



SANGFOR
深信服科技

信服云眼 V2.0

用户手册

深信服科技股份有限公司

2018. 03

目录

目录	2
1 行业用户	3
1.1 用户注册	3
1.2 首页	4
1.3 业务监测	6
1.4 风险管理	7
1.5 报告中心	7
1.6 设置	8
1.7 篡改应急处置	9
1.7.1 登陆并配置 IP	9
1.7.2 DNS 配置	10
1.8 个人中心	12
2 开通主管单位账号	13
2.1 账号开通	13
2.2 总览	13
2.3 事件中心	14
2.4 单位管理	14
2.5 报告中心	15
2.6 设置	16
3 开通渠道账号	16
3.1 渠道首页介绍	18
3.2 渠道用户管理	20
4 微信公众号	27
4.1 事件通知	28

1 行业用户

1.1 用户注册

1、登陆信服云眼，进入注册页面

页面链接：<https://saas.sangfor.com.cn>



2、点击注册，同时绑定深信服推荐人或本地服务商，点击提交进行注册



账号：

设置密码：

密码确认：

单位名称：

单位地址：

联系人：

联系电话：

邮箱地址：

完成，下一步



开通类型：

服务有效期：

授权域名数：

信服推荐人：

Moa验证码：

1.2 首页

首页每 1 分钟监测一次，子目录每 5 分钟检测一次，实时显示监测进度，如果发生篡改

页面背景变红提示并微信推送篡改事件



持续无篡改事件 38 天 15 小时

监测业务：15个 | 监测频率：5分钟（首页1分钟） | 持续监测：37.34 万次 | 潜在篡改风险：46个

[微信推送](#) [报警](#) [设置](#) [帮助](#) [反馈](#)



正在对12个业务进行监测，发现1个篡改事件

• 2017/09/15 11:45


[查看详情](#)

首页展示网站目录结构和监测次数和进度

篡改监测

测试9009 (http://www.melkoo.biz/9009)

第 6974 次监测 (2017-09-15 11:45) 45%



当前监测业务

业务名称	监测进度
中山景城_驾车路口T-pageadmin政府网站管理系统-Pow... (Index.aspx?Itemid=1057&id=5)	正在监测...
南澳渔场-pageadmin政府网站管理系统-Powered by Pag... (Index.aspx?Itemid=62&subItemid=920)	正在监测...
海康威视-pageadmin政府网站管理系统-Powered by Pag... (Index.aspx?Itemid=102&subItemid=1076)	正在监测...
抚州市户外广告设施管理工作汇报会-pageadmin政府网站管... (Index.aspx?Itemid=1076&id=792)	正在监测...
抚州市社会工作网上展示厅-pageadmin政府网站管理系统... (Index.aspx?Itemid=1076&id=962)	正在监测...
抚州市行政服务中心自助服务系统-pageadmin政府网站管理系... (Index.aspx?Itemid=1076&id=961)	正在监测...

