SANGFOR
深信服科技

面向未来，有效保护

网络安全面临的挑战与对策

第十六届民航信息化发展论坛

SANGFOR
深信服科技

1 网络安全面临的挑战

2 面向未来，有效保护

3 持续进化的安全能力

SANGFOR
深信服科技

网络安全面临的挑战

安全威胁快速进化，不断升级

基于业务发展的安全保护思考

SANGFOR
深信服科技

面向未来，有效保护

面向未来、有效保护的安全架构

SANGFOR 深信服科技

智力进化

基于全球情报智能学习的智力进化

安全云脑

安全云守

订阅服务

网

检测

防御

端

智能检测

静态特征

云

东西可视统一策略

南北

技能进化

以防御为核心--》以检测为核心

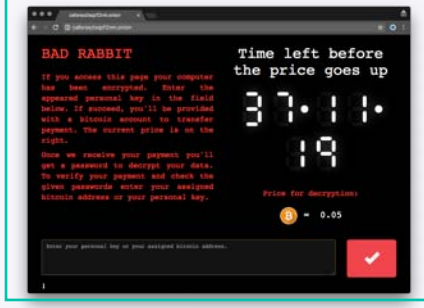
SANGFOR
深信服科技

持续进化的安全能力

本地智能化引擎

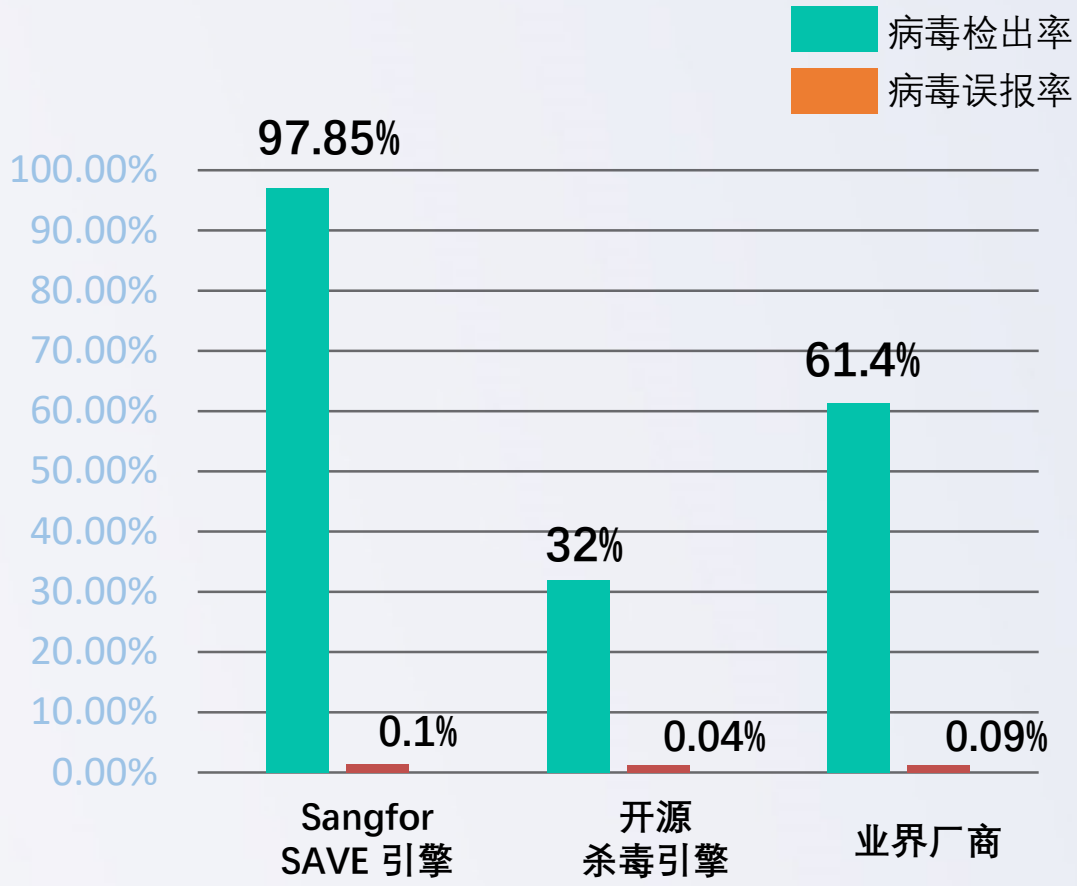
SAVE安全智能检测引擎
Sangfor AI-Based Vanguard Engine

