NSFOCUS

绿盟网站安全监测服务

产品白皮书

■ **适用性声明**

完全公开

目录

插图索引

一.引言

随着 Web 应用的日益广泛及其中蕴藏价值的不断提升，引发了黑客的攻击热潮，如网站机密信息被窃取、网站被植入木马、网站页面内容被篡改、DNS 投毒或劫持、SSL 证书劫持、钓鱼网站金融欺诈、DDoS 攻击造成重要业务中断等安全事件的反复发生，极大地困扰着网站提供者，给企业形象、信息网络甚至核心业务造成了严重的破坏。

虽然可以通过部署入侵防御系统、高性能防火墙等相关防护类产品来起到一定的防护效果，然而，用户难以更早的发现风险隐患，预防这些安全事件发生。另外，安全管理员需要维护大量的安全设备，分析众多日志信息，承担更多额外的工作量。

若能主动地发现网站的风险漏洞，并及时采取修补措施，则可以降低风险和减少损失。针对这些需求，绿盟科技推出网站安全监测服务。通过持续的远程监测，为客户网站提供安全检查、安全事件监测、实时响应和安全趋势分析服务，使其成为用户网站安全体系的最好补充。

二.绿盟网站安全监测服务

2.1 服务概述

绿盟网站安全监测服务（NSFOCUS WebSafe Service，原叫 PAWSS），是一款托管式服务。您无需安装任何硬件或软件，无需改变目前的网络部署状况，无需专门的人员进行安全设备维护及分析日志。您只需将网站域名告知绿盟科技工作人员，获得授权后即可享受 7×24 小时的远程网站安全监测服务。一旦发现您的网站存在风险状况，绿盟安全专家团队会第一时间通知您，并提供专业的安全解决建议。除此之外，经验丰富的绿盟安全

专家团队会定期为您出具周期性的综合评估报告，让您整体掌握网站的风险状况及安全趋势。

通过绿盟科技专业化的服务产品来实时监测和周期度量网站的风险隐患，您可以轻松评估您网站的安全状态，跟踪改进情况，能够将网站管理人员从繁重的日常安全维护工作中解放出来，降低投入和管理成本，获得最专业、最有效、最便捷的服务，同时还遵从了政府和行业的信息安全法规要求。

2.2 服务架构

绿盟网站安全监测服务的体系架构依托于绿盟安全云，其主要分为四层：数据采集层、数据计算层、数据存储层和数据可视层。

图 2.1 绿盟网站安全监测服务架构

数据采集层

绿盟安全云的数据采集层负责采集用户的资产数据，采集待评估的漏洞数据，采集待分析的可用性和完整性数据。

数据计算层

数据计算层从缓存服务器队列中取出采集回来的数据，进行精准化的检测和智能化的分析工作，并将处理后的结果保存到数据库服务器集群中。

数据存储层

数据存储层由数据库服务器集群构成，主要存储了用户的资产信息，安全风险信息，安全事件信息等三大块内容。

数据可视层

数据可视层将数据库服务器集群中保存的资产信息、漏洞信息、告警信息进行可视化呈现，再由 7x24 小时值守团队在 30 分钟之内将人工验证后的结果通过电话、短信或邮件方式通告用户。同时，绿盟安全专家团队还会定期为用户出具专业安全报告，让用户可以对自身网站安全状况及趋势一目了然。除此之外用户可以通过登录 Portal 能够一目了然的看到风险、事件在地域上以及组织单位上的分布，同时针对暴露的漏洞风险及事件进行跟踪管理。最后用户如果在户外可以随时随地登陆手机 APP 进行漏洞生命周期管理工作。

2.3 服务优势

- 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**

    平台每 15 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。
  - **定位问题快**

    用户各单位的风险及事件以组织架构形态做可视化呈现，让用户对于所辖单位暴露的问题一目了然，同时用户在排查问题时可以得到更多的诊断信息的帮助，例如：“通断时长、链路、监测点，协议等”
- 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、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。

