



安全度量：构建企业安全评价体系之路

王宇

蚂蚁金服平台安全部总监

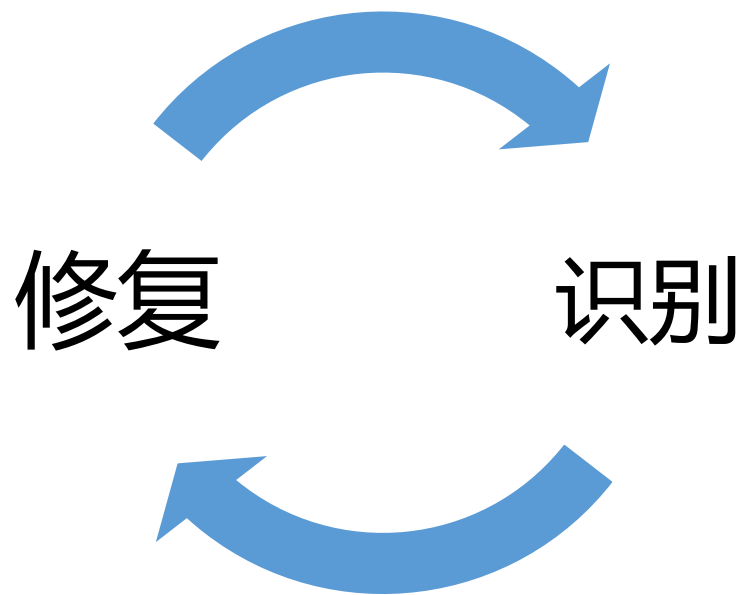
- 安全建设的困境
- 安全度量的意义
- 什么是好的度量体系
- 度量体系的建设思路
- 总结

来自C*O和业务方的“拷问”

- 安全防御有效性如何？
- 现在状况比去年更好么？
- 和同行做对比我们如何？
- 资金资源投入对不对？

来自自身的反思和疑问

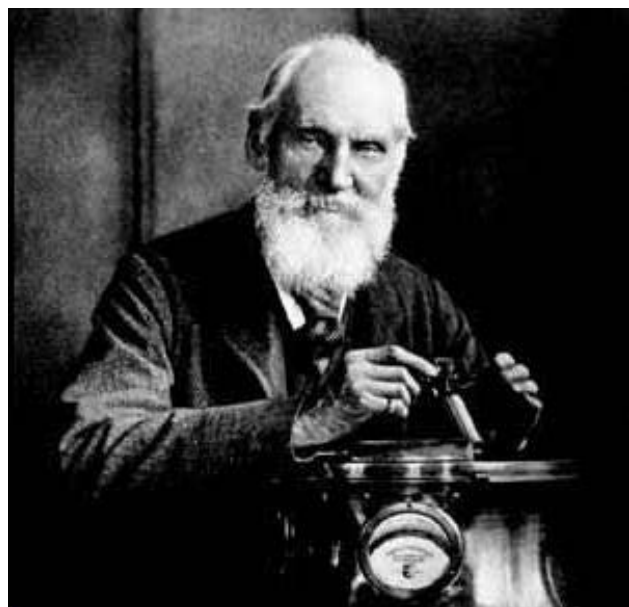
- 我的安全水位到底如何？
- 我能抵御住多大强度的对手？
- 我的当下投入重点和力度是恰当的么？
- 安全什么时候是个头？



识别风险到修复风险的无尽怪圈

提问->答案！，避免“安全是一种感觉”的陷阱

- 安全是一门实践性的学科，充斥着大量的不确定和含义模糊的概念
 - 常见过于关注琐碎的东西，而非全局
 - 现有评价体系过于模糊、非量化
 - 不能很好的支撑决策
- 安全预算大部分投入到产品，而不是运营或过程建设
 - 安全追求的是能力，而工具产品只是能力的载体
- 人们倾向去做最容易识别的问题



If you can not measure it,
you can not improve it

~ Lord Kelvin

安全度量是消除不安全感、不确定和疑虑的框架

- 定性的度量：做正确的事
 - 安全的价值
 - 投入焦点集中在能够增加价值的行为上
 - 一个软件加固的例子
- 定量的度量：明白我们在哪里
- 过程改进

- 与指标关注者息息相关，促使采取行动或决策
- 简单易懂，避免主观
- 自动采集、方便计算
- 数值或者百分比，避免高中低之类的“感性”标签
- 计量单位，如“漏洞数”、“小时”
- 不求全、体现现阶段关注重点，同时牵引整体安全建设

