密级	公开

WebSOC 知道网站立体监控系统

产品白皮书

[KSSC-2012-WebSOC-01 V2.2]

北京知道创宇信息技术有限公司

2012 年 6 月

目录

1. 网站安全现状与挑战

著名的信息技术研究和分析公司 Gartner 统计，近些年来，超过 70%的攻击都来自于 Web 攻击；IBM X-Force 研究团队的统计也显示出 Web 安全类事件也呈现出逐年增加的趋势；CNCERT 2011 年中国互联网网络安全报告显示，2011 年境内被篡改网站较 2010 年增加 5.1%。

一系列的数据显示，传统的 Web 安全防护与监测已经难以应对当前形势，Web 安全的常态化监测、预警与态势分析已经是 Web 安全的当务之急。

2. 产品介绍

知道创宇是国内首家提出大规模网站持续、多维度安全监测理念的公司，自主研发的 WebSOC 知道网站立体监控系统（简称 WebSOC），是专注于大规模网站集中监控的安全产品。该产品案例丰富、成熟度高，为国家三大互联网监管机构提供了有力的技术支撑，目前该系统实际监控的网站数量已经超过 20 万。

WebSOC 功能简介：

- **可用性监测**

  WebSOC 通过 HTTP(S)请求、域名解析、Ping 等方式分析响应时间，及时发现网站出现链路异常、访问延迟、解析错误等情况。

- **漏洞监测**

  Web 漏洞规则达 500 条以上，对常见的 SQL 注入、跨站脚本、跨站请求伪造（CSRF）等代码层漏洞具备强大的检测能力，支持 SQL 注入专家检测模式；支持常见 Web 应用层安全漏洞的检测；支持第三方应用组件（如：论坛、BLOG、编辑器）的识别与零日漏洞检测。

- **安全事件监测**

  支持挂马、暗链、内容变更和关键字监测，挂马和暗链的检测精确度高

达 99.9%；可精确定位内容变更和关键字位置。

- **资产识别**

  可根据用户给定的地址范围发现 Web 资产，并自动加入监控列表中，进行周期性检测；可识别包括服务端指纹识别、第三方应用组件指纹识别、服务器端口、ICP 备案、IP 及地理位置等信息。

- **统计报表**

  支持在线和离线报表，提供独立站点的历史数据趋势分析功能，并且可对多个站点的扫描结果以不同维度进行 TOP10 统计。

- **事件告警**

  系统支持页面、邮件和短信三种告警方式，用户可根据需求自由定制告警方式和告警内容。

- **二次开发接口**

  系统支持 API 二次开发接口，通过调用 API 接口可实现二次定制开发，并与已有安全平台实现对接，系统目前已支持与国内主流 SOC 平台对接。

3. 产品特色

3.1. 日均处理十亿级 URL 形成的云端知识库

知道创宇早在 07 年就建立了国内首个基于云技术的互联网安全云数据中心，用于对国内七百余万域名进行实时的网页挂马、暗链等安全事件监测，每日分析处理的 URL 数量多达上十亿条。同时，知道创宇安全研究团队每日都会对监测结果进行深度、持续的分析，从而形成基于真实案例的检测规则，并将规则定期更新到产品中，提升产品检测能力。

3.2. 高效的监测引擎，坚实的技术核心

系统具备超强监测性能，单台设备具备每天监测 50 万以上页面数量的能力，为大规模、周期性的监测提供坚实的核心保障。

产品的挂马监测引擎基于云端动态行为检测技术，可精准识别网页挂马事件。暗链检测引擎基于人工智能自动分类识别算法，能够在第一时间发现最新的互联网暗链、黑链特征。漏洞检测引擎默认采用快捷模式，大量采用了自动化智能识别技术，自动优化检测参数，不需人工交互，检测速度快，精确度高，同时提供专家模式，能够对目标网站进行更深入、更全面的风险探测。

