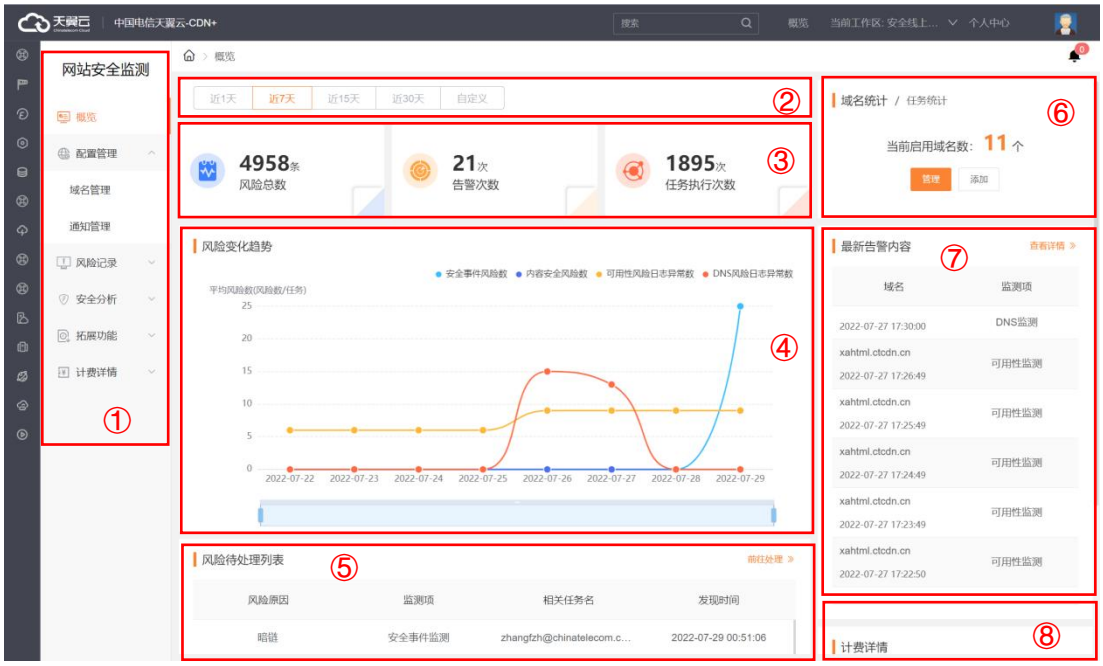


3 操作指导

3.1 控制台简介

天翼云网站安全监测控制台帮助您快速新增域名，并完成监测项任务配置操作，同时提供统计分析和报告下载等服务，帮助您对业务情况进行跟踪管理。

图 3-1 网站安全监测控制台-概览页



1、左侧栏导航

功能	概述
概览	可展示近 1 天、近 7 天最高 3 个月时间跨度数据，数据内容包括风险数、告警数、任务执行数、风险变化趋势、启用中域名数。同时展示风险和告警预览可一键跳转处理。计费详情展示产品订购情况。
配置管理	新增域名、管理删除已有域名，并可以对已新增的域名进行对应监测任务配置和管理，同时提供监测机节点 IP 列表供查询。
风险记录	查询告警记录和风险记录，管理风险记录进行相应加白、URL 封禁等操作，风险日志详情有助于定位风险。
安全分析	查看 5 类监测项的在线看板并管理漏洞报告和网站安全评估报告。
扩展功能	包含封禁管理和态势感知大屏，风险日志操作封禁后可在封禁管理内操作解禁和重新封禁等，态势感知大屏实时一站式展示安全数据。

计费详情	展示基础套餐和扩展服务的订购详情及订购状态。

2、概览页-筛选条件

筛选统计时间周期，作用域包含总览指标、风险变化趋势。默认选择 7 天的数据进行汇总统计显示，最长可选择 3 个月时间跨度。

3、概览页-总览指标

以客户为维度，展示统计周期限定下，总计的风险数、告警次数和任务执行次数。

4、概览页-风险变化趋势

以客户为维度，折线图形式，展示统计周期限定下，风险数变化的趋势。

5、概览页-风险待处理列表

以客户为维度，时间倒序展示当前发现的风险原因、对应监测项、相关任务名和风险发现时间。

6、概览页-域名统计/任务统计

以客户为维度，展示当前已启用服务的域名数总和，以及当前正开启中的任务数总和。

7、概览页-最新告警内容

以客户为维度，时间倒序展示当前发生告警的域名和对应产生告警的监测项，可以一键跳转至告警中心查看详情。

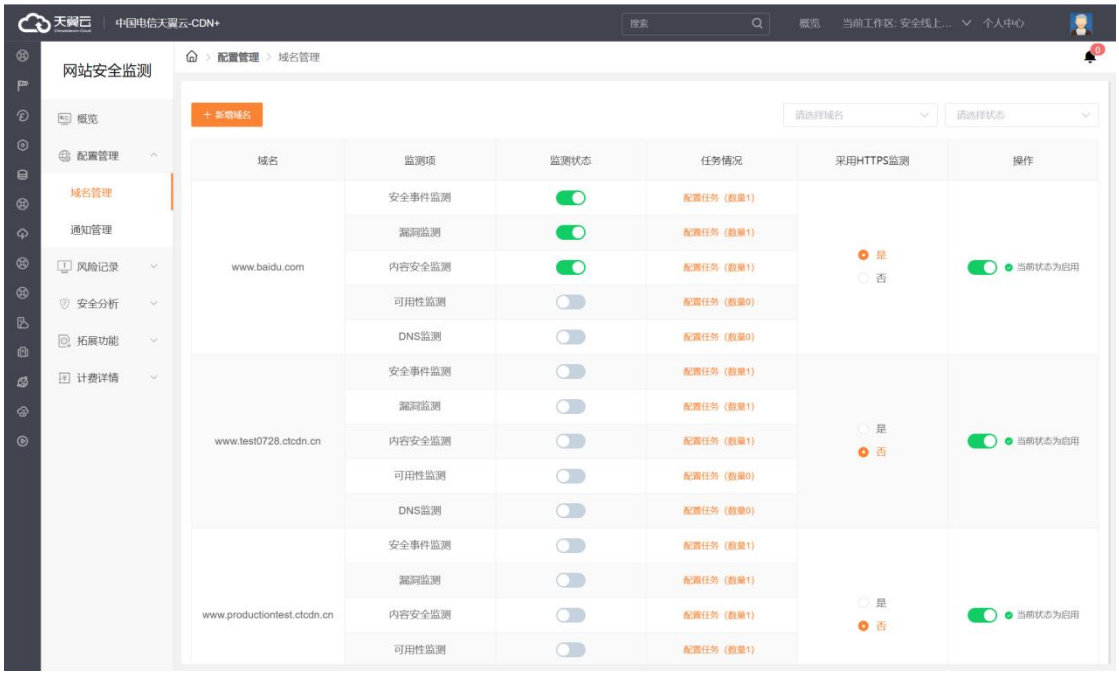
8、概览页-计费详情

展示主套餐和扩展服务状态。

3.2 域名管理

进入网站安全监测客户控制台配置管理模块，选择【域名管理】即可进入域名管理页面，在此页面您可以新增域名，或查看、编辑已添加的域名的信息，包括对应域名的监测项任务配置情况、监测状态、是否采用 HTTPS 监测和启用/关停开关。

图 3-2 域名管理页面

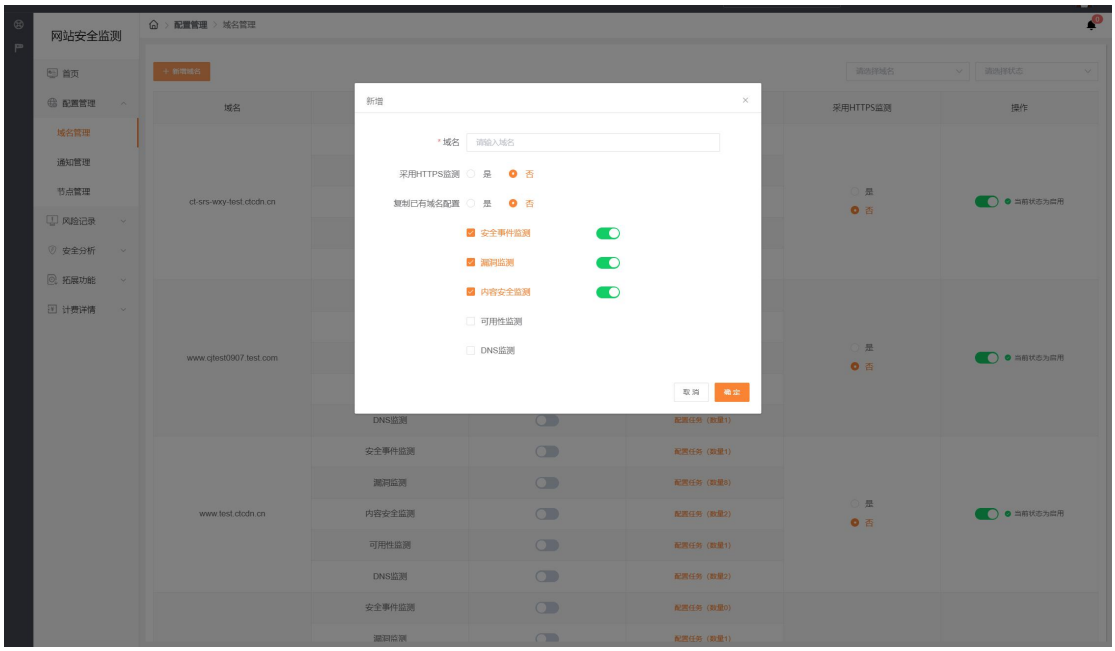


下面分步骤介绍域名新增、 删除的操作：

1、新增域名

点击【+新增域名】，弹出新增域名表单，填写域名新增信息。根据页面的引导填写域名、是否采用 HTTPS 监测、是否复制已有域名配置、若非复制已有域名配置则需要选择开启的子功能项（安全事件监测、漏洞监测、内容安全监测、可用性监测和 DNS 监测），选项填毕后点击确定即可完成域名的新增。