- **监测点分布广**

  支持多点监测，覆盖全国各省、三大运营商线路，覆盖部分海外城市。

✧ **免**

- **免物流**

  直接远程交付服务，无需走物流发货流程。

- **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。

- **免维护**

  无需处理软硬件故障、升级等问题，完全托管，无需亲自运维。

✧ **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

  能够通过分级告警的方式，更加贴合用户实际管理规范。

2.4 主要功能

“绿盟网站安全监测服务”主要包括五方面内容，资产核查、脆弱性检测、完整性检测、可用性检测和认证检测，其中资产核查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；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，完整性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；此后，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；最后，认证检测主要能够为用户提供钓鱼网站监测的功能，一经发现，我们会尽力协助客户向相关机构举报，由相关机构进行关停处理。

图 2.2 绿盟网站安全监测服务内容

2.4.1 资产核查

- **IP 资产核查服务**

  主要通过绿盟云端强大资产检测引擎为指定的 IP 网段进行资产扫描，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。

2.4.2 脆弱性检测

- **远程网站漏洞扫描服务**

  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，由绿盟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，并且用户可以通过绿盟网站安全监测系统平台，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。

2.4.3 完整性检测

- **远程网页挂马及黑链监测服务**

  绿盟科技基于安全云平台，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。

- **远程网页篡改监测服务**

  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。用户可参考绿盟科技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。

- **远程网页敏感内容监测服务**

  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。用户可参考绿盟科技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。

2.4.4 可用性检测

- **远程网站域名监测服务**

  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 授权服务器的可用性，以及它们对被监测域名的解析结果情况。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。用户可参考绿盟科技提供的安全建议恢复域名正常解析，避免域名不可用给访问者带来不好的体验，甚至给自身造成经济损失。另外，针对用户 DNS 授权服务器，提供每周一次的 DNS 记录配置核查，包括：A 记录、CNAME 记录、NS 记录、MX 记录、SOA 记录、PTR 记录。

- **远程网站平稳度监测服务**

  从各省运营商网络线路 114 个点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，根据事先定

义好的网站通断级别，第一时间通知相应的用户。并告知其通断时长以及详细链路、协议以及各监测点的诊断信息。用户可参考绿盟科技提供的安全建议优化网站性能，避免网站业务中断或响应延迟给访问者带来不好的体验，甚至给自身造成经济损失。用户也可以视情况选择合适的网站响应时间告警阈值。

2.4.5 认证检测

- **远程钓鱼网站监测服务（暂时受控）**

  通过对用户域名进行 500 多种变形来监测针对用户的钓鱼网站，还可根据用户提供的关键词组，持续对主流搜索引擎返回的搜索结果进行监测，防止钓鱼攻击者利用搜索引擎这种途径来传播钓鱼网站。另外，该服务也可对客户过期域名持续监测，防止客户过期域名被钓鱼攻击者利用。一旦发现钓鱼网站，绿盟安全专家团队会第一时间通知用户，提供必要的信息，方便用户及时提醒其客户识别钓鱼网站，以免上当受骗。用户也可书面授权绿盟安全专家团队协助客户向相关机构举报，由相关机构进行关停处理。争取最大限度缩小钓鱼网站影响范围，从而保护用户利益及网站品牌信誉。

2.5 服务流程

您只需将网站域名告知绿盟科技工作人员，约定服务交付细则，获得授权后即可享受绿盟网站安全监测服务。绿盟安全专家团队会在绿盟安全云 7×24 小时值守，远程实时监测您的网站。一旦发现您的网站存在风险状况，绿盟安全专家团队会在第一时间通过电话、短信和邮件方式通知您，并且提供专业的安全解决建议。同时，经验丰富的绿盟安全专家团队会定期为您出具周期性的综合评估报告，让您整体掌握网站的风险状况及安全趋势，最后您也可以登录绿盟自助门户系统（Portal）随时随地掌握最新暴露的真实漏洞等信息。

