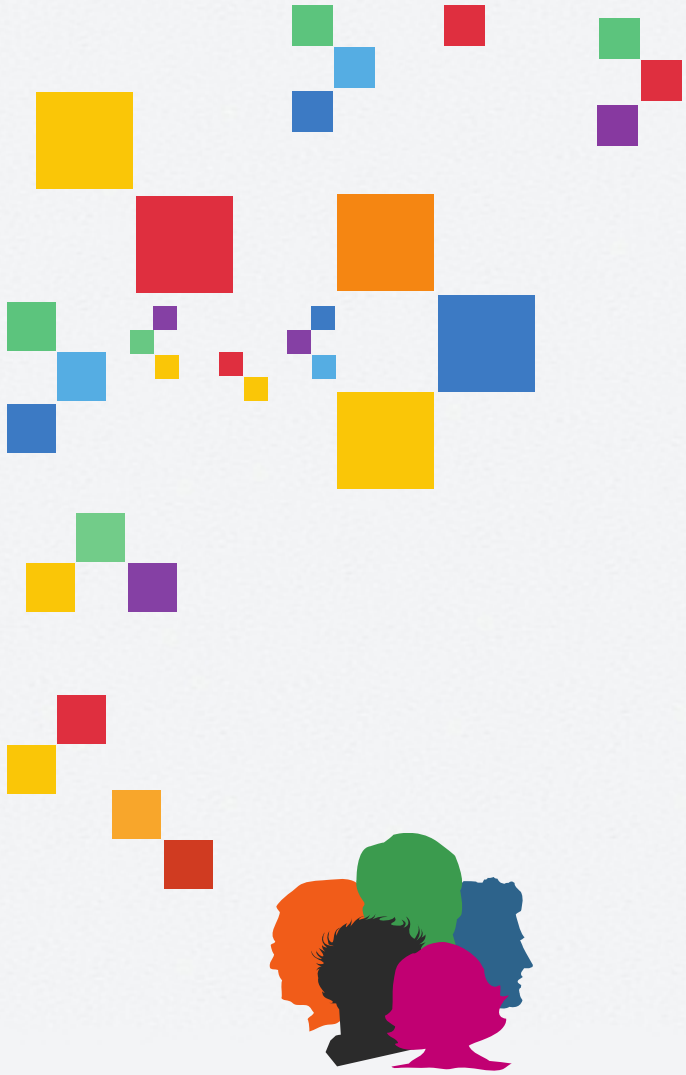
互联网安全架构

林鹏



- Lion_00
- CCIE security
- CISSP
- 安全爱好者

- 互联网安全特色
- 常见威胁与攻击
- 安全架构设计

互联网安全特色

- Web为主
- 攻防技术相对先进
- 三快二多:响应快;应急快;速度快;黑客多☺;影响范围多（动辄几十万至几千万）

互联网安全特色

- 几个经典案例

缺陷编号： **WooYun-2014-66599**
漏洞标题： 凤凰网SQL注入之3（19859用户可脱）
相关厂商： **凤凰网**
漏洞作者： **sql**
提交时间： 2014-06-29 13:
漏洞类型： SQL注射漏洞
危害等级： 高
漏洞状态： 等待厂商处理

缺陷编号： **WooYun-2014-60658**
漏洞标题： 小米科技某安全漏洞影响88W+360W数据（另一漏洞）
相关厂商： **小米科技**
漏洞作者： **爱上平顶山**
提交时间： 2014-05-14 10:23
公开时间： 2014-06-28 10:24
漏洞类型： 用户资料大量泄漏

缺陷编号： **WooYun-2014-66578**
漏洞标题： 安全诟病之一无秘网络边界可被绕过 成功进入内网
相关厂商： **秘密**
漏洞作者： **猪猪侠**
提交时间： 2014-06-28 21:11
漏洞类型： 网络敏感信息泄漏
危害等级： 高
漏洞状态： 等待厂商处理

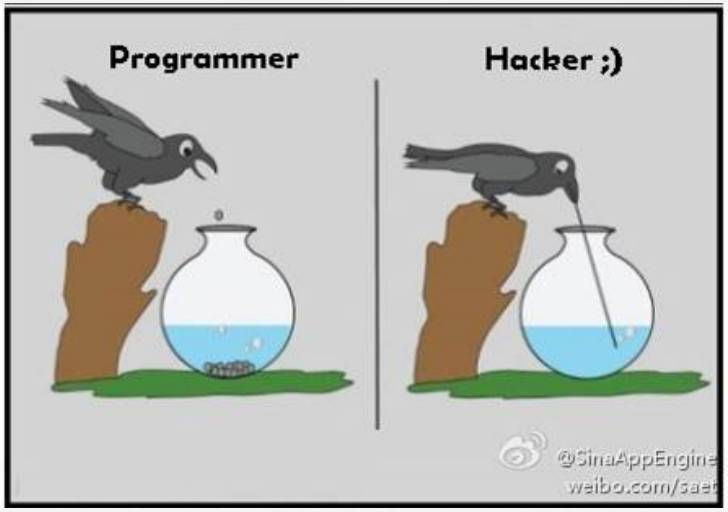
缺陷编号： **WooYun-2014-54302**
漏洞标题： 携程安全支付日志可遍历下载 导致大量用户银行卡信息泄露(
相关厂商： **携程旅行网**
漏洞作者： **猪猪侠**
提交时间： 2014-03-22 18:18
漏洞类型： 敏感信息泄露
危害等级： 高
漏洞状态： 厂商已经确认

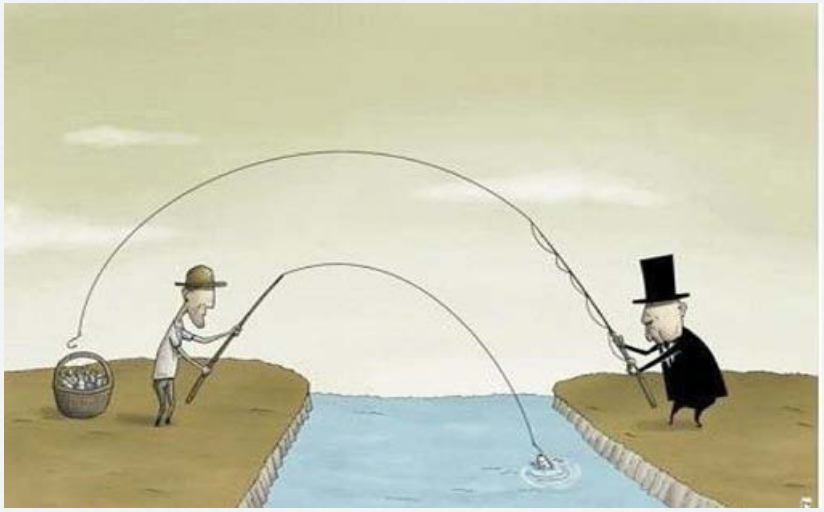
互联网安全特色

- 2017年主要安全事件
  - 信息泄露
  - **WannaCry&永恒之蓝**
  - **勒索&比特币**
  - **STRUTS2漏洞**
  - 网络安全法
  - 人脸识别
  - **CVE-2017-11882**
  - 黑产

