“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

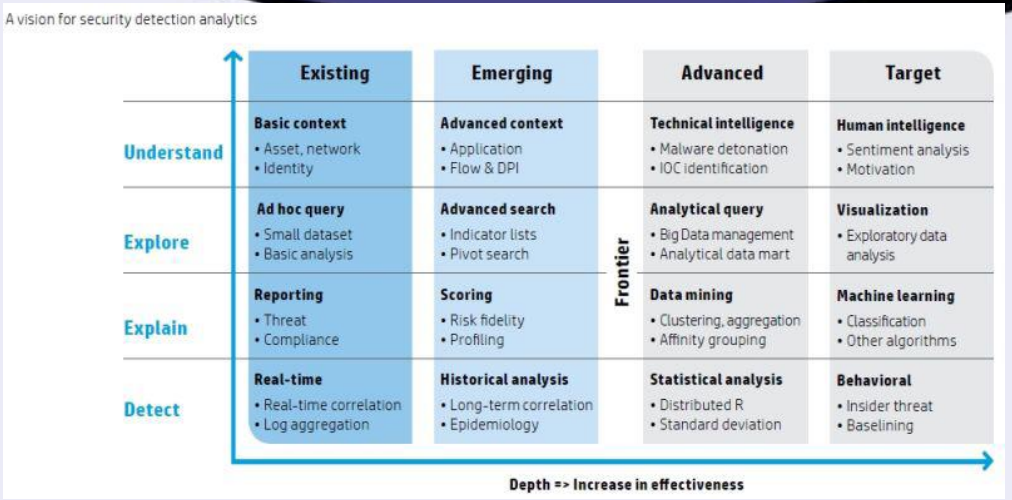
李宗洋微信号

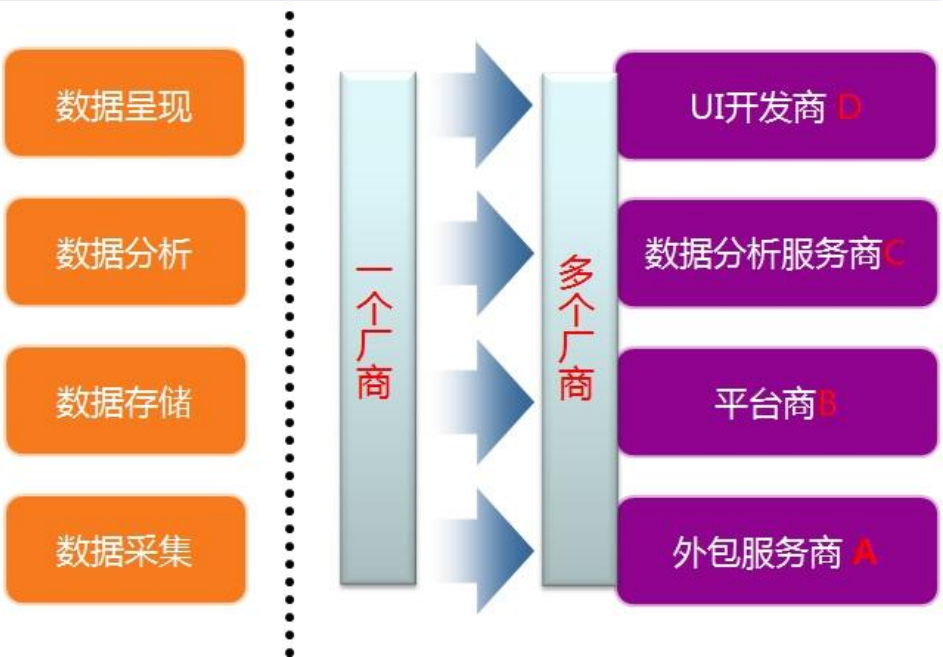
zhuyue@sec-un.org

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





大数据平台安全之“外防+内控”