创新**人工智能**无特征技术
准确检测未知病毒/勒索病毒

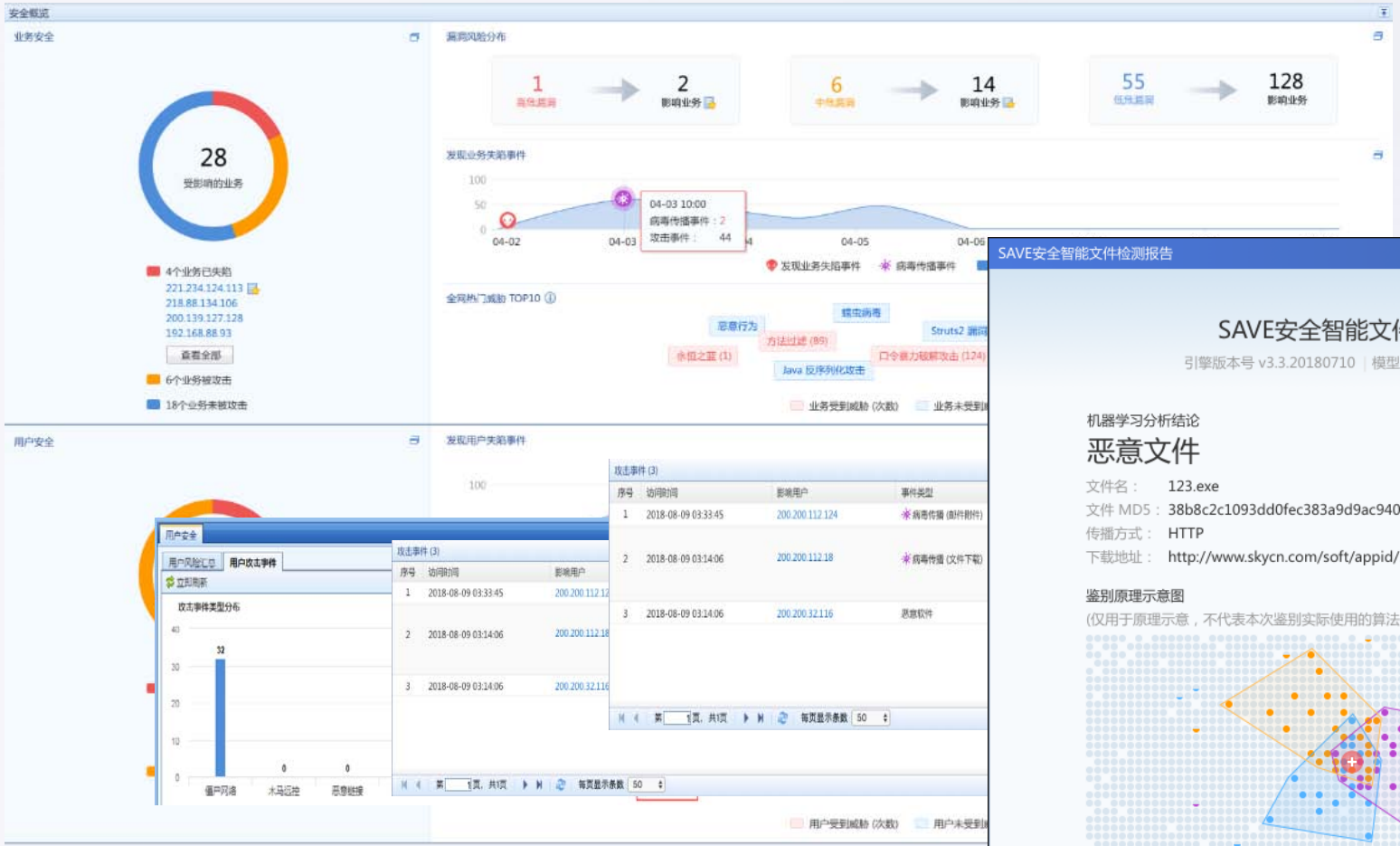


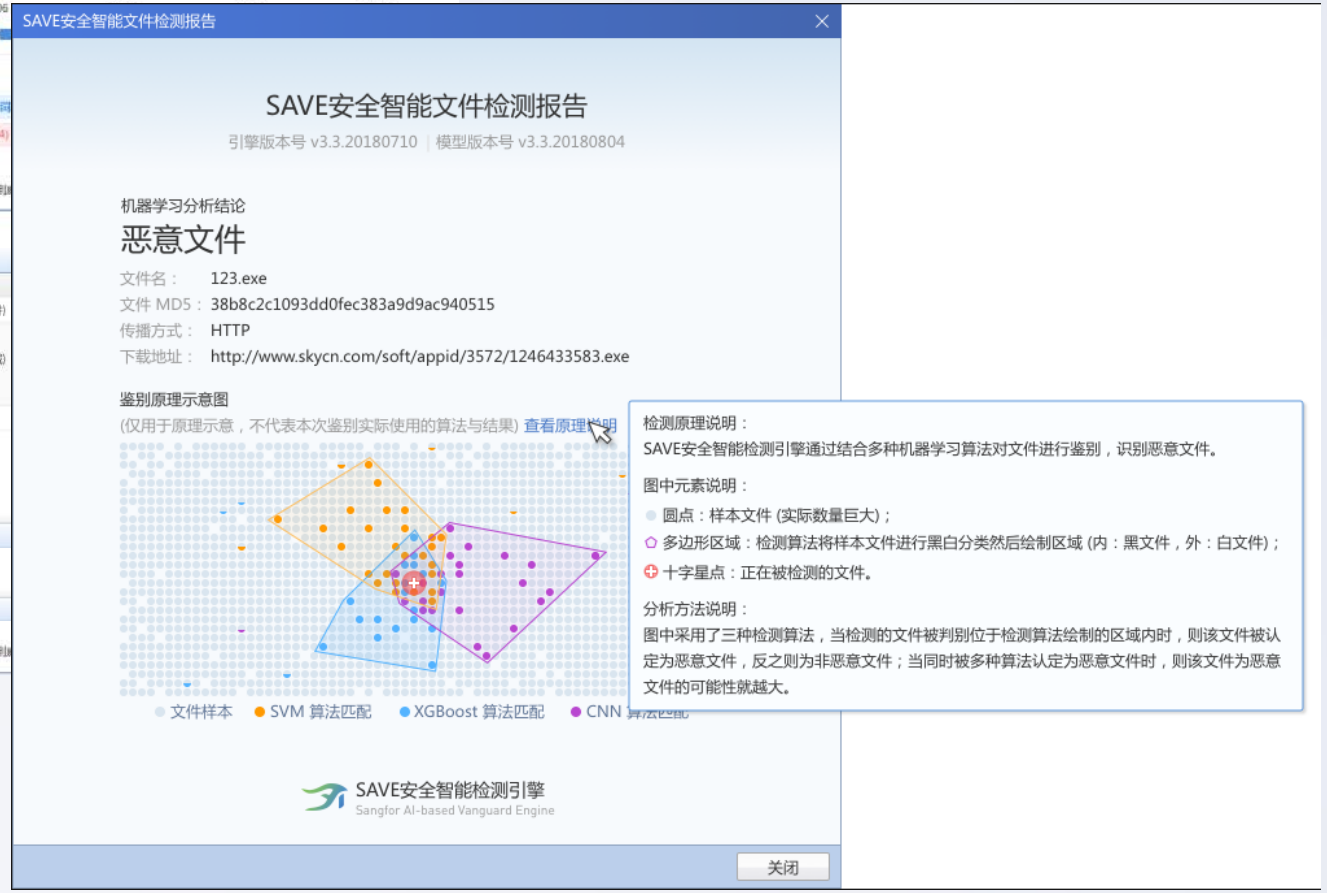
Bad Rabbit
（17年底出现的最新勒索病毒）

查杀成功率**100%**



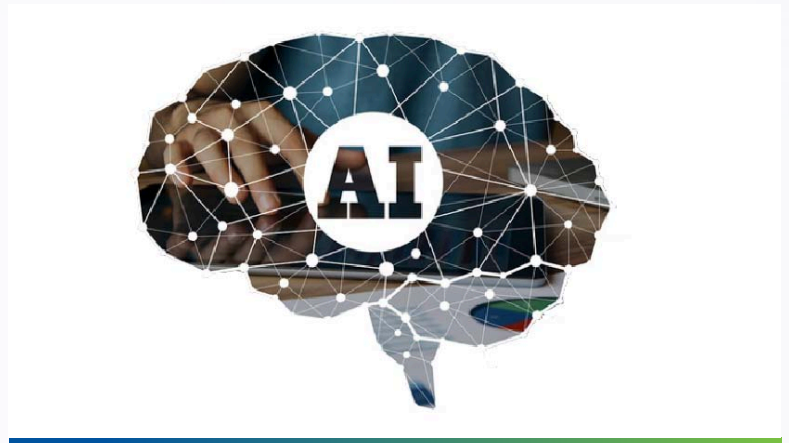
本地智能化引擎


安全概览
业务安全
28
受影响的业务
4个业务已失陷
221.234.124.113
218.88.134.106
200.139.127.128
192.168.88.93
查看全部
6个业务被攻击
18个业务未被攻击
漏洞风险分布
1
2
影响业务
6
14
影响业务
55
128
影响业务
发现业务失陷事件
04-03 10:00
病毒传播事件：2
攻击事件：44
发现业务失陷事件
病毒传播事件
全网热门威胁 TOP10
恶意行为
蠕虫病毒
Struts2 漏洞
方法过滤 (89)
余弦之蓝 (1)
口令暴力破解攻击 (124)
Java 反序列化攻击
业务受到威胁 (次数)
业务未受到威胁
用户安全
发现用户失陷事件
攻击事件 (3)
序号
访问时间
影响用户
事件类型
1 2018-08-09 03:33:45 200.200.112.124 病毒传播 (邮件附件)
2 2018-08-09 03:14:06 200.200.112.18 病毒传播 (文件下载)
3 2018-08-09 03:14:06 200.200.32.116 恶意软件
用户安全
用户风险汇总
用户攻击事件
立即刷新
攻击事件类型分布
僵尸网络
木马远控
恶意链接
每页显示条数 50
用户受到威胁 (次数)
用户未受到威胁


