关注企业安全最后一公里

金融行业企业安全建设

安信证券 • 聂君

目 录
CONTENTS

安全观安全

安全本质

- 互联网本来是安全的，自从有了研究安全的人，就变得不安全了
- 信任。计算机用0和1定义整个世界，而企业的信息安全问题是解决0和1之间的广大灰度数据，运用各种措施，将灰度数据识别为0（不值得信任），或1（值得信任）
- 不同的信任假设决定了安全方案的复杂程度和实施成本，安全需要平衡

安全观安全·安全原则

持续改进

纵深防御

非对称

安全世界观

信息安全就是博弈和对抗，是一场人与人之间的战争。交战双方所争夺的都是信息资产的控制权，也就是在博弈和对抗中，牢牢的把控住各类信息资产的控制权。

正确处理几个关系

科学与艺术

管理与技术

业务与安全

目 录
CONTENTS

企业安全需求

- 体系化的安全防护措施和技术手段，如安全域隔离。初级SDL和代码安全检视能力，对应用交付有自主评估和修补能力
- 非自身发现的互联网应用安全漏洞小于一定数量，对互联网网站等高风险系统具备一定的态势感知和未知漏洞防护能力
- 内部系统能够有效防止非专业人员有意或者无意的数据泄露，能发现对重要服务器和高价值终端的普通内部黑客攻击
- 满足监管合规要求，建设外规到内规，内规到检查，检查到整改的合规链，内部违规违纪和内外部安全审计发现持续降低