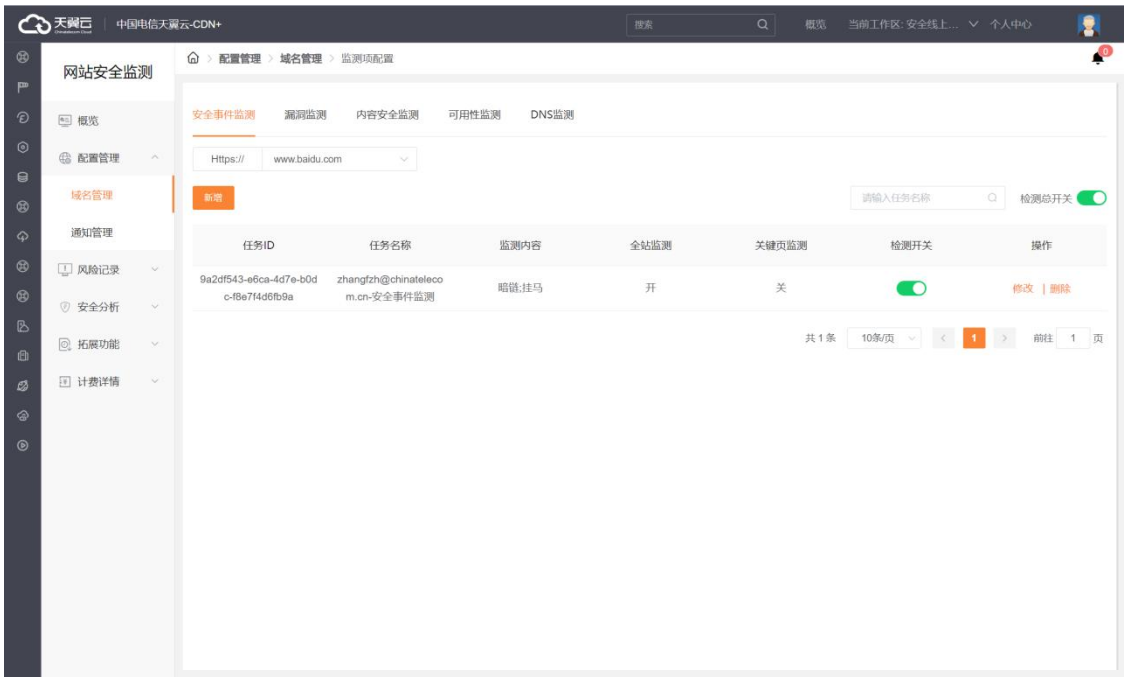
图 3-3 添加域名配置页



在域名添加完成后，可以按需配置监测项，您可以在某一域名的配置页面下切换不同的

监测子功能，并在子功能页面内配置任务。

图 3-4 域名安全配置信息页



温馨提示，为简化您的服务启用操作，新增域名（不复制已有域名配置）将默认开启安全事件监测、漏洞监测、内容安全监测 3 个监测项，并分别生成 3 条含默认配置的任务。5 个监测项对应的任务配置默认值请参照下表：

监测项	新增域名后默认配置项及默认值
安全事件监测	任务名称：客户名-安全事件监测 检测开关：开启 监测任务：全站监测开关开启，监测周期：1440 分钟，监测深度：监测当前页面及一级链接，关键页面监测开关关闭，是否抓取子域名开关关闭 监测内容：勾选暗链、黑链和挂马，域名和 URI 白名单默认为空 告警设置：连续检测 3 次异常通知 扫描开始时间：次日凌晨 1 点 通知方式：邮件
漏洞监测	任务名称：客户名-漏洞监测 检测开关：开启 监测漏洞等级：高危 检测范围：/ 检测当前目录以及一级链接 检测排除范围：空 检测计划：单次 扫描开始时间：次日凌晨 1 点 通知方式：邮件
内容安全监测	任务名称：客户名-内容安全监测 检测开关：开启 监测周期：60 分钟 检测 url：/ 检测当前目录及一级链接

	监测内容：文本检测-AI 审核-宽松 连续检测 3 次异常则产生通知 通知方式：邮件
可用性监测	任务名称：客户名-可用性监测 检测开关：开启 监测周期：30 分钟 检测 url：/favicon.ico 请求方法：head 检测区域：全选 告警设置：可用性 5xx 状态全选，大于等于 50% 连续监测 3 次则产生异常通知 通知方式：邮件
DNS 监测	任务名称：客户名-DNS 监测 检测开关：开启 监测周期：60 分钟 dns 查询类型：A 记录 是否指定 dns 服务器：否 预期解析值：1.2.3.6 （新增域名自己填写） 监测区域：全选 告警设置：解析不匹配数量 大于等于 50% 连续监测 3 次异常则产生通知 通知方式：邮件

2、删除域名

在所有监测项的监测状态都关闭，且域名的状态同时关闭后，将显示【删除】文字链，可操作域名删除。

图 3-5 域名安全配置信息页

3.3 域名归属权限验证

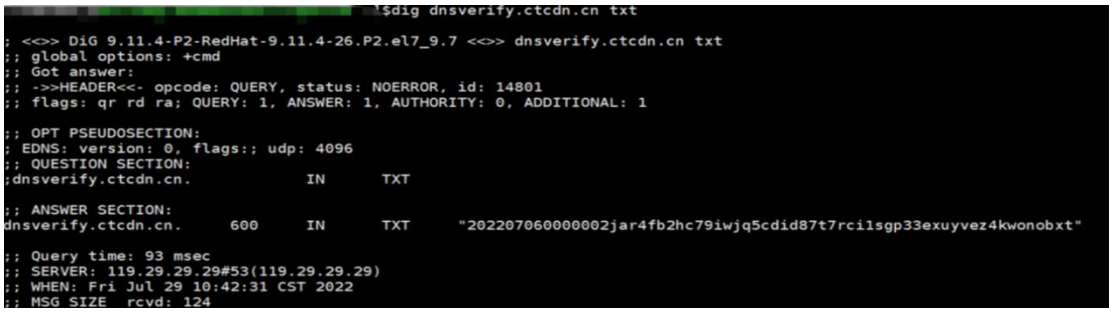
可根据如下方法一、方法二，任意选择一种方式进行操作验证即可。

3.3.1 方法一：DNS 解析验证

1、客户需在自己的域名解析服务商，添加天翼云控制台返回的 TXT 记录值（如下记录值仅为示例）。

记录类型	主机记录	记录值
TXT	dnsverify	202207060000002jar4fb2hc79iwjq5cdid87t7rci1sgp33exuyvez4kwonobxt

2、域名解析操作完成后，等待（建议 10 分钟）DNS 解析生效后即可进行解析验证。
解析命令：dig dnsverify.ctcdn.cn txt



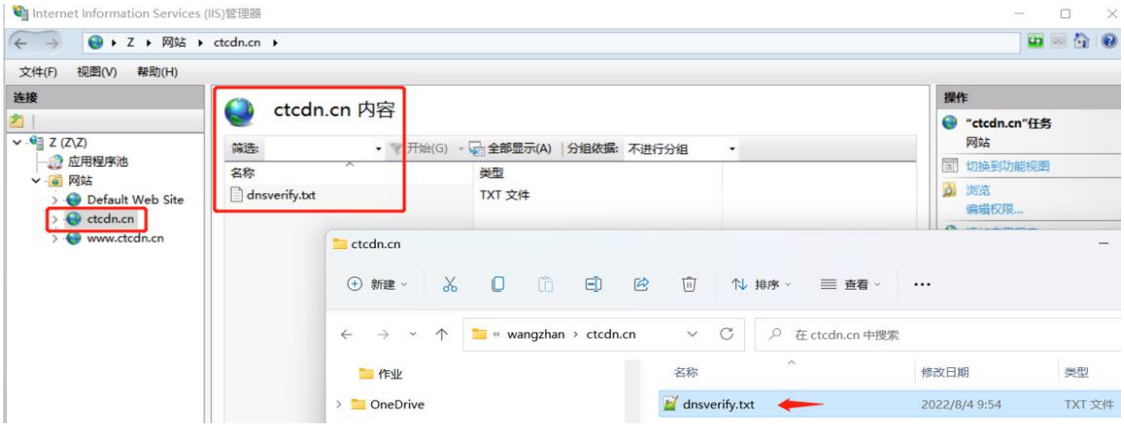
3、如解析出来的 txt 值和天翼云控制台返回的 TXT 记录值一致，则表示配置正确。
确认配置正确后，可前往天翼云控制台，在新增域名界面点击验证，验证通过就可以正常操作新增域名。

3.3.2 方法二：文件验证

示例为 ctcdn.cn 的解析配置

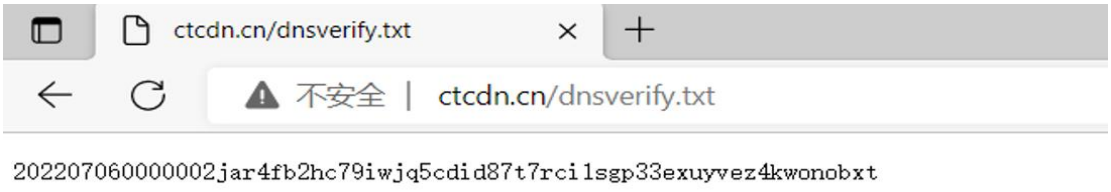
1、在您的源站根目录下，创建文件名为：dnsverify.txt 的文件，文件内容为天翼云控制

台返回的 TXT 记录值（如下记录值仅为示例）



2、文件在源站根目录下创建完成后，即可进行访问验证（示例为访问 http://ctcdn.cn/dnsverify.txt）

windows 验证：



linux 验证：

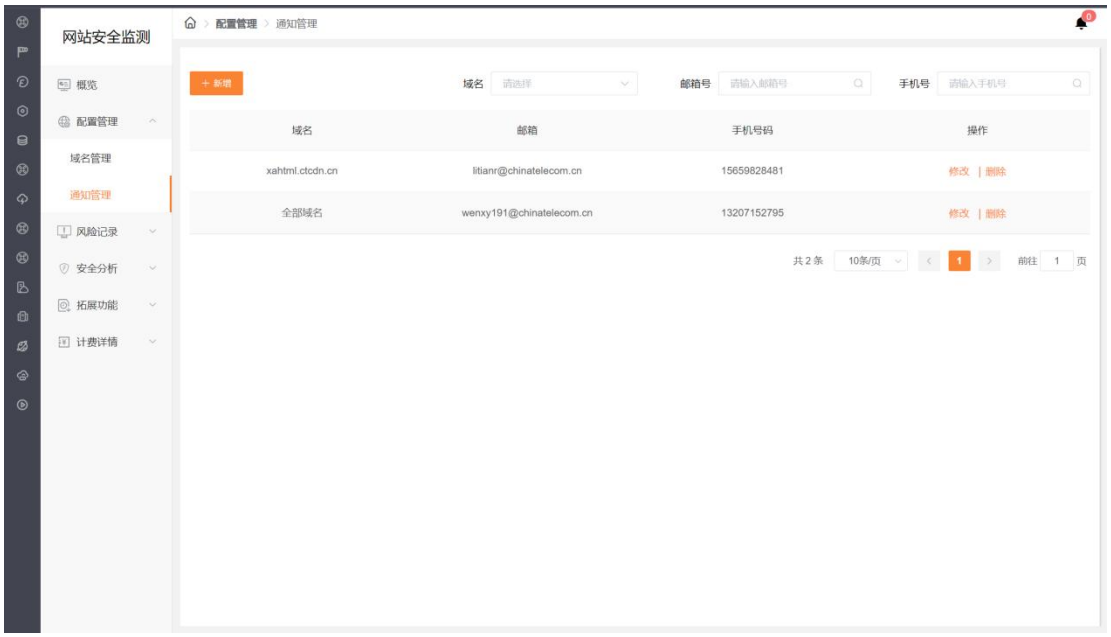
3、如访问展示的文件内容和天翼云控制台返回的 TXT 记录值一致，则表示配置正确。