总体业务漏洞评估结果总览


漏洞评估

风险分布 (上次评估: 2018-03-15) | 预计下次评估: 2018-04-15

168

风险总数

- 存在篡改风险: 46
- 非篡改类风险: 122



存在篡改问题TOP5

漏洞类型	数量
XSS注入	30
SQL注入	15

非篡改类风险TOP5


漏洞类型	数量
信息泄露	35
CSRF跨站	30
信息发现	25
暴力破解	10
点击劫持	10

监测时间，篡改样本来源展示

云眼监测中心

持续篡改监测 86 天 | 10:19:48

安全专家 48位



样本来源分布

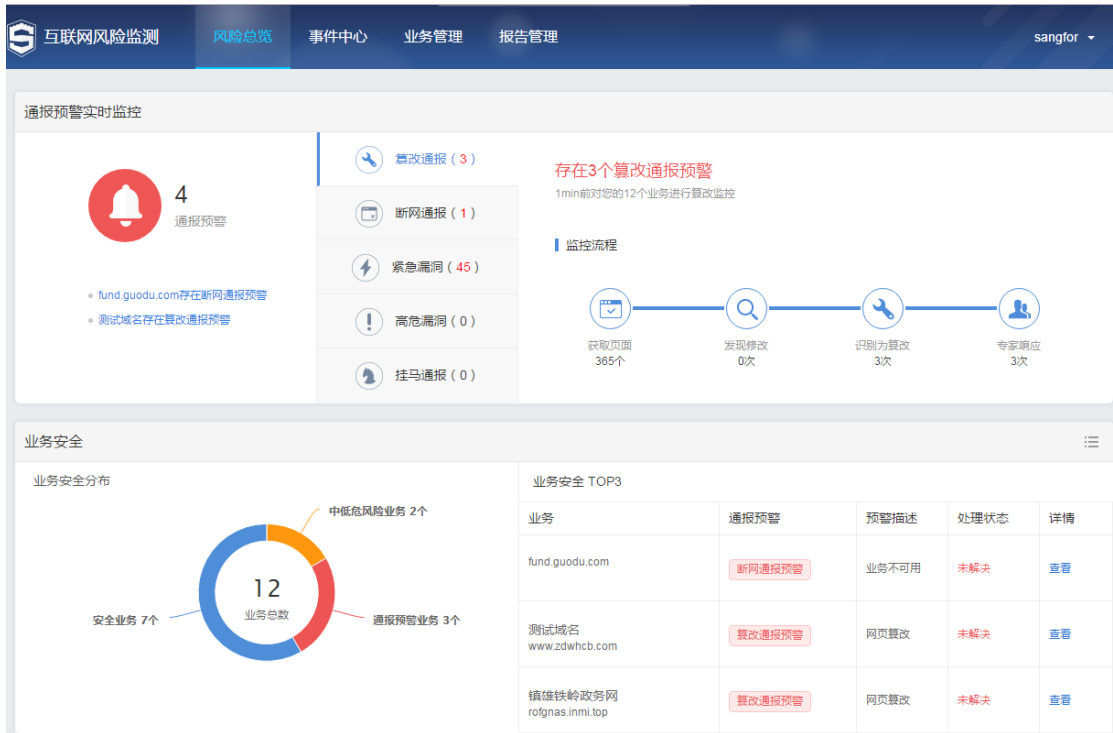
11075

样本总数

- 携程云眼: 3509
- 深信服云眼: 2681
- 深信服vuln: 4885

新增样本

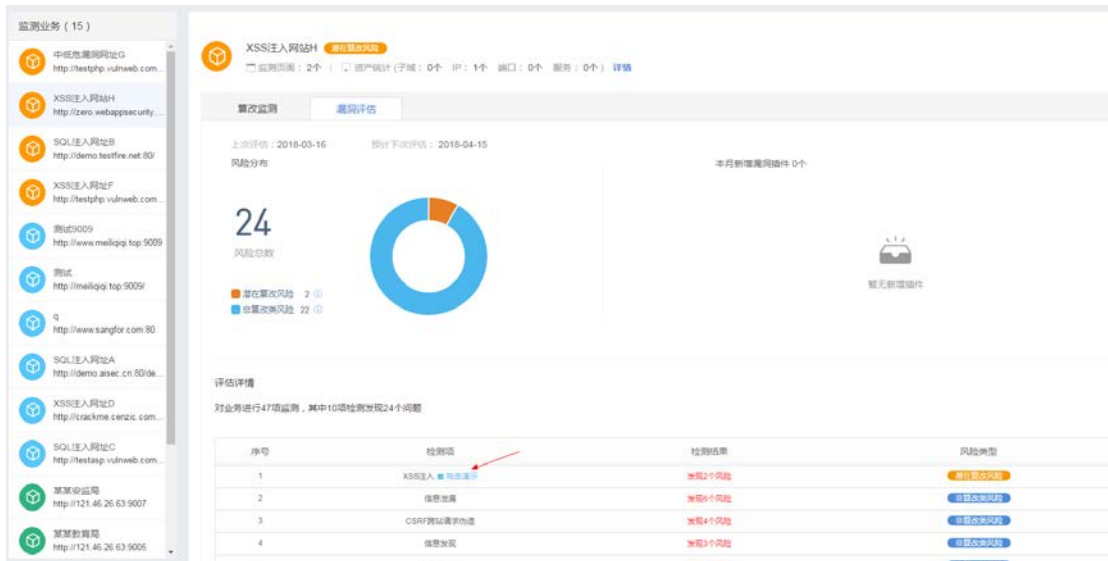
2018-03-16 13:42	监测到四川省委***公司在***篡改	携程云眼
2018-03-14 12:13	监测到辽宁省委***公司在***篡改	携程云眼
2018-03-13 14:43	监测到浙江省委***公司在***篡改	携程云眼