面临的问题

企业安全的内容是什么

安全服务质量保持在稳定区间

安全工程化能力

企业安全的内容是什么

安全服务质量保持在稳定区间

安全工程化能力

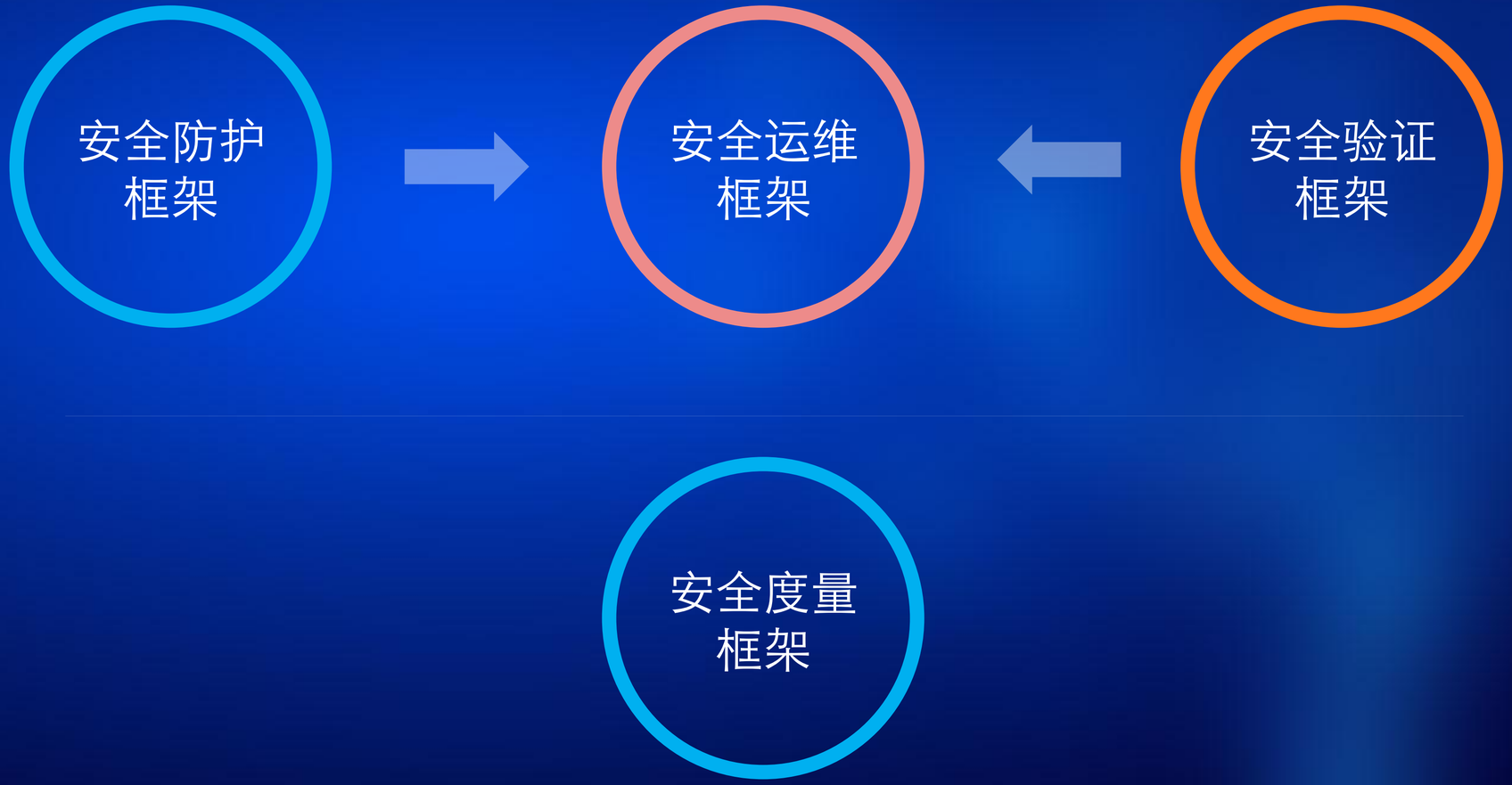
安全运营的思路

架构

工具

资源

安全运营架构



架构·安全防护框架

纵深防御

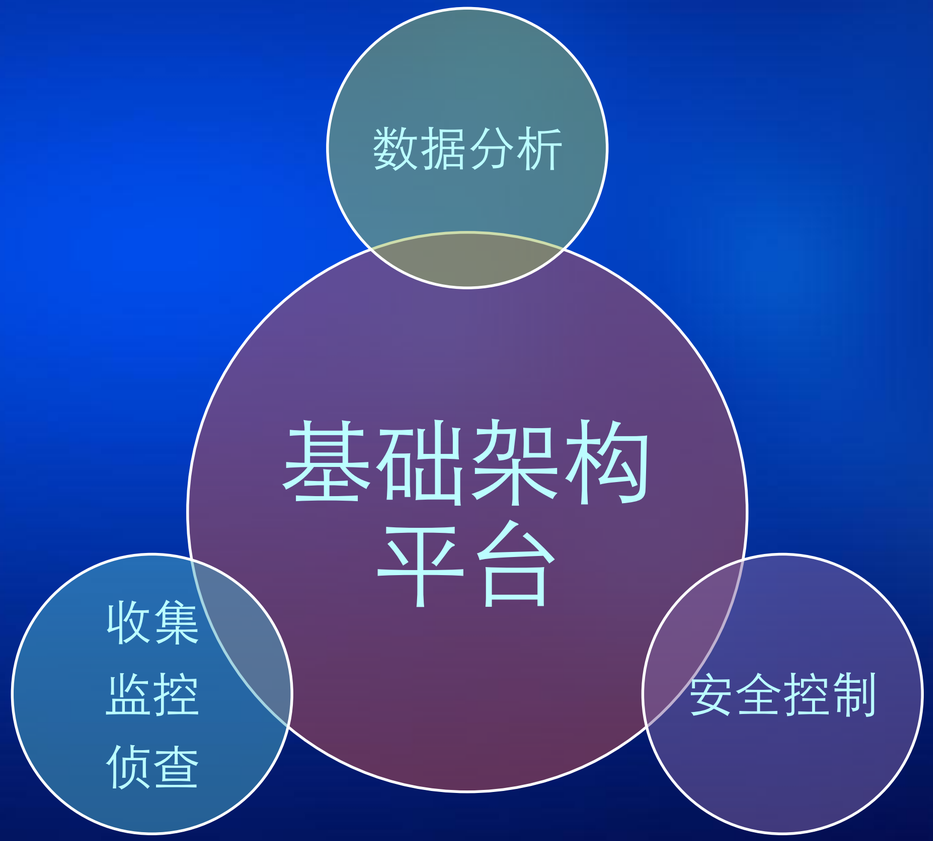
安全总控层安全	日志统一管理、SOC安全总控中心
用户层安全管控	安全客户端、双重身份认证、堡垒机
数据层安全管控	数据库防护，数据据防泄漏、邮件DLP、文印系统
应用层安全管控	开发安全规范、应用防护，网站防篡改 应用层漏洞扫描，安全控件
系统层安全管控	安全基线、恶意软件检测，异常流量， 系统漏洞扫描，蜜罐、终端安全管理
虚拟层安全管控	虚拟层安全防护、虚拟主机安全加固
网络层安全管控	安全域划分、防火墙，异常流量 入侵检测防御，信道加密，DNS防护

架构·企业安全领域

- ①网络安全
- ②平台和业务安全
- ③广义的信息安全
- ④IT风险管理、IT审计&内控
- ⑤业务持续性管理
- ⑥安全品牌营销、渠道维护
- ⑦CXO们的其他需求

传统行业，建议做①③④⑤
对于互联网公司，建议做①②⑤
金融行业，我建议做①③④，能力强的安全团队，建议做①③④⑥⑦。

架构·安全运维框架



架构·安全验证框架

- 白盒检测（过程验证）
- 黑盒检测（结果验证）

安全验证框架·白盒检测

- 白盒检测（过程验证）

① 验证安全Sensor安全监测功能有效；
② 验证安全Sensor所产生监测信息到SIEM平台的信息采集有效；
③ 验证SIEM平台的安全检测规则有效；
④ 验证告警方式（邮件、短信与可视化　展示平台）有效

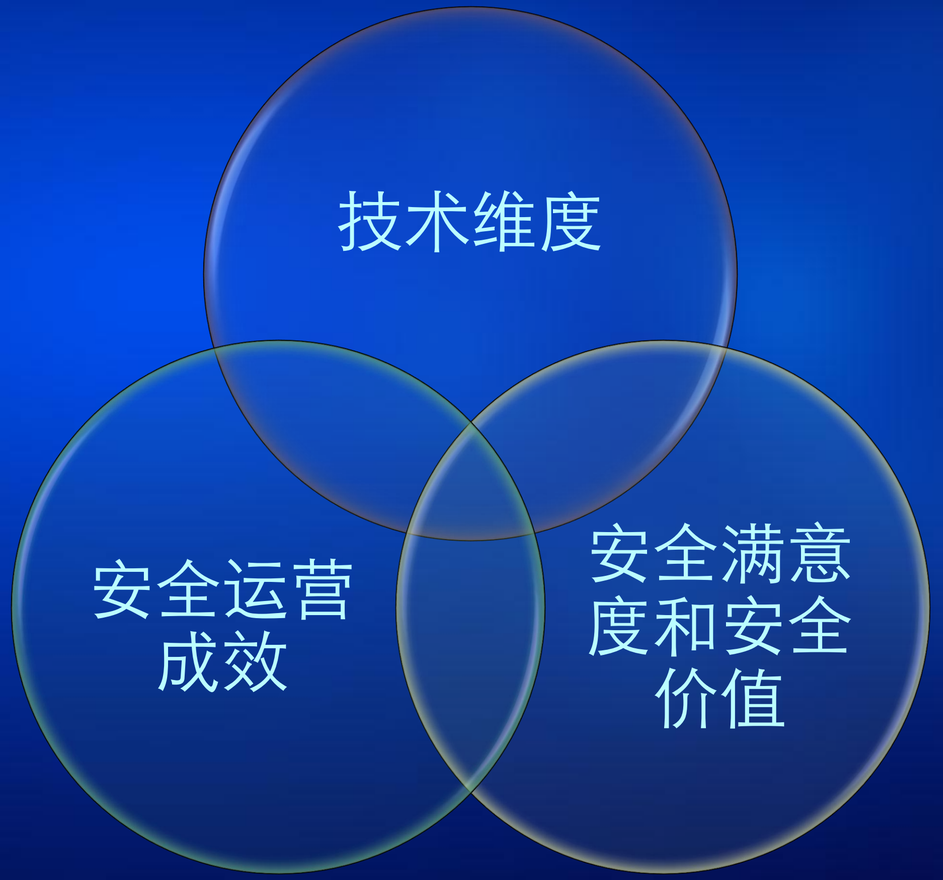
安全验证框架·黑盒检测

- 黑盒检测（结果验证）

① 安全众测

① 红蓝对抗演习

架构·安全度量框架



度量·安全为业务服务

- 减少资损（创收）
- 降低系统性能压力（降本）
- 智能预警威胁感知（提效）
- 同人模型降低安全交付认证复杂度（提升用户体验）
- 安全应急和危机公关（保持和提升品牌公信力）
- 积累风险库和模型反驱动业务规则优化（反欺诈、降低坏账等）

比如风控系统做好了，以前需要发验证码的交易，现在不用发了。提升客户体验，验证码费用大幅降低。某行风控系统上线后，动码发送率降低七成。短时间节约几千万费用

安全运营的工具

SIEM平台

标准化流程工具

安全控制自动化工具

工具·SIEM规则

① 单一检测条件规则

某个shell进程的cwd和exe组合起来不是/usr/sbin/sshd -> 可疑shell连接

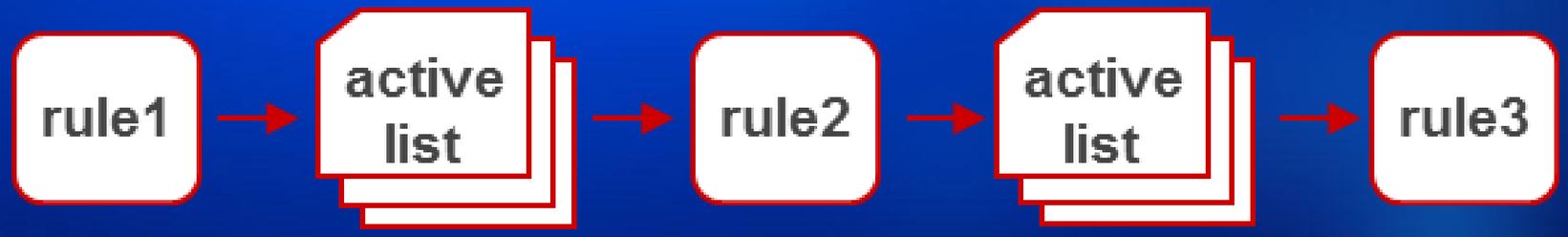
工具·SIEM规则

② 跨平台安全监测信息关联检测

防火墙Permit日志中Dst包含威胁情报注入的恶意IP或域名->木马等恶意软件?

工具·SIEM规则

③ 针对长时间缓慢低频度攻击的检测规则



内网单台机器对同一个域名的查询达到某个阈值（如10分钟内1000个查询）->DNS Tunnel?

工具·SIEM健康度监控

- **SIEM健康度**

① 安全监测信息采集器失效
② SIEM检测规则失效；
③ 安全告警失效；
④ 安全告警处理失效；

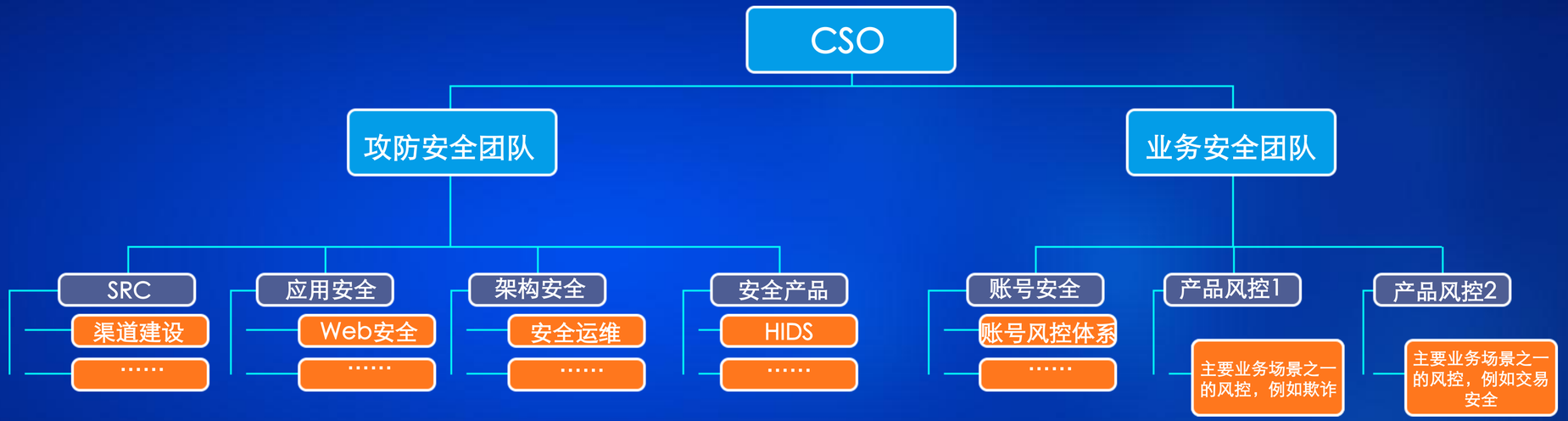
- Sensor的安全性

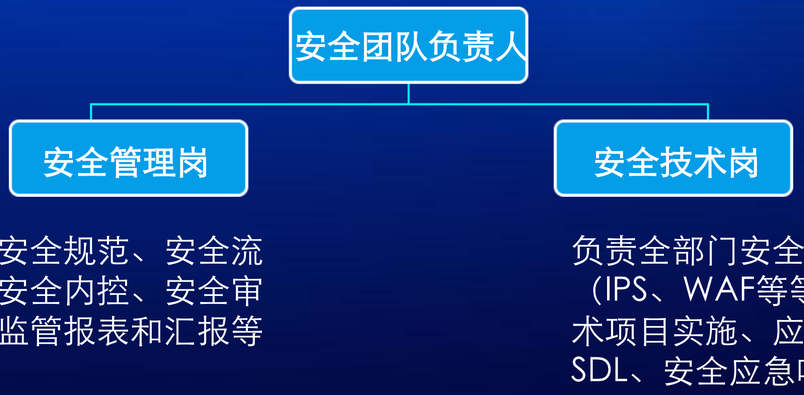
① 控制指令仅允许固化的指令，严禁在Sensor端预留执行系统命令接口；
② 更新包必须经过审核之后上传至更新Server保存，更新仅允许选择更新Server上已有的安装包，最好校验更新包的MD5；
③ 控制指令下发时必须人工审核确认后才执行；

资源·流程与机制

- 安全事件处理流程
- 安全运营持续改进流程

资源·组织与人员





负责安全制度、安全规范、安全流程、安全检查、安全内控、安全审计、安全月报、监管报表和汇报等

负责全部门安全设备日常运维（IPS、WAF等等）、安全防护技术项目实施、应用上线安全检测、SDL、安全应急响应等

目 录
CONTENTS

企业安全建设思考

- 安全运营
- 安全趋势
- 安全合规
- 安全考核
- 安全汇报

安全运营的思考

难点

失效

白名单
Or
黑名单

什么样的安全
和安全运营

➢难点·为什么SOC容易失败

- 企业自身基础设施成熟度不高
- 安全运维不能包治百病
- 难以坚持

思考·安全检测为什么会失效

- 单点检测深度不足
- 覆盖率不足
- 安全运维平台可用性出了问题
- 告警质量问题
- 人的问题

➢思考·白名单还是黑名单

- 黑名单的优点：假阳性较低，认知理解容易；
  缺点：漏报率高，靠概率和运气；
- 白名单的缺点：假阳性较高，运营成本高，
  所以需要安全检测具有自学习能力，形成自
  动或半自动可收敛的安全检测规则；
- 白名单可能会越来越受到重视