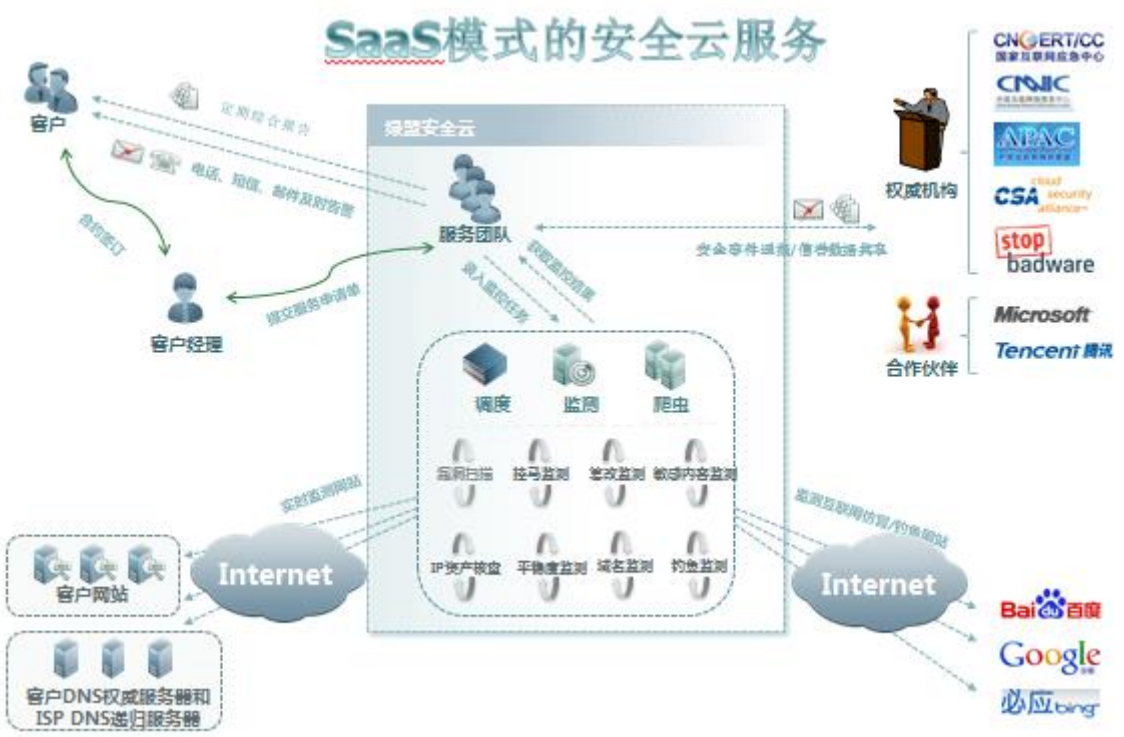

图 2.3 绿盟网站安全监测服务流程

三.客户利益

- **降低风险**

  实时监控您的网站安全状况，一旦发现存在风险隐患，第一时间通知您采取应对措施，将风险影响消灭在萌芽状态，降低网站运营风险，减少业务损失。

- **提高效率**

  通过专业的安全外包服务，您能够从繁重的日常安全维护工作中解放出来，提高工作效率，将精力集中在核心业务上。

- **减少成本**

  远程托管式安全服务，按需付费，经济实惠，大大节省您在安全软件或设备方面的投入和维护成本，并且减少安全人员投入，节省您的人力资源成本和管理费用。

四.总结

绿盟网站安全监测服务，是一款纯托管式服务。您无需安装任何硬件或软件，无需改变目前的网络部署状况，无需专门的人员进行安全设备维护及分析日志，就可以享受的 7×24 小时服务，无论白天、黑夜，绿盟安全云与绿盟安全专家团队总是能第一时间捕获到已发生的安全事件，将该事件所造成的消极影响进行最小化处理。同时绿盟安全专家团队还能够非常敏锐的洞悉您站点的安全风险变化，并对这些存在风险的点，给出合理的修补建议来，最终让您达到“降低风险、提高效率、减少成本”的网站运营目标。