OWASP 中国
The Open Web Application Security Project

威胁情报（外防）

GLOBAL
Situational
Threat Intelligence

- Reputation
- Interactions
- Applications
- Sites
- ……

情境感知（内控）

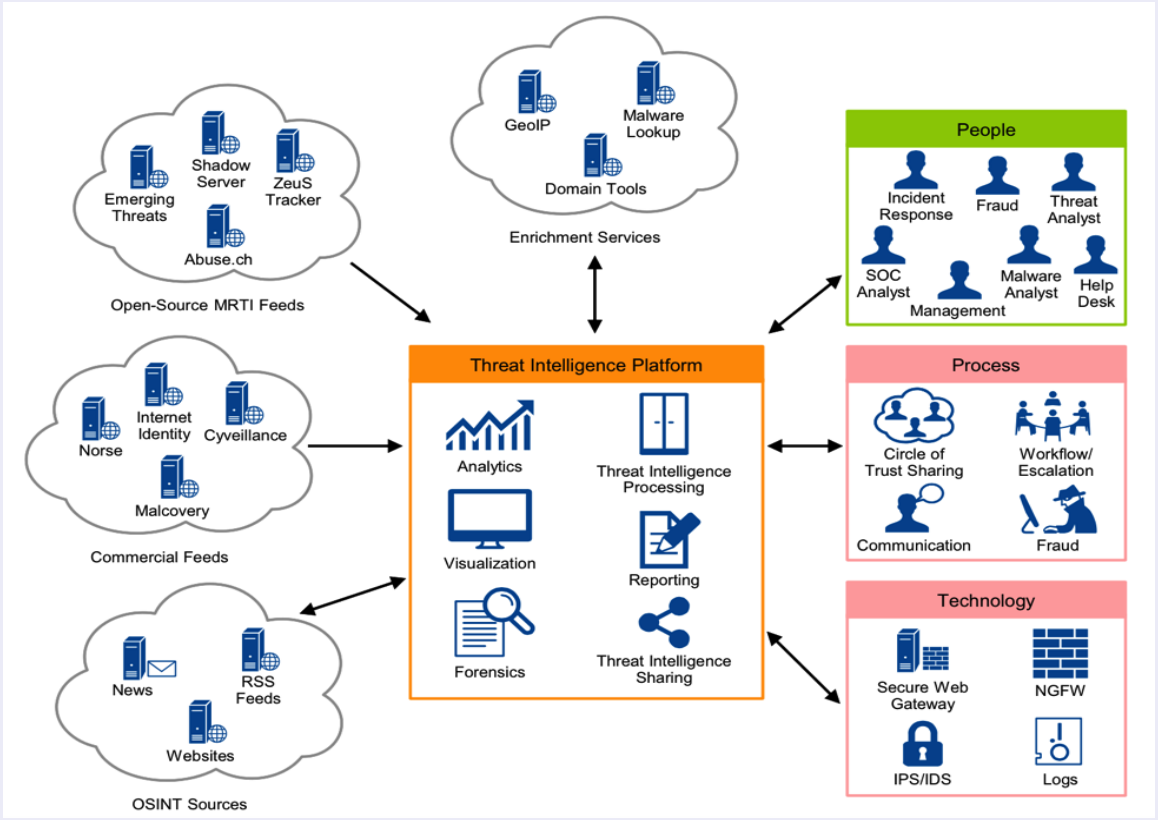
LOCAL
Business Context

- Who
- What
- How
- Where
- When
- why

外防：情报共享驱动防御体系

OWASP 中国
The Open Web Application Security Project

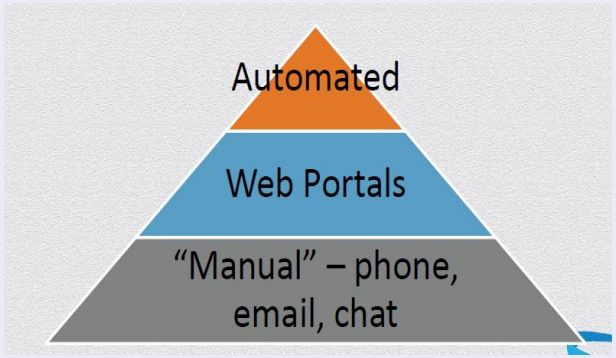
在基本信息安全体系不完整，不具备分析能力的情形下，安全威胁情报作用十分有限。



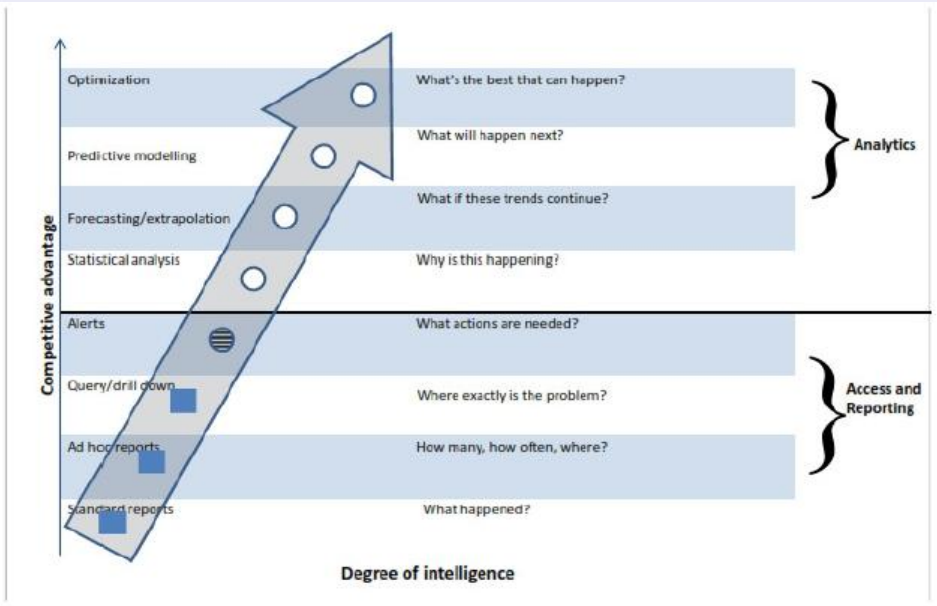
安全情报以“空间”换“时间”，用集体协作来应对“P”，通过情报驱动防御体系的转变

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



- 黑客或欺诈团体渗透
- 社会媒体和开源信息监控
- 定向漏洞研究
- 深度、定制的人工分析
- 技术指示器升级
- 网络行为门户
- 实时事件通知
- 品牌监控和保护
- 凭据恢复
- 事故调查
- 钓鱼网站下线
- 欺诈交易纠正和通知
- 伪造域名检测

