安全解决方案@安心投

1 WEB应用安全整体解决方案

安心投现状分析

- 网站随时可能DDOS、CC的攻击。
- 本次被攻击是因为受到互联网漏洞影响，可能造成了数据丢失。
- 阿里云盾防护可能出现潜在的误拦截。
- 安全运维制度不够完善，应急处理经验不足。
- 没有对主要业务定期进行安全检查。

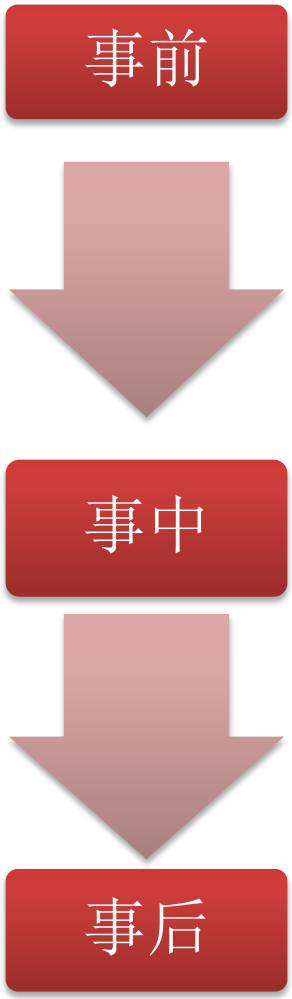
特针对如上问题制定全面的安全解决方案。

WEB应用安全整体解决方案

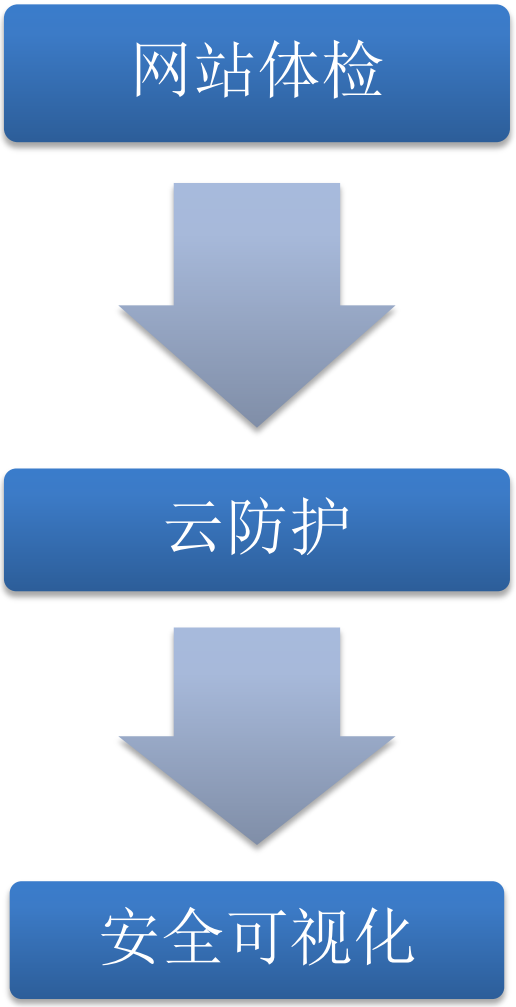
攻击来源

1. 来自于竞争对手雇佣黑客进行攻击
2. 小黑客好奇，显示自己的技术能力
3. 黑客通过对用户网站的攻击，向用户索要钱财

未来应用安全整体规划



=

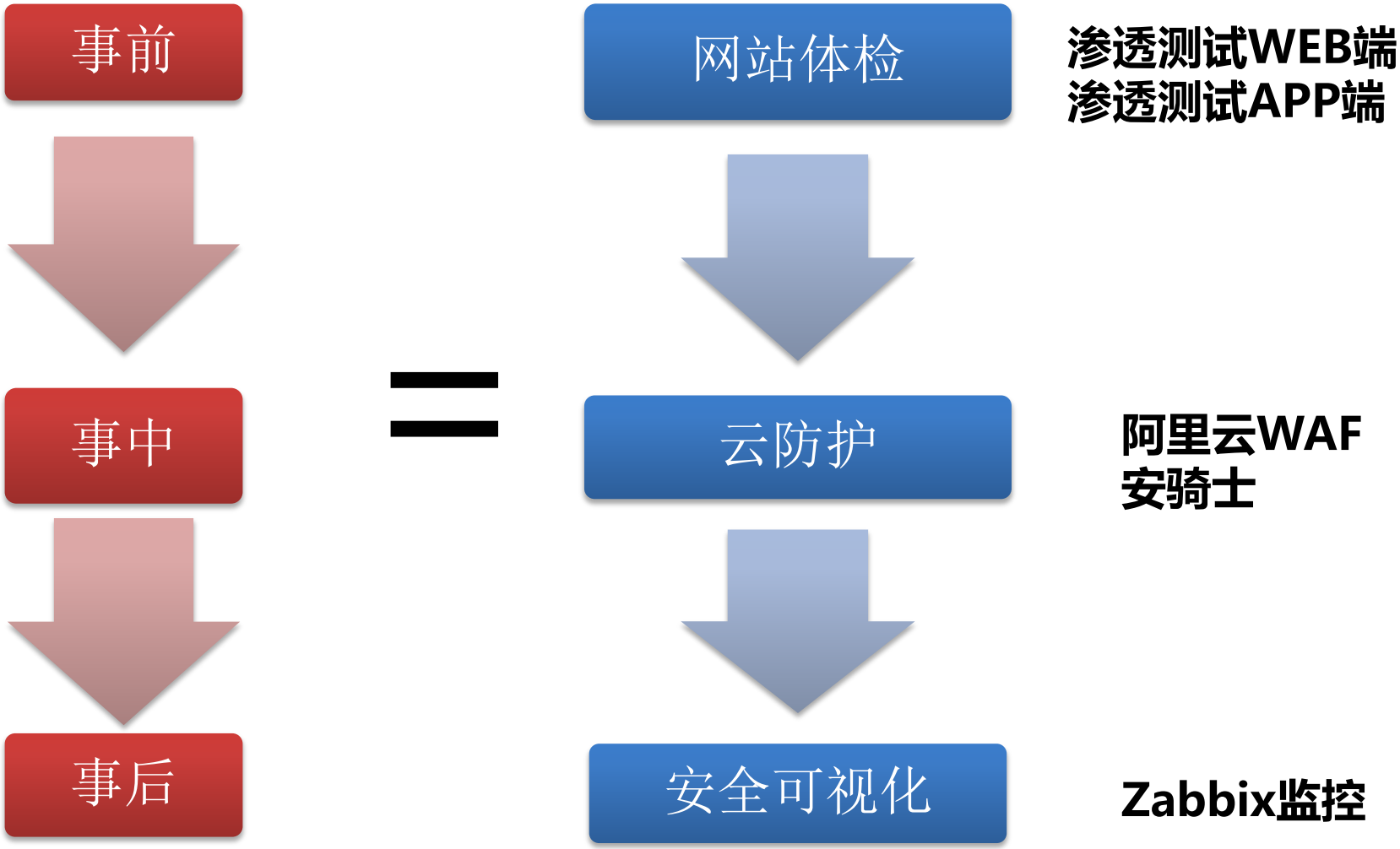


渗透测试WEB/APP
扫描器日常扫描
撞库测试
应急演练
安全意识培训
行业安全资讯

云WAF企业版
抗DDOS服务
CDN

安全报表
应急响应服务
入侵检测
风控、反欺诈
异地灾备

根据现状的建议解决方案



根据现状的建议解决方案描述