1.3 业务监测

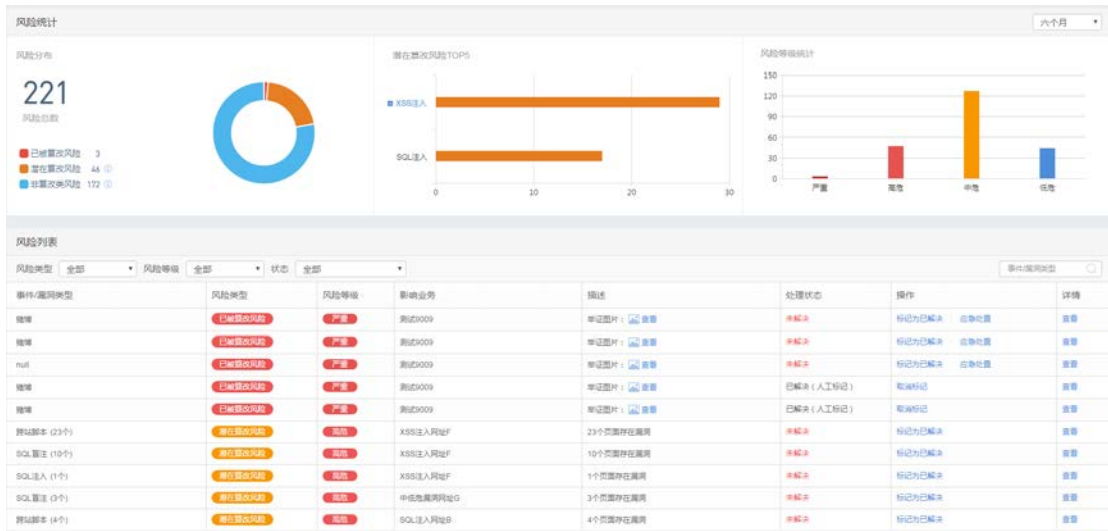
单个网站业务安全情况，同类型漏洞攻击演示，全面了解漏洞危害





1.4 风险管理

风险分布、风险等级统计, 高危风险解决/未解决标识



1.5 报告中心

报告中心

序号	报告类型	报告描述	生成时间	操作
1	云扫描报告-特殊	评估http://www.sangfor.com/80第1个链接,发现高危风险0个,中危风险1个,低危风险1个	2018-03-16 19:29:06	查看报告
2	每日安全通报	每日安全通报20180316	2018-03-16 00:10:06	查看报告
3	每日安全通报	每日安全通报20180315	2018-03-15 00:12:07	查看报告
4	每日安全通报	每日安全通报20180314	2018-03-14 00:08:38	查看报告
5	云扫描报告-特殊	评估http://www.sangfor.com/80第1个链接,发现高危风险0个,中危风险0个,低危风险0个	2018-03-13 03:19:30	查看报告
6	每日安全通报	每日安全通报20180313	2018-03-13 00:09:49	查看报告
7	每日安全通报	每日安全通报20180312	2018-03-12 00:07:38	查看报告
8	每日安全通报	每日安全通报20180311	2018-03-11 00:09:07	查看报告
9	每日安全通报	每日安全通报20180310	2018-03-10 00:08:29	查看报告
10	每日安全通报	每日安全通报20180309	2018-03-09 00:08:53	查看报告

显示第 1 到第 10 条记录, 总共 263 条记录 每页显示 10 条记录

序号	报告类型	报告描述	生成时间	操作
1	两会值守报告	两会值守报告20170316	2017-03-16 13:15:16	查看报告

显示第 1 到第 1 条记录, 总共 1 条记录

除了菜单栏中展示的六种报告外, 还可以选择右上角“导出值守报告”自定义时间导出值守报告

导出值守报告

名称: sangfor

时间范围: 选择日期范围

2018年2月

日	一	二	三	四	五	六
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	1	2	3
4	5	6	7	8	9	10

2018年3月

日	一	二	三	四	五	六
25	26	27	28	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	今天
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

1.6 设置

添加和删除业务, 应急处置设置 (用于篡改处置, 替换篡改页面)

序号	业务名称	域名	应急处置设置	监测状态	操作
1	SQL注入网址A	http://demo.aesec.cn:80/demo/aesec/	未设置	监测中	↶ ✖
2	SQL注入网址B	http://demo.testfire.net:80/	未设置	监测中	↶ ✖
3	某某安全网	http://121.45.26.63:9007	未设置	监测中	↶ ✖
4	某某教育网	http://121.45.26.63:9005	未设置	监测中	↶ ✖
5	某某公安局	http://121.45.26.63:9001	未设置	监测中	↶ ✖
6	某某税务局	http://121.45.26.63:9003	未设置	监测中	↶ ✖
7	中低危漏洞网址G	http://testphp.vulnweb.com:80/AJAX/	未设置	监测中	↶ ✖
8	XSS注入网址F	http://testphp.vulnweb.com:80/	未设置	监测中	↶ ✖
9	测试9009	http://www.mallqig.top:9009	✔ 设置成功	监测中	↶ ✖
10	测试	http://mallqig.top:9009/	未设置	监测中	↶ ✖

显示第 1 到第 10 条记录, 总共 15 条记录 每页显示 10 条记录

1.7 篡改应急处置

发生篡改了，严重时可导致监管通报，舆论影响，甚至领导下课.....为了避免篡改带来的严重影响，用户只要将网站接入安全云平台，当篡改事件发生时，一键选择将网站断网，第一时间规避篡改带来的通报问题。

以下是篡改应急接入教程：

1.7.1 登陆并配置 IP

2、进入业务配置界面，选择要配置的域名，点击编辑按钮

序号	业务名称	域名	应急处置设置	监测状态	操作
1	SQL注入网址A	http://demo.aesec.cn:80/demo/aesec/	未设置	监测中	↶ ✖
2	SQL注入网址B	http://demo.testfire.net:80/	未设置	监测中	↶ ✖
3	某某安全网	http://121.45.26.63:9007	未设置	监测中	↶ ✖
4	某某教育网	http://121.45.26.63:9005	未设置	监测中	↶ ✖
5	某某公安局	http://121.45.26.63:9001	未设置	监测中	↶ ✖
6	某某税务局	http://121.45.26.63:9003	未设置	监测中	↶ ✖
7	中低危漏洞网址G	http://testphp.vulnweb.com:80/AJAX/	未设置	监测中	↶ ✖
8	XSS注入网址F	http://testphp.vulnweb.com:80/	未设置	监测中	↶ ✖
9	测试9009	http://www.mallqig.top:9009	✔ 设置成功	监测中	↶ ✖
10	测试	http://mallqig.top:9009/	未设置	监测中	↶ ✖