另外，系统采用的网页爬虫模块兼容 IPV6 协议，支持 Web2.0、HTML5 及 WAP 网站。

3.3. 独创的网站安全属性监测功能

- 站点资产自动发现

系统能够自动发现给定网段中的存活 IP 并精准识别应用服务类型，并可将发现的资产自动加入到周期检测任务中，以帮助管理员实现对老旧的业务系统、孤岛网站、测试系统的监控与管理。

- 站点安全属性 WSP（WebSite Security Profile）功能

系统独创的 WSP 功能通过多种探测技术精确识别被检测系统上运行的各类应用信息和第三方 Web 组件（如：论坛、BLOG、在线编辑器等）版本，从而实现精确的版本管理与配置管理，也可为安全管理人员安全预警提供参考。

3.4. 全面、实时、多维度的安全监测

系统从脆弱性、可用性、域名劫持、挂马、暗链、网页篡改等多个维度对网站进行周期性监测。并且，用户可以根据实际业务应用场景定制不同监测目标的监测内容、监测周期和优先级策略。

3.5. 灵活的告警方式，全面的趋势分析

系统的告警功能支持细粒度配置，可针对不同监测功能进行独立的邮件告警配置，来达到周期告警的目的。而对于紧急安全事件，可设置即时短信告警，以帮助管理人员对网站安全事件做出实时响应。

系统除在线报表功能外，还支持 Word 及 PDF 格式的离线报表下载。在系统的报表功能中，还能够根据历史监测结果绘制趋势图，从而为网站安全管理提供直观的决策数据支持。

3.6. 多样部署，简易扩展

产品使用 B/S 架构，配置简单、管理方便，接入网络后配置 IP 即可使用，全部管理过程无需安装软件，使用浏览器可实现全部日常管理。

系统支持单机、集群、分布式和虚拟化等多种部署方式，可根据检测规模弹性扩展，并且拥有 10 台以上服务器集群部署的真实案例。

为了实现良好的大规模检测能力，系统采用了多种国际主流的云平台基础技术，包括分布式 NOSQL 数据库系统、分布式远程任务调度系统等先进技术。

系统提供了开放式 API 扩展接口，从而提升系统的外部扩展能力，另外，系统还可实现与国内主流 SOC 平台的无缝对接。

3.7. 众多的成熟案例

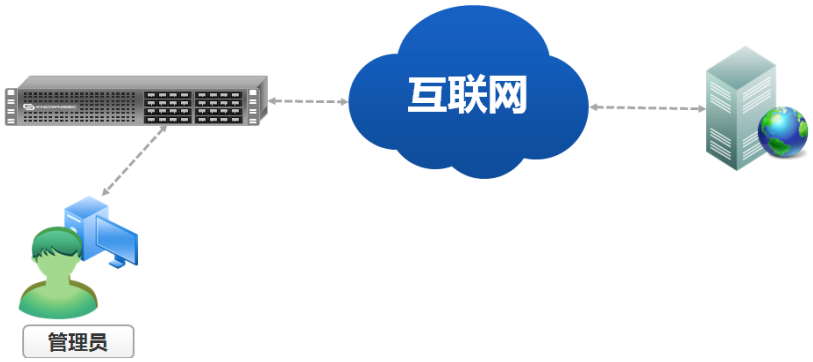
WebSOC 在国内外拥有大量的成功案例，目前，其案例数量远超国内其他厂商的同类监控产品。