确认配置正确后，可前往天翼云控制台，在新增域名界面点击验证，验证通过就可以正常操作新增域名。

3.4 通知管理

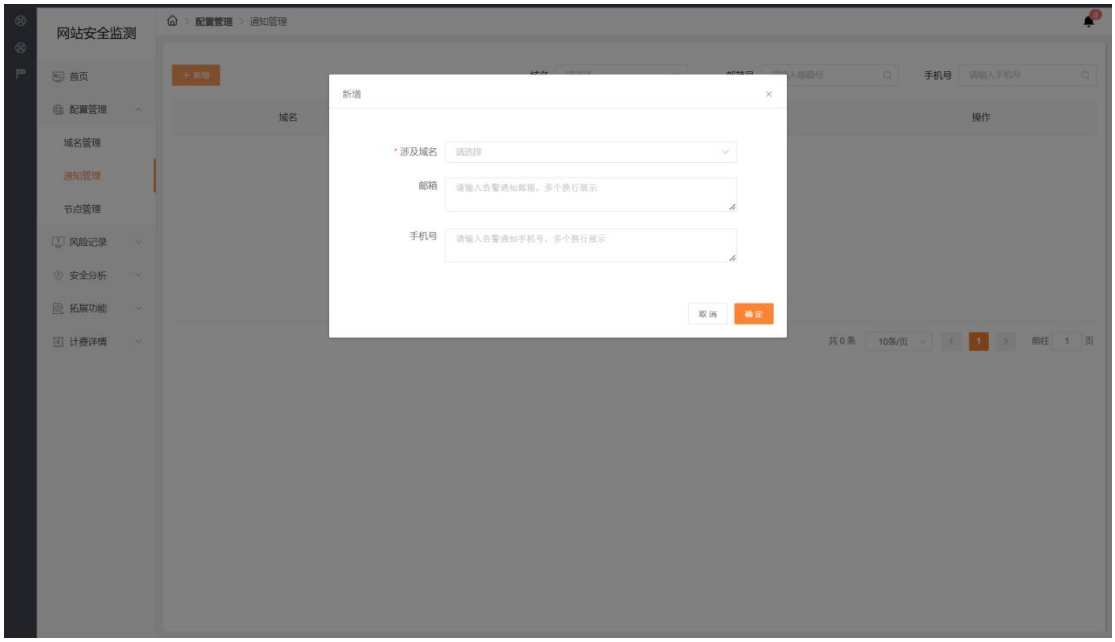
在【通知管理】中查看通知管理列表，可以查看已添加的域名对应通知邮箱、手机号码，和对应操作修改或删除。

图 3-6 通知管理列表页



通知方式可以通过新增按钮增加，点击【新增】，弹窗出现如下所示，可以将涉及的域名、邮箱、和手机号输入，这里邮箱和手机号支持多个输入。

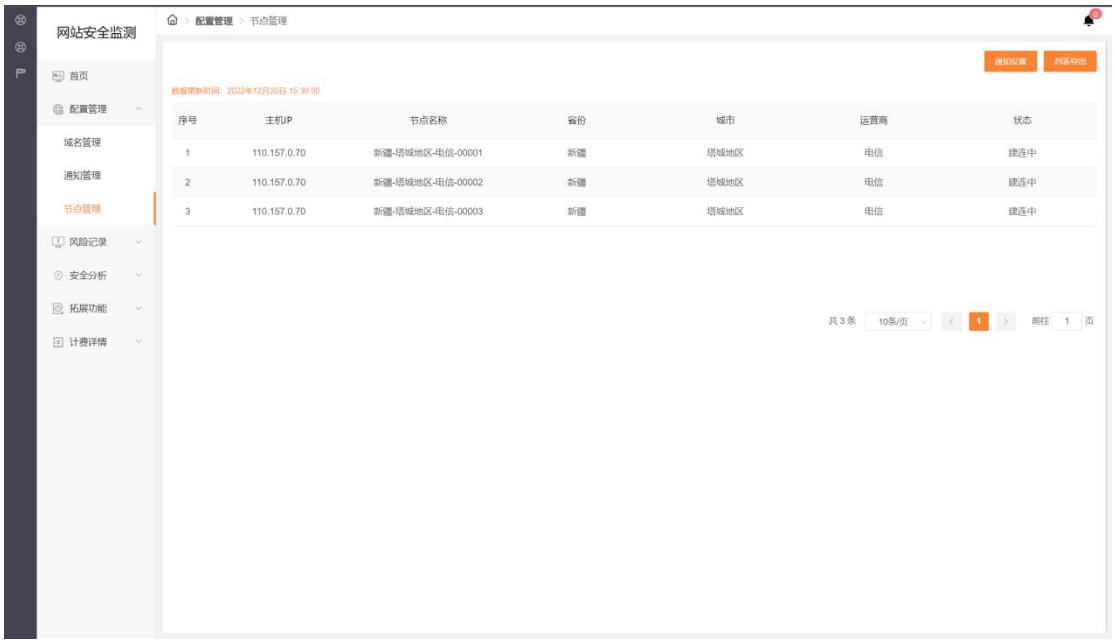
图 3-7 通知管理新增表单



3.5 节点管理

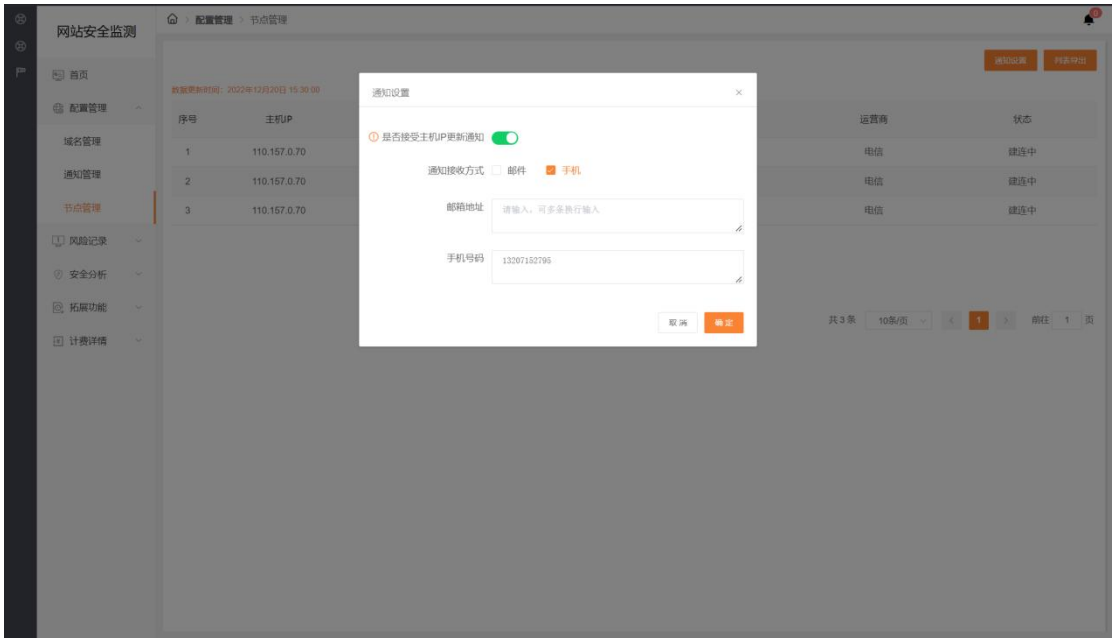
进入【节点管理】可以查看和导出服务中的监测机节点 IP 地址和省份、运营商、状态等详情列表，便于您进行服务器加白操作。

图 3-8 监测机 IP 详情列表



监测机服务状态发生变更时，将以邮件或手机短信的方式通知您，请点击【通知设置】进入表单页设置您的邮箱地址和手机号码以顺利接收信息，若不想接收此信息可以关闭通知开关。

