新零售安全解决方案

王晓东（麓飞）

无处不在的安全威胁

新零售以互联网为依托，对线上服务、线下体验以及现代物流进行深度融合的零售新模式，进而重塑业态结构与生态圈。因此新零售与我们每个人的生活息息相关，电商交易系统不仅存有海量的用户敏感数据，而且直接涉及到资金交易。因此，零售行业面临着多种多样的安全威胁。

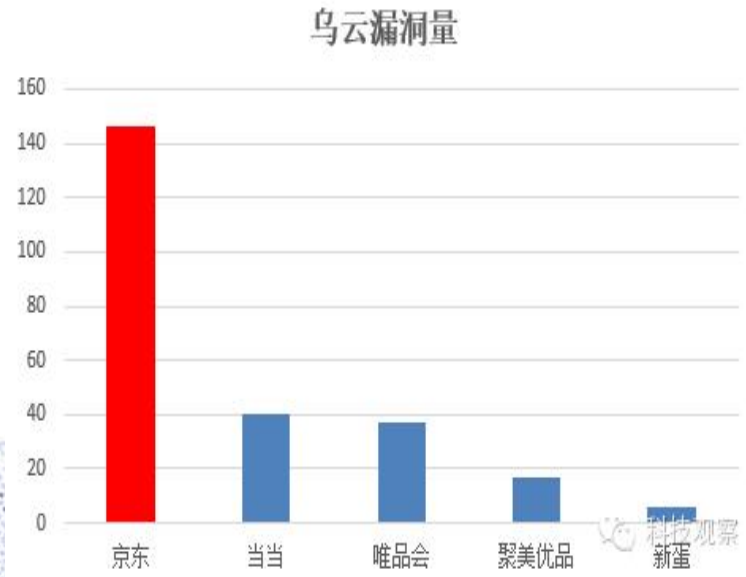
电商行业著名数据泄露

eBay遭黑客入侵，大量用户数据泄露

H3lvin 2014-05-22 +10 共115849人围观，发现 22 个不明物体 资讯

日前，据外媒报道，财

“1号店”等用户信息泄漏 互联网安全问题遭拷问



络 作者：我是大美女123

件已导致数百用户被

数百万。用户们已经准备对京东发起集体诉讼。维权成功与否先不谈，出于对京东安全现状以及对信息泄漏问题

者重点对两个问题进行了探究，一是京东安全做的如何？二是诈骗分子的京东订单数据从何而来？

京东安全做得如何呢？

笔者特地去漏洞报告平台乌云WooYun.org看个究竟：（京东漏洞在乌云平台的地址：http://www.wooyun.org/corps/%E4%BA%AC%E4%B8%9C%E5%95%86%E5%9F%8E）

京东存在的安全漏洞数量巨大

从漏洞报告平台的统计来看，京东总共有146条安全漏洞的记录，是其他同类网站的4倍以上。

WannaCry席卷全球，让
需要重新审视安全体系

2017年5月12号全球爆发大规模勒索软件WannaCry感染事件，我国大量行业企业内网大规模感染。截止到5月13日23时，病毒影响范围进一步扩大，包括医疗、电力、能源、银行、教育、交通等多个行业均遭受不同程序的影响。

阿里云早在WannaCry漏洞公开之初，就针对该勒索病毒开启内部应急响应机制。在用户允许的前提下，为用户关闭高危端口，修复漏洞。同时，对阿里云上的客户安全进行持续监测，精准定位受影响主机和客户，最大程度化解风险。

