系统最佳实践
--大数据安全

王军旺

SequeMedia 盛拓传媒 IT168.com ChinaUnix.net ITPUB

苏宁易购 suning.com

安全的本质

攻击

防御

时间	攻击源	目标	目的	手段	技术	攻击者画像	

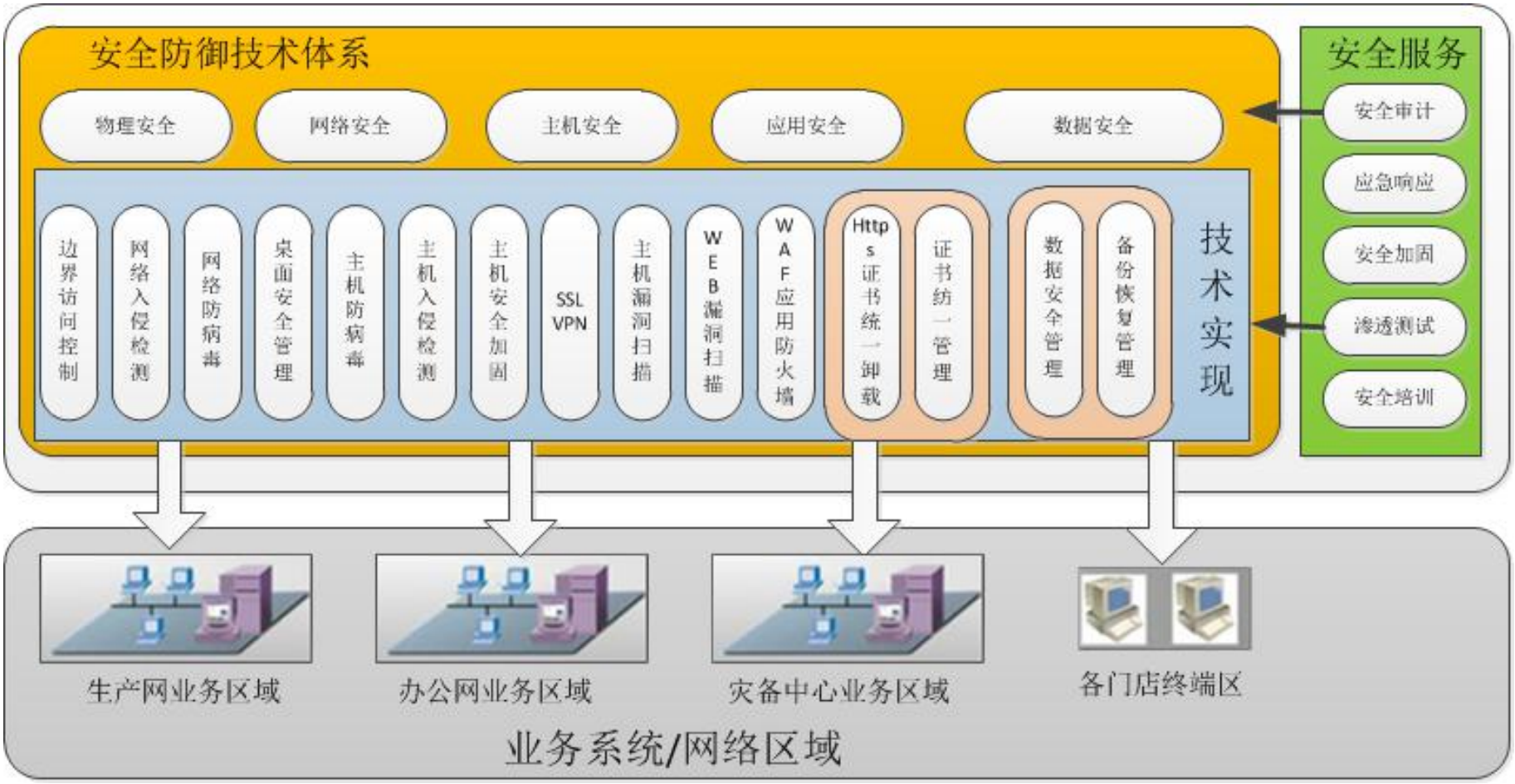
谁在什么时间为了什么目的通过什么手段/技术攻击了哪些资产！

目录

SUNING 苏宁

电商平台的安全防御体系

SUNING 苏宁



电商平台的安全防御体系-技术实现

SUNING 苏宁

网络安全

主机安全

Nessus®

应用安全

arachni

web application security scanner framework

电商平台的安全防御体系-安全服务

SUNING 苏宁

安全事件事前

1 漏洞扫描
-主机、网络漏洞扫描
-WEB漏洞扫描

2 安全加固
-基线加固
-漏洞打补丁
-漏洞修复

3 渗透测试
-WEB渗透测试（依据owasp top10进行测试）
-移动端渗透测试
-输出渗透测试报告

4 安全培训
-SDL开发流程培训

安全事件事中

1 安全监控
-WAF拦截告警
-网络流量监控
-安全状态监控

2入侵拦截及告警
-NIDS拦截告警
-HIDS拦截告警

3 应急响应
-白帽子提交漏洞的修复
-突发安全事件应急处理
-高危漏洞的修复

安全事件事后

1事件溯源
-突发安全事件应急处理
-输出故障分析报告
-日志关联分析，及潜在风险的排除

2 日志审计
-SSLVPN访问日志审计
-数据库访问日志审计
-输出审计异常报告

电商平台的安全体系建设可谓相当完善，但安全问题是否得到解决，是否可以预防攻击了呢？

答案：NO

目录

某白帽子内网二日游

1 存在未授权访问
2 开放了脚本命令行执行功能
3 Jenkins以root运行

开始攻击

1 创建用户
2 开启ssh隧道

RabbitMQ

redis

：我进来了，你发现了吗？

黑客如何绕过各种防御

SUNING 苏宁

www.suning.com/./../../../../../etc/passwd

VIP

您请求的页面没有找到，但不要着急哦！

控制台 HTML CSS 脚本 DOM 网络 Cookies

清除 保持 所有 HTML CSS JS XHR 图片 Flash 媒体

URL	状态	域	大小	远程 IP	时间线
GET passwd	403 Forbidden	suning.com	39.2 KB	10.19.110.31:8080	