1.根据现状，我司应在阿里云上准备一个备用公网IP，当方式攻击时及时切换IP。

2.建议进行一年四次的网站渗透测试，一年两次的APP渗透测试或有重大版本迭代时提前进行渗透测试。

3.根据业务流量的增加，当阿里云上WEB服务器超过15+台时应筹备切换至IDC机房。

4.如进行市场活动宣传或重大活动时应注意防范DDOS攻击，必要时购买DDOS防御服务。

5.定期对阿里云的日志进行查看，发现未知问题要及时处理。

6.当在云盾发现每日多次的SQL注入、XSS等攻击时要注意有可能黑客已经在尝试绕过，需更换独立云WAF设备。

7.针对最新发现的应用漏洞、WEB漏洞要及时更新补丁。

2 渗透测试服务介绍

专家人工服务

机器扫描的缺点

【漏洞扫描器】、【安全评估】等方法都是基于【Checkliset】的僵硬措施。真实的黑客入侵往往是从【Checklist】之外的地方突破，所以很多通过了安全标准认证的公司仍然被黑

机器扫描的缺点

漏洞扫描器

1. 许多登录后页面、验证码页面无法扫描到
2. 大部分扫描器无法检测Ajax、Flash安全扫描器无法检测业务逻辑漏洞
3. Checklist式的安全检查方式无法对猜解密码，或者社工进行检测
4. 无法有效反映漏洞的危害程度

