

# “安全情报与情境感知” 谈大数据分析平台的最后一公里建设



**OWASP 中国**  
The Open Web Application Security Project

# About Me



**OWASP 中国**  
The Open Web Application Security Project



李宗洋

北京 海淀



扫一扫上面的二维码图案，加我微信

李宗洋微信号

[zhuyue@sec-un.org](mailto:zhuyue@sec-un.org)



天融信官方微信

# 大数据安全平台最后一公里 关注点



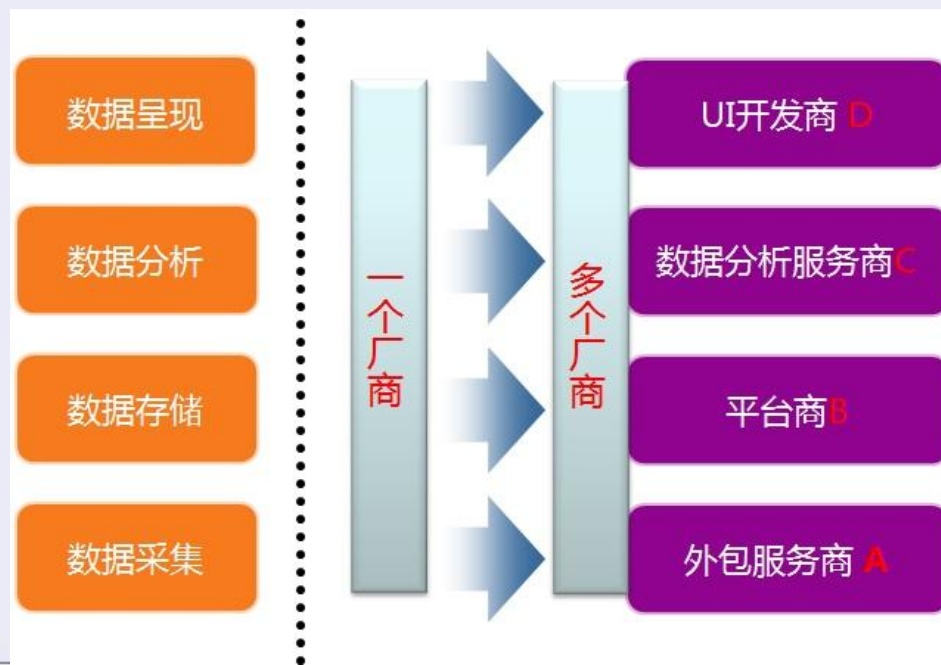
OWASP 中国  
The Open Web Application Security Project

- DT时代的数据价值如何体现
  - 关注:从“平台”到“内容”
  - 数据分析很关键
- 着眼用户需求:
  - 刚需? 显性、隐性?
  - 用户、客户?
  - 紧迫度、频度? 点、面
  - “痛点? 痒点? 兴奋点?”
- 分工更细致

A vision for security detection analytics

	Existing	Emerging	Advanced	Target
Understand	<b>Basic context</b> <ul style="list-style-type: none"><li>Asset, network</li><li>Identity</li></ul>	<b>Advanced context</b> <ul style="list-style-type: none"><li>Application</li><li>Flow &amp; DPI</li></ul>	<b>Technical intelligence</b> <ul style="list-style-type: none"><li>Malware detonation</li><li>IOC identification</li></ul>	<b>Human intelligence</b> <ul style="list-style-type: none"><li>Sentiment analysis</li><li>Motivation</li></ul>
Explore	<b>Ad hoc query</b> <ul style="list-style-type: none"><li>Small dataset</li><li>Basic analysis</li></ul>	<b>Advanced search</b> <ul style="list-style-type: none"><li>Indicator lists</li><li>Pivot search</li></ul>	<b>Analytical query</b> <ul style="list-style-type: none"><li>Big Data management</li><li>Analytical data mart</li></ul>	<b>Visualization</b> <ul style="list-style-type: none"><li>Exploratory data analysis</li></ul>
Explain	<b>Reporting</b> <ul style="list-style-type: none"><li>Threat</li><li>Compliance</li></ul>	<b>Scoring</b> <ul style="list-style-type: none"><li>Risk fidelity</li><li>Profiling</li></ul>	<b>Data mining</b> <ul style="list-style-type: none"><li>Clustering, aggregation</li><li>Affinity grouping</li></ul>	<b>Machine learning</b> <ul style="list-style-type: none"><li>Classification</li><li>Other algorithms</li></ul>
Detect	<b>Real-time</b> <ul style="list-style-type: none"><li>Real-time correlation</li><li>Log aggregation</li></ul>	<b>Historical analysis</b> <ul style="list-style-type: none"><li>Long-term correlation</li><li>Epidemiology</li></ul>	<b>Statistical analysis</b> <ul style="list-style-type: none"><li>Distributed R</li><li>Standard deviation</li></ul>	<b>Behavioral</b> <ul style="list-style-type: none"><li>Insider threat</li><li>Baselining</li></ul>

