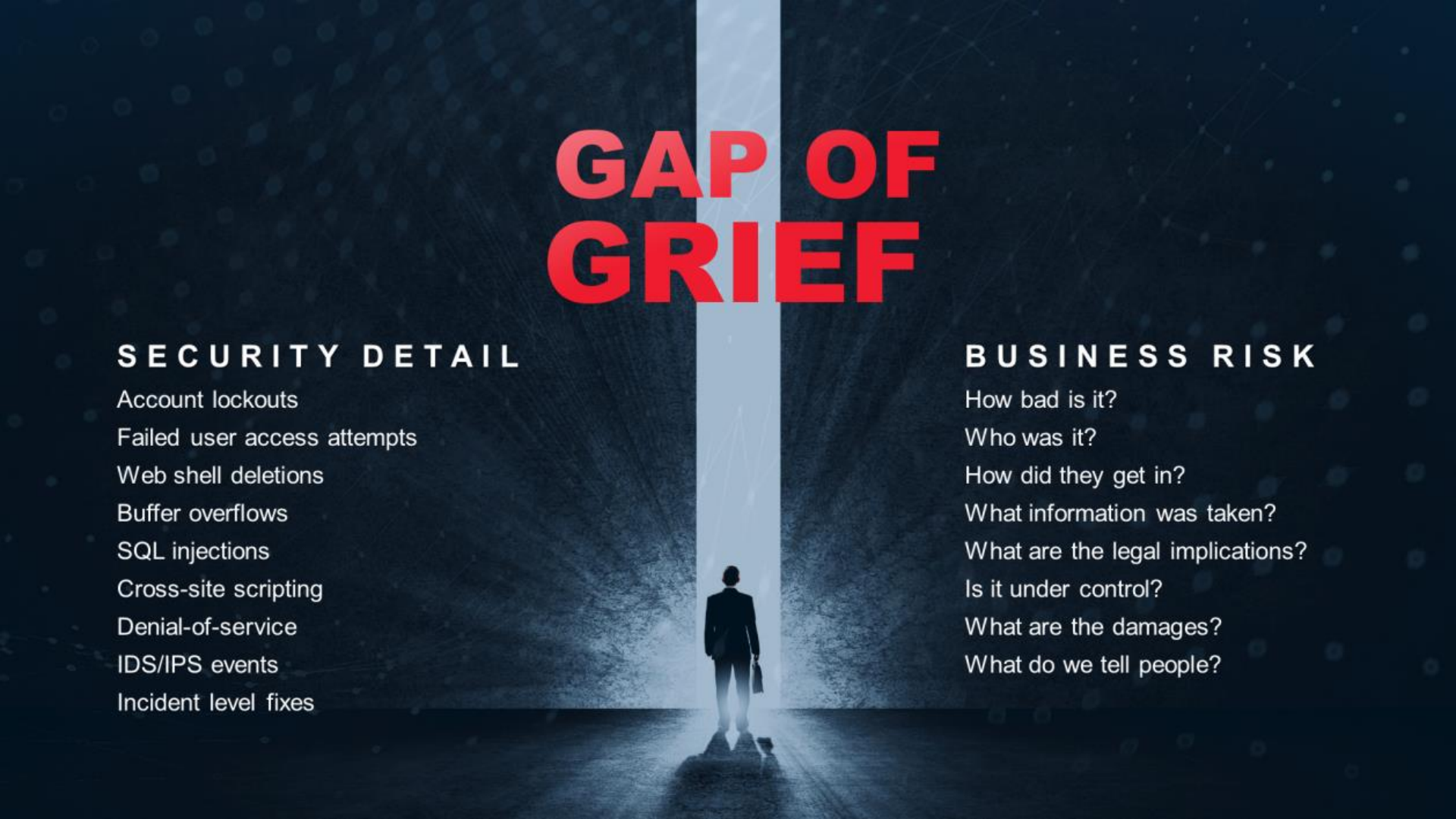
Alibaba Group 阿里巴巴集团 × 蚂蚁金服 ANT FINANCIAL

基于业务 构筑安全

BUSINESS
DRIVEN
SECURITY

兰云科技

GAP OF GRIEF



SECURITY DETAIL

Account lockouts
Failed user access attempts
Web shell deletions
Buffer overflows
SQL injections
Cross-site scripting
Denial-of-service
IDS/IPS events
Incident level fixes

BUSINESS RISK

How bad is it?
Who was it?
How did they get in?
What information was taken?
What are the legal implications?
Is it under control?
What are the damages?
What do we tell people?

