



AHsec安全服务是通过专业的技术手段，采用立体、模块化的标准服务体系，为企业量身订制个性化的安全服务，帮助中小企业用户以最少的成本，防患企业信息安全风险，实现事前可控，事中可管、事后可追溯的全方位安全防护体系。

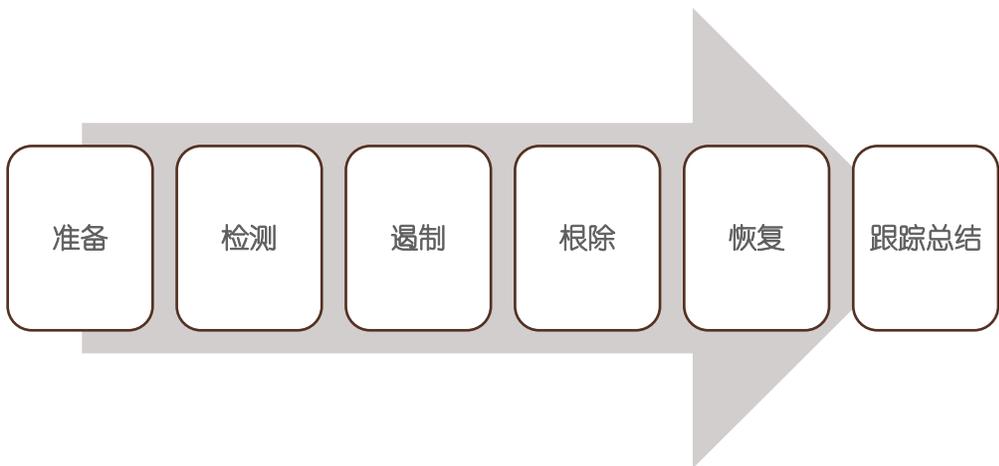


## 应急响应

### EMERGENCY RESPONSE

通过对信息系统的网络安全事件采取措施和行动，解决因0day漏洞、非法入侵、病毒感染等事件所造成的系统宕机、业务中断等事件，以便实现快速恢复整个信息系统的可用性及完整性。

- 一般性信息安全事件响应 (5\*8小时)
- 重大信息安全事件响应 (7\*24小时)
- 重大信息安全事件通告



## 安全加固

### SECURITY REINFORCE

通过高可靠、高扩展的建设原则，对信息系统统一规划设计、突出防护重点、实现技术和管理并重协同防护，保障业务系统的正常运行以便为企业带来价值。

- 配置加固服务
  - 补丁加固服务
  - 产品加固
- 
- 专业加固人员熟悉各类安全标准，一次加固多次通关
  - 高危加固项通过多次模拟测试，系统运行影响小。
  - 准备充分、案例详实，人员专业，加固时间减少30%