互联网安全特色

- 黑客

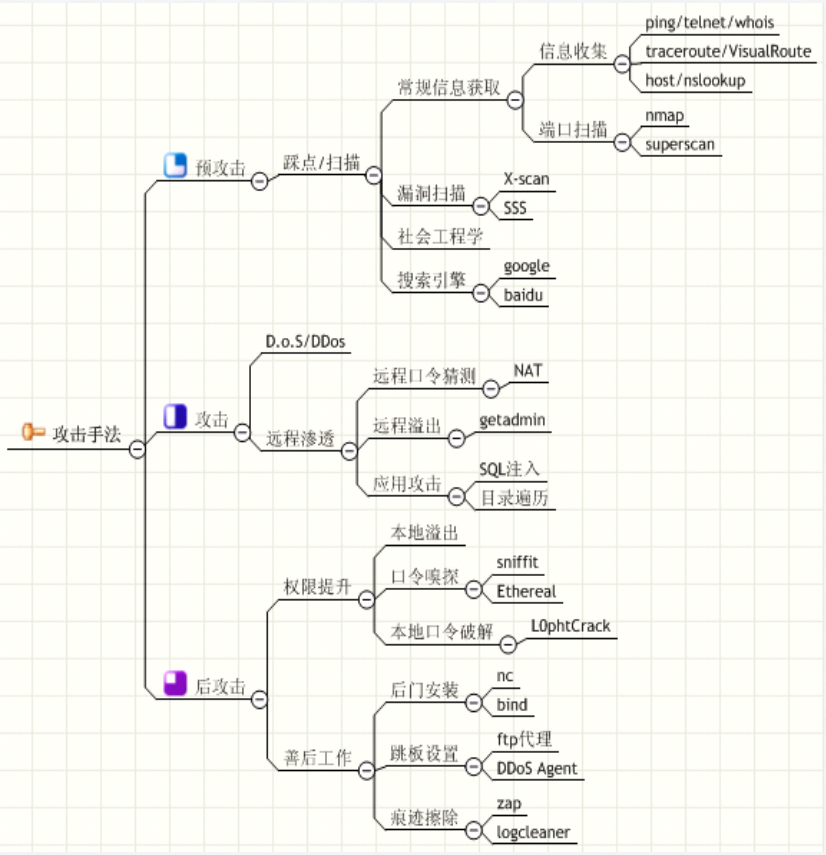


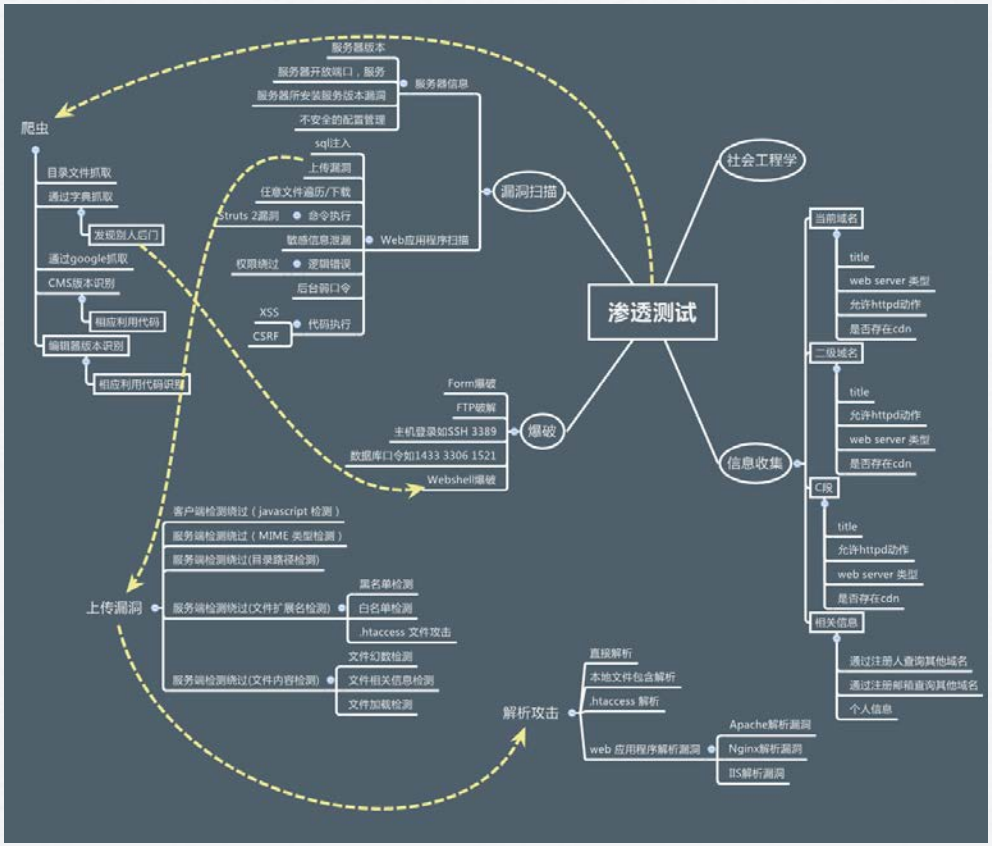


互联网安全特色

常见威胁与攻击

- 黑客攻击的“套路”





常见威胁与攻击

WEB层面,参照OWASP TOP 10

下面是常见的WEB威胁

攻击类型	工具普及度	上手程度	危害程度
SQL 注入	★★★★★	★★★★★	★★★★★
扫描器	★★★★★	★★★★★	★★
跨站攻击	★	★	★★★
上传漏洞	☆	★★★★	★★★★
WEB0DAY		★	★★★★★

