奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

奇智威胁情报峰会

情报内生 聚合应变

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

大型企业威胁情报体系应用实践分析

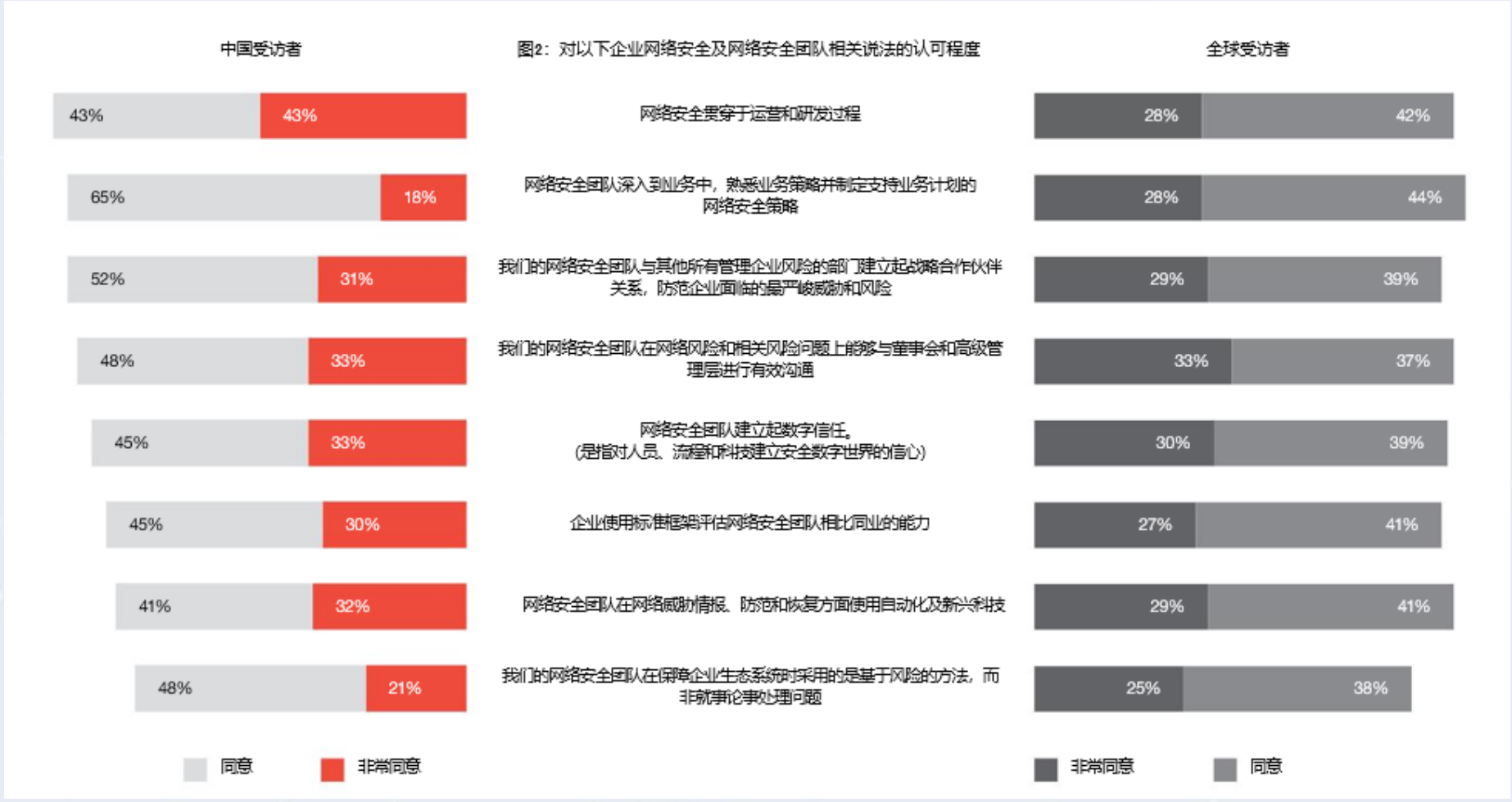
数字化转型给企业带来更大的安全风险

普华永道2019数字信任洞察之中国报告

数字化转型为促进企业发展和创新带来了大量机会的同时，也导致了企业需要应对转型期间所来带的特有风险。从中国企业高管和IT专业人士的角度来看，数字化进程中面临的最严峻风险是数据治理或隐私问题（中国：28%；全球：11%）。中国企业普遍对数据收集和传输存在顾虑，而加强信息安全和对个人数据收集的保护是国家战略重点。