SAVE安全智能文件检测报告
SAVE安全智能文件检测报告
引擎版本号 v3.3.20180710 | 模型版本号 v3.3.20180804
机器学习分析结论
恶意文件
文件名： 123.exe
文件 MD5： 38b8c2c1093dd0fec383a9d9ac940515
传播方式： HTTP
下载地址： http://www.skycn.com/soft/appid/3572/1246433583.exe
鉴别原理示意图
(仅用于原理示意，不代表本次鉴别实际使用的算法与结果) 查看原理说明
文件样本
SVM 算法匹配
XGBoost 算法匹配
CNN 算法匹配
检测原理说明：
SAVE安全智能检测引擎通过结合多种机器学习算法对文件进行鉴别，识别恶意文件。
图中元素说明：
圆点：样本文件 (实际数量巨大)；
多边形区域：检测算法将样本文件进行黑白分类然后绘制区域 (内：黑文件，外：白文件)；
十字星点：正在被检测的文件。
分析方法说明：
图中采用了三种检测算法，当检测的文件被判别位于检测算法绘制的区域内时，则该文件被认定为恶意文件，反之则为非恶意文件；当同时被多种算法认定为恶意文件时，则该文件为恶意文件的可能性就越大。
SAVE安全智能检测引擎
Sangfor AI-based Vanguard Engine
关闭

