

“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



天融信官方微信

大数据安全平台最后一公里 关注点



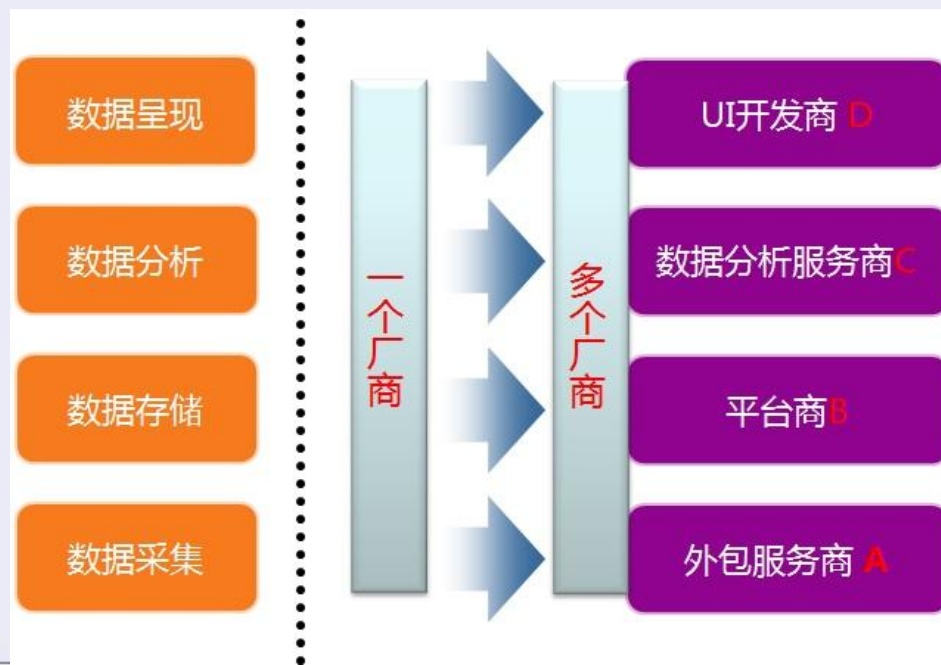
OWASP 中国
The Open Web Application Security Project

A vision for security detection analytics

	Existing	Emerging	Advanced	Target
Understand	Basic context <ul style="list-style-type: none">Asset, networkIdentity	Advanced context <ul style="list-style-type: none">ApplicationFlow & DPI	Technical intelligence <ul style="list-style-type: none">Malware detonationIOC identification	Human intelligence <ul style="list-style-type: none">Sentiment analysisMotivation
Explore	Ad hoc query <ul style="list-style-type: none">Small datasetBasic analysis	Advanced search <ul style="list-style-type: none">Indicator listsPivot search	Analytical query <ul style="list-style-type: none">Big Data managementAnalytical data mart	Visualization <ul style="list-style-type: none">Exploratory data analysis
Explain	Reporting <ul style="list-style-type: none">ThreatCompliance	Scoring <ul style="list-style-type: none">Risk fidelityProfiling	Data mining <ul style="list-style-type: none">Clustering, aggregationAffinity grouping	Machine learning <ul style="list-style-type: none">ClassificationOther algorithms
Detect	Real-time <ul style="list-style-type: none">Real-time correlationLog aggregation	Historical analysis <ul style="list-style-type: none">Long-term correlationEpidemiology	Statistical analysis <ul style="list-style-type: none">Distributed RStandard deviation	Behavioral <ul style="list-style-type: none">Insider threatBaselining

Depth => Increase in effectiveness

- 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”



威胁情报(外防)

GLOBAL Situational Threat Intelligence



情境感知(内控)