Depth => Increase in effectiveness





# 大数据平台安全之 “外防+内控”



## 威胁情报(外防)



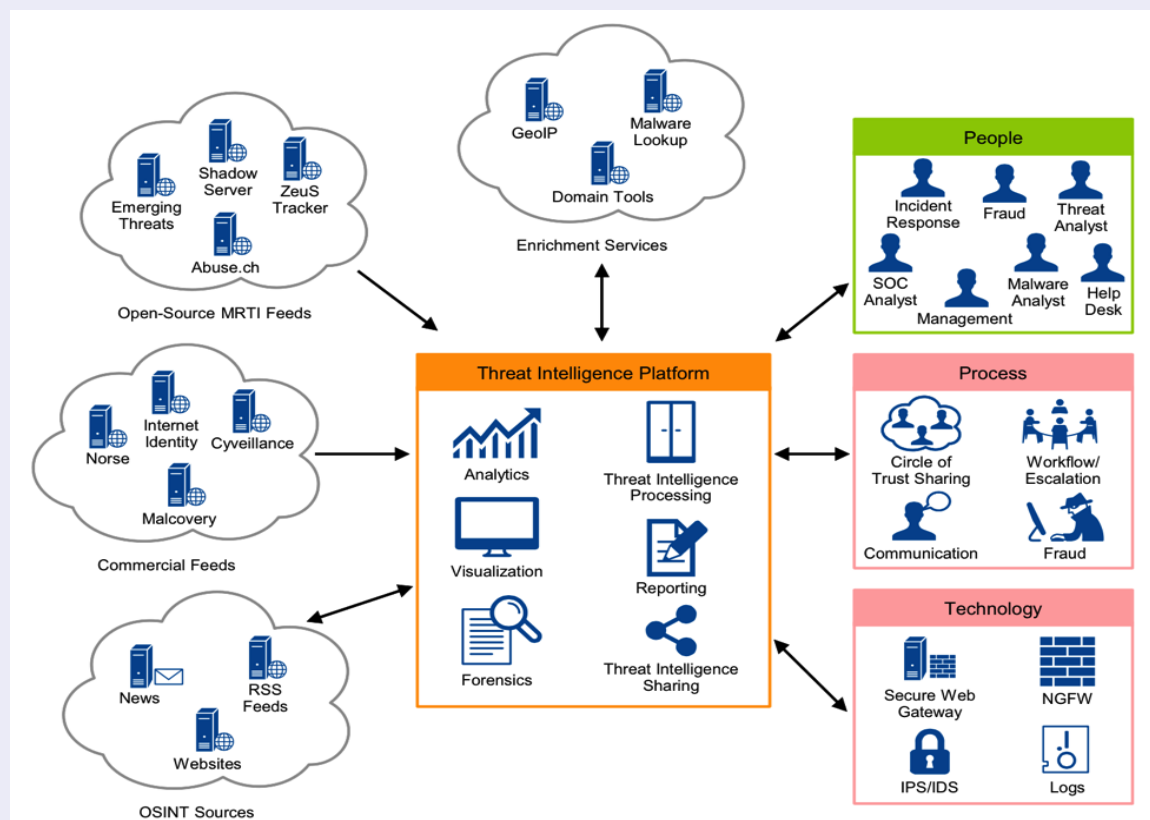
## 情境感知(内控)



# 外防:情报共享驱动 防御体系



在基本信息安全体系不完整, 不具备分析能力的情形下, 安全威胁情报作用十分有限。

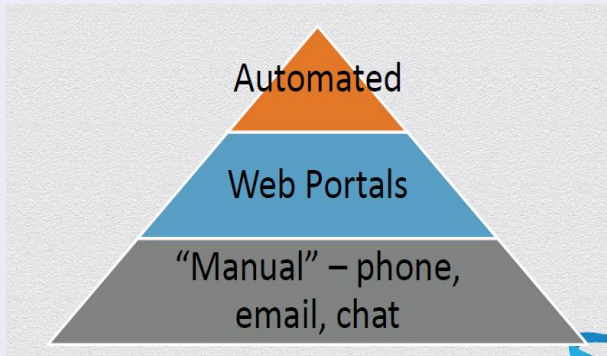


安全情报以“空间”换“时间”，用集体协作来应对“P”，通过情报驱动防御体系的转变

# 外防之：安全情报再分析



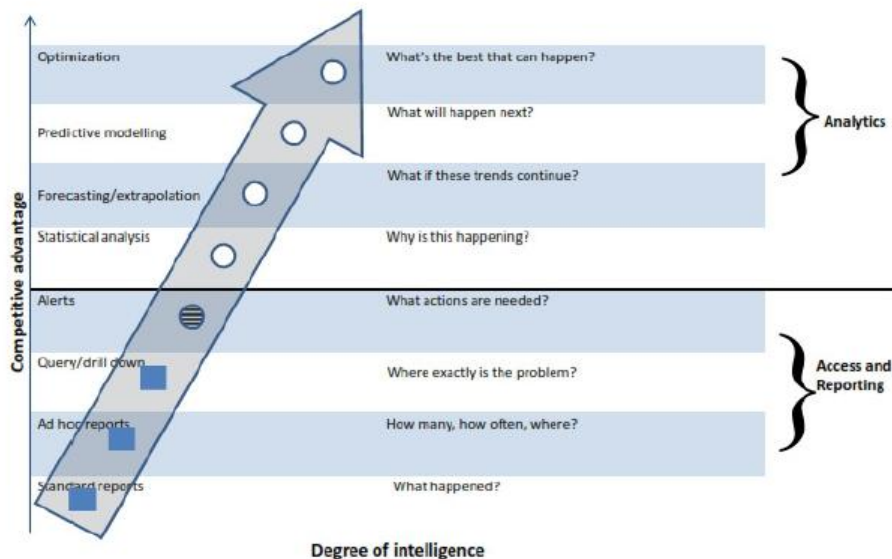
OWASP 中国  
The Open Web Application Security Project



