2023

智安网络

ZHIAN NETWORK

# 云眼-网站漏扫与内容监测系统

# 技术白皮书

AQ-SC-070 V1.2

## 市场指南

深圳市智安网络有限公司

www.zhiannet.com

智安网络
ZHIAN NETWORK

# 目录

# 1. 背景介绍

## 1.1 国家政策趋势

随着互联网的高速发展，网络安全问题也被国家日渐关注。从 14 年 2 月 27 日成立中央网络安全和信息化领导小组，到 15 年习近平主席多次提及网络空间安全，再到 2016 年 4 月 19 日习近平主持召开网络安全与信息化工作会谈并发表重要讲话，网络安全已然提升为国家战略层面。对于网站安全国家同样十分重视，近年来进行了多次网站安全大检查，同时发布了一系列文件促进网站安全的落实。

## 1.2 公安部条令

互联网安全保护技术措施规定（公安部令第 82 号）作为我国早期关于互联网安全的相关规定，就提出了对于网站安全防护的问题。其中第九条、第三款规定：“开办门户网站、新闻网站、电子商务网站的，能够防范网站、网页被篡改，被篡改后能够自动恢复”。

## 1.3 网络安全法

2016 年 11 月 7 日全国人民代表大会常务委员会于发布《中华人民共和国网络安全法》，并于 2017 年 6 月 1 日起正式施行。网络安全法提出制定网络安全战略，明确网络空间治理目标，明确了政府各部门的职责权限，将监测预警与应急处置措施制度化、法制化。

## 1.4 主席讲话

2016 年 4 月 19 日，中共中央总书记、国家主席、中央军委主席、中央网络安全和信息化领导小组组长习近平在北京主持召开网络安全与信息化工作会谈并发表重要讲话。

“第三，全天候全方位感知网络安全态势。知己知彼，才能百战不殆。没有意识到风险是最大的风险。网络安全具有很强的隐蔽性，一个技术漏洞、安全风险可能隐藏几年都发现不了，结果是“谁进来了不知道、是敌是友不知道、干了什么不知道”，长期“潜伏”在里面，一旦有事就发作了。”

“维护网络安全，首先要知道风险在哪里，是什么样的风险，什么时候发生风险，正所谓“聪者听于无声，明者见于未形”。感知网络安全态势是最基本最基础的工作。要全面加强网络安全检查，摸清家底，认清风险，找出漏洞，通报结果，督促整改。要建立统一高效的网络安全风险报告机制、情报共享机制、研判处置机制，准确把握网络安全风险发生的规律、动向、趋势。要建立政府和企业网络安全信息共享机制，把企业掌握的大量网络安全信息用起来，龙头企业要带头参加这个机制。”

## 1.5 外部网络环境日益恶化

随着互联网的发展，网站入侵工具发展日益成熟，入侵工具传播日益便捷， 入侵门槛也就变得越来越低，相应的针对网站的攻击变得越发频繁。

网络攻击也从早期的泛攻击逐渐转变为以经济、政治为目的的攻击。尤其近年来国外的一些黑客组织针对我国的党政机关、企事业单位等网站进行的篡改攻击，充满了政治意味，尤其以反共黑客为主，其定期在国外发布网站篡改结果。每逢我国举办重大活动期间，我国网站均会遭受大范围攻击。

# 2. 产品介绍

智安云眼（网站漏扫与内容监测系统），是根据应对黑客攻击的特点以及符合国家相应的政策文件为出发点专门针对网站频发的安全事件精心研发的一款监测预警产品，通过爬虫技术和漏洞扫描等技术以云 SaaS 形态为客户提供主动的网站安全监控与检测， 能够主动监测网站安全问题，监测网站脆弱性。并提供专业的修补意见，降低安全风险，防范于未然。并且提供网站监测平台 7*24 小时不间断监测，保持监测的持续性。突发攻击事件发生时，及时进行响应与处理，构建完善的网站安全体系。对于大范围的网站利用自动化的技术手段进行监测，减低人工成本。通过统一的指标进行全方位监控，为统一监管提供技术依据和关键指标。