网络安全计划与业务发展并进

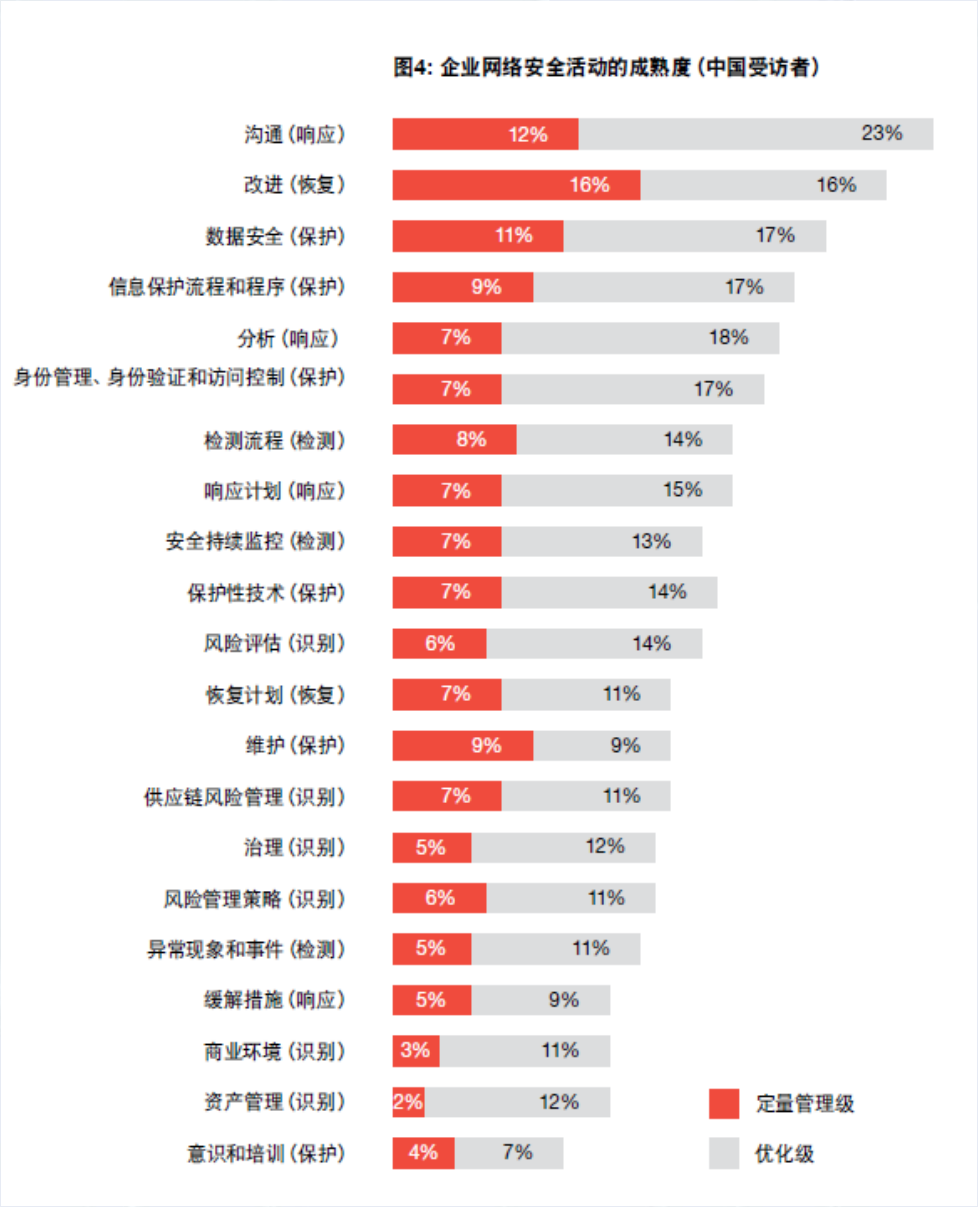
从一系列衡量指标来看，多数中国受访者的网络安全与业务发展相配的程度高于全球受访者。83%的受访者表示，其网络安全团队正嵌入企业的业务当中，他们不仅熟悉业务策略，而且制定了支持业务需要的网络安全策略（全球：72%）。83%的受访者认为，其网络安全团队与其他所有管理企业风险的部门建立起战略合作关系，防范企业面临的最严峻威胁和风险 （全球：68%）。81%的受访者认为，其网络安全团队在网络风险和相关风险问题上能够与董事会和高级管理层进行有效沟通（全球：70%）。