首席执行官们谈论和关心的是商业风险

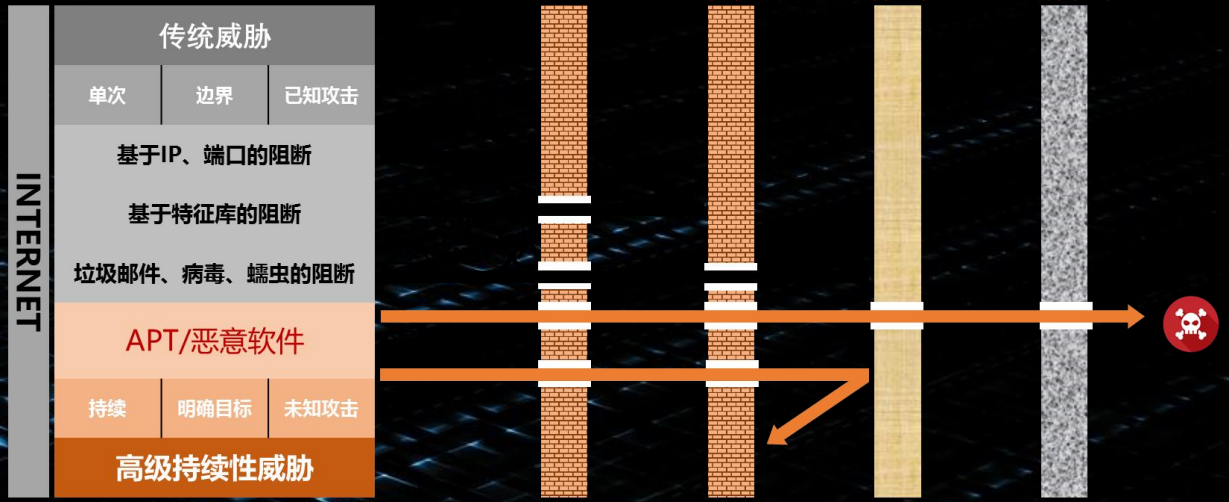
“他们关心安全措施的有效性，关心他们如何应对其间的风险”

网络安全事件层出不穷

美国大选t事件：2016年年底，美国大选双方互报黑料，以及投票系统遭遇黑客攻击

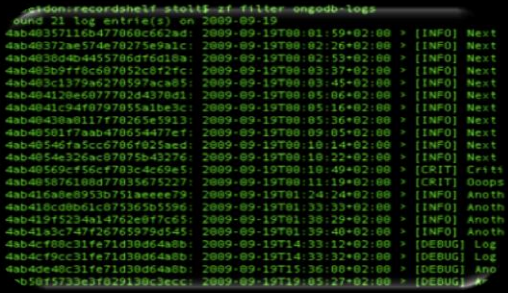
路由器事件：2016年11月，德国电信90万台路由器遭遇Mirai僵尸网络攻击。

DII事件：2016年9月，日本DII（国防信息基础设施）遭遇入侵。



网络安全问题纷繁复杂

传统安全设备无法发现APT攻击，客户不知道已经被攻击



告警信息泛滥，海量数据堆积，运维人员疲于应付

网络中部署的安全产品彼此孤立，无法呈现整网安全态势

发生攻击事件，缺乏攻击还原手段，管理员无法有效追责

典型的安全方案是怎样的？

BUT NOW

- 防护范围变化：单机安全->边界安全->无边界安全
- 攻击目的变化：技术炫耀->经济利益/政治目标

攻击只是手段，获利才是目标。
获利必须通过获取目标网络中的高价值信息实现

“世界在变，我们也需要改变”