CSV、XML和类似标准格式



DJ的札记



黑客或欺诈团体渗透

品牌监控和保护

社交媒体和开源信息监控

凭据恢复

定向漏洞研究

事故调查

深度、定制的人工分析

钓鱼网站下线

技术指示器升级

欺诈交易纠正和通知

网络行为门户

伪造域名检测

实时事件通知

# 外防：安全情报共享体系实施步骤



**OWASP 中国**  
The Open Web Application Security Project

- 大：专家的介入
- 中：依托外部信息（公有云）
- 小：自成共享体系（私有云）



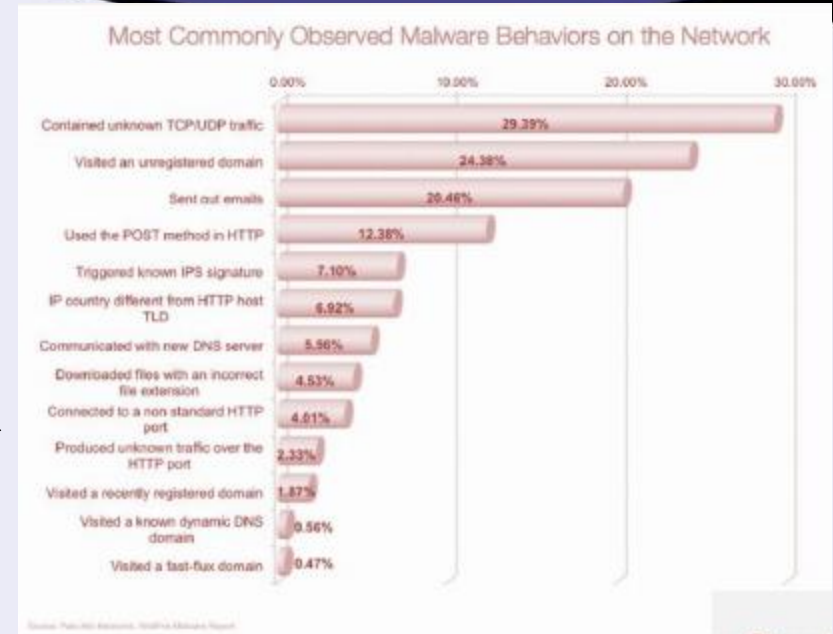




**OWASP 中国**  
The Open Web Application Security Project

1、“如果说”基于特征匹配的检测防范了已知威胁“、基于”虚拟执行的检测阻止了未知恶意代码进入系统内部”，那么对于已经渗透进入系统内部的恶意代码而言，“异常行为检测成为了识别该类威胁的唯一机会”，而机器学习成为了该类问题的首选解决方案。”

**流量和行为终究无法隐藏**



2、



## LEGITIMATE USERS ARE THE MOST COMMON VEHICLE FOR CYBER ATTACK

Adversaries from outside or from the inside collect covert information about the targeted enterprise, learn about its employees and network structure, slowly accumulate privileges by compromising legitimate users, move laterally like legitimate users and exfiltrate the target information in very small doses so as not to arouse suspicion.

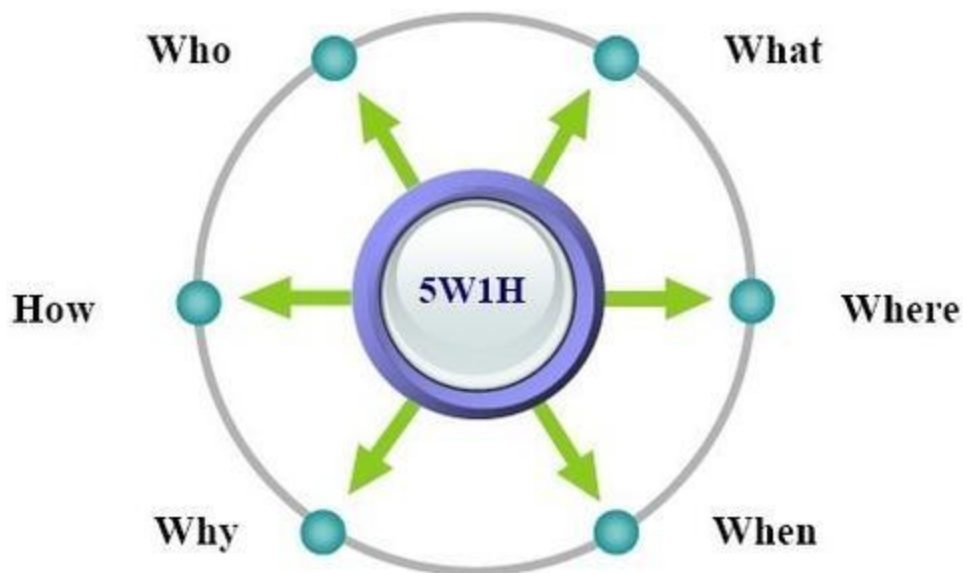
“76% OF NETWORK INTRUSIONS EXPLOITED WEAK OR STOLEN CREDENTIALS OF USERS”  
(VERIZON 2013 DATA BREACH INVESTIGATION REPORT)