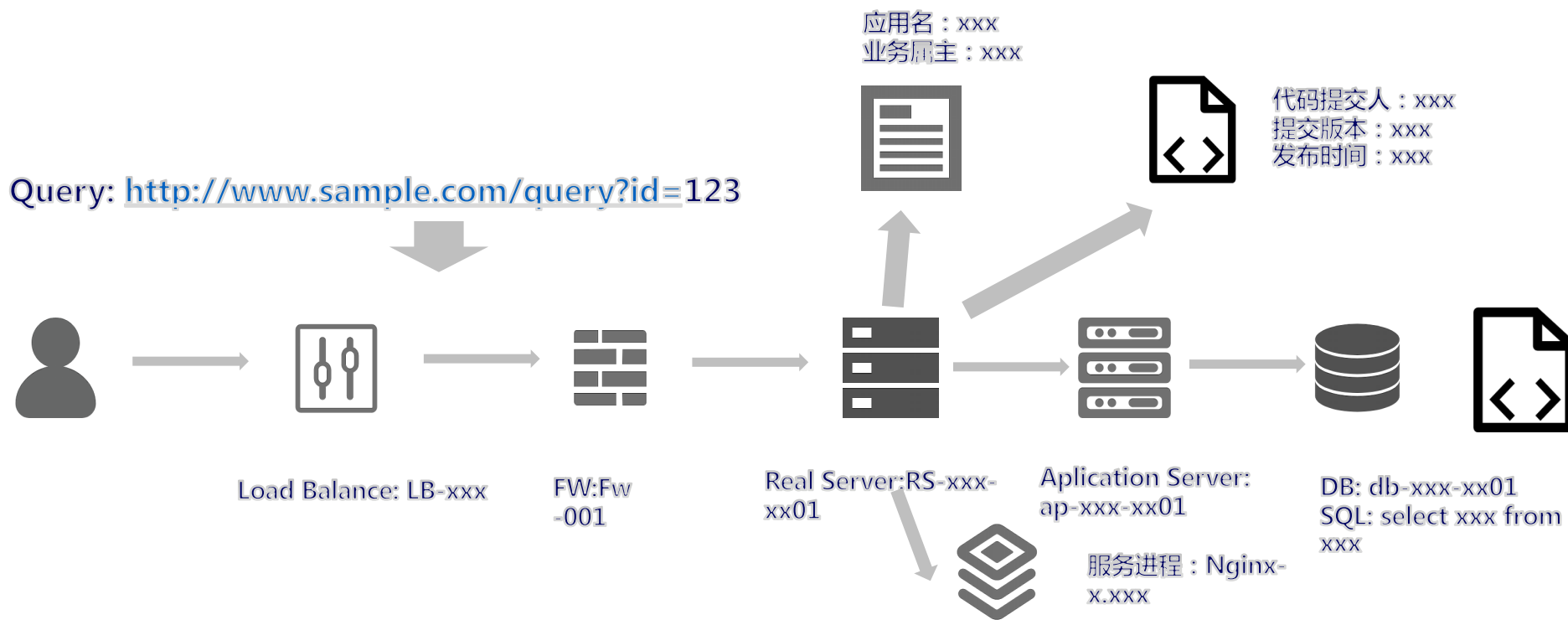
- 不通对象侧重点不同：CEO vs CISO vs SDL主管
- 指标大域分类
 - 防御能力水位
 - 覆盖和管控能力
 - 可用性、可靠性
 - 应用和业务风险

- 关注全局，突出核心能力并支持下钻：
 - 整体安全水位
 - 系统性风险
 - 资源投入和重心的产出
 - 我需要采取哪些行动帮助你？
- 举例：
 - 威胁感知率
 - 发现处置时常
 - 高危漏洞数
 - 员工违规数

细分领域指标：以安全资产平台为例

2019北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE



资产透明化, 自动化交叉验证, 资产覆盖率, 核心资产覆盖率

[illegible]