常见威胁与攻击

系统运维层面

攻击类型	危害程度	上手程度
弱口令扫描	★☆	★★
运维配置不当	★★★★	★★★
DDOS	★★★★	☆

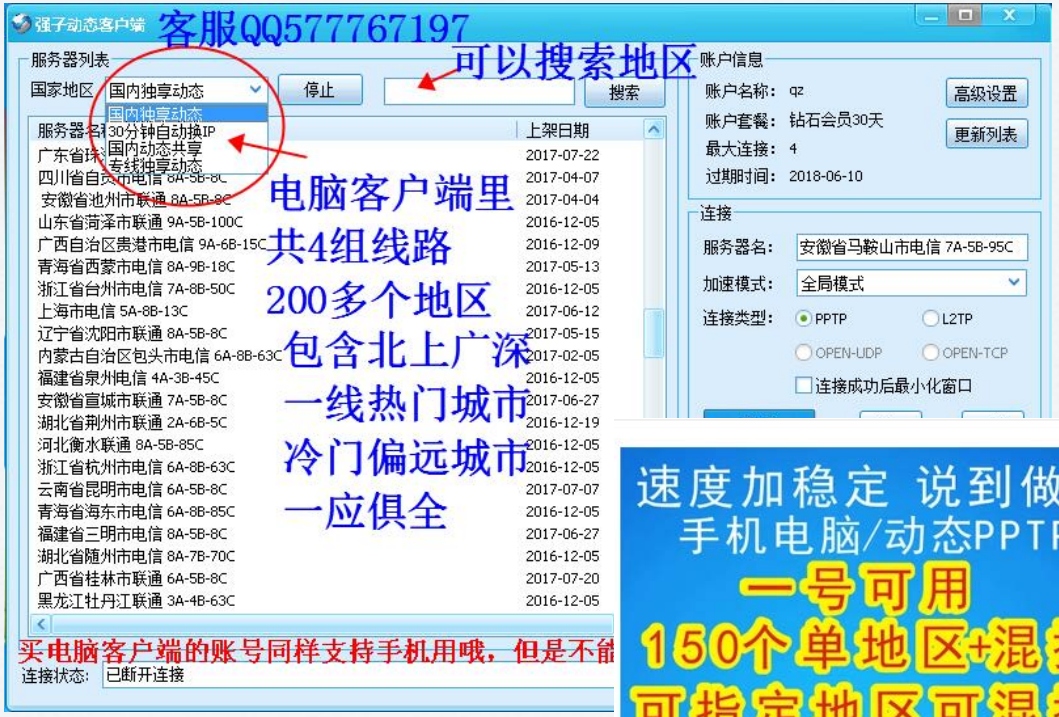
常见威胁与攻击

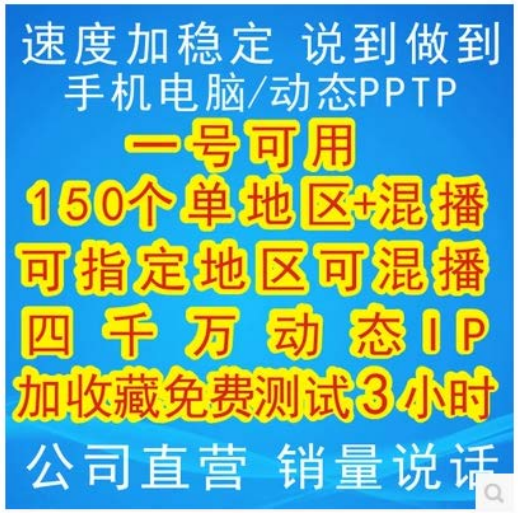
逻辑问题及其他

- 密码找回问题
- 支付问题
- 框架问题

常见威胁与攻击

- 隐藏在黑暗中的对手------黑产
- 隐藏于市井中的对手------黄牛


强子动态客户端
客服QQ577767197
可以搜索地区
服务器列表
国家地区
国内独享动态
停止
搜索
国内独享动态
30分钟自动换IP
国内动态共享
专线独享动态
服务器名称
上架日期
广东省珠海市电信 2017-07-22
四川省自贡市电信 8A-5B-8C 2017-04-07
安徽省池州市联通 8A-5B-8C 2017-04-04
山东省菏泽市联通 9A-5B-100C 2016-12-05
广西自治区贵港市电信 9A-6B-15C 2016-12-09
青海省西蒙市电信 8A-9B-18C 2017-05-13
浙江省台州市电信 7A-8B-50C 2016-12-05
上海市电信 5A-8B-13C 2017-06-12
辽宁省沈阳市联通 8A-5B-8C 2017-05-15
内蒙古自治区包头市电信 6A-8B-63C 2017-02-05
福建省泉州电信 4A-3B-45C 2016-12-05
安徽省宣城市联通 7A-5B-8C 2017-06-27
湖北省荆州市联通 2A-6B-5C 2016-12-19
河北衡水联通 8A-5B-85C 2016-12-05
浙江省杭州市电信 6A-8B-63C 2016-12-05
云南省昆明市电信 6A-5B-8C 2017-07-07
青海省海东市电信 6A-8B-85C 2016-12-05
福建省三明市电信 8A-5B-8C 2017-06-27
湖北省随州市电信 8A-7B-70C 2016-12-05
广西省桂林市联通 6A-5B-8C 2017-07-20
黑龙江牡丹江联通 3A-4B-63C 2016-12-05
电脑客户端里
共4组线路
200多个地区
包含北上广深
一线热门城市
冷门偏远城市
一应俱全
买电脑客户端的账号同样支持手机用哦，但是不能
连接状态:
已断开连接
账户信息
账户名称: qz
账户套餐: 钻石会员30天
最大连接: 4
过期时间: 2018-06-10
高级设置
更新列表
连接
服务器名: 安徽省马鞍山市电信 7A-5B-95C
加速模式: 全局模式
连接类型: PPTP L2TP
OPEN-UDP OPEN-TCP
连接成功后最小化窗口