# 内控：异常行为分析 模型和方法



**OWASP 中国**  
The Open Web Application Security Project



5W1H 对象	包含信息
WHO	行为执行者，包括自然人姓名，主、从帐号，所属人员组织，所属业务组织。
WHEN	行为发生的时间或时间段。
WHERE	行为发生地点，包括 IP 地址、网段、地域。
WHAT	资源：应用、主机、数据库、网络与安全设备等；对象：数据库表、文件、模块、菜单、配置等。。
WHY	行为操作凭据，主要是指行为操作的工单等依据。
HOW	所执行的行为操作，包括登录、认证、帐号与授权、敏感数据操作、关键操作（增加、删除、修改、查询、下载）等。





## 用户眼中的安全:“业务安全”

- 数据泄露
- 业务违规
- 业务可用性
- .....

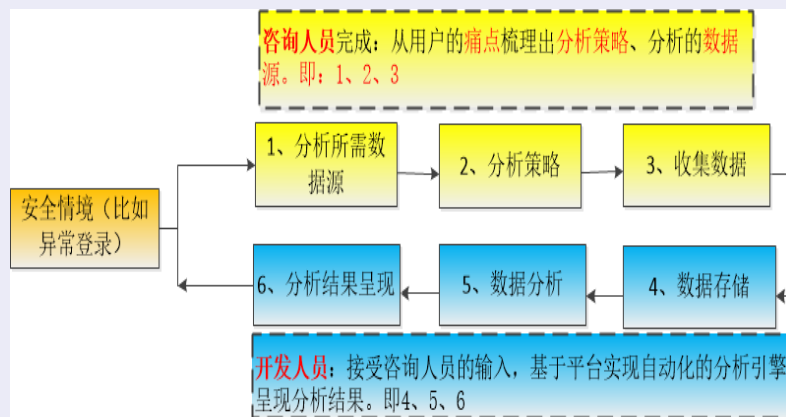
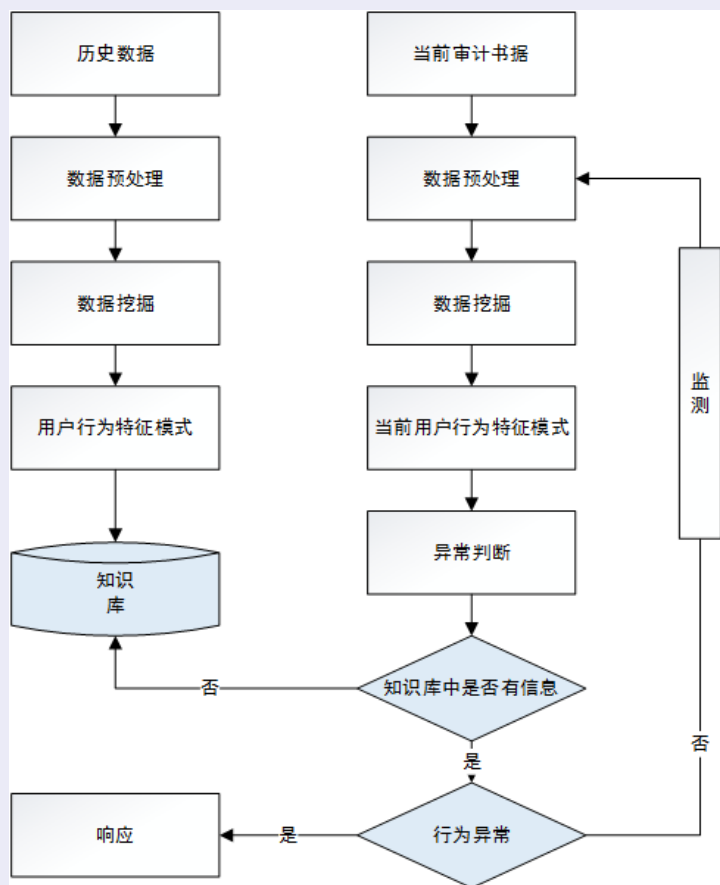