细分领域指标：以SDL为例

2019 北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE

应用名	千行代码 违规数 (下钻到人)	千行代码 漏洞数	线上漏洞 数	中高危漏 洞数	漏洞发现 渠道	漏洞类型	带伤时长	漏洞修复 率	漏洞超期 率	漏洞修复 时长	是否介入 调查	调查结论
xxx1	10	3	5	1	主动测试	XXE	1D	80%	10%	120min	Y	XXX
xxx2	5	1	3	0	SRC	CORS	15min	90%	0%	15min	N	

分析视角：

- 员工研发安全意识
- 线上产品质量
- 风险敞口



- 威胁感知率
- 风险处置能力
- 风险自主发现率

引导其他指标update

细分领域指标：以入侵检测为例

2019 北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE

系统平台指标度量

日志源	覆盖基数	覆盖率	送达率	平均时延	完整性	核心系统基数	核心系统覆盖率	核心系统送达率	平均时延	最新版比率
HIDS	1000000	95%	95%(+1%)	5min	99%(+1%)	1000	97%(-1%)	99%	1min	50%
...										

检测处置能力度量

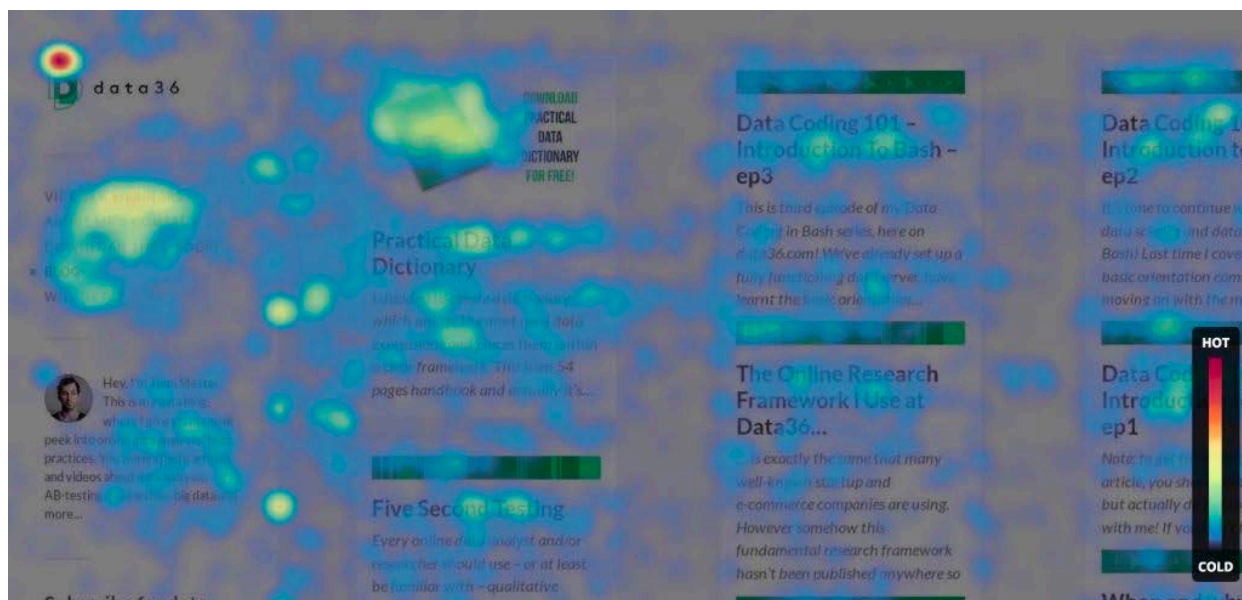
日志源	可见能力矩阵	检测能力比率	平均发现时间	最长发现时间	平均响应时间	最长响应时间

- 既要也要还要
 - 避免单指标项导致的重心偏移
 - 漏洞检出率 vs 主动发现率
- 三方计数和多维度比对
- 红蓝对抗验证

- 员工安全意识
 - 安全常识：安全敏感性
- 研发安全意识
 - “愚蠢” 编码设计问题的发生概率
- 运维安全意识
 - 违规操作比率
- 特殊工种安全意识
 - 重点风险识别和违规数