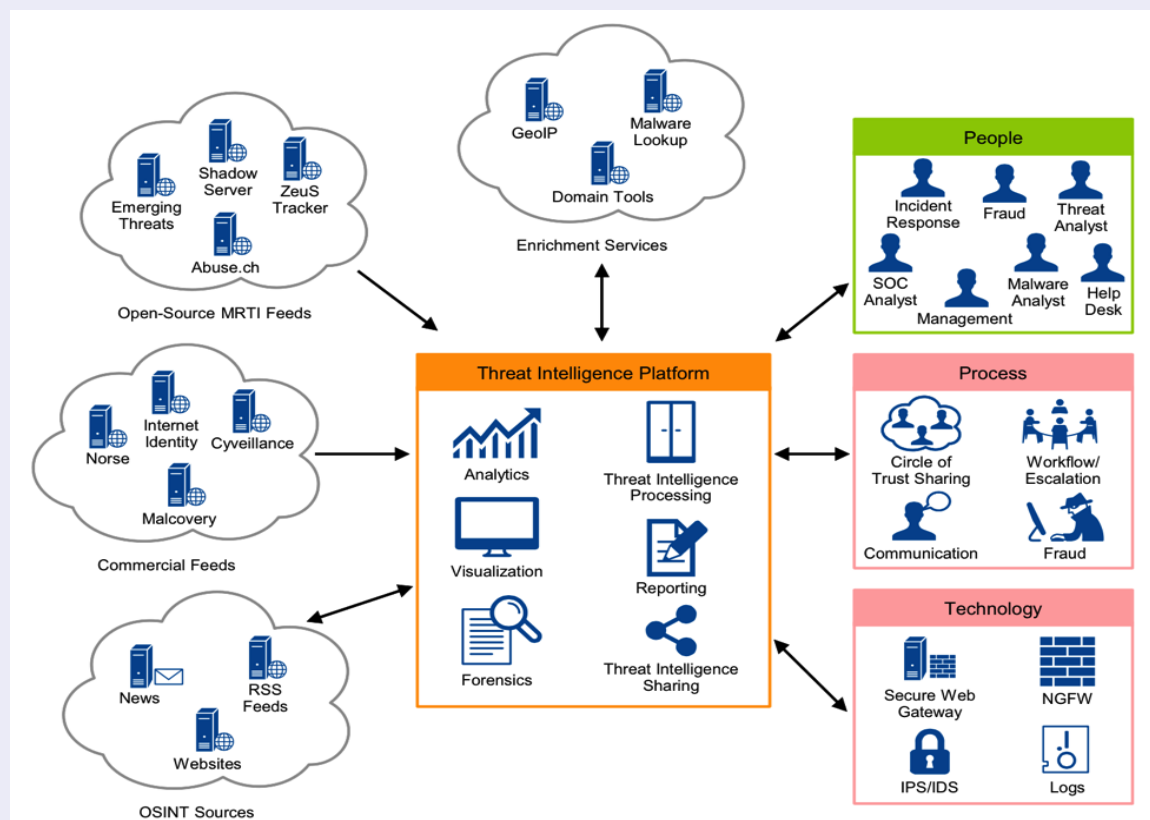
LOCAL Business Context



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。

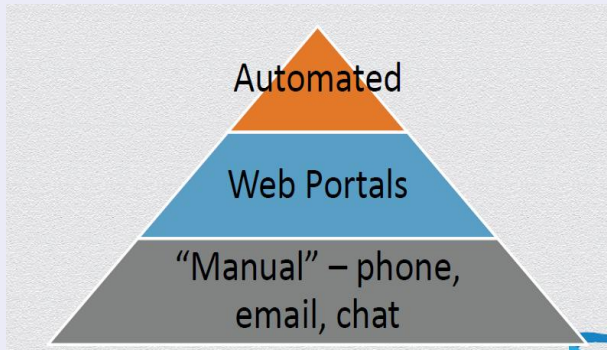


安全情报以“空间”换“时间”，用集体协作来应对“P”，通过情报驱动防御体系的转变

外防之：安全情报再分析



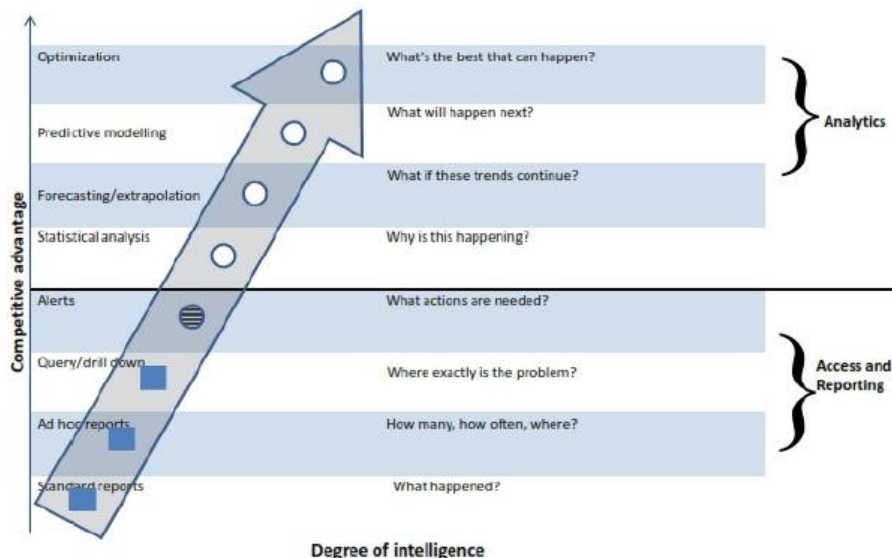
OWASP 中国
The Open Web Application Security Project



CSV、XML和类似标准格式



DJ的札记



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）

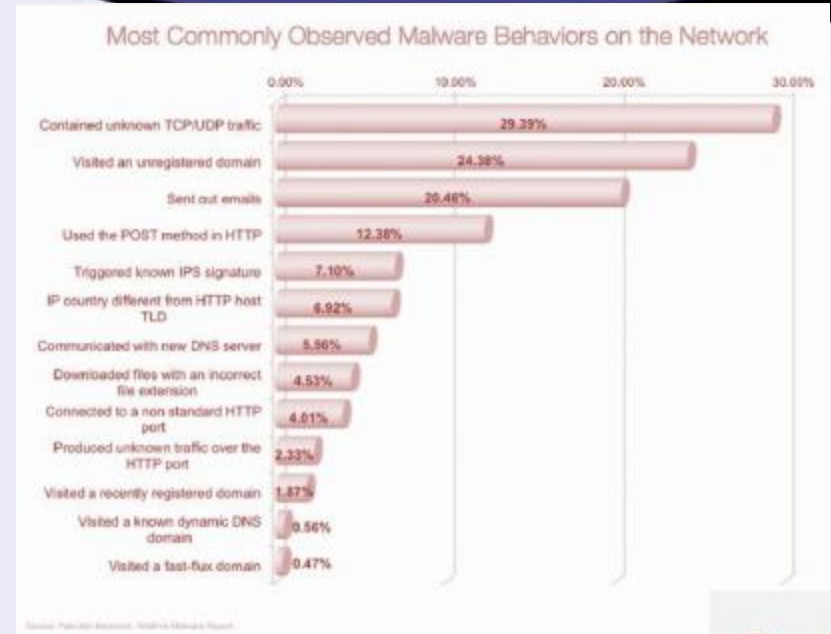




OWASP 中国
The Open Web Application Security Project