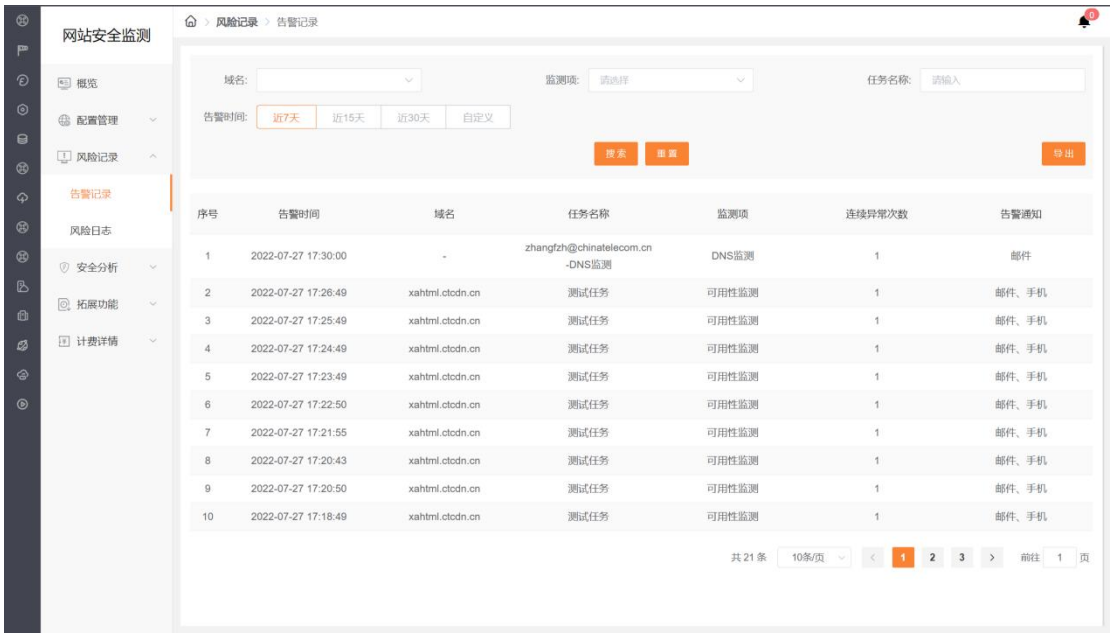
图 3-9 监测机变更通知设置



3.6 告警记录

在【告警记录】中查看告警通知，点击【导出】按钮，可以 Excel 文件形式导出告警记录列表，筛选区域方便您从域名、监测项、任务名称和告警时间多维度过滤告警信息。

图 3-10 告警记录列表页



3.7 风险日志

通过查看风险日志，您可以了解网站安全监测产品各项子功能模块下风险、漏洞发生的情况，并批量处理不同风险、漏洞。

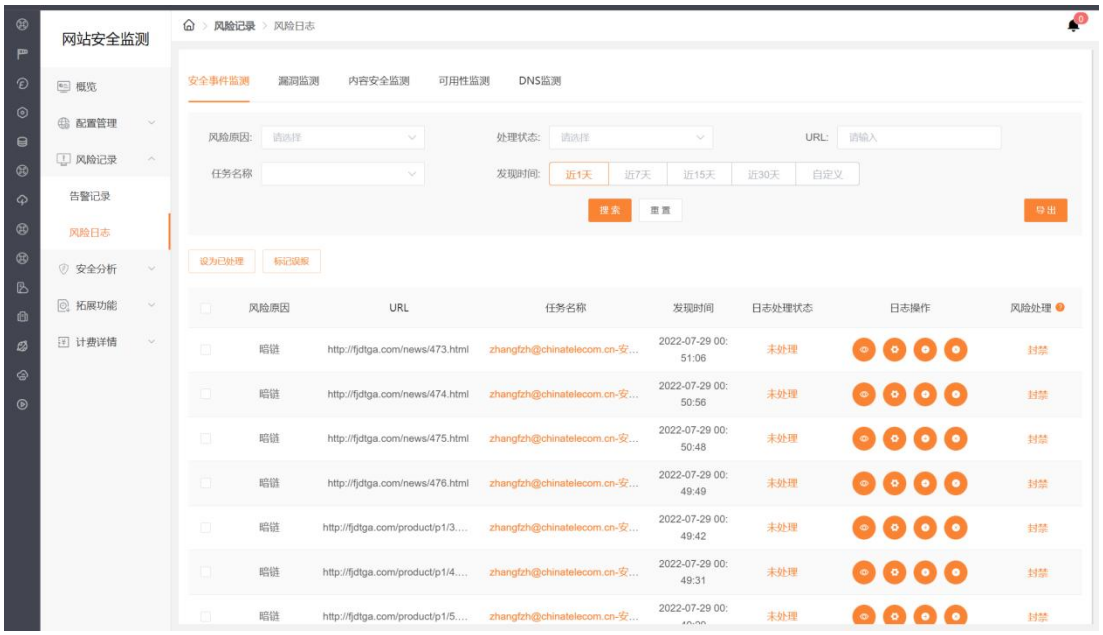
3.7.1 风险日志-安全事件监测

可通过筛选项进行组合查询，筛选项包括风险原因、处理状态、URL 和发现时间等，若没有选择条件则显示所有风险列表；

列表呈现信息为风险原因、对应 URL、发现时间和处理状态，其中可操作的范围随处理状态变化，若风险未处理可以将风险设为已处理、加入白名单或者标记误报，若风险已处理或加入白名单则可以刷新基线；

若同域名同时开通了 Web 应用防火墙（边缘云版），则可以使用风险处理功能，一键封禁发现风险的 URL，同时可以在 Web 应用防火墙（边缘云版）的威胁管控-封禁/解封查看到下发的任务。

图 3-11 安全事件监测风险日志



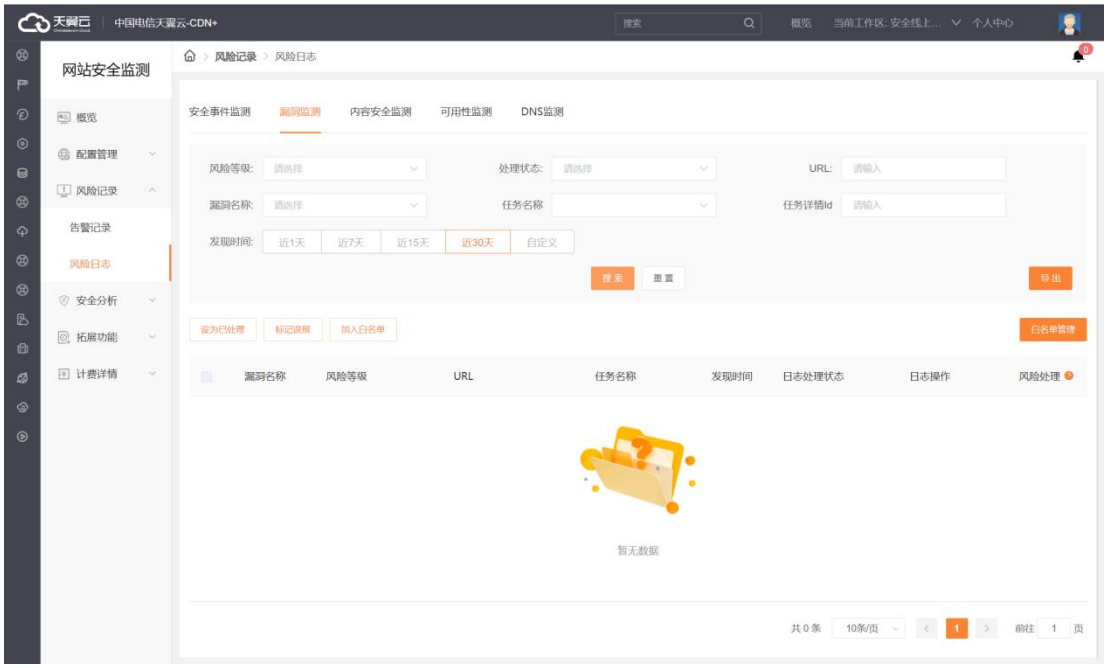
3.7.2 风险日志-漏洞监测

可通过筛选项进行组合查询，筛选项包括风险等级、处理状态、漏洞名称、URL 和发现时间等，若没有选择条件则显示所有漏洞列表；

列表呈现信息为漏洞名称、风险等级、URL、发现时间和处理状态，其中可操作的范围随处理状态变化，若风险未处理可以将风险设为已处理、加入白名单或者标记误报，若风险已处理或加入白名单则可以刷新基线，同时可以查看漏洞情况。

若同域名同时开通了 Web 应用防火墙（边缘云版），则可以使用风险处理功能，一键封禁发现风险的 URL，同时可以在 Web 应用防火墙（边缘云版）的威胁管控-封禁/解封查看到下发的任务。

图 3-12 漏洞监测风险日志

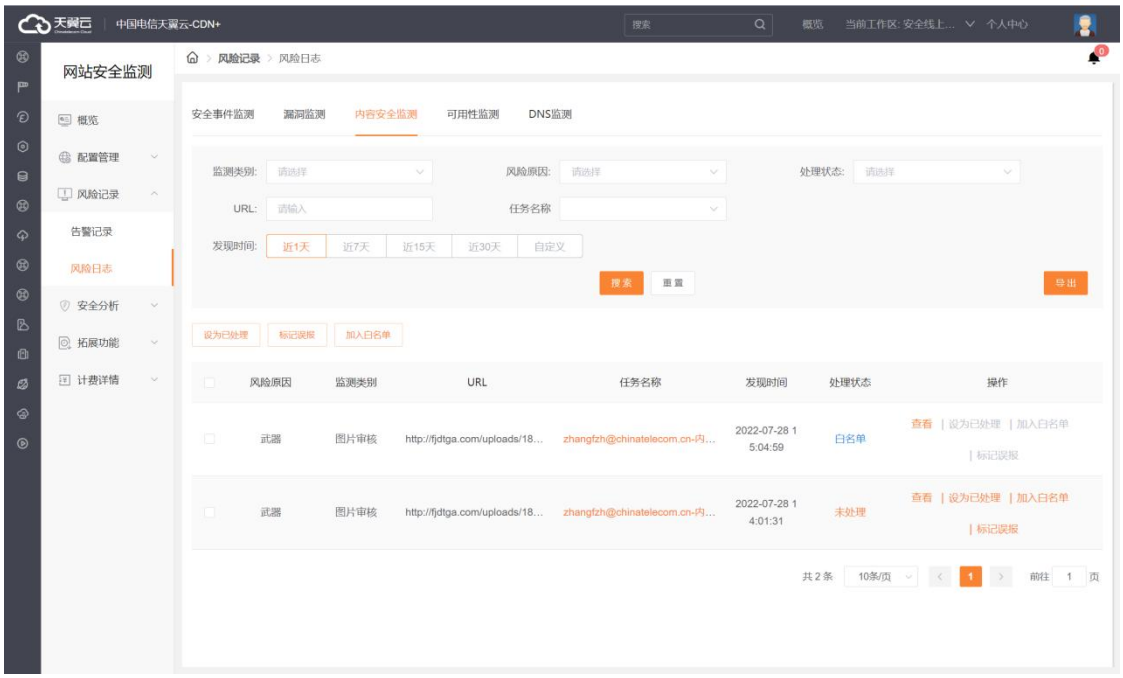


3.7.3 风险日志-内容安全监测

可通过筛选项进行组合查询，筛选项包括监测类别、风险原因、处理状态、URL 和发现时间等，若没有选择条件则显示所有风险列表；

列表呈现信息为风险原因、监测类别、URL、发现时间和处理状态，其中可操作的范围随处理状态变化，若风险日志未处理则可以操作设为已处理、加入白名单和标记误报，加白操作后状态将更新为白名单，同时操作可以批量进行。

