



企业级安全服务解决方案

让安全无法撼动
Make Security Entrenched Still

2016年9月



国内最大的互联网安全新媒体，同时也是爱好者们交流、分享技术的最佳平台



连接全球顶尖安全专家，高效透明的企业级安全服务平台



下一代安全监控与风险分析平台



- 国内首家互联网安全新媒体
- 主办国内规模最大的互联网安全创新峰会（FIT互联网安全创新大会）
- 发布国内首个金融行业安全风险报告
- 国内首家提出基于业务场景的安全测试模型
- **国家应急安全响应中心（CNCERT）省级支撑单位**
- **国家信息安全漏洞库（CNNVD）三级支撑单位**
- **国家信息安全漏洞共享平台（CNVD）漏洞报送突出贡献单位**
- **上海市信息安全行业协会（SISA）理事单位**
- **2016 红鲱鱼亚洲100强（Red Herring），亚洲地区唯一上榜中国安全企业**
- 上海市信息安全测评中心网安金服合作单位
- 上海市网络与信息安全应急实务中心合作单位
- 民航信息安全管理与测评中心战略合作单位

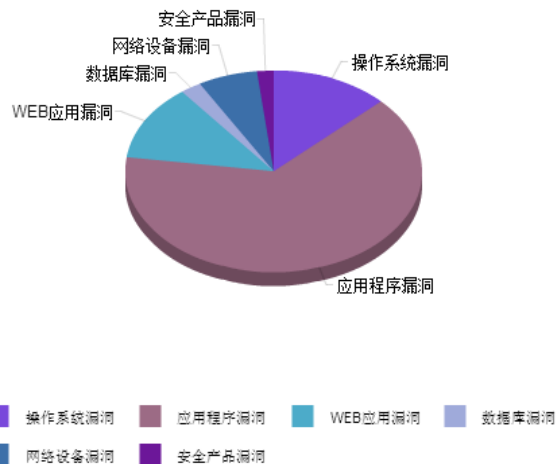
CNVD漏洞库显示应用程序漏洞比重最大，65%的漏洞发生在应用层

贡献单位排名

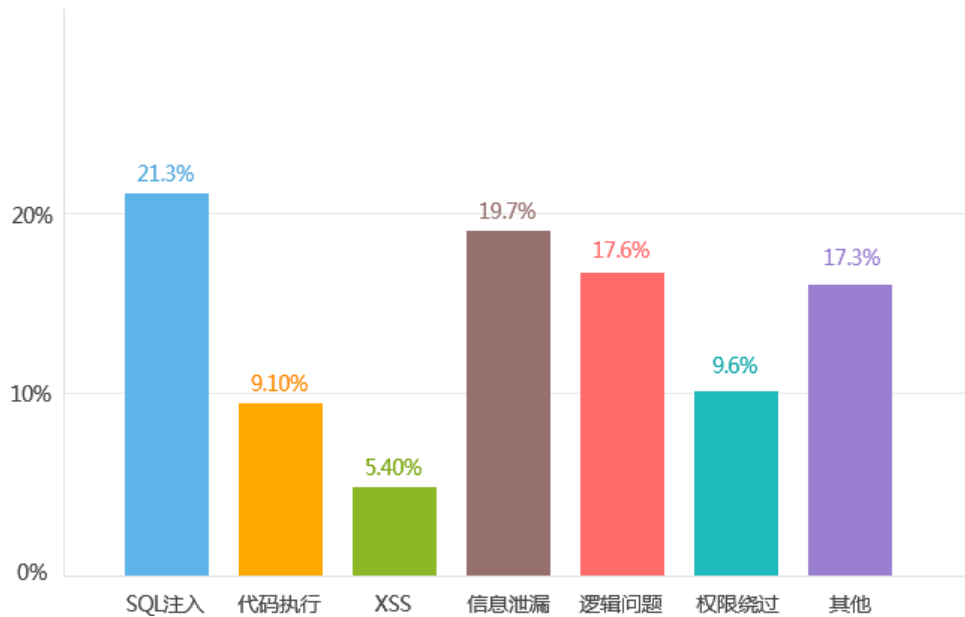


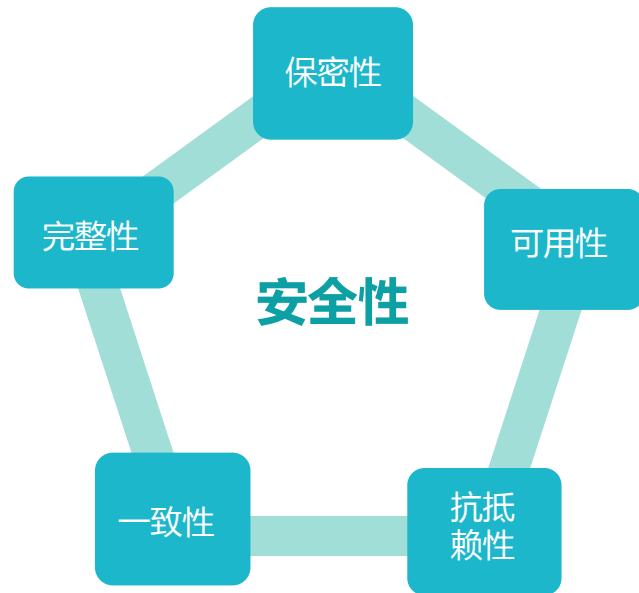
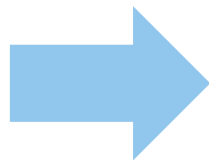
漏洞分布

