奇安信网站云监测

技术白皮书

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|

|  |  |
| --- | --- |
| █文档编号  | █密级 完全公开 |
| █版本编号 V2.0 | █日期 2020年5月 |

 |

|  |
| --- |
| █ **版权声明** |
| 奇安信集团及其关联公司对其发行的或与合作伙伴共同发行的产品享有版权，本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程描述等内容，除另有特别注明外，所有版权均属奇安信集团及其关联公司所有；受各国版权法及国际版权公约的保护。对于上述版权内容，任何个人、机构未经奇安信集团或其关联公司的书面授权许可，不得以任何方式复制或引用本文的任何片断；超越合理使用范畴、并未经上述公司书面许可的使用行为，奇安信集团或其关联公司均保留追究法律责任的权利。 |

|  |
| --- |
| █ **版本变更记录** |
|

|  |  |  |  |
| --- | --- | --- | --- |
| **时间** | **版本** | **说明** | **修改人** |
| 2016-6-7 | V1.0 | 创建 | 陈晨、佟亚微 |
| 2017-7-10 | V1.1 | 修改 | 张吉州 |
| 2018-4-20 | V1.2 | 修改 | 张允成 |
| 2019-4-15 | V1.3 | 修改 | 张允成 |
| 2020-4-16 | V1.4 | 修改 | 杜雍新 |
| 2020-5-20 | V2.0 | 修改 | 李国辉 |

 |

|  |
| --- |
| █ **适用性说明** |
| 本模板用于撰写奇安信集团中各种正式文件，包括技术手册、标书、白皮书、会议通知、公司制度等文档使用。 |

目录

[目录 2](#_Toc41049904)

[1 背景与现状 3](#_Toc41049905)

[1.1 我国网站安全现状和形势 3](#_Toc41049906)

[1.2 国家政策法规驱动 4](#_Toc41049907)

[1.3 传统网站监测面临的问题 5](#_Toc41049908)

[2 网站云监测平台概述 6](#_Toc41049909)

[3 产品架构 7](#_Toc41049910)

[3.1 业务层 7](#_Toc41049911)

[3.2 数据层 8](#_Toc41049912)

[3.3 引擎层 8](#_Toc41049913)

[4 产品功能 9](#_Toc41049914)

[4.1 全面发现资产 9](#_Toc41049915)

[4.2 深度漏洞扫描 10](#_Toc41049916)

[4.3 网站黑链检测 11](#_Toc41049917)

[4.4 违规内容检测 12](#_Toc41049918)

[4.4.1 敏感页面深度学习技术原理 12](#_Toc41049919)

[4.4.2 云监测违规内容使用深度学习技术的效果 13](#_Toc41049920)

[4.5 内容变更检测 13](#_Toc41049921)

[4.6 网页挂马检测 14](#_Toc41049922)

[4.7 网站可用性监测 15](#_Toc41049923)

[4.8 FGHK监测 16](#_Toc41049924)

[4.9 IPv6网站监测 16](#_Toc41049925)

[4.10 漏洞情报 16](#_Toc41049926)

[4.11 网站监测报告 17](#_Toc41049927)

[5 产品优势 17](#_Toc41049928)

[6 服务支持 18](#_Toc41049929)

[7 应用场景 18](#_Toc41049930)

[8 相关附件 20](#_Toc41049931)

[8.1 网站监测能力参数 20](#_Toc41049932)

# 背景与现状

## 我国网站安全现状和形势

近年来，我国互联网市场规模和用户数量高速增长，随着在各行业的业务互联网化,越来越多的组织、机构和企业都在以Web系统来承载业务；大量的金融、游戏、电子商务、电子政务等网站业务已经上线。与此同时，我国的Web网站存在的安全风险越来越高，Web服务日益成为网络攻击的重点目标，存在严重的安全隐患，DNS攻击、暴力破解、零日漏洞利用、APT攻击依然让网站弱不禁风。数据泄露、网页篡改、网页挂马、钓鱼攻击、拒绝服务等安全事件频繁出现。恶意用户利用Web漏洞给社会造成了巨大的损失。