订阅服务-安全云脑

全球情报中心



智能进化中心

安全赋能中心

订阅服务-安全云脑

SANGFOR 深信服科技

热门威胁10分钟响应

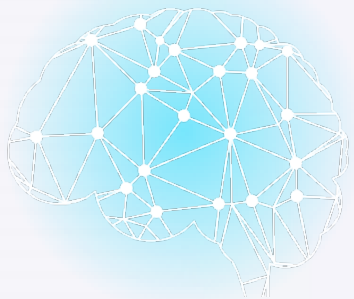
全球热点事件1小时响应

安全能力高频更新

响应速度变快

情报生态

资深数据分析与攻防团队



安全云脑

前瞻的数据架构

情报信誉

云端查杀

云端安全能力赋能

安全规则

云端沙箱

安全能力增强

安全威胁情报

安全规则更新

规则

安全分析能力

未知威胁防护

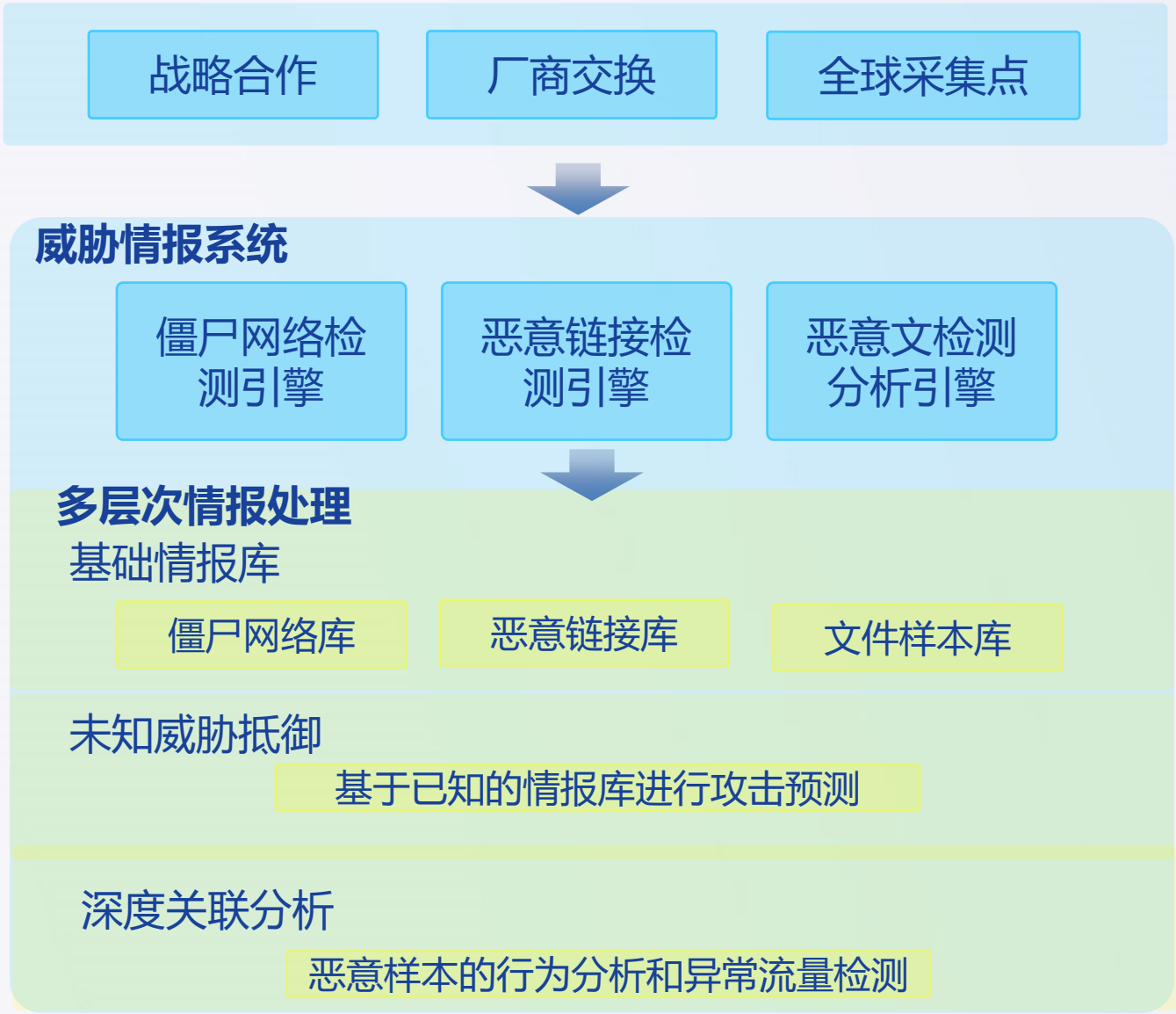
算法

IOC事件库

热门威胁事件库