外防:安全情报共享体系实施步骤

OWASP 中国
The Open Web Application Security Project

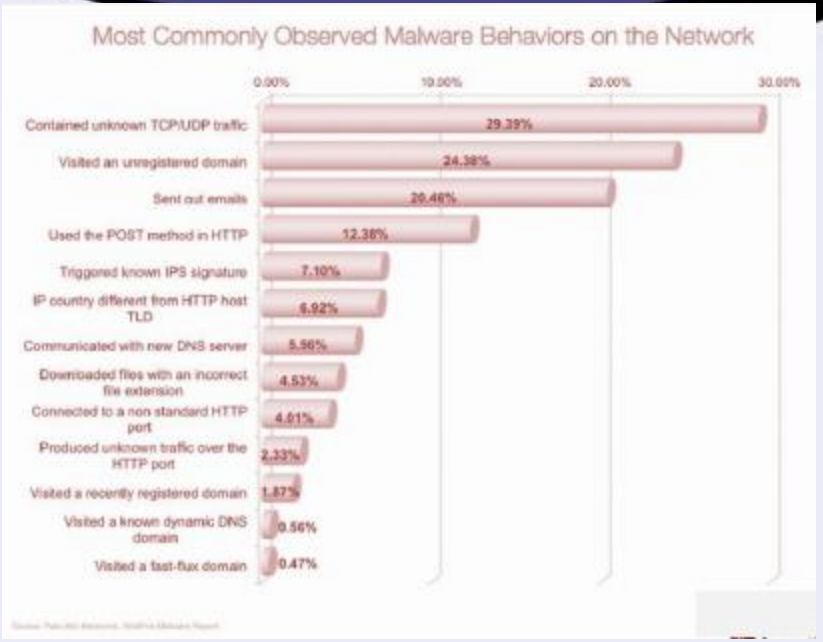
- 大 :专家的介入
- 中:依托外部信息（公有云
- 小:自成共享体系 (私有云)

内控:异常行为检测

OWASP 中国
The Open Web Application Security Project

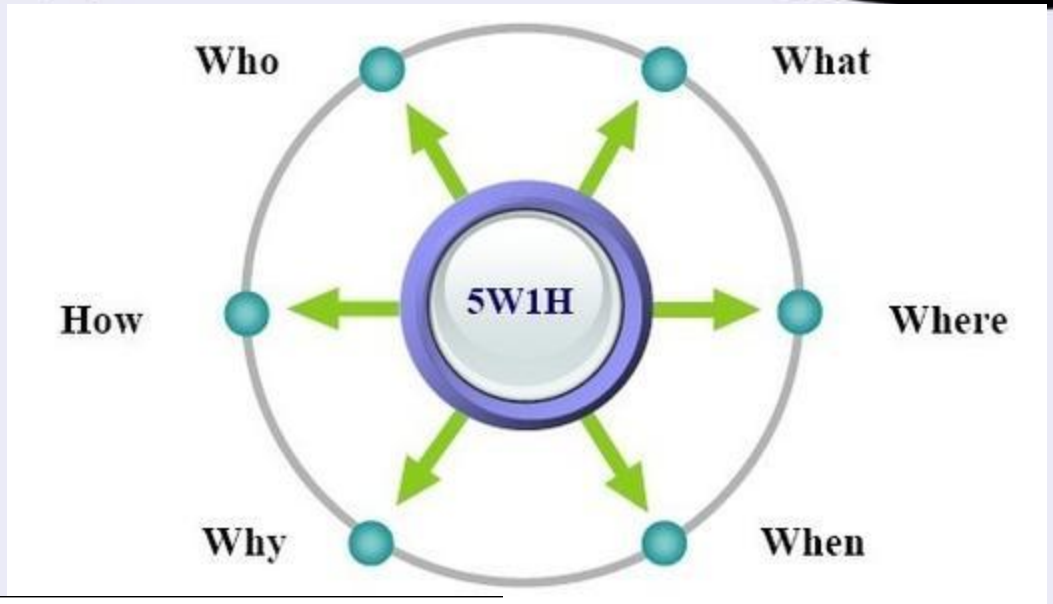
1、“如果说”基于特征匹配的检测防范了已知威胁“、基于”虚拟执行的检测阻止了未知恶意代码进入系统内部”，那么对于已经渗透进入系统内部的恶意代码而言，“异常行为检测成为了识别该类威胁的唯一机会”，*而机器学习成为了该类问题的首选解决方案。”*