在网站漏洞方面，2018年1-12月，奇安信网站云监测平台的统计如下：

* 共扫描网站149.2万个，其中，扫出存在漏洞的网站110.3万个，占比为73.9%；
* 共扫描出1230.4万次漏洞；
* 扫出存在高危漏洞的网站23.1万个，占扫描网站总数的15.5%；
* 共扫描出217.0万次高危漏洞，占扫描出漏洞总数的17.6%；。

由以上统计可以看出Web网站的漏洞普遍存在，高危漏洞更容易被病毒、木马、黑客等侵入，导致软件崩溃或者盗取重要信息、密码等，其危害性更大，影响更深远。另外99%的CVE漏洞，被公布1年之后仍可被利用。通过网站漏洞进行网页篡改的现象越来越普遍,网站挂马、暗链等恶意代码严重威胁到网站的信息安全，据CNCERT监测，2019年，我国境内遭篡改的网站有约18.6万个，其中被篡改的政府网站有515个，较2018年增长138.4%。

此外，随着我国IPv6规模部署工作加速推进，支持IPv6的网站范围不断扩大。2019 年，根据CNCERT监测数据显示，攻击源、攻击目标为IPv6地址的网站后门事件有2,262起，共涉及攻击源IPv6地址131个、被攻击的IPv6地址解析 网站域名66个。

Web应用安全依然是互联网安全的最大威胁来源之一，我国的网站安全形势日益严峻,新的网络安全漏洞和黑客攻击手法,给网站Web服务器的安全、稳定运行带来了极大的威胁。如何快速高效检测网站漏洞和页面篡改等安全问题变得非常紧迫。

## 国家政策法规驱动

面临日趋严峻的网络安全形势，党和国家高度重视信息安全建设，国务院办公厅、工信部、公安部等相关监督和管理单位相继出台了针对网络、关键基础设施管理、资产管理、风险预警通告等方面的相关政策法规：

2014年中央网络安全和信息化领导小组的成立，习近平总书记明确指出：“没有网络安全就没有国家安全”，将我国网络安全提升到国家安全和国家战略的高度。

2016年4月19日，习近平总书记在全国网络安全和信息化工作座谈会上的讲话中谈到：“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。”；

2016年12月27日，国家互联网信息办公室发布《国家网络空间安全战略》提出“网络空间安全（以下称网络安全）事关人类共同利益，事关世界和平与发展，事关各国国家安全。

2017年6月1日《网络安全法》正式实施。《网络安全法》明确规定“国家建设网络与信息安全保障体系，提升网络与信息安全保护能力”，“中华人民共和国计算机信息系统安全保护条例([1994]国务院147号令)

同时其他国家与行业相关法令也对网络空间资产管理与风险预警提出的明确的要求：

《关于信息安全等级保护工作的实施意见》（公通字[2004]66号）

《关于信息安全等级保护工作的实施意见》（公通字[2004]66号

《信息安全等级保护管理办法》（公通字[2007]43号)

《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007]861号）

《信息安全等级保护备案实施细则》(公信安[2007]1360号)

《网络安全等级保护条例 2.0》

《中华人民共和国网络安全法》

《2018年省级基础电信企业网络与信息安全工作考核要点与评分标准》

《工业和信息化部 国务院国有资产监督管理委员会关于开展基础电信企业网络与信息安全责任考核有关工作的指导意见》

## 传统网站监测面临的问题

传统的网站监控依靠Web扫描器进行网站监控，这具有很大的弊端：

全国区域无法覆盖

传统扫描器在对企业网站进行可用性监控时，只能通过单一节点进行安全监控。网站业务是面向全国用户的，单一节点的安全监控无法掌握全国不同区域用户对企业站点的访问情况，监测体系存在盲点。除此之外，也无法了解当前站点的全局访问情况。

0 day漏洞无力感知

传统扫描器在漏洞探测时，主要通过系统规则探测，探测效果完全依赖规则的更新与准确性，一方面规则更新存在时间差，在漏洞曝光的时候如果没有及时升级规则库，则会出现扫描空窗期，另一方面对于零日漏洞的探测上，传统扫描器没有源头支撑，无法有效支撑零日漏洞的探测。