数字化转型要求网络安全团队主动识别风险

深入了解网络安全团队的哪些做法能更好地与企业目标相配无疑非常重要，与此同时，衡量网络安全团队现有的网络安全措施成熟度同样大有裨益。此次调研在这方面对企业进行评价，评价的依据是美国国家标准与技术研究院（NIST）所发布的《网络安全框架》5中的具体类别，包括五个主要网络安全功能：识别、保护、检测、响应和恢复。

成熟度方面，中国网络安全团队在**“响应”和“保护”**两项功能中成熟度最高，在**“识别”**功能中成熟度最低。这一情况堪忧，因为这说明调研受访者只处于响应状态，在风险发生后采取缓解措施，而未能充分识别风险并防范于未然。这表明网络安全团队在识别关键资源和企业情况，从而根据企业风险管理策略和业务需要促使企业重点保障网络安全方面较为薄弱。于是，网络安全团队只能进行损害控制，或只能在侦测到事故后为企业提供支持，而且对企业的保护方式也只是减弱或遏制事件的影响。



大型企业所面临的安全困境

想不到

数字化转型中的业务创新、不断提升的用户体验增加了业务流程和验证环节在互联网上的暴露程度，每个业务逻辑或系统的漏洞都可能被恶意利用

看不见

攻击者利用新型的攻击手段占有主动性的优势，企业受到系统多样、数据复杂的制约，难以及时发现攻击行为

抓不着

受到监控技术、响应速度、证据留存等多方面管理和技术因素的限制，企业在遭受攻击后，难以对攻击者进行定位

做不了

信息安全事件的事中响应处置、事后分析整改需要多个部门的协同配合，单靠安全团队难以提升企业整体的安全水平

以情报为核心构建新业态下的安全体系

结合企业自身信息安全战略和人员情况进行安全体系建设，通过组织架构和运营流程加强体系落地

以情报数据为核心，根据业务场景安全需求，收集全面的监控数据，实现精准化、主动化安全监控

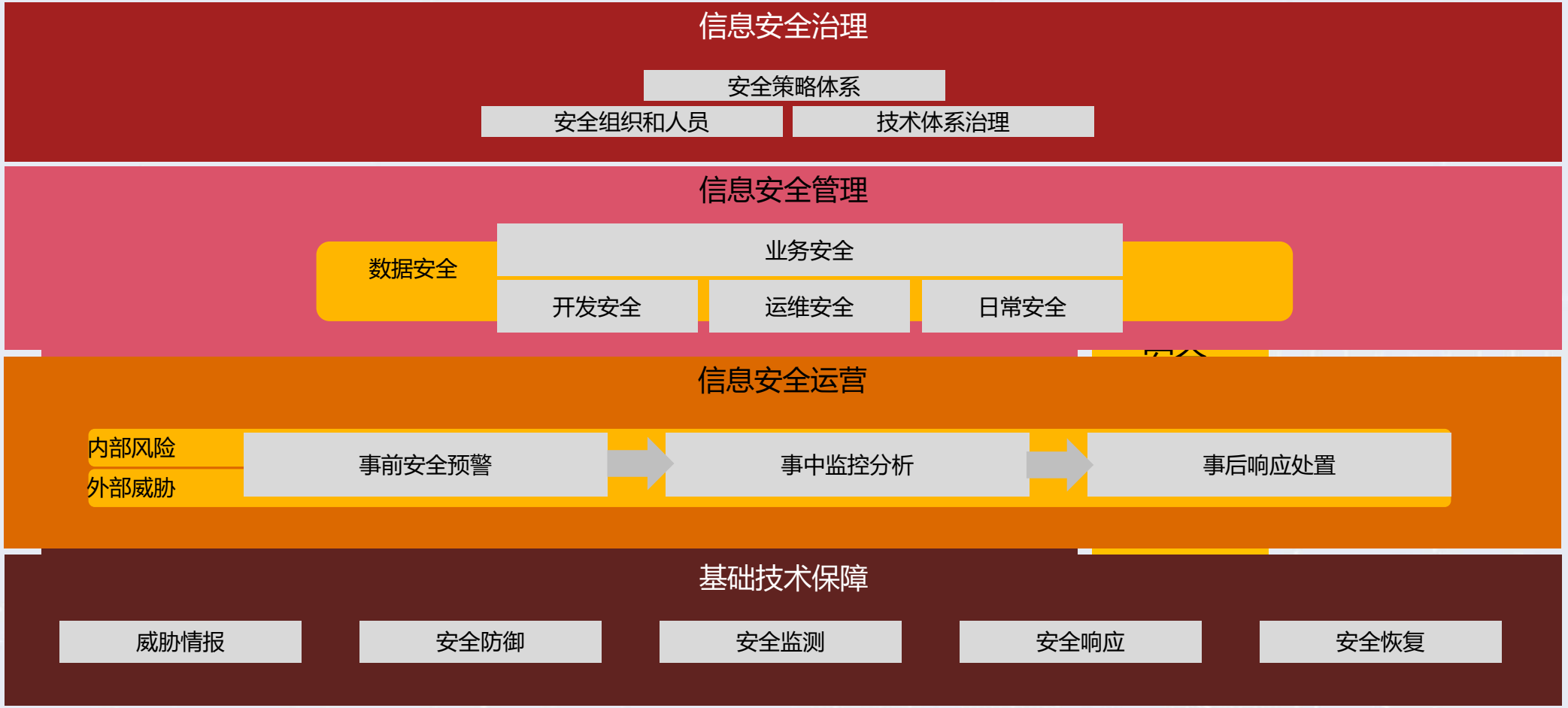
从事前、事中、事后阶段构建安全运营能力，突出事前预警和事中分析能力，让安全应急无急可应

安全体系目标

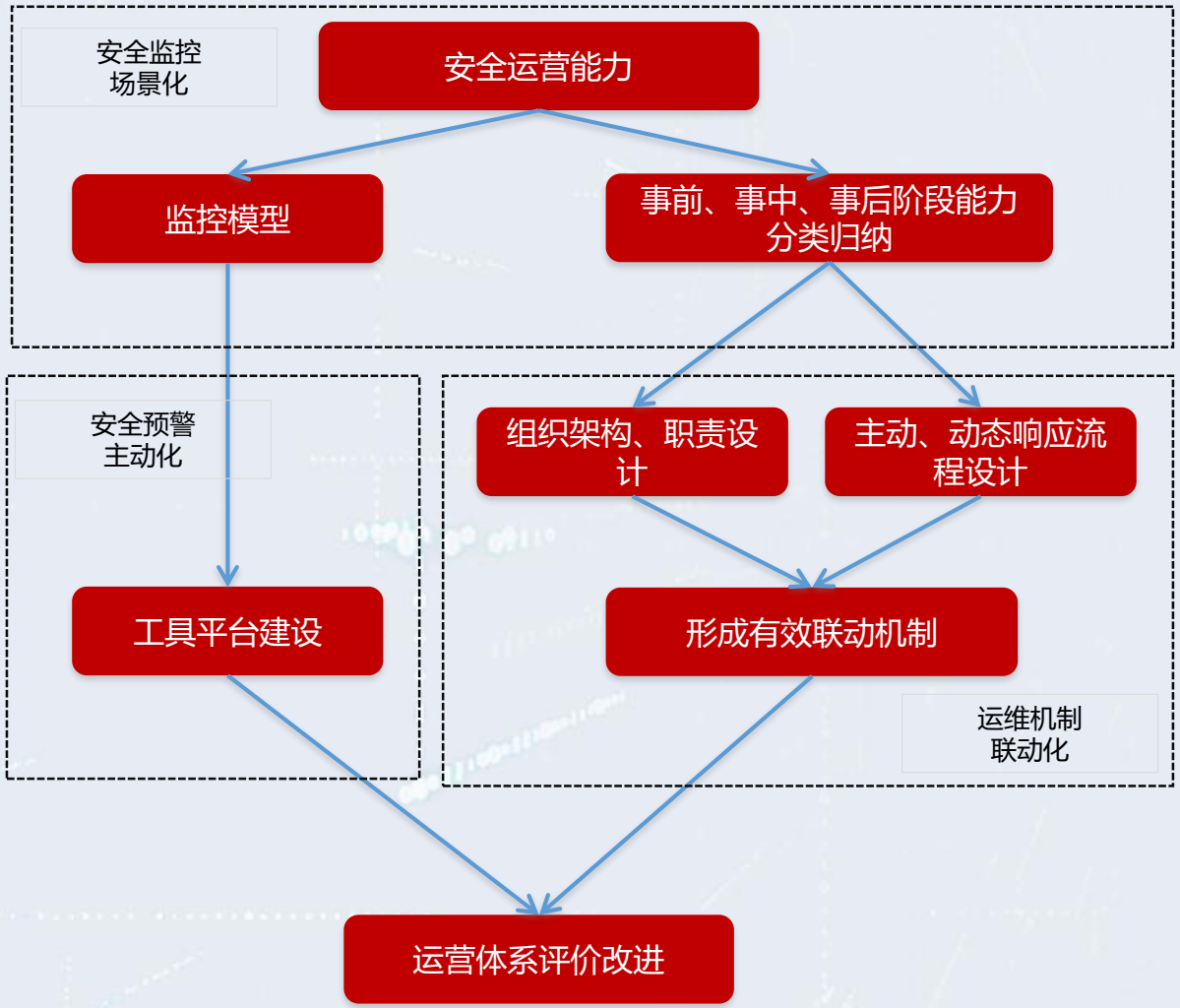
- 覆盖业务场景的监控平台和运行机制
- 业务安全监控和预警
- 安全攻击监控和预警
- 内部高危操作监管和预警