事件

订阅服务-安全云脑



优质样本来源

- 广泛来源
- 快速采集
- 准确识别
- 攻击预测

订阅服务-云端沙箱

完整支持的沙箱阵列

全面覆盖的样本类型

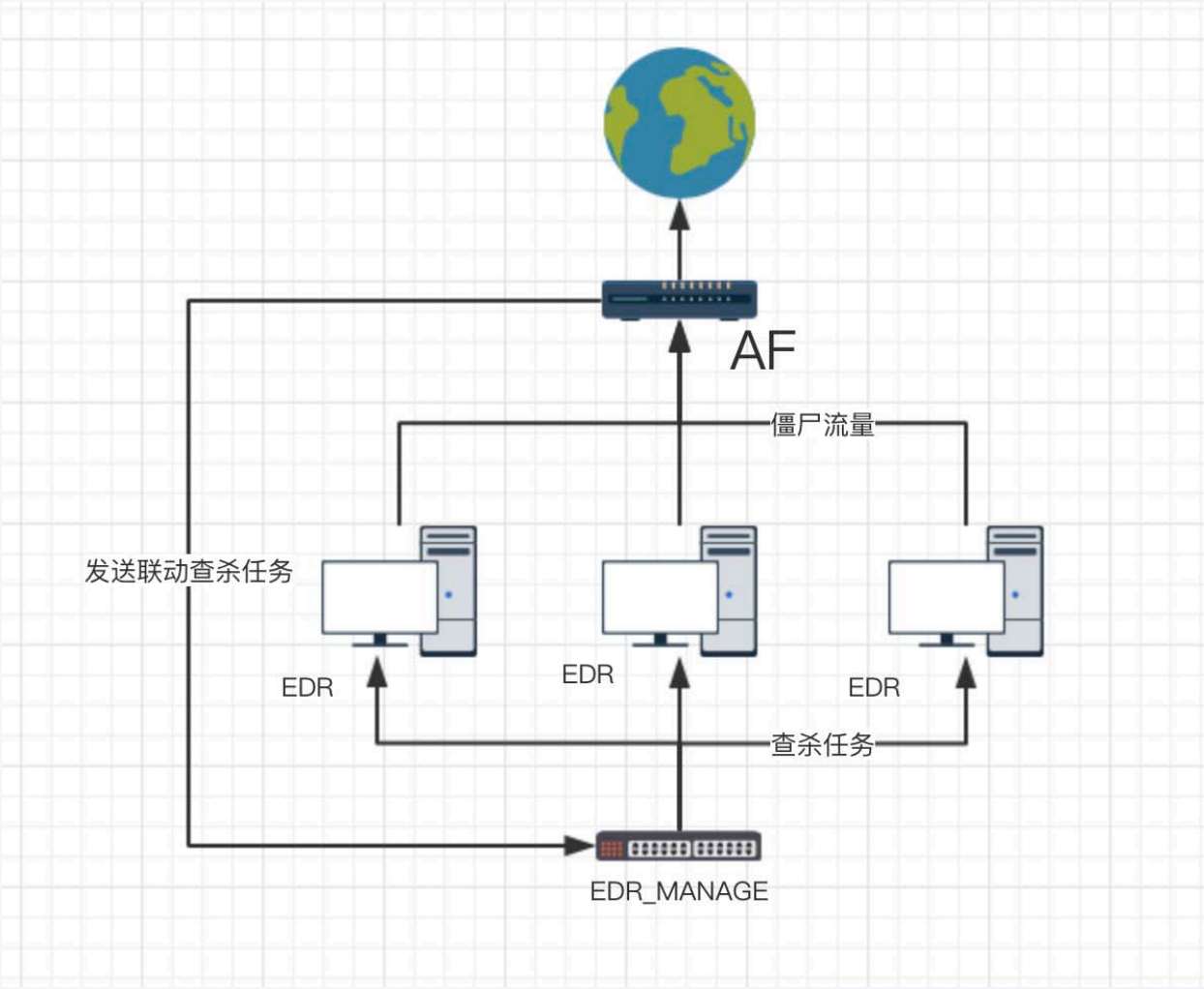
业界领航的沙箱技术

1、反逃逸系统

2、驱动层行为监控

3、完整的进程链追踪

联动



通过网、端、云的方式来提升整体安全能力，通过在企业的不同位置做好安全应对措施来降低来自于不同介入点的风险；

当内网系统中感染了病毒、木马等恶意软件的终端，其病毒、木马试图与外部通信的时候，AF可以基于流量进行行为深度分析，定位失陷主机，同时联动EDR对问题端点进行扫描、取证、查杀。