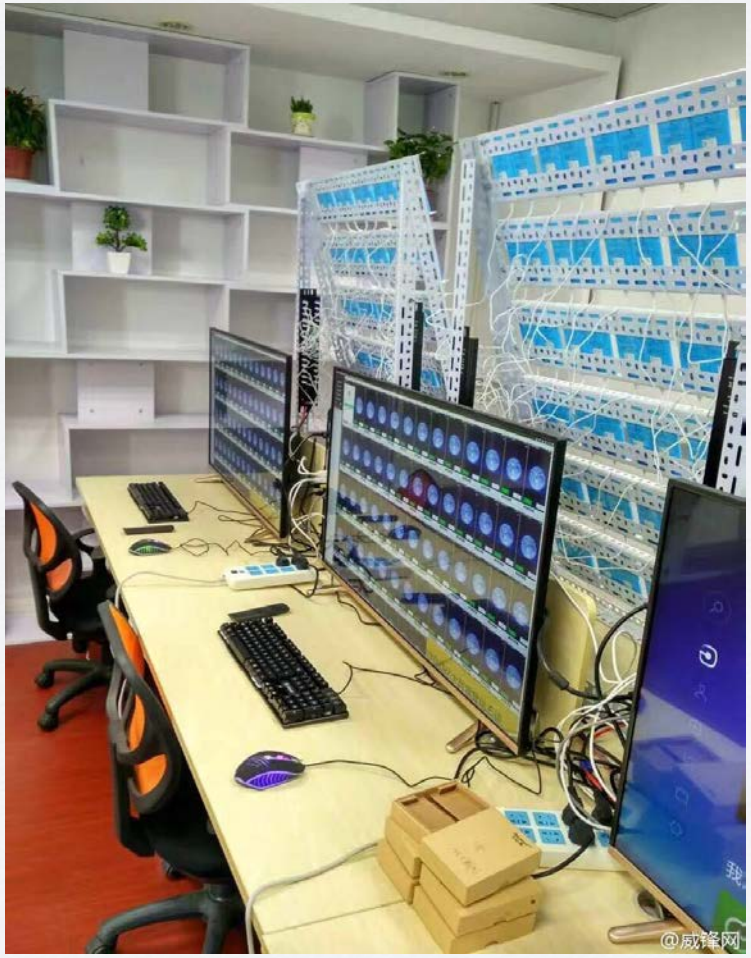

速度加稳定 说到做到
手机电脑/动态PPTP
一号可用
150个单地区+混播
可指定地区可混播
四千万动态IP
加收藏免费测试3小时
公司直营 销量说话


国内PPTP动态IP拨号adsl手机电脑秒换ip全国混拨pptp手动自动vps
价格
￥125.00
10027
累计评论
3821
交易成功
配送
浙江杭州至 北京昌平区
快递 免运费
使用时长
日付（24小时）
周付
月付
付费方式
月付
服务器套餐
套餐1
套餐2
数量
1
件(库存92439293件)
立即购买
承诺
不支持7天无理由
虚拟物品
支付
集分宝
收藏宝贝 (4274人气)
分享

关键字:（姓名/证件号） 张斌 点击查询

姓名	性别	年龄	生日	身份证号码	手机号码	E-MAIL	家庭地址	入住登记时间	操作
张斌	男	48	19670325	310102[illegible]252414	138173[illegible]	year99@sh163.n[illegible]	-	2012-[illegible] 16[illegible]	
张斌	男	49	19661123	612321[illegible]123553x	138111[illegible]		陕西	2012[illegible]3:52:38	
张斌	男	31	19841201	120104[illegible]2010833	1382119[illegible]		天津市	2012[illegible]3:55:17	
张斌	男	39	19761109	342601[illegible]09061	18949842[illegible]	xzb@163.[illegible]	-	2[illegible]3-11 [illegible]58	
张斌	男	35	19800430	120104[illegible]430041X	158221228[illegible]	anagatae[illegible]@yahoo.com.cn	-		
张斌	男	34	19810511	310115[illegible]5111719	139175276[illegible]	nce_zm@y[illegible]com.cn	-		
张斌辉	男	42	19730705	310101[illegible]7051619	13916866[illegible]	hangbinhui20[illegible]63.com	上海柳埠路135弄32号103	201[illegible]13 [illegible]4	
张斌	男	46	19691121	320122[illegible]121003X	1391396[illegible]				
张斌	男	41	19740505	340803[illegible]5052451	1385566[illegible]				
张斌	男	35	19801230	3101048[illegible]0361	13818511[illegible]				
张斌	男	39	19761021	3101011[illegible]0211611	18652787[illegible]				
张斌	男	32	19830621	12010[illegible]06215812	138207927[illegible]				
张斌	男	50	19650730	31011[illegible]07301617	1590051[illegible]				
张斌	男	38	19770607	320583[illegible]6070233	138062[illegible]				


@威锋网


@威锋网

August 9th 2017, 15:38:29.560	/ffan/v5/member/login	1529 7114	-	118.26.137.124	android	Android18
August 9th 2017, 16:39:54.268	/ffan/v5/member/login	1383 83895	fc7296a3b39f41c0826d6877115ed168	118.26.137.124	android	Android22
August 9th 2017, 17:59:37.876	/ffan/v5/member/login	1820 44157	-	118.26.137.124	android	Android17
August 9th 2017, 20:07:46.485	/ffan/v5/member/login	1473 02195	-	118.26.137.124	android	Android11
August 9th 2017, 10:55:43.265	/ffan/v5/member/login	1505 30126	-	118.26.137.124	android	Android16
August 9th 2017, 12:40:06.269	/ffan/v5/member/login	189 722144	-	118.26.137.124	android	Android21
August 9th 2017, 09:23:43.731	/ffan/v5/member/login	1513 15684	-	118.26.137.124	android	Android12
August 9th 2017, 12:04:14.478	/ffan/v5/member/login	1347 4990	-	118.26.137.124	android	Android6
August 9th 2017, 12:18:58.123	/ffan/v5/member/login	1828 9371	-	118.26.137.124	android	Android13
August 9th 2017, 12:46:09.405	/ffan/v5/member/login	15178 0786	-	118.26.137.124	android	Android21
August 9th 2017, 16:43:56.742	/ffan/v5/member/login	1833 051	-	118.26.137.124	android	Android10
August 9th 2017, 16:52:37.434	/ffan/v5/member/login	1587 249	-	118.26.137.124	android	Android15

- 常见威胁与攻击
  - 基础攻击/传统威胁
  - 业务缺陷

安全架构设计

- 不同阶段不同方法
- 注意ROI
  - 用6位数的密码保护2位数的存款是没有意义的
- 服务于业务
- 沟通交流

安全架构设计

- 人
- 技术
- 制度

安全架构设计

- 人
  - 惰性
  - 创造力
  - 规律性
  - 能力/态度
  - 社会工程学

- 技术
  - 安全防护
  - 漏洞管理
  - 扫描器（主动/被动）
  - 死角
  - 技术趋势
  - 概率/关键字/机器学习

- 安全防护
  - 未知攻焉知防
  - 告警准确与否
  - 异常检测
  - 工具定制化

Make Professional Discovery

MPD

基于攻击IP的统计

IP地址	次数统计
124.88.117.214	36219
103.243.255.163	23655
203.195.149.227	23626
203.195.150.120	23462
203.195.149.198	23368
36.110.144.150	6937
36.110.144.138	6767
103.37.138.14	3584
103.37.138.10	3545
114.55.251.30	2291

基于告警名称的统计

告警名称	次数统计
JAVA未知爬虫	405191
百度爬虫	2415
BBScan扫描器	399
Google爬虫	285
TOMCAT MANAGER扫描探测	204
PYTHON未知爬虫	83
系统敏感信息探测	6
SQL 注入攻击测试	2
SVN 敏感文件探测	2
GIT 敏感文件探测	1

基于域名的统计

域名	次数统计
trade-prd-tc.wandafilm.com	254363
data-prd-tc.wandafilm.com	74179
portal.ffan.com	36148