- 取证、溯源:讲究司法上的证据链完整性
- 完整的防护包括防御、检测、回溯分析和预测能力

# 内控：“安全情境”梳理方法



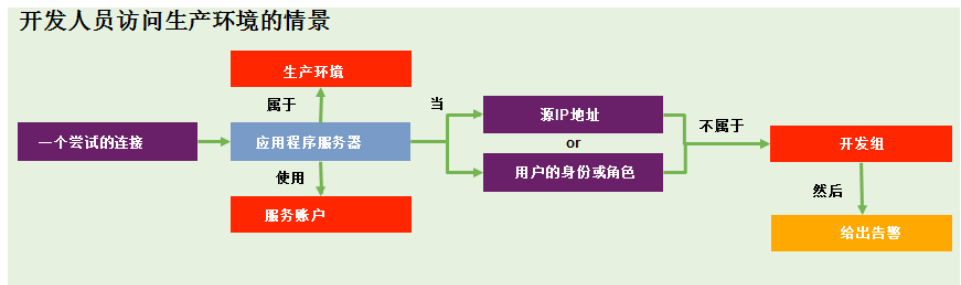
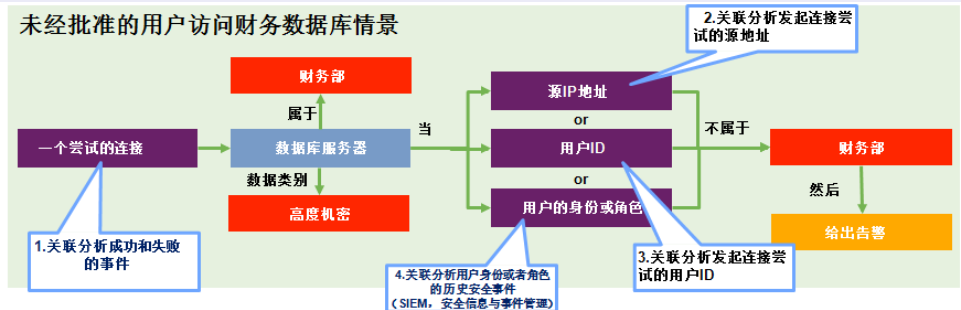
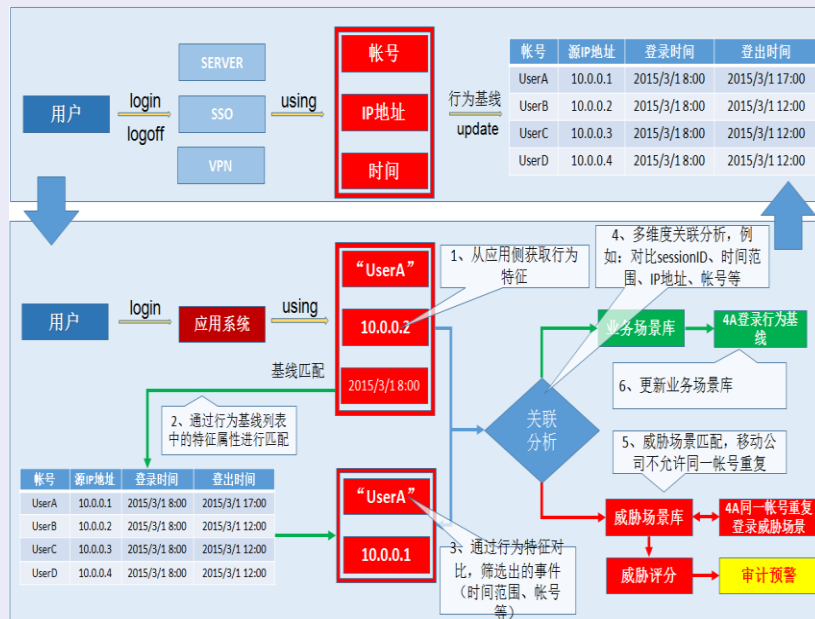
OWASP 中国  
The Open Web Application Security Project







## • 针对人为核心的行为基线建模





- 针对敏感数据为核心的行为基线建模
  - 分布：敏感数据的分布？
  - 访问：基于个体或部门的访问频次
  - 流转：敏感数据的流转范围、时间、有权限的使用者、敏感数据类型、大小等
  - 高危操作：RAR打包、内部服务器的下载操作。



