大汉 WEB 安全监控解决方案

北京国信大汉科技有限公司
南京大汉网络有限公司

概述

门户网站安全的重要性不言而喻。随着技术的发展，操作系统、中间件和数据库、以及软件开发架构都会暴露出当时技术的局限性和安全的不完善，黑客针对性攻击技术能力也在不断提高，门户网站安全防护成为一个长期的、不断改进的过程，安全防护方案必须依靠长期的运维服务作为支撑，统筹协调、持续实施、步骤清晰，才能更好地对政府门户网站安全保护。

南京大汉网络有限公司作为国内政府门户网站建设专家，在十多年的网站建设过程中，实施过众多政府门户网站安全等级保护项目，建立了完善的政府门户网站安全应急问题响应机制，核心团队具有多年处理安全故障的深厚技术以及最佳安全攻防实践能力，拥有全面的安全监控体系，能够对门户网站的安全进行深度扫描，及时发现安全隐患和风险，提供最新、最及时、最有针对性的门户网站安全防护工作。

大汉科技通过专业的网站安全监测平台，结合安全研究团队人工分析的方式，通过远程的方式实现对监控对象的页面篡改、网页挂马、网站可用性等情况进行7*24 小时安全监测，第一时间告警系统异常，并启动应急响应预案，就安全事件进行快速检测、抑制、根除、恢复和总结。

应用方向

- **网页木马监控**

借助专业安全监测平台，采用特征分析和沙箱行为分析技术对网站进行远程7*24小时网页挂马监测和分析，监测精度高达99%，实现快速、准确的发现和定位网页木马。发现安全事件及时对木马程序告警信息进行人工审核，确认无误后向联系人发布木马程序预警，通告木马程序信息，并协助相关人员及时进行处置。

- **网页篡改监控**

借助安全监测平台，对网站首页及二级页面进行远程7*24小时的高精度网页篡改监控，采用页面内容自动化比对技术，特别针对一些越权篡改、暗链篡改等情形进行严密监控，一旦发现被篡改情况，第一时间通知管理人员，协助及时修复，避免篡改事件影响扩散，给用户带来声誉和法律风险。

- **网站可用性监控**

安全监测服务提供三个级别的网站可用性监测功能，分别从域名可用性、网站服务可用性再深入到网站程序可用性的监测，较为全面的实现了网站可用性的监测功能。

- **网页敏感内容监控**

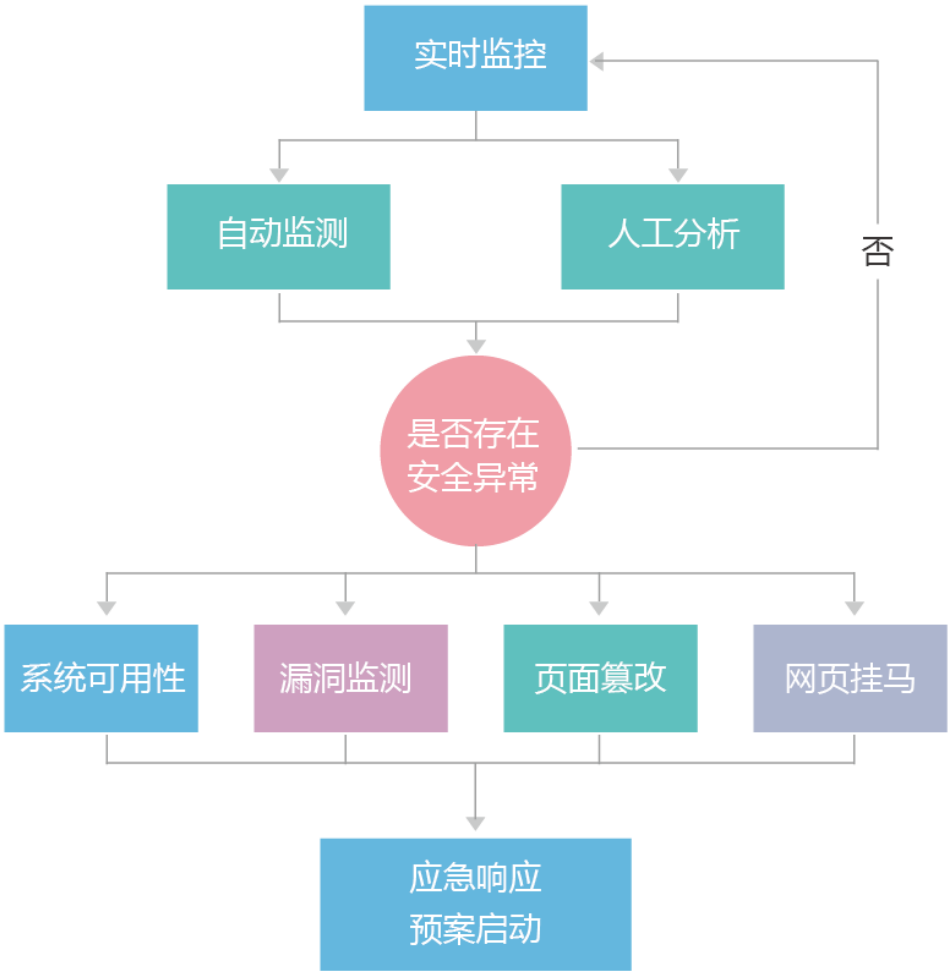
采用中文关键词以及语义分析技术对网站首页及二级页面进行敏感关键字监测，实现精确的敏感字识别，确保网站内容符合互联网相关规定，避免出现敏感信息以及被监管部门封杀。