图 3-13 内容安全监测风险日志

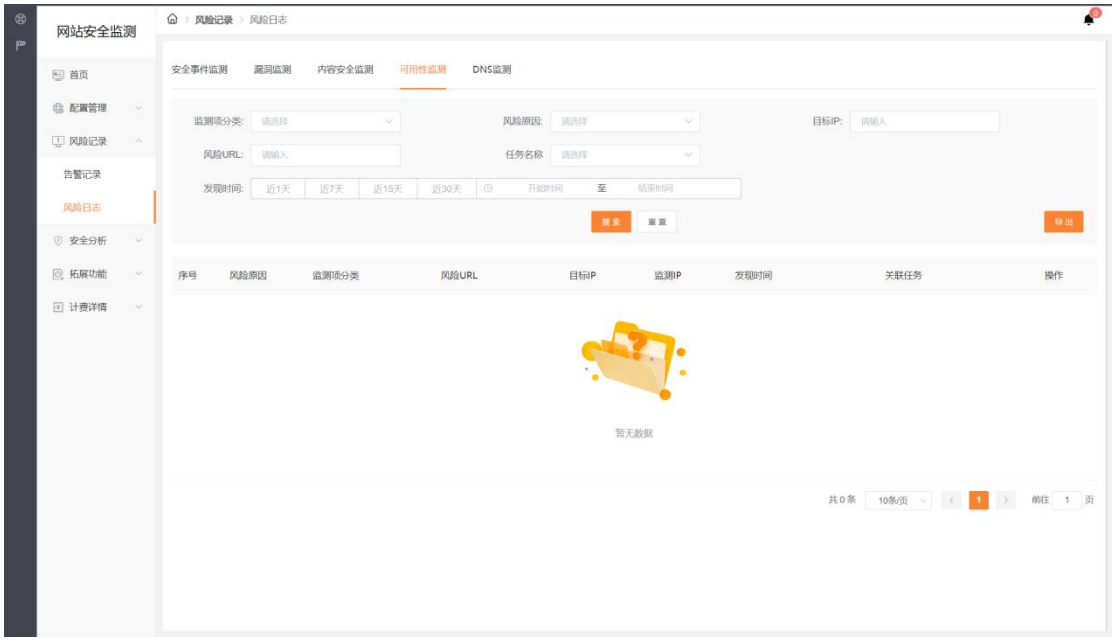


3.7.4 风险日志-可用性监测

可通过筛选项进行组合查询，筛选项包括风险等级、处理状态、漏洞名称、URL 和发现时间等，若没有选择条件则显示所有风险列表；

列表呈现信息为风险原因、监测项分类、URL、目标 IP、监测节点和发现时间，可用性监测的每条风险日志通过关联任务查看详情。

图 3-14 可用性监测风险日志

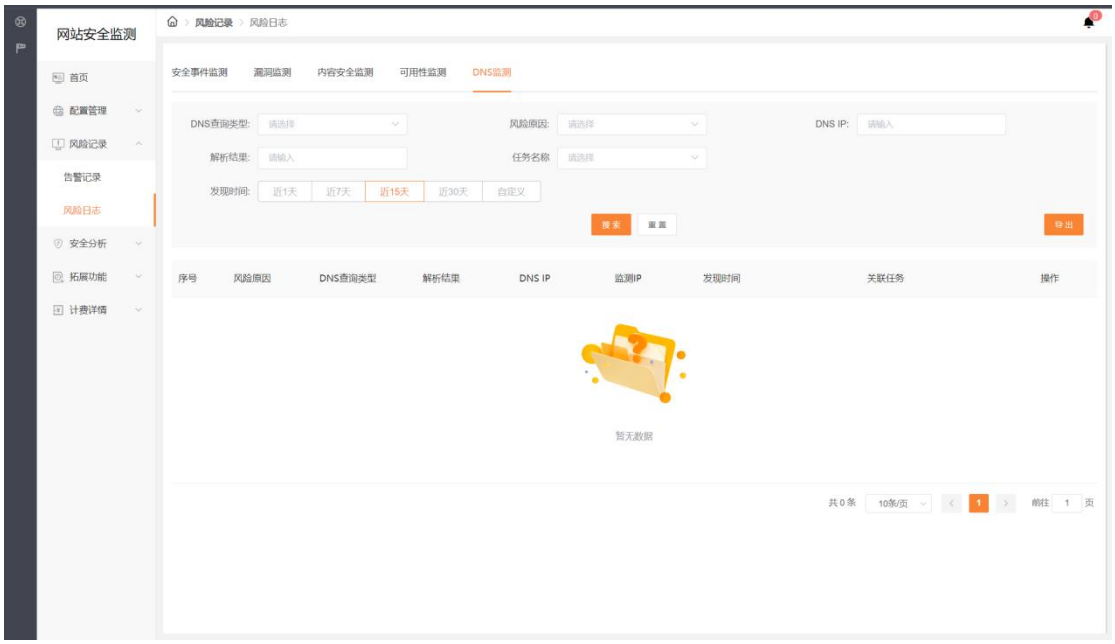


3.7.5 风险日志-DNS 监测

可通过筛选项进行组合查询，筛选项包括风险原因、DNS 查询类型、DNS IP、预期解析值和发现时间等，若没有选择条件则显示所有风险列表；

同可用性监测，列表呈现信息为风险原因、DNS 查询类型、解析结果、DNS IP、监测 IP 和发现时间，可用性监测的每条风险日志通过关联任务查看详情。

图 3-15 DNS 监测风险日志



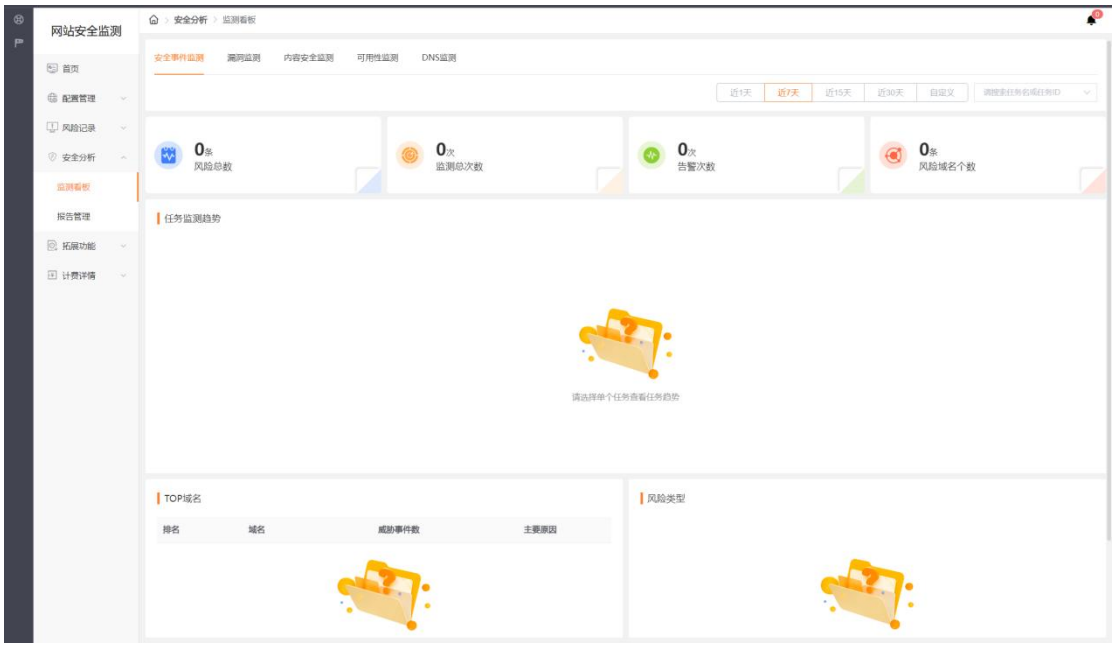
3.8 监测看板

网站安全监测客户控制台的【安全分析】页面，客户可以查看各子功能项监测报表。

3.8.1 安全报表-安全事件监测

可通过筛选项进行组合查询，筛选项包括不同时间维度和任务；指标数据展示区域包括总览数据、任务监测趋势、TOP 域名、风险类型、TOP URL。

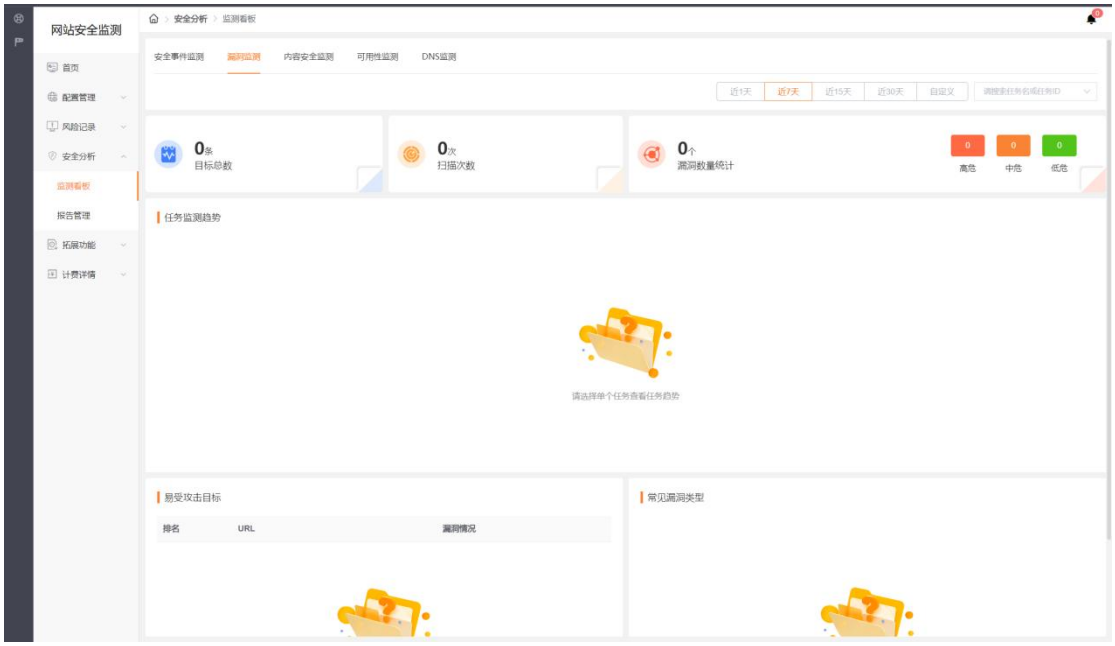
图 3-16 安全事件监测报表



3.8.2 安全报表-漏洞监测

漏洞监测看板可通过筛选项进行组合查询，筛选项包括不同时间维度、不同域名和任务；多块数据展示区域包括总览数据、任务监测趋势、TOP 易受攻击目标、常见漏洞类型。

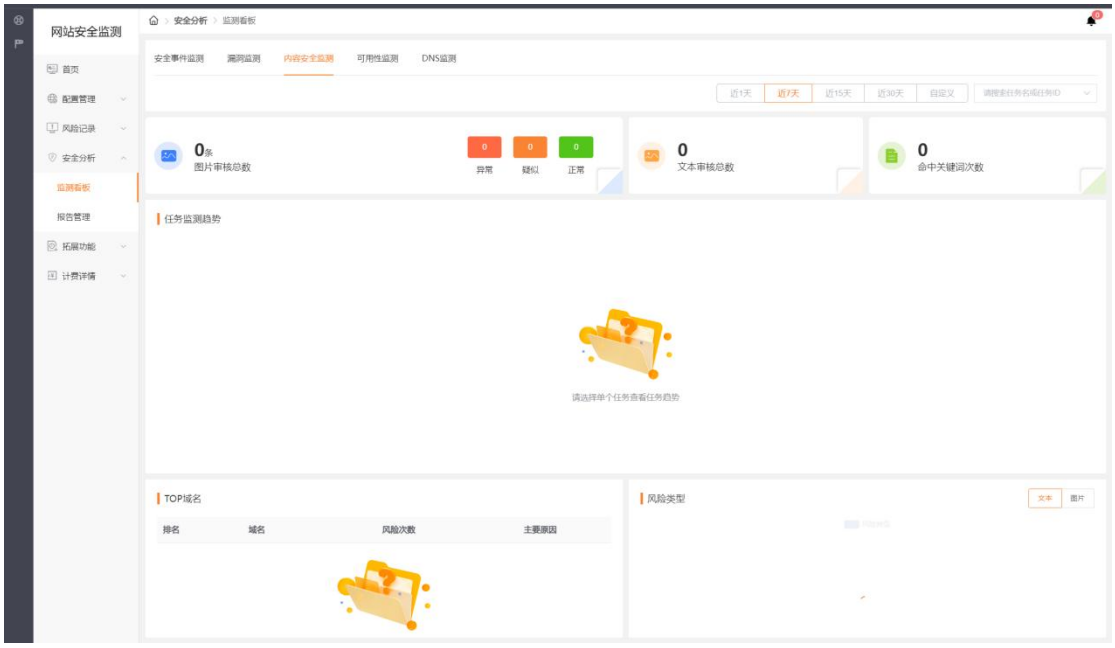
图 3-17 漏洞监测报表



3.8.3 安全报表-内容安全监测

可通过筛选项进行组合查询，筛选项包括不同时间维度、不同域名和任务；
多块数据展示区域包括总览数据、任务监测趋势、TOP 域名、风险类型。

图 3-18 内容安全监测报表

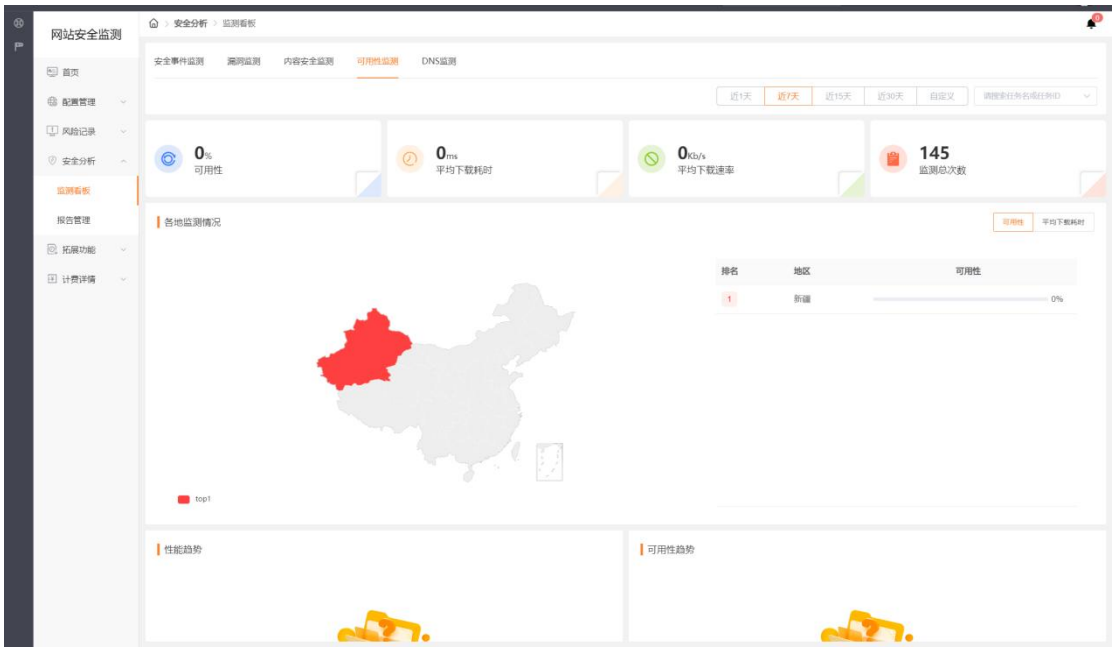


3.8.4 安全报表-可用性监测

可通过筛选项进行组合查询，筛选项包括不同时间维度、不同域名和任务；

多块数据展示区域包括总览数据、各地监测情况、性能趋势、可用性趋势、性能趋势、步骤耗时。

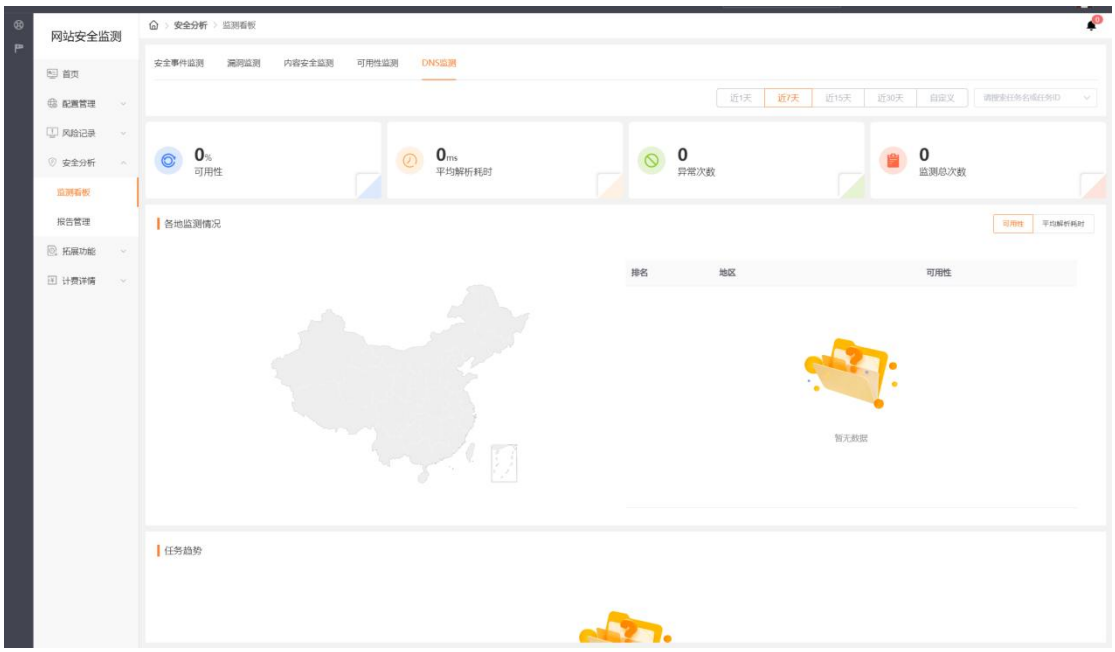
图 3-19 可用性监测报表



3.8.5 安全报表-DNS 监测

可通过筛选项进行组合查询，筛选项包括不同时间维度、不同域名和任务；
多块数据展示区域包括总览数据、各地监测情况、任务趋势、错误类型、劫持情况。

图 3-20 DNS 监测报表

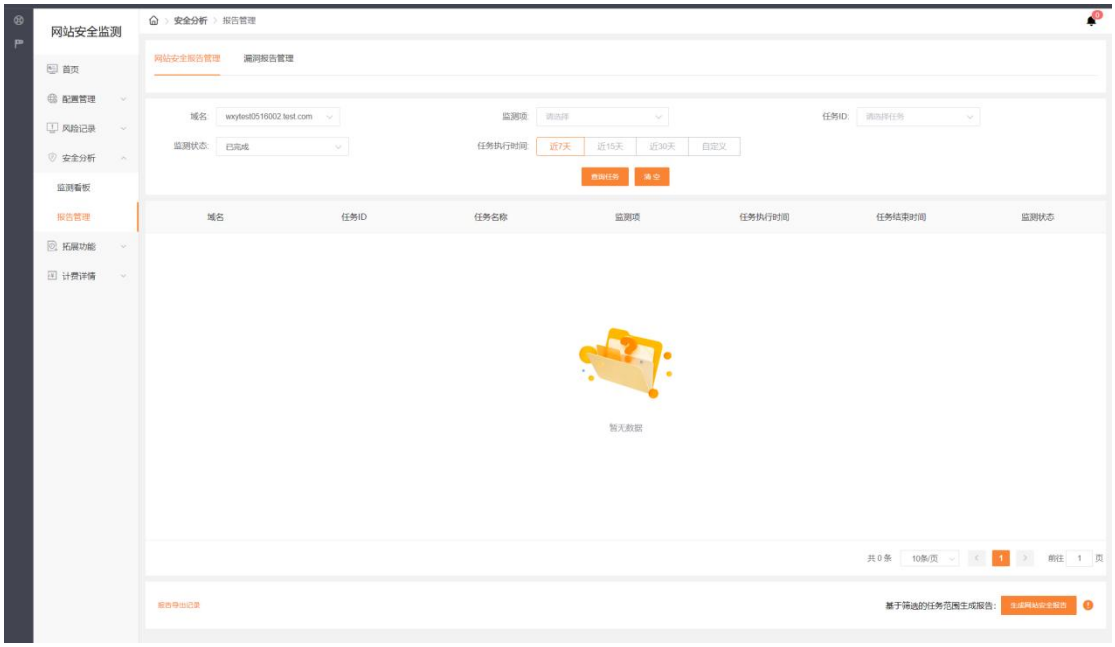


3.9 报告管理

3.9.1 网站安全报告管理

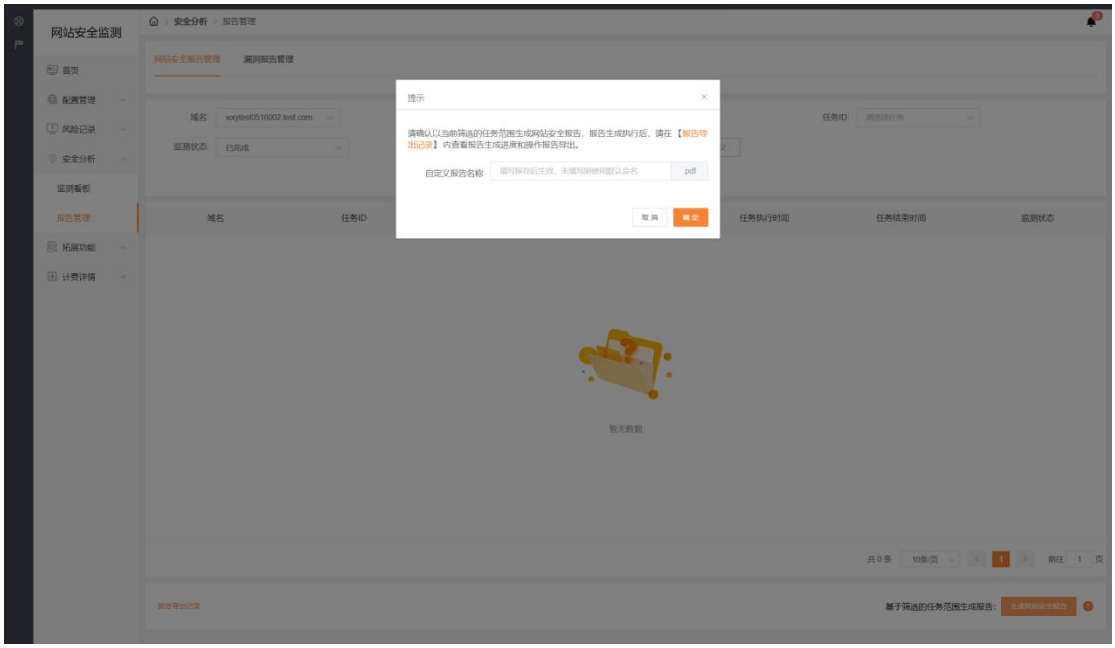
导航安全分析板块，选择【报告管理】，即可进入网站安全报告管理页。根据选择的域名其下的任务记录，可以生成相应任务的结果聚合报告——《网站安全评估报告》。