漏洞影响对象类型 开始时间: 2015-01-01 结束时间: 2016-05-23 查询



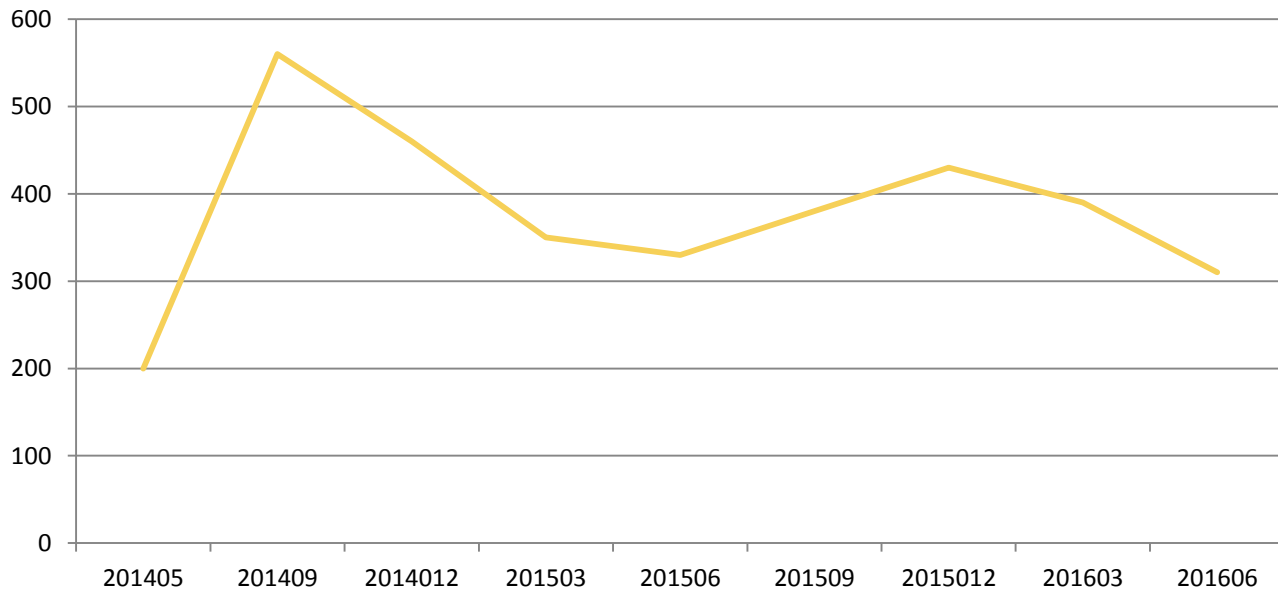
主要风险来自于SQL注入、信息泄露、业务逻辑问题。





保险业

通过白帽子给漏洞盒子所提交的漏洞数量来看每月约有200多个关于保险业漏洞提交，且一直有新的白帽子参与进来



漏洞盒子互联网安全测试：重新定义安全服务



培训与应急响应服务

网藤
风险感知平台

漏洞盒子
企业级安全测试平台

覆盖端到端
安全测试链



User



Content/Data
Deliver Network