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

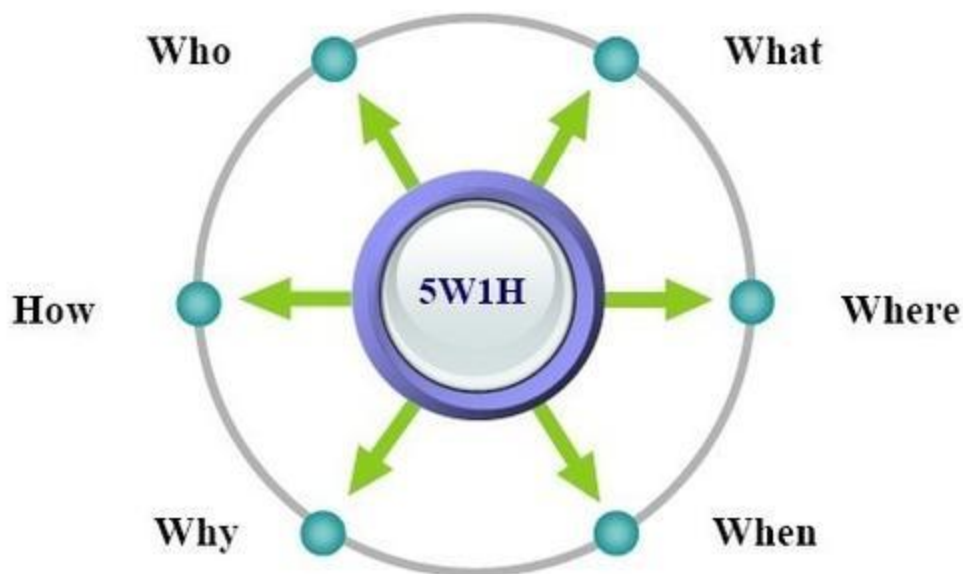
Adversaries from outside or from the inside collect covert information about the targeted enterprise, learn about its employees and network structure, slowly accumulate privileges by compromising legitimate users, move laterally like legitimate users and exfiltrate the target information in very small 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。