未知资产难以发现

传统扫描器在扫描过程中，完全依赖于对已知域名以及IP的探测，但是在企业中存在私搭乱建的网站，这些网站没有经过报备，扫描器无法获取域名或者IP进行探测。但是这些站点会开放Web业务，提供对外的访问权限，存在安全漏洞，大大增加了企业的安全风险。

缺少安全闭环处理

企业在监测设备发现问题后，由于缺少整体的安全闭环处理通报机制，无法做到快速同步到人，也缺少问题修复人员与网站管理者之间的沟通桥梁，尤其在网站大规模集群的运维过程中，脱节的安全管理使得问题发现越来慢，安全加固越来越困难。

面对频发的各类WEB安全事件，如何做到有效监测、快速响应、高效处置，已经成为各行各业必须面对的问题。

# 网站云监测平台概述

奇安信网站云监测平台是一个SAAS服务系统，集网站漏洞扫描、网站可用性监控、网页篡改监测、网站黑链监测、网页挂马监测等功能为一体的综合性的云端网站安全检测平台。可帮助客户自动发现网站关联资产，并进行高效精准的自动化漏洞扫描和网页内容监测等，结合情报大数据、白帽渗透测试实战经验和深度机器学习，提供全面网站资产安全检测，包括：

* 漏洞扫描
* 违规内容（涉赌、涉政、涉黄等）
* 内容变更
* 网站黑链
* 网页挂马
* 网站可用性
* 未知资产发现
* IPv6网站监测
* 漏洞情报

客户只需开通网站云监测平台的SAAS账号，导入资产后即可对网站进行持续性的安全扫描和检测，同时，云端安全专家团队提供7x24小时的实时漏洞告警验证，页面篡改验证等安全运营服务，第一时间将发现的安全风险通告下发给客户，并提供专业的修复建议，降低企业安全风险。奇安信网站云监测系统运营示意图如下：



# 产品架构

产品架构为分层结构，包含业务层，数据层和引擎层三部分，如下图所示：



## 业务层

业务层包括以下主要业务功能：

**监测任务调度**：对漏洞扫描，可用性监测，网站黑链，内容变更，违规内容和反共黑客监测等任务进行调度，支持周期性任务，也支持一次性任务调度；

**监测策略管理**：每类监测任务都有对应的策略模板，用户可以设置偏好的策略；

**监测告警通知**：支持告警的自动通知下发，也支持手动下发告警通知，支持邮件和短信两种通知方式。

**告警数据运营**：本平台为云端安全运营专家提供7x24在线验证漏洞告警，篡改告警等数据运营，给用户提供零误报的安全通告服务；

**资产管理**：资产录入/删除，监测生效/失效，已知资产管理，资产详情（OS，端口，服务，中间件，应用，ICP备案等信息）； 发现的未知资产信息**：**全面发现域名资产关联的子域名、web服务器IP等，并提供详细的资产指纹信息，如中间件、应用程序、OS、端口、服务等，让安全不留死角。