# 安全巡检

## SAFETY CHECKLIST

通过高可靠、高扩展的建设原则，对信息系统统一规划设计、突出防护重点、实现技术和管理并重协同防护，保障业务系统的正常运行以便为企业带来价值。

- 桌面系统安全巡检

- 防病毒系统巡检

- 系统补丁巡检



- 网络及系统设备巡检

- 应用系统安全巡检

- 信息基础环境巡视巡检

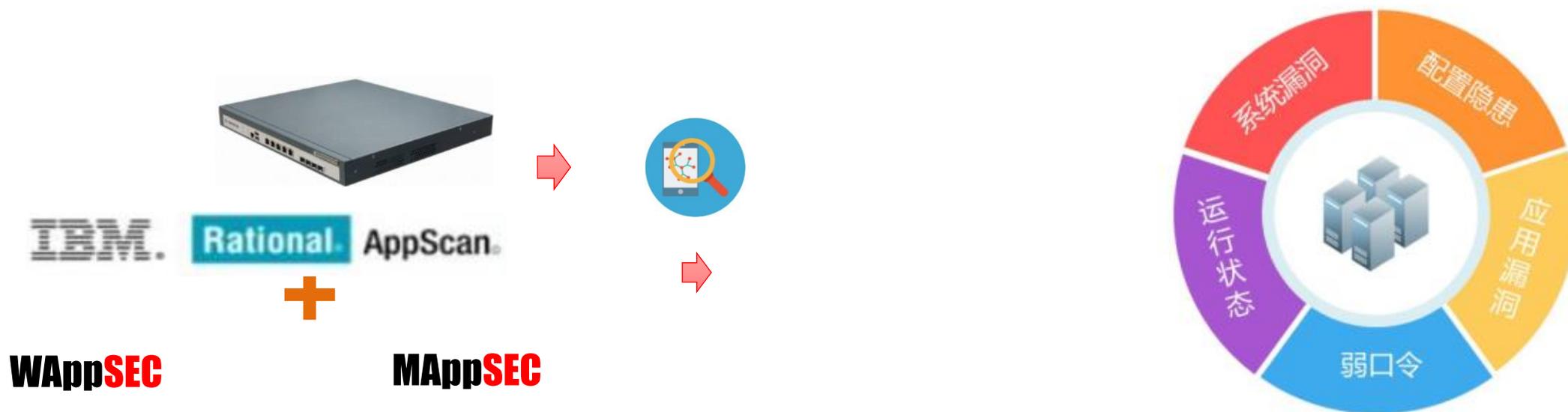
主机系统常见安全漏洞列表.pdf  
主机系统常见安全漏洞列表1.pdf  
SUSclient端设置说明.doc  
SUSclient端设置说明.pdf  
使用IP策略封目的端口139-443.pdf  
WSUS安装手册.pdf  
厂商技术支持资料列表.doc  
病毒事件应急处理工作指南.doc  
病毒事件应急处理工作指南.pdf

Solaris安全配置指南v0.9.doc  
Window2000系统安全配置指南.doc  
Window2003系统安全配置指南.doc  
Window2003系统安全配置指南V1[1].1.pdf  
IIS系统安全配置指南v0.9.doc  
SQL Server数据库系统安全配置指南v0.9.doc  
Windows桌面操作系统安装及初始化流程v0.9.doc  
Oracle数据库系统安全配置指南v0.9.doc  
AIX安全配置指南v0.9.doc  
安全服务部文件索引.pdf  
信息系统识别和描述操作指南.pdf  
应用系统安全检查操作指南v0.pdf  
XX操作系统安全检查操作指南v0.pdf

## 安全扫描

### SECURITY SCANNING

通过高可靠、高扩展的建设原则，对信息系统统一规划设计、突出防护重点、实现技术和管理并重协同防护，保障业务系统的正常运行以便为企业带来价值。



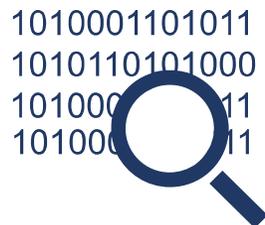
# 源码审核

## CODE INSPECTION

通过自动化及人工检查的方式对应用系统源代码进行检查，协助开发人员准确的查找和定位源代码中可能存在的编码缺陷及逻辑后门，从主动防御的角度出发，将安全隐患扼杀在萌芽状态。