总结过去，主要集中在以下几个方面：

1、安全意识的错位

——事后补救，而不是事前监控和预防。

——把内网隔离等同于安全。

——缺乏对数据进行定期备份的意识。

2、安全责任的缺位

3、整体安全能力的缺乏

网络信息安全关系国家安全

信息安全管理不仅是规范性要求，还涉及国家法律

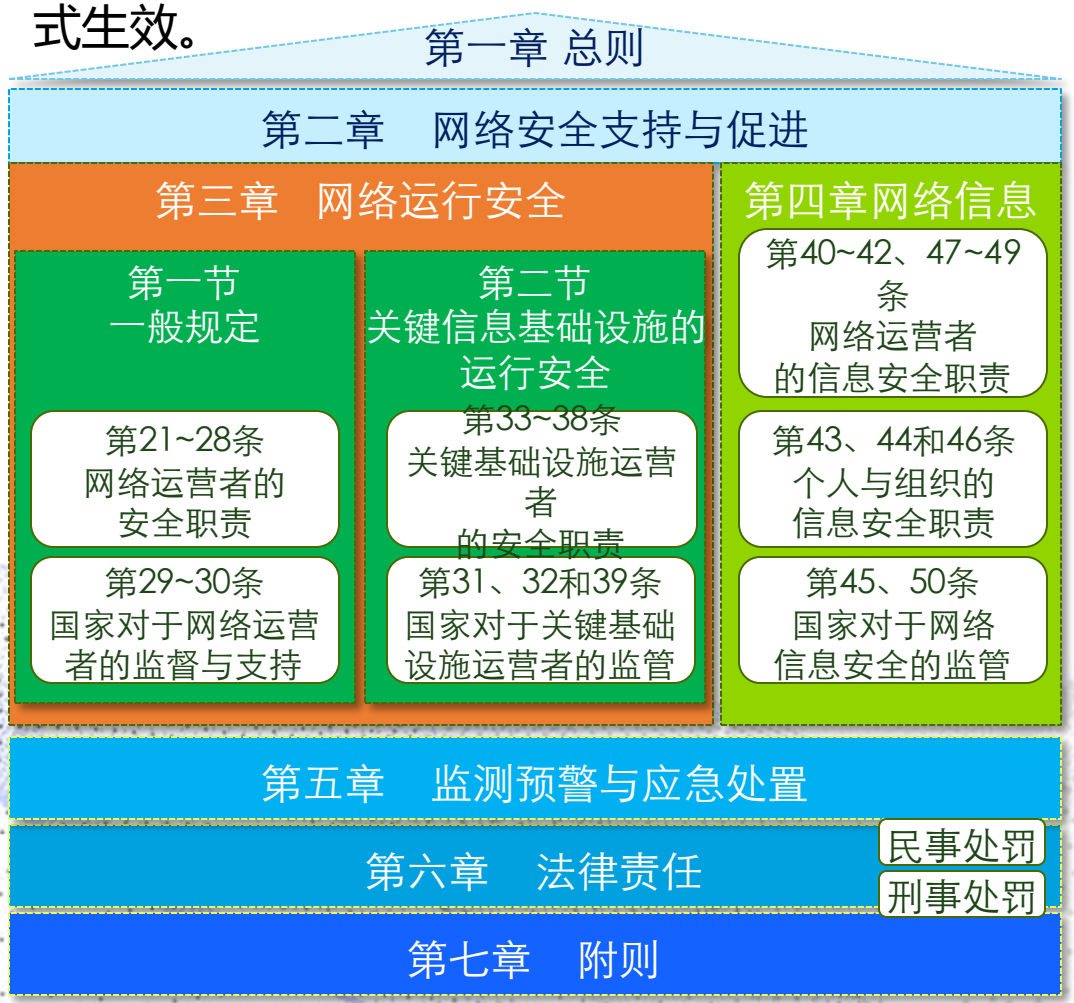
“没有网络安全就没有国家安全，没有信息化就没有现代化”——习近平

网络安全法：

如果违反了这部法律的相关规定，责任主体会承担相应的法律责任：作为网络运营者、网络产品或服务提供者，根据不同的违法情形，可被处以警告、罚款、没收违法所得暂停相关业务、停业整顿、关闭网站、吊销许可证或营业执照等处罚，对直接负责的主管人员和其他责任人员也会有罚款的处罚；作为个人，根据违法情形，可被处以罚款、拘留、没收违法所得、追究刑事责任等。更为严重的是，一旦受到处罚，会根据情形限制其从事网络安全管理和网络运营关键岗位的工作时限，最长可以限制终身。

网络安全法带来的转

随着我国对网络安全的重视程度不断提高，《网络安全法》也应运而生。在历时一年多的立法过程后，于2016年11月由全国人大表决通过，于2017年6月正式生效。



✧第21条，等级保护、网络攻击防护、网络入侵防护、日志保存60天

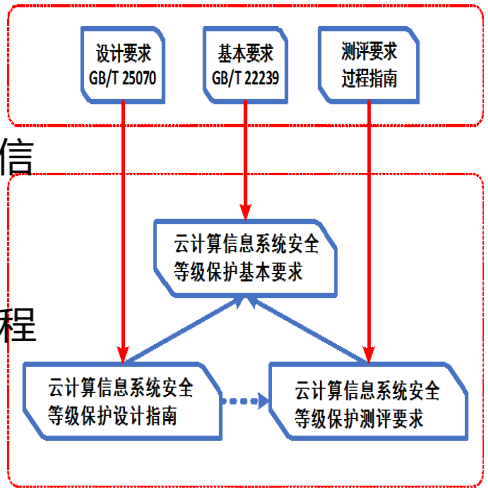
✧第24条，实名制要求；

✧第25条，应急预案；

✧第42条，个人信息保护；

等级保护进入2.0时代

- 阿里云成为全国首家云等保试点示范平台
  - 金融云平台通过等保四级备案、测评；稳步成为国家关键信息基础设施
  - 电子政务云平台等保三级备案、测评；助力“政务互联网+”工程
  - 公共云平台通过等保三级备案、测评；普惠安全



国务院147号令
正式要求实行安全等级保护

1994

1999

国家质检
GB17859-1999
第一个国家信息安全强制标准

中办发[2003]27号文件
公通字[2004]66号文件
公通字[2007]43号文件

2003-2007

2008

GB/T22239和GB/T22240发布
国家信息安全专项（发改高技【2008】1736号）-酝酿全国测评体系公安部三定方案：等级保护，各地网警
发改高技[2008]2071号：电子政务应用一证两报告

