HUAWEI

HUAWEI IT大咖说 知识共享平台

华为云技术私享会

华为云安全官网

私享会专场用户，优享云安全大礼包，每人1份

欢迎体验华为云安全核心竞争力产品，大礼包价值￥9680，
列表如下：

大礼包内容	适用范围	礼券价值
DDoS高防代金券	高防所有标准套餐	3000元
WAF代金券	WAF所有标准套餐	880元
DBSS代金券	DBSS所有标准套餐	5800元

华为云
技术
私享会

私享会专场用户，优享云安全专属优惠

华为云服务	标准套餐	适用场景	专属优惠政策
DDoS高防	10~30G保底防护套餐	业务初期，非核心竞争业务	6折起售
	≥100G超强防护包年套餐	业务成熟期，核心竞争业务	1折起售 (赠送5~10万按需代金券)
Web应用防火墙	WAF所有标准套餐	所有网站，业务数据敏感	旗舰版5折 其他版6折
数据库安全DBSS	DBSS所有标准套餐	数据库安全合规，防拖库等	高级版5折 专业版6折 基础版7折

华为云
技术
私享会

HUAWEI

HUAWEI

HUAWEI IT大咖说 知识共享平台

华为云
技术
私享会

华为云DDoS高防2.0解决方案

胡巍　　华为云安全产品总监

华为云全栈防护体系

运营安全

运营管理

- 运营牌照
- 租户生命周期
- 服务生命周期

交易管理

- 责任边界
- 合同管理

租户安全

安全服务

- 自研服务
- 合作生态

云服务安全

- SaaS
- PaaS
- IaaS

基础设施安全

云平台安全

- 数据安全
- 主机安全
- 虚拟网络安全

边界防御安全

- 防火墙
- VPN
- WAF
- IPS
- Anti-DDoS

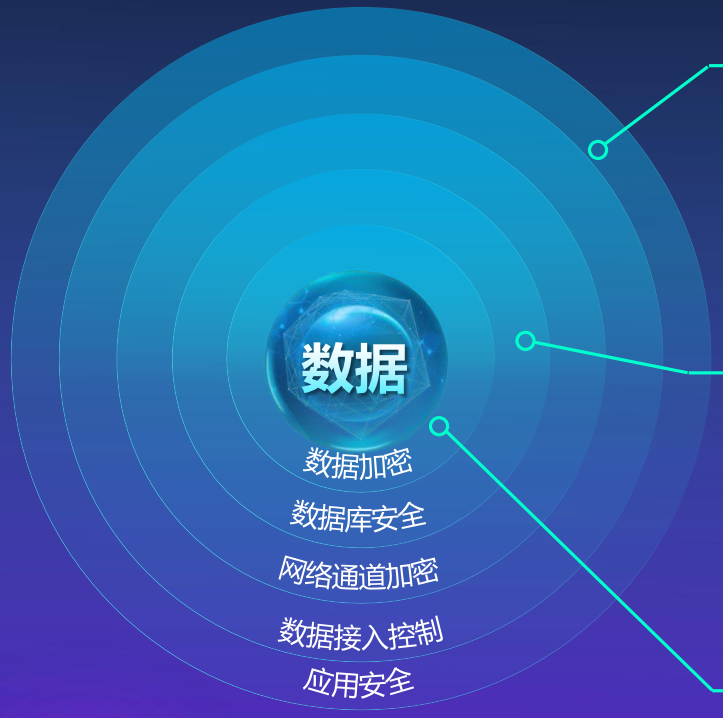
运维安全

- 检测
- 分析
- 感知
- 响应

合规安全（标准和认证）

可信云认证 | 信息安全等保 | ISO27001 | CSA STAR | PCI | SOC | ……

以数据安全为中心，构建的全栈安全服务



安全风险和方案

进不来（应用安全）
- XSS跨站
- 恶意插件
- 木马上传
- 非授权访问
- SQL注入
- 自动学习

看不到（数据库安全）
- 自动发现
- 动态脱敏
- 全面控防
- 精准审计

拿不走（数据加密）
- 密钥管理
- 第三方HSM
- 国际标准算法
- 强合规性

化理念为实践

安全服务

网络安全
- Anti-DDoS
- DDoS高防
- 云防火墙
- 端云协同防护

主机安全
- 资产管理
- 入侵检测
- 漏洞管理
- 基线检查
- 网页防篡改

应用安全
- Web应用防火墙
- Web扫描
- 中间件（含DB）扫描
- 主机扫描
- 弱密码扫描
- 业务逻辑扫描
- 编码扫描

数据安全
- 数据库审计
- 数据脱敏
- 数据库防火墙
- 数据专属加密
- EVS/VBS/IMS/OBS/RDS加密
- 密钥管理
- 密钥对登陆

安全管理
- 态势感知
- 云堡垒机
- 证书管理
- 安全监测
- 主机安全体检
- 网站安全体检
- 应急响应
- 安全加固

DDoS攻击发展趋势

有组织的黑客产业链

- 专业的运作链条
- 成本低
- 难定位

秒级加速，流量更大，更加专业

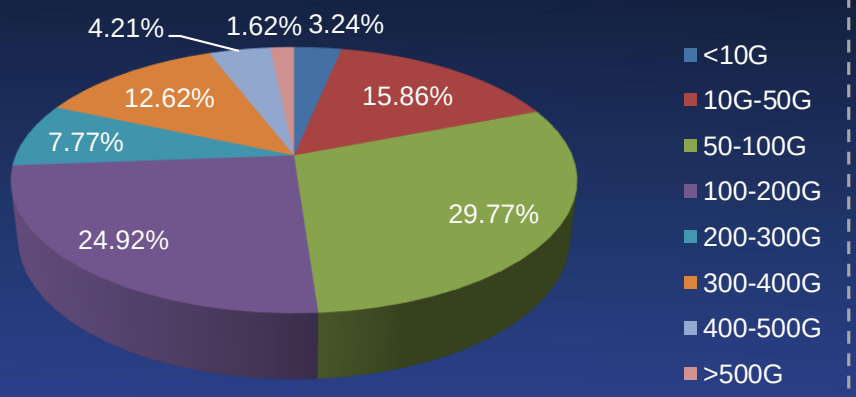
- 攻击流量上升快，几秒即可超百G
- 反射攻击持续升温，不断有新型的开放服务器被挖掘
- 攻击手段越来越专业，混合流量占比高，不断调整攻击手法

IoT终端加入僵尸网络大军

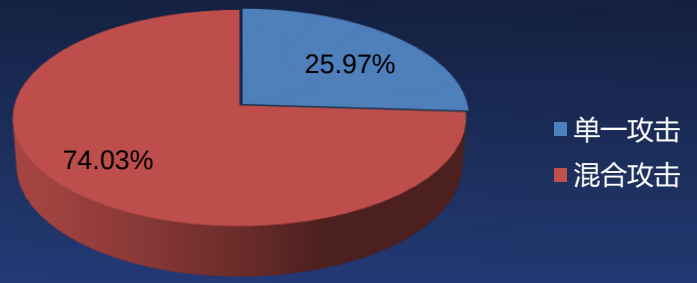
- 安全机制缺失，IoT终端成僵尸网络发展壮大的温床
- 海量IoT僵尸发起T级攻击
- 入侵CCTV摄像头形成僵尸网络，每个摄像头每秒可以发送1到30M数据包