**OWASP 中国**

The Open Web Application Security Project

- 行为基线难以确认
- 海量数据
- 信息采集不完整
- 业务特性的降维



# 内控：行为的量化-黑、白、灰



OWASP 中国  
The Open Web Application Security Project

## 主体 ( who )

主帐号名称	组织结构	主帐号角色	自然人姓名	联系电话
liuyuewen-30080068	河北分公司	普通员工	刘跃文	13931212221
sextzjsongyu-3003938	河北分公司	普通员工	宋晓惠	13931212221
songxiaohui-30000004	河北分公司	普通员工	宋晓惠	13931212221
liqiang-30000019	河北分公司	普通员工	李强	13931212221
lililiang-30083588	河北分公司	普通员工	李连贵	13931212221
zhangshiyong-30062244	河北分公司	普通员工	张世勇	13931212221
liuxin-30000017	河北分公司	普通员工	刘欣	13931212221
caiyuanliang	河北分公司	普通员工	caiyuanliang	13931212221
wusuihua-30000005	河北分公司	普通员工	吴德华	13931212221
hejunqing-30000006	河北分公司	普通员工	梅俊清	13931212221
songxiaohui-30000004	河北分公司	普通员工	宋晓惠	13931212221
gongjili-ls	河北分公司	普通员工	贡吉利	13931212221
fengliang-30000057	河北分公司	普通员工	冯亮	13931212221
fengliang-30000057	河北分公司	普通员工	冯亮	13931212221
jiadongqi-30000018	河北分公司	普通员工	贾东启	13931212221
jijushun-30000724	河北分公司	普通员工	吉雨顺	13931212221
guoxin-agx	河北分公司	普通员工	郭新	13931212221
wuqian-30040061	河北分公司	普通员工	吴倩	13931212221
maxixing-30039959	河北分公司	普通员工	马喜兴	13931212221
yudandan-30039958	河北分公司	普通员工	于丹丹	13931212221
huiqianer-0924	河北分公司	普通员工	金全二	13931212221
sunhongjuan-sa987	河北分公司	普通员工	孙红娟	13931212221
wangxiaona-30000392	河北分公司	普通员工	王晓娜	13931212221
lichunyan-aalcy	河北分公司	普通员工	李春燕	13931212221
liguocao-aalg	河北分公司	普通员工	李国超	13931212221
jiangdong-aajd	河北分公司	普通员工	江东	13931212221
guotong-30038577	河北分公司	普通员工	郭同	13931212221
jiaoyanchi-aajrc	河北分公司	普通员工	焦艳池	13931212221
fenuiqing-atrg	河北分公司	普通员工	樊瑞青	13931212221
chenyuan-acy	河北分公司	普通员工	陈远	13931212221
wangniao-30000278	河北分公司	普通员工	王淼	13931212221
chernia-aachn	河北分公司	普通员工	陈娜	13931212221
gaoliabong-sagxh	河北分公司	普通员工	高小红	13931212221
zhangspining-30039239	河北分公司	普通员工	张培明	13931212221
gaole-30039244	河北分公司	普通员工	高乐	13931212221

## 动作 ( how )

高危操作	操作说明	级别
bootlist	显示并改变可用于系统的引导设备列表	高
bosboot	创建引导映像	高
cfgmgr	通过运行“配置规则”对象类中指定的	高
chdev	更改设备的特征。	高
chfs	更改文件系统的属性。	高
chginet	重新配置因特网实例	高
chgroup	更改组的属性	高
chgrp	更改文件或目录的组所有权	高
chitab	更改 /etc/inittab 文件中的记录。	高
chlv	只更改逻辑卷的特征。	中
chlvcopy	将镜像副本标记为分割镜像或取消将其	中
chmod	更改文件方式。	中
chown	更改与文件关联的所有者或组。	中
chpasswd	为用户更改密码。	中
chps	更改调页空间的属性	中
chpv	更改卷组中的物理卷的特征	中
chvg	设置卷组的特征。	中
exportvg	导出卷组	中
fsck	检查文件系统的一致性并且以交互方式	中
installp	在一个兼容的安装软件包里安装可用的	中

## 客体 ( what )

字段	字段说明
1. PAYACCOUNT_NO	支付账号编号
2. PAYACCOUNT_NAME	支付账号名称
3. PAYACCOUNT_DESC	支付账号描述
4. BALANCE_DATE	记账日期
5. BALANCE_TURN	记账开关
6. CHK_STATUS	记账状态
7. DOWNLOAD_TYPE	下载地址
8. ADDRESS	下载地址
9. PORT	下载端口号
10. PATH	路径
11. USERNAME	用户名
12. PASSWORD	密码
13. VERSION	版本号
14. DATA_PATH	记账数据存放路径
15. DATA_PATH	记账数据存放路径
16. IS_REPLAY	1. 是否回放流程, 2. 是否回放开始记账
17. IS_OUTFILE	手工记账日期
18. DATE	手工记账日期
19. STATUS	手工记账状态
20. BEGIN_DATE	手工记账开始日期
21. FILE_TYPE	ALL所有记账文件, PAY支付记账文件, PMS记账文件
22. PAYING_ID	支付机构编号
23. DEAL_CLASS	记账文件处理类

以网厅es\_pgw\_payaccount配置表为例:

“网厅“配置”敏感关键字库

“特征提取”

关键字 出现频率 敏感特征

用户名 1敏感信息

密码 1用户信息

路径 1敏感信息

开关 4敏感信息

配置属性 5敏感信息

“特征匹配”