头信息 响应 缓存 HTML Cookies

安全之疼

SUNING 苏宁

1. APT攻击持续存在，检测难度大

SONY

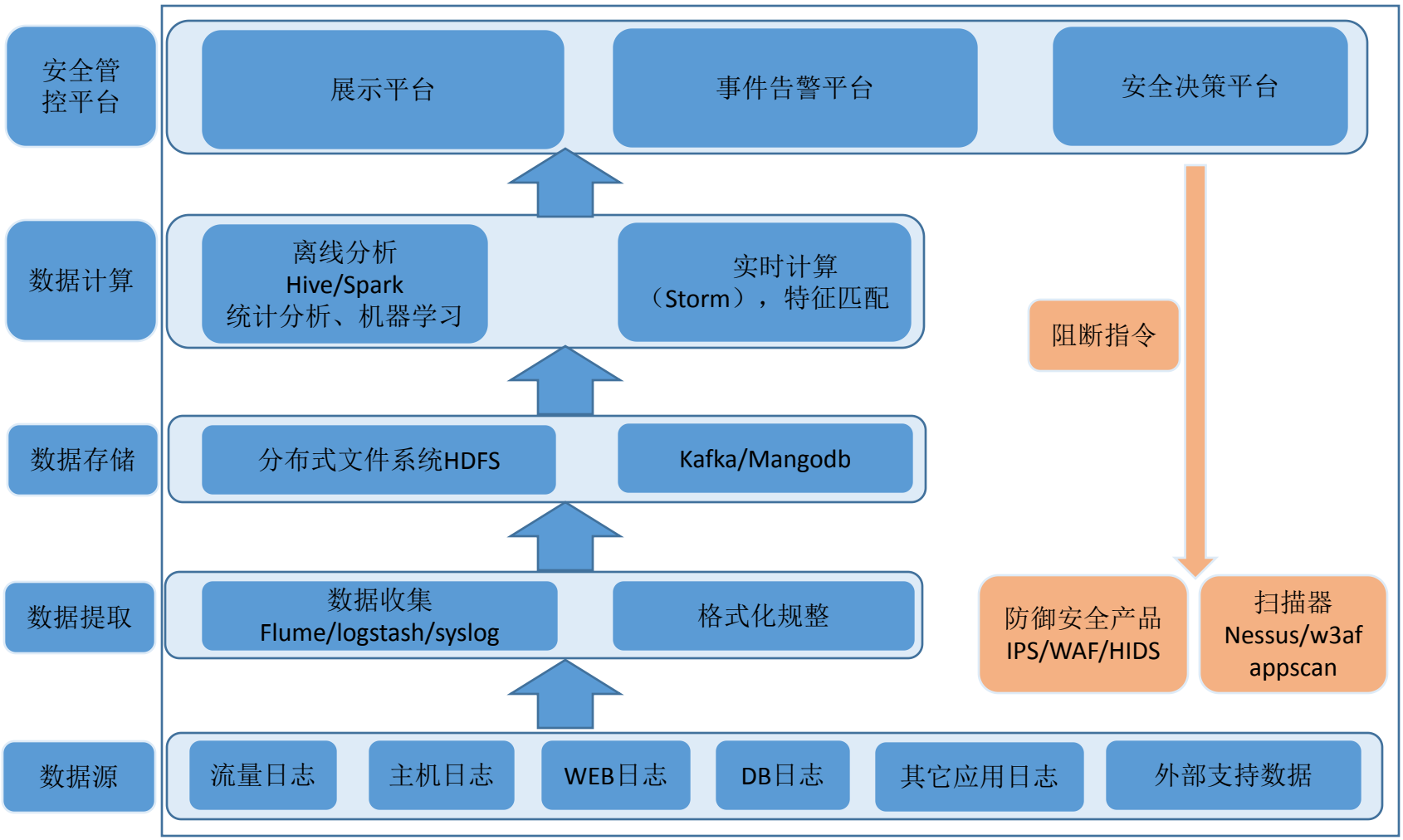
2. 防御体系各系统相互独立，数据互不共享

3. 如何从海量数据中提取有效数据，把攻击者的行为显露于水面，成了亟待解决的问题。

谁在什么时间为了什么目的通过什么手段/技术攻击了哪些资产！

目录

天网平台—系统架构


安全管控平台
展示平台
事件告警平台
安全决策平台
数据计算
离线分析
Hive/Spark
统计分析、机器学习
实时计算
（Storm），特征匹配
阻断指令
数据存储
分布式文件系统HDFS
Kafka/Mangodb
数据提取
数据收集
Flume/logstash/syslog
格式化规整
防御安全产品
IPS/WAF/HIDS
扫描器
Nessus/w3af
appscan
数据源
流量日志
主机日志
WEB日志
DB日志
其它应用日志
外部支持数据

天网平台—数据管理

SUNING 苏宁

数据源抓取、格式化

Nginx Logs

LUA WAF

```
log_format sec_json    '"remote_addr": "$remote_addr", '
                       '"http_x_forwarded_for": "$http_x_forwarded_for", '
                       '"time_iso8601": "$time_iso8601", '
                       '"request_method": "$request_method", '
                       '"document_uri": "$document_uri", '
                       '"uery_string": "$uery_string", '
                       '"server_protocol": "$server_protocol", '
                       '"status": "$status", '
                       '"body_bytes_sent": "$body_bytes_sent", '
                       '"request_time": "$request_time", '
                       '"http_referer": "$http_referer", '
                       '"http_user_agent": "$http_user_agent", '
                       '"http_user_agent": "$http_user_agent", '
                       '"server_addr": "$server_addr", '
                       '"upstream_addr": "$upstream_addr", '
                       '"upstream_response_time": "$upstream_response_time", '
                       'WAF';

access_log /opt/logs/sec_access.log sec_json;
```