联动

云端增值服务

通过防火墙 AF 叠加云端增值服务，构建设备和云端深度融合的一体化安全方案；
提供应对外部不断变化的威胁应对方案和用户场景化的需求方案。

如何购买或续费

云端威胁对抗

防火墙联动安全云脑，对未知的威胁进行鉴别，挖掘潜伏的高级威胁，构建应对未知和高级威胁对抗方案。

- 未知威胁鉴别
- 高级威胁分析

进入

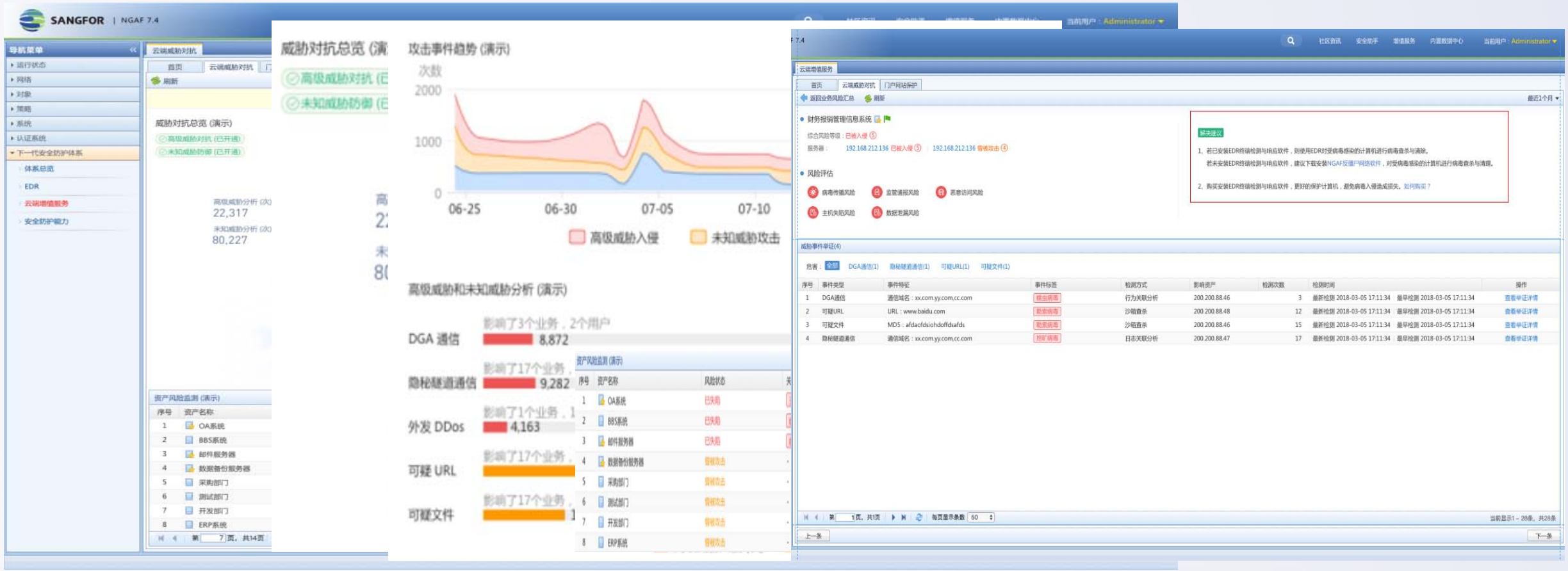
门户网站保护

立体化的网站保护方案：联合终端防篡改保护、边界防火墙篡改检测、云端篡改监测构建网站全方位的立体保护。

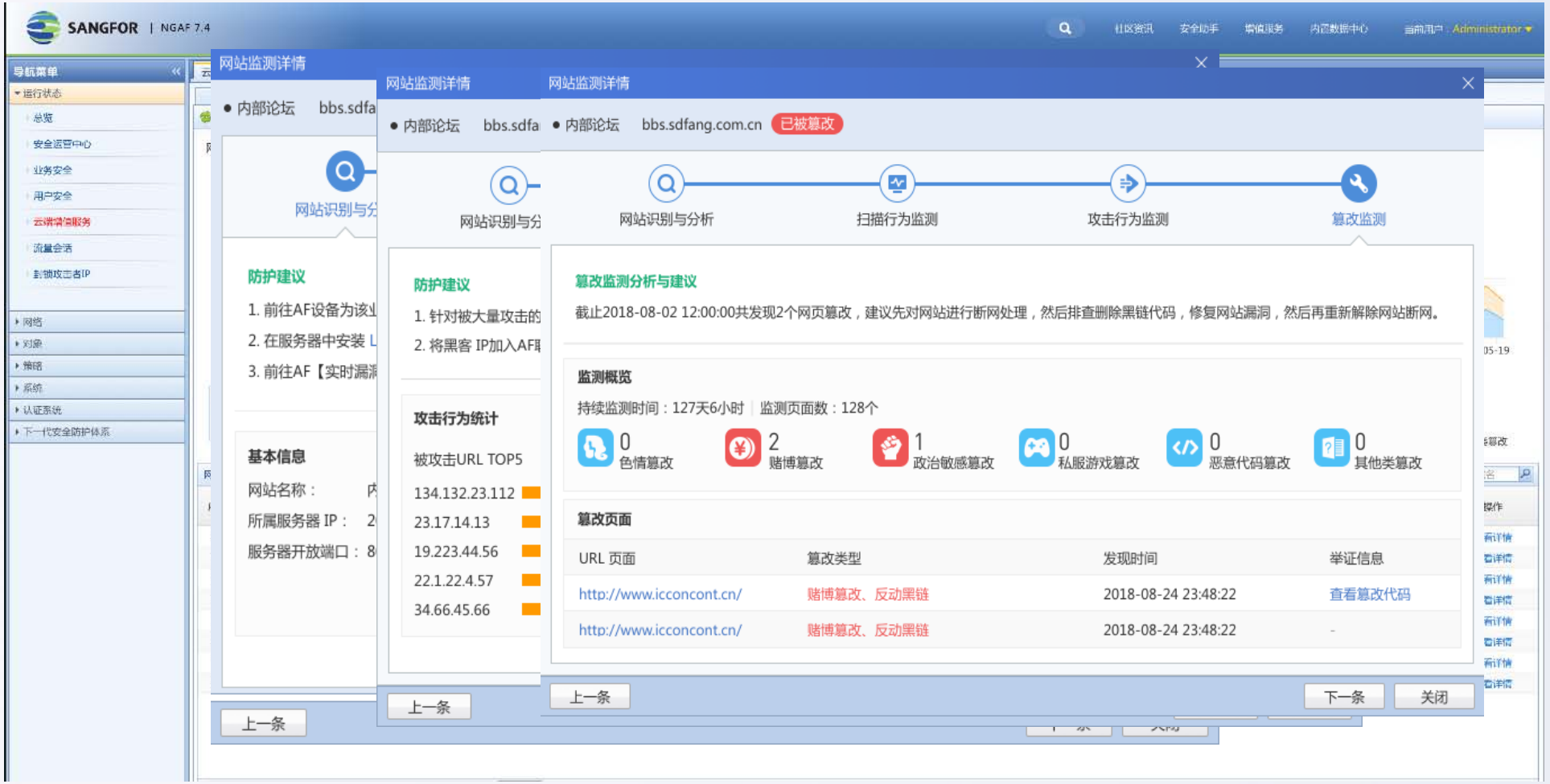
- 网站安全状况监测
- 网站风险监测

进入

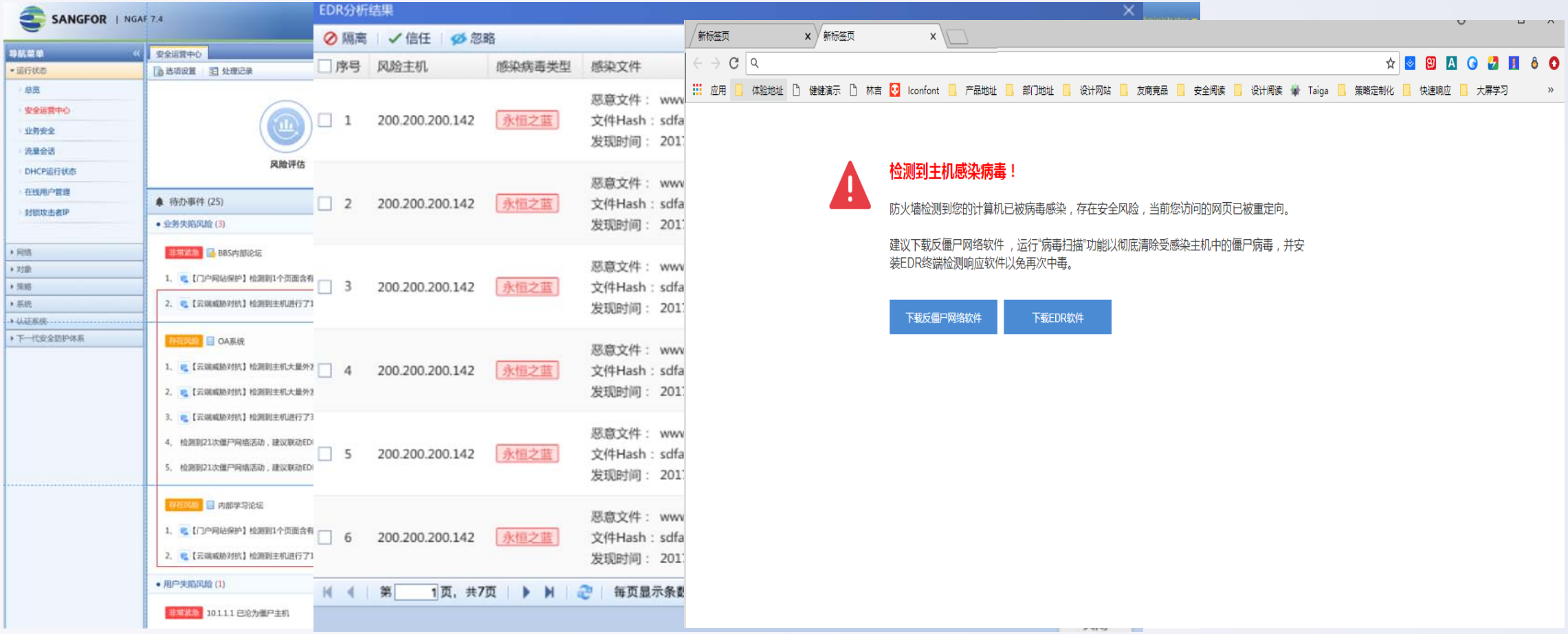
联动


SANGFOR | NGAF 7.4
威胁对抗总览 (演示)
攻击事件趋势 (演示)
高级威胁和未知威胁分析 (演示)
DGA 通信
隐秘隧道通信
外发 DDos
可疑 URL
可疑文件
资产风险监测 (演示)
威胁事件举证(4)

联动


SANGFOR | NGAF 7.4
网站监测详情
内部论坛 bbs.sdfa
网站识别与分
防护建议
1. 前往AF设备为该业
2. 在服务器中安装
3. 前往AF【实时漏洞
基本信息
网站名称：
所属服务器 IP：
服务器开放端口：
上一条
网站监测详情
内部论坛 bbs.sdfa
网站识别与分
防护建议
1. 针对被大量攻击的
2. 将黑客 IP加入AF
攻击行为统计
被攻击URL TOP5
134.132.23.112
23.17.14.13
19.223.44.56
22.1.22.4.57