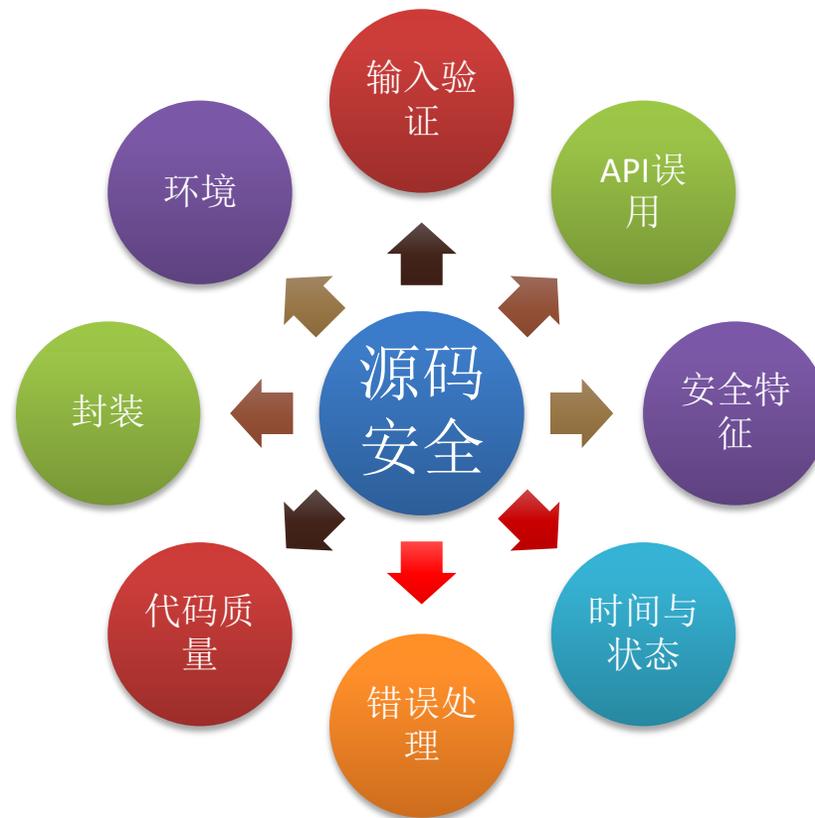
源代码



扫描工具



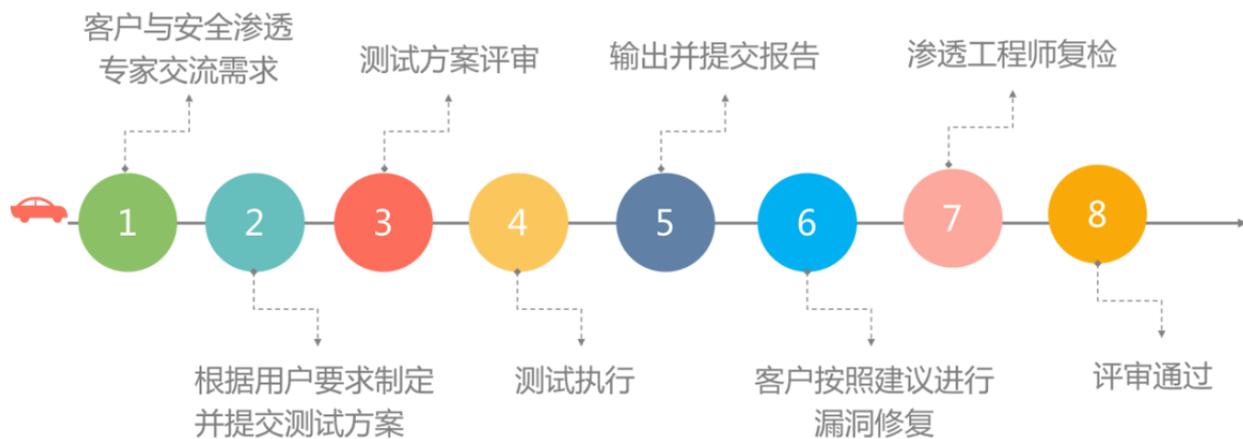
数据库



# 渗透测试

## PENETRATION TESTING

模拟恶意黑客攻击的方式，通过对系统存在的任何弱点、技术缺陷或漏洞的主动分析评估应用系统安全，协助系统管理人员准确找出信息系统存在的深度问题。



# APP检测

## APPLICATION CHECK

通过多种APP检测工具，对APP可能存在的安全漏洞（逆向反编译保护、漏洞检测、数据安全、算法安全、组件安全、接口安全等）进行检测，采用手工验证的方式确认安全问题并出具扫描报告。