全国公安机关网络安全保卫部门
全国安全测评体系-测评机构
发改高技[2012]1986号
联合国资委发文-推动中央企业
金融等级保护标准颁布

2009-2013

2014

公安部组织云计算、物联网、工控、移动互联等保国家标准编制申报
阿里云参与并牵头

国务院5号
公安部推动全国等级保护建设体系建设
网络安全法

2015年

2016

等保标准更名
云计算等保标准国家、部委、行业持续推进
阿里云成为全国首家云等保试点示范平台，高分通过四级云平台诞生

等级保护2.0时代

咨询设计

目标：全面识别安全风险和安全需求，提出符合内部发展与外部监管相结合的安全方案。

主要工作：

- ✓ 现状调研
- ✓ 系统定级、备案
- ✓ 差距分析
- ✓ 风险评估
- ✓ 方案设计

整改建设

目标：基于等级保护结合其他合规要求，对现有系统进行安全整改，并建立起安全防护体系框架。

主要工作：

- ✓ 安全感知能力建设
- ✓ 安全防御能力建设
- ✓ 安全响应能力建设
- ✓ 安全运维能力建设
- ✓ 安全管理能力建设

安全测评

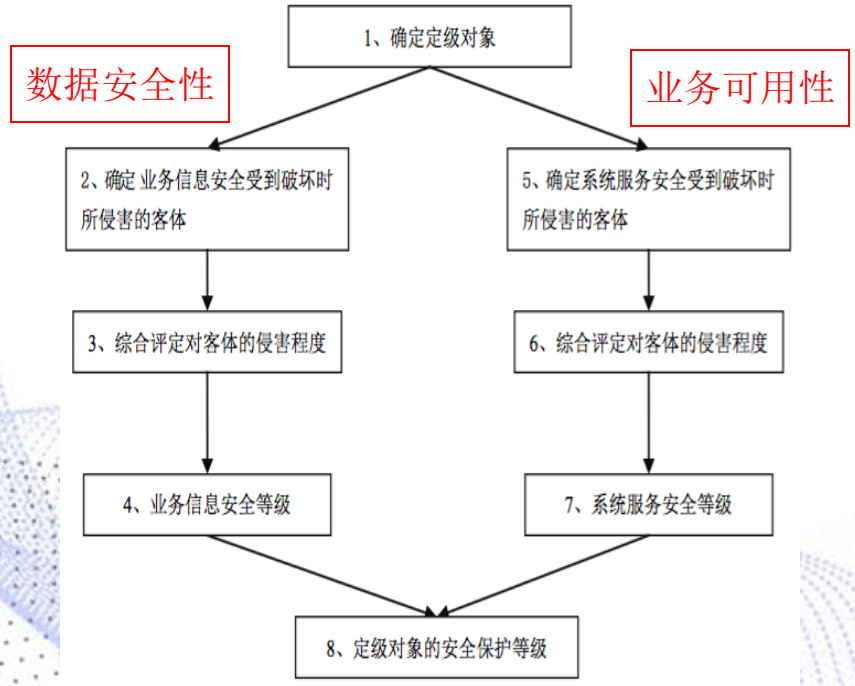
目标：邀请第三方安全测评机构对信息系统进行整体安全测评，出具测评报告。

主要工作：

- ✓ 信息安全等级保护测评
- ✓ 红蓝军对抗防护效果评估

咨询设计阶段：系统

定级备案 → 现状调研 → 差距分析 风险评估 → 方案设计

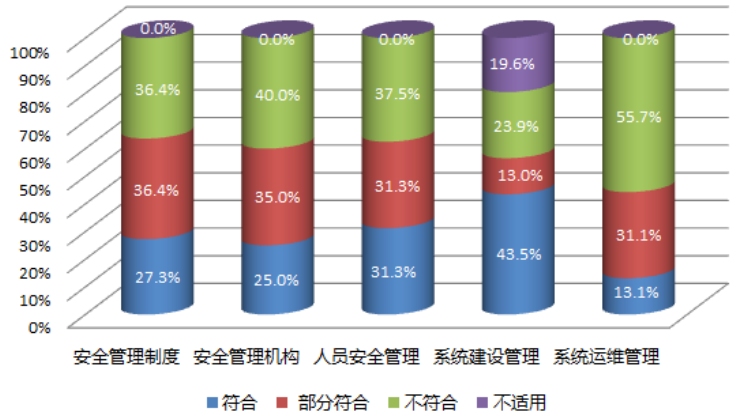


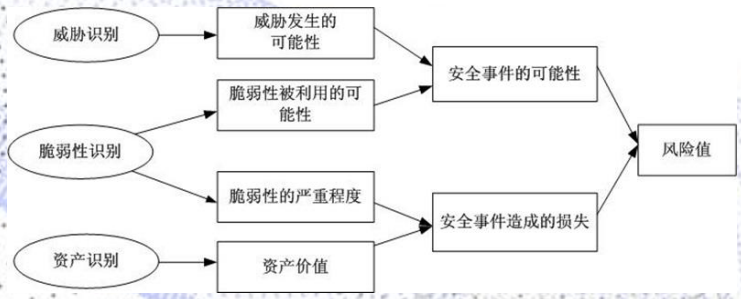
- **信息系统定级原则**：“自主定级、专家评审、主管部门审批、公安机关审核”。
- **定级工作流程**：摸底调查、确定定级对象、对信息系统进行重要性分析、确定信息系统安全保护等级、组织专家评审、主管部门审批、公安机关审核。

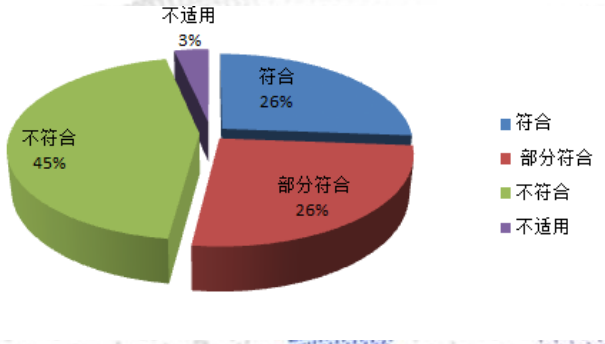
咨询设计阶段：差距

定级备案 → 现状调研 → **差距分析 风险评估** → 方案设计

根据现状调研和风险分析，根据《信息安全技术 信息系统安全等级保护基本要求》的要求及信息系统的定级标准，结合信息系统的现场调研和基本要求的相应等级指标，进行等级保护差距分析，明确不符合项及与安全要求之间的差距及可能造成的风险。

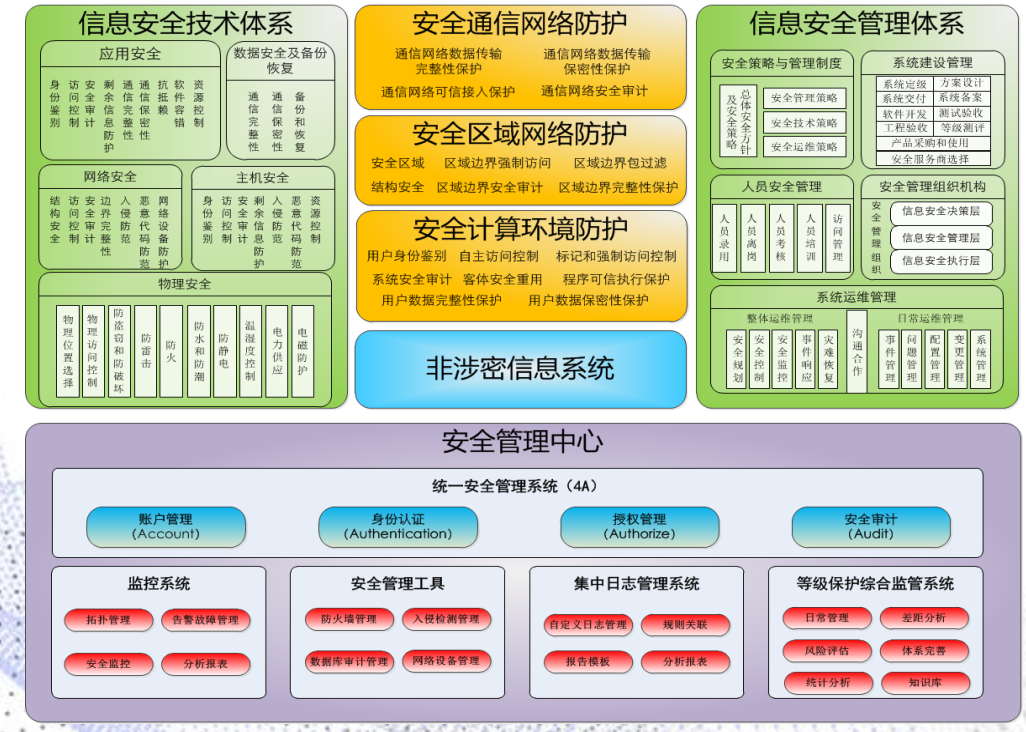






咨询设计阶段：方案

定级备案 → 现状调研 → 差距分析 风险评估 → 方案设计



方案主要内容：

信息安全技术体系设计（安全通信网络设计、安全区域设计、安全计算环境设计）、信息安全管理体系设计（策略与管理制度设计、安全管理组织机构及人员安全管理设计、系统建设管理设计、系统运维管理设计）、安全管理中心设计、产品选型及投资估算

主要政策标准：

- GB/T 22239.1《信息系统安全等级保护基本要求》
- GB/T 22239.2《等级保护云计算扩展要求》
- GB/T 31168《云计算服务安全能力要求》