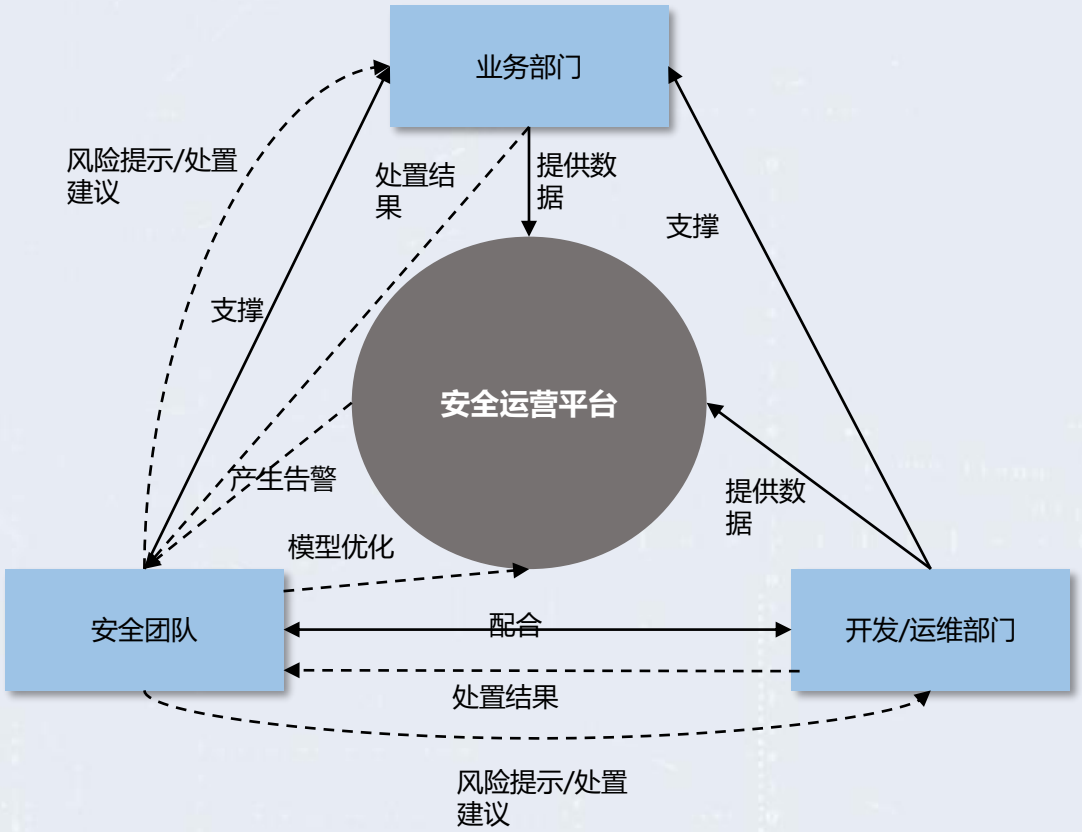
从威胁出发，构建动态安全体系

- 安全治理体系和安全管理体系明确信息安全工作目标和机制，**解决“想不到”**和**“做不了”**的挑战
- 以安全运营为核心，打通技术体系和管理体系，给安全团队赋能并有效运转，**解决“看不见”**和**“抓不着”**的问题