 <h3>静态扫描</h3> <p>快速扫描APP，检测恶意特征</p> <p>静态分析样本，对样本进行特征扫描。支持Android应用程序与WindowsPhone应用程序。</p>	 <h3>静态代码分析</h3> <p>深度分析APP，检测敏感及恶意行为</p> <p>通过反编译等逆向手段静态分析样本，支持Android及WindowsPhone应用程序。扫描结果包括应用程序敏感行为、权限分析、敏感内容分析等。</p>	 <h3>动态行为检测</h3> <p>自动激活与APP行为记录</p> <p>在真机与虚拟机环境下自动激活与运行应用程序，监控应用程序运行时本地、网络行为，支持自动触发。</p>
 <h3>专项安全检测</h3> <p>内容安全与脆弱性分析</p> <p>支持应用程序内容安全检测，提供应用程序媒体文件提取及分析功能，支持图片的OCR识别；支持网络数据的实时抓取与展示。</p>	 <h3>源代码审计</h3> <p>针对源代的安全分析</p> <p>检查源代码中的缺点和错误信息，分析并找到这些问题引发的安全漏洞，并提供代码修订措施和建议。</p>	 <h3>综合判研</h3> <p>应用安全性综合评价</p> <p>综合静态扫描、代码分析及动态行为分析结果，综合分析应用分析安全性，支持人工辅助研判。</p>

以公开班、学术交流、企业现场培训、项目实施培训等方式，针对信息系统规划、设计、实施、运行维护等阶段的需要，可定制相关的课程。

- 安全意识培训
- 信息安全等级保护基础
- 信息安全法律和政策
- 信息安全标准介绍
- 信息安全等级保护定级指南

意识  
Awareness



- 物理安全测评
- 网络安全测评
- 数据库安全培训
- 主机安全测评
- 应用安全测评
- 渗透测评技术

技术  
Technology



- 信息安全保障基本实践
- 信息安全管理体系
- 信息安全风险管理
- 重要安全管理过程
- 信息安全工程原理
- 信息安全工程实践

管理  
Management



- 信息安全工程原理
- UNIX安全管理
- Windows系统安全
- 安全攻防
- 防火墙安全技术

职教  
Profession

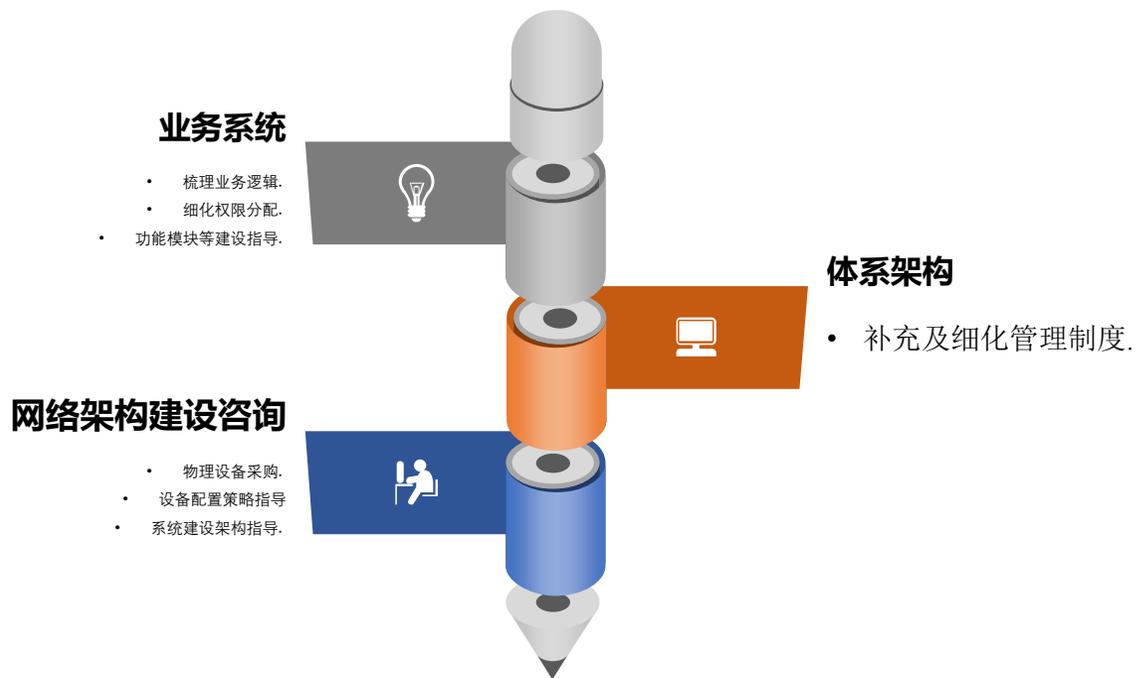


- CISP (第三方合作培训)
- CISSP (第三方合作培训)
- CISA (第三方合作培训)
- ITIL (第三方合作培训)