Firewall



Web&APP Server



Code



Datastore



Physical

贯穿安全漏洞测试 全生命周期

漏洞挖掘

漏洞管理

递归收敛复测

培训、渗透演练



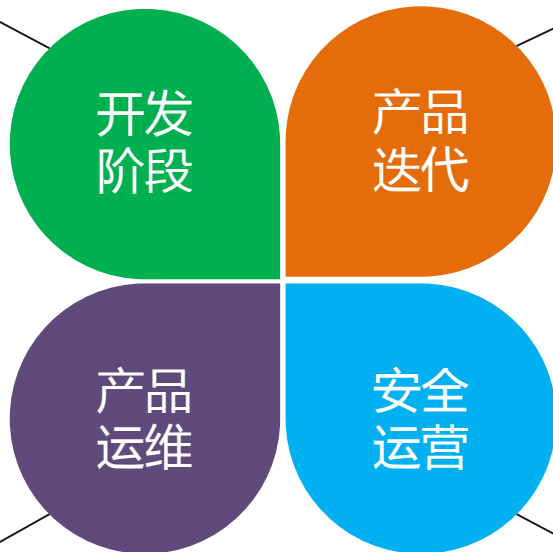
漏洞盒子 | 安全测试

- 专家级互联网安全测试
- 深度漏洞及漏洞链分析
- 架构层面安全修复



漏洞盒子 | 安全测试

- 分析业务变化及威胁分析
- 发布前安全测试
- 漏洞修复与处理



- 实时安全云端监控
- 应急响应，迅速解决线上问题
- 企业级APT渗透演练

- 安全情报获取
- 互联网漏洞预警
- 安全事件响应与公关

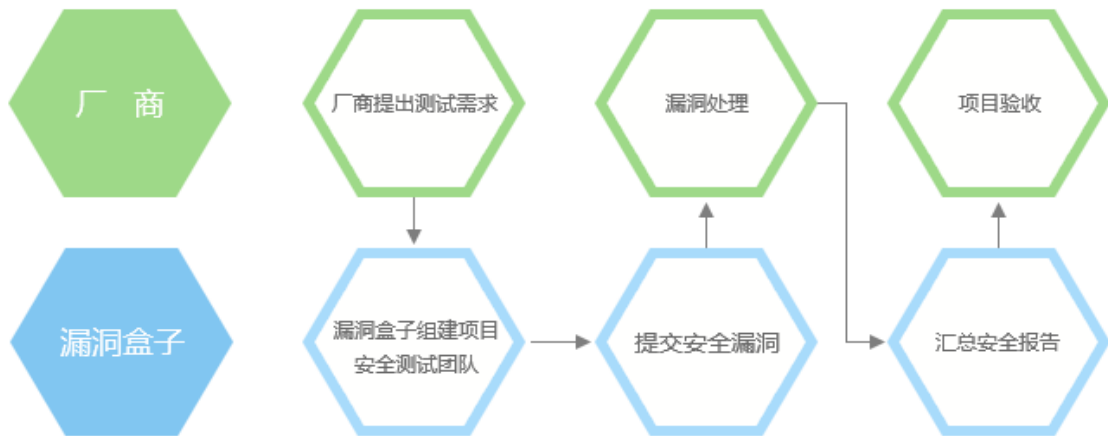


网藤漏洞感知

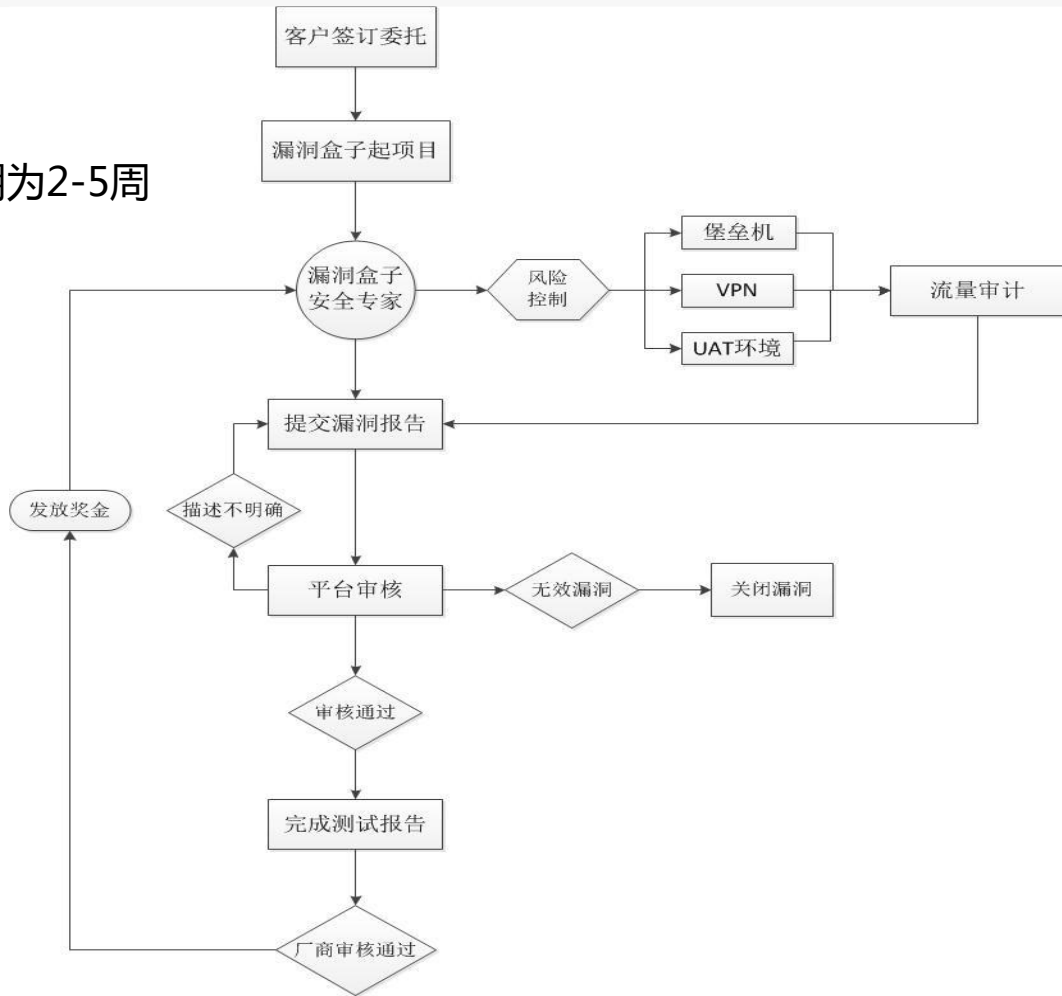


漏洞盒子 | 情报中心

■ 单次测试一般周期为2-5周



■ 单次测试一般周期为2-5周



利用全球互联网安全专家资源，模拟真实环境的黑客漏洞挖掘与演练，将产品安防壁垒做到最高

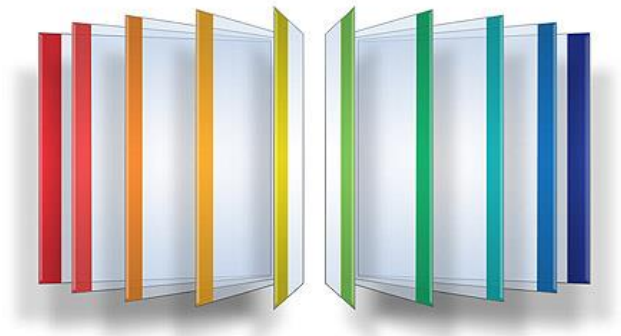
漏洞盒子安全测试将**自有安全团队、核心白帽子团队、认证白帽子专家结合**，服务全程可靠安全