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
-

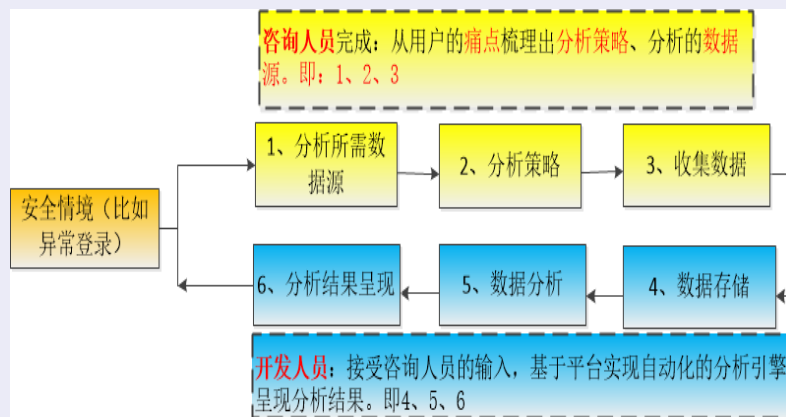
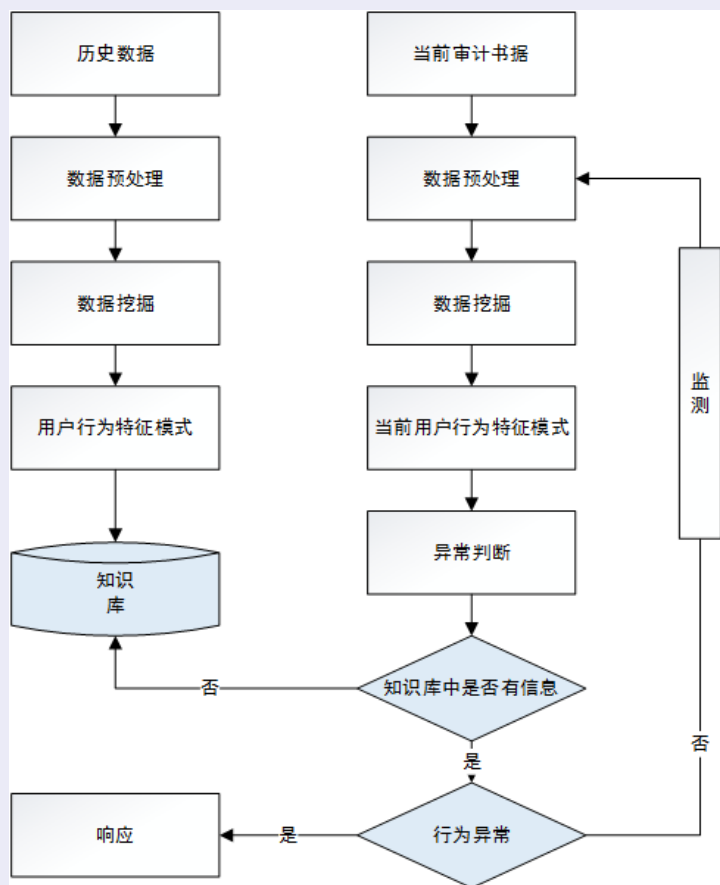