3、输入对应的 IP 地址，请确保 IP 地址输入正确。

编辑

域名： http://www.meiliqiqi.top:9009

名称： 测试9009

指向地址： 121.46.26.63

保存 取消

输入成功后，根据提示进入 DNS 配置教程

1.7.2 DNS 配置

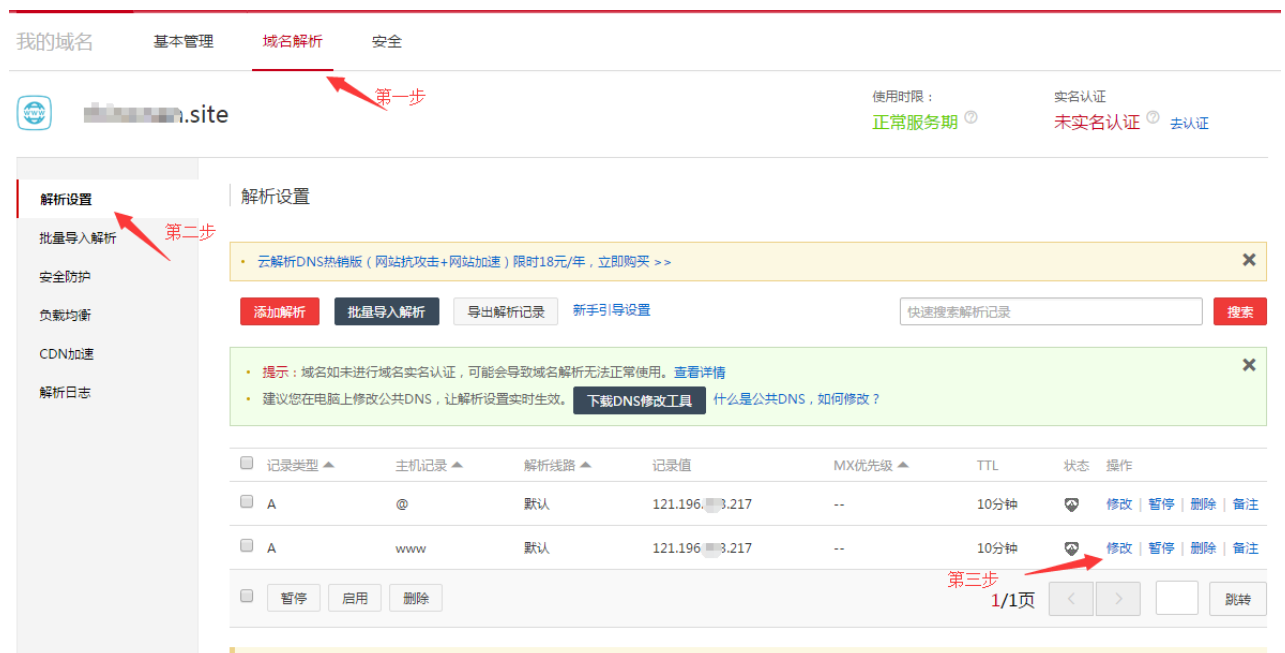
修改需要防护业务的 DNS，指向深信服的智能 DNS（以阿里云为例）

- 1、登录您购买域名时的网站，进入域名管理。



2、选择顶部 域名解析 ， 选择左侧 解析设置 。

然后如图所示点击修改。



3、点击修改 DNS,将 DNS 修改为 cloudwafdns.sangfor.com。



然后点击确定, DNS 解析会在24小时之内生效。

注: 修改 DNS 以后, 由于运营商 DNS 缓存机制, 深信服的智能 DNS 服务不会马上生效,

可修改 TTL 改变 DNS 缓存时间,这个时间越短越好, 因为这样, 能更快地接入域名。

1.8 个人中心

UI 路径: 导航栏->公司名称: [sangfor]->修改密码



用户可以自行修改初始密码

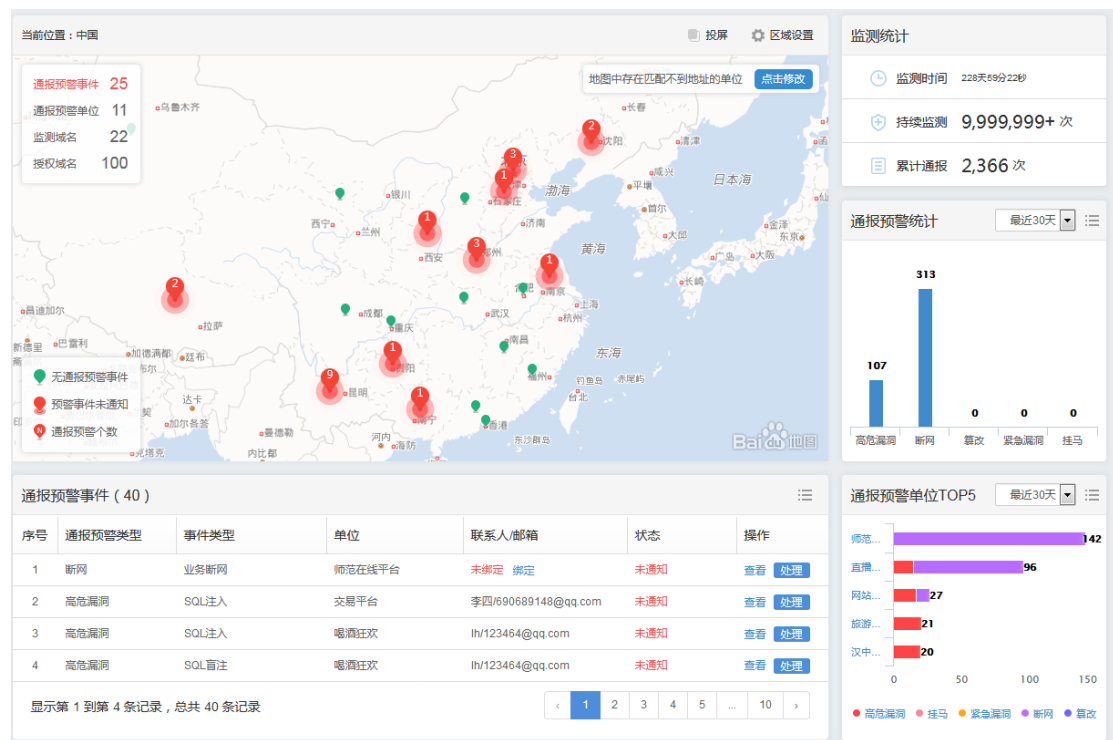
2 开通主管单位账号

2.1 账号开通