基于业务 构筑安全

BUSINESS
DRIVEN
SECURITY

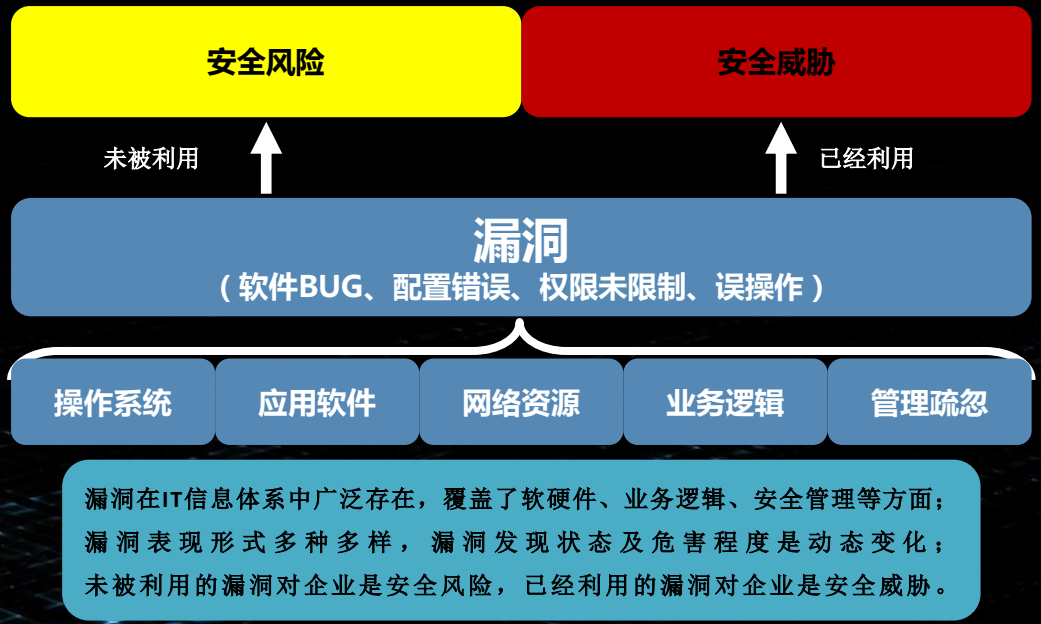
HOW TO DO ?

?

发掘入侵事件

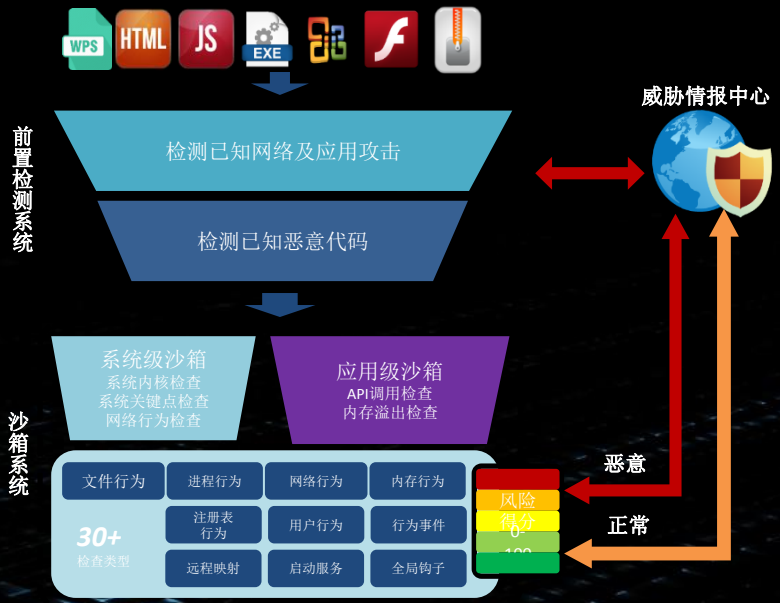
而不是停留在发现攻击企图

从安全风险管理向安全威胁检测过渡



漏洞在IT信息体系中广泛存在，覆盖了软硬件、业务逻辑、安全管理等方面；漏洞表现形式多种多样，漏洞发现状态及危害程度是动态变化；未被利用的漏洞对企业是安全风险，已经利用的漏洞对企业是安全威胁。