整改建设阶段：技术

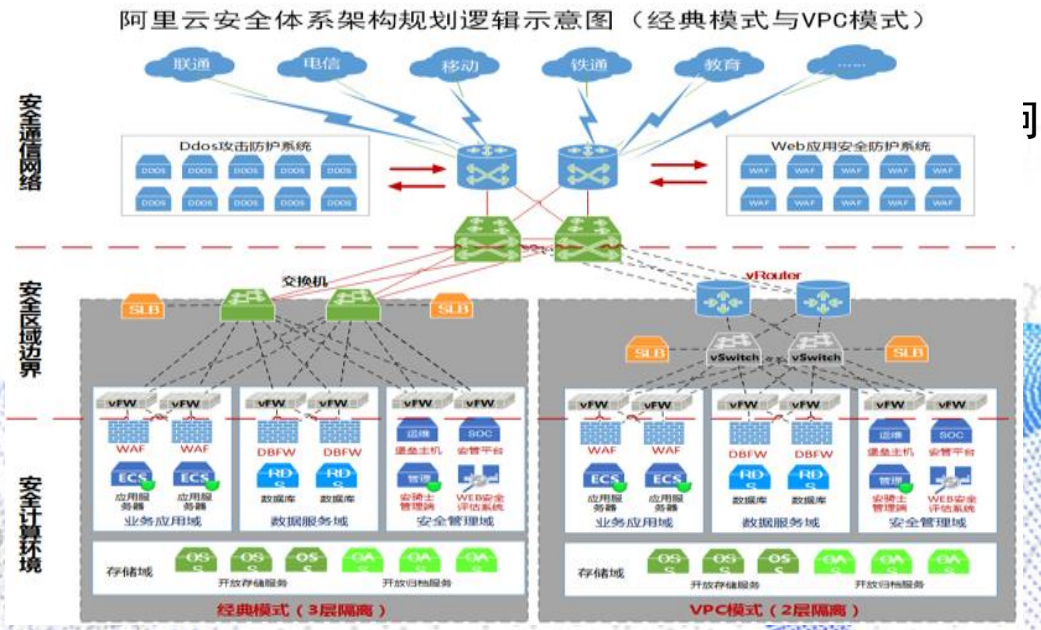
技体系术实施 → 管理体系实施 → 服务体系实施 → 系统试运行

安全域改造

集成实施

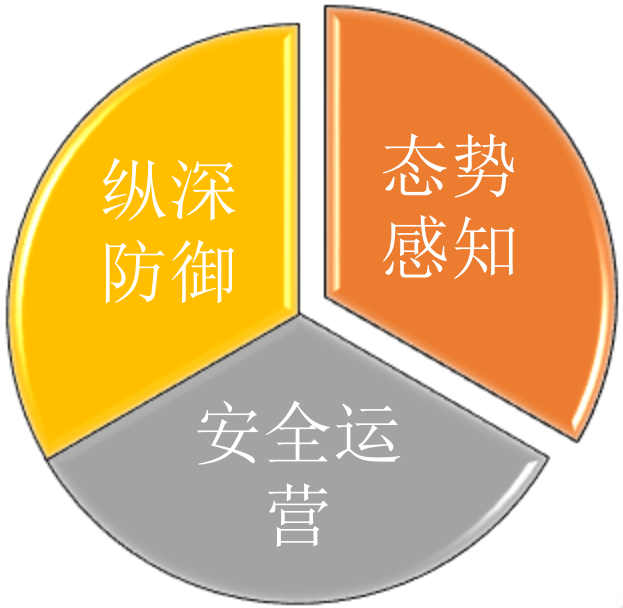
策略部署

- 安全域建设是基于网络和系统进行安全建设的部署依据；
- 安全域与及域边界防护使纵深防护能够进行有



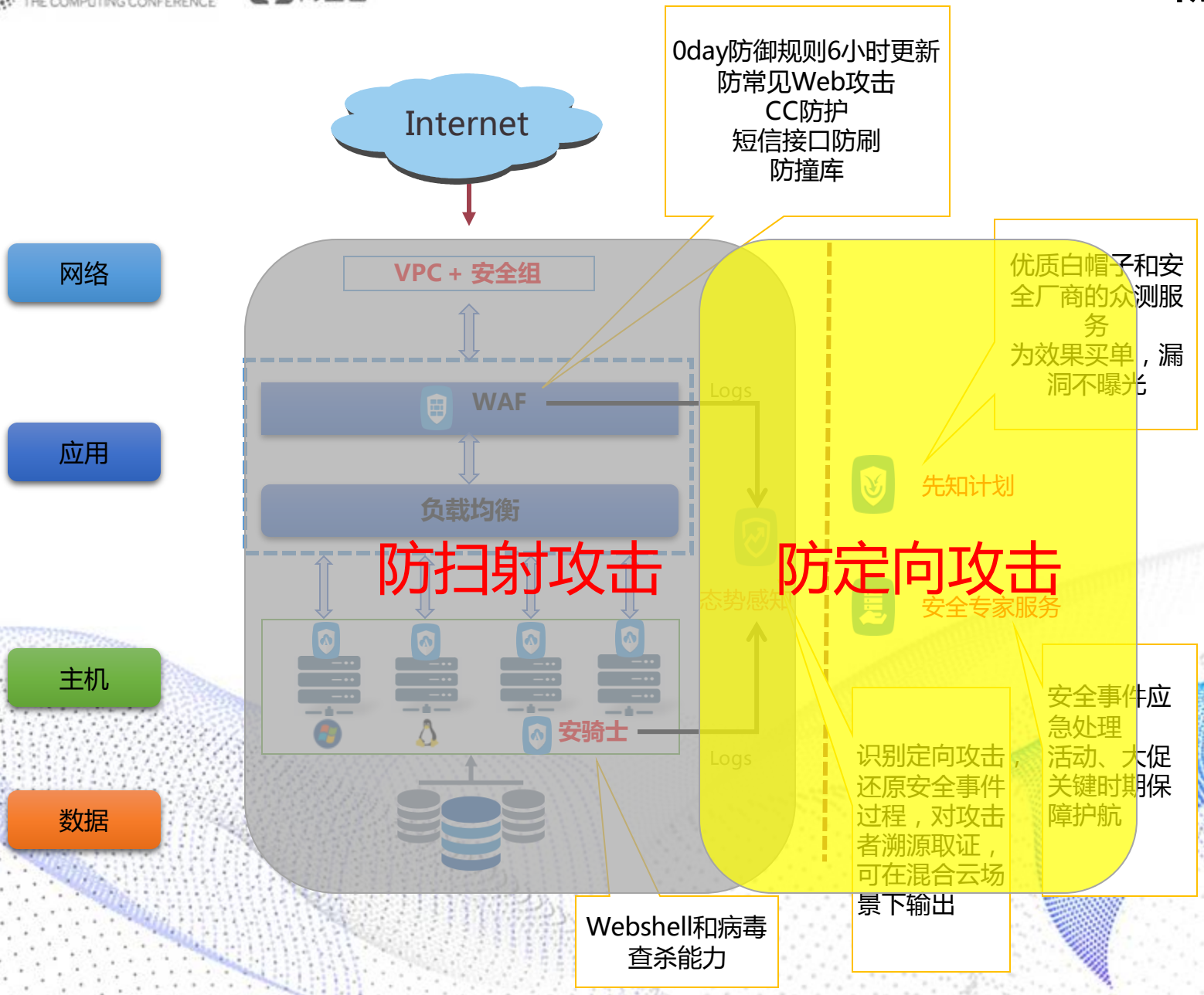
安全效果衡量指标： 漏洞数 安全事件数

DDoS高防
WAF
主机入侵防护
数据加密



基于威胁情报和大数据分析，“看清”安全现状

SDL
红蓝对抗
应急响应


0day防御规则6小时更新
防常见Web攻击
CC防护
短信接口防刷
防撞库
Internet
网络
应用
主机
数据
VPC + 安全组
WAF
负载均衡
安骑士
防扫射攻击
防定向攻击
Logs
Logs
态势感知
优质白帽子和安全厂商的众测服务
为效果买单，漏洞不曝光
先知计划
安全专家服务
安全事件应急处理
活动、大促关键时期保障护航
识别定向攻击，还原安全事件过程，对攻击者溯源取证，可在混合云场景下输出
Webshell和病毒查杀能力