开通主管单位的用户，需要联系当地销售，并提供授权函，由深信服客服开通。

2.2 总览

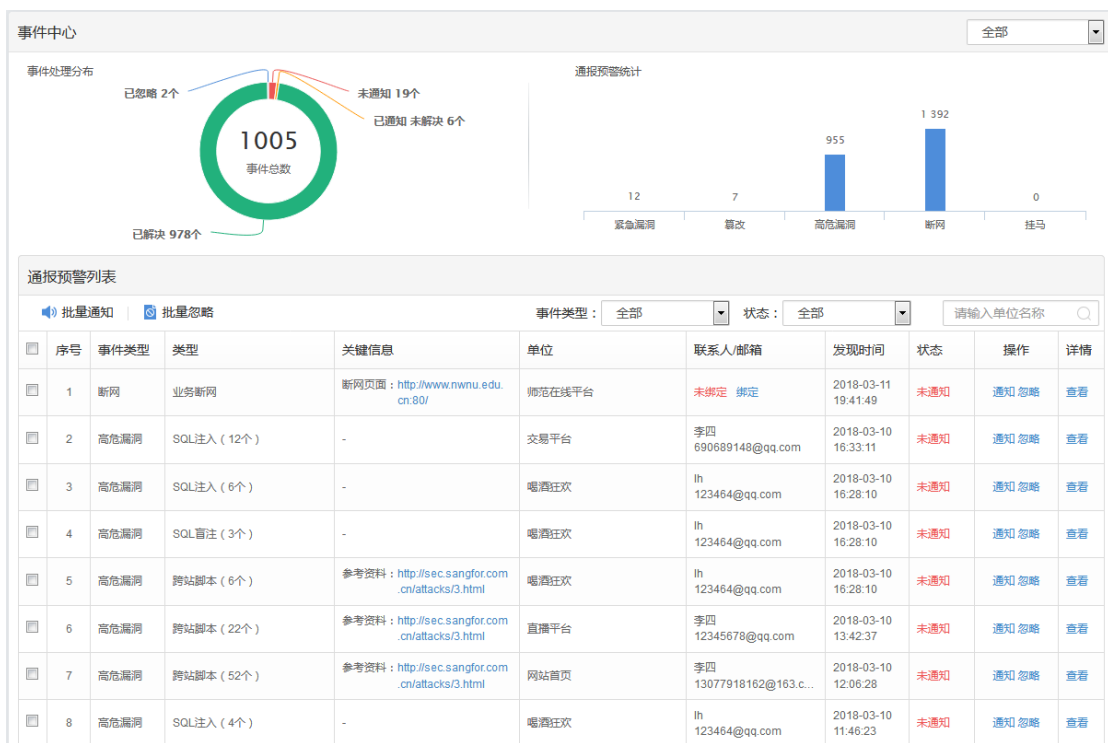
总览表中包含监测域名个数，风险个数，监测时间等，另有投屏功能根据地图位置展示风险（红色表示存在风险，绿色表示业务安全）





2.3 事件中心

事件处理分布，通报预警统计，对于下属单位通知/忽略漏洞



2.4 单位管理

新增/删除下属管理单位，每个单位详细的安全状况，左侧列表存在风险的单位有红点凸起，排列在列表前面

单位列表 (56) 新增

请输入关键字

- 桃花源旅游局
- 旅游区
- 皇阁会议中心
- 师范在线平台
- 镜子里的世界
- 捷克老将克莱
- 网站首页
- 伽马市国土资源局
- 交易平台
- 直播平台
- Sangfor HK
- testing
- s
- Gardenia
- 百度
- 星际垃圾处理
- 哈利波特

桃花源旅游局 通报预警

联系人: lh 邮箱: 123457@qq.com
电话: - 地址: 河南郑州

通报预警事件 域名管理

全部

0/0 更改 (未解决/总数) | 7/11 高危漏洞 (未解决/总数) | 0/0 紧急漏洞 (未解决/总数) | 0/0 挂马 (未解决/总数) | 0/2 断网 (未解决/总数)