基于URL的统计

URI 地址	次数统计
/ucenter/v2/verifyCodes?imei=null_c649dcc4e754fa23&clientversion=11000&version=1	739

攻击者IP对应的告警名称(uniq)数量

IP地址	次数统计
183.131.151.220	5
115.238.232.90	3

编辑攻击规则

规则类别*	OTHER
Request.url*	/test\.lion
Request.user-agent*	test4attack
Request.content-type*	request.content-type:特征匹配(需正则)
Request.body*	request.body:特征匹配(需正则)
Response.body*	response.body:特征匹配(需正则)
Response.code*	state code:200,404...
Rule Description*	平台攻击检测测试
权重*	1
Rule 告警名称*	平台攻击检测测试

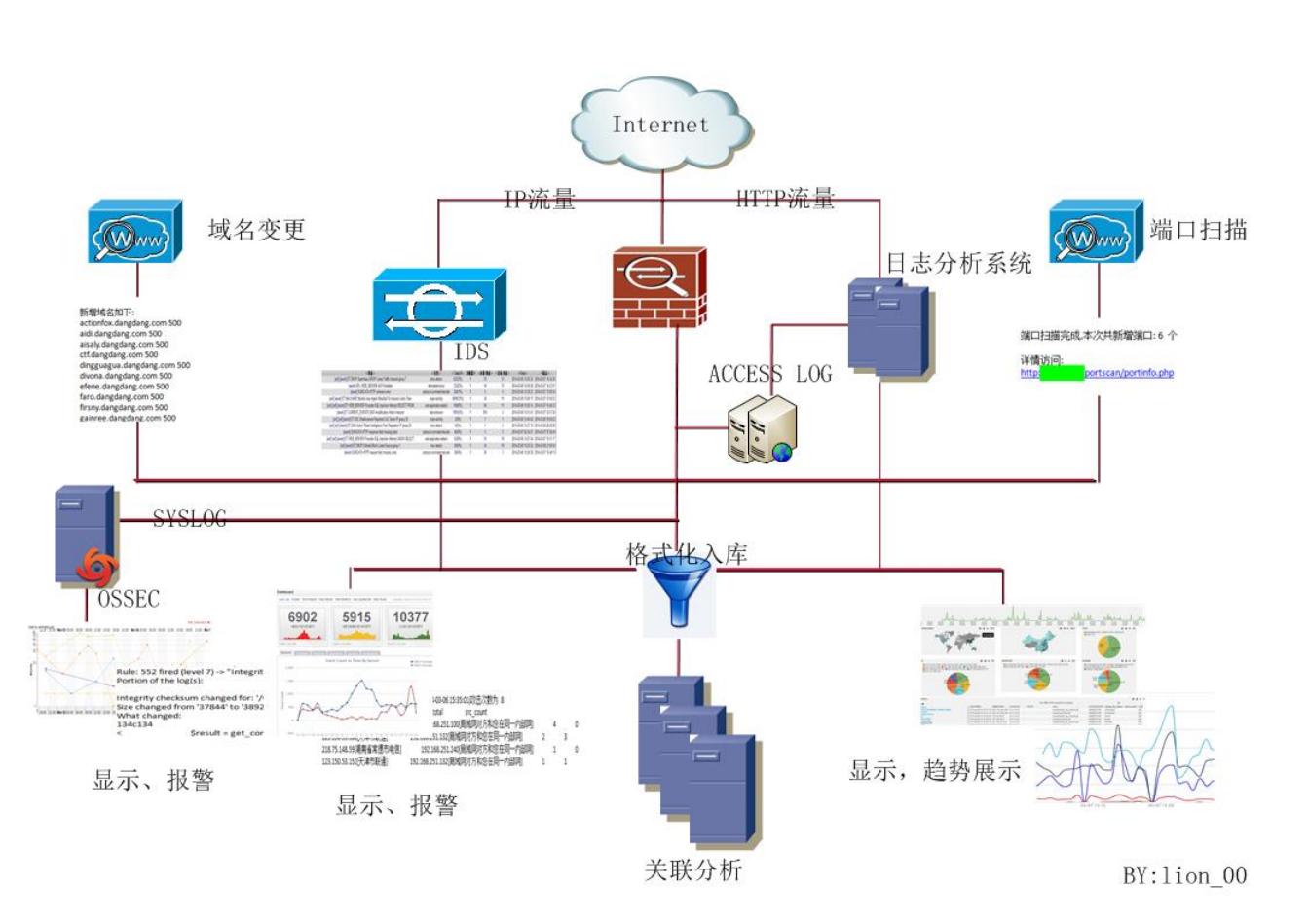
- 漏洞管理

1 漏洞级别
2 规定漏洞修复时间
3 漏洞跟进
4 漏洞复测

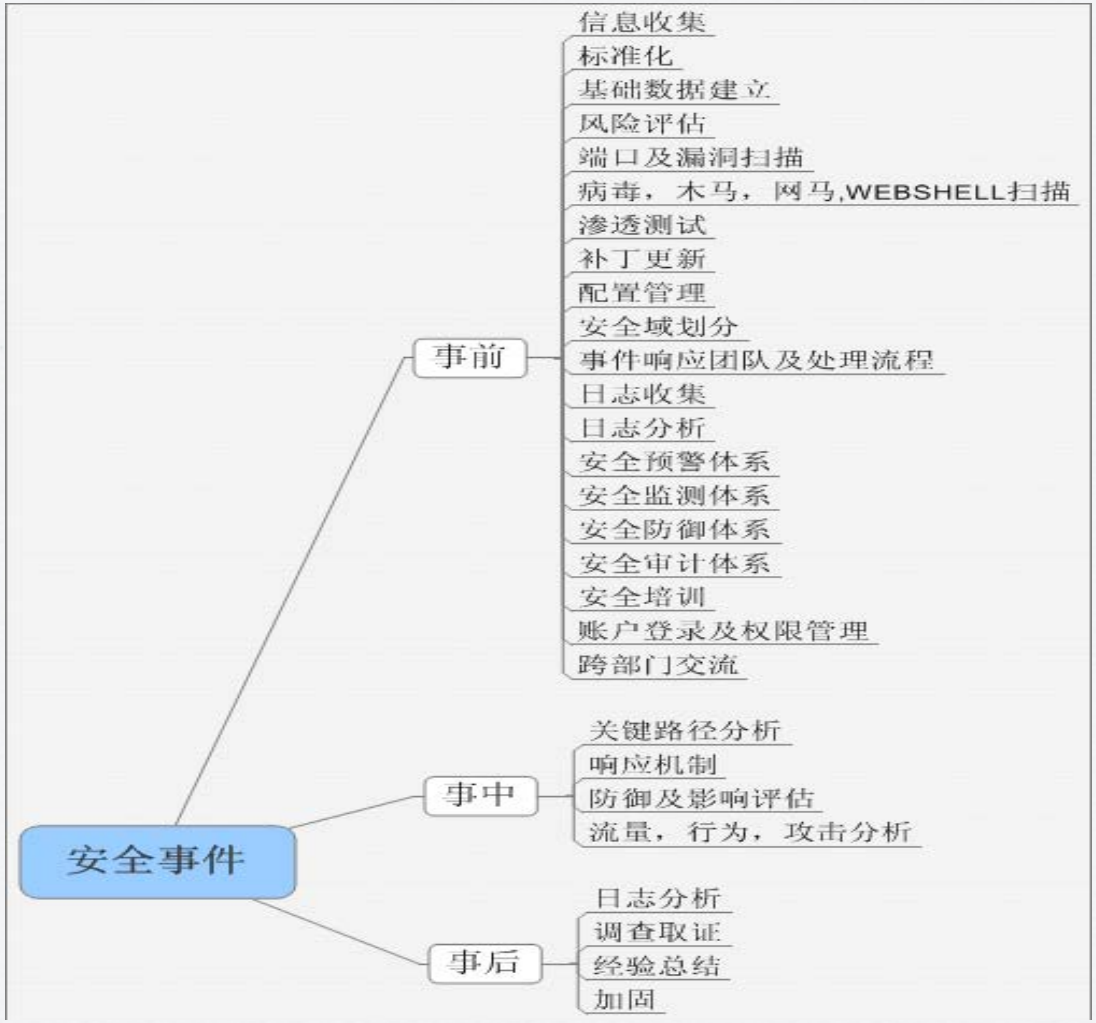
Make Professional Discovery
MPD

- 技术趋势

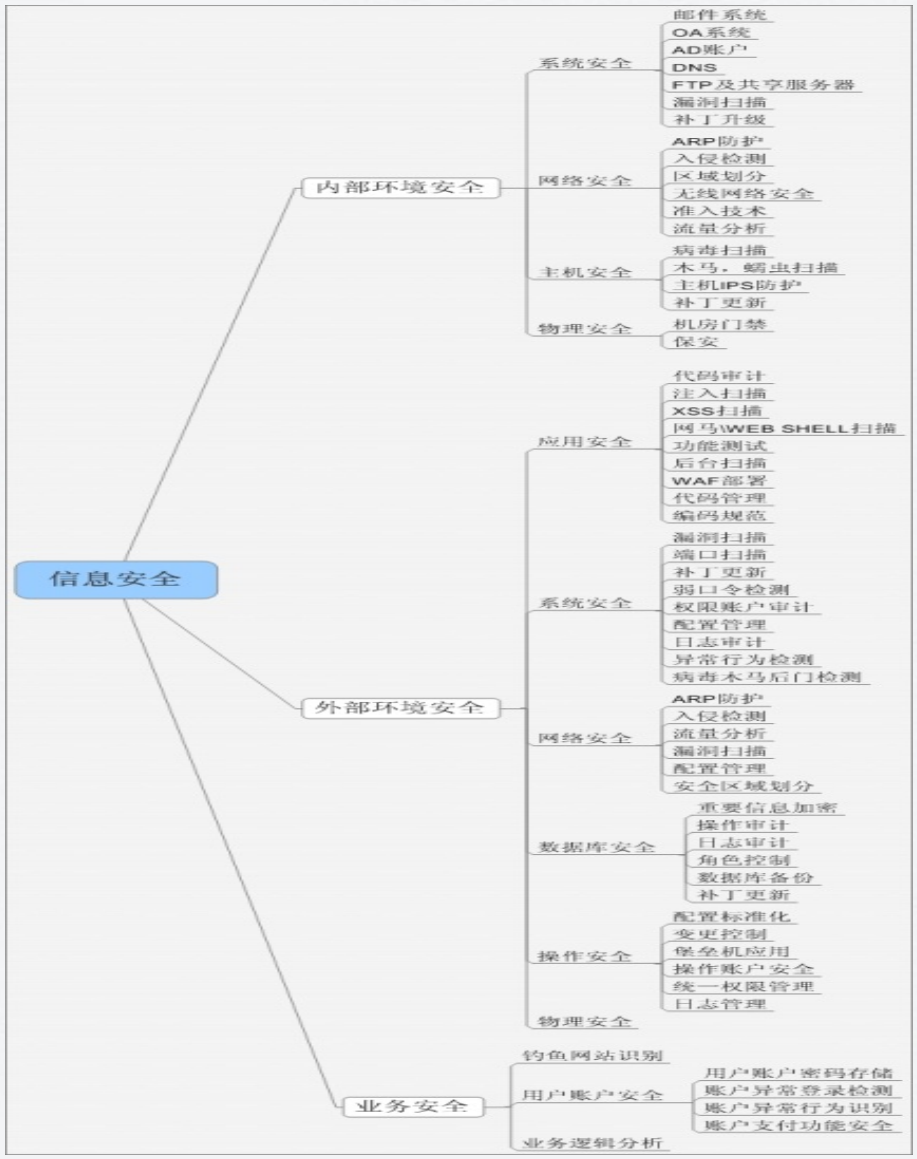
安全架构设计


Internet
IP流量
HTTP流量
域名变更
端口扫描
日志分析系统
IDS
ACCESS LOG