华为云高防2017年DDoS攻击监测数据分析

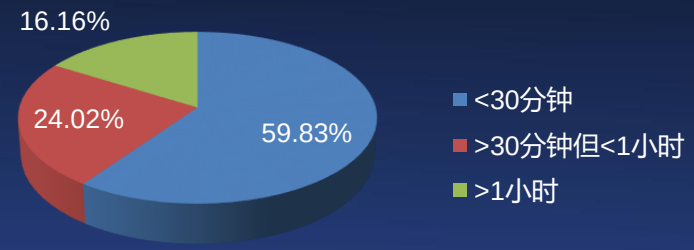
攻击规模量级占比



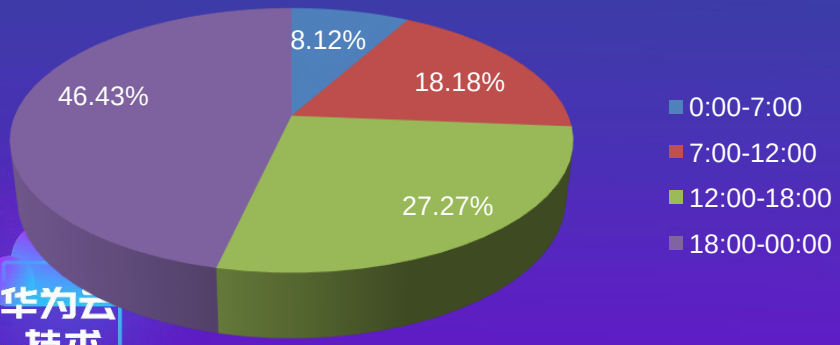
攻击矢量分布



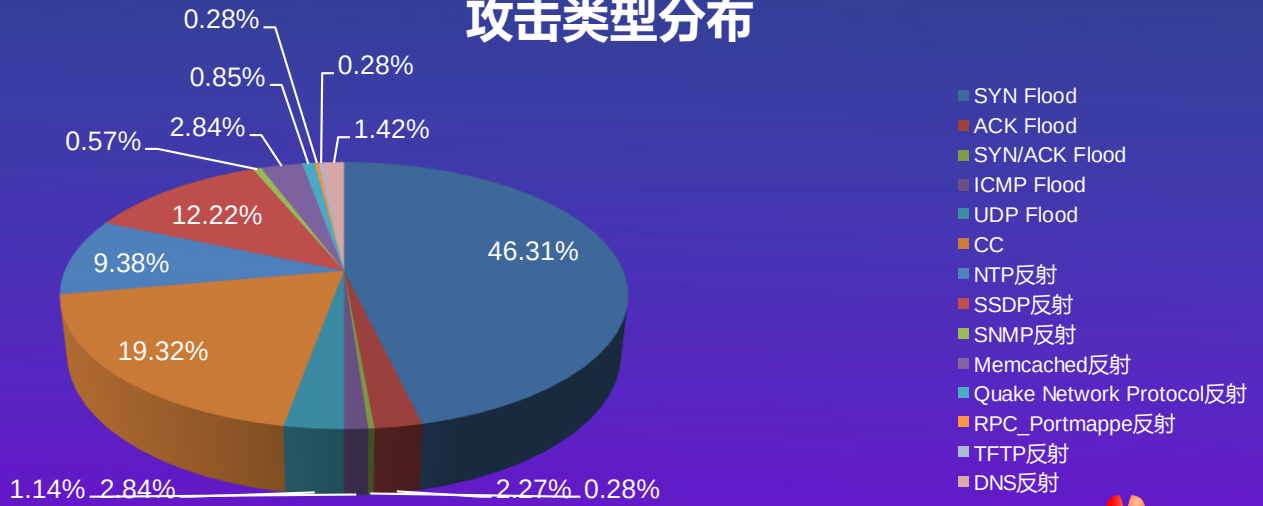
攻击时长占比



攻击发生时间段占比



攻击类型分布

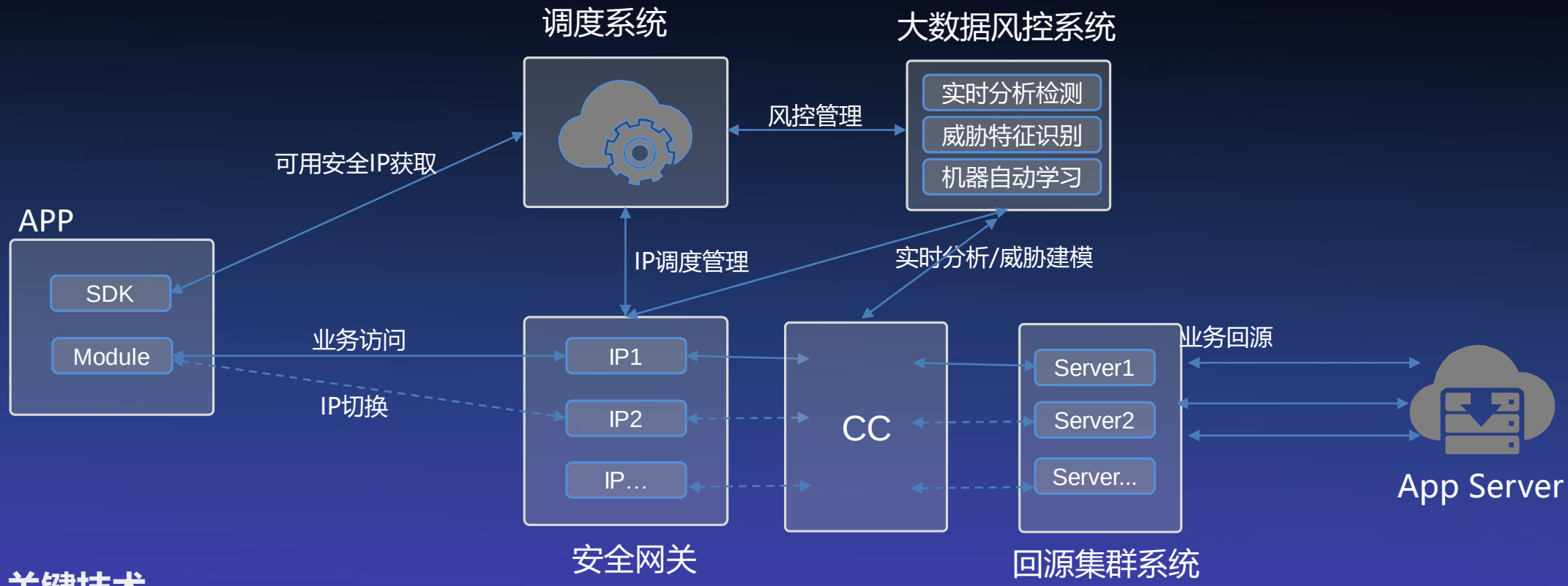


互联网行业为何成为俎上鱼肉

同行竞争激烈，黑客敲诈勒索

- 互联网业务对可用性和连续性要求高，DDOS攻击流失大量用户。游戏协议私有，TCP CC防御难度非常大。攻击成本低，效果好。
- 棋牌类游戏等为迅速抢占市场份额，敏捷快速开发，WEB、APP存在安全漏洞，整体架构存在众多攻击薄弱点。
- 外包或购买开源的代码，无自身技术团队保障，黑客偏爱此类运营商，经不起黑客打击，成为发展重大瓶颈。

高防2.0——端云协同+大数据风控解决方案



关键技术

智能调度：分组、资源调度

流量染色：加密染色，一人一密/一机一密，防误杀、防破解，正邪一识即破

SDP单包认证：解决APP、端游的CC问题

全球分布式节点部署，智能优选接入

全球10+清洗节点
带宽储备：10TB
单节点最大防护能力：2TB

（具备无限流量清洗能力）

华为云游戏高防2.0解决方案特点

快速流畅

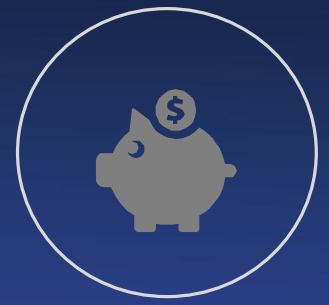
- SDK秒级切换攻击
- 多线BGP高速接入

智能学习

- 业务风控智能隔离
- 黑客攻击机器学习

精准防护

- 流量染色技术
- SDP认证技术



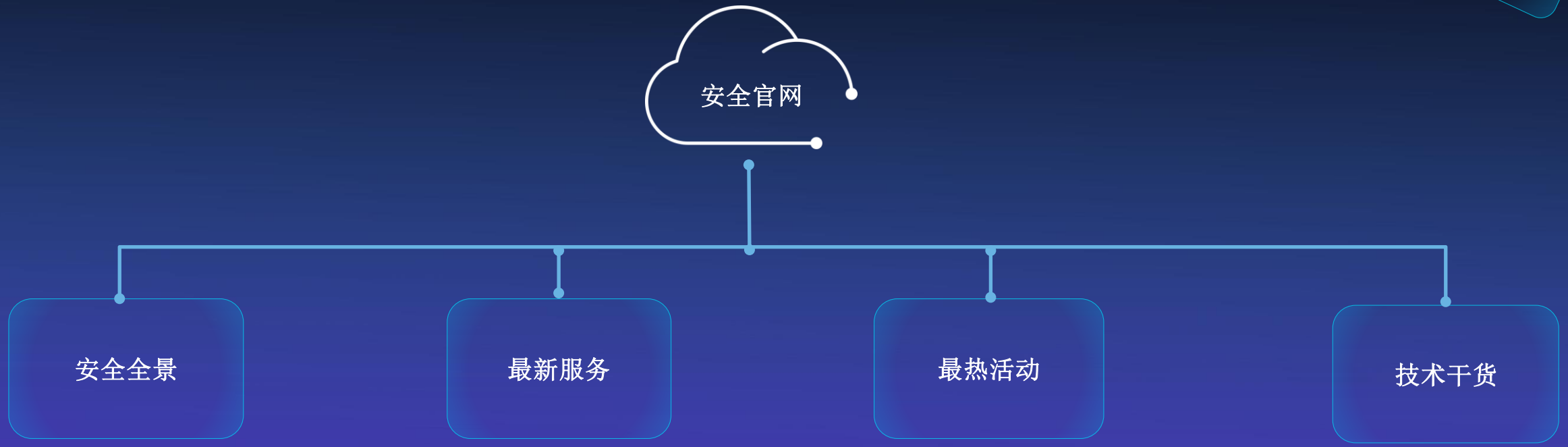
高性价比

- 无限攻击防御能力
- 定制方案成本可控

一个中心，一网打尽——华为云安全中心

云安全，一个网址就够——华为云安全官网

全新发布



华为云
技术
私享会

HUAWEI

THANK YOU

HUAWEI

HUAWEI IT大咖说 知识共享平台

华为云技术私享会

网络安全等级保护工作开展交流

吴进学　广东南方信息安全研究院

Part 01

政策背景

什么是网络安全等级保护

网络安全等级保护

网络安全等级保护是指对国家秘密信息、法人和其他组织及公民的 专有信息以及公开信息和存储、传输、处理这些信息的信息系统**分等级 实行安全保护**，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件**分等级响应、处置**。

信息系统安全等级测评

为了验证信息系统是否满足相应安全保护等级的评估过程。

必要性1：网络安全等级保护制度

第二十一条

国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）**制定内部安全管理制度和操作规程**，确定网络安全负责人，落实网络安全保护责任；

（二）**采取防范计算机病毒和网络攻击、网络侵入**等危害，网络安全行为**的技术措施**；

（三）**采取监测、记录网络运行状态**、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于**六个月**；（日志留存）；

（四）采取数据分类、重要数据备份和加密等措施；（数据安全）；

（五）法律、行政法规规定的其他义务。

第三十一条

国家对**公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务**等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能**严重危害国家安全、国计民生、公共利益的关键信息基础设施**，在网络安全等级保护制度的基础上，**实行重点保护。**关键信息基础设施的具体范围和安全保护办法由国务院制定。

网络安全工作监管

管辖对象：

- 网络运营者（定义：网络的所有者、管理者和网络服务提供者）
- 关键信息基础设施的运营者
- 跨境传输者
- 网络产品或者服务的提供者

监管机构：

监管方式：

依法约谈 → 开展调查 → 责令整改 → 给予警告 → 依法处罚

《网络安全法》部分处罚条款

第五十九条

网络运营者不履行本法**第二十一条、第二十五条**规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，**处一万元以上十万元**以下罚款，对**直接负责的主管人员处五千元以上五万元以下罚款**。

关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

第六十条

违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，**对直接负责的主管人员**处一万元以上十万元以下罚款：

（一）设置恶意程序的；

（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；

（三）擅自终止为其产品、服务提供安全维护的。

游戏行业等保开展情况

4月15日 完成备案

10月1日完成测评

5月15日完成备案

12月前完成测评

?

执法简介

单位未落实等级保护被黑：单位被罚10000，法人被罚500

2017-08-14 四川在线 游侠安全网

8月12日，记者从四川省公安厅网安部门获悉，因未落实网络安全等级保护制度，近日宜宾市翠屏区教师发展培训与教育研究中心被处一万元罚款，法人代表唐某某被处五千元罚款。这是今年6月1日《中华人民共和国网络安全法》(以下简称《网络安全法》)实施以来，我省公安机关依法处置的第一起违反《网络安全法》行政案件。

为落实网络安全责任以致黑客攻击

7月22日，宜宾市翠屏区"教师发展平台"网站因网络安全防护工作落实不到位，导致网站存在高危漏洞，

河南一图书馆网站被黑 因未履行网络安全保护获罚

2018-02-01 大河报 游侠安全网

原标题：网站被黑却又遭罚，这是为啥？ 新乡一图书馆网站遭到黑客攻击，因未履行网络安全保护义务被罚2万元

1月29日上午，河南省公安厅网络安全保卫总队官方微博"河南网警巡查执法"对外发布消息：今年1月12日，新乡市封丘县图书馆网站遭到黑客攻击，致使网页被篡改。依据相关法律，对封丘县图书馆及相关责任人作出了处罚。


广州市信息安全等级保护工作协调小组办公室

广州市信息安全等级保护工作协调小组
办公室关于通报未依法开展等级测评
单位及信息系统（第二批）的通知

各有关单位：


关于通报未依法开展等级测评单位及信...

518K

PDF

汕头网警支队办理首宗适用《网络安全法》行政案件

原创 2017-07-25 汕头网警巡查执法 汕头网警巡查执法

2017年6月1日起，《中华人民共和国网络安全法》（以下简称《网络安全法》）正式施行，这是我国第一部全面规范网络空间安全管理的基础性法律。该法明确了网络运营者的网络安全义务，建立了网络安全等级保护制度，为网络安全执法提供了重要的法律依据。近日，汕头网警支队办理了首宗适用《网络安全法》的行政案件，为进一步贯彻落实和适用《网络安全法》积累了经验。

为了进一步推进网络安全等级保护工作，按照省厅严打整治网络犯罪"安网"专项行动的部署，汕头网警支队对全市网络安全等级保护重点单位进行执法检查。2017年7月20日，检查中发现，汕头市某信息科技有限公司于2015年11月向公安机关报备的信息系统安全等级为第三级,经测评合格后投入使用，但2016年至今未按规定定期开展等级测评。

根据《信息安全等级保护管理办法》第十四条第一款规定，信息系统安全保护等级为第三级的信息系统应当每年至少进行一次等级测评。根据新出台的《网络安全法》规定，定期开展测评属于第二十一条第（五）项规定的"法律、行政法规规定的其他义务"。

汕头市某信息科技有限公司之行为已违反《信息安全等级保护管理办法》第十四条第一款和《网络安全法》第二十一条第（五）项规定，构成未按规定履行网络安全等级测评义务。根据《网络安全法》第五十九条第一款规定，依法对该单位给予警告处罚并责令其改正。