认证  
Certification



依据高可靠、高扩展的建设原则，对信息系统统一规划设计、突出防护重点、实现技术和管理并重协同防护，保障业务系统的正常运行以便为企业带来价值。



为规范企业的信息系统入网/上线/验收安全评估检查流程，通过入网/上线/验收安全检查，及时发现和消除存在的安全隐患，降低信息系统安全风险，保证信息系统符合等级保护或风险评估要求，保障信息系统安全稳定运行。

### 第三方开发及运营的系统 符合安全的要求吗？



### 等级保护二级整体解决方案套餐：

服务名称	服务内容	服务范围	服务次数	可交付成果	报价	
基于等级保护标准的风险评估	根据《信息系统安全等级保护基本要求》二级要求对信息系统开展测评	1个定级信息系统 (5台服务器)	采取实在察看、配置核查、工具测试和人员访谈等方式对信息系统网络与通信安全、设备与计算安全、应用和数据安全、安全管理策略等方面开展测评, 系统整体测评分析, 对不符合项给出整改建议, 综合测评结论, 编制测评报告	1	《差距测评报告》	60000
安全加固	1. 针对于 Windows、Linux 操作系统所发现的补丁漏洞进行修补 2. 依据信息安全等级保护三级要求, 对中间件、数据库、操作系统、网络设备进行配置加固	1个定级信息系统 (5台服务器)	补丁加固： 操作系统： Linux：ubuntu, centos, Redhat, debian, aix Windows：2003、2008、2012、2016 配置加固： 操作系统： Linux：ubuntu, centos, Redhat, debian, aix Windows：2003、2008、2012、2016 中间件：Tomcat、Apache、weblogic、websphere、IIS 数据库：SQL server、oracle、mysql、DB2 网络设备：防火墙、路由器、交换机、上网行为管理	1次	《加固报告》	12800
	WappSec 网站防护	1台 web 服务器	对 WEB 服务器中的 操作系统： Windows:2003、2008、2012、2016 Linux：CentOS/REDHAT、Ubuntu, SUSE 中间件 Tomcat:全版本支持、Apache：支持 2.0/2.2/2.4、Nginx: 支持 1.0-最新、IIS: 支持 6/7/8、Weblogic、Nginx	1年	《安全测试报告》	8000
等级保护验收测评	协调第三方测评机构为运营单位提供等级保护验收测评服务	1个定级信息系统 (5台服务器)	采取实在察看、配置核查、工具测试和人员访谈等方式对信息系统网络与通信安全、设备与计算安全、应用和数据安全、安全管理策略等方面开展测评, 系统整体测评分析, 对不符合项给出整改建议, 综合测评结论, 编制测评报告	1次	《测评报告》	60000
应急响应 (增强)	派遣技术工程师至现场进行事件协助处理、提供修复建议	3个 IP 设备	7*8 小时 中级：造成网络和系统速度下降、但仍可以工作、如果持续下去可能造成网络和系统无法工作的事件。如 DDOS 攻击事件。	1次 (两个工作日)	《安全事件报告表》	4000

# AHsec为科技护航



# AHsec为科技护航



**AHsec安全服务**  
专业 安全 共享

## 安鸿的初心

- 互联网服务安全评估机构

- 提供满足政府信息安全要求的一站式方案服务平台。
- 最具灵活的安全服务选购方案，全面解决IDC里应用系统安全问题。

AHsec

安全为科技护航

ICS 35.040  
A 90

GA

中华人民共和国公共安全行业标准

GA 1278—2015

信息安全技术  
互联网服务安全评估基本程序及要求

Information security technology—Basic procedures and  
requirements for internet service security evaluation