天网平台—数据管理

SUNING 苏宁

黑名单库

1 黑名单URL库
-恶意域名库
2 黑名单IP库
-恶意IP库
3 恶意UA库
-黑客工具指纹库
4 WEB攻击特征库
-SQLi、XSS、目录遍历等
5 WEBShell库
-webshell特征库
-webshell密码库

白名单库

1 白名单URL
-白名单域名库
2 白名单IP库
-白名单IP库
3 白名单UA库
-爬虫白名单

社工库

1 黑客特征库
-黑客用户名库
-黑客密码库
2 邮箱、QQ、身份信息
-邮箱社工库
-QQ社工库
-手机、身份证社工库

大数据分析无外乎特征匹配及行为检测。

如何得来，各厂家可是八仙过海，各显神通，或多或少，或真或假！

天网平台—数据分析

SUNING 苏宁

数据分析方法

1. 静态特征匹配

特征正则匹配、基线或阈值匹配

名单库异常匹配等

2. 统计分析

x次登录失败后有一次登录成功

网络上的多台主机遭受同一台主机的攻击或探测

创建非管理员账户之后进行权限提升

VPN用户在工作时间外登录，并向网络之外传输大量数据

从同一个工作站以多个用户名登录

在几分钟内有许多Web 404、401、500和其他web错误码

3、机器学习

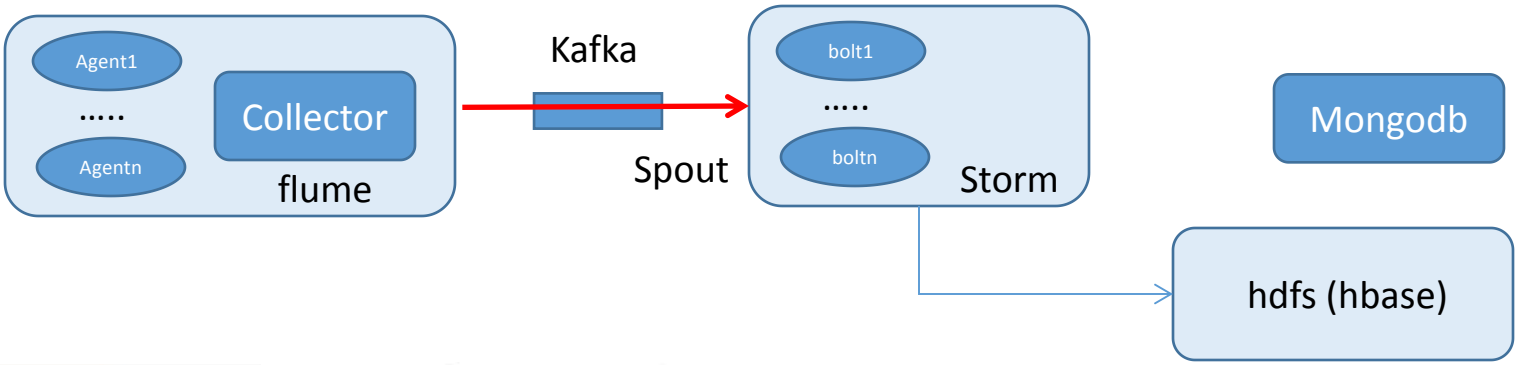
支持向量机SVM

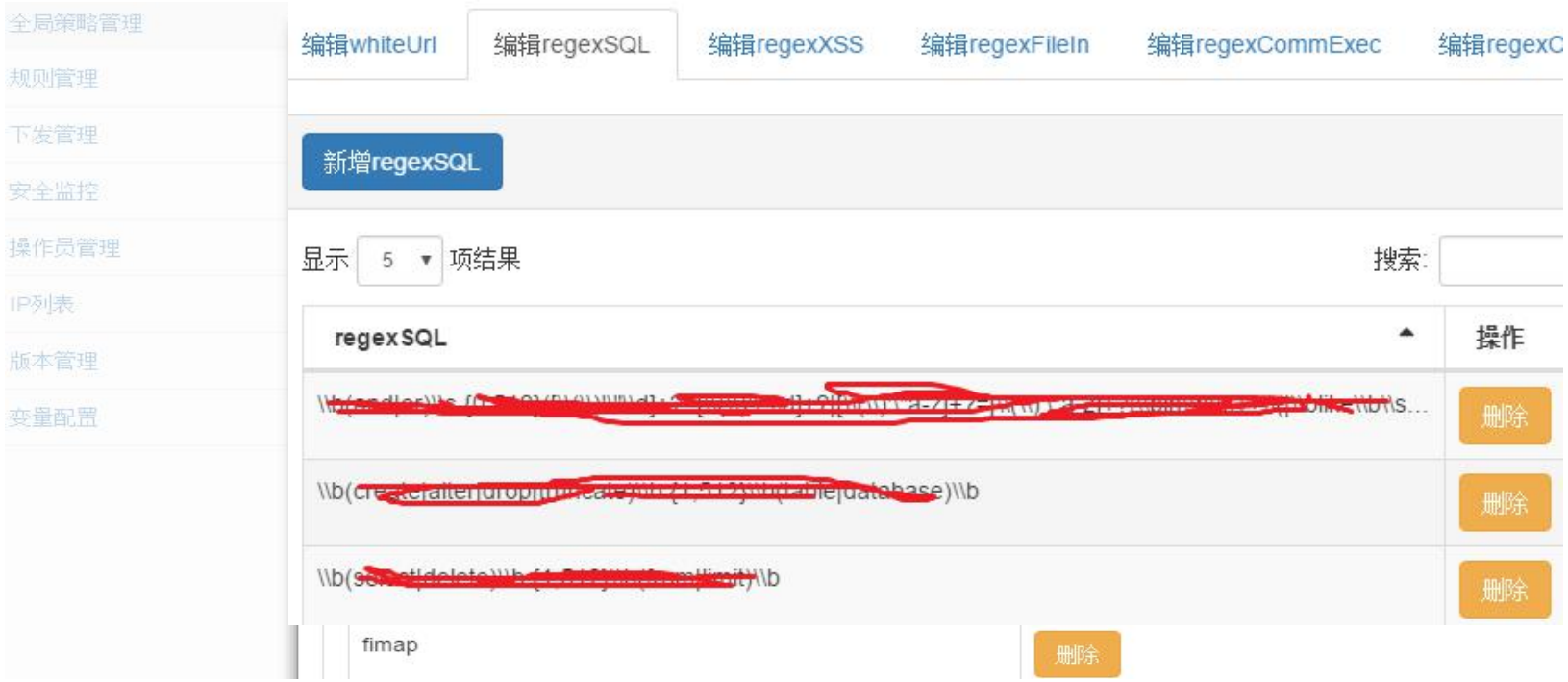
朴素贝叶斯算法

天网平台—数据分析