➢思考·需要什么样的安全和安全运营

- 适合自己的就是最好的
- 投入和收益比最大
- 企业安全建设三个阶段

①基础安全建设；
②系统建设阶段；
③安全高阶建设。

思考·安全运营成熟度

- 一级：自发级
- 二级：基础级
- 三级：自动化级
- 四级：智能级
- 五级：天网级

需求是一辆自行车，结果来了一辆专机

思考·安全趋势

安全度量

历史问题免疫

安全成为属性

思考·安全合规

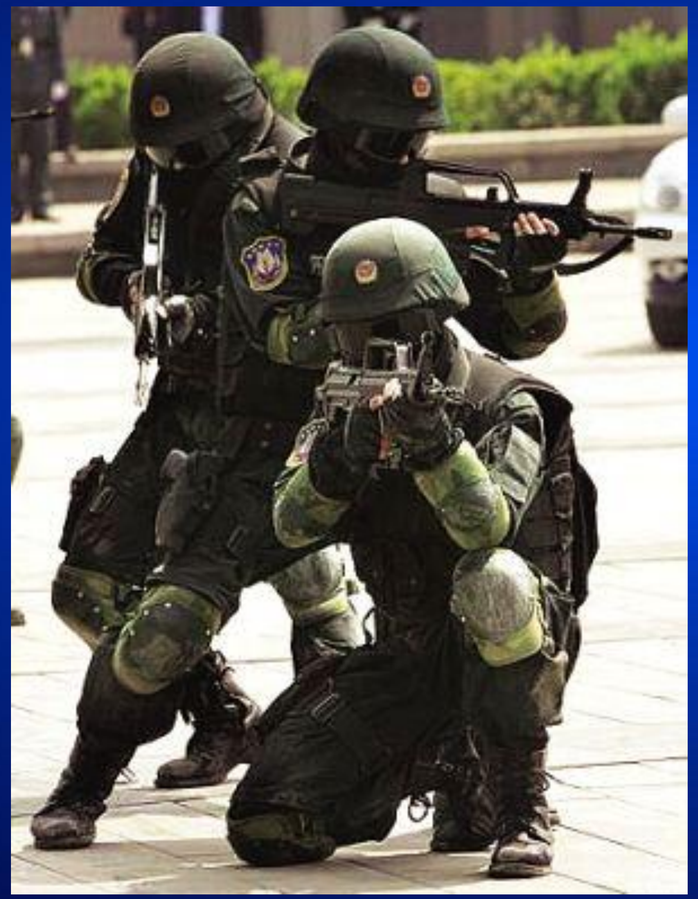
- 低成本、有效
- 一套体系，各路神仙
- 外规到内规，内规到检查、检查到整改，整改到考核的合规链

思考·安全考核

- 平行团队考核
- 安全团队考核

思考·安全汇报

- 高级管理层
- IT部门、总经理
- 安全团队



世界变好了吗

反恐，越反越恐！

关于我

好读书，不求甚解，足球、军事，兴趣广泛。

金融业企业安全建设微信群

有兴趣加入的朋友请关注微信公众号“君哥的体历”（扫右侧二维码），后台留言，**微信号+公司名称**，验证身份后入群。

和我交流·君哥的体历

人生最美好的莫过于各种经历和难忘的体验，过程比较痛苦的，结果都还比较好。如果大家和我一样，在企业做安全中遇到各种颇为“痛苦”的体历，过后你一定会感谢和怀念这份体历的。

聂君·君哥的体历