**网站监测报告**：支持日报，周报，月报和季报等周期性报告，也可以手动定制日期和告警类型即时生成安全监测报告。

**多级用户管理**：支持监管单位用户的分级用户管理，五级以上；支持单位用户的多角色管理，每个角色的权限不一样；

## 数据层

**告警日志数据：**主要存储监测的告警类数据，包括漏洞，可用性，网站黑链，违规内容，内容变更，网页挂马和反共黑客等告警类型的数据；

**知识库类数据：**主要包括web指纹库，服务指纹库，全球鹰漏洞库等；

**资产情报类数据**：主要包括；Whois数据库，DNS数据库，ICP备案数据库和IP资产归属等数据。

**资产暴露面信息**：包括资产探测的信息，如OS，端口，服务，中间件，应用，ICP备案等信息；

## 引擎层

引擎层又包含了四个引擎子系统：

**网站监测引擎**：为分布式的集群系统，包括爬虫，漏洞扫描，内容变更，网站黑链，违规内容监测等模块。

**可用性监控引擎**：为分布式部署，在全国不同的区域和运营商都部署探测节点，对用户网站的可服务线进行持续监测。

**资产探测引擎**：对监测的网站进行全方位的资产探测，获得资产的OS，端口，服务，中间件，应用，ICP备案等信息，以及关联的未知子域名资产信息；

**反共黑客监测引擎**：实时监控境外FG黑客组织的情报；

# 产品功能

网站云监测为用户提供统一云平台管理账号，用户处无需部署任何软硬件产品，可以随时随地，利用任何可联网终端通过浏览器对监控对象进行7x24小时的监控、查看与管理。解决用户处因硬件资源申请流程长，设备资源利用率不高，开发及运维人员成本迅速升高等瓶颈减缓安全建设的步伐的问题。为用户关注的WEB资产提供统一监测平台，实现WEB资源的统一管理、WEB生态的安全管理、通报事件跟踪管理；提供多维度统计分析的报表数据，为行政管理考核提供依据。

网站云监测平台的功能主要包括：全面发现资产，Web漏洞扫描，网站黑链检测，违规内容检测，内容变更检测，网页挂马检测，可用性监测，FGHK监测，IPv6网站监测，漏洞情报和网站监测报告等11个大的功能模块。

## 全面发现资产

传统的web漏洞扫描只是对网站页面进行爬取，基于爬取的url进行漏洞扫描，但web服务器上其他的应用如果存在漏洞，也会导致网站不安全，而且随着攻击手段等不断高级化，针对黑客等跳板式攻击，全面发现已知网站域名的关联资产变得非常重要，探测资产指纹详情，发现薄弱环节，不放过可能的风险，对关联资产进行全方位的漏洞扫描，让安全不留死角。

云监测已有涵盖全国的存活IP资产指纹，域名资产，全网端口指纹库和全网web指纹库，拥有最新whois数据库，ICP备案库。利用云端大数据优势，可以进行全面的资产发现，资产发现包括两部分：对已知资产进行全面探测和对关联的未知资产进行发现。

已知资产的暴露面探测：包括域名关联的服务器IP地址，端口，操作系统，服务，应用类型，以及Web框架/中间件等资产详细信息。根据探测出来的暴露面，可以做进一步精确的漏洞扫描，发现薄弱环节。

未知子域名资产的发现：自动发现已知域名相关联的子域名列表，且属于未在云监测的监测范围内的资产，这部分资产可能属于客户未报备的私搭网站，存在较大的安全风险，一旦发现会马上通报客户，方便客户管理监控。



 资产发现的过程

## 深度漏洞扫描

如果网站存在的漏洞得不到及时的修复和加固，将给不法分资提供可乘之机，容易造成系统被入侵、植入后门甚至瘫痪等安全问题。因此，需要对网站进行全面、持续的安全漏洞扫描，发现系统存在的各类安全隐患。

奇安信网站云监测提供深度专业的漏洞扫描，可以扫描以下漏洞：

|  |  |
| --- | --- |
| **漏洞类型** | **漏洞** |
| 认证和授权类 | 遍历数据、越权访问、弱口令、文件上传、任意文件下载、任意文件读取等 |
| 命令执行类 | 远程命令执行、各类反序列化漏洞、文件包含等 |
| 注入攻击类 | SQL注入、XSS注入、XML注入、XPATH注入、CRLF注入、链接或框架注入等 |
| 服务端攻击类 | 应用服务未授权访问 |
| 信息泄漏类 | 版本管理软件信息泄漏、web服务器控制台地址或网站后台泄漏、phpinfo()信息泄漏、目录遍历、敏感信息泄漏、安装或测试文件未删除、cookie信息泄漏、心脏滴血漏洞等 |
| 其他 | 各类CMS漏洞（织梦、骑士、大汉等）、各类webserver/中间件漏洞、struts 2组件相关漏洞、IIS组件漏洞、服务端请求伪造（SSRF）、URL重定向、DNS域传送漏洞、HTTP Host头攻击等 |