发现已知和未知单点威胁



关联不同阶段的威胁，发现入侵事件

基于业务，跳出安全，实现安全

而不是孤立的，就安全，做安全

从恶意特征库转变为业务行为模型

- 我们无法获得所有现有攻击特征，更无法预知所有新的攻击技术，因此基于恶意的特征检测无法满足业务安全要求；
- 业务系统千差万别，但单一企业的业务系统是有限而稳定的，其正常业务模型是可预知，易于学习建模的，因此基于业务行为的模型检测更符合业务安全要求；

恶意特征库检测

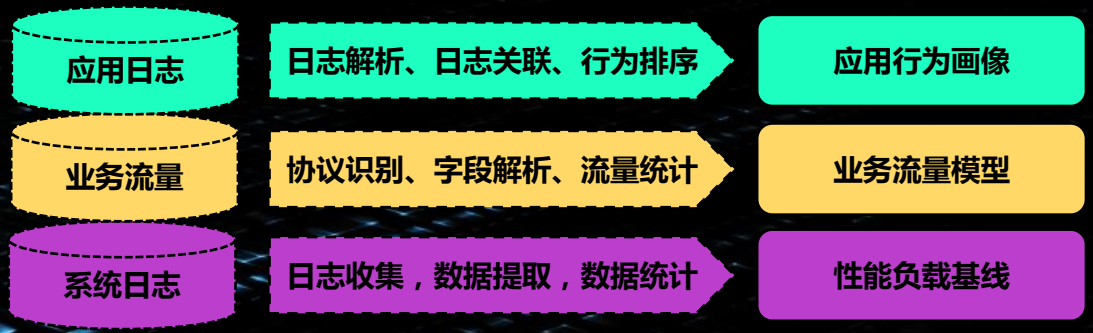
- 收集并提炼已知攻击信息，匹配攻击明显特征检测并阻断；
- 无法覆盖所有攻击特征。

业务行为异常检测

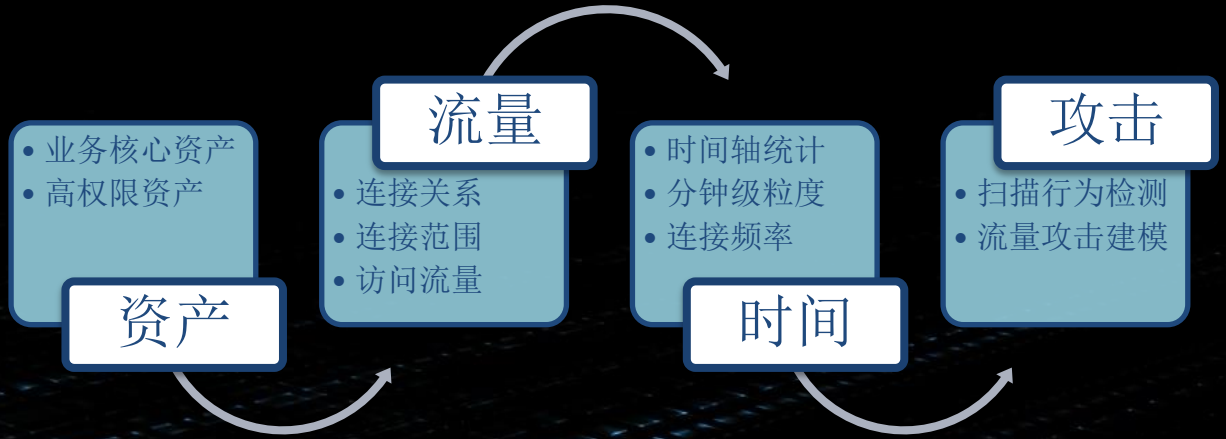
- 基于正常业务的系统、应用、流量建立白名单模型检测，对检测出的威胁定制响应体系；
- 检测准确率高，能发现所有不符合正常业务要求的威胁；