图 3-21 网站安全报告管理



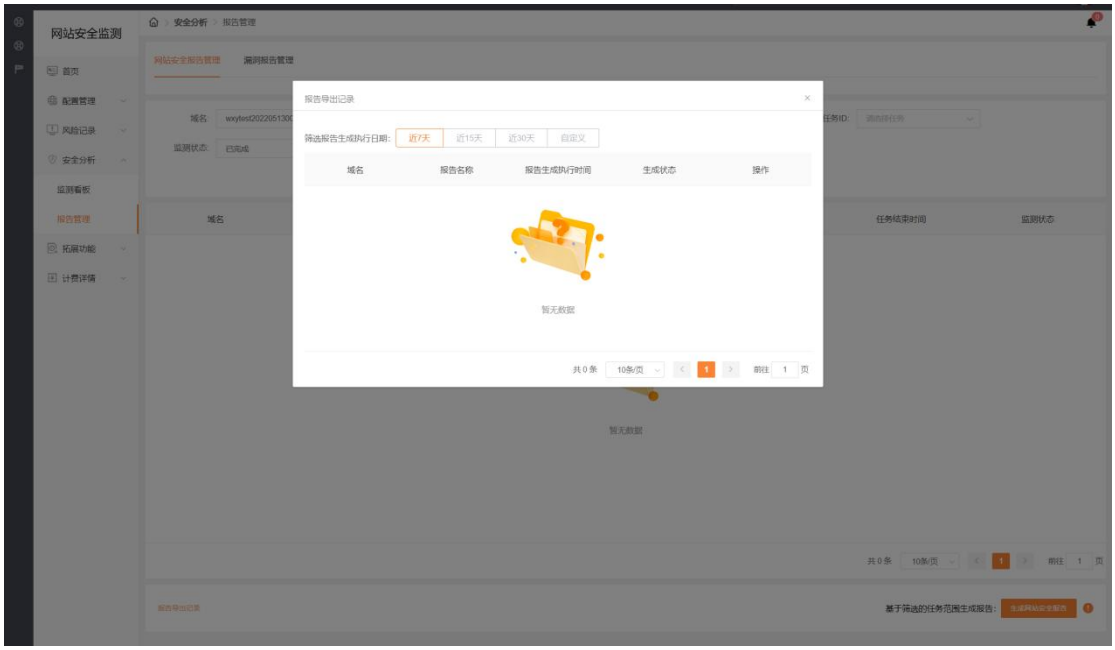
根据筛选项选出想要生成结果报告的监测任务后（注意仅已完成的任务可以用于报告生成），点击【生成网站安全报告】，可进入下图所示表单确认报告名称，默认以时间戳形式命名报告，点击确认即可生成报告。

图 3-22 网站安全报告导出



报告生成的结果，可点击左下角【报告导出记录】进行查看，操作导出或删除报告。

图 3-23 网站安全报告导出记录

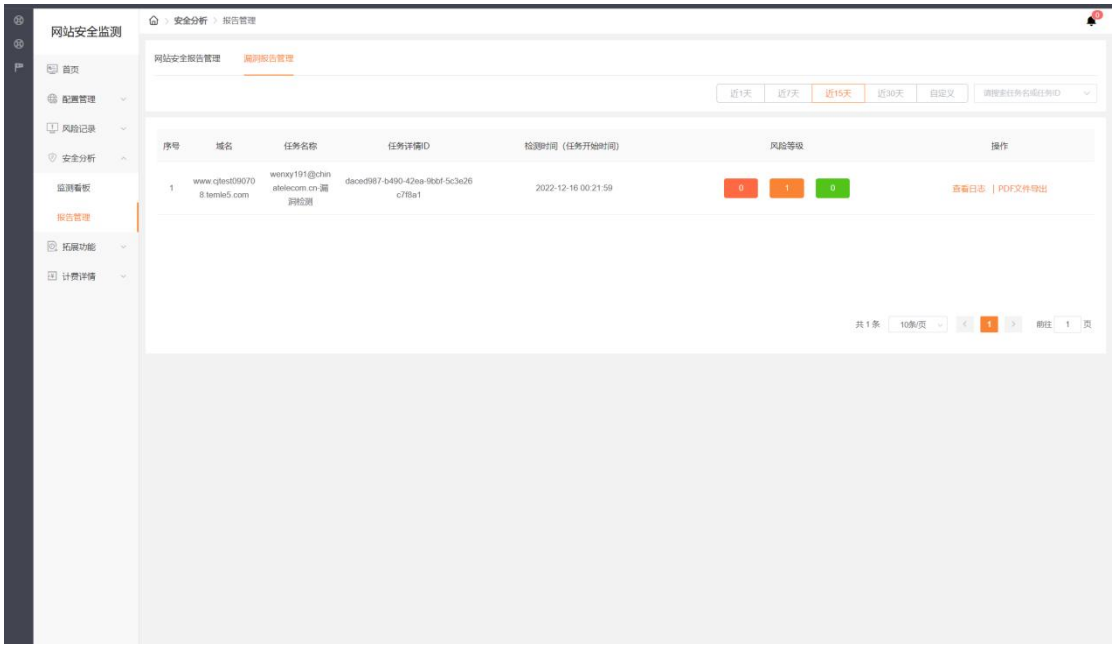


3.9.2 漏洞报告管理

点选 TAB【漏洞报告管理】即可切换页面对漏洞扫描报告进行管理。

可选择不同时间周期下，不同任务的漏洞扫描结果，结果记录以列表呈现，展示域名、任务名称、任务详情 ID、任务开始时间和漏洞等级分布情况，可操作导出 PDF 报告（发现漏洞时生成报告）或查看风险日志。

图 3-24 漏洞报告管理



3.10 封禁管理

导航拓展功能模块下【封禁管理】仅在您同域名同时开通 Web 应用防火墙（边缘云版）时可以使用。

从风险日志中操作封禁成功后，会在封禁管理生成对应封禁记录，同时会进行联动 Web 应用防火墙（边缘云版）威胁管控下发封禁任务。您可以在封禁管理内操作解封和重新封禁。

图 3-25 封禁管理

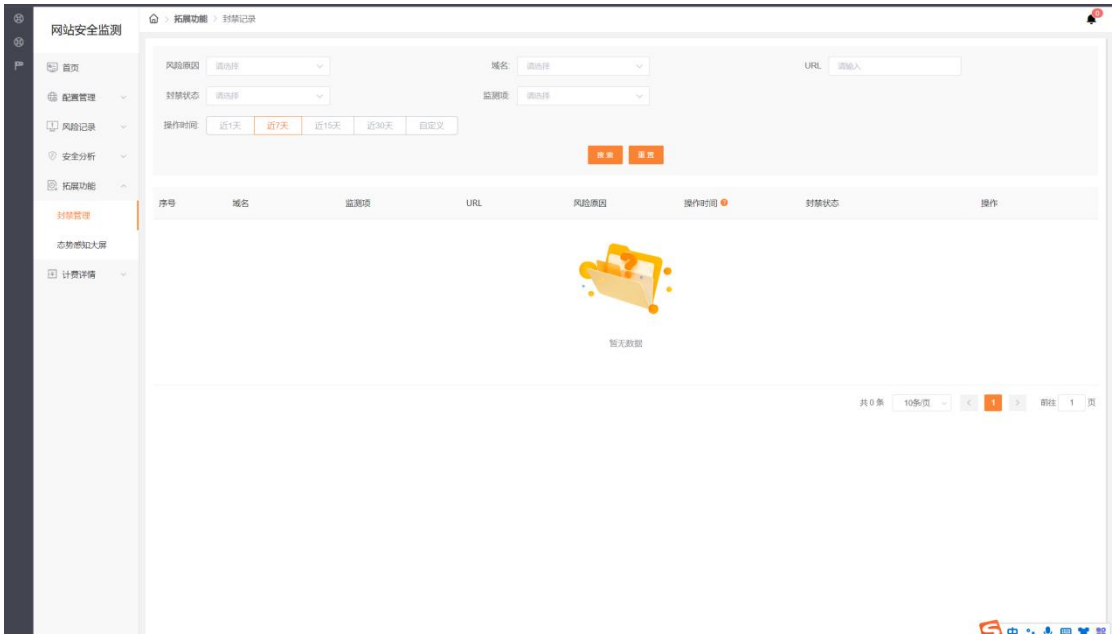


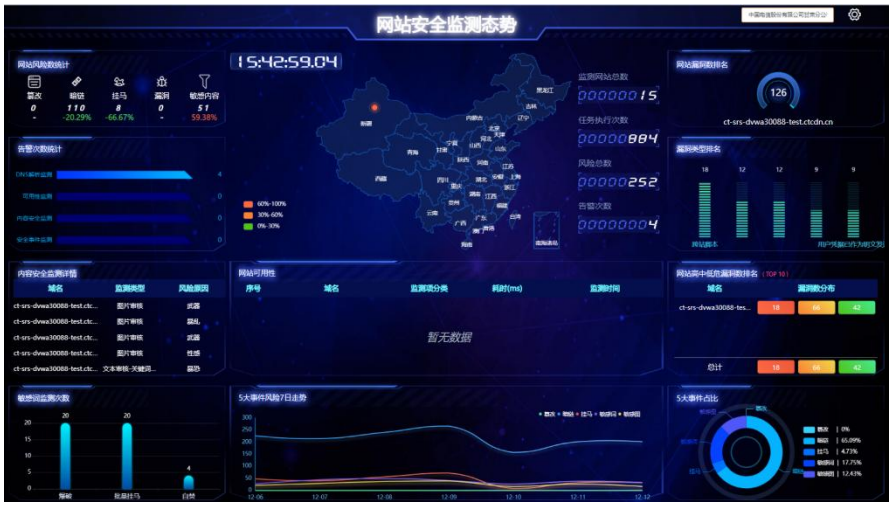
图 3-26 封禁管理列表详情

3.11 态势感知

导航拓展功能模块下点击【态势感知大屏】即可进入态势感知大屏页面，您在控制台配置的全部域名，其对应的业务数据将在此态势感知大屏中一站式呈现，助您实时跟踪网站风险态势，及时定位问题，明确处理方向。