# 3. 产品功能

智安云-安全监测服务主要包括四方面内容，资产测绘、可用性监测、脆弱性检测测和安全检测，其中资产测绘服务主要帮助用户识别违规上线的应用，让用户对于外网暴露 IP、端口有一个全面的了解；可用性检测能够帮助用户了解其站点此时的通断状况，延迟状况；其次，脆弱性检测主要帮助用户检测其网站面临的安全风险，为其提供专业化的安全建议；再次，安全监测能够为用户甄别出其站点页面是否发生了恶意篡改，是否被恶意挂马，是否被嵌入敏感内容等信息。

## 3.1 资产测绘

主要通过智安强大资产检测引擎为指定的 IP 或 IP 网段进行资产扫描，发现站点、子域名、IP、SSL 证书、服务、C 段、指纹等资产数据。通过与现有资产比对发现新上线的网站及变更的网站系统，并及时向用户通告。在用户确认资产变更内容后，更新现有资产列表并将变更的资产纳入到安全监测体系中，以便及时发现漏洞与安全事故。

## 3.2 可用性检测

可用性检测主要涉及以下指标：网站可用性、网站从不同线路来访问得速度情况、网站响应时间，从而判断是否能达到最优、最安全的服务质量。通过智安安全监测系统，从各省运营商网络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、首页加载时间等反映网站性能状况的内容，一旦发现网站无法访问， 第一时间通知用户。

可用性监控引擎能同时检测网站的 HTTP、TCP、PING 响应，提供自定义的安全阀值，从而为网站快速诊断提供帮助；同时，能够计量服务器掉线等安全事件发生的

频率、时间段，并提供报警操作。

### 3.2.1 HTTP 监测

网站应用通过监听指定的 TCP 端口，来获取客户端浏览器的访问请求。通过对监控网站的 URL 发起 HTTP 请求，计算从监控节点打开网站所需实际时间。结合预设置的阈值，如果在达到阈值时还无法得到响应，平台将会放弃请求，判定网站 WEB 服务为不可用，得到 HTTP 响应报文的 200 状态码作为是否可用的判断标准，并支持对包括使用 301、302、307 等等状态码进行重定向的网站进行监测， 支持自定义匹配网站响应内容。

### 3.2.2 TCP 监测

TCP 检测指定的多个地址的端口监听状态（相关服务），如 redis 集群等，主要用于简单的服务是否可用的检测。

### 3.2.3 PING 监测

监测网站若非禁止 PING，WEB 监测中心可通过发送 ICMP 请求报文至监测网站，通过预设的阈值，并计算实际 ICMP 响应报文的响应时间，如果在达到阈值时还无法得到响应，监测中心判断网站网络不可达。

## 3.3 脆弱性检测

### 3.3.1 远程网站漏洞扫描

网站的风险漏洞是站点被攻击的根源。通过远程的网站漏洞扫描服务，由智安安全专家团队定期进行网站漏洞扫描，高中危漏洞验证工作，并且用户可以通过智安安全监测系统平台，在无需采购任何 Web 应用扫描产品前提，即可获得网站的漏洞态势，以及每个漏洞的修补建议，从而开启漏洞生命周期管理工作，获取当前漏洞的所处状态，根据待验证、待修复、待复验等状态的指引，做好漏洞闭环整改处置。

该服务支持远程扫描 6 种系统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，支持自定义周期扫描和报告导出。

### 3.3.2 主机系统漏洞扫描

可针对网络主机（如网络打印机、服务器、客户机等）、网络设备（Cisco、3Com、Checkpoint 等主流厂商网络设备）、操作系统（Microsoft Windows 9X/NT/2000/XP/2003、Sun Solaris、HP Unix、IBM AIX、IRIX、Linux、BSD 和国产麒麟操作系统等）以及应用系统等进行漏洞扫描检测，可以针对当下主流的数据库，如 Oracle、MySQL、DB2、PostgreSQL、SQL Server 等进行漏洞检测。通过判断主机开启的服务，可进一步对更多的主机应用进行漏洞扫描。

### 3.3.3 弱口令监测

平台提供弱口令检查引擎，可以基于调度任务对网站进行远程自动扫描，获得所述网站主机诸如：SSH、FTP、ORACLE 等服务的弱口令信息，包括：用户名、密码。检查引擎通过内置的用户名字典和密码字典以及组 合字典，可以进行标准模式破解以

及组合模式破解两种扫描方式进行弱口令扫描， 扫描一方面同弱口令字典中的弱口令进行匹配，另一方面使用获取到的口令进行 模拟登陆验证，从而实现弱口令检查功能，从而有效提高弱口令检测效率。

## 3.4 业务监测

### 3.4.1 远程网页挂马及黑链监测

智安安全监测安平台，采用业内领先的智能挂马检测技术，可高效、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，使网站管理员能够第一时间得知自己网站的安全状态，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。

### 3.4.2 远程网页篡改监测

远程实时监测目标站点页面状况，发现页面被篡改情况，第一时间通知用户。用户可参考智安提供的安全建议及时修复被篡改页面，避免篡改事件影响扩散，给自身带来声誉和法律风险。

远程周期性监测网页被植入的各类恶意链接，发现情况，第一时间通知用户，减缓这些恶意链接对于系统整体的影响。

### 3.4.3 远程网页敏感内容监测

远程实时监测目标站点页面状况，发现页面出现敏感关键词，第一时间通知用户。用户可参考智安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，敏感词库也在持续新增优化中，目前包含多个种类的敏感词。用户也可以自定义所关心的敏感关键词。

# 4. 产品优势

## 4.1 快

- 应用快：7*24 小时全天候服务，按需购买，即买即用，无需安装部署；
- 检测快：平台最快 1 分钟监测一次，高密度发现网站异常情况；
- 响应快：安全专家 30 分钟内分析告警，及时响应告警事件；

## 4.2 广

- IP 资产覆盖广：支持给定 IP 段的全 IP 资产进行探测，对于存活的 IP 资产、端口信息进行告警通知；
- 漏洞覆盖广：支持扫描网站系统漏洞，支持扫描 WASC 25 种 Web 应用漏洞，全面覆盖 OWASP Top 10 Web 应用风险；
- 事件覆盖广：支持监测挂马、篡改、敏感内容、可用性、黑链等事件，并可以在用户门户上做可视化呈现；

## 4.3 免

- 免安装：纯 SaaS 服务，无需安装任何软硬件，成本低；
- 免部署：无需改变网络结构，无需占用机房或办公空间；

## 4.4 准

- 精准验证高中危漏洞：能够针对所有扫描出的高中危漏洞提供专家级漏洞验证；
- 精准贴合用户业务需求：能够通过自定义可用性监测级别，更加贴合用户业务场景；
- 精准贴合用户管理规范：能够及时告警，更加贴合用户实际管理规范。

# 5. 交付方式

## 5.1 SaaS 交付模式

产品完全云化部署，我们根据邮件申请，创建好账号之后，发送给客户。用户只需登录平台配置其网站域名并添加运行任务即可。平台会根据监控周期定时对网站安全进行监测，并支持报告的生成和导出。

# 6.关于我们

深圳市智安网络有限公司（简称：智安网络）是深圳市高新技术企业，下设成都智安云御网络有限公司（安全运营中心）和深圳市智安网络有限公司南京分公司（研发中心）两个子公司，成立于 2017 年 12 月 27 日，注册资本 2,000 万(元)。

作为安全运营中心，成都智安云御网络有限公司（简称：智安云御）成立于 2021 年 3 月，智安云御立足四川，放眼全球，坚持用户需求为导向，安全合规为目标，自主研发为宗旨，力争成为云安全领域领先者，在数字时代为用户的云安全及数据安全保驾护航。

智安云御基于企业安全能力模型 IPDRC（风险识别、安全防御、安全检测与响应、安全管控）构建安全 API 即服务的能力，搭建了智安安全中台。通过该中台，衍生了 6 条产品线路，形成“云 X 系列”的产品服务体系。

智安云御产品体系有：**云检**（流量检测--基于 snmp 与 flow 流量分析协议实现流量的采集、归类、威胁识别与告警）、**云测**（安全测试--提供可用性、漏洞、基线、权限、内容方面的风险测试和体检报告）、**云防**（攻击防御--提供主机/容器安全防护 cwpp 和网站/APP 安全防护 waap 能力）、**云控**（访问控制--基于零信任 SDP 与 IAM 理念实现下一代 VPN 技术）、**云保**（等保整改---一站式等保 2.0 建设服务平台）、**云密**（密码整改---一站式商用密码建设服务平台）