4. 部署方式

4.1. 典型部署

1. 单机部署

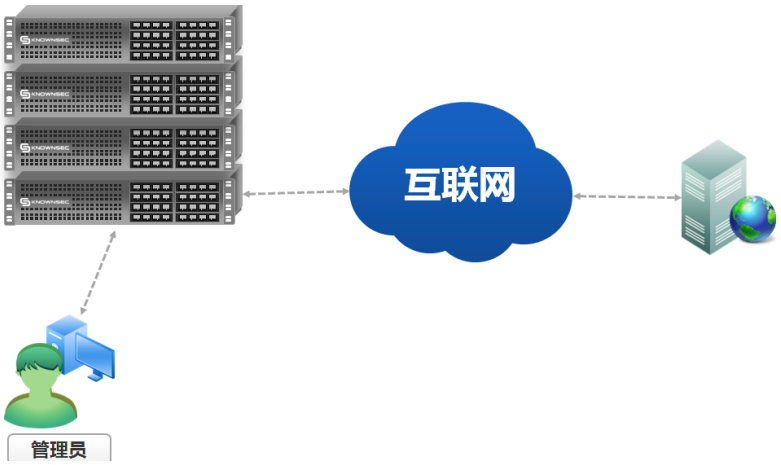
系统的单机部署方式简单，只需将产品接入到用户网络并确保产品与被检测目标间网络可达，在使用过程中，管理员通过浏览器访问 WebSOC 即可下达和查看监测结果。



图：WebSOC 单机部署

2. 集群部署

对于监控范围广、网页数量多、监测规模大的用户来说，可采用一台控制服务器，多台检测引擎的集群部署模式，使用该部署模式，可大幅度提升监测能力，并且可通过控制服务器实现简便的统一管理。