注：使用态势感知大屏功能需开通态势感知大屏扩展服务。

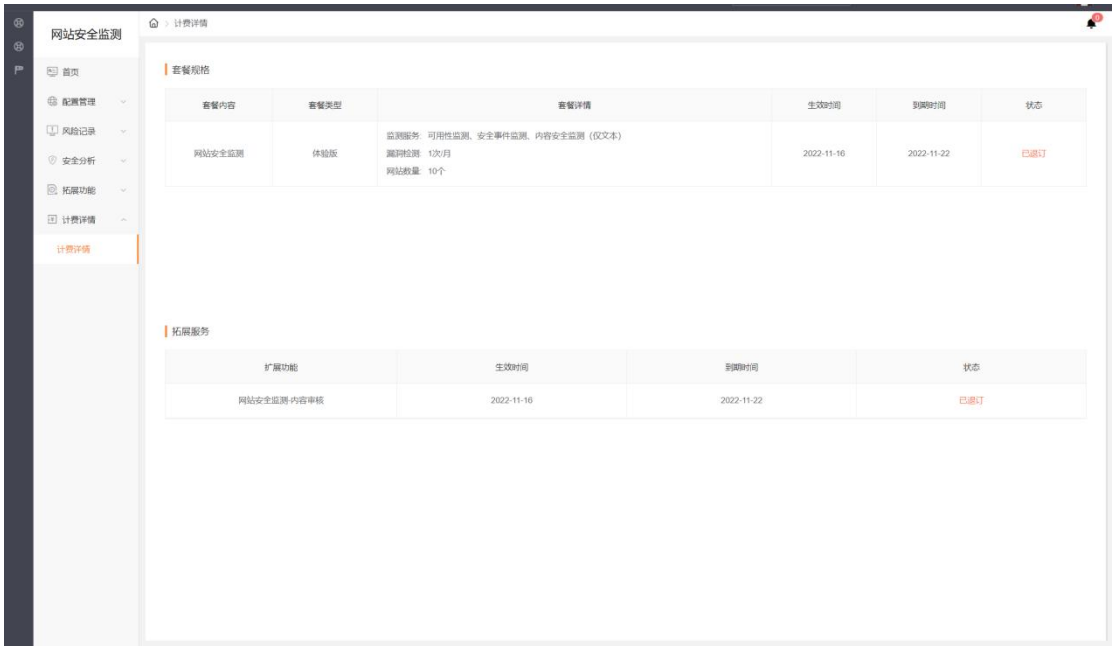
图 3-27 态势感知大屏



3.12 计费详情

进入网站安全监测客户控制台的【计费详情】页面，您可以查看所购买的套餐和扩展服务，其各自的详情和使用状态。

图 3-28 计费详情



4 常见问题

4.1 营销推广类

Q:网站安全监测产品有不同规格、应该选择哪个，该如何选择？

A:网站安全监测当前有体验版、专业版和旗舰版三个版本，每个版本在功能和漏洞检测频率有差异。基础业务安全监测需求推荐使用体验版，提供可用性监测、安全事件监测、内容安全监测等。如果有图片审核需求推荐专业版的套餐，提供基础业务安全监测的同时，也提供图片审核功能。用户需要自定义配置需求就推荐旗舰版套餐，可支持自定义配置和人工验证等操作，按需购买即可。

Q:网站安全监测的产品是否支持试用？

A:可以支持试用，可以在 BCP 门户申请试用，目前官网暂未开通试用通道，试用期限为一个月，支持可用性监测，安全事件监测、内容安全监测和图片审核限量 100 张，漏洞检测一次。

Q:产品网站安全监测产品有哪些优势？

A:应用快、免安装，使用便捷，纯 SaaS 服务，无需安装任何软硬件，只需在控制台提交域名和具体的监测项即可，随买随用。

资源丰富，全网服务，分布式部署，支持多点检测，资源覆盖全国。

可视化管理平台，对用户友好，可视化看板、报表和态势跟踪全方位辅助业务数据跟踪，更好地进行业务管理。

高效率，高专业度：集中监控和分散维护相结合，值班工程师 7×24 小时集中监控，网络工程师 7×24 小时在线支持。

Q:如果客户目前使用的是非天翼云的服务，是否可以使用网站安全监测产品？

A:网站安全监测产品对客户使用服务是没有限制的，只要购买服务，在控制台配置域名和监测项即可，无需客户改变任何网络架构，不需要修改 CNAME。

Q:版本和扩展服务的有效期之间是否有关联？

A:是的，扩展服务的有效期是与版本的有效期一致的，如果用户的版本过期，扩展服务的功能也随之失效。

Q:用户可以直接购买扩展服务进行使用吗？

A:不能直接购买扩展服务使用，用户需要选择版本后，可以购买扩展服务态势感知大屏进行使用，订购扩展服务的前提是必须订购版本且版本在服务中的状态。

4.2 计费类

Q:图片审核的功能怎么收费？

A:图片审核功能是按需收费，图片审核分为两种方式，一种是确认审核的图片，一种是不确认审核的图片，当前指针对确认审核的图片进行按需计费，不确认审核的图片不收取费用。收费标准为 1.3 元/千张。

Q:网站安全监测的版本，是否支持变更？

A:目前套餐支持升级，暂时不支持降级，本月升级，立即生效。

Q:网站安全监测的计费项有哪些？

A:计费模式分为预付费和按需付费两种：版本和网站数量为预付费，图片审核为按需付费。

Q:网站安全监测每个版本中的域名数量阶梯收费怎么理解？

A:每个版本对应的域名数量价格是不同的，体验版每个域名是 560 元/月，专业版每个域名是 1260 元/月，旗舰版每个域名是 2160 元/月，每个版本的域名是根据客户接入的域名数量

进行阶梯收费，每个版本域名数量>=10 个时，为版本域名价格的 6 折 ；>=30 个时，为 5 折；>=50 个时，为 4 折。

Q:网站安全监测服务中的图片审核怎么开通和收费？

A:图片审核功能为按需服务，可以直接在控制台开通，按需收费，开通之后根据客户的实际用量收取费用。

4.3 开通接入类

Q:怎么样开通网站安全监测服务和使用？

A:网站安全监测服务的开通首先需要注册天翼云官网的账号,通过产品栏目找到网站安全监测，点击开通；开通后会跳转到网站安全监测控制台，在控制台上配置需要监测的域名，配置成功后就已经开始对您的域名提供监测服务了。

Q:欠费后网站安全监测服务会被关停吗？

A:账户余额不足以支付服务费用将导致欠费，发生欠费后，网站安全监测服务的域名将被关停。

Q:关停网站安全监测服务后怎样重新开启服务？

A:客户补足欠款后，客户的天翼云账号恢复使用，被停止的域名需要客户到网站安全监测控制台域名管理模块，点击启用域名，开启被停用的域名，当域名状态变更为已启用后，服务就重新开启了。

Q:网站安全监测服务配置完成后大概多久生效？

A:网站安全监测域名接入配置在控制台完成配置后一般 30 分钟内生效,若 30 分钟后仍未生效，请提交工单处理；

Q:接入网站安全监测服务的域名有什么要求吗？

A:接入网站安全监测服务的域名，需要在工信部完成 ICP 备案。

Q:关闭网站安全监测服务后，域名配置会保留吗？

A:欠费导致服务关闭，域名配置会保留，但不会继续为所配置域名提供业务安全监测服务。

Q:删除网站安全监测域名后，域名配置会保留吗？

A:删除域名后，其配置将不会保留。

Q:网站安全监测服务被暂停了，为什么？

A:业务被暂停有以下几种情况：

欠费

未备案或备案已过期

内容违规

套餐包过期

4.4 功能类

Q:如何判断网站安全监测服务配置生效？

A:在控制台域名管理模块配置域名和监测项，当域名状态为已启用时，表示已经接入监测服务。

Q:天翼云网站安全监测服务支持 https 协议监测吗？

A:支持 https 协议监测。

Q:天翼云网站安全监测支持监测哪些业务？

A:网站安全监测服务支持远程扫描 Web 漏洞和按照国际权威安全机构 WASC 分类的 25 种 Web 应用漏洞，全面覆盖 OWASP Top 10 Web 应用风险。

Q:天翼云网站安全监测可以提供漏洞扫描服务吗？

A:支持漏洞扫描服务，无需用户采购任何 Web 应用扫描产品前提下，即可获得网站的漏洞态势，以及每个漏洞的详情介绍和修补建议。

Q:天翼云网站安全监测的安全事件监测都能做什么？

A:通过后端引擎根据预定义规则高效、准确识别网站页面中的恶意代码，以及敏感词汇的恶意链接，使网站管理员能够及时清除网页木马及黑链，避免给访问者带来安全威胁，影响网站信誉。

Q:使用前后页面对比的方式，辅以恶意文本核查分析，实时监测目标网站页面的篡改情况，发现页面被篡改情况，第一时间通知用户，避免篡改事件影响扩散，给自身带来声誉和法律风险。

Q:天翼云网站安全监测内容安全都包含哪些能力？

A:基于大量数据训练的深度学习模型，对待监测页面进行敏感内容检测，输出相关敏感信息和类别。发现页面出现敏感关键词后，，避免事件影响扩散，给自身带来声誉和法律风险。用户也可以自定义所关心的敏感关键词。

Q:天翼云网站安全监测可用性监测都监测哪些业务项？

A:多线路远程实时检测目标站点在多种网络协议下的响应速度、可访问性和 DNS 可用性监测

等反映网站性能状况的内容，一旦发现网站无法访问，或访问出现延迟。根据事先定义好的网站通断级别，第一时间通知用户。

Q:用户可以查看网站的攻击情况吗？

A:可以的，用户可以通过网站安全监测控制台查看网站的监测日志，也可以通过购买扩展服务态势感知大屏来实时了解网站的业务安全情况。