批量通知 | 批量忽略

事件类型: 全部 状态: 全部

序号	事件类型	类型	关键信息	发现时间	状态	操作	详情
1	高危漏洞	IIS配置文件名泄露 (2个)	-	2018-03-10 10:14:30	未通知	通知忽略	查看
2	高危漏洞	HTTP.sys远程代码执行漏...	-	2018-02-08 03:58:31	已通知 未解决	--	查看
3	高危漏洞	跨站脚本 (6个)	参考资料: http://sec.sangf...	2018-02-08 03:58:31	已通知 未解决	--	查看
4	断网	业务断网	断网页面: http://www.huax...	2017-09-30 10:49:54	已解决	--	查看
5	断网	业务断网	断网页面: http://www.huax...	2017-09-24 16:38:42	已解决	--	查看

显示第 1 到第 5 条记录, 总共 5 条记录

2.5 报告中心

每日安全播报, 和安全评估报告

报告列表

刷新 | 导出报告

序号	报告类型	报告描述	生成时间	操作
1	每日安全播报	每日安全播报20180317	2018-03-17 00:19:19	查看报告
2	每日安全播报	每日安全播报20180316	2018-03-16 00:18:53	查看报告
3	每日安全播报	每日安全播报20180315	2018-03-15 00:19:42	查看报告
4	每日安全播报	每日安全播报20180314	2018-03-14 00:14:57	查看报告
5	每日安全播报	每日安全播报20180313	2018-03-13 00:16:46	查看报告
6	每日安全播报	每日安全播报20180312	2018-03-12 00:13:59	查看报告
7	每日安全播报	每日安全播报20180311	2018-03-11 00:15:46	查看报告
8	云扫描报告-持续	评估http://www.nnix.cn:80等22个站点, 发现高危风险107个, 中危风险222个, 低危风险70个	2018-03-10 16:37:58	查看报告
9	每日安全播报	每日安全播报20180310	2018-03-10 00:15:36	查看报告
10	每日安全播报	每日安全播报20180309	2018-03-09 00:15:04	查看报告

导出报告, 云扫描报告可导出每个下属管理单位的单个扫描报告, 安全运营报告可导出自定义时间内的值守报告

导出报告

云扫描报告需先生成后才能导出, 且只能导出最新的云扫描报告

报告类型: 云扫描报告 安全运营报告

时间范围: 2018-02-17 - 2018-03-17

生成报告 取消

导出报告

报告类型: 云扫描报告 安全运营报告

时间范围: 选择时间范围

2018年2月

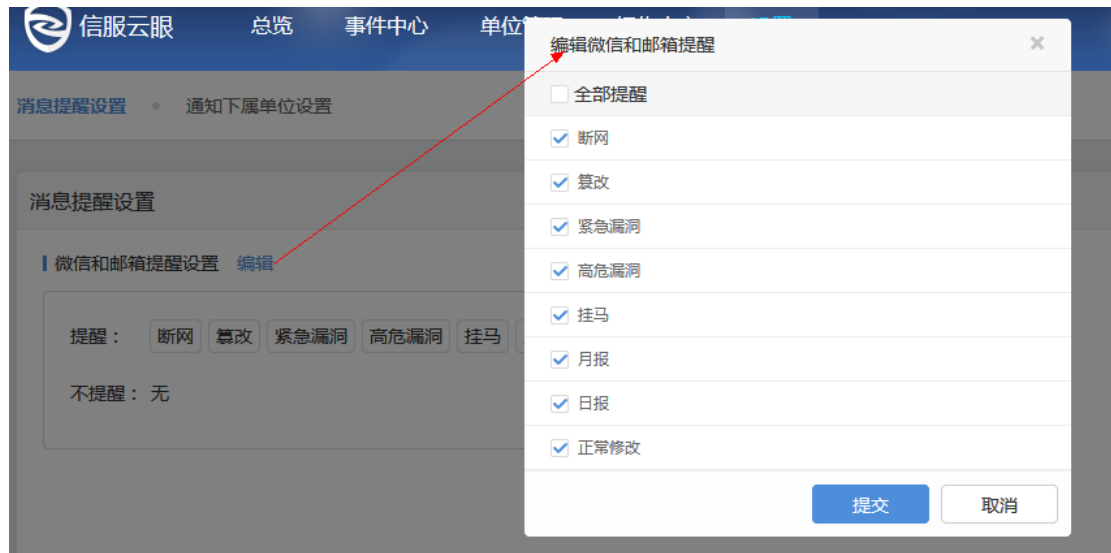
日	一	二	三	四	五	六
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	1	2	3
4	5	6	7	8	9	10

2018年3月

日	一	二	三	四	五	六
25	26	27	28	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	今天
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

2.6 设置

自定义下属单位通知模板，选择通报类型。



3 开通渠道账号

1、进入注册页面

页面链接：https://saas.sangfor.com.cn/src/html/login/register_channel.html

2、完善基本资料，同时绑定深信服推荐人，点击提交进行注册

互联网风险监测 已有账号？去登录

渠道注册

* 账号：

* 密码： ①

* 确认密码：

* 单位名称：

* 单位地址：

* 联系人：

* 电话：

* 深信服推荐人： 请填写深信服当地销售经理的工号

* 验证码：

授权网络安全评估

3、注册成功，进入互联网风险监测平台进行登录

登陆入口：<https://saas.sangfor.com.cn>



信服云眼
风险预警 危情可控

- ④ **持续评估**
感知资产变化，复查高危风险，减少暴露周期
- ⚠ **应急对抗**
云端金牌防御，专家在线值守，有效控制危情
- 🔄 **实时监测**
监测安全事件，微信可视通知，争取处置时间
- 🛑 **篡改处置**
页面快速替换，遏制事件传播，规避法律问题
- 📊 **全面可视**
风险统一管理，状态一目了然，辅助精准防护