必要性2：等保2.0新的标准即将发布

既要满足通用要求，又要满足安全扩展要求

- 《信息安全技术 网络安全等级保护基本要求 第1部分：安全通用要求》
- 《信息安全技术 网络安全等级保护基本要求 第2部分：**云计算**安全扩展要求》
- 《信息安全技术 网络安全等级保护基本要求 第3部分：**移动互联**安全扩展要求》
- 《信息安全技术 网络安全等级保护基本要求 第4部分：**物联网**安全扩展要求》
- 《信息安全技术 网络安全等级保护基本要求 第5部分：**工业控制**安全扩展要求》

2.0

定级备案

建设整改
安全监测
通报预警
应急处置
安全可控
…

等级测评
渗透测试
攻防对抗
特勤安保
有效性评价
…

监督检查
专项检查
机构管理
案事件调查
…

网络安全等级保护带来的意义

责任分担

完成等级保护工作意味着你单位目前的安全现状是符合要求的。如果没有进行等级保护工作意味着你最基本的工作都没做，一旦发生安全事件，单位将承担主要责任，网监部门会按照相关法律规定进行严厉的处罚。

安全体系

以等级保护为标准开展安全建设，可以让单位自身安全建设更加体系化，从物理、网络、主机、应用和数据多个方面成体系的进行安全建设，再也不是头痛医头脚痛医脚。

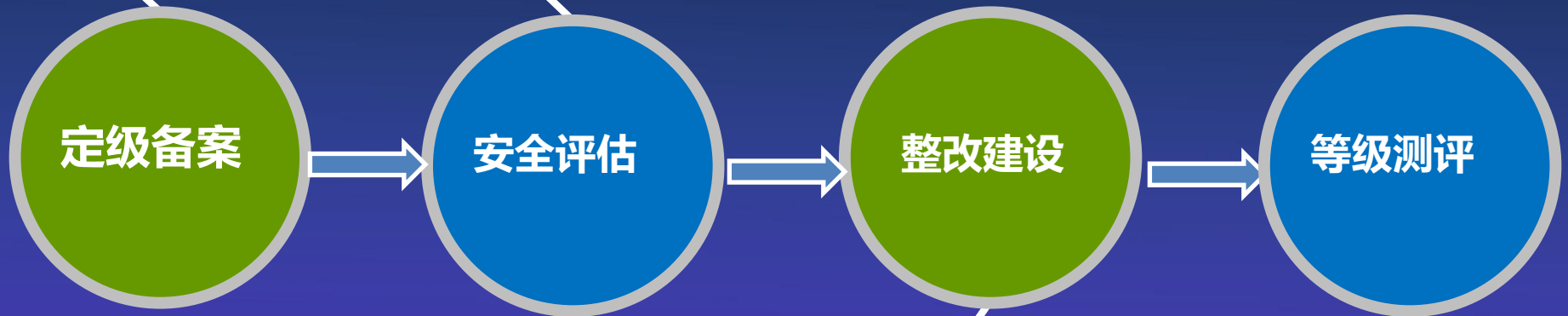
Part 02

等级保护总体工作流程

等级保护工作总体流程

梳理信息系统情况，确定等级，提交定级报告和备案表到当地网警部门。

聘请第三方测评机构进行安全检查和评估，找出现状问题，提交问题报告和整改方案。



根据差距检查结果，进行技术+产品+人工+管理制度等方面的整改建设工作

聘请第三方测评机构，进行等级保护测评工作，提交相应的等级保护测评报告到网警部门

信息系统的安全保护等级

等级	对象	侵害客体	侵害程度	监管强度
第一级：	自主建设	公民、法人和其他组织的合法权益	损害	自主保护
第二级：	一般信息系统	公民、法人和其他组织的合法权益	严重损害	指导
		社会秩序和公共利益	损害	
第三级：	一般信息系统	社会秩序和公共利益	严重损害	监督检查
		国家安全	损害	
第四级：	重要信息系统	社会秩序和公共利益	特别严重损害	强制监督检查
		国家安全	严重损害	
第五级：	特别重要信息系统	国家安全	特别严重损害	专门监督检查

三级系统每年开展测评，四级系统每半年开展一次测评

《信息系统安全保护等级定级指南》GB/T 22240-2008

游戏行业-信息系统的安全保护等级

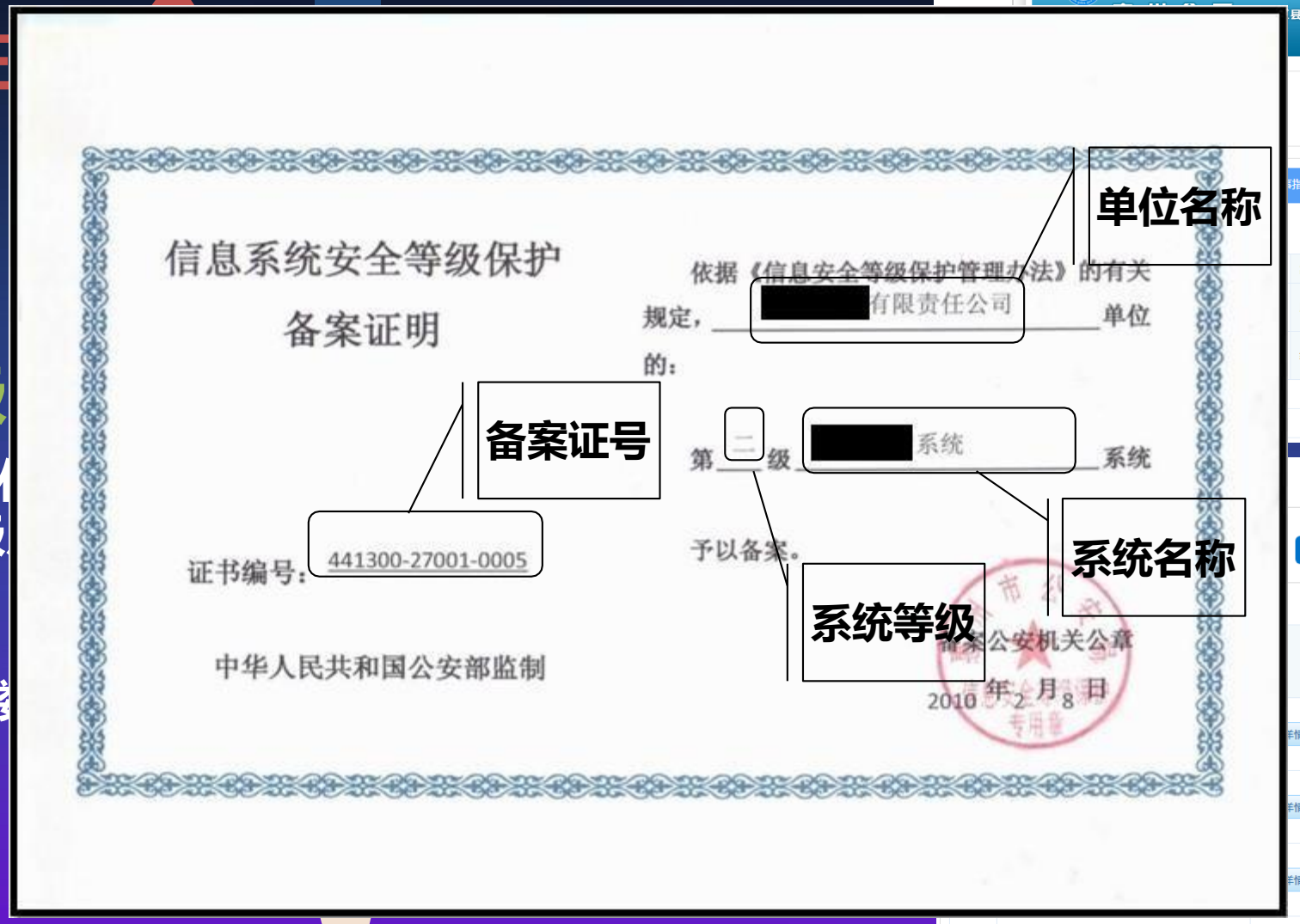
序号	信息系统	建议安全保护等级			
		实名用户数量不足三十万级	实名用户数量达到三十万级	自有支付系统	纯宣传类
1	门户网站系统	-	-	-	第二级
2	用户管理系统 认证计费系统	第二级	第三级	第三级	-
3	游戏论坛、社区等交互系统	第二级	第三级	-	-
4	战网类游戏平台	第二级	第三级	第三级	-
5	游戏信息系统	第二级	第三级	第三级	-

定级备案

发备案证

确认等级

★信息系统安全
等级确定（二级
上）
★填写备案表
★生成备案电子



华为云技术私享会

测评内容

- 数据备份及恢复
- 应用安全
- 主机安全
- 网络安全
- 物理安全
- 系统运维管理
- 系统建设管理
- 人员安全管理
- 安全管理制度
- 安全管理机构