34.66.45.66
上一条
网站监测详情
内部论坛 bbs.sdfang.com.cn 已被篡改
网站识别与分析
扫描行为监测
攻击行为监测
篡改监测
篡改监测分析与建议
截止2018-08-02 12:00:00共发现2个网页篡改，建议先对网站进行断网处理，然后排查删除黑链代码，修复网站漏洞，然后再重新解除网站断网。
监测概览
持续监测时间：127天6小时 | 监测页面数：128个
0 色情篡改
2 赌博篡改
1 政治敏感篡改
0 私服游戏篡改
0 恶意代码篡改
0 其他类篡改
篡改页面
URL 页面 篡改类型 发现时间 举证信息
http://www.icconcont.cn/ 赌博篡改、反动黑链 2018-08-24 23:48:22 查看篡改代码
http://www.icconcont.cn/ 赌博篡改、反动黑链 2018-08-24 23:48:22 -
上一条
下一条
关闭

联动


SANGFOR
EDR分析结果
隔离
信任
忽略
序号
风险主机
感染病毒类型
感染文件
1 200.200.200.142 永恒之蓝
2 200.200.200.142 永恒之蓝
3 200.200.200.142 永恒之蓝
4 200.200.200.142 永恒之蓝
5 200.200.200.142 永恒之蓝
6 200.200.200.142 永恒之蓝
检测到主机感染病毒！
防火墙检测到您的计算机已被病毒感染，存在安全风险，当前您访问的网页已被重定向。
建议下载反僵尸网络软件，运行"病毒扫描"功能以彻底清除受感染主机中的僵尸病毒，并安装EDR终端检测响应软件以免再次中毒。
下载反僵尸网络软件
下载EDR软件

SANGFOR
深信服科技

THANKYOU

第十六届民航信息化发展论坛