每周更新一次最新的漏洞POC；

支持漏扫策略的自定义配置，包括代理设置、流量限制，扫描时间等，；支持自定义扫描周期，默认扫描周期是7天。漏洞扫描的类型包括快扫，全扫两种：

* 快扫：当第一次加入web资产进行监测时，会进行一次快扫，快扫只是对网站首页和二级页面进行扫描，以便快速的检测一次网站的脆弱性。
* 全扫：常规扫描，将对网站的全部页面进行爬取和扫描，无死角的扫描每一个页面，尽可能检测出更多的漏洞。

**漏洞的危害分类**：高危、中危、低危和提示；

漏洞又分为精准扫描和通用扫描，精准扫描出来的漏洞是准确没有误报的，通用扫描是需要人工验证的。

## 网站黑链检测

黑链也称暗链，是一种隐蔽链接，是黑帽SEO利用高权重网站外链来提升自身站点排名的一种作弊手段。一般来说，黑链攻击是黑客通过隐形篡改技术在一些网站中植入链接。这些链接再用户直接访问网站时是不可见或极易被忽略的，然而搜索引擎却能通过分析网页源代码将这些链接进行收录。如果在大量网站或者一些高权重网站中植入它们，可以迅速提升这些暗链网站的网页排名。

黑链攻击植入的链接大多数与博彩信息、虚假医疗、诈骗信息、游戏私服、非法办证及一些诈骗信息相关。由于各类网站中，教育网站和政府网站的社会关注度和搜索引擎权重较高，所以经常成为黑链的宿主。

网站黑链检测技术主要包括以下几点：

* 黑链是针对搜索引擎进行SEO优化的，所以要发现黑链，需要将爬虫伪装成搜索引擎的爬虫，需要在http请求headers中加上搜索引擎爬虫的User-Agent、Referer等信息；
* 关键词：通过观察被注入黑链的网页样本，可以发现黑链标签文本包含明确的SEO关键词，数据表明绝大多数的关键词都与博彩信息、虚假医疗、诈骗信息、游戏私服、非法办证及一些诈骗信息相关；
* 黑链域名特征：由于黑链所指向的网页大多数为非法网页，其域名常常有相似之处（如数字域名等），因此黑链的域名在黑链检测中是一个重要的特征；

黑链隐藏结构特征：通过对大量网页暗链样本进行观察，发现网页黑链大都是利用HTML和JavaScript源代码属性对超链接实现隐藏功能，通过统计可以得到高频黑链隐藏结构，并以此作为黑链检测的特征依据。

## 违规内容检测

基于海量样本数据和先进的人工智能技术，精准高效识别网站含淫秽、污秽、色诱、文爱等涉黄内容，精准识别赌博、刀枪、毒品等违禁内容；可支持自定义敏感词检测，提前防御网站内容风险。除了网页文本的检测外，还支持针对图片中的违规文字内容通过OCR技术进行识别。

### 敏感页面深度学习技术原理

随着深度学习技术的发展，尤其是卷积神经网络（Convolutional Neural Networks，CNN）的发展，文字识别和场景文字识别在近年来有了飞速的发展，在网站安全监测领域受到了广泛的应用。文字识别主要分为两步：文字检测和文字识别。其中，敏感文字检测主要采用了以下方式：



### 云监测违规内容使用深度学习技术的效果



基于上千万的历史样本数据进行模型训练，支持敏感词，黑链和OCR的模型检测，提升敏感页面监测效果；检测效果：召回率99%，减轻运营人员50%以上的工作量，检测准确率大大提升，通报更及时。

## 内容变更检测

网页内容变更事件往往预先检查和实时防范较难，由于网络环境复杂而难以追查责任，攻击工具简单且向智能化发展。目前虽然有防火墙、入侵检测系统等安全设备作为安全防范手段，但Web应用攻击有别于其他攻击方式，很难被传统的安全设备所检测到。

网站云监测的网页内容变更检测采用网页指纹技术，即对每一个爬取的网页进行指纹提取，如果发现网页指纹与之前备份的不同，则可断定该网页内容发生了变更；监测的页面包括两种页面，一个网站首页，另外一个是重点页面。网站首页检测内容：变更部分如果包含外链、敏感词、黑词、HTML之外内容产生告警；重点页面检测内容：只要页面发生了变化就产生告警。

## 网页挂马检测

网页挂马是攻击者通过在正常的页面中（通常是网站的主页）插入一段代码。浏览者在打开该页面的时候，这段代码被执行，然后下载并运行某木马的服务器端程序，进而控制浏览者的主机。通俗点说就是将网页木马这样的攻击程序放在网页上，浏览这个网页的人，不需要任何点击动作就会中毒。

网页挂马检测主要是通过沙箱技术来进行检测的。当篡改检测模块确认一个URL被篡改以后，会自动进入到沙箱中进行检验，并将检验结果同步到监测平台大数据。

沙箱检测技术主要针对网页挂马行为的相关技术进行检测，判断样本文件是否存在恶意利用代码。本检测技术包含动态检测引擎和半动态检测引擎。动态引擎依赖于漏洞利用环境重现，其虚拟机执行引擎运行Windows操作系统以及相关应用程序，注入检测模块，对恶意文件利用行为特征进行检测。使用Hook、指令流分析、模拟执行等检测手段对shellcode执行生命周期的各个阶级的特定行为进行检查，检测流程如下所示：



**沙箱检测技术优势：**传统的挂马检测依靠挂马特征库，这种方式依赖挂马库的积累，一旦出现新的挂马库，将无法发现。沙箱检测技术通过虚拟机执行引擎运行Windows操作系统以及相关应用程序，注入检测模块，对恶意文件利用行为特征进行检测，可以快速、精准的定位挂马行为。

## 网站可用性监测

网站可用性是指端到端全网所能提供的无故障服务时间与全部运行时间之比。网络管理目标有时就是关注网站的可用性，即使网站的可用性尽可能地接近100%，任何关键地网络设备地停机都将影响到网站地可用性。

云监测基于奇安信自有的IDC节点，真实模拟用户访问行为，多点结果汇总分析得出网站访问故障告警。云监测可用性监测引擎子系统提供了http、https、dns等可用性监控方式，每个资产具有独立的可用性监控配置及灵活的告警策略，加上可任意扩展、选择探测节点的架构方式，满足本项目对网站可用性监测的需要。

HTTP/HTTPS的监控：服务器不可达，RTT超时，请求域名不存在，服务器阻断请求等；

DNS的监控：域名解析超时，域名无效，DNS解析的A记录结果不匹配等；



 可用性监测过程

## FGHK监测

云监测持续监测境外fangongheike组织针对Jboss，Weblogic，Struts2等架构的网站服务器发起攻击，造成网页被篡改的的安全隐患，一旦篡改影响非常恶劣。云监测以分钟级的频率进行监测，并第一时间通过短信，邮件通知客户。

## IPv6网站监测

在网络攻击方面，据统计，2019年“两会”期间，共拦截攻击源为IPv6地址的网络攻击8000万起 ；在针对283家政府、高校、中央企业云托管网站来自IPv6网络的攻击中，目录遍历攻击、WEB Shell攻击、SQL注入等典型WEB攻击超过90% ，在安全漏洞方面，目前，截止2019年7月，CVE漏洞库中已收录IPv6相关漏洞381条，涵盖硬件、系统、协议、应用等不同层面。所以针对IPv6网站的监测刻不容缓，非常重要。

奇安信网站云监测系统全新升级支持IPv6协议，满足网站发展需要，监控内容包括：

IPv6网站漏洞扫描

IPv6网站黑链

IPv6网站挂马

IPv6网站违规内容

IP网页内容变更。

## 漏洞情报

奇安信补天漏洞响应平台注册白帽子达61000 +，该平台以互联网漏洞响应的模式，充分发挥民间白帽的力量，实现实时的、高效的漏洞挖掘与响应，已发现漏洞数41万+。网站云监测会定时从补天平台匹配用户的网站相关的漏洞，将相关漏洞情报及时通知给客户，特别是网站的逻辑漏洞。