1.安全控制间测评

2.层面间测评

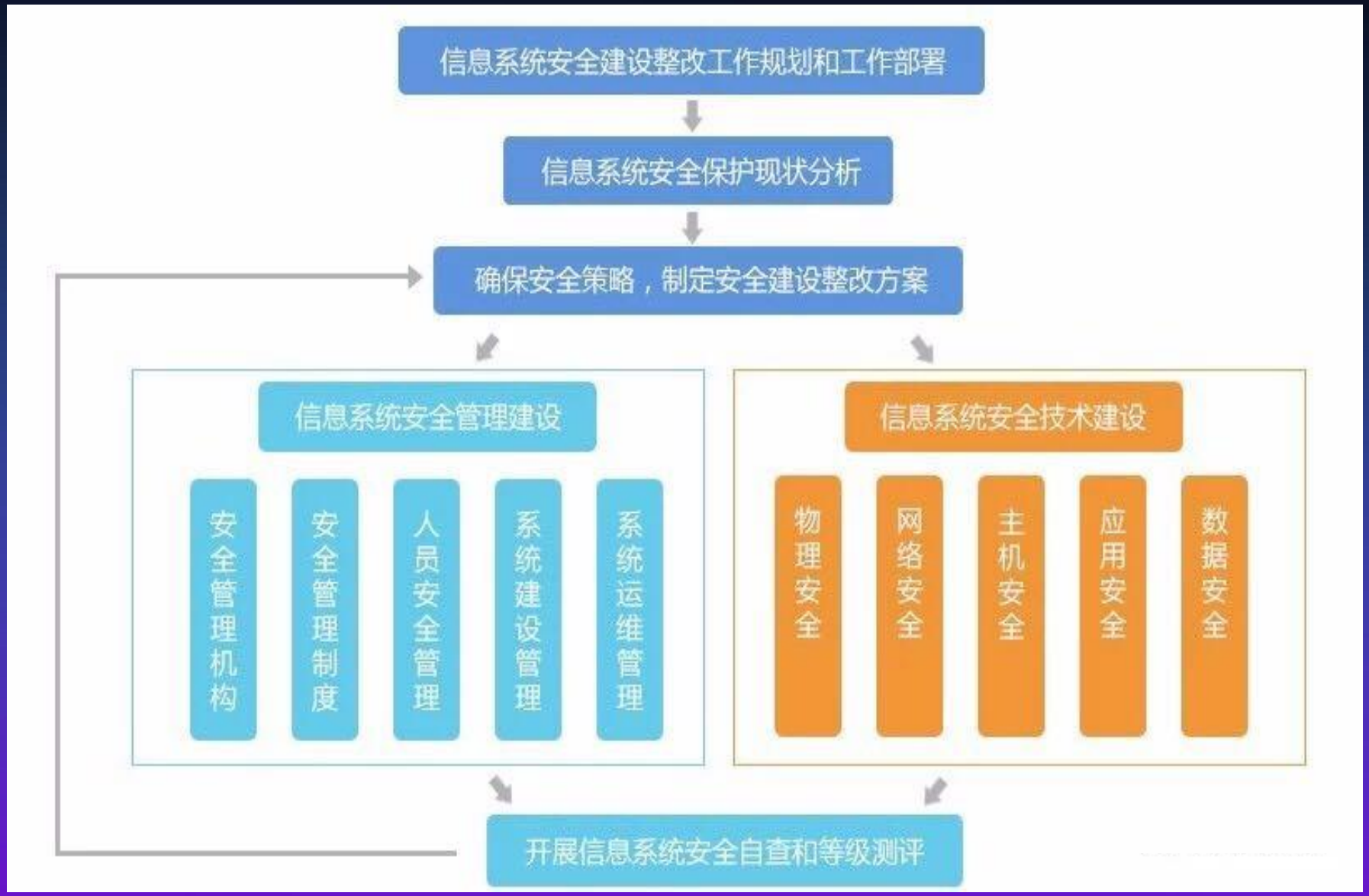
3.区域间测评

测评指标

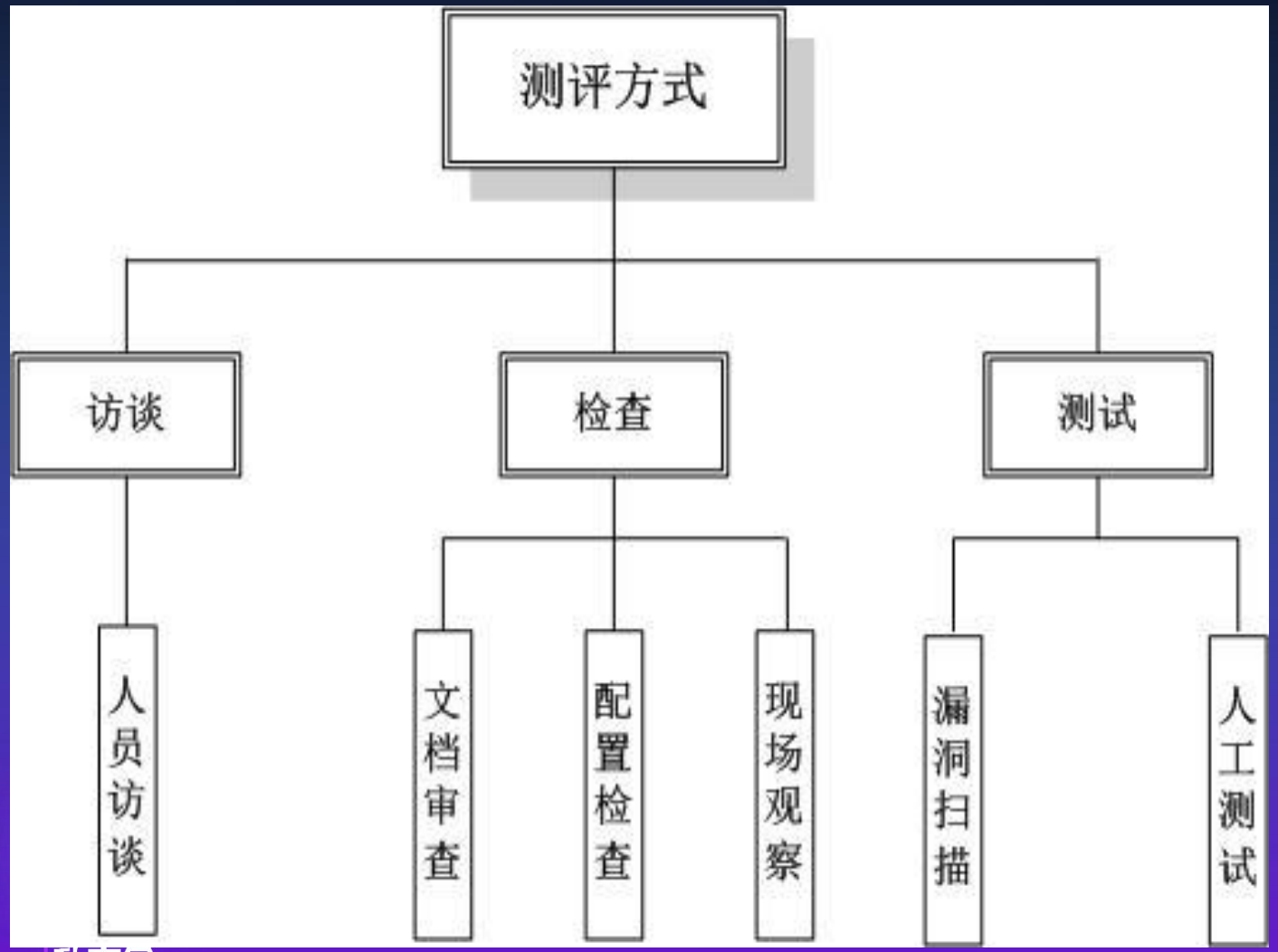
安全要求类	层面	一级	二级	三级	四级
技术要求	物理安全	9	19	32	33
	网络安全	9	18	33	32
	主机安全	6	19	32	36
	应用安全	7	19	31	36
	数据安全及备份恢复	2	4	8	11
管理要求	安全管理制度	3	7	11	14
	安全管理机构	4	9	20	20
	人员安全管理	7	11	16	18
	系统建设管理	20	28	45	48
	系统运维管理	18	41	62	70
合计	/	85	175	290	318

《信息安全技术 信息系统安全等级保护基本要求》 GBT 22239-2008

等保测评流程



等保测评方式



在等级保护测评实施过程中，需配合事项有：

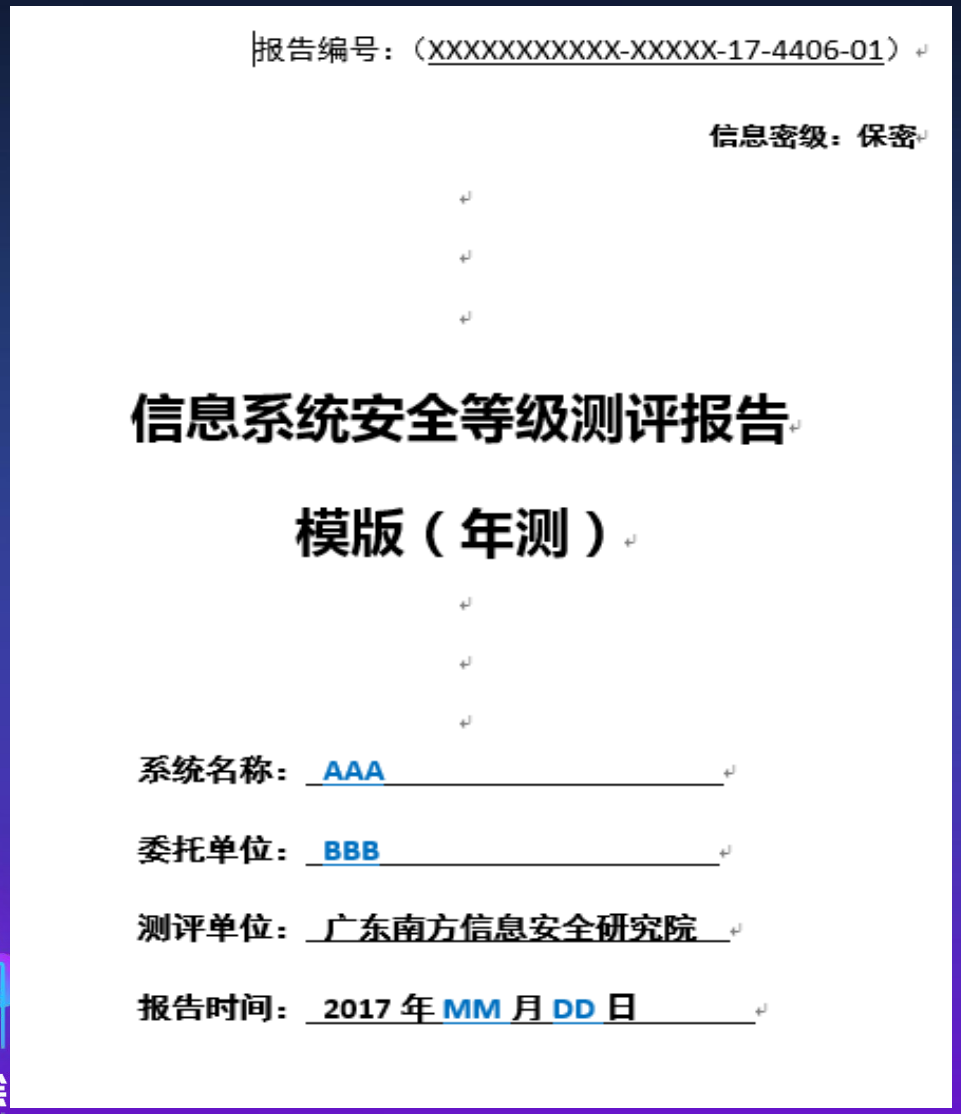
- 明确参与本项目的信息主管领导、项目负责人和各管理人员
- 提供测评的办公环境、网络环境
- 提供被测评系统的相关建设资料、测评账号、网络拓扑等
- 在系统定级、备案时须配合进行报告和备案表的盖章、递送
- 在提供现有的管理制度集
- 物理机房的进出流程等

信息系统等级保护测评结论

综合**单元测评、整体测评、测评结果汇总、风险分析**和评价部分的测评与分析结果，对信息系统基本安全保护状态进行综合判断，并给出等级测评结论，表述为**“符合（100分）、“基本符合（60-99分）”或者“不符合（<60分）”**

测评结论	符合性判别依据	综合得分计算公式
符合	信息系统中未发现安全问题，等级测评结果中所有测评项得分均为5分。	100分
基本符合	信息系统中存在安全问题，但不会导致信息系统面临高等级安全风险。	$\frac{\sum_{k=1}^{p} \text{测评项的多对象平均分} \times \text{测评项权重}}{\sum_{k=1}^{p} \text{测评项权重}} \times 20$，$p$为总测评项数，不含不适用的控制点和测评项，有修正的测评项以5.5章节中的修正后测评项符合程度得分带入计算。
不符合	信息系统中存在安全问题，而且会导致信息系统面临高等级安全风险。	$60 - \frac{\sum_{j=1}^{l} \text{修正后问题严重程度值}}{\sum_{k=1}^{p} \text{测评项权重}} \times 12$，$l$为安全问题数，$p$为总测评项数，不含不适用的控制点和测评项。
注：修正后问题严重程度赋值结果取多对象中针对同一测评项的最大值。		