注册
- 建议使用：滑动验证
- 防垃圾注册
- 防短信攻击

登录
- 建议使用：风险识别+滑动验证
- 防刷库撞库

活动
- 建议使用：风险识别
- 防活动作弊

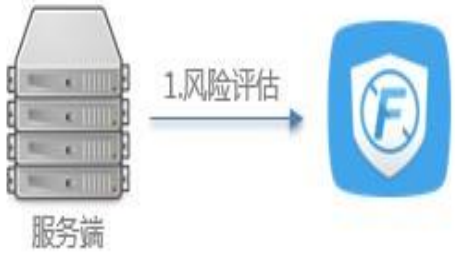
下单交易
- 建议使用：风险用户查询
- 防刷单炒信

数据风控

滑动验证

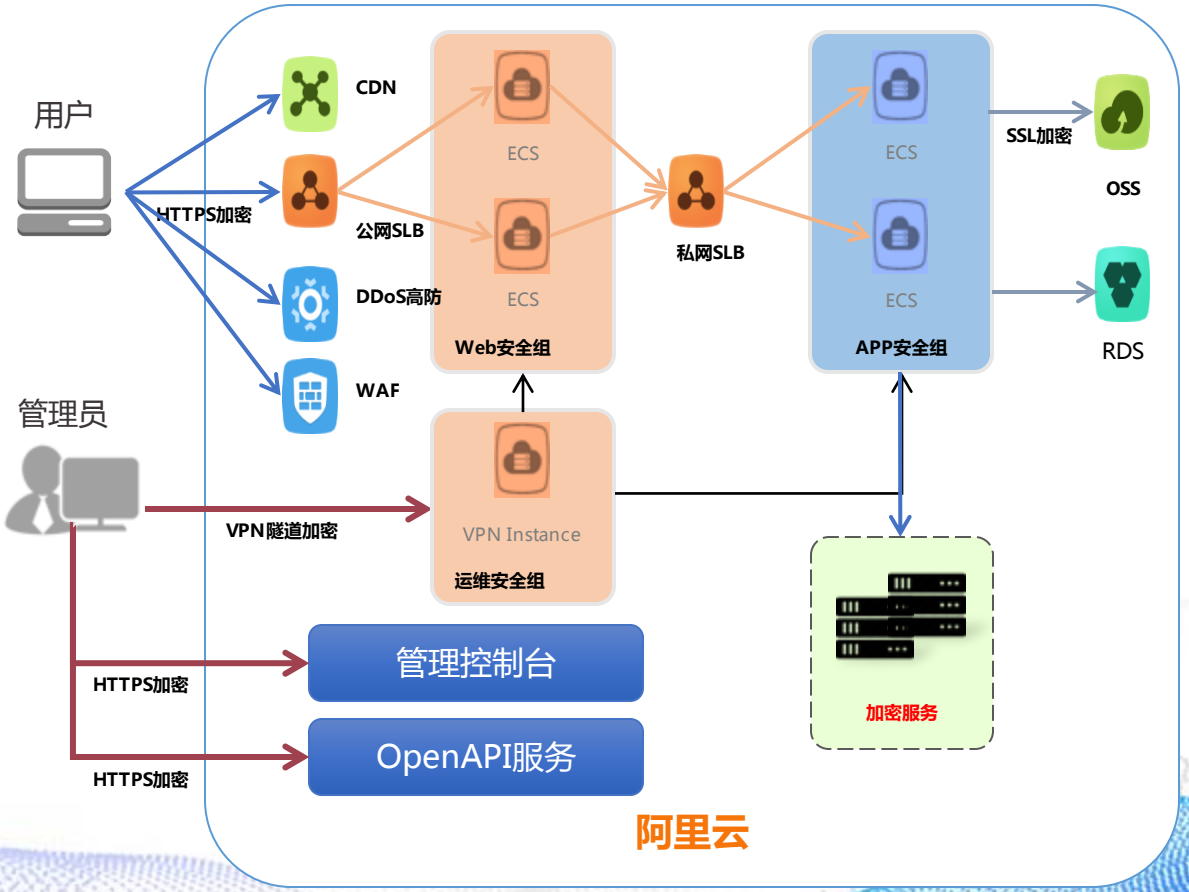
风险识别

风险用户查询



云盾证书服务帮助您轻松实现全站HTTPS，防劫持、防窃听，满足Apple要求

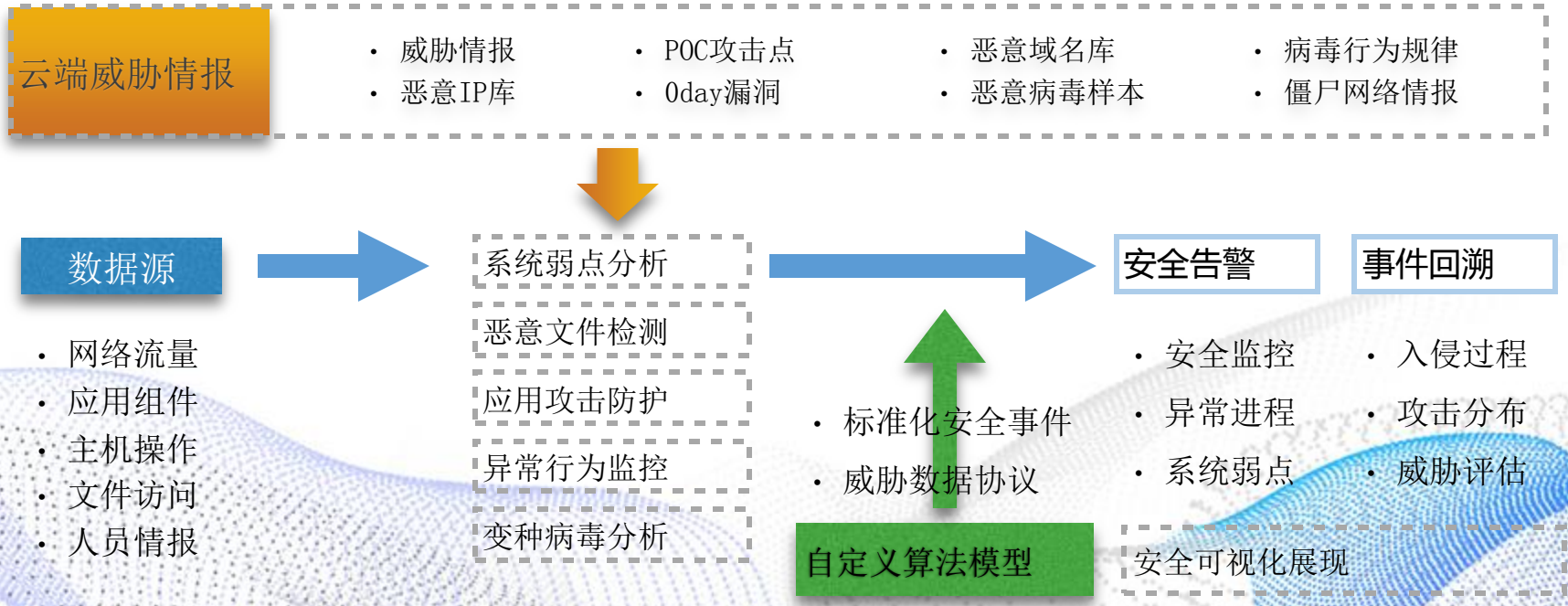
云盾加密服务让您的敏感数据加密存储，未经授权员工及黑客都拿不到数据



证书服务　　加密服务

以态势感知为核心的安全管理

大数据安全分析平台：降低因黑客攻击导致数据泄露的问题，识别攻击和入侵，并回溯入侵点，可追溯到黑客姓名全记录入侵后的恶意操作。通过海量异构数据的关联分析，对APT攻击进行精准识别。



基于加密服务解决个人信息保护

对称加密算法

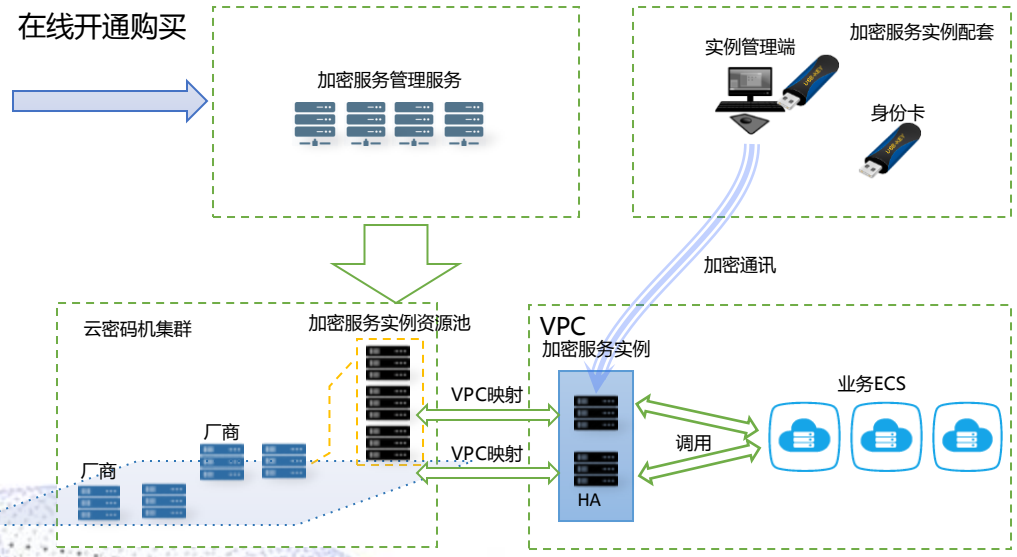