打破组织壁垒，构建动态运营管理机制



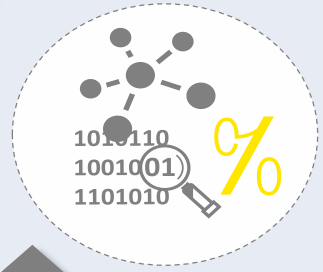


动态安全运营组织和流程

通过六步走，将内部威胁情报精准化场景化

1. 安全场景识别

1.1.监控领域识别：



（1A）历史数据法
（1B）模型分析法
（1C）业务梳理法

2. 关键安全因素识别

2.1.安全监控环节梳理

采用访谈的方式，对业务、运维等监控领域的环节进行识别，作为潜在的异常行为监控埋点。通过专家征询的方式，对安全监控的环节进行定义

3. 细化安全指标

3.1.安全指标细化

对每个安全监控环节按照可能出现异常的点进行进一步细化，如将用户登录环节细化为登录地点、登录设备、认证失败次数等安全指标。

4. 指标赋值

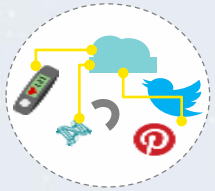
4.制定指标赋值规则

（4A）专家经验法
（4B）四分位赋值法
（4C）比较赋值法

5. 形成模型

5.1.模型构建：

（5A）二元逻辑回归法
（5B）朴素贝叶斯法
（5C）神经网络法



6. 模型验证与调优

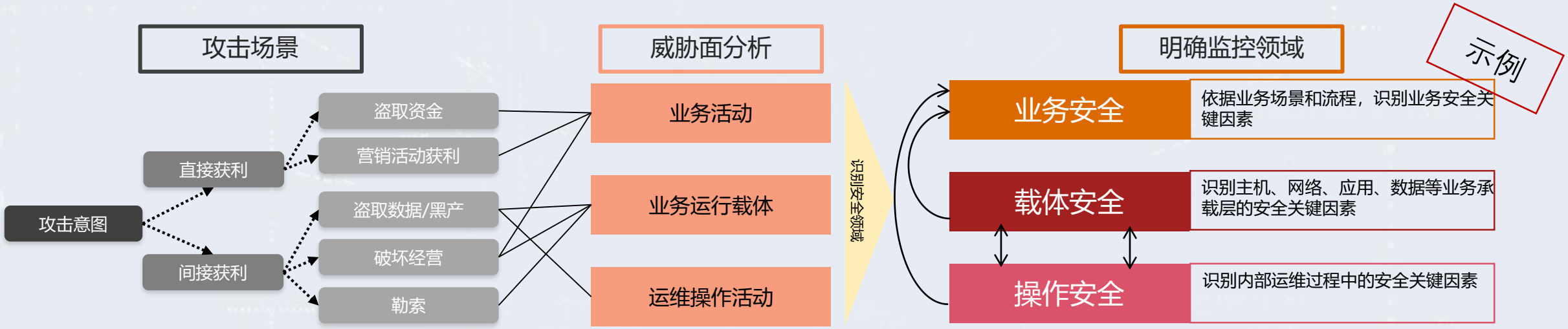
6.1.模型准确性验证

（6A）均方根误差法
（6B）交叉验证
（6C）混淆矩阵

6.2.模型调优

根据验证结果，对模型进行参数调优或引入新的变量。

1.结合业务场景，从攻击者视角，明确监控领域



思路：
信息安全本质上可看做攻防双方在资源投入方面的对抗，从攻击者的视角进行攻击行为分析。

优势：
借助成熟的威胁模型，从攻击者视角，场景识别全面。

思路：
通过分析攻击行为的攻击路径（kill chain），对攻击行为的共性攻击环节进行归纳，总结出对企业信息系统所面临的攻击面。

优势：
结合专家经验，识别重要威胁。

思路：
根据攻击面分析明确安全监控的重点领域。在各个领域按照业务场景、类别等维度进行信息安全关键因素进行识别。

优势：
监控领域覆盖重点需求

2.进一步细化识别安全关键因素

业务安全领域

业务流程梳理

定义关键环节

建立异常行为埋点

业务专家验证

优势：结合业务流程和专家经验，选取关键的安全因素

载体安全

操作安全

异常行为埋点数据

数据层

应用层

主机层

网络层

内部人员异常登录

违规操作

异常查询

重要数据访问

示例

业务安全关键因素集

- 用户登录
- 用户注册
- 访问账户信息
- 支付行为
- 转账行为
- 虚拟资产操作
- 风控辅助数据
- 环境设备数据
- 用户访问页面
- 用户浏览顺序
- 操作停留时间
- 鼠标轨迹

载体安全关键因素集

- 网络链接异常
- 服务器被攻击
- 病毒感染
- 主机存在漏洞
- 数据窃取
- 数据泄露
- 应用存在漏洞
- 应用被攻击

操作安全关键因素集

- 用户提权操作
- 非法外联
- 配置变更
- 内网机器违规访问外网
- 下载/导出个人信息数据
- 查询量波动
- 敏感数据访问
- 非工作时段查询
- 跨条线查询

3.利用安全因素，细化梳理安全监控指标

思路：利用安全因素集，结合专家经验，识别出安全指标。
优势：贴合企业现状，确保指标有效性。

部分业务安全监控指标示例

示例

编号	安全场景		安全领域	安全因素	安全指标
1	业务安全	业务数据	用户账户	用户登录	登录地点改变
2					登录设备指纹异常
3					触发账户登录失败锁定
4					不活跃账号登录
5				用户注册	账号创建后未进行业务操作
6					账号创建后短时间删除
7					同一设备创建多个账号
8				访问账户信息	频繁查询账号信息但未进行过业务操作
9					更改账户认证信息失败
10			用户资产	支付行为	支付时间不在交易对象的常规营业时间
11					用户支付时间与历史数据异常
12					发生支付的商户类型异常
13					发生支付的对象类型异常
14					支付习惯异常
15					高于历史数据的单笔大额支付
16					高于历史数据的单日支付总额
17					高于历史数据的月均支付总额
18					高于历史数据的支付频次
19					收货地址不在常用收货地址
20				转账行为	高于历史数据的单笔大额转账
21					高于历史数据的单日转账总额
22					高于历史数据的月均转账总额
23					高于历史数据的转账频次
24					转账习惯异常
25				虚拟资产操作	虚拟资产兑换的商户类型异常
26					虚拟资产兑换的对象类型异常
27					收货地址不在常用收货地址

4.对安全监控指标进行赋值计算

思路：

- 二元逻辑回归要求自变量和因变量均为离散数值，因此需对自变量和因变量进行二项赋值；
- 安全事件是否发生作为因变量，安全指标作为自变量；
- 采用专家经验和四分位赋值法对指标进行赋值。

优势：

- 赋值准确，结合历史数据排除异常因素干扰
- 专家经验，选取业务关键指标

指标判定及赋值示例

二项分布指标

根据质变的判定规则进行判断，符合判定规则的事件，赋值为1，未达到判定条件的，赋值为0.

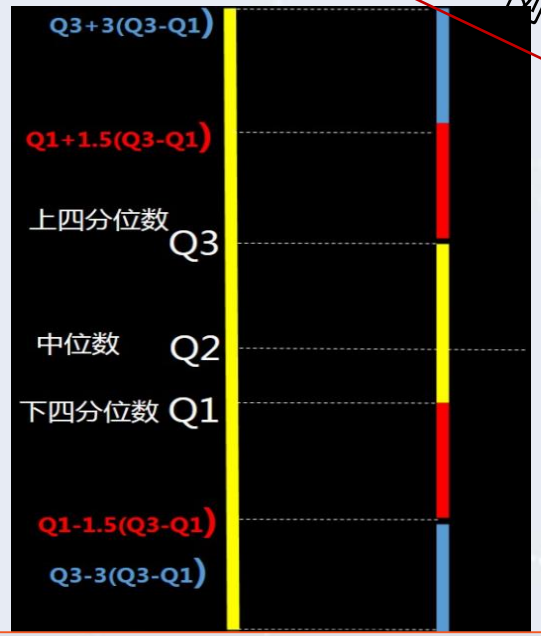
例如“登录地点改变”指标，当系统监控到用户本次登录的IP地址与上一次登录的IP地址发生变化时，该指标赋值1

