云磐云安全服务平台

用户指南

厦门服云信息科技有限公司
www.safedog.cn

目 录

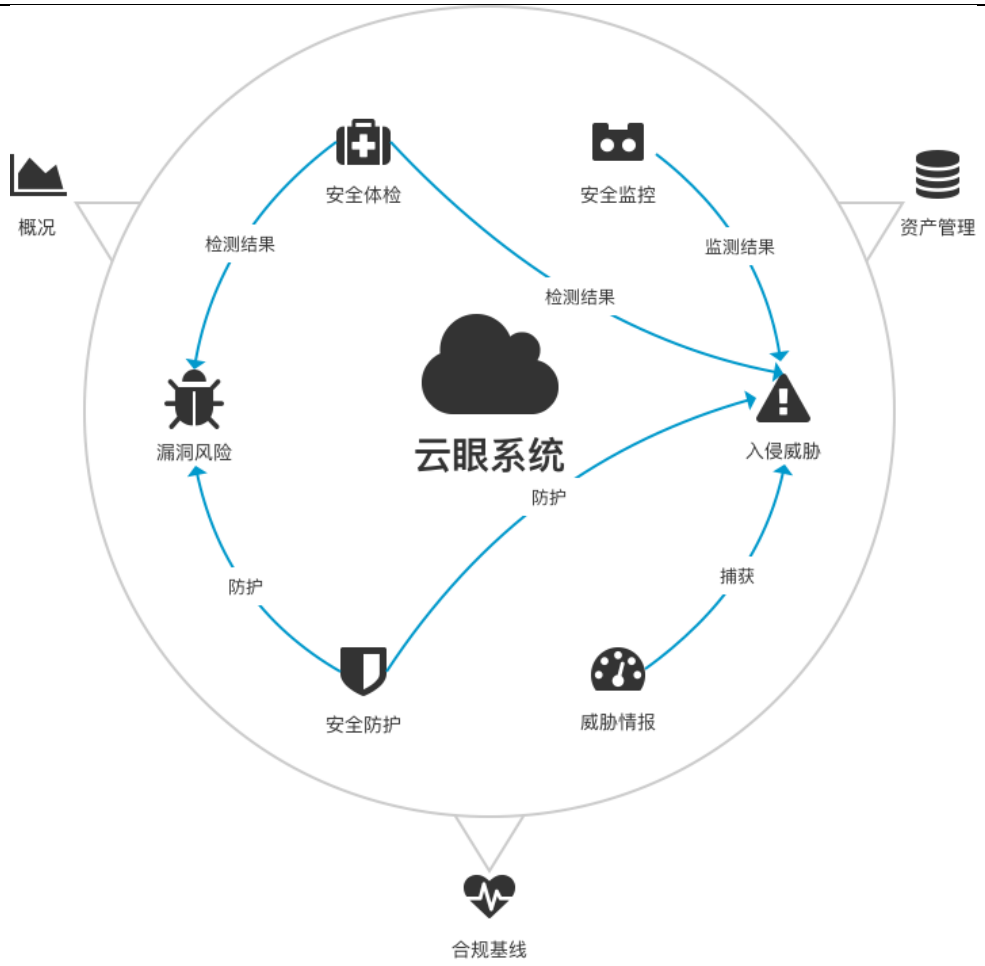
1登录

用户（子账号）在前台登录。

前台登录界面

2云眼产品核心功能

云眼系统的组成有概况、资产管理、安全体检、安全监控、漏洞风险、入侵威胁、合规基线、威胁情报等多个功能模块，各个模块进行联动，模块间数据联通，形成闭环系统，为企业提供强有力的采集、检测、监测、防御、捕获能力，对主机进行全方位的安全防护。



云眼模块间数据流示意图

2.1 概况

概况页用以显示云眼系统基本概况，展示资产管理、漏洞风险、入侵威胁、安全监控基本数据信息及数据图表，同时也作为各个模块的快速入口。

2.2 资产管理

资产管理功能定期获取并记录主机上的端口、网站、Web 容器、第三方组件、数据库、进程、账号等信息，进行统一的管理和清点。

通过资产管理功能可实时掌握 IT 系统内部的资产情况，支持资产变更分析对各类资产的变动情况进行记录，便于审计历史变动，自主发现异常资产行为；支持主机分组及各类资产信息标签添加；支持

资产采集频率设置；支持资产信息导出；支持主机及对应资产双维度查看。

2.3 安全体检

安全体检中用户可主动发起主机深度检测，检测的项目包括：系统漏洞、弱口令、高危账号、配置缺陷、病毒木马、网页后门、反弹 shell、异常账号、日志删除、异常进程、系统命令校验等。安全体检检测出的问题系统自动进行问题归类类到漏洞风险及入侵威胁模块中。