SM1、SM4、DES、3DES、AES等

非对称加密算法

SM2、RSA（1024-2048）等

摘要算法

SM3、SHA1、SHA256、SHA384等



物理运算

- 加解密运算全部通过物理加密运算芯片来完成，过程可靠

参考运算能力

- SM1加密运算：4000次/秒
- SM2签名运算：2300次/秒
- SM2验签运算：1600次/秒
- RSA2048公钥运算：2400次/秒
- RSA2048私钥运算：200次/秒

可以通过增加加密服务实例，快速实现运算能力的叠加

云上的数据保险箱

密钥由您完全掌控

黑客拖库或未经授权

员工看不懂数据

利用社会资源解决企业安全测试

用社会化（白帽子、安全公司）的方式帮助电商企业发现安全问题，为电商企业提供及时、安全、私密的安全情报服务平台。

私有的安全中心

- 不公开任何漏洞标题及细节；不进行任何的漏洞炒作。
- 测试范围及漏洞奖励计划自行定义；
- 可自主指定入驻平台的白帽子及安全公司作为测试人员。

可靠的安全专家

- 测试人员全部通过支付宝实名认证；叠加身份认证及企业认证；安全可靠。
- 全部签署平台保密协议。
- 接受企业提供测试环境或者VPN供测试，服务全程可监控，漏洞可追溯。