信息系统等级保护测评报告



报告编号：（XXXXXXXXXXX-XXXXX-17-4406-01）

信息密级：保密

信息系统安全等级测评报告

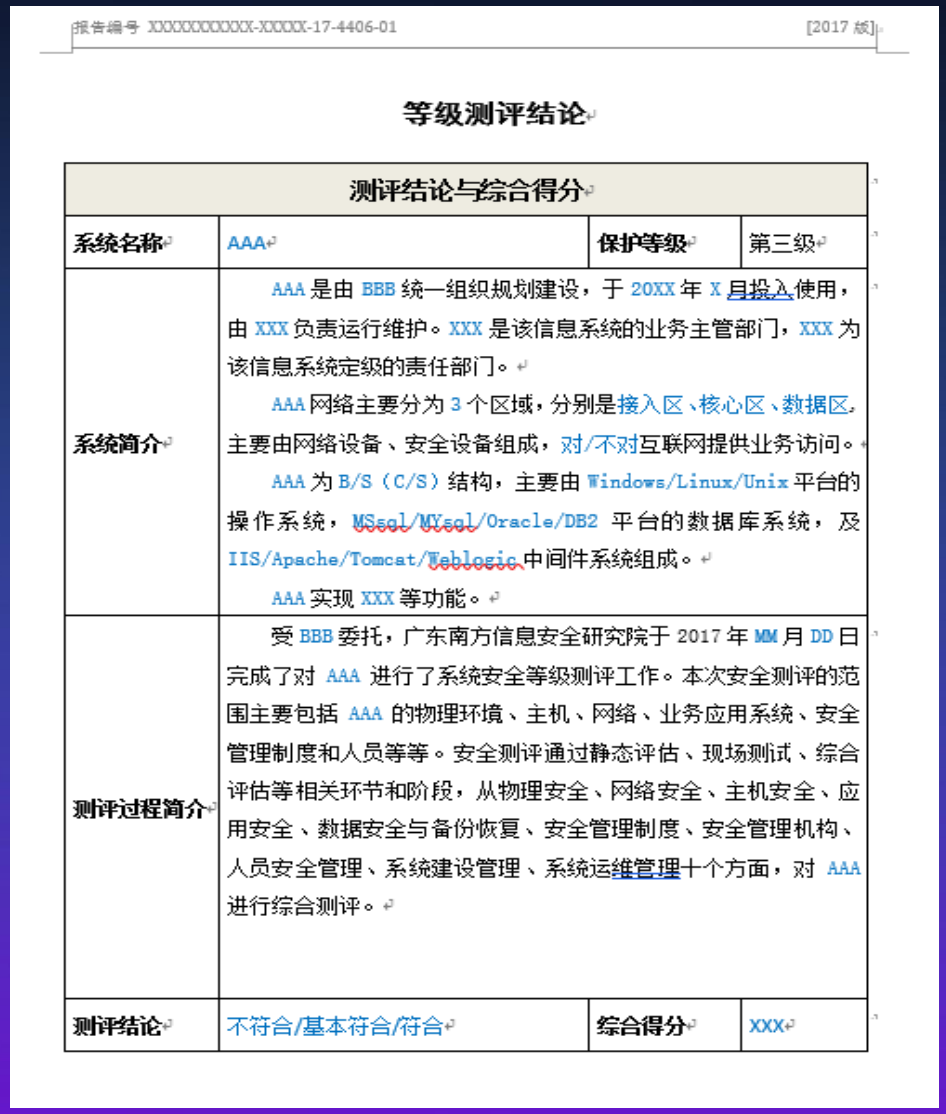
模版（年测）

系统名称：AAA

委托单位：BBB

测评单位：广东南方信息安全研究院

报告时间：2017 年 MM 月 DD 日



等级测评结论

测评结论与综合得分			
系统名称	AAA	保护等级	第三级
系统简介	AAA 是由 BBB 统一组织规划建设，于 20XX 年 X 月投入使用，由 XXX 负责运行维护。XXX 是该信息系统的业务主管部门，XXX 为该信息系统定级的责任部门。 AAA 网络主要分为 3 个区域，分别是接入区、核心区、数据区，主要由网络设备、安全设备组成，对/不对互联网提供业务访问。 AAA 为 B/S（C/S）结构，主要由 Windows/Linux/Unix 平台的操作系统，MSsql/MYsql/Oracle/DB2 平台的数据库系统，及 IIS/Apache/Tomcat/Weblogic 中间件系统组成。 AAA 实现 XXX 等功能。		
测评过程简介	受 BBB 委托，广东南方信息安全研究院于 2017 年 MM 月 DD 日完成了对 AAA 进行了系统安全等级测评工作。本次安全测评的范围主要包括 AAA 的物理环境、主机、网络、业务应用系统、安全管理制度和人员等等。安全测评通过静态评估、现场测试、综合评估等相关环节和阶段，从物理安全、网络安全、主机安全、应用安全、数据安全与备份恢复、安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理十个方面，对 AAA 进行综合测评。		
测评结论	不符合/基本符合/符合	综合得分	XXX

提交测评报告回执

提交测评报告回执

[redacted]根据国家信息安全等级保护的政策要求、标准规范要求，于2015年[redacted]月[redacted]日提交了[redacted]网站系统、[redacted]管理信息平台系统、[redacted]业务办公系统、[redacted]信息联动平台系统、[redacted]资源平台系统的信息系统安全等级测评报告。

广州市信息安全等级保护工作协调小组办公室

2015年9月8日

Part 03
机构介绍

关于南方信息安全研究院

- 广东南方信息安全研究院成立于2009年4月，是经广东省科技厅批准、民政厅注册的非盈利性质的民办非企业单位。
- 是公安指定的**国家信息安全等级保护测评机构（粤-006）**。
- 通过2018年CNAS能力验证。
- 信委、省公安厅及各地市公安网监指定重点领域网络与信息安全检查工作技术支撑单位。

授权资质

计算机信息系统安全等级证书

电子政务服务能力证书

信息安全等级保护测评机构推荐证书

ISO 27001：2013

AAA级信用等级证书

华为云技术私享会

典型案例

政府单位

- 广东省财政厅
- 广东省水利厅
- 广东省交通厅
- 广东省审计厅
- 广东省科学技术厅
- 广东省国土资源厅
- 广东省文化厅
- 广东省住房和城乡建设厅
- 广东省知识产权局
- 广东省国家税务局
- 广州市教育局
- 越秀区教育局及其下属学校（100多个）
- 佛山市公安局
- 潮州市公安局
- 中山市公安局
- ……

通信行业及云平台

- 中国移动（深圳、肇庆、广东、广州）
- 中国联合网络通信（潮州、广州、珠海）
- 中国联合网络通信（广东省分公司、肇庆）
- 中国联通广东省分公司
- 中国电信（肇庆、汕头、潮州）

- 中山大学国家超级计算广州中心云超算平台
- 品高云平台
- ……

典型案例

大型国企

- 广州地铁（含广佛线）
- 广汽集团（含下属投资企业）
- 广东省粤电集团（含28个下属单位）
- 南方报业传媒集团
- 广东交通集团
- 广东粤海控股集团
- 珠江船务股份
- 南方电网（省内下属所有电厂及供电局）
- 粤海商业数据有限公司
- 珠海水务集团
- 广东电网
- 珠海烟草、汕尾烟草
- 航运集团
- 越秀地产
- 保利地产
- 广东省广业资产经营有限公司
- ……

金融证券

- 粤海财务控股
- 粤电财务
- 交通银行
- 光大银行广州分行
- 惠州联讯证券
- 广州证券
- 万联证券有限责任公司
- 安联财产保险
- 广东新佳联投管理有限公司
- 东莞证券有限责任公司
- 东莞华联期货有限公司
- 广州期货有限公司
- 诚汇通金融
- 第三方金融
- 前海惠德金融
- 万惠投资
- ……

典型案例

广电传媒

- 广东省电视台
- 广州市电视台
- 广东广电网络
- 南方电视台
- 肇庆人民广播电台
- 珠海斗门电视台
- 惠州广播电视传媒集团
- 佛山电视台
- 佛山广播电视网络
- 佛山人民广播电台
- 东莞广播电视台
- 珠江传媒集团
- 岭南美术出版社
- 南方报业传媒集团
- 惠州市日报传媒集团
- ……

电力生产

- 云浮供电局
- 广东电力
- 广州蓄能水电厂
- 广州蓄能水电厂
- 广东国华粤电台山发电
- 广东珠海金湾发电
- 阳西海滨电力发展
- 广东韶关粤江发电
- 深能合和电力（河源）
- 广东惠州天然气发电
- 珠海深能洪湾电力
- 广东粤电大埔发电
- 广东粤电新丰江发电
- 惠州平海发电厂
- 广东粤电长潭发电
- ……

典型案例

大型活动安保工作

- **广州市亚运会（含残运会）**
- 信息安全检查服务项目
- **广州市信息安全测评中心**
- 电子政务外网信息系统上线、入网、信息化项目
- **广东省经信委**
- 重点领域网络与信息安全抽查工作
- **肇庆市网信办**
- 关键信息基础设施安全检查工作
- **第十九次全国代表大会**
- 广东省网络安全保障工作
- **2017年广州财富全球论坛**
- 广东省网络安全保障工作
- ……

卫生医疗

- **广东省人民医院**
- **广东省第二人民医院**
- **广东省中医院**
- **广州市卫生局**
- **东莞市卫生局**
- **珠海市卫生局**
- **佛山市卫计局**
- **惠州市卫计局**
- **广州市中医医院**
- **广州中医药大学第一附属医院**
- **南方医科大学南方医院**
- **广东省疾病预防控制中心**
- **中山大学中山眼科医院**
- **茂名市人民医院**
- **广东省中医院珠海医院**
- ……