- **支持自定义体检项体检、自定义路径体检**

用户可自行选择体检项目 ,其中病毒木马检测支持快速扫描、全盘扫描及自定义路径扫描三种方式，网页后门检测支持自定义路径扫描。

- **支持即时体检及定时体检**

云眼支持即时体检及定时体检两种体检模式，即时体检即检测命令下发后后立即执行体检命令；定时体检用户设置扫描周期、扫描时间段后系统会按照设置规则定时执行体检命令。

- **支持批量体检策略下发**

云眼支持批量体检策略下发，通过设置体检的类型、体检的项目、体检的主机范围进行批量体检策略下发。并且支持定时体检策略与即时体检策略两种类型。

- **支持体检报告生成导出**

云眼支持体检报告生成及导出，体检报告展示体检分数、健康指数，体检结果图表化展示及详细体检问题说明展示，可导出 Word 格式的体检报告

- **支持体检结果自动评分**

云眼支持体检结果自动评分 ,通过检测的结果与预置的体检评分规则进行匹配可自动对主机健康情况进行打分，0-59 分为不健康主机，60-89 分为亚健康主机，90-100 为健康主机。

2.4 安全监控

安全监控中用户可对主机开启各类监控包括登录监控、完整性监控、操作审计、进程监控、资源监控、性能监控。从主机安全角度，全天候监控主机的运行情况，能确保第一时间发现服务器问题，排除故障时间提速 10 倍，帮助企业快速发现安全风险和性能瓶颈。安全监测监测出的问题系统自动进行问题归类类到漏洞风险及入侵威胁模块中。

2.5 漏洞风险管理

漏洞风险包含两个部分，一是主机自身的安全漏洞如系统漏洞(Windows 漏洞及 Linux 系统漏洞)、网页漏洞等；二是人为原因造成的风险因素如弱口令（操作系统弱口令、数据库弱口令等）、高危账号（高权限账号、空密码账号、用户名和密码相同的账号）、配置缺陷（操作系统配置缺陷、Web 容器配置缺陷、数据库配置缺陷等）。

漏洞风险管理模块会显示当前主机上的漏洞风险情况，同时提供修复方案供用户进行参考；该模块执行时会从云端下载漏洞策略库在本地执行检测，对于存在漏洞风险的主机，会上报应用软件的名称、版本号、路径、发现时间，这个过程不会提取任何涉及用户隐私的数据。对于检测出的各类漏洞风险进行风险等级评估。

2.6 入侵威胁管理

入侵威胁管理用以展示及处理各类入侵事件及具有高度威胁的事件，支持识别并处置的入侵威胁事件包括：病毒木马、网页后门、反弹 shell、异常账号、日志删除、异常登录、异常进程、系统命令校验等。

云眼对接国内外主流查杀引擎，可检测出恶意进程及软件，并提供隔离、信任等功能。

2.7 安全防护

云眼提供强大的安全防护功能支持端口安全防护、防护控制、暴力破解防护、扫描防护、病毒防护、

IP 黑白名单设置、进程行为控制。通过对各类攻击事件的采集分析生成攻击趋势图、攻击分布图等图表，直观展现各类攻击事件。根据攻击事件危害程度自动匹配风险等级，并提供详实的攻击特征描述，用户可以此为参考对攻击者 IP 进行加黑处理，也可导出攻击事件做后续攻击分析。

2.8 合规基线

在等级保护检查、测评、整改工作过程中，对定级业务系统进行对应级别的安全风险检查是技术方面的必要工作，通过使用云眼的合规基线功能进行基线检查即可轻松完成。

云眼对国家等级保护规范进行了详细整理，把技术标准落实到每一种应用的配置检查工作上。云眼结合等级保护工作过程，对业务系统资产进行等保定级跟踪，根据资产定级自动进行对应级别的安全配置检查，对合规情况出具等保符合性报告，保证系统建设符合等保要求，促使等保监督检查工作高效执行。

- **提供官方等保基线模板，满足等保二级及等保三级要求；**
- **支持用户自定义基线模板；**
- **支持合规基线检查策略批量下发；**

2.9 威胁情报

云眼威胁情报来自安全狗云端的分析成果，针对高级持续性威胁、新型木马、特种免杀木马进行规则化描述。威胁情报通过人工智能结合大数据知识以及攻击者的多个维度特征还原出攻击者的全貌，包括程序形态，不同编码风格和不同攻击原理的同源木马程序，恶意服务器（C&C）等，通过全貌特征'跟踪'攻击者，持续的发现未知威胁，最终确保发现的未知威胁的准确性，并生成了可供大数据分析平台使用的威胁情报。

2.10安全报表

整体网络态势感知，根据主机有无被入侵、是否有监控异常、体检不健康主机数评判当前整体网络态势；

自定义时间区间分析生成全站攻击趋势、攻击类型分布、资产分布、漏洞风险分布、漏洞发现趋势、入侵威胁分布、入侵威胁发现趋势、新增监控异常分布、监控异常变化趋势等图表。