- 取证、溯源:讲究司法上的证据链完整性
- 完整的防护包括防御、检测、回溯分析和预测能力

内控：“安全情境”梳理方法

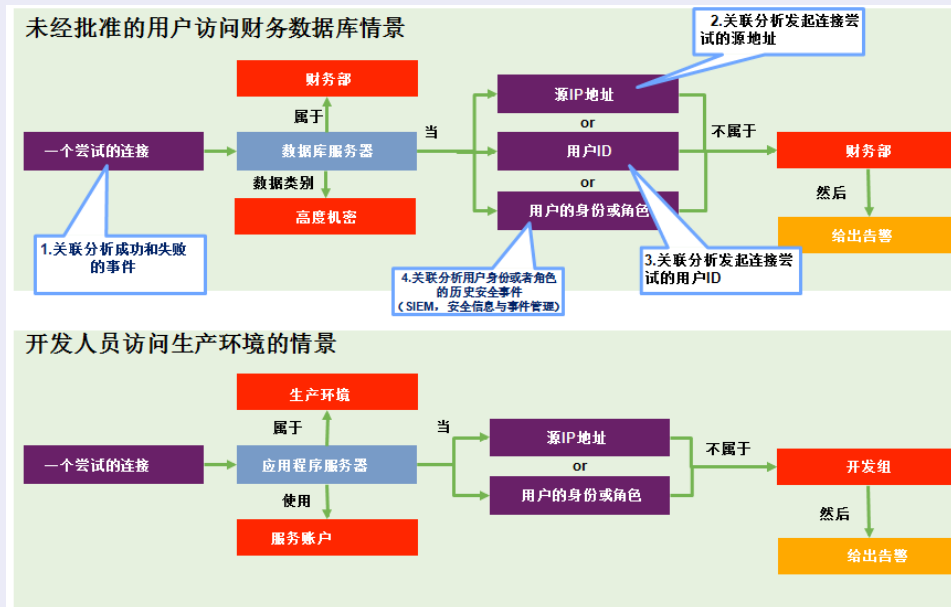


OWASP 中国
The Open Web Application Security Project





• 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

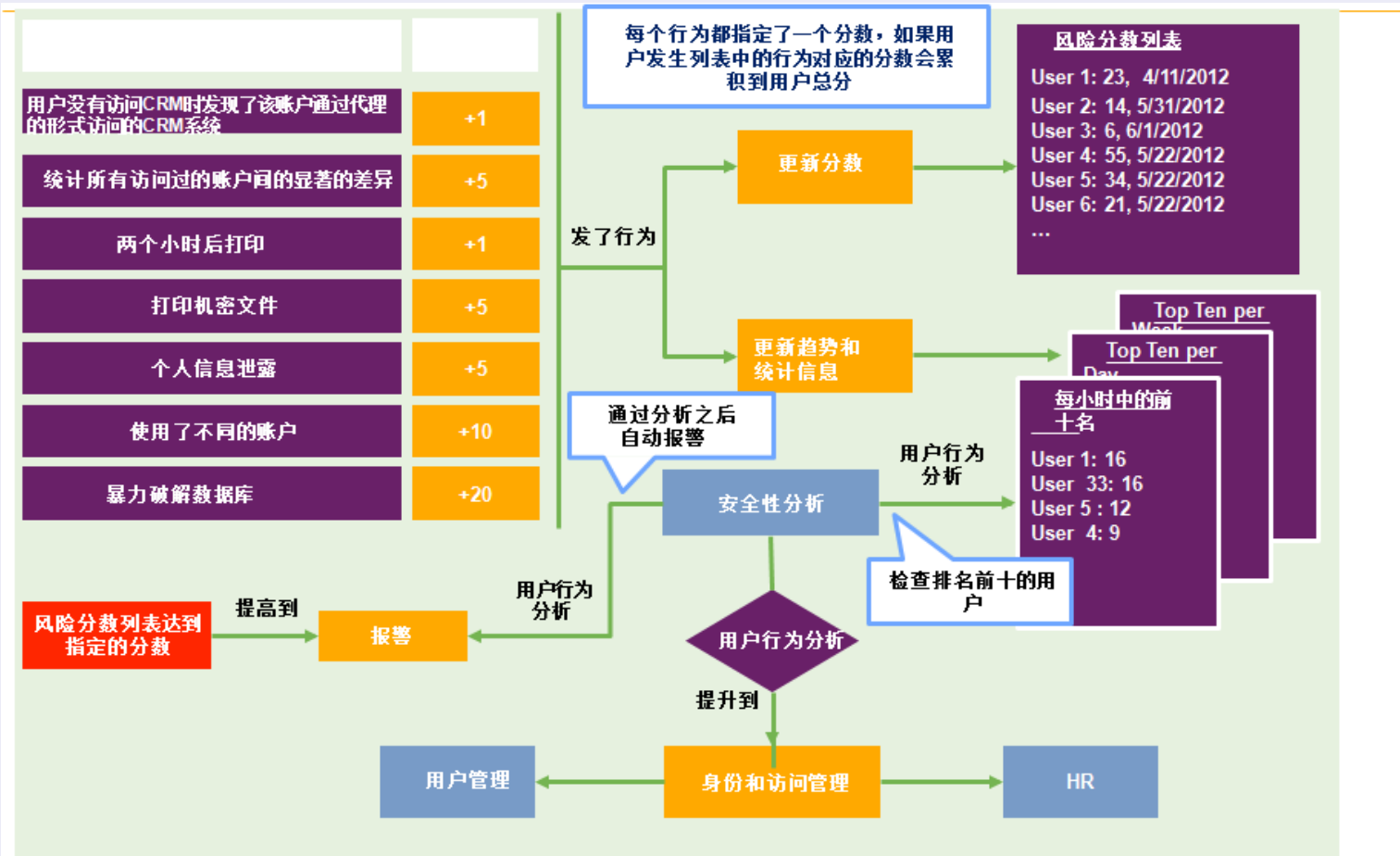
The Open Web Application Security Project