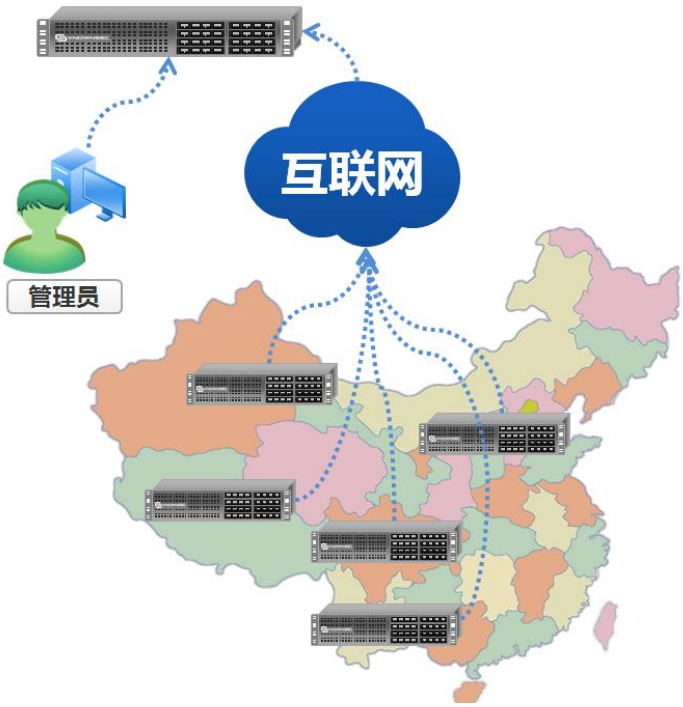


图：WebSOC 集群部署

3. 分布式部署

对于被检测目标数量大但分布广的情况，可通过分布式的方式进行部署，通过分布式部署可在集中下达任务时优先选择距离被监测目标最近的监测节点，从

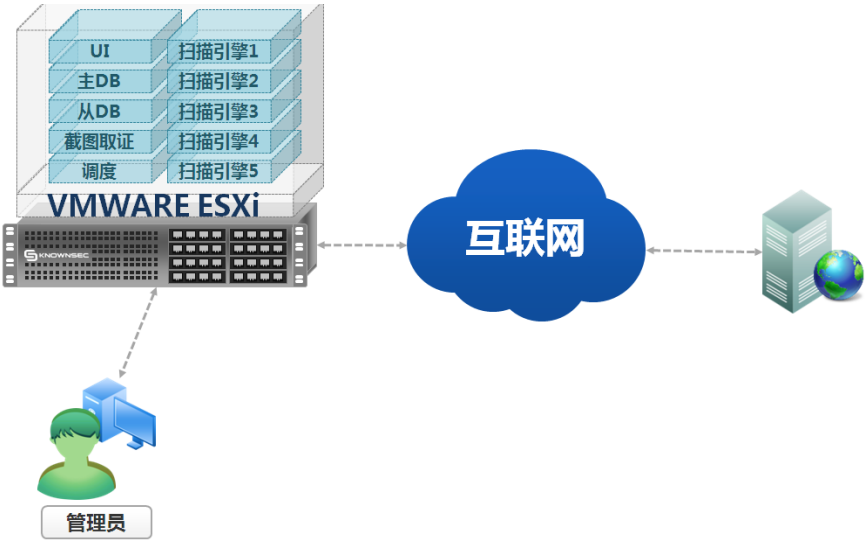
而提升监测效率和精确度。



图：WebSOC 分布式部署

4. 虚拟化部署

系统除了传统的硬件部署方式外，还可支持在 VMWARE ESXi 平台下的虚拟化部署，通过虚拟化部署，可实现更优的资源自动分配，从而在最小化的硬件投入成本下，实现最大化的资源利用。



图：WebSOC 虚拟化部署

4.2. 硬件规格

硬件型号	技术参数	监控参数
P100 	硬件规格 ：1U 内　　存 ：4G C P U　　：1 颗/4 核/主频>2.2GHz 硬　　盘 ：500G	域名：100 个 URL：50 万/天

表：P100 硬件规格

硬件型号	技术参数	监控参数
P300 	硬件规格 ：2U 内　　存 ：8G C P U　　：2 颗/共 8 核/主频>2.2GHz 硬　　盘 ：500G	域名：300 个 URL：100 万/天

表：P300 硬件规格

5. 成功案例

国际典型客户

- 美国微软（Microsoft）公司
- 香港赛马会（HKJC）
- 韩国 NSHC 公司

国内典型客户

- 国务院国家事务管理局
- 工信部国家计算机网络应急技术处理协调中心
- 中国信息安全产品测评认证中心
- 公安部国家计算机病毒应急处理中心
- 公安部第一研究所

- 天津市发展和改革委员会
- 广东省信息安全评测中心
- 河北省信息安全测评中心
- 江苏省信息安全测评中心
- 山东省信息安全测评中心
- 深圳市信息安全测评中心
- 北京通信管理局
- 上海通信管理局
- 国家电网中国电力科学研究院
- 中信证券股份有限公司
- 中国金融认证中心
- 中国移动通信研究院
- 中国电信上海公司
- 中国移动珠海分公司
- 国家医学考试中心
- 中国科技网

6. 关于我们

北京知道创宇信息技术有限公司（以下简称知道创宇）是国内最早提出网站安全云监测及云防御的高新企业，始终致力于为客户提供基于云技术支撑的下一代 Web 安全解决方案。

知道创宇总部设在北京，在香港、上海、广州、成都设有分公司，客户及合作伙伴来自中国、美国、日本、韩国等。凭借强大的云安全技术与产品的高可用性、易管理性、合规性和业务连续性、以及动态保障关键 Web 数据资产安全的能力，帮助用户应对变化多端的互联网安全威胁，赢得了企业、政府与公共机构的青睐。知道创宇安全实验室在零日安全威胁与云安全技术方面的研究得到了业内的广泛认同并享有极高知名度。

自创立以来，知道创宇业绩卓著，得到了各大互联网管理机构、多家世界五百强企业的高度认可。2009 年公司被亚洲 CIO 杂志评选为 20 家最有价值企业，中国地区仅有知道创宇与阿里巴巴获此殊荣。2012 年公司 CEO 赵伟被福布斯评为中国 30 位青年创业者之一。知道创宇卓越的解决方案覆盖众多行业领域，拥有极高的客户忠诚度，这完全得益于精湛的技术、合理的总拥有成本、产品的易管理性以及优质的客户服务。

公司网站　　http://www.knownsec.com

北京总部　　电话：010-51295887　　传真：010-52723966

上海分公司　　电话：021-36529579　　传真：021-36351567

广州分公司　　电话：020-37813982　　传真：020-37813982

成都分公司　　电话：028-61554586　　传真：028-61554586