SYSLOG
格式化入库
OSSEC
显示、报警
显示、报警
显示，趋势展示
关联分析
BY:lion_00

安全架构设计


安全事件
事前
信息收集
标准化
基础数据建立
风险评估
端口及漏洞扫描
病毒，木马，网马,WEBSHELL扫描
渗透测试
补丁更新
配置管理
安全域划分
事件响应团队及处理流程
日志收集
日志分析
安全预警体系
安全监测体系
安全防御体系
安全审计体系
安全培训
账户登录及权限管理
跨部门交流
事中
关键路径分析
响应机制
防御及影响评估
流量，行为，攻击分析
事后
日志分析
调查取证
经验总结
加固

安全架构设计


信息安全
内部环境安全
系统安全
邮件系统
OA系统
AD账户
DNS
FTP及共享服务器
漏洞扫描
补丁升级
网络安全
ARP防护
入侵检测
区域划分
无线网络安全
准入技术
流量分析
主机安全
病毒扫描
木马、蠕虫扫描
主机IPS防护
补丁更新
物理安全
机房门禁
保安
外部环境安全
应用安全
代码审计
注入扫描
XSS扫描
网马\WEB SHELL扫描
功能测试
后台扫描
WAF部署
代码管理
编码规范
系统安全
漏洞扫描
端口扫描
补丁更新
弱口令检测
权限账户审计
配置管理
日志审计
异常行为检测
病毒木马后门检测
网络安全
ARP防护
入侵检测
流量分析
漏洞扫描
配置管理
安全区域划分
数据库安全
重要信息加密
操作审计
日志审计
角色控制
数据库备份
补丁更新
操作安全
配置标准化
变更控制
堡垒机应用
操作账户安全
统一权限管理
日志管理
物理安全
业务安全
钓鱼网站识别
用户账户安全
用户账户密码存储
账户异常登录检测
账户异常行为识别
账户支付功能安全
业务逻辑分析