敏感特征 命中次数

敏感信息 12

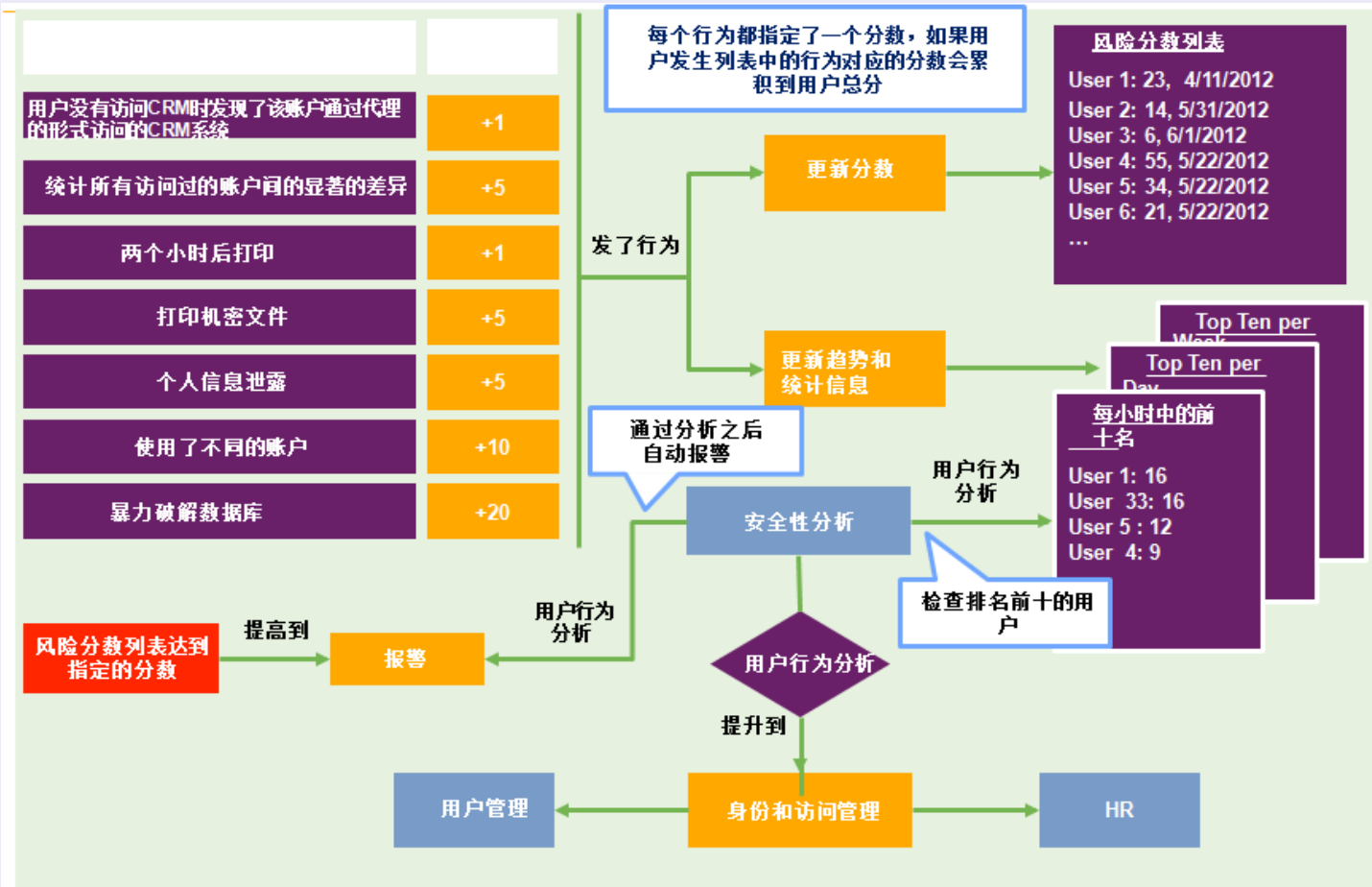
用户属性 1

es\_pgw\_payaccount 为敏感信息表, 可信度权重值为 56.5% (23个字段中有13个字段命中敏感信息即: 13/23=0.565) 存在口令等信息可适当进行加权。

# 内控：行为的量化-聚合



OWASP 中国  
The Open Web Application Security Project



# 内控：行为的量化-聚合



OWASP 中国  
The Open Web Application Security Project

业务情境	风险分值
高危操作	+5
非办公时间高危操作	+10
合作伙伴终端MAC非常规办公区接入	+4
同一帐号多终端登录	+5
核心域内非程序帐号交互	+15
终端域IP直连核心域	+20
只查询不办理	+5
只查询不办理（一小时超过20次）	+20
数据库高危对象操作（增）	+10

操作趋势聚合

客体风险聚合

主体威胁聚合

场景	排名	命中次数
TA	1	1000
TB	2	100
TC	3	10
TD	4	1
TE	5	1

资产	排名	分值/日/月/年
A	1	5133/日
B	2	1102/日
C	3	102/日
D	4	82/日
E	5	12/日

自然人	排名	分值/小时/分
userA	1	1000
userB	2	100
userC	3	111
userD	4	11
userE	5	1



# 内控：异常行为分析产品形态



**OWASP 中国**  
The Open Web Application Security Project



Figure 1: Use the Community Threat Analysis to find devices with the most connections