HUAWEI
IT大咖说
知识共享平台
华为云
技术
私享会
THANK YOU

HUAWEI

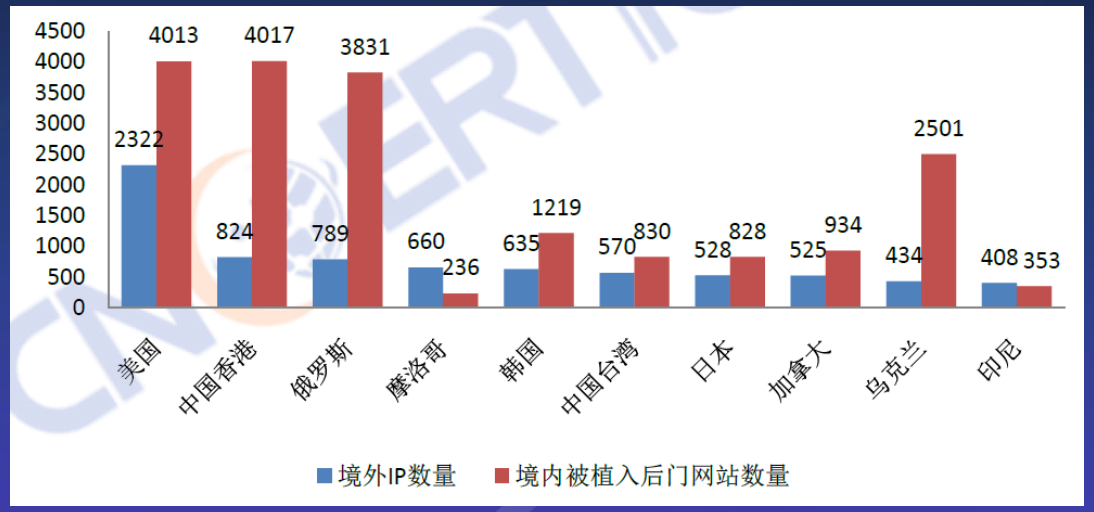
HUAWEI IT大咖说 知识共享平台

华为云
技术
私享会

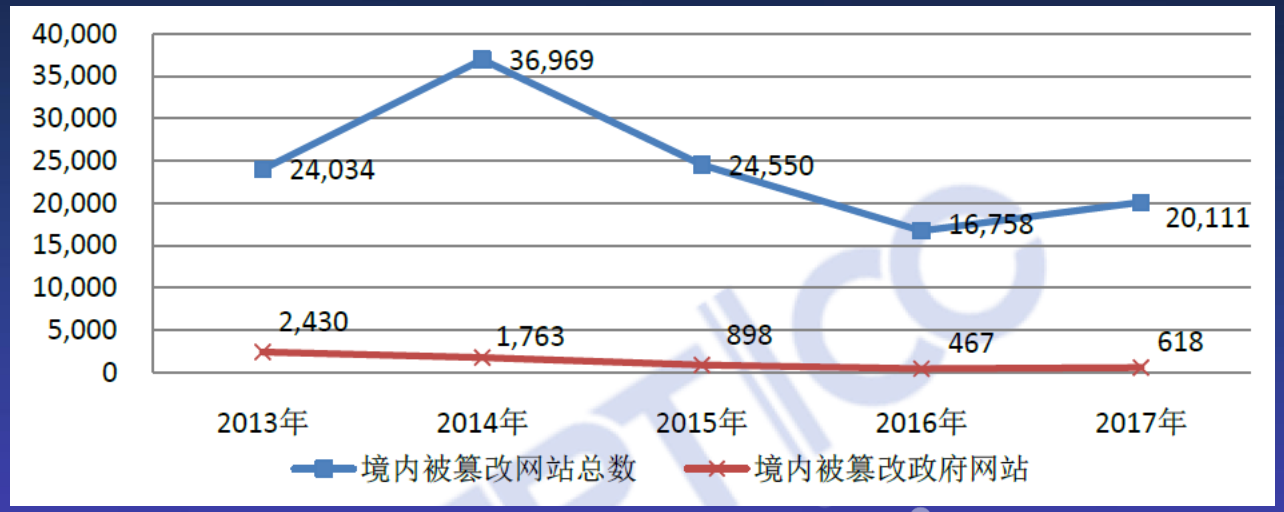
华为云游戏网站Web防护方案

闫峰 华为云应用安全产品总监

中国互联网Web安全现状



2017年境外向我国境内网站植入后门IP地址所属国家或地区TOP10



2013 - 2017年我国境内被篡改网站数量情况

数据来源：国家互联网应急中心《2017年我国互联网网络安全态势综述》

游戏行业Web安全事件

A游戏官网游戏入口被篡改B游戏

2017年10月，某游戏官网被黑客植入非法内容

2018年2月，某游戏网站因泄漏用户数据导致大量账号被盗

Web应用防火墙，专为Web安全而生

基于业务属性，配置针对性的安全策略

通过漏洞扫描服务，发现潜在漏洞

事前准备

扫描、探测行为的拦截

注入、跨站等OWASP 10攻击行为拦截

0day威胁防御

CC攻击的精准防护

事中防御

爬虫、自动化软件的拦截

Web应用防火墙

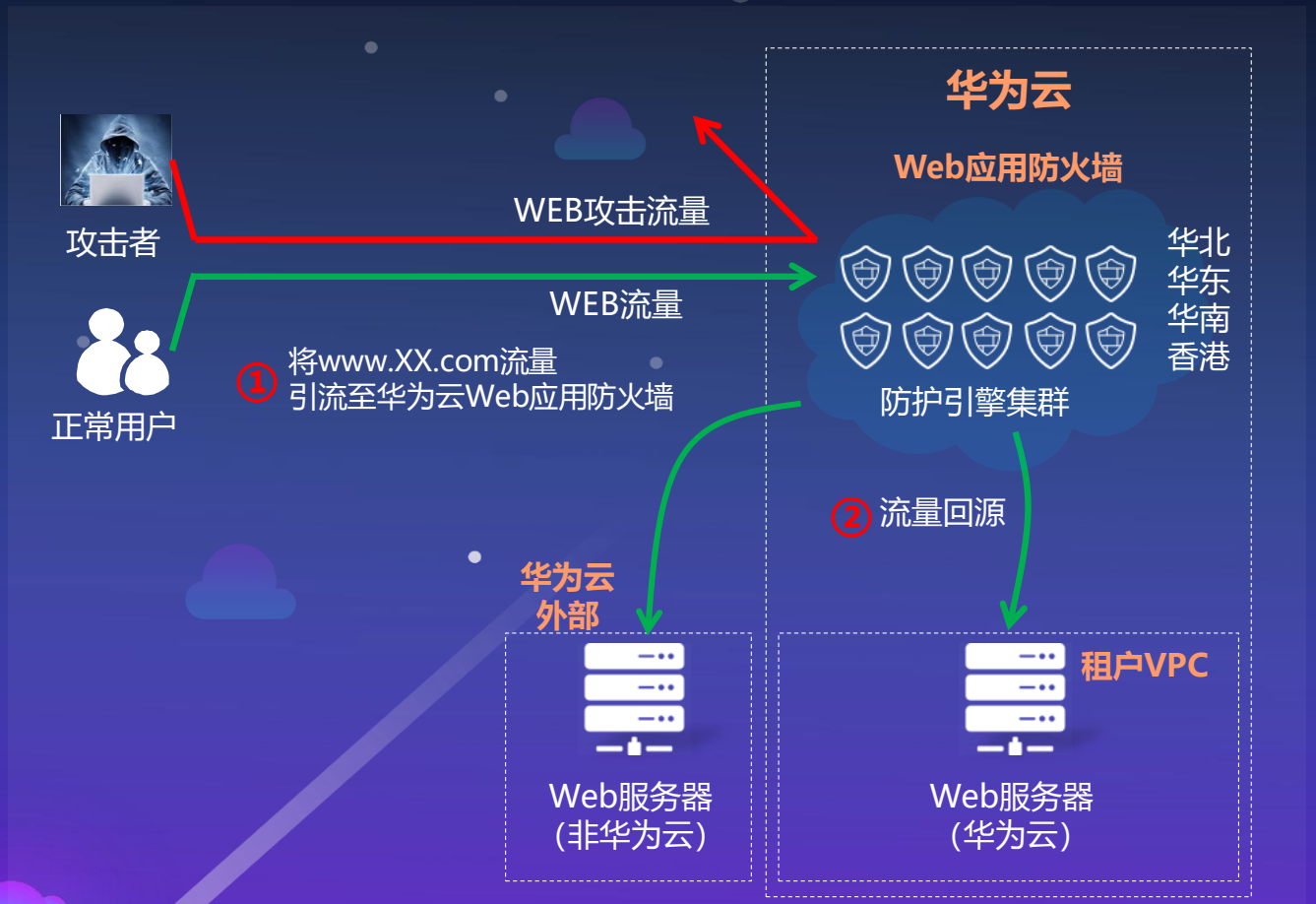
事后审计

输出丰富的安全态势

输出详细的安全事件

华为云技术私享会

华为云WAF，Web服务的“最佳搭档”



“WAF的主要好处就是可以防范企业开发的Web应用代码中“自己造成的”安全漏洞，并且防范主流Web应用软件中的安全漏洞。” ——Gartner 2017

技术创新

- **三引擎架构：** **独创**语义+正则+AI三引擎架构，威胁检出率**提升30%以上**
- **动态防爬虫：** **领先**基于加密技术的防爬虫算法，有效防止爬虫导致的数据泄露
- **防CC：** **领先**IP+Cookie双重验证阻断CC攻击，有效提升业务可用性

专业可靠

- **国内异地容灾：** 确保业务不中断
- **实时监控：** 专业运营团队7*24小时监控
- **隐私保护：** 防止租户隐私泄露

简单易用

- **零维护成本：** 无组件安装，零运维
- **极简UI：** 界面简洁易懂
- **专家咨询：** 安全专家在线答疑解惑

三引擎架构，威胁检出率提升30%以上

正则引擎

防御OWASP通用攻击

语义引擎

高效防护XSS/SQL注入攻击

AI引擎

防御高级威胁/0day等攻击

领先的动态防爬虫算法，有效防止数据泄露

JS JavaScript解析

浏览器指纹

加密验证技术

三管齐下，精准识别&防御CC攻击

基于IP

根据IP地址识别客户端

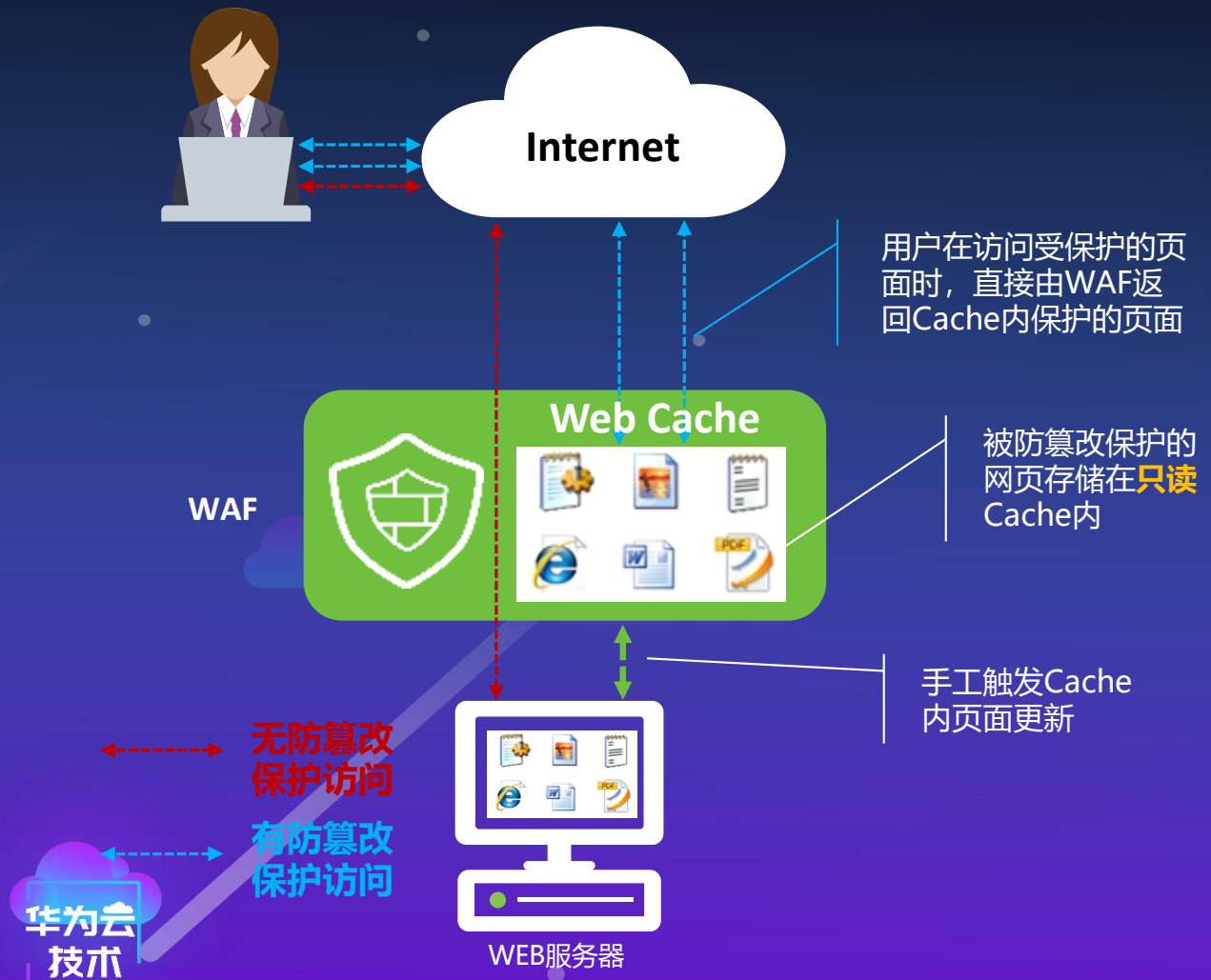
基于Cookie

根据Cookie字段识别客户端

基于AI

利用AI技术实现“人机识别”

多重防护机制，有效阻止网页被篡改



挂马检测

从源头上阻断网页被篡改

Web Cache机制

缓存网页，“视觉”防篡改

健康状态监测

监控网页健康状态，实时告警

AI引擎，智能推荐防御规则

场景	AI引擎
黑名单	自动识别有恶意行为的IP，并推荐给用户进行拦截。
CSRF防护	自动找出经常被盗链的页面（URI），并自动识别正常情况下的上一跳，推荐Referer字段
恶意爬虫	识别有爬虫行为的IP，找出对应特征（如IP、UA），并推荐给用户进行拦截
隐私防护	自动识别具有用户名、密码、用户地址等敏感信息的页面
误报检测	自动分析用户所选的误报条目，总结误报原因，向用户推荐白名单策略
CC攻击	对不同的页面，不同的客户端IP，自动分析出总访问次数门限值和各个IP访问次数门限值
WebShell	根据页面之间的链接关系和用户访问频次识别出WebShell页面