流量和行为终究无法隐藏



2、

内控：异常行为分析模型和方法



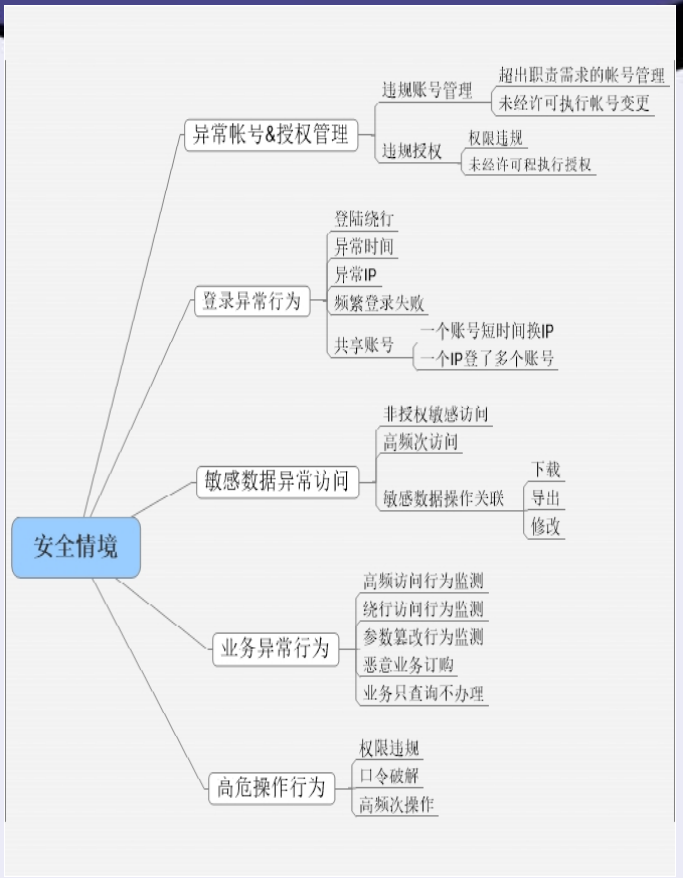
5W1H 对象	包含信息
WHO	行为执行者，包括自然人姓名，主、从帐号，所属人员组织，所属业务组织。
WHEN	行为发生的时间或时间段。
WHERE	行为发生地点，包括 IP 地址、网段、地域。
WHAT	资源：应用、主机、数据库、网络与安全设备等；对象：数据库表、文件、模块、菜单、配置等。。
WHY	行为操作凭据，主要是指行为操作的工单等依据。
HOW	所执行的行为操作，包括登录、认证、帐号与授权、敏感数据操作、关键操作（增加、删除、修改、查询、下载）等。

内控:用户关注点:“安全情境”

OWASP 中国
The Open Web Application Security Project

用户眼中的安全:“业务安全”