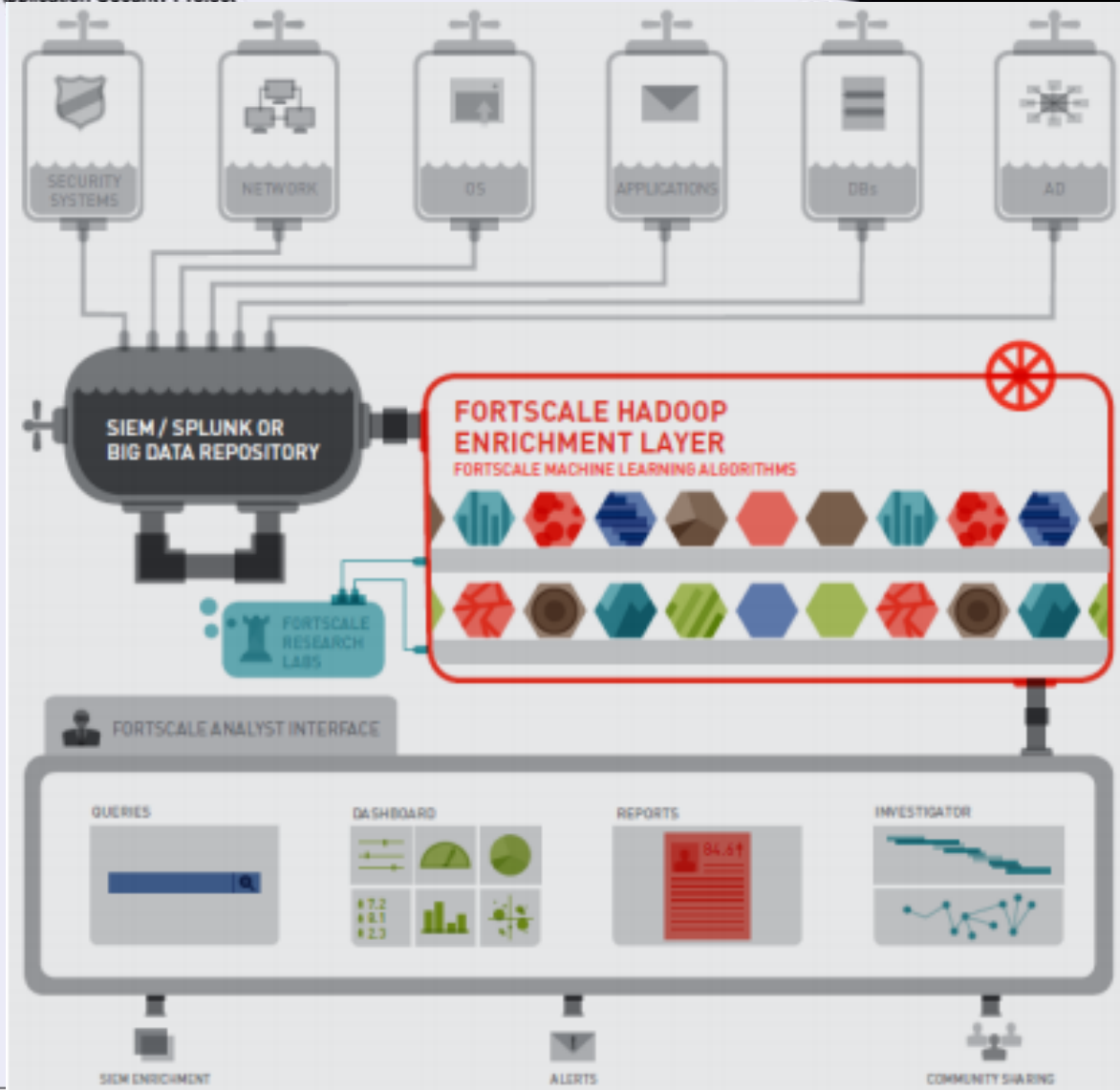


Figure 2: Click the star next to host name to tag the host as a key asset

# 内控：异常行为分析产品形态

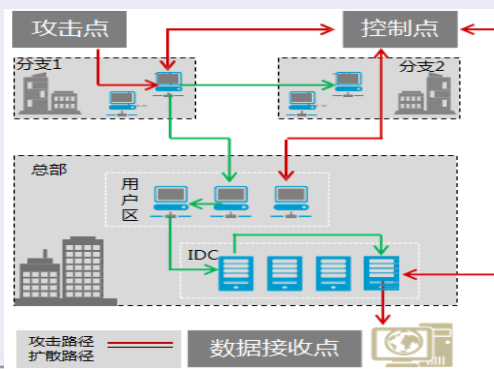


**OWASP 中国**  
The Open Web Application Security Project





- 序列、统计、关联做好的话效果很好。(充分了解用户的业务场景)
- 人工不易确定行为基线、数据量大，预测式的检测需要机器学习。机器学习解决海量的问题。
- 取证、溯源(多点追踪):
  - 从网络访问、系统登陆、应用访问、数据操作的关联;
  - 统一的用户身份认证(IAM)、统一的时间NTP







**可视化**

**云化(业务形态、技术能力)**

**平台化、生态圈、社区化**

**数据化**

**入口---平台&生态---数据--价值**

**安全行业的入口：漏洞、教育、众测、情报、加固、事件处理等。**