支持全站安全信息报表生成导出；

3 云御产品核心功能

云御系统的组成有概况、攻击分析、安全防护、虚拟补丁、系统设置等多个模块。安全防护模块主要用于设置 WAF 节点的防护规则、黑名单管理和封禁区域管理；攻击分析模块主要功能为对 WAF 防护规则拦截的攻击行为进行分析展示，以及攻击源 IP 进行分析；虚拟补丁模块展示了云御 WAF 虚拟补丁内容及虚拟补丁拦截的攻击行为；系统设置模块为云御 WAF 安装部署指导功能；概况页面展示所有站点的攻击统计、攻击类型分布以及访问趋势情况。

3.1 概况

概况页用以显示云御系统基本概况，用户可根据需求选择不同站点以及时段展示对应信息。展示攻击总数、攻击 IP、独立访客、浏览次数统计数据，WEB 攻击趋势以及访问趋势，攻击来源 IP Top5、攻击来源区域 Top5、攻击类型分布以及攻击站点分布统计图，统计图可直接进入攻击分析模块。

3.2 攻击分析

云御攻击分析包括攻击事件分析和攻击源分析。

3.3 安全防护

防护列表显示当前所有 WAF 节点以及站点信息。WAF 节点信息包括 IP 地址，防护状态，RASP 防护，Agent 类型，站点个数，安装时间等，可进行手动关闭开启防护。

点击站点个数下拉显示站点列，点击操作-展开显示站点列表，点击站点数下拉显示站点列表，再次点击隐藏下拉显示。节点下的站点支持手动添加以及删除。

3.4 封禁区域

支持对特定地区的来源 IP 进行封禁，在对应的域名开启防护模块后，可对封禁区域进行设置，支持国内各省份和国外。可批量导入导出。

3.5 虚拟补丁

CVE 上公布了 2000 多个数据库安全漏洞，这些漏洞给入侵者敞开了大门。数据库厂商会定期推出数据库漏洞补丁，由于数据库打补丁工作的复杂性和对应用稳定性的考虑，就可能无法及时更新补丁。云御提供了虚拟补丁功能，在网络层创建了一个安全层，自动下载虚拟补丁供客户使用，对 WEB 漏洞利用进行有效拦截，从而及时消除 Web 漏洞，完成 WEB 漏洞防护，形成“从漏洞监控到虚拟补丁”的闭环管理。

云御虚拟补丁功能提供了虚拟补丁详细信息，包括漏洞名称、漏洞描述、补丁更新时间以及安全建议。同时提供查看虚拟补丁拦截的攻击行为。

4 云固云管理平台核心功能

云固系统的组成有概况、服务器管理、安全防护、系统设置等多个模块。各个模块进行联动，模块之间数据联通，形成闭环系统。

4.1 概况

概况页用以显示云固系统基本概况，用户可根据需求选择不同时段展示对应信息。系统对被篡改站点和被篡改站点恢复站点进行统计，并且以扇形图形式体现。被篡改网站列表展示被篡改网页被篡改时间、被篡改文件路径、web 服务器以及状态等，可通过站点域名或站点域名进行筛选。

4.2 服务器管理

服务器管理显示当前主/备发布服务器、WEB 服务器。可分别对服务器类别、服务器状态、配置状态进行筛选。可对某一个服务器进行修改、删除、备注，选中某一条展开，显示其对应的防护方案。可批量导出服务器信息。

主/备发布服务器，可以设置多个 FTP Host 供选择。FTP 模式可选自动或被动。

WEB 服务器设置数据通道端口范围。

4.3 安全防护

通过新建方案，对网页进行防护。通过安全防护名称来区别各方案，所以名称不可重复，发布服务器（主）和 WEB 服务器必选。依次完成基础设置-发布服务器设置-WEB 服务器设置。

在基础设置中，若发布服务器（主）为 Windows 系统，则发布服务器（备）只能选择 Windows 系统的，WEB 服务器可选 Windows 或 Linux 系统。

主/备发布服务器设置中监控站点的路径要在 FTP 根目录下。FTP Host 可根据需求进行选择。

如果主/备发布服务器在服务器配置时，FTP 模式选主动模式，对应的 web 服务器端口范围就由客户配置的下发。

新建方案将会同步到服务器管理列表中。可对各方案进行修改，不可修改主发布服务器以及 WEB 服务器，若新建方案时未配置发布服务器（备），可新增。已配置过的发布服务器（备）则不能修改。

4.4 告警

当网页被篡改会发送告警消息，可对告警进行设置，设置告警手机或邮箱。将记录所有历史告警信息。如果没有过滤，导出全部所有的告警；如果有过滤条件，导出全部导出筛选过后的告警数据。