SUNING 苏宁

实时特征匹配分析法



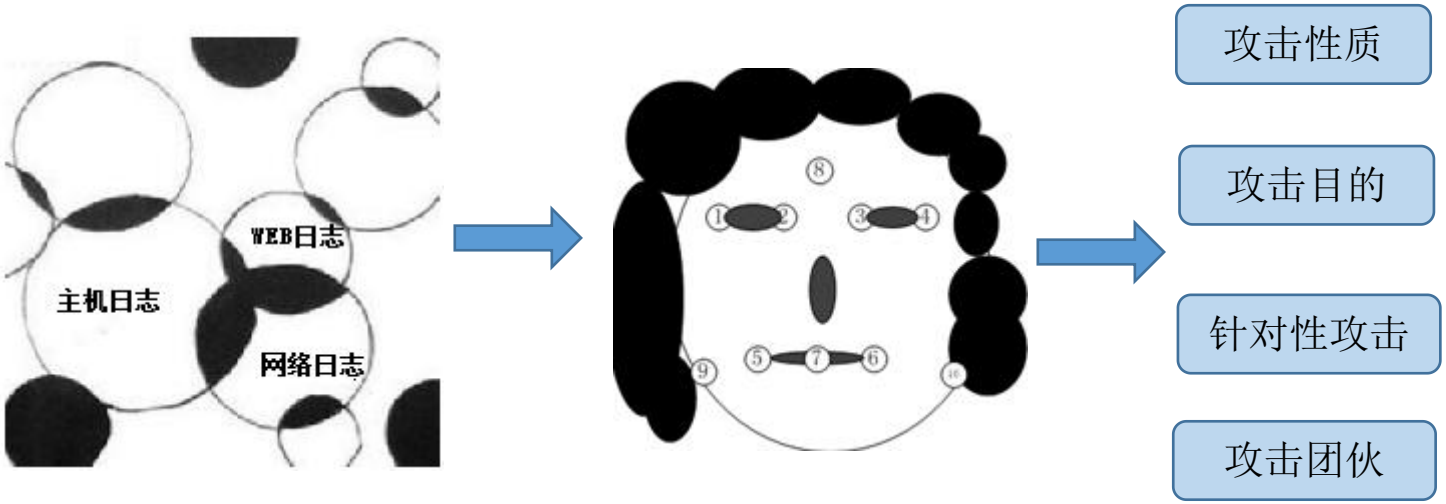


天网平台—数据分析

SUNING 苏宁

行为统计分析法

利用hive的离线批处理功能进行统计分析；

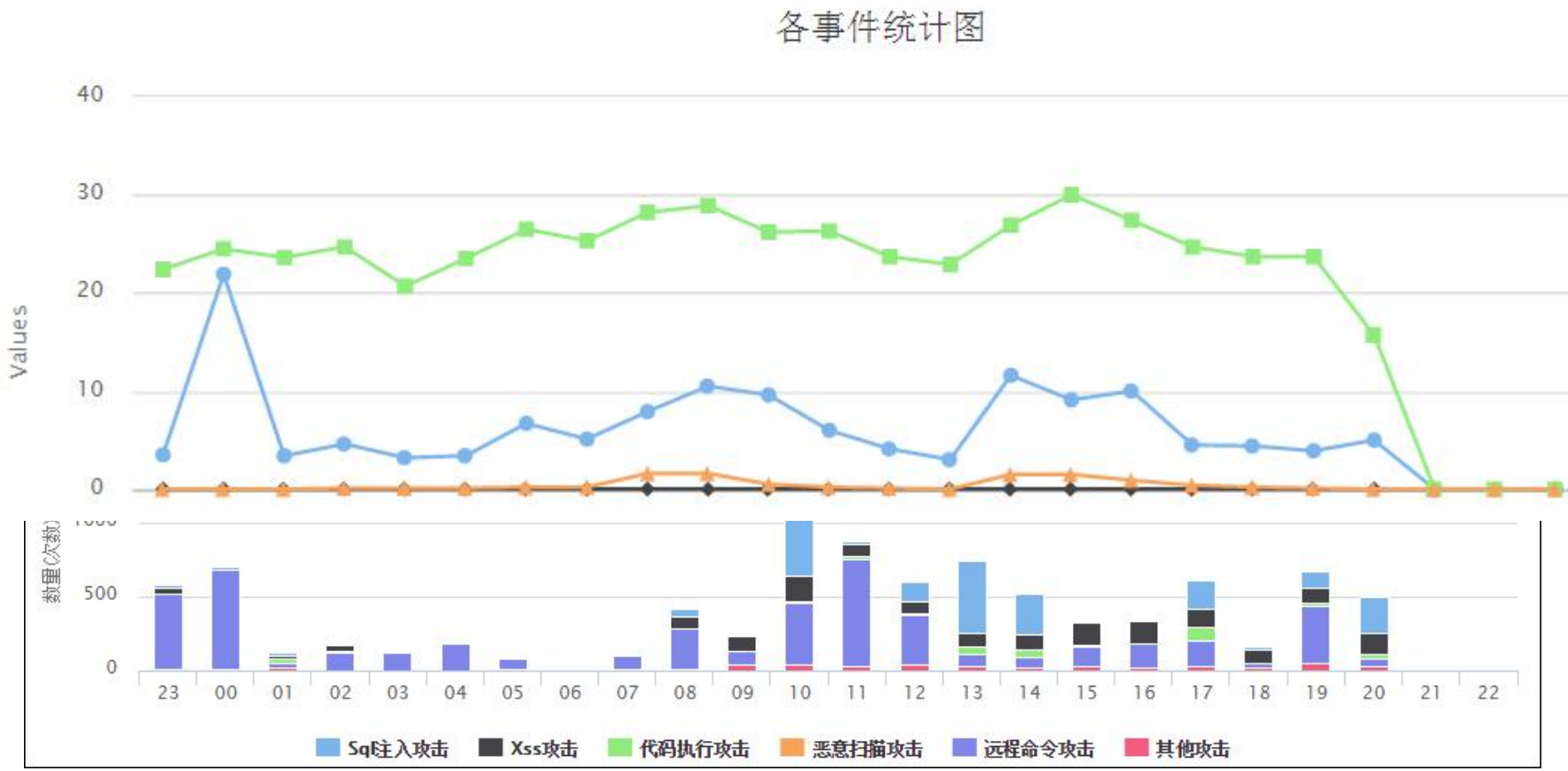


基于黑名单/机器学习发现的异常特征，进行相关联的统计分析，把与特征相关联用户、ip的访问行为进行串联起来；并进行评分，发送不同级别的告警；对于高级别的告警在发送告警的同时向防御产品（IPS、FW、WAF等）发起联动阻断指令。并发动扫描器进行针对性类型的漏洞扫描工单，扫描检测是否存在类似的漏洞。

天网平台—数据展示

SUNING 苏宁

概览



天网平台—告警联动

SUNING 苏宁

可疑IP　已加入黑名单IP

显示 10 项结果　　搜索:

ip	分钟/天	次/分钟	用户数量	服务器数量	页面深度	深度偏差	页面广度	跳转广度	真人度	操作
61.[illegible]	1438	64	1	3	1	0	0	2	10%	移出黑名单
61.[illegible]7	1438	70	1	3	1	0	0	2	10%	移出黑名单
61.[illegible]6	1437	63	1	3	1	0	0	2	10%	移出黑名单
6[illegible]9	1436	65	1	3	1	0	0	2	10%	移出黑名单

可疑IP　已加入黑名单IP

显示 10 项结果　　搜索:

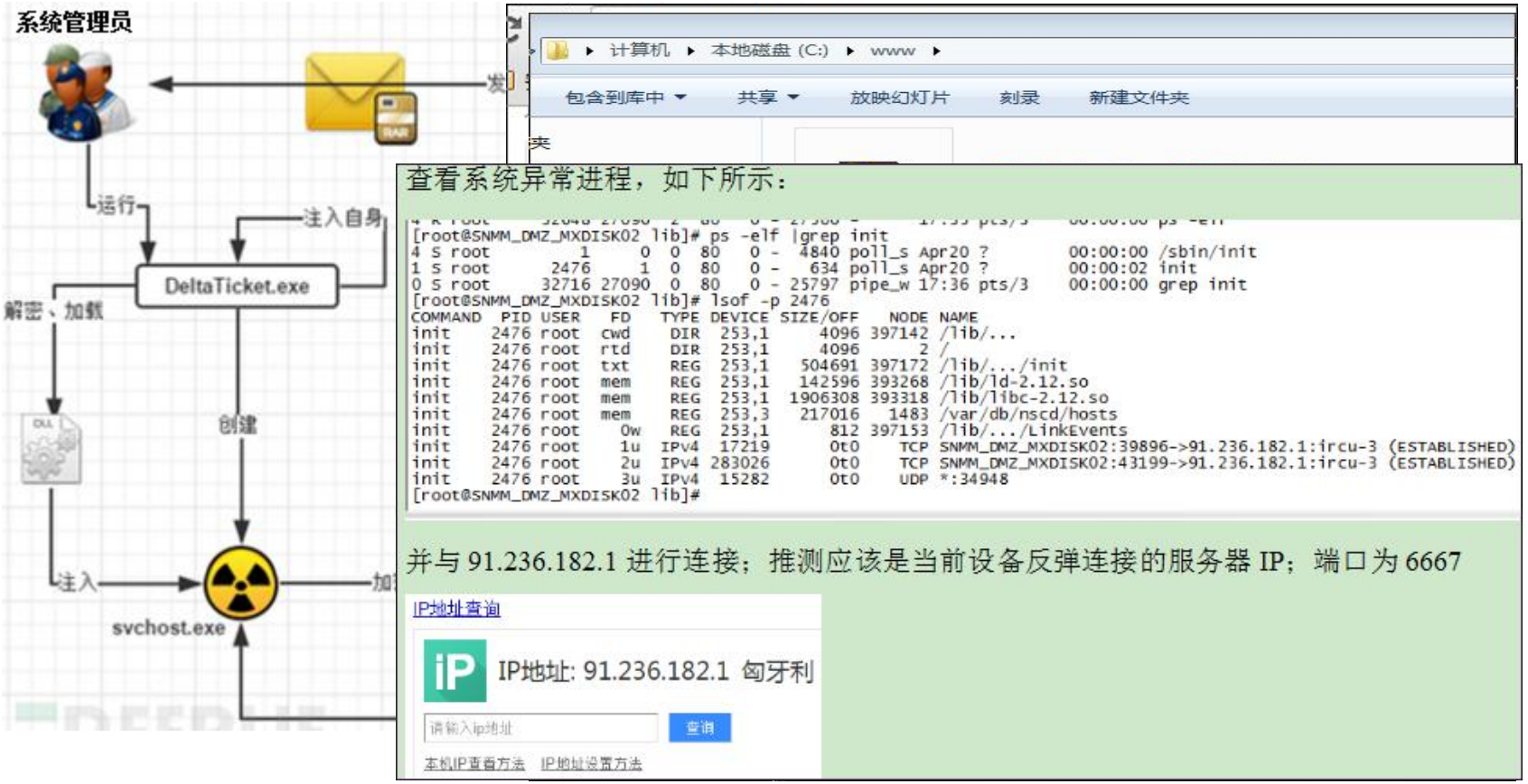
ip	分钟/天	次/分钟	用户数量	服务器数量	页面深度	深度偏差	页面广度	跳转广度	真人度	操作
[illegible]	1440	24	1	1	2.73	0.54	0.81	1	10%	刷黑
10[illegible]	1440	22	1	3	1.48	0.12	10.09	2	10%	刷黑
10[illegible]	1440	147	1	1	4	0	0	1	10%	刷黑

天网平台—案例分析(APT攻击检测模型)

SUNING 苏宁

攻击链模型

1.情报收集 → 2.恶[illegible]码 → 3.投送 → 4.激活 → 5.安装植入 → 6.命令与控制（C&C) → 7.获取



天网平台—案例分析

SUNING 苏宁

APT攻击检测模型

6.命令与控制（C&

7.获取

CC服务器

CC服务器

。 。 。

CC服务器

受害主机

受害主机

特征提取

反向连接特征

1活跃时间点
2响应率
3激活率

心跳特征

1 心跳行为
2 平稳度

异常行为检测

获取行为检测

1 会话信息类指标
2应用分布类指标
3指示位标识类指标
4地址分发指标

目录

SUNING 苏宁

天网平台主动保障系统安全

SUNING 苏宁

天网平台主动保障系统安全

SUNING 苏宁

目录

SUNING 苏宁

大数据安全平台的未来趋势

SUNING 苏宁

1.机器学习更精准，更低的误报率和漏报率。

2.从监督到半监督到无监督，把安全人员从特征提取中尽可能解放出来；

3. 为了提升异常检测结果的准确度，持续分析

THANKS

SequeMedia 盛拓传媒 IT168.com ChinaUnix ITPUB