专业可靠，源于华为安全的16年积累

稳定可靠

冗余保障、异地容灾

专业易用

规则库实时更新、day漏洞修补

隐私保护

华为“三不”原则

华为云
技术
私享会

深圳某游戏公司的Web防护方案

客户介绍

XX游戏是中国领先的互联网游戏开发和运营商，致力于多元化的网络游戏开发、运营和授权代理，拥有优秀的研发、发行团队，并不断更新技术和理念，一直在行业内保持着领先地位。

解决方案

为XX游戏提供DDoS高防、Web应用防火墙等**弹性**安全服务。

客户价值

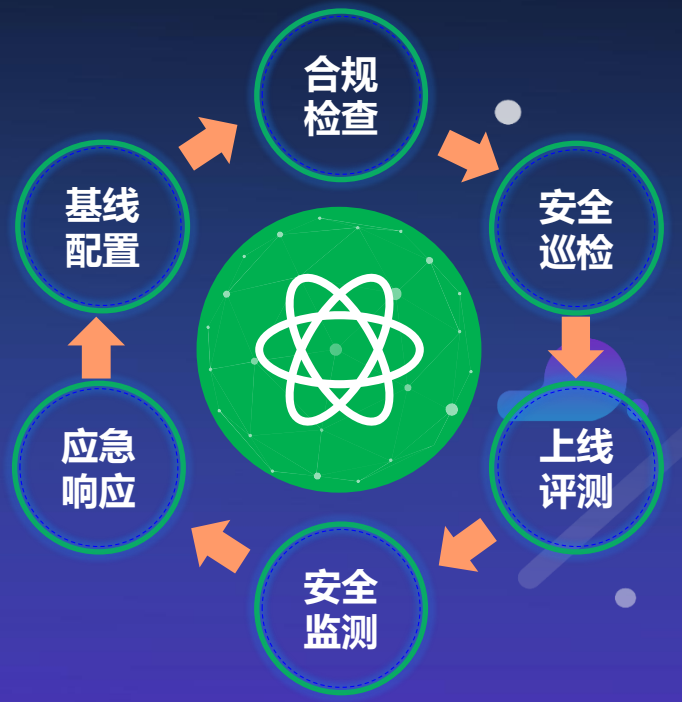
在WAF上线以来，平均每天成功抵御数万次的Web攻击，为XX游戏的在线业务和在线交易保驾护航。WAF灵活的弹性架构可以很好的满足XX游戏当前和未来的业务需求。

漏洞扫描服务全面升级，覆盖业务全生命周期

全面升级

开发阶段

（安全）运维阶段



漏洞扫描服务

- 编码安全性检查
- 主机扫描
- Web扫描
- 逻辑扫描
- 数据库扫描
- 安全基线
- 弱口令
- 中间件扫描

华为云技术私享会

THANK YOU

HUAWEI

HUAWEI IT大咖说 知识共享平台

华为云
技术
私享会

云上数据库一体化保险箱

——华为云数据库安全服务

陈龙　华为云安全解决方案总监

数据库安全客户关注点1：等保合规

【第二十一条】 国家实行网络安全等级保护制度。网络运营者应当按照**网络安全等级保护制度**的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

- （一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；
- （二）采取防范计算机病毒和**网络攻击、网络侵入**等危害网络安全行为的技术措施；
- （三）采取**监测、记录网络运行状态、网络安全事件的技术**措施，并按照规定留存相关的网络日志不少于六个月；
- （四）采取**数据分类、重要数据备份和加密**等措施；
- （五）法律、行政法规规定的其他义务。

- **解读：**
- （二）本条要求采取防范网络入侵的措施。对数据库而言，可采用数据库防火墙，保护数据库不被入侵
- （三）本条要求监测运安全事件。对数据库而言，可采用数据库监控和审计，对攻击行为进行记录；且日志的存储期限不低于6个月。
- 法律责任：第五十九条：（警告）->（1~10万罚款）
- 责任人：5千~5万罚款
- 此外，在【第二十五条：应急预案】，【第二十八条：配合协助】，【第四十二条：个人信息保护】等也有类似要求。

游戏 | 狭义政府 电子政务 公共服务 | 三甲医院 | 互联网金融 信用社 证券公司 | 普教 高校 | 科研型企业 | 电力公司 | 轨道交通 | …

数据库安全客户关注点2：敏感数据泄露

敏感数据来源于哪里

数据泄露的主要途径

1. 黑客攻击：SQL注入，脱库撞库，高级持续性威胁，弱口令扫描等
2. 内部人员泄露：滥用和恶意使用云服务，内外串通等
3. 第三方集成商/开发商：数据未加密/脱敏，身份、凭证和访问管理不足，不安全的接口和应用程序编程接口等

数据脱敏是防止数据泄漏的主要方法

脱敏所有：所有数据都被脱敏。

空：以空字符串返回。

信用卡脱敏：显示信用卡的最后四位数字，其他字符被脱敏。

显示随机数：显示随机数而不是原始数据。

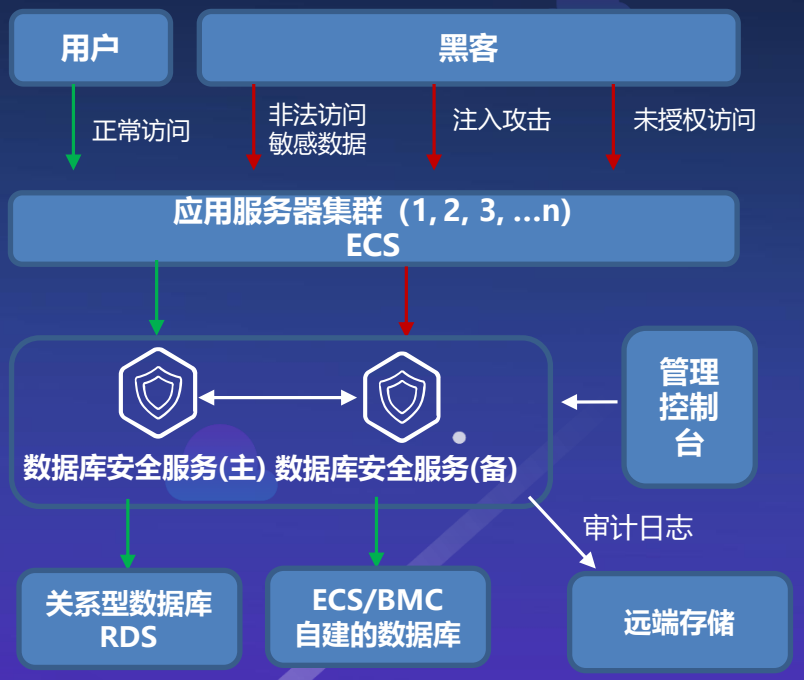
全邮箱脱敏：电子邮件地址的用户名和域都被脱敏。例如： ‘abcdefg@company.com’ 转换为 ‘XXXXXXX@XXXXXXX.com’

隐藏所有数字：脱敏字符串中的所有数字。例如：邮政编码中的所有数字都被脱敏如下： ‘123456’ 转换为 ‘******’

固定字符串：用 ‘CONFIDENTIAL’ 替换列中的所有值

华为数据库安全服务整体介绍

华为云数据库安全服务架构



华为云数据库安全服务特点

部署简单

- 首创的数据库反向代理技术
- 适合云的架构，并获得专利保护

功能丰富

- 在目前公有云提供商中，是数据库安全功能最全的产品

防护实时

- 反向代理部署架构真正做到实时阻断恶意请求

超低误报

- 支持业界通用的SQL注入特征库
- 叠加机器学习模型+评分机制，误报率低

多种合规

- 内置合规知识库，满足法律法规遵从
- 动态脱敏技术，敏感数据实时保护

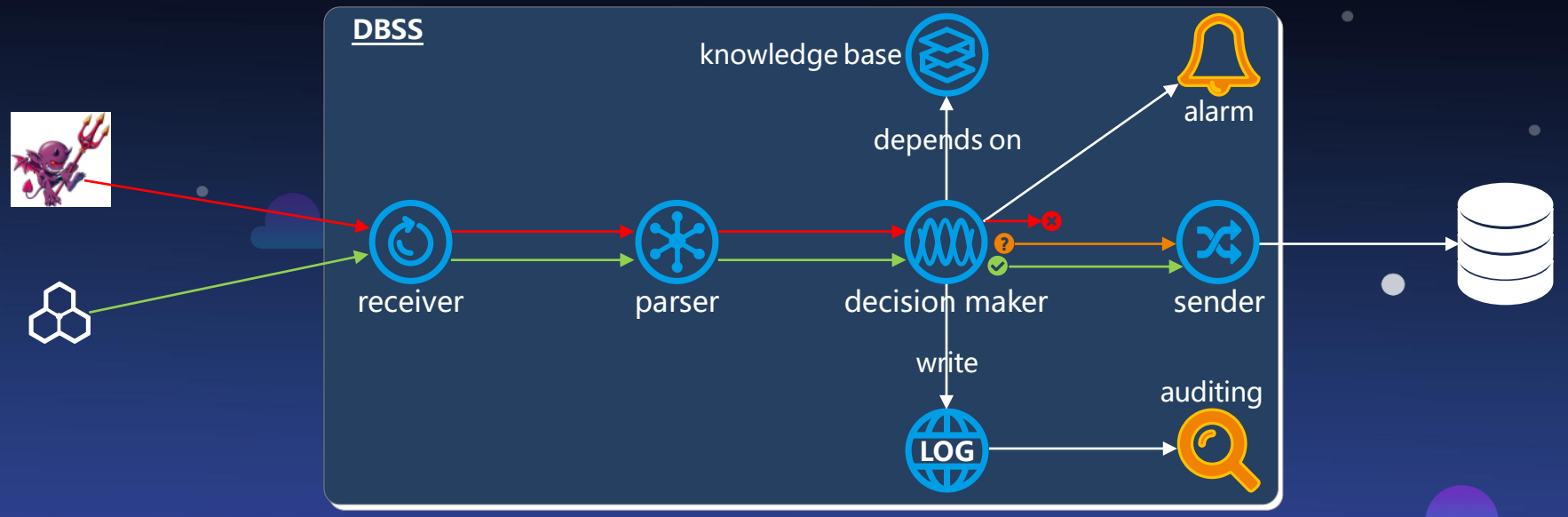
精细控制权限

- 弱耦合机制，不修改用户权限同时，实现细粒度权限控制

华为云 技术 私享会

HUAWEI

从一个示例看反向代理技术对数据库业务的安全防护



示例：
select * from user where username = 'c' or 1 =1

1. 该SQL具备攻击的三个潜质：
① 查询所有，而不是所需
② 用户名明显是非法的
③ 恒等式1=1

4. 对解析后的SQL匹配知识库，识别是否有风险：
① 违反规则，用户可以选择Block，并告警
② 不违反规则，放行后，转发到给DB
③ 记录日志，供审计分析

client → receiver → parser → decision maker → sender → DB

2. 原封不动地接收SQL请求

3. 不同数据库有各自协议，支持：
✓ MySQL、SQL Server、PG等
✓ 无法识别的协议发送到DB

5. 显示该SQL无法通过
✓ 设置了block，则直接返回并告警
✓ 设置不阻塞，会下发到DB并告警

事前：数据库中针对数据泄露保护的几个设计

敏感数据发现

- ✓ 根据合规要求**自动发现**敏感数据，一键进行合规检查
- ✓ 根据发现结果**自动生成**规则，降低运维复杂度
- ✓ 用户**自定义正则表达式**，满足特定场景数据发现要求
- ✓ 用户**自定义发现频率**，可定期检查持续改进

数据动态脱敏

- ✓ **细粒度脱敏**，实现行级、列级、表级、视图级脱敏，以及按指定条件脱敏
- ✓ **高性能**的数据动态脱敏，不影响数据库和应用，非生产应用访问生产数据时数据不泄露