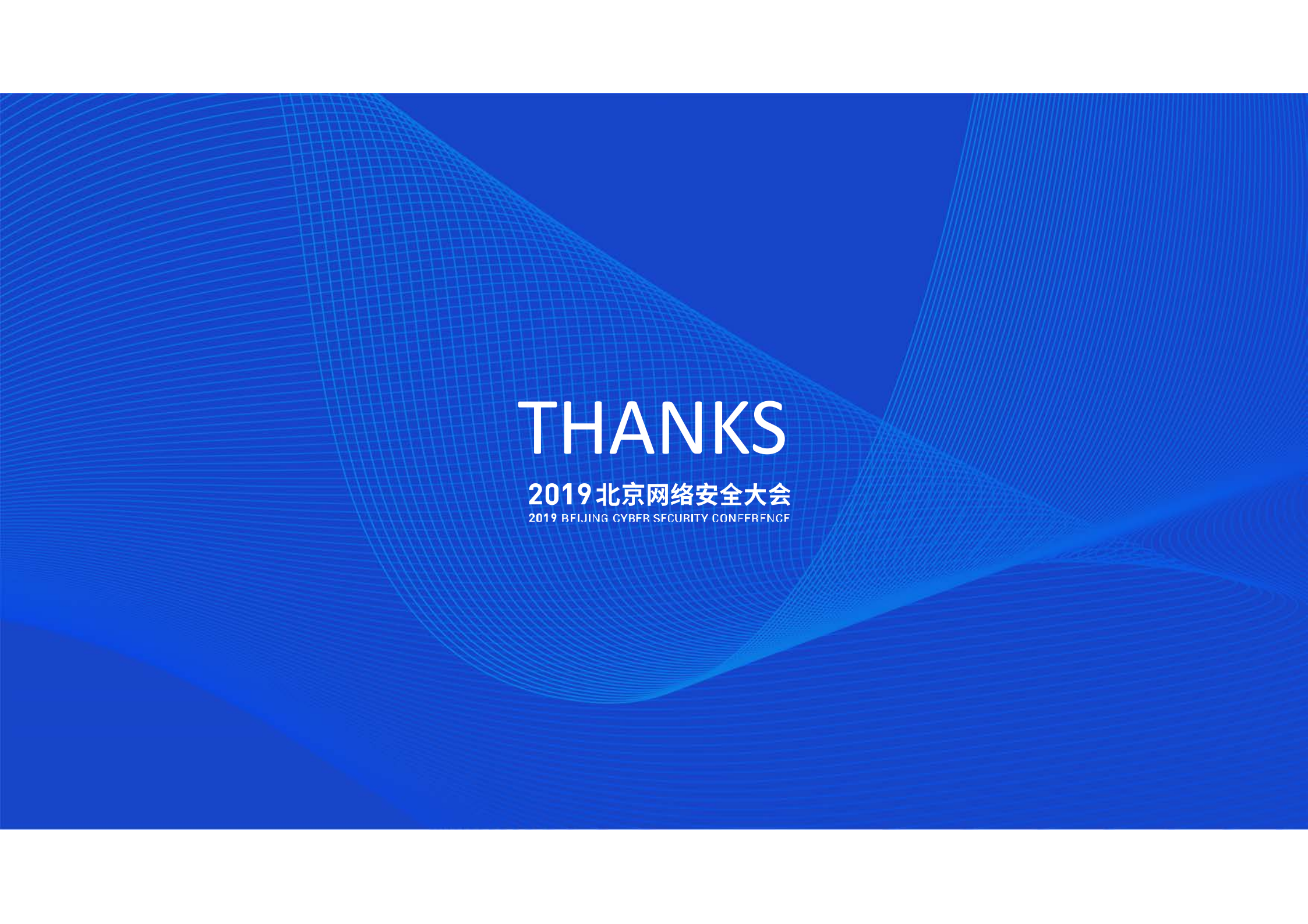
跨领域学习：微观度量的一个例子

2019 北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE



热力图可以帮助提升运营效率

- 安全度量是消除恐惧、不确定和疑虑的框架
- 针对不同的受众，需要采取不同的安全度量角度和维度
- 好的安全指标简单易懂、稳定，且易于计算，并能牵引多项安全能力建设
- 交叉学科的引入，会有有效的提升指标能力

The background is a solid blue color with a subtle, abstract pattern of thin, light blue lines that form a grid or mesh-like structure, particularly visible on the left side where it curves around the text.

THANKS

2019 北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE