中小型互联网企业网络安全建设实践

黄鹏华(PH22)

目录

CONTENTS

01 网络安全现状

02 网络安全建设的体系化思考

03 网络安全建设的实践

04 工作推进中的一些思考

OWASP
Open Web Application Security Project

01

网络安全的现状

OWASP
Open Web Application Security Project

网络安全的现状

国家间的网络战

2010年6月首次被检测出来的震网（Stuxnet）蠕虫病毒，第一个专门定向攻击真实世界中基础（能源）设施的“蠕虫”病毒

2019年3月7日晚，委内瑞拉发生了大面积停电事件，全国大范围陷入黑暗。

合规监管

2017年6月1日正式实施的《中华人民共和国网络安全法》

2019年12月1日要正式实施的等保2.0

安全事件频发

2013年雅虎30亿账户信息泄漏

2018年万豪集团旗下的喜达屋酒店客房预定信息泄漏

OWASP
Open Web Application Security Project

02

网络安全建设的体系化思考

OWASP
Open Web Application
Security Project

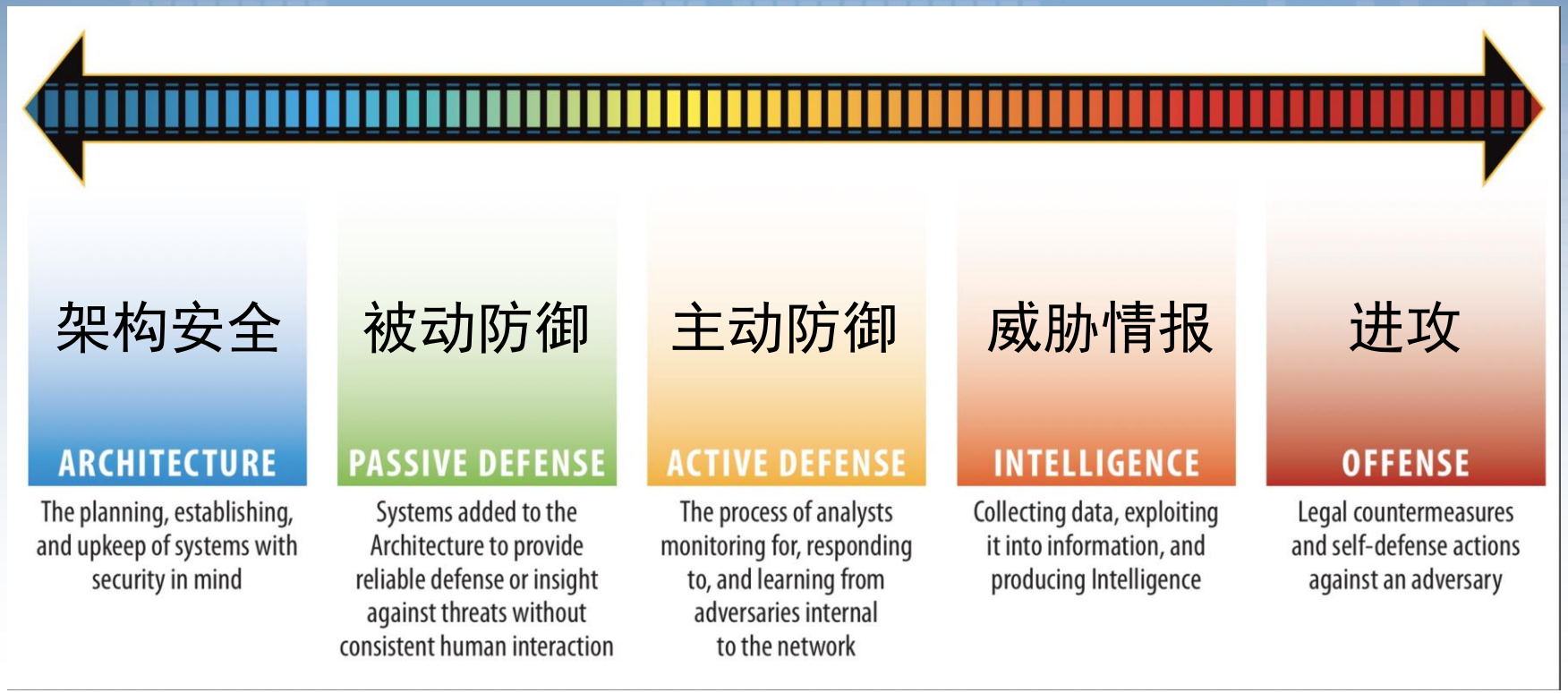
网络安全建设的体系化思考

- 全局思考面临的安全风险
- 明确安全建设的目标
- 指导安全建设有序进行
- 不断积累不断优化完善

OWASP
Open Web Application Security Project

网络安全滑动标尺模型

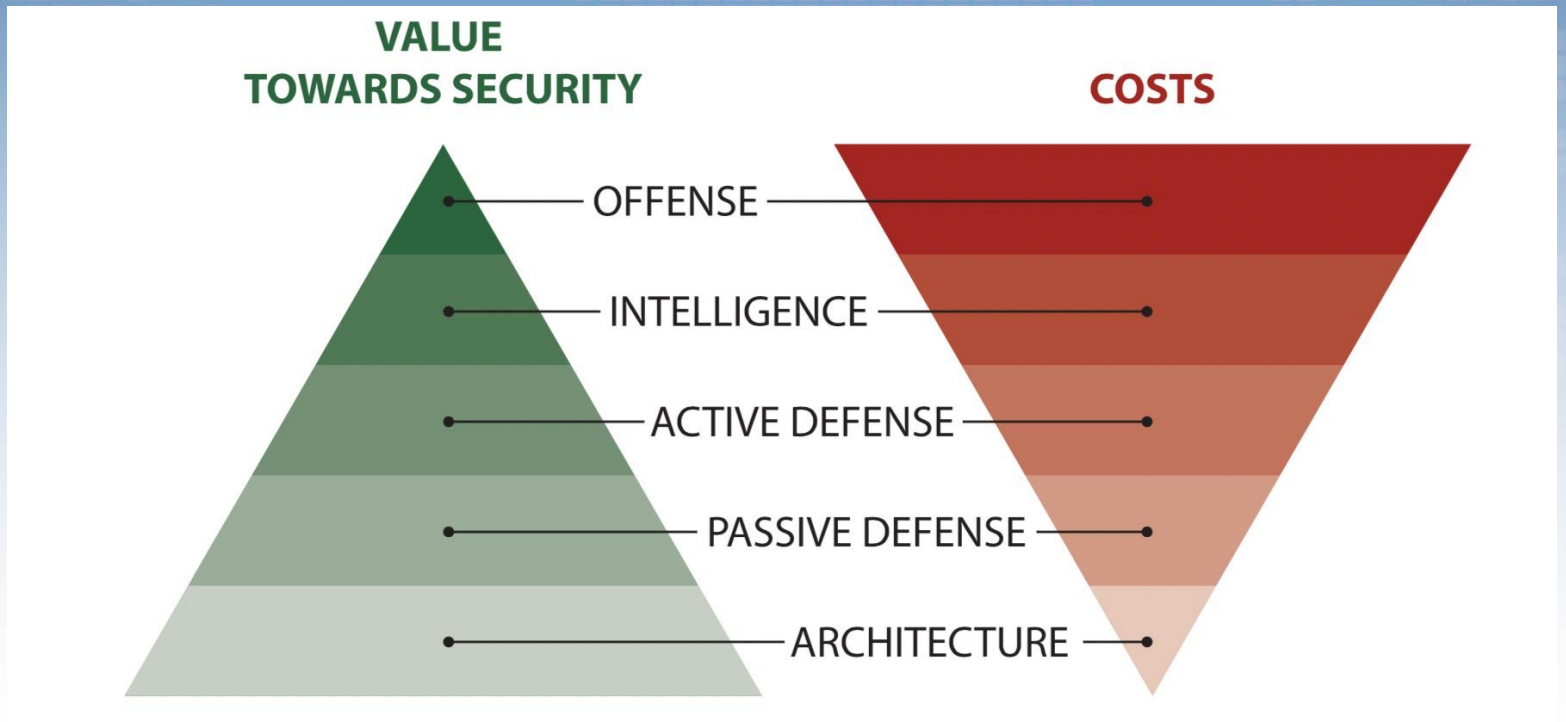
OWASP
Open Web Application Security Project



网络安全滑动标尺模型

- 左侧是右侧的基础，没有高低之分
- 从左往右投入的成本逐渐递增
- 从左往右应对更高级别的网络威胁

网络安全滑动标尺模型



安全价值投入与成本的关系

03

网络安全建设实践

OWASP
Open Web Application Security Project

互联网安全建设的要求

- 没有银弹，漏洞不能避免，提高攻击者入侵成本
- “唯快不破”：快速响应，快速恢复，快速溯源
- 影响可感知：不影响业务的正常运行

OWASP
Open Web Application Security Project

网络安全建设的原则

- 纵深防御
- 多维防御
- 河防思想
- 持续安全运营，闭环优化

OWASP
Open Web Application Security Project

多维防御

- 不局限在单一维护的防护能力
- 同一个攻击多个维度检测和防护

网络资产梳理

- 网络设备资产
- 主机资产
- 应用资产
- 运维的CMDB联动
- 网络资产探测

OWASP
Open Web Application Security Project

安全巡检系统

- 主机端口资产探测
- 弱口令扫描
- 漏洞POC验证
- 外围探测扫描

OWASP
Open Web Application Security Project

WEB应用防火墙(WAF)

- 配置管理、规则管理
- 报表、日志管理
- CC攻击防御
- 与业务安全联动
- 机器学习的探索

OWASP
Open Web Application Security Project

主机入侵检测系统(HIDS)

- 资产采集：进程监控、端口监控、网络连接
- 日志收集：主机日志、应用日志
- 入侵检测：rootkit、webshell、virtualtotal、文件完整性检测
- 合规基线：等保三级基线检查

OWASP
Open Web Application Security Project

自动化漏洞扫描

- 集成到CI发布流程，代码提交自动触发
- 上层封装支持多种扫描器切换
- 支持POC验证
- 一票否决：漏扫不通过不予发布

OWASP
Open Web Application Security Project

安全运营中心

- 分阶段，层层推进
- 日志集中管理：主机日志、应用日志、业务日志
- 基础功能：异常告警、应急响应
- 高级功能：自动化响应、威胁情报、溯源

OWASP
Open Web Application Security Project

应急响应-PDCERF模型

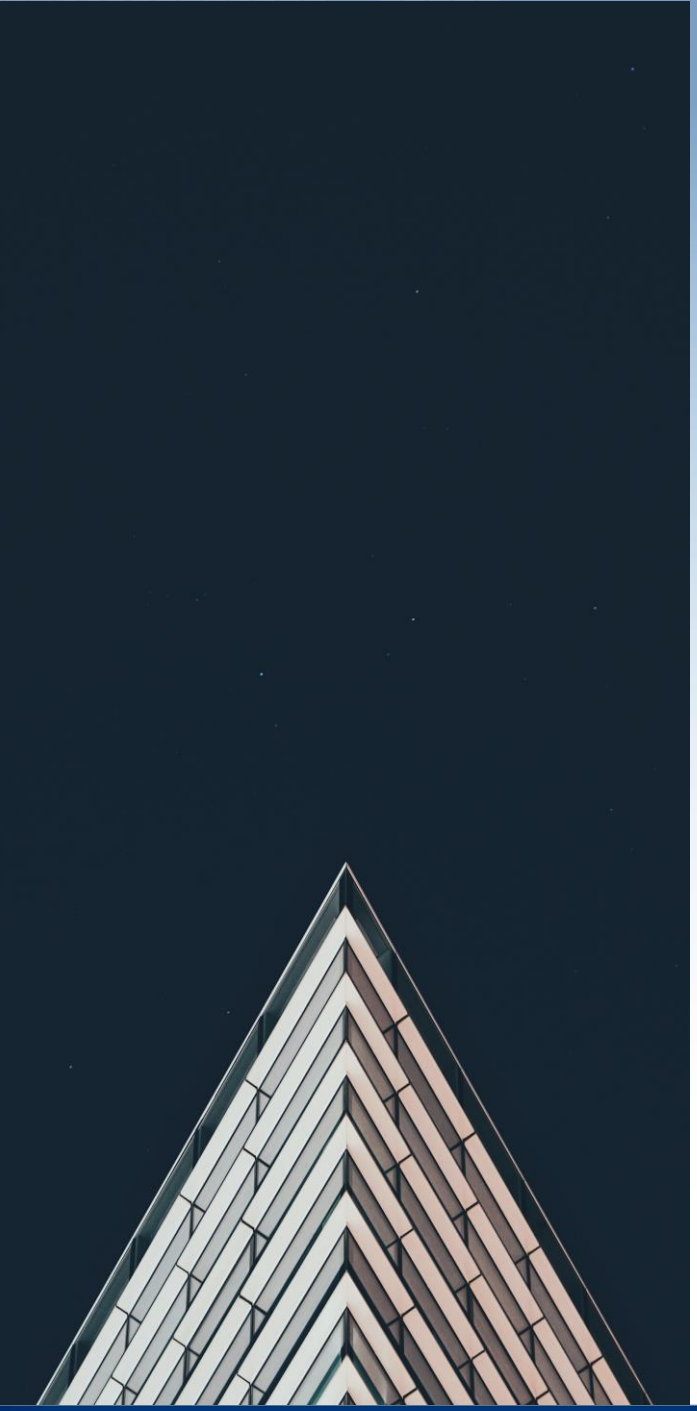
准备阶段　检测阶段　抑制阶段　根除阶段　恢复阶段　跟踪阶段

OWASP
Open Web Application Security Project

安全运营

- 持续运营，告警优化
- 保障各安全措施正常运行
- 持续用蓝军验证防护能力

OWASP
Open Web Application Security Project



04

工作推进中的一些思考

OWASP
Open Web Application Security Project

PDCA戴明环

ACTION 处理

PLAN 计划

CHECK 检查

DO 实施

OWASP
Open Web Application Security Project

工作推进中的一些思考

- 安全工作获得领导认可，向上管理
- 和谐良好的沟通推进安全工作
- 安全服务于业务，保障业务可持续性
- 手中有锤，心中无锤

OWASP
Open Web Application Security Project

OWASP
Open Web Application Security Project

谢谢观看