信服云眼

没有帐号？去注册



注：渠道账号的默认使用期限为 3 个月，到期后如需继续使用，请联系深信服当

地销售经理。

3.1 渠道首页介绍

1. 虚拟资产使用及用户分布一览无余

首页详细展示购买的域名授权总数以及当前已经授权提供服务的域名数, 并将已经授权的域名用户划分为试用用户、付费用户、无意向用户, 根据不同类型挖掘商机并提供不同程度的运营服务。



注: 授权给付费用户的域名数量, 会占用渠道购买的域名数量 (试用用户不占用渠道的域名), 比如: 渠道 A 一共购买了 200 个域名授权, 把其中 100 个域名授权给付费用户 B, 剩余的可授权域名就只剩 100 个。

如需更多域名授权, 请联系深信服当地销售经理。

2. 试用用户转化率排行

针对试用用户的使用行为和安全状况进行排序, 给出前面 5 个挖掘价值最大的试用用户。

试用用户转化率排行								☰
排序	用户名称	通报预警	查看报告次数	登录次数	中低危风险个数	微信绑定	服务时间	操作
TOP 1	自动化	断网通报预警	0	👤 0 🗨️ 0	0	未绑定	已使用6个月...	查看
TOP 2	null	断网通报预警	0	👤 0 🗨️ 0	0	未绑定	已使用6个月...	查看
TOP 3	null	断网通报预警	0	👤 0 🗨️ 0	7	未绑定	已使用6个月...	查看
TOP 4	null	断网通报预警	0	👤 0 🗨️ 0	0	未绑定	已使用6个月...	查看
TOP 5	null	断网通报预警	0	👤 0 🗨️ 0	0	未绑定	已使用6个月...	查看

3.付费用户安全排行

针对付费用户的安全状况以及使用行为进行可视化战术，为渠道端运营以及进一步商机挖掘提供数据支撑。

付费用户安全排行								☰
排序	用户名称	通报预警	查看报告次数	登录次数	中低危风险个数	微信绑定	服务时间	操作
TOP 1	自动化	高危漏洞通报预警 断网通报预警 篡改通报预警	0	👤 0 🗨️ 7	9	已绑定	已使用6个月...	查看
TOP 2	自动化	断网通报预警	4	👤 0 🗨️ 12	0	未绑定	已使用6个月...	查看
TOP 3	自动化	断网通报预警	0	👤 0 🗨️ 0	0	未绑定	已使用6个月...	查看
TOP 4	sangfor	断网通报预警	0	👤 0 🗨️ 0	27	未绑定	已使用6个月...	查看
TOP 5	sangfor3	断网通报预警	0	👤 0 🗨️ 0	0	未绑定	已使用6个月...	查看

4.近期潜在商机

针对最近 7 天就要到期的用户以及最近过期的试用用户，将在右侧展示，及时掌握商机动向和潜在目标客户。

最近7天到期的试用用户TOP5		
 自动化	试用6个月	1天内到期
 北研北...	试用6个月	1天后到期

最近过期的试用用户TOP5	
 自动化	已过期2天
 Sangfor	已过期4天
 sangfor	已过期5天
 adm12345	已过期6天
 sangfor	已过期6天

3.2 渠道用户管理

用户管理为渠道提供一体化的用户维护和运营。通过用户管理可以掌握到用户商机需求、用户安全状况、用户域名运营。

根据用户的适应行为和安全状况以及线下跟踪，将用户转换为付费或者无意向用户，通

过数据积累快速实现用户商机运营。

The screenshot displays a user management interface. At the top, a user profile is shown with a trial period of 11 years (3857 days remaining). Below this, there are statistics for pushes (37), reports (0), and logins (0), along with a note that the user is not bound to WeChat. Two buttons are available: '转化为付费用户' (Convert to paid user) and '标记为无意向用户' (Mark as uninterested user). On the right, contact information is listed as '联系人: -', '电话: -', and '邮箱: liulixin9311@163.com'. The main content area is divided into '用户安全' (User Safety) and '域名管理' (Domain Management). Under '用户安全', there are two cards: '通报预警 (个)' with a count of 2 and '中低风险 (个)' with a count of 0. A '导出报告' (Export report) button is located to the right. The '历史事件' (History) section shows a timeline of events: a '月度报告' (Monthly report) on 2017-05-08 at 03:40:09, another '月度报告' on 2017-05-05 at 03:33:09, and a '断网通报预警' (Network outage notification) on 2017-04-28 at 15:16:25, which is marked as '已解决' (Resolved). The outage details include '影响业务: hahahahah (http://www.ntester.cn:80)' and '断网时长: 7天' (Outage duration: 7 days).