历史区间指标

利用中位数，25/%分位数，75/%分位数，上边界，下边界等统计量来来描述数据的整体分布情况。通过计算这些统计量，生成一个箱体图，箱体包含了大部分的正常数据，而在箱体上边界和下边界之外的，就是异常数据。

例如“高于历史数据的单笔大额支付”指标，系统会对本次支付额度与历史支付额度统计数据进行对比，判断异常情况。

示例



四分位法示意图，红色为中度异常区间，蓝色为极度异常区间

5.通过大量情报数据，对模型进行训练

安全模型训练方法

历史安全告警记录

↓

参照指标集提取因变量

↓

因变量拟合分析

↓

有效指标/形成模型

因变量拟合分析

选取向后似然比方式进行因变量拟合。向后法则将所有自变量纳入模型，然后再往外剔除。相对来说向后法损失的信息较少。

选取数据分析算法

-二元逻辑回归算法：

-朴素贝叶斯算法：

-神经网络算法：

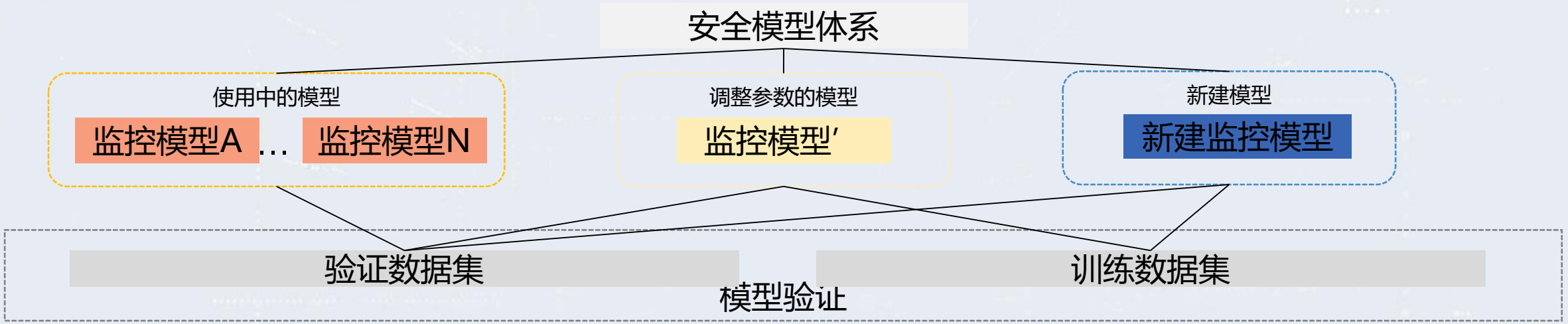
优势：

指标拟合过程中信息损失小，预测准确率高

示例

B	标准误差	瓦尔德	自由度	显著性	Exp(B)
-.029	.036	.650	1	.420	.971
-.014	.007	4.178	1	.041	.986
.646	.338	3.651	1	.056	1.908
.934	.395	5.588	1	.018	2.544
1.657	.682	5.894	1	.015	5.242
		6.986	2	.030	
-.903	.431	4.397	1	.036	.405
.295	.535	.303	1	.582	1.343
1.358	1.065	1.626	1	.202	3.889

6.对模型有效性进行验证，达到持续改进



精准区间

在该阈值范围的模型可判断为精准模型，继续使用

调优区间

在该阈值范围的模型可判断为待优化模型。调整参数后使用训练数据和验证数据进行验证，达到精准区间后可使用

废弃区间

在该阈值范围内的模型可判断为废弃模型，可能由于精度过低或被攻击者绕过失去监控预警效果

根据监控模型实际运行效果和企业的风险偏好，动态调整对模型精准度的判断标准，达到模型体系的动态调整和持续改进，从而更好的应对快速变化的外部安全威胁。


谢谢观赏！