法律合规遵从

PCI DSS 第三方支付行业数据安全标准

HIPAA 美国医疗行业合规法案

Sarbanes-Oxley Act 塞班斯法案

- ✓ 内置PCI-DSS、HIPAA、SOX等**合规知识库**，满足国际企业合规要求
- ✓ **自定义合规**规则
- ✓ 生成友好的遵从**合规报告**，方便审计

华为云技术私享会

示例：敏感数据发现的配置和结果呈现

- 某个金融客户数据库中有员工敏感数据。
- 数据库被黑客攻破以后，将敏感数据全盗取。

```
mysql> select * from workmates;
+----+-----------+-----+---------+------------+-----+--------------------+------------------+
| id | name      | sex | addr    | birth      | age | email              | creditcard       |
+----+-----------+-----+---------+------------+-----+--------------------+------------------+
|  1 | Guojing   | m   | Shaanxi | 1988-04-28 |  29 | guojing@gmail.com  | 6222222222222222 |
|  2 | Yangguo   | m   | Hubei   | 1987-12-01 |  30 | yangkang@qq.com    | 6333333333333333 |
|  3 | Huangrong | f   | Zhejiang| 1988-08-15 |  29 | huangrong@126.com  | 6444444444444444 |
|  4 | Lilei     | m   | Beijing | 1977-05-21 |  40 | lilei@gmail.com    | 6555555555555555 |
|  5 | Han       | f   | Xinjiang| 1978-01-05 |  39 | hanmeimei@163.com  | 6666666666666666 |
+----+-----------+-----+---------+------------+-----+--------------------+------------------+
5 rows in set (0.00 sec)
```

- 用户使用敏感数据发现功能：发现了敏感字段。客户选择了一键生成脱敏规则。

表	列	匹配类型	合规	级别	扫描行数	匹配结果	监控规则	脱敏规则
confidential.workmates	email	E-Mail	HIPAA	suspected	6	100%	☐	☑
confidential.workmates	creditcard	regex-sample	GROUP-SAMPLE	sensitive	6	17%	☐	☑

生成

示例：敏感数据发现的配置和结果呈现

- 客户选择一键生成了脱敏规则

成功创建2条脱敏规则

> 显示执行信息

CSV

表	列	匹配类型	合规	级别	扫描行数	匹配结果	监控规则	脱敏规则
confidential.workmates	email	E-Mail	HIPAA	suspected	6	100%	☐	☑
confidential.workmates	creditcard	regex-sample	GROUP-SAMPLE	sensitive	6	17%	☐	☑

- 黑客再次查询的时候，就发现敏感数据被脱敏了：

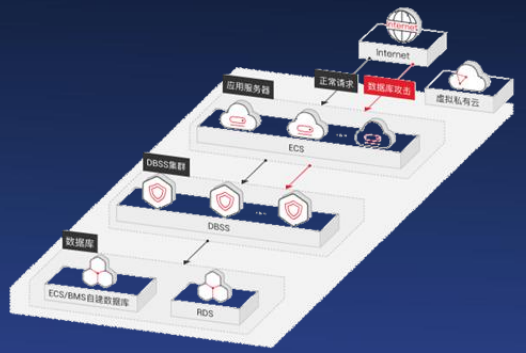
```
mysql> select * from workmates;
+----+-----------+-----+----------+------------+-----+--------------------+--------------------+
| id | name      | sex | addr     | birth      | age | email              | creditcard         |
+----+-----------+-----+----------+------------+-----+--------------------+--------------------+
|  1 | Guojing   | m   | Shaanxi  | 1988-04-28 |  29 | XXXXXXXXXXXXXXXXX  | XXXXXXXXXXXXXXXXX  |
|  2 | Yangguo   | m   | Hubei    | 1987-12-01 |  30 | XXXXXXXXXXXXXXX    | XXXXXXXXXXXXXXXXX  |
|  3 | Huangrong | f   | Zhejiang | 1988-08-15 |  29 | XXXXXXXXXXXXXXXXX  | XXXXXXXXXXXXXXXXX  |
|  4 | Lilei     | m   | Beijing  | 1977-05-21 |  40 | XXXXXXXXXXXXXXX    | XXXXXXXXXXXXXXXXX  |
|  5 | Han       | f   | Xinjiang | 1978-01-05 |  39 | XXXXXXXXXXXXXXXXX  | XXXXXXXXXXXXXXXXX  |
+----+-----------+-----+----------+------------+-----+--------------------+--------------------+
5 rows in set (0.04 sec)
```

事中：数据库防火墙对于非法访问和入侵的防御设计

细粒度访问控制

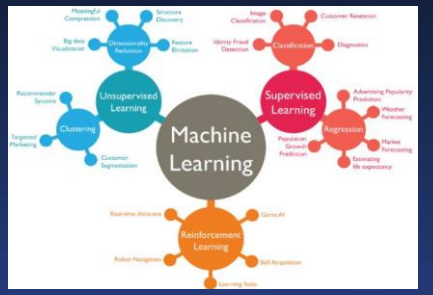
- ✓ **基于角色的访问控制**，如：
  - 查询者分配只读权限
  - DBA只分配创建权限，不分配读权限
- ✓ **最小权限分配原则**，实现客户化定义，谁在什么时间允许干什么
- ✓ **细粒度管控，**可以到表、行、列、事件等

数据库入侵防御



- ✓ **内置知识库**，基于攻防经验的入侵检测、防御
- ✓ **SQL注入攻击防御，**可疑或者危险的查询无法到达数据库
- ✓ 针对特定安全等级**设置门槛值**
- ✓ 可以整合业界**攻击特征库**，减少误报率

规则自学习



- ✓ **机器学习能力**，定期自我学习，生成安全模式规则，应用到数据库防火墙策略中
- ✓ 学习后的规则**可直接**应用于生产环境
- ✓ 可创建查询组，作为防火墙策略的**有效模式规则**（白名单）或者作为一个**不被允许的模式**（黑名单）

示例：数据库防火墙的策略定义和效果呈现

- 客户近期发现数据库的数据频频收到注入攻击。
- 注入的攻击最后呈现的语句如下：

```
mysql> select * from userinfo where name='' or '1'='1' and passwd = '' or '1'='1';
+----+-----------+---------------+---------+
| id | name      | passwd        | comment |
+----+-----------+---------------+---------+
|  1 | 郭靖      | Guojing@12    | NULL    |
|  2 | 黄蓉      | Huangrong@12  | NULL    |
|  3 | 洪七公    | Hongqigong@12 | NULL    |
|  4 | 风清扬    | Shuaige@12    | NULL    |
+----+-----------+---------------+---------+
4 rows in set (0.06 sec)
```

- 客户决定使用数据库防火墙，
- 并配置SQL注入防护规则。

示例：数据库防火墙的策略定义和效果呈现

- 防护之后，客户发现数据库侧的SQL注入攻击已经没了。

```
mysql> select * from userinfo where name='' or '1'='1' and passwd = '' or '1'='1';
ERROR 1045 (HY000): ACCESS DENIED
mysql>
```

- 同时在管理页面发现有SQL入侵日志。

事件ID	#1	规则ID	#2
日期	2018-05-03 17:30:45	规则类型	Risk Based - IPS/IDS
动作	阻止	SQL注入	55
风险结果	该条查询具有OR token。 检测到真表达式（SQL重言式）。 该条查询含有空的密码表达。		
动作原因	风险计算		
模式	select * from userinfo where name = ? or ? = ? and passwd = ? or ? = ?		
原查询	select * from userinfo where name='' or '1'='1' and passwd = '' or '1'='1'		

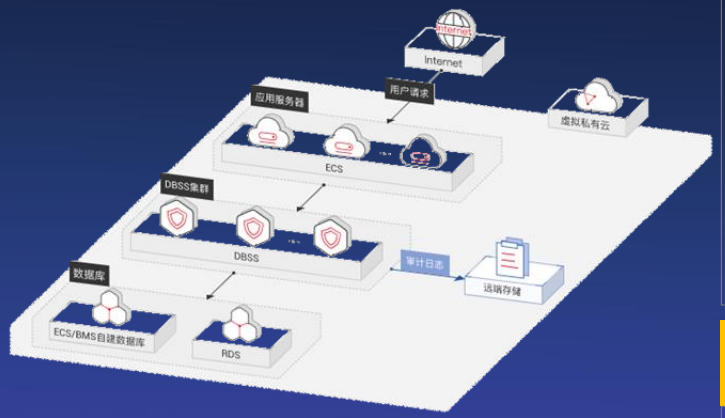
事后：用数据库审计技术来对黑客行为进行震慑

异常监控

- **行为异常监控：**
  ①提供登录行为异常监控； ②列级、表级、存储过程级别的访问异常监控 ③提供管理员权限准入异常监控等
- **数据异常监控：** 提供原始数据修改标识，包括源IP地址、用户、应用名称、受影响的行、修改时间等信息
- **性能异常监控：** 提供CPU、内存、网络流量等资源监控能力

日志记录

- **记录流量日志**
- **记录入侵日志**
- **记录异常监控日志**
- **记录数据脱敏日志**
- **远程日志能力**



报告审计

- **PII事前事后的审计**
- **内置入侵检测报告**，包括入侵IP、入侵用户、阻止的应用程序、阻止的查询和错误登录源等信息
- **针对普通用户的审计**，包括用户设置、用户访问权限、非活跃用户、密码永不过期用户等
- **针对管理员的审计**，包括管理员的活动动作、登录、权限、操作等
- **用户可以自定义审计**

实时告警

- **提供实时告警：** SQL注入告警、拖库攻击告警、漏洞利用告警等
- **TOP活动提醒：** 高活跃用户、高活跃IP、高活跃用户角色和高活跃应用等

示例：数据库审计定义和效果呈现

- 客户有个关键的用户信息表，希望审计所有对该表的查询以及操作。
- 使用数据库审计功能，先创建审计的规则（已经提前配置好了远端数据库）

示例：数据库审计定义和效果呈现

- 所有对数据库的查询都已经记录

FusionGuard HexaTier：报告

报告标题: 操作日志

报告日期: 2018-05-03 17:39:37

编号	ID	审计日期	查询概要	数据库	用户名	客户端IP
1	4	2018-05-03 17:38:32	UPDATE TABLE `confidential`.`userinfo`	confidential	root	客户端操作的IP
2	3	2018-05-03 17:38:05	SELECT FROM TABLE `confidential`.``.`userinfo`	confidential	root	客户端操作的IP
3	2	2018-05-03 17:38:01	SELECT FROM TABLE `confidential`.``.`userinfo`	confidential	root	客户端操作的IP
4	1	2018-05-03 17:37:48	SELECT FROM TABLE `confidential`.``.`userinfo`	confidential	root	客户端操作的IP

总结：三步打造云上数据库安全

Before 事前

Detection 事中

After 事后

数据泄露保护 DLP

- 敏感数据发现
- 动态数据脱敏

数据库防火墙 DBF

- SQL注入防御
- 责权分离
- 漏洞检测防御
- 合规检查
- 拖库检测

数据库审计防护 DAP

- 数据库活动监控
- 合规报表
- 日志分析

总结：关于数据库安全部署时的几点建议

- 如果数据库正在“裸奔”，先到漏洞库公告网站（如CNNVD，CNCERT或数据库官网等）查询并打上补丁，并立即制定安全防护方案
- 对您的数据库中类型、数据保密等级进行分析，高价值资产优先保护
- 考虑数据库安全部署方式的时候，统筹考虑审计、脱敏、防火墙等功能
- 法律法规的要求需要立即遵从，不要等罚款时再整改
- 培养DBA和数据库运维人员的信息安全和风险管理意识，安全永远不但是技术问题，还是管理问题

THANK YOU