1) 渠道添加用户

进入用户管理，点击用户列表旁边的[+]新增用户

互联网风险监测

总览 用户管理

试用用户 付费用户 无意向用户

用户列表 (15) +

深圳高级中学 试用期30天/ 剩余5天

推送 20次 | 查看报告 10次 | 登录次数 15 | 20 | 已绑定微

转化为付费用户 标记为无意向用户

用户安全 域名管理

+ 新增域名

序号	名称	域名
1	struts2漏洞	https://www.awef.com/
2	struts2漏洞	https://www.awef.com/
3	bash漏洞	https://www.awef.com/

开通试用账号，默认使用期限为 15 天，域名限制 3 个，如需更多授权或更长的试用时间，请联系当地销售经理。

新增用户 ×

用户类型: 开通付费账号 开通试用账号

账号:

单位名称:

公司地址:

联系人:

电话:

服务有效期: 15天

授权域名数:

域名: +

剩余可配2个

授权网络安全评估

开通付费账号，默认使用期限为 1 年，如果需要更长时间，请联系当地销售

新增用户 ×

用户类型: 开通付费账号 开通试用账号

账号:

单位名称:

公司地址:

联系人:

电话:

服务有效期: 1年 (2017年6月2号至2018年6月2号)

授权域名数:

域名: +

剩余可配9个

授权网络安全评估

2) 试用用户转化为付费用户

互联网风险监测 总览 用户管理

试用用户 付费用户 无意向用户

用户列表 (15) + 新增租户

请输入关键字

- 深圳大学 3天后到期
- 深圳高级中学 5天后到期
- 深圳宝安中学
- 深圳红岭小学
- 深圳建安小学 3天后到期
- 深圳南油小学 已过期

深圳高级中学 试用期30天/ 剩余5天

推送 20次 | 查看报告 10次 | 登录次数 15 | 20 | 已绑定微信

转化为付费用户 标记为无意向用户

用户安全 域名管理

+ 新增域名

序号	名称	域名	危险
1	struts2漏洞	https://www.awef.com/	断网

转化时，请填写正式授权的域名数量

转化为付费用户

名称: 自动化

服务有效期: 1年 (2017年5月1号至2018年5月1号)

授权域名数:

授权网络安全评估

提交 取消

3) 如何导出用户的总结报告

用户的总结报告为一段时间的总结报告 (可自定义选择时间)，包含了这段时间内发生的全部安全事件



试用期11年 / 剩余3857天

推送 37次 | 查看报告 0次 | 登录次数 0 | 未绑定微信

[转化为付费用户](#) [标记为无意向用户](#)

联系人: -

电话: -

邮箱: liulixin9311@163.com

用户安全

域名管理

安全状况



2

通报预警 (个)



0

中低危风险 (个)

[导出报告](#)

历史事件

- 2017-05-08
03:40:09

○

月度报告
- 2017-05-05
03:33:09

○

月度报告
- 2017-04-28
15:16:25

○

断网通报预警 已解决

影响业务: hahahahah (http://www.nlester.cn:80)

断网时长: 7天

互联网风险监测

[风险总览](#) | [事件中心](#) | [业务管理](#) | [报告管理](#)

湖南润阳医药有限公司

报告列表

报告类型: [全部](#) | [安全事件报告](#) | [云扫描报告](#) | [每日值守报告](#) | [安全运营报告](#) | [重大活动值守报告](#)

[导出报告](#)

序号	报告类型	报告描述	生成时间	操作
1	每日安全播报	每日安全播报20170416	2017-04-16 00:13:22	查看报告
2	每日安全播报	每日安全播报20170415	2017-04-15 00:14:59	查看报告
3	每日安全播报	每日安全播报20170414	2017-04-14 00:15:48	查看报告
4	每日安全播报	每日安全播报20170413	2017-04-13 00:18:33	查看报告
5	每日安全播报	每日安全播报20170412	2017-04-12 00:19:52	查看报告
6	每日安全播报	每日安全播报20170411	2017-04-11 00:21:01	查看报告
7	每日安全播报	每日安全播报20170410	2017-04-10 00:21:38	查看报告
8	每日安全播报	每日安全播报20170409	2017-04-09 00:23:49	查看报告
9	每日安全播报	每日安全播报20170408	2017-04-08 00:23:36	查看报告
10	每日安全播报	每日安全播报20170407	2017-04-07 09:48:27	查看报告

4) 用户域名管理

提供用户安全运营接口，实现用户——渠道——厂商三方快速响应机制，渠道可以根据自己购买的域名授权数给客户提供安全运营。

用户安全		域名管理				
+ 新增域名		监控站点 已配20个/上限20个				
序号	名称	域名	网络状态	域名审核状态	应急处置接入状态	操作
1	-	http://www.test2.com:80	-	审核中	未接入	✎ ✕
2	-	http://www.test1.com:80	-	审核中	未接入	✎ ✕
3	-	http://200.200.88.210:80/#!@\$%^&	-	审核中	未接入	✎ ✕
4	-	http://200.200.88.112#:80/	-	审核中	未接入	✎ ✕
5	-	http://www.test3.com:80	-	审核中	未接入	✎ ✕
6	-	http://www.test4.com:80	-	审核中	未接入	✎ ✕
7	-	http://www.test7.com:80	-	审核中	未接入	✎ ✕
8	-	http://www.test6.com:80	-	审核中	未接入	✎ ✕
9	-	http://www.test5.com:80	-	审核中	未接入	✎ ✕
10	-	http://200.20.88.210:80/test/#test...	-	审核中	未接入	✎ ✕

4 微信公众号

客户关注“深信服安全云”监控服务，右下角“管理”-->“账号管理”绑定云眼账户查收安全评估系统推送的安全事件报告。



4.1 事件通知

