OWASP 中国 Open Worldwide Application Security Project

OWASP 中国 | 北京分会 Open Worldwide Application Security Project

网安加社区

探真科技 TensorSecurity

开源网安 SECZONE GROUP

BrainAu 脑动极光 BRAINAU

安全系统建设的挑战与解决方案

演讲人：柯徐亭

2024 OWASP中国安全技术论坛

全球视野下的网络安全趋势

目录
CONTENTS

安全系统建设的甲乙方

① 职责的变迁

甲方：从交付到运营

乙方：从签约到交付

② 考核的变迁

甲方：从降低成本到提升价值

乙方：从考核收入到考核利润

③ 能力的变迁

甲方：从专业到系统架构、项目管理

乙方：从产品功能理解到解决方案

安全系统建设的甲乙方

	甲方	乙方
从甲方视角看	• 需求永远是合理的，哪怕是没考虑清楚的需求蔓延或变更 • 专业、负责、可信任 • 付钱的上帝	• 不专业、不负责、不可信任； • 唯利是图、评估人天吓死人 • 签约前天花乱坠、执行中认清现实、执行后悄无声息
从乙方视角看	• 对业内最佳实践缺乏了解，沉浸在个性化需求中； • 怕承担责任，不敢签字 • 经常需求变更，说不清楚流程和需求	• 专业、负责、可信任 • 方案引领甲方、业内资深的企业和专家身份 • 成熟的实施方法论

安全系统建设中的挑战

- 人的因素永远是最重要的，再多的正确抵不过授权和信任；
- 抛弃技术思维，回到项目实施方法论里；
- 做安全系统建设的监理方，构建甲乙方平等双赢。

- 甲方的安全系统规划是优先事务，整合是必然发生的；
- 每一次接触都在进行供应商评价，被否决可能只是一次迟到；
- 一个契合甲方行业、公司、需求的案例胜过一百个高逼格客户案例。

- 如何体现运营能力；
- 如何进行三权分立；
- 如何处理供应商关系。

安全系统选型期解决方案

需求调研

平衡安全目标、业务需求和管理层期望

综合评估系统功能、性能、兼容性、可扩展性和灵活性

解决方案

乙方拜访

考察供应商的技术支持能力、成功案例和客户反馈

分析POC结果，评估系统是否满足需求，同时提出改进建议

POC验证

案例交流

了解实施过程中的挑战、解决方案、及最佳实践

确保数据安全、明确责任和SLA、评估合同条款的合理性

合同条款

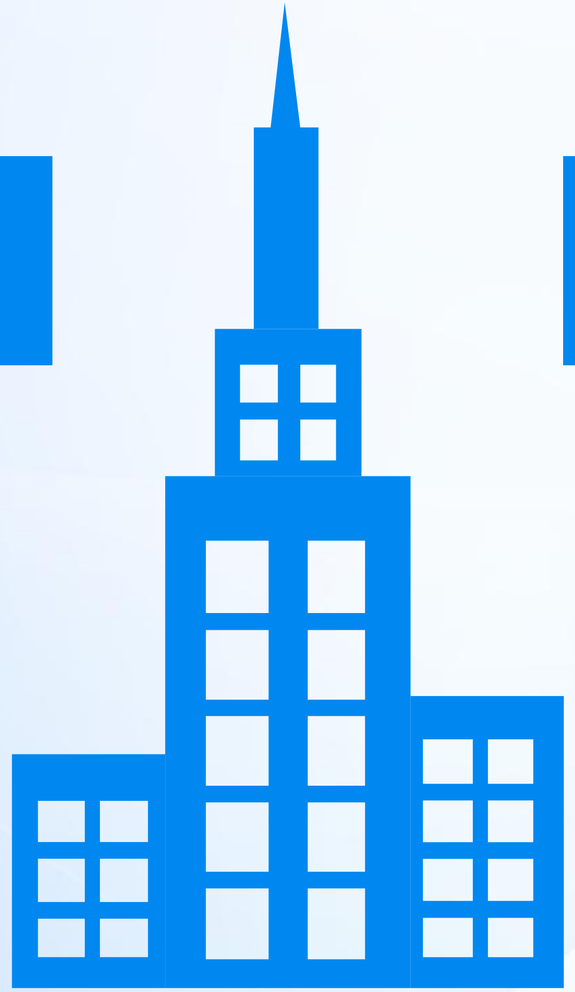
安全系统实施期解决方案

管理层授权

获得高层对项目的支持和资源承诺、明确项目目标和优先级、确保项目符合公司战略方向

干系人沟通

确定所有相关干系人并建立沟通渠道、定期更新项目进展和关键决策、收集反馈并及时调整项目计划



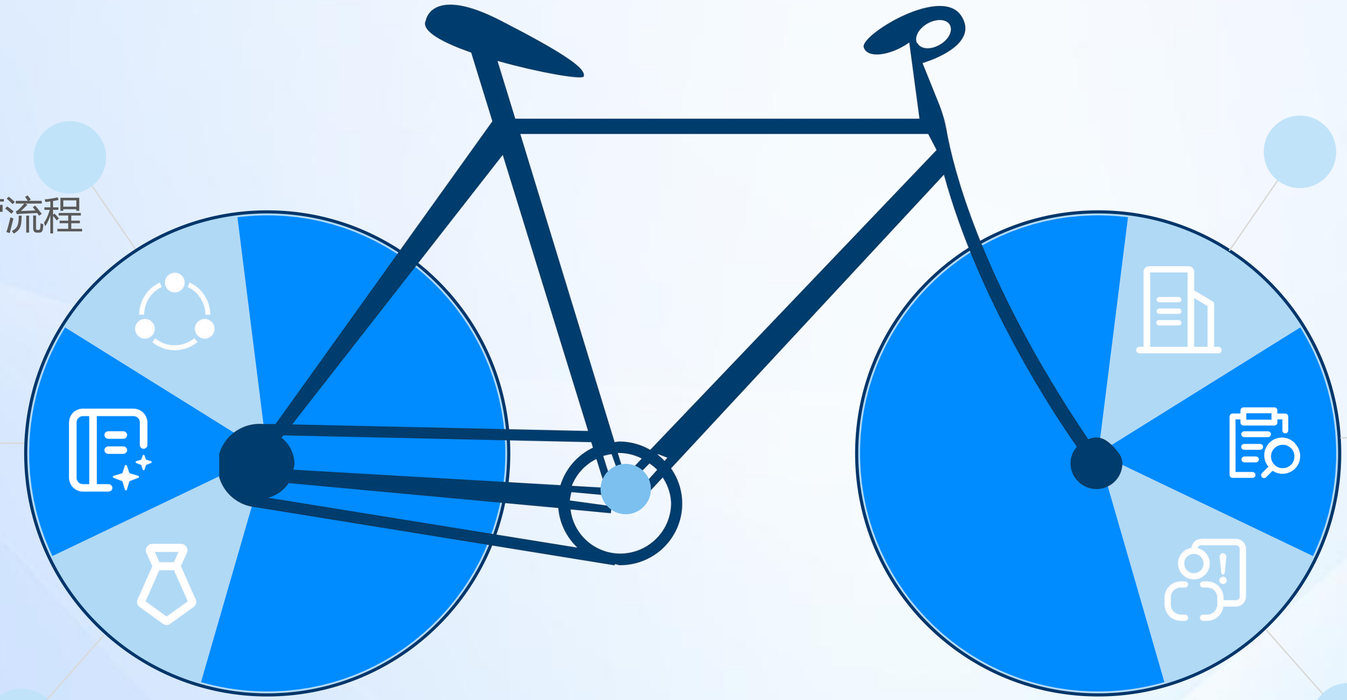
可行WBS

将项目分解为可管理的任务和阶段、明确每个任务的目标、时间和资源需求、确保计划具有灵活性以应对变化

分步骤实施

按优先级逐步部署解决方案、在每个阶段结束后进行评估和调整、确保每一步都符合预期的质量和标准

安全系统运营期解决方案



运营自洽

建立能够逻辑自洽的安全运营流程

深入系统

了解系统、学习系统、用好系统

做好服务

当好一线服务台

厂商管理

ITIL的思路管理好厂商或代理商

内部控制

借鉴ITSOX把系统的内部控制做好

价值提升

系统操作、流程优化、系统运营

OWASP 中国 Open Worldwide Application Security Project

OWASP 中国 | 北京分会 Open Worldwide Application Security Project

网安加社区

探真科技 TensorSecurity

开源网安 SECZONE GROUP

BrainAu 脑动极光 BRAINAU

THANKS

感谢您的观看

2024 OWASP中国安全技术论坛

全球视野下的网络安全趋势