- 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-聚合



OWASP 中国
The Open Web Application Security Project



内控：异常行为分析产品形态



OWASP 中国
The Open Web Application Security Project

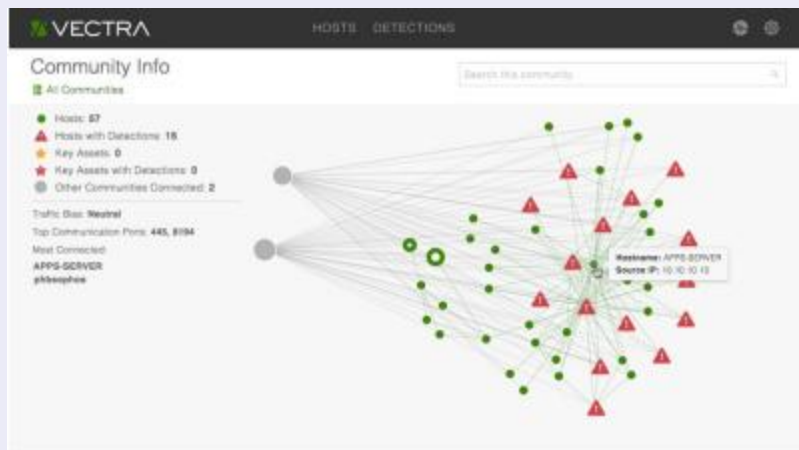


Figure 1: Use the Community Threat Analysis to find devices with the most connections