本平台还使用了主辅关键字技术，使关键的告警控制在更有为效的范围之内，如“法轮功”为告警主关键字，但与“打击”、“抵制”等辅关键字在一起时则不会触发告警行为。更为合理的关键字监测降低人工二次确认的庞大工作量。

- **Web 漏洞监控**

监测平台集成了漏洞扫描功能，该功能继承了网站弱点扫描器的所有优点，可以实现快速、准确的定位出网站存在的问题，并且具有丰富的可配置接口便于配置个性化的扫描要求。

监测流程



方案特点

- **功能合规性**

本平台提供的监测功能充分考虑了各行业对网站监测的要求，如政府行业《国务院办公厅关于进一步加强政府网站管理工作的通知》所要求的监测类型、等级保护对电子政务及金融的要求，如银监会、证监会等金融监管机构对门户网站、网上业务系统的监测要求，从而确保监测平台的服务能满足各行业政策及监

管的要求。

- **监测范围全面**

监测平台提供的监测功能覆盖安全时间轴的事前漏洞监测；事中实时网马监测、关键字监测、可用性监测；事后篡改监测。协助用户实现网站安全可用的安全保障目标。

- **取证式监测**

监测平台采用业界最先进的监测与取证技术，确保监测到的每一个安全问题都能进行取证式确认，极大地降低了误报率：如 SQL 注入漏洞取证数据库内容、跨站脚本取证跨站效果代码、篡改监测取证篡改截图等。一方面减少运维人员对 WEB 安全知识的严重依赖，提高安全监管的效率；另一方面为用户确认和修复问题提供更为直接的帮助。

- **安全势态跟踪**

监测平台提供网站历史安全势态的跟踪功能，提供横向安全对比报告便于监管人员对网站进行考评、跟踪网站的安全处理情况。如：网站风险值评定与排名、漏洞修复状态跟踪、篡改事件汇总与修复跟踪等。

- **性能可扩展性**

监测平台采用先进的技术架构实现性能无极扩展，依据不同的业务需求可配置相应规模的监测引擎，从而实现不需用户端的任何修改即可实现对数千网站的远程安全监测。

相关产品

- 大汉 JGuard 网页防篡改系统
- 大汉 WEB 应用弱点扫描系统
- 大汉 WEB 应用防火墙

联系我们

www.hanweb.com

全国客户服务热线：400-608-1068

南京大汉网络有限公司（总公司）

联系电话：0086-025-84788569

传　　真：0086-025-84721840

地　　址：南京市钟灵街 50-1 号紫金大厦 3 楼、4 楼

北京分公司：北京市朝阳区朝外大街 22 号泛利大厦 1601 室

上海分公司：上海市闸北区江场西路 299 弄 49 号 601-B25 室

杭州办事处：莫干山路 789 号（莫干山路与教工路交路口）美都广场 D 座 919 室

宁波办事处：宁波市江东区百丈路 168 号会展中心大厦 15H 室

济南办事处：济南市经一路 88 号明珠商务港 2509 室

长沙办事处：长沙市岳麓区高新区麓谷大道 662 号软件大楼 653 室

兰州办事处：兰州市城关区临夏路街道庆阳路 488 号

成都办事处：成都市锦江区东大街牛王庙段 100 号 1 栋 1 单元 19 层 1905 号附 A25 号