## 网站监测报告

针对网站监测的的结果形成专业简洁的网站安全监测报告。多角度分析资产安全风险；多元化数据呈现，将安全数据智能分析和整合，使安全现状清晰明了，对扫出来的安全漏洞进行归类，并提供专业的修复建议。

支持手动生成报告和周期自动生成报告，周期性报告支持周报，月报和季报三种。

通过报告模版支持灵活的监测报告内容配置，可配置的内容包括：时间范围，网站筛选条件，告警类型，威胁等级等。

报告的格式：支持PDF，WORD和EXCEL三种报告格式。

# 产品优势

* **全方位风险覆盖，安全不留死角：**

全面覆盖WEB漏洞扫描、弱口令检测、涉赌涉黄涉政等违规内容、网页挂马、网站黑链、内容变更，网站可用性和FGHK等各类网站风险。全面支持源码、文本、图片等内容格式。同时从白帽视角，全方位发现未知资产和关联资产风险，避免关联资产成为网站安全木桶的短板，影响整体安全效果。

* **检测准确率高，零误报告警通知**

采用深度启发式Web 2.0爬虫技术，基于动态解析，链接抓取更准、更全、更深；结合大数据和机器学习的能力，快速准确的发现违规内容和网站黑链等安全告警；云端安全运营团队7x24小时进行告警运营，将发现并验证审核过的安全告警第一时间零误报通知给客户。

* **零部署低成本，一键开启SAAS服务**

无需安装部署，无需购买设备，开通账号5分钟生效，一键开启网站安全监测SAAS服务。无需人工升级，实时直接享用最新漏洞库和风险算法。可随时随地登录管理控制台，实时查看安全告警结果和监测报表。

* **IPv6网站监测**

随着我国IPv6网络和业务开始上线，IPv6网络攻击事件也开始出现，2019年，根据CNCERT监测数据显示，攻击源、攻击目标为IPv6地址的网站后门事件有2,262起，共涉及攻击源IPv6地址131个、被攻击的IPv6地址解析 网站域名66个。云监测已经支持IPv6网站的漏洞扫描，违规内容，网站黑链，内容变更等监测业务，为IPv6网站安全保驾护航。

# 服务支持

* SAAS服务开通；



* 安全运营服务：



# 应用场景

|  |  |  |
| --- | --- | --- |
| **应用场景** | **场景痛点** | **产品价值** |
| 监管单位日常安全检查 | 1，监管范围的资产底数不清，资产的责任单位不明；2，监管范围内的资产安全风险状态未知，安全预警不及时；3，监测网站数量多，没有足够的本地安全专家处理安全告警； | 1，全面掌握辖区资产的安全动态：发现未知资产，完善网站备案信息；事前发现安全漏洞，事中发现黑链，违规内容，挂马和FGHK等安全事件；云监测平台支持10万以上网站的监测能力。2，快速专业的安全威胁预警：7x24小时云端安全专家运营团队实时监控辖区网站资产安全告警，发现安全问题立即验证审核，第一时间零误报通知给客户； |
| 监管单位重保安全检查 | 1，重大活动需要确保监管范围资产的网站安全，重保之前来不及摸清资产安全风险状态，重保期间安全预警不及时；2，没有足够的本地安全专家处理安全告警； | 1，监管单位零部署，一键开启SAAS账号即可开始网站监测；2，全面掌握辖区资产的安全动态：发现未知资产，完善网站备案信息；事前发现安全漏洞，事中发现黑链，违规内容，挂马和FGHK等安全事件；3，快速专业的安全威胁预警：7x24小时云端安全专家运营团队实时监控辖区网站资产安全告警，发现安全问题立即验证审核，第一时间零误报通知给客户；  |
| 政企客户安全自查 | 1，私搭网站，未报备网站不掌握，已知资产风险状态不明，面临被上级监管单位通报；2，网站内容存在违规内容，无法及时发现，给企业带来极大的法律风险；3，安全能力不足，漏洞和黑链告警无法验证； | 1，提升客户安全处置能力：用户可对发现的未知资产进行有效资产管理，事前发现安全漏洞，事中发现黑链，违规内容，挂马和FGHK等告警；7x24小时云端安全专家团队实时验证漏洞和黑链等安全告警，提前处理安全事件，保护资产安全，避免被通报，防范于未然。2，零部署低成本，一键开启SAAS服务：奇安信云监测服务通过SaaS方式为客户提供漏洞扫描和安全事件监测服务，客户无需购买任何硬件设备，也无需占用带宽资源。 |
| 政企客户日常安全监测 | 1，资产互联网暴露面和风险状态未知；2，网站在全国一些地区无法访问，影响到用户的正常使用；3，页面被恶意篡改无法及时获知，影响公司形象4，网站内容存在违规内容，无法及时发现，给企业带来极大的法律风险；5，IPv6网站风险无法监测；6，安全能力不足，漏洞和黑链告警无法验证； | 1，可对网站进行全国多个节点的可用性持续监测，快速准确的检测可用性告警；2，可对IPv6网站进行安全监测；3，提升客户安全处置能力：用户可对发现的未知资产进行有效资产管理，事前发现安全漏洞，事中发现黑链，违规内容，挂马和FGHK等告警；7x24小时云端安全专家团队实时验证漏洞和黑链等安全告警，提前处理安全事件，保护资产安全，避免被通报，防范于未然。4，零部署低成本，一键开启SAAS服务：奇安信云监测服务通过SaaS方式为客户提供漏洞扫描和安全事件监测服务，客户无需购买任何硬件设备，也无需占用带宽资源。 |