构建业务访问模型检测威胁

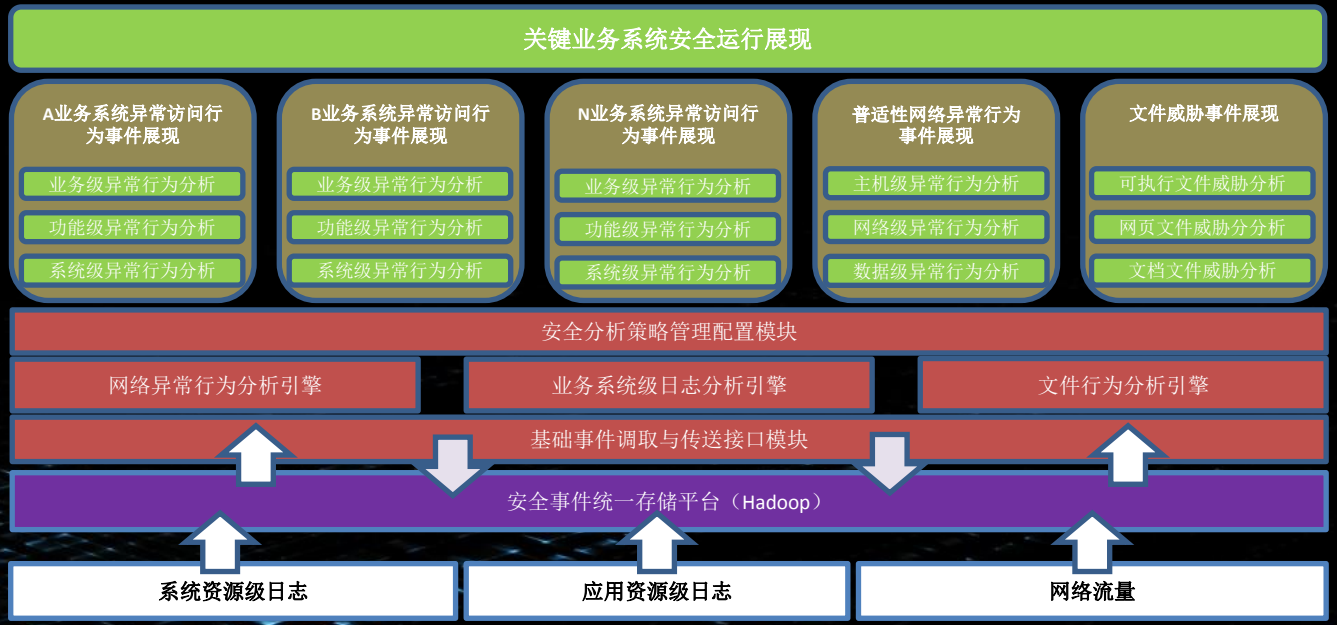
- 依据业务安全需要建立分层检测模型，用于各层次的检测使用；
- 通过分层检测模型，满足运维故障定位、高级威胁入侵、业务逻辑攻击等检测需求；



威胁检测的正向模型及反向模型



业务系统异常行为分析


关键业务系统安全运行展现
A业务系统异常访问行为事件展现
业务级异常行为分析
功能级异常行为分析
系统级异常行为分析
B业务系统异常访问行为事件展现
业务级异常行为分析
功能级异常行为分析
系统级异常行为分析
N业务系统异常访问行为事件展现
业务级异常行为分析
功能级异常行为分析
系统级异常行为分析
普适性网络异常行为事件展现
主机级异常行为分析
网络级异常行为分析
数据级异常行为分析
文件威胁事件展现
可执行文件威胁分析
网页文件威胁分分析
文档文件威胁分析
安全分析策略管理配置模块
网络异常行为分析引擎
业务系统级日志分析引擎
文件行为分析引擎
基础事件调取与传送接口模块
安全事件统一存储平台（Hadoop）
系统资源级日志
应用资源级日志
网络流量

企业安全威胁态势管理方案

流量分析　旁路获取流量，还原真实攻击过程

文件分析　洞察文件行为，识别恶意代码企图

日志分析　全量日志查询，关联分析调查取证

交互分析　分析访问记录，检测异常访问行为

访问分析　威胁线索查询，还原完整攻击场景

兰云科技

www.lanysec.com