- 制度
  - 没有规矩，不成

安全制度　查看更多

网科集团安全应急响应中心漏洞管理规范

网科集团业务信息安全要求

网科集团信息系统开发安全管理办法

网科集团数据安全管理规范

网科集团安全开发编码规范

网科集团应用安全基线

危险等级	内容描述	描述	通报时限	修补时限
严重	风险等级最高，可启动应急响应流程或应急预案。 内容包括且不限于： 1）可以篡改或者查看极为敏感的数据（如在线业务的涉及客户资料，用户账户密码，包含核心业务敏感配置文件的源码，数据库账户密码等） 2）可以取得服务器或者应用程序高级权限并利用漏洞入侵成功的安全问题（如直接操作服务器或者控制应用程序） 3）可以直接影响应用程序服务的安全问题（如使应用程序停止服务，严重影响用户体验） 4）可以直接对网科集团造成重大经济损失（大于 5000 元）的安全问题（如支付漏洞） 5）其他信息安全部门评估认定为严重的安全问题	1）含有敏感信息的SQL注入（可读取用户账号密码、业务核心配置、用户个人信息或者订单信息等敏感资料） 2）命令执行（可直接操作业务系统或者服务器） 3）webshell（已上传后门且可解析运行的上传漏洞，通过其他途径获得webshell的漏洞） 4）越权访问（可越权遍历订单信息或查看极为敏感信息等问题） 5）核心业务弱口令（通过弱口令拿到业务系统响应权限并进行其他操作的问题） 6）满足严重内容描述的其他漏洞	立刻通报	收到相关安全问题通报（如邮件等） 1天内完成修复
高危	风险等级为高，且影响到部分用户的安全问题。 内容包括且不限于： 1）可以篡改或者查看、遍历数据的安全问题（数据非极为敏感数据，如用户评论数据等） 2）可以取得系统或者服务器的非最高权限的安全问题 3）使用成本较低且影响较大的安全问题 4）可以直接对网科集团造成经济损失（1000 元以上 5000 元以下）的安全问题 5）其他信息安全部门评估认	1）不含敏感信息的SQL注入（可遍历非核心内容或非敏感内容的注入） 2）文件包含（包含远程可执行文件，或本地系统配置的漏洞） 3）越权访问（包括但不仅限于绕过认证直接访问管理后台，弱密码或删除他人订单等） 4）高风险的逻辑设计缺陷（包括但不仅限于查看用户信息、修改相关状态等） 5）高风险的信息泄露 6）存储型 XSS（可大面积影响且持久影响用户或后	半天内通报	收到相关安全问题通报（如邮件等） 3天内完成修复

目录

信息安全国际最佳实践

标准	制定组织	制定目的/应用范围
COBIT	ISACA	❑ 针对IT过程管理制定的一套基于最佳实践的控制目标
Internal Control-Integrated Framework	COSO	❑ 内控整体框架，为企业运作的有效性、财务报告的可靠性及与相关法律法规的合规性提供必要保障
ISO/IEC 17799	ISO	❑ 信息安全管理框架标准，为重要的企业信息提供保密性、完整性的保障
ISO/IEC 13335	ISO	❑ 信息安全管理方面的指导性标准 ❑ 目的是为有效实施信息安全管理提供建议
ITIL	OGC	❑ 关于IT服务管理最佳实践的建议和指导方针 ❑ 侧重于具体的实施流程
CISSP	$(ISC)^2$	❑ 信息安全专家的培训及认证标准
NIST SP 800系列	NIST	❑ 针对信息安全技术的实践参考指南


需求
设计
实施
测试
发布和响应
安全需求分析
关键目标识别
受攻击面分析
威胁建模
安全设计方案
开发安全规范
静态分析
Fuzzing 测试
渗透测试
代码审计
集成测试
最终安全评审
安全响应和预警

信息安全体系实施的关键成功因素

关键成功因素

1 业务驱动

信息安全任务的实施一定要从业务的角度出发，在实施时必须时刻考虑到业务的需求，在信息安全建设过程中获得业务部门的支持与配合，共同推动信息安全建设的开展。

2 高层的支持

信息安全任务通常情况下会涉及到各个部门的参与、配合乃至利益关系，因此在实施过中需要国信高层的支持甚至是参与协调各部门的关系，建立跨部门的协作机制，以保证项目的顺利实施。

3 有效的实施管理和监控

为了获取建设的最大收益，并最大程度降低风险，需要落实强有力的实施管理和监控措施，在跟踪总体计划的同时，合理安排各任务的进度和资源，强化对各任务/子任务的管理和监控。

4 长期可靠的合作伙伴

选择良好的合作伙伴对于保证信息安全建设能够成功实施是十分重要的。通过长期可靠的合作关系，快速引进外部专业资源和先进技术，帮助推动信息安全建设工作。

安全工作规划建议

项目规划综合分析

通过下面公式计算的值描述项目施的优先级。
项目实施优先级计算公式：

$$优先级 = 紧迫性 \times 可实施性 + \frac{难易程度 + 预期效果}{2}$$

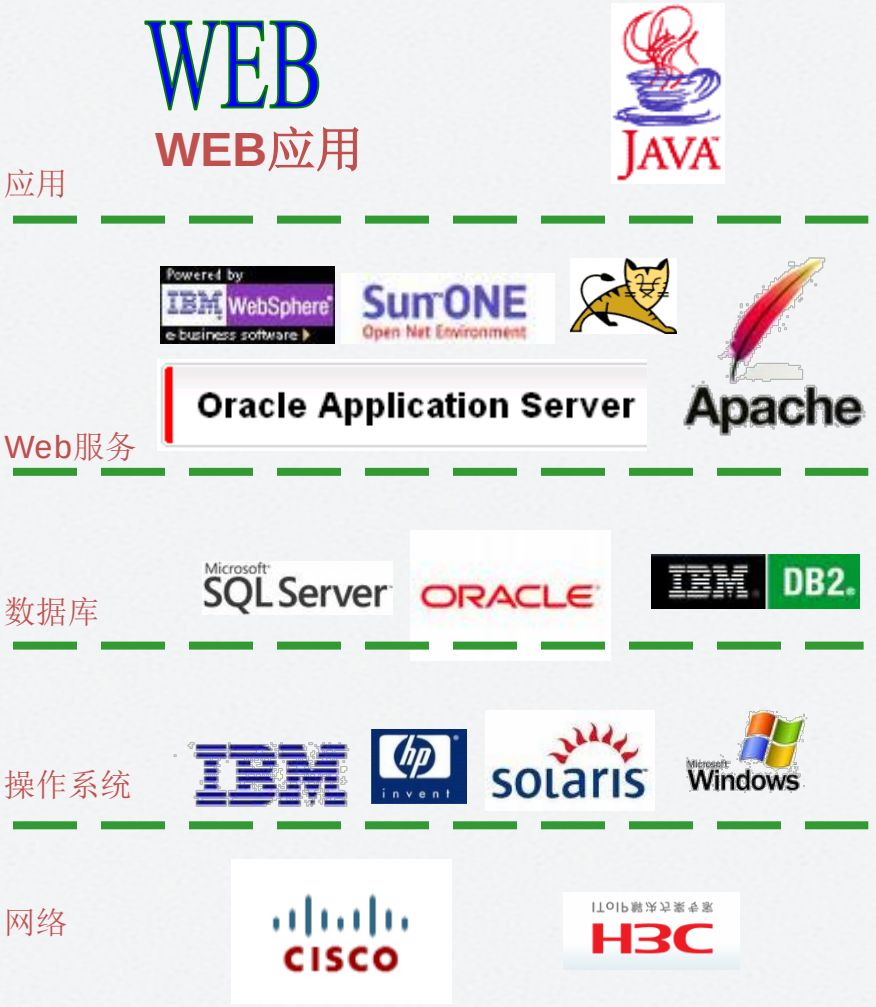
序号	安全规划因素	赋值说明		
		高（3分）	中（2分）	低（1分）
1	紧迫性	必须尽快实施（一般为一年内）	需要尽快实施（一般为二年内）	不要求短期内完成（一般为三年内）
2	可实施性	现有条件下或申购的资源到位后可实施	需要再申请一定资源后才可以实施或实施的前提条件不太成熟	很难申请到必要的资源或目前不具备实施的前提条件
3	难易程度	实施难度较大	有一定实施难度	不存在实施难度
4	预期效果	预期效果会非常好	预期效果较好	预期效果一般

安全工作规划建议

序号	项目	优先级	紧迫性	可实施性	实施难易度	预期效果
1	信息安全风险评估任务	12	3	3	3	3
2	安全域建设任务	12	3	3	3	3
3	开发安全管理体系建设任务	12	3	3	3	3
4	网上交易认证改进任务	12	3	3	3	3
5	信息资产安全管理任务	12	3	3	3	3
6	安全运营中心（SOC）建设任务	11.5	3	3	2	3
7	终端安全任务	11.5	3	3	2	3
8	信息安全治理任务	9	3	2	3	3
9	信息安全组织任务	9	3	2	3	3
10	信息安全管理体系任务	9	3	2	3	3
11	应用安全任务	8.5	2	3	2	3
12	服务器安全任务	8.5	2	3	2	3
13	网络安全任务	8.5	2	3	2	3
14	物理设施安全任务	6.5	2	2	2	3
15	监控审计任务	6.5	2	2	2	3
16	应急响应任务	6.5	2	2	2	3

安全基线检查涉及的系统范围

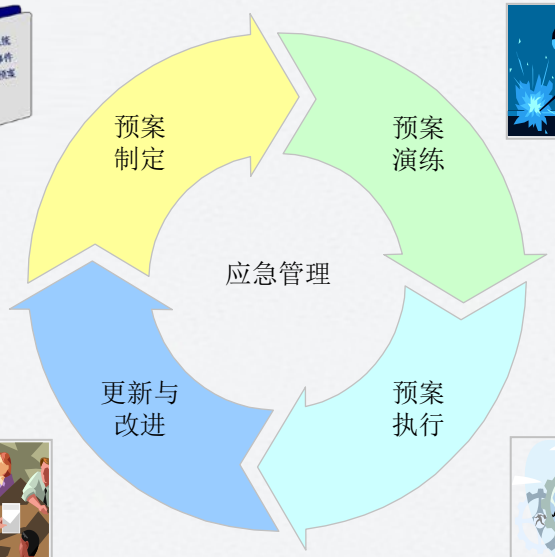
1、应用系统： ▪Web应用安全基线，针对Web应用的威胁，创建较为通用的Web应用基线。 ▪源代码安全基线，针对应用开发语言Java建立代码安全基线。	2、中间件： ▪SUNONE ▪Apache ▪WebSphere ▪Tomcat ▪Oracle Application Server
3、数据库： ▪Oracle ▪DB2 ▪SQL Server	4、主机： ▪Windows ▪AIX ▪HP-UX ▪Solaris
5、设备： ▪Cisco ▪H3C	



应急响应任务

应急管理

- 成立应急小组编制应急预案
- 确定应急相应的组织、事件种类、启动条件、响应方式、响应流程
- 应针对不同的保护对象分别制定应急预案，如EMAIL、DNS、网络、各应用系统等



- 设计应急预案的演练场景，制定演练计划，执行演练并进行总结
- 演练应该定期进行，针对不同场景演练、积累经验

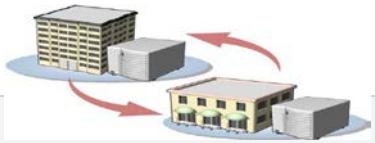
- 演练和执行应急预案结束后，要查清事件发生的原因和对处置过程进行评价，总结经验教训，确定改进措施
- 要由专人对演练中的问题进行跟踪，确保问题被解决

- 当以外事件发生，根据应急预案流程相应和处理
- 如果事态难以控制或短期无法解决，通知应急指挥部门启动更高级别应急预案或灾难恢复计划

灾备体系完善

- **内容与步骤**

  基于****应用系统建设情况，将新系统纳入灾难备份的范畴中，同时建设自己的异地灾备中心，确保在发生灾难情况下能够通过灾备切换尽快恢复信息技术服务，从而最大限度地降低对外服务中断对****业务的影响。




安全系统
安全防御系统
日志分析系统
业务监控
业务安全
风控系统
权限控制
应用权限管理
审计系统
SDL
代码安全
应用安全框架
日志分析系统
数据分级
数据库安全
数据访问控制
数据监控系统
系统扫描
系统加固
HIDS
日志分析系统
网络扫描
网络区域
访问控制
流量分析系统
综合分析系统
应急响应小组

Make Professional Discovery

MPD

感谢您参加本届MPD！

www.mpd.org.cn

400-812-8020