# 相关附件

## 网站监测能力参数

|  |  |  |
| --- | --- | --- |
| 能力项 | 监测范围 | 监测频率 |
| 未知资产发现 | 发现已知域名下的未知子域名 | 1天 |
| 漏洞扫描 | 1. 支持的漏洞类型：

认证和授权类：遍历数据、越权访问、弱口令、文件上传、任意文件下载、任意文件读取等；命令执行类：远程命令执行、各类反序列化漏洞、文件包含等；注入攻击类：SQL注入、XSS注入、XML注入、XPATH注入、CRLF注入、链接或框架注入等；服务端攻击类：应用服务未授权访问；信息泄漏类：版本管理软件信息泄漏、web服务器控制台地址或网站后台泄漏、phpinfo()信息泄漏、目录遍历、敏感信息泄漏、安装或测试文件未删除、cookie信息泄漏、心脏滴血漏洞等；其他漏洞：各类CMS漏洞（织梦、骑士、大汉等）、各类webserver/中间件漏洞、struts 2组件相关漏洞、IIS组件漏洞、服务端请求伪造（SSRF）、URL重定向、DNS域传送漏洞、HTTP Host头攻击等。2，每周更新一次最新的漏洞poc。 | 默认周期7天，可配置最短3天 |
| 网站黑链检测 | 1，检测目标为网页中的外链；2，检测黑链内容有：涉黄、涉政、涉赌、涉毒、违禁品、医疗推广、游戏推广等； | 30分钟全站检测 |
| 违规内容检测 | 1，检测目标为站内网页；2，检测违规内容有：涉黄、涉政、涉赌、涉毒、违禁品、医疗推广、游戏推广等；3，通过OCR技术可以检测图片中违规文字内容； | 30分钟全站检测 |
| 内容变更检测 | 1，对首页、重点页面进行网页内容变更检测；2，首页检测：变更部分包含外链、敏感词、黑词、HTML之外内容产生告警；3，重点页面检测：只要内容有变化就告警； | 30分钟 |
| 网页挂马检测 | 检测网页中是否存在网页挂马。包括iframe挂马、vbscript挂马等。 | 30分钟全站 |
| 可用性监测 | 支持http/https/dns监控，全球18个探测节点，监控频率、告警策略可自定义； | 2分钟 |
| FGHK监测 | 监测境外fangongheike组织针对Jboss，Weblogic，Struts2等架构的网站的网页篡改； | 1分钟 |
| 漏洞情报 | 对接补天漏洞平台，匹配客户网站的漏洞情报数据 | 1天 |