显著的测试效果

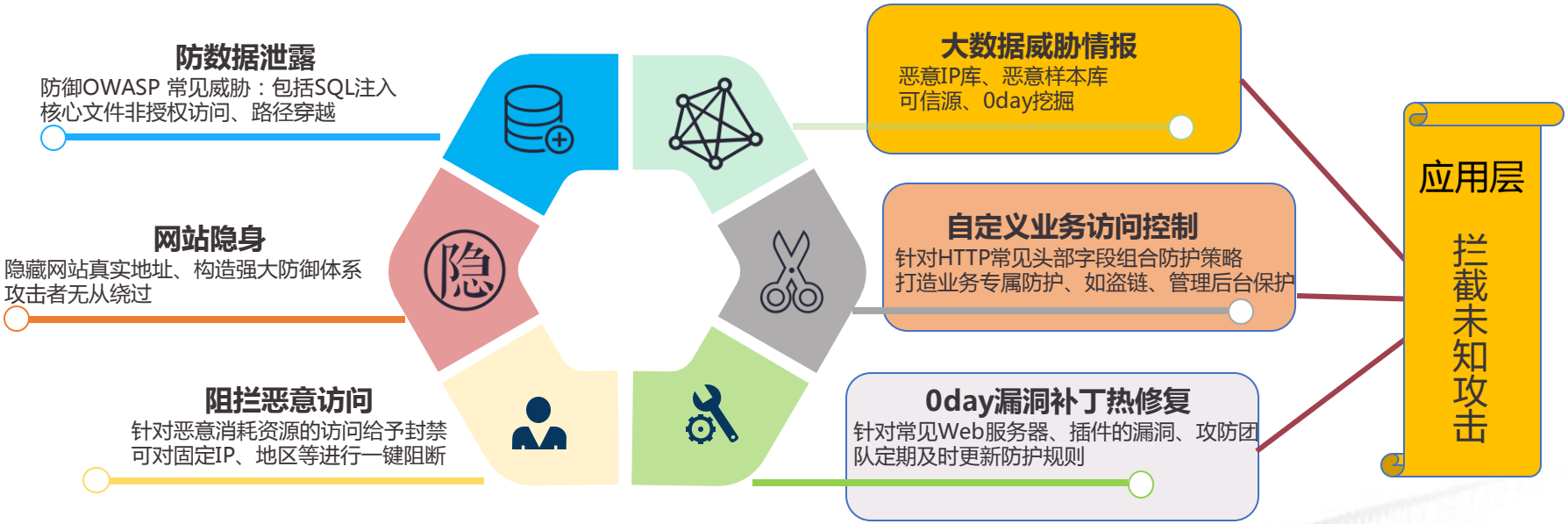
- 安全专家平均为每个入驻的企业提交50个漏洞；其中高危漏洞占比30%。
- 安全专家遵循平台优胜劣汰机制，持续提升测试效果和服务质量。
- 按效果付费机制，无漏洞不收费。

完整的漏洞闭环

- 共享阿里内部专业漏洞运营团队，免费提供漏洞审核、漏洞修复咨询服务。
- 可选增值服务，完整管理漏洞生命周期。

1 获取使用资格 → 2 企业实名认证 → 3 充值预付费 → 4 设置测试范围 → 5 审核漏洞 → 6 按效果付费

解决web攻击、信息泄露等



防御规则是核心，安全运营是关键：

- 零部署、零维护
- 全面覆盖OWASP TOP10攻击
- 专业的攻防团队0day漏洞研究，0day防御规则快速更新
- 强大的CC防护能力，保障网站可用性
- 经过阿里电商、支付宝实践验证

通过数据风控解决秒杀、刷单等

数据风控服务是阿里大数据风控服务能力的对外输出，通过**整合**包含互联网金融、电商、第三方支付等**众多行业的数据**，配合领先的**行为收集技术**，经过**机器学习模型**、**大数据关联分析和指标计算**，**解决**账号、活动、交易等**关键业务环节**存在的欺诈威胁。

整改建设阶段：管理

技体系术实施 → **管理体系实施** → 服务体系实施 → 系统试运行

策略、方针（一级文件）

制度、规范、流程（二级文件）

指南、细则、表单（三级文件）

- 第一级文件

  安全策略、方针性文件，规定信息安全工作的总体目标、范围、原则和安全框架，是管理制度体系的灵魂和核心文件，如《信息安全策略总纲》

- 第二级文件

  安全管理活动中涉的规范、制度、流程性文件，是具体管理内容的体现，如《人员管理规定》、《信息安全组织及岗位职责管理规定》等

- 第三级文件

  系统日常管理活动中遵循的具体操作规程，是管理人员或操作人员执行的具体指南、细则、指导书、表单等文件，如《系统变更申请表》、《网络巡检表》等 。

整改建设阶段：服务

技体系术实施 → 管理体系实施 → 服务体系实施 → 系统试运行

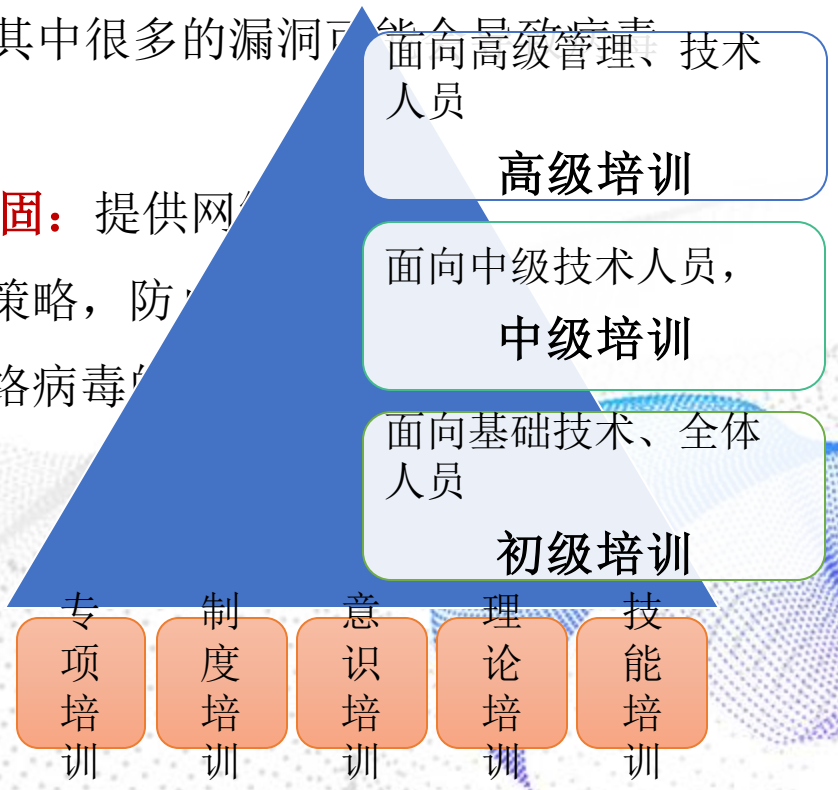
安全加固

评估服务

安全培训

安全加固内容：

- **系统安全加固：**目前使用的各种服务器操作系统存在大量已知和未知的漏洞，其中很多的漏洞可能会导致病毒的入侵。
- **网络设备和安全设备加固：**提供网络和安全设备的加固建议和策略，防范模蠕虫病毒的攻击，将网络病毒的影响降至最低。