渗透测试

像黑客一样思考

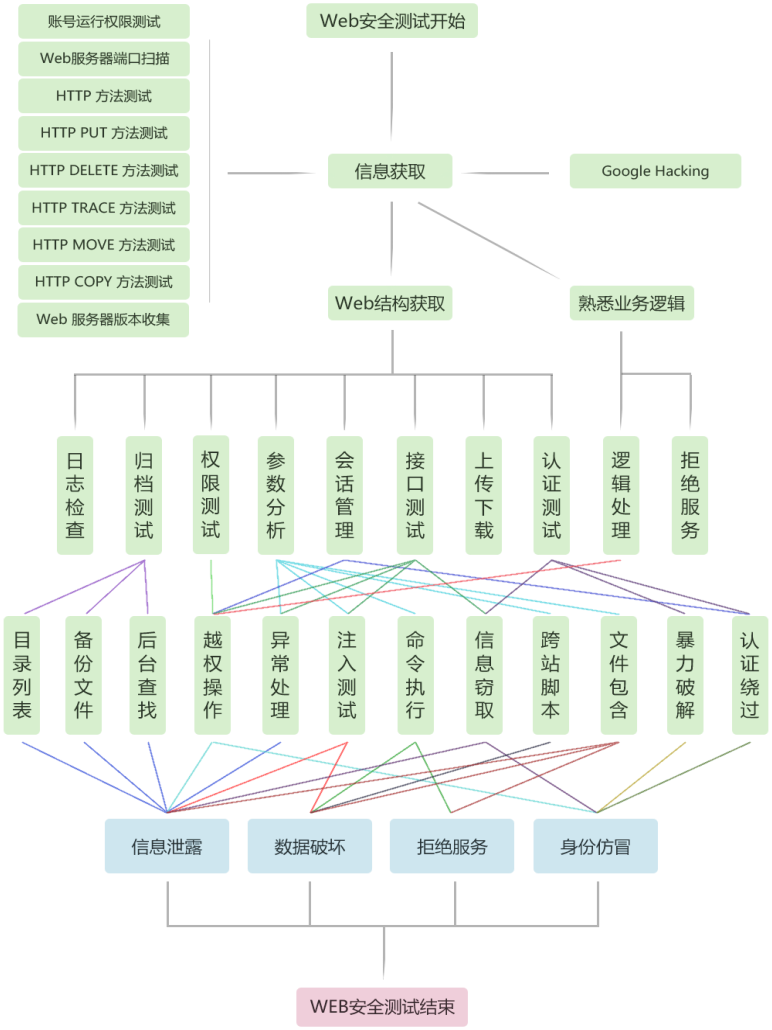
渗透测试服务是在用户的授权之下，完全模拟黑客的行为，对客户网站进行入侵尝试。帮助用户理解黑客是如何思考的，比黑客更早发现问题

渗透测试

渗透测试

1. 真实验证每个漏洞的危害大小
2. 有效验证网站是否可被黑客入侵
3. 找到安全标准的「checklist」之外的薄弱点，这是真正的威胁。

渗透测试



真实验证每个漏洞的危害大小

渗透测试服务尝试利用每一个漏洞获取【敏感数据】【管理后台】【服务器权限】让你真正理解漏洞危害的大小。7个工作日完成一次渗透并提供报告。

渗透测试

值得信赖的团队

具有丰富安全行业经验的渗透团队

主要渗透技术工具和手段都是最先进和流行的

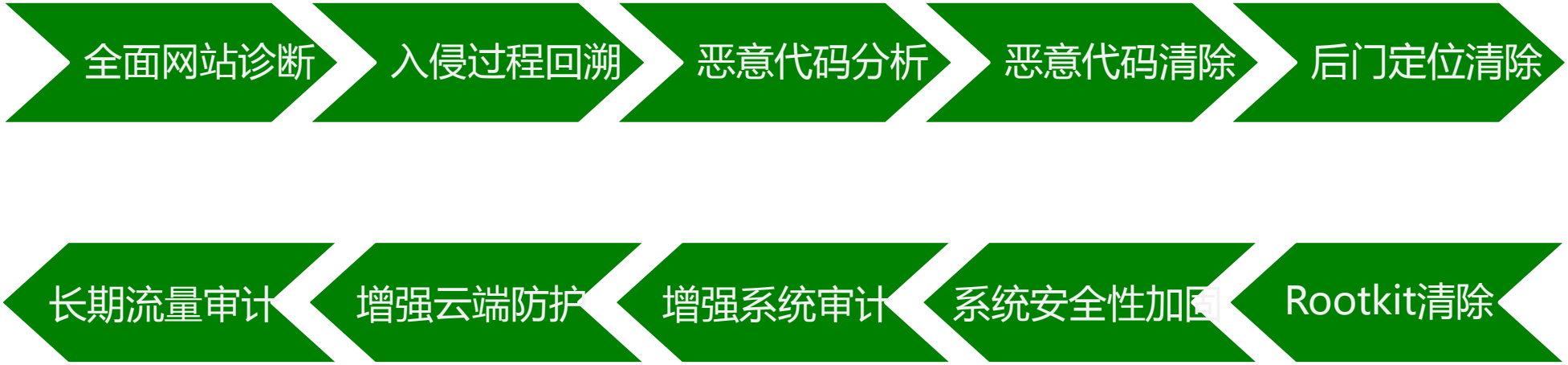
坚持每一次渗透测试都是由安全专家手动实施

根据测试结果提出可实施性强的专业修复建议

应急响应服务

客户的网站遭受黑客入侵后，由安全专家进行远程或现场的事件处理服务。主要服务内容包括后门清除 ，日志分析以找到黑客利用的漏洞，安全修复建议

应急响应服务流程


全面网站诊断
入侵过程回溯
恶意代码分析
恶意代码清除
后门定位清除
长期流量审计
增强云端防护
增强系统审计
系统安全性加固
Rootkit清除

服务价格

服务名称	单位	单价	备注
WEB渗透测试服务	1次	35000	包含一个主域名下的所有子域名，购买4次8折。
APP渗透测试服务	1次	40000	200个API接口之内，购买4次8折。
应急响应服务	1次	35000	5台WEB服务器之内