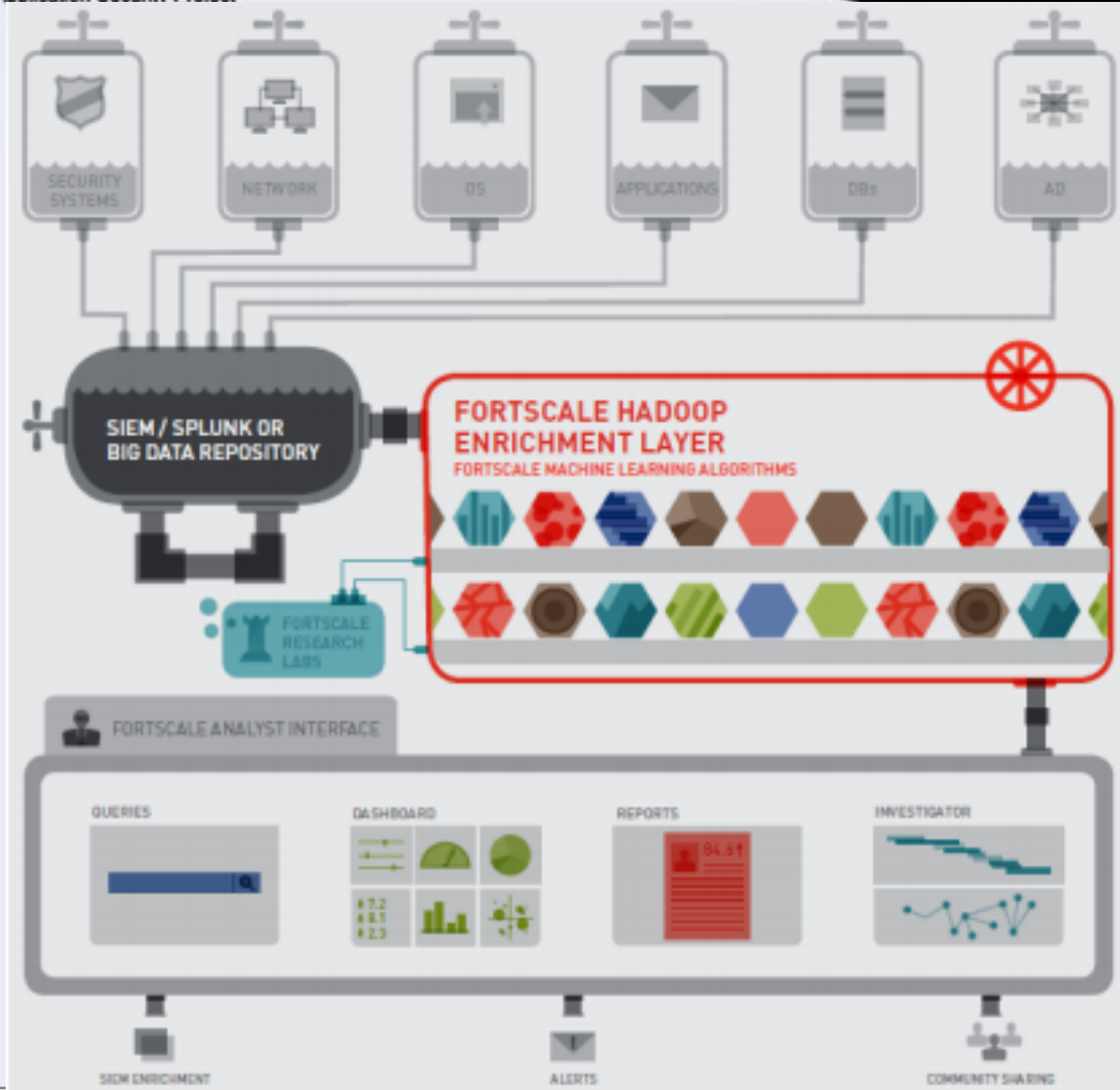


Figure 2: Click the star next to host name to tag the host as a key asset

内控：异常行为分析产品形态

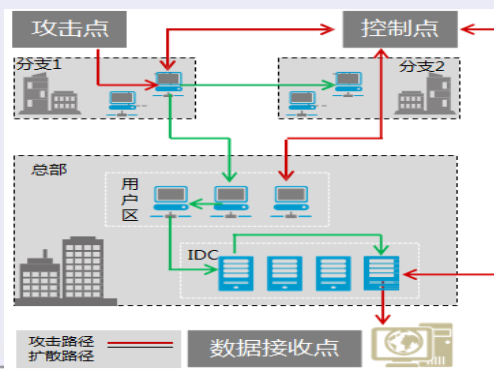


OWASP 中国
The Open Web Application Security Project





- 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。