等级测评

本阶段主要由测评机构开展测评，运营单位、阿里云负责配合测评，参与访谈、技术验证、资料准备和问题整改。

测评准备

- 掌握被测系统的详细情况，准备测试工具，为编制测评方案做好准备。

方案编制

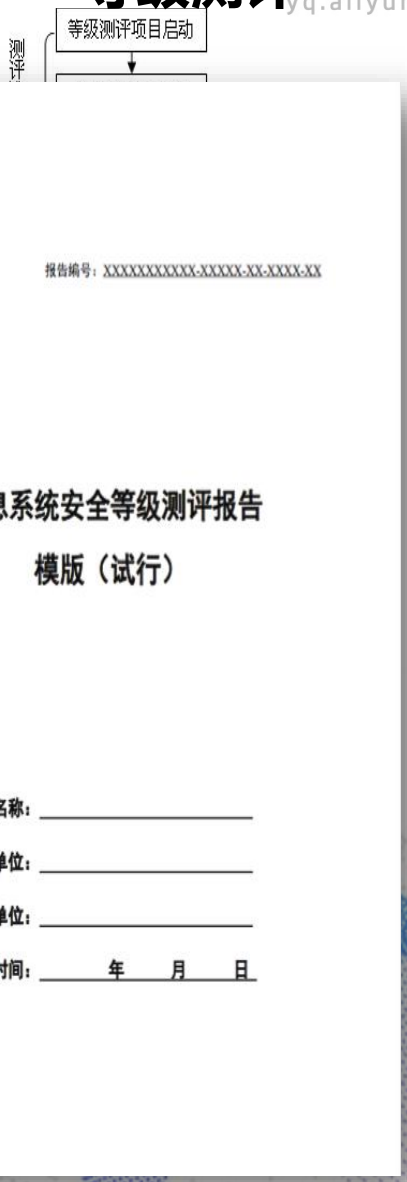
- 确定与被测信息系统相适应的测评对象、测评指标及测评内容等，并根据需要重用或开发测评指导书测评指导书，形成测评方案。

现场测评

- 按照测评方案的总体要求,严格执行测评指导书测评指导书，分步实施所有测评项目，包括单元测评和整体测评两个方面，以了解系统的真实保护情况,获取足够证据，发现系统存在的安全问题。

分析与报告编制

- 根据现场测评结果和GB/T 28448-2012，通过单项测评结果判定、单元测评结果判定、整体测评和风险分析等方法，找出整个系统的安全保护现状与相应等级的保护要求之间的差距，并分析这些差距导致被测系统面临的风险，从而给出等级测评结论，形成测评报告文本。



感知能力，用大数据分析解决原来看不到的安全问题

- NetFlow
- 主机Flow
- 操作日志
- 数据库日志
- 资产收集

- 入侵线索
- 历史数据关联
- 流量和进程关系

- 攻击和入侵识别
- 高级APT识别
- 是否阻断请求
- 漏洞修补
- 社工信息修补

阿里云云盾基于实战构建起的安全

全中国30%的网站

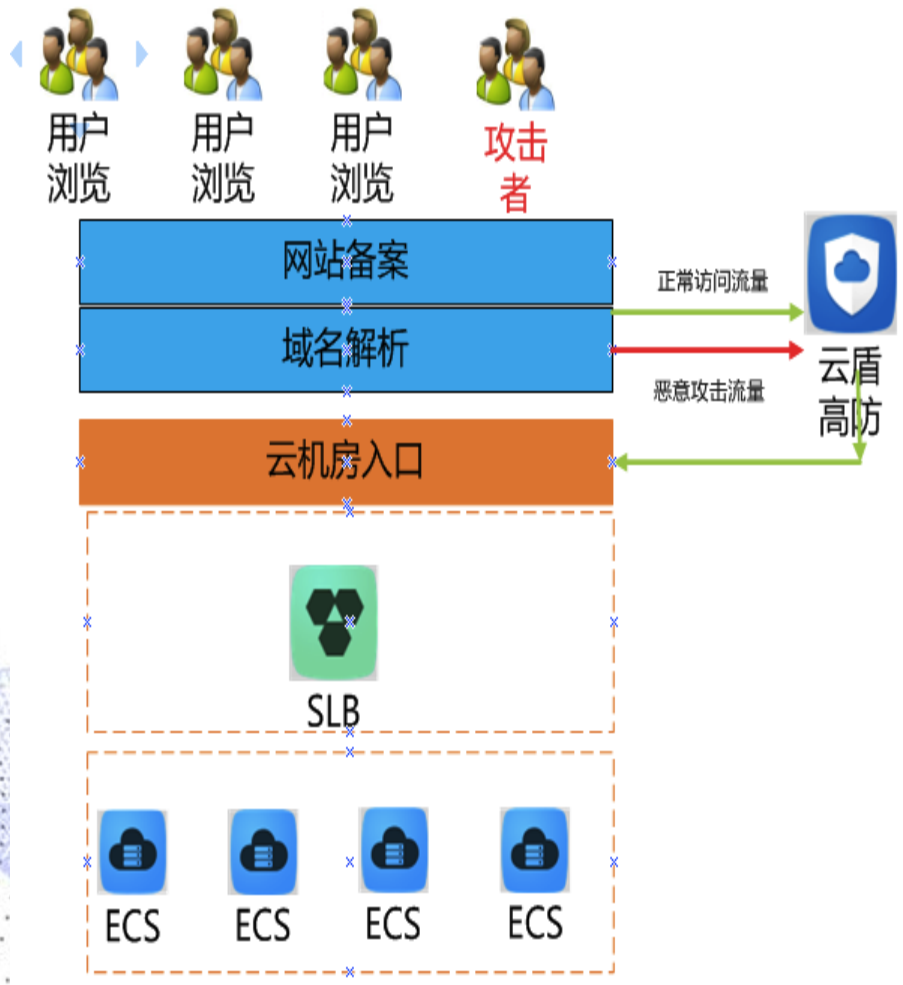
每天抵御1000次以上DDoS攻击

每天抵御2000万次Web应用攻击

每天防御超过2亿次密码暴力破解攻击

2014年12月 = 453.8 Gbps DDoS

案例：某电商客户大促防DDoS



案例：某轻奢品电商

背景：白帽子发现了客户的0元支付漏洞，测试成功，仓库直接发货了，先知平台对白帽子测试准入和行为均做了严格要求，测试白帽子遵守平台规定，并没有收测试成功的商品，得到客户赞赏。

- 测试花费：5万
- 测试时间：持续测试一个月，提交漏洞**174**个，有效漏洞**61**个，高危和严重漏洞**8**个。

- 严重漏洞导致的业务损失：

  1、公司付款私钥泄露；

  2、订单价格随意修改，可0元支付。

案例：某垂直行业TOI

- 行业：电商
- 测试花费：7.5万
- 测试时间：**10**个小时，提交漏洞**306**个，有效漏洞**132**个，高危和严重漏洞**9**个。

- 严重漏洞导致的业务损失：

  1、用户敏感信息泄露；

  2、越权，可操作任意用户账户；

  3、控制核心服务器。

2017云栖大会·成都峰会
THE COMPUTING CONFERENCE
阿里云

飞天·智能

APSARA INTELLIGENCE

2017云栖大会·成都峰会

5月23日 成都世纪城天堂洲际大酒店