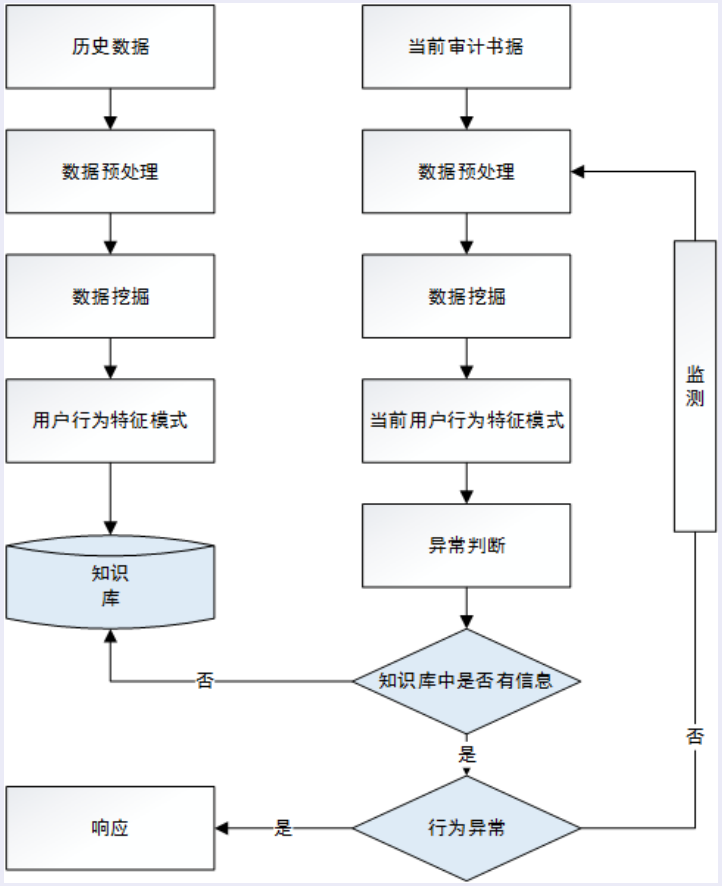
- 数据泄露
- 业务违规
- 业务可用性
- ……

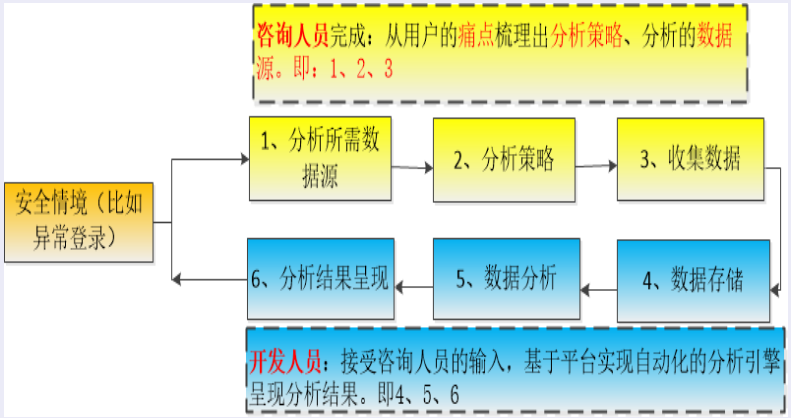


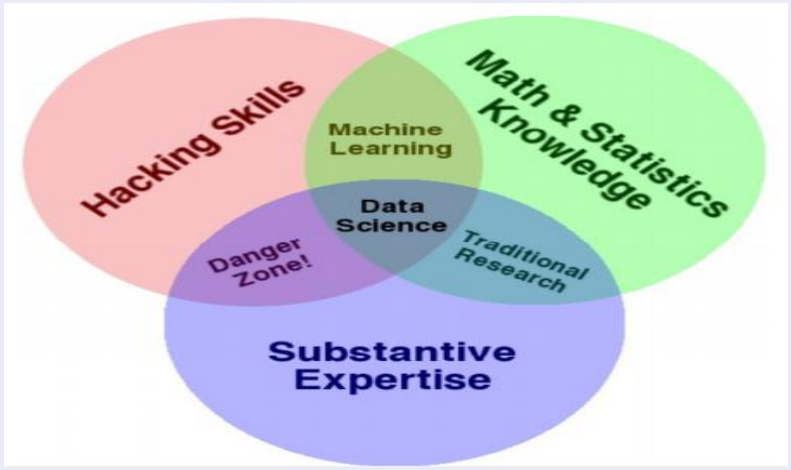
- 取证、溯源:讲究司法上的证据链完整性
- 完整的防护包括防御、检测、回溯分析和预测能力

内控:“安全情境”梳理方法

OWASP 中国
The Open Web Application Security Project



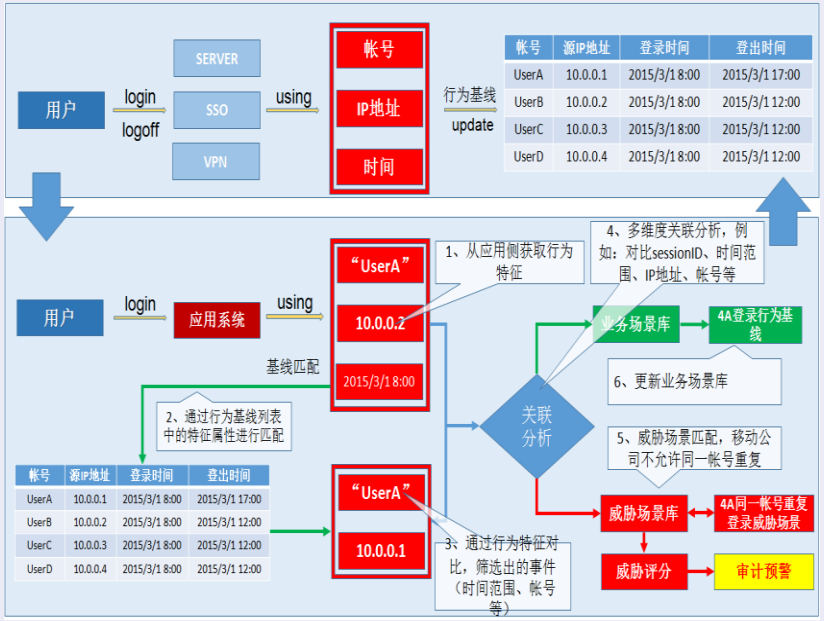


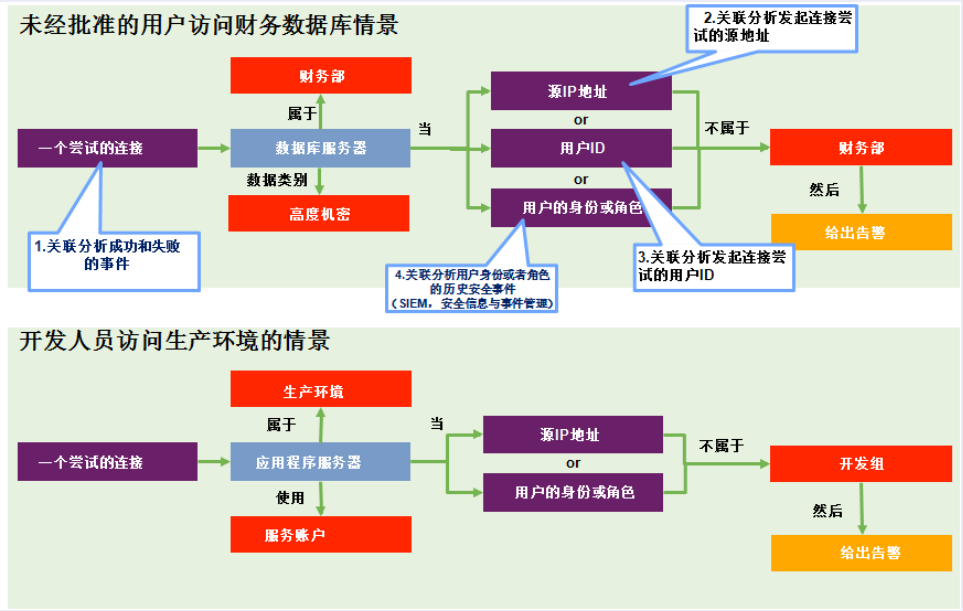


内控:行为基线建模

OWASP 中国
The Open Web Application Security Project

- 针对人为核心的行为基线建模





内控:行为基线建模

OWASP 中国
The Open Web Application Security Project

- 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。

内控:异常行为检测的难点

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

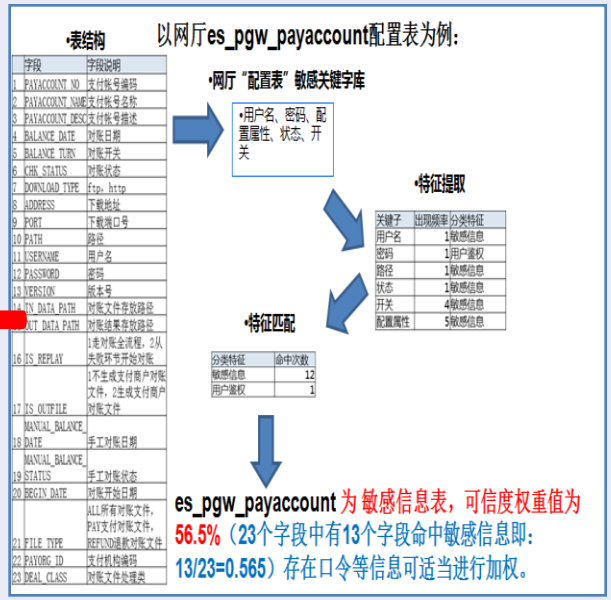
主体（who）

主帐号名称	组织结构	主帐号角色	自然人姓名	联系电话
liuyuewen-30080008	河北分公司	普通员工	刘跃文	[redacted]
soxtzgjsongyu-3003938	天职公司	普通员工	天职国际宋宇	1865[redacted]
songxiaohui-30000004	河北分公司	普通员工	宋晓惠	1391[redacted]
liqiang-30000019	河北分公司	普通员工	李强	1381[redacted]
lilliangui-30083588	河北分公司	普通员工	李连贵	1591[redacted]
zhangshiyong-30002244	河北分公司	普通员工	张世勇	1391[redacted]
liuxin-30000017	河北分公司	普通员工	刘欣	1391[redacted]
caiyanliang	河北分公司	普通员工	caiyanliang	1366[redacted]
wusuihua-30000005	河北分公司	普通员工	吴穗华	1391[redacted]
kejunqing-30000006	河北分公司	普通员工	柯俊清	1391[redacted]
sonxiaohui-30000004	河北分公司	普通员工	宋晓惠	1391[redacted]
gongjili-ls	河北分公司	普通员工	贡吉利	1391[redacted]
fengliang-30000057	河北分公司	普通员工	冯亮	1591[redacted]
fengliang1-30000057	河北分公司	普通员工	冯亮	1591[redacted]
jiadongqi-30000018	河北分公司	普通员工	贾东启	1881[redacted]
jiyushun-3000072c	河北分公司	普通员工	吉雨顺	1881[redacted]
guoxin-agx	河北分公司	普通员工	郭新	1391[redacted]
wuqian-30040061	业务支撑中	普通员工	吴倩	1371[redacted]
maxixing-30039959	业务支撑中	普通员工	马喜兴	1581[redacted]
yudandan-30039958	业务支撑中	普通员工	于丹丹	1361[redacted]
huiqianer-0924	业务支撑中	普通员工	会签二	1[redacted]
sunhongjuan-aa987	业务支撑中	石家庄分公司	孙红娟	1391[redacted]
wangxiaona-30000392	业务支撑中	普通员工	王晓娜	1391[redacted]
lichunyan-aalcy	业务支撑中	石家庄分公司	李春燕	1391[redacted]
liguoce-aalgc	业务支撑中	石家庄分公司	李国策	1381[redacted]
jiangdong-aajd	业务支撑中	石家庄分公司	江东	1376[redacted]
guotong-30038577	业务支撑中	石家庄分公司	郭同	1581[redacted]
jiaoyanchi-aajyc	业务支撑中	石家庄分公司	焦艳池	1393[redacted]
fanruiqing-afrq	业务支撑中	石家庄分公司	范瑞青	13603119875
chenyuan-acy	业务支撑中	石家庄分公司	陈远	13603119637
wangmiao-30000278	业务支撑中	石家庄分公司	王淼	13931126662
chenna-aachn	业务支撑中	石家庄分公司	陈娜	13903116963
gaoxiaohong-aagxh	业务支撑中	石家庄分公司	高小红	13603116460
zhangpeining-30039239	业务支撑中	石家庄分公司	张培明	13930156037
gaole-30039244	业务支撑中	石家庄分公司	高乐	13513216221

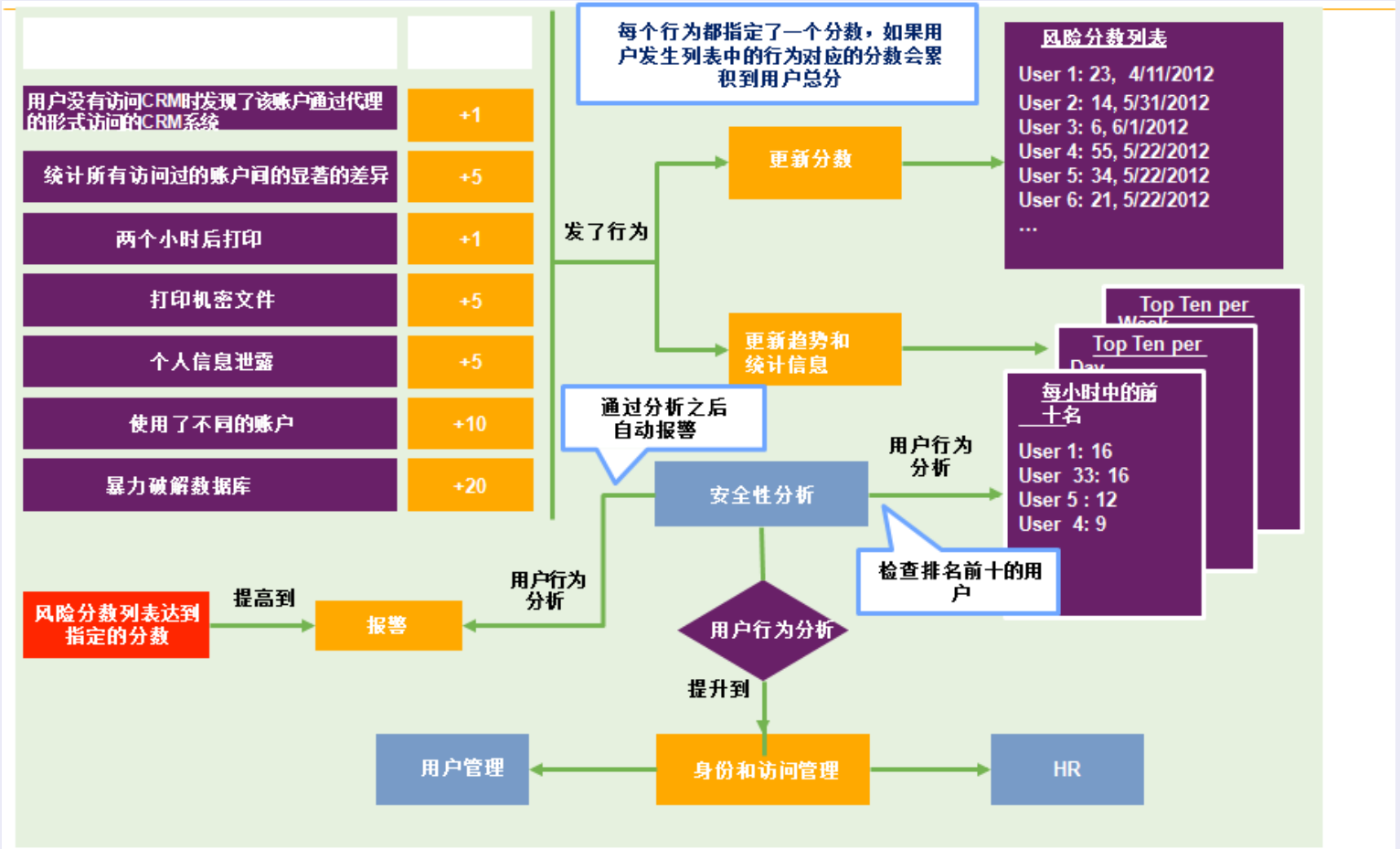
动作（how）

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”对象类中指定的程	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标	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修	中
installp	在一个兼容的安装软件包里安装可用的软	中

客体（what）



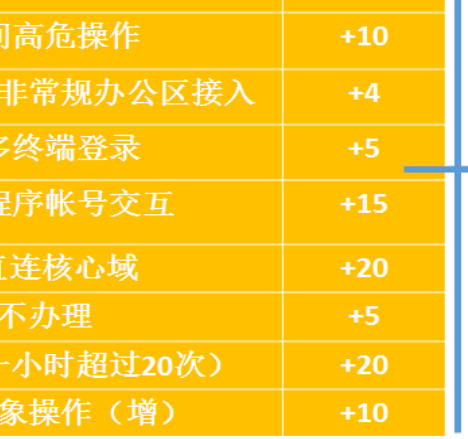
内控:行为的量化-聚合


用户没有访问CRM时发现了该账户通过代理的形式访问的CRM系统
+1
统计所有访问过的账户间的显著的差异
+5
两个小时后打印
+1
打印机密文件
+5
个人信息泄露
+5
使用了不同的账户
+10
暴力破解数据库
+20
每个行为都指定了一个分数，如果用户发生列表中的行为对应的分数会累积到用户总分
发了行为
更新分数
风险分数列表
User 1: 23, 4/11/2012
User 2: 14, 5/31/2012
User 3: 6, 6/1/2012
User 4: 55, 5/22/2012
User 5: 34, 5/22/2012
User 6: 21, 5/22/2012
...
更新趋势和统计信息
Top Ten per
Top Ten per
每小时中的前十名
User 1: 16
User 33: 16
User 5 : 12
User 4: 9
通过分析之后自动报警
用户行为分析
安全性分析
检查排名前十的用户
风险分数列表达到指定的分数
提高到
报警
用户行为分析
用户行为分析
提升到
用户管理
身份和访问管理
HR

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



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

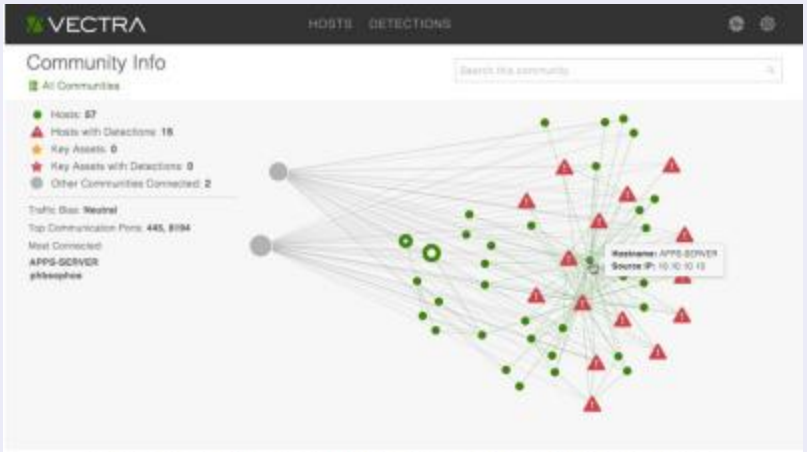
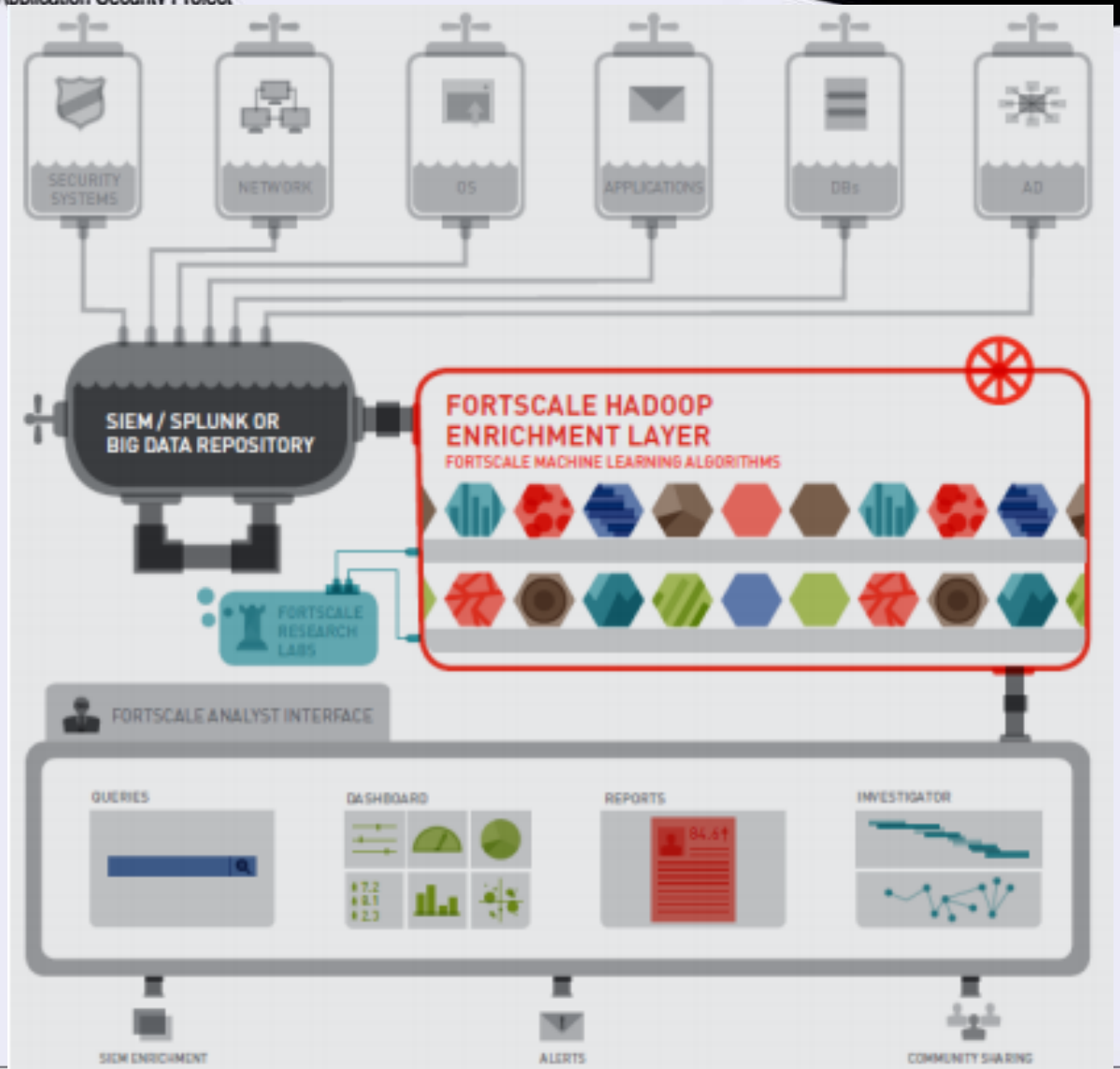


Figure 1: Use the Community Threat Analysis to find devices with the most connections

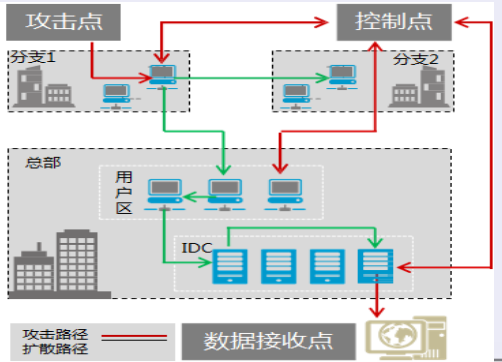
Figure 2: Click the star next to host name to tag the host as a key asset

内控:异常行为分析产品形态



内控:异常行为分析实践

- 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



结束语:安全产品(交付)方向思考

OWASP 中国
The Open Web Application Security Project

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。