- **全球专家资源**：全球2万名安全专家与技术团队资源，覆盖各领域专家
- **测试团队组建**：漏洞盒子自有安全团队与签约外部安全专家/团队结合；
- **风险控制**：测试人员资质审核、实名认证及测试过程管控；
- **漏洞生命周期管理**：测试过程全透明，企业掌握主动权；
- **安全加固**：一站式的安全建议和加固服务，贯穿整个产品开发生命周期；
- **应急响应**：7*24小时技术支持与应急响应

■ 漏洞盒子安全团队（自有安全团队）

大多是曾供职于百度、阿里巴巴、Facebook、微软的高级安全研究人员，团队负责人张天琪（CTO）多次为Google、微软、Facebook、eBay等知名企业提交高价值安全报告并获官方致谢，在全球顶尖安全峰会发表演讲，在国际上享有盛誉。








The image shows two screenshots of web pages. The top screenshot is from Google's Application Security page, specifically the 'Reward Recipients' section for Q2 2014. It lists several researchers, with a red arrow pointing to 'Tianqi Zhang' from '漏洞盒子安全团队' (VulBox Security Team). The bottom screenshot is from Microsoft's 'Security Researcher Acknowledgments for Microsoft Online Services' page for November 2014. It lists several researchers, with a red arrow pointing to 'Tianqi Zhang' from 'VulBox Security Team'.

Quarter	Researcher	Contact Info
Q2 2014	Jitendra Jaiswal	facebook
Q2 2014	dushyant	dushyantbing.com
Q2 2014	Tianqi Zhang	漏洞盒子安全团队
Q2 2014	Marc Monbaron	@WindMarc
Q2 2014	Nathaniel Wakelam	http://www.nnwakelam.com
Q2 2014	Ganpithan (Gopinath)	மதுரை (Madurai)
Q2 2014	Jann Horn	thejh.net

Researcher	Team/Company
Michael Gottburg	Individual
Omar Azouggarh	Individual
Abdul Wasay	Exismedia.com
Minhal Mehdi	Devil's Cafe
Babar Khan Akhuzada	Individual
Rafael Pablos	Individual
Tianqi Zhang	VulBox Security Team
Caner Koroglu	Symturf

- 漏洞盒子平台认证白帽子专家（经过资质审核与签约）共计22137名，核心白帽子团队（经过资质审核与签约，身份审核，技能考核）5274人。

排行	昵称	奖金	Rank	金币	准确率	勋章
1	 旺角扛把子	¥236520	3420	6	90%	
2	 匿名者	¥208880	3748	84	86%	
3	 greg.wu	¥195350	2874	32	86%	 
4	 匿名者	¥175705	2898	35	82%	
5	 匿名者	¥106350	1963	9	79%	
6	 pwnsh4d0w	¥103900	1250	0	70%	  
7	 gdygdy	¥89050	2391	0	88%	
8	 匿名者	¥62340	1094	6	78%	
9	 匿名者	¥55620	829	60	92%	
10	 匿名者	¥55610	1098	127	58%	

法律角度限制：

- 1、与白帽子有保密协议；
- 2、测试边界制定。

1、VPN - 统一流量审计；

2、堡垒机 - 测试过程行为监控；

3、平台内置工单处理机制 - 第一时间进行漏洞处理。用待处理、工单中、已修复、已忽略等状态来验证漏洞的真实性。

风险管理

项目管理角度限制：

- 1、实名登记，包括身份证、联系方式、银行卡账号等信息；
- 2、相应奖罚制度对于违规者有严厉的惩处措施；
- 3、记录参与项目白帽子信息，包括IP，名称，时间等。以及内置即时聊天工具可以很好的和白帽

人员管理角度限制：

- 1、平台白帽子严格等级划分制度；
- 2、测试团队组建：自有测试团队（30%）+ 核心白帽子团队（70%）。提供10~50名测试人员，具体数量可根据企业需求调整。



资质审核与签约

实名认证制度保证核实测试人员真实身份，确保测试人员的资质真实可靠；
远程面试确认真实存在；
签署服务合同与保密合同，确保合法备案，保障双方权益

严格把控，实现**0风险**



技能考核

通过内部搭建环境对白帽技能进行级别考察和技能分类。
保证项目参与人员最大化符合项目需求。

身份审核

与多机构合作，落实背景调查：包括工作单位、个人背景等。
保证回溯性，可第一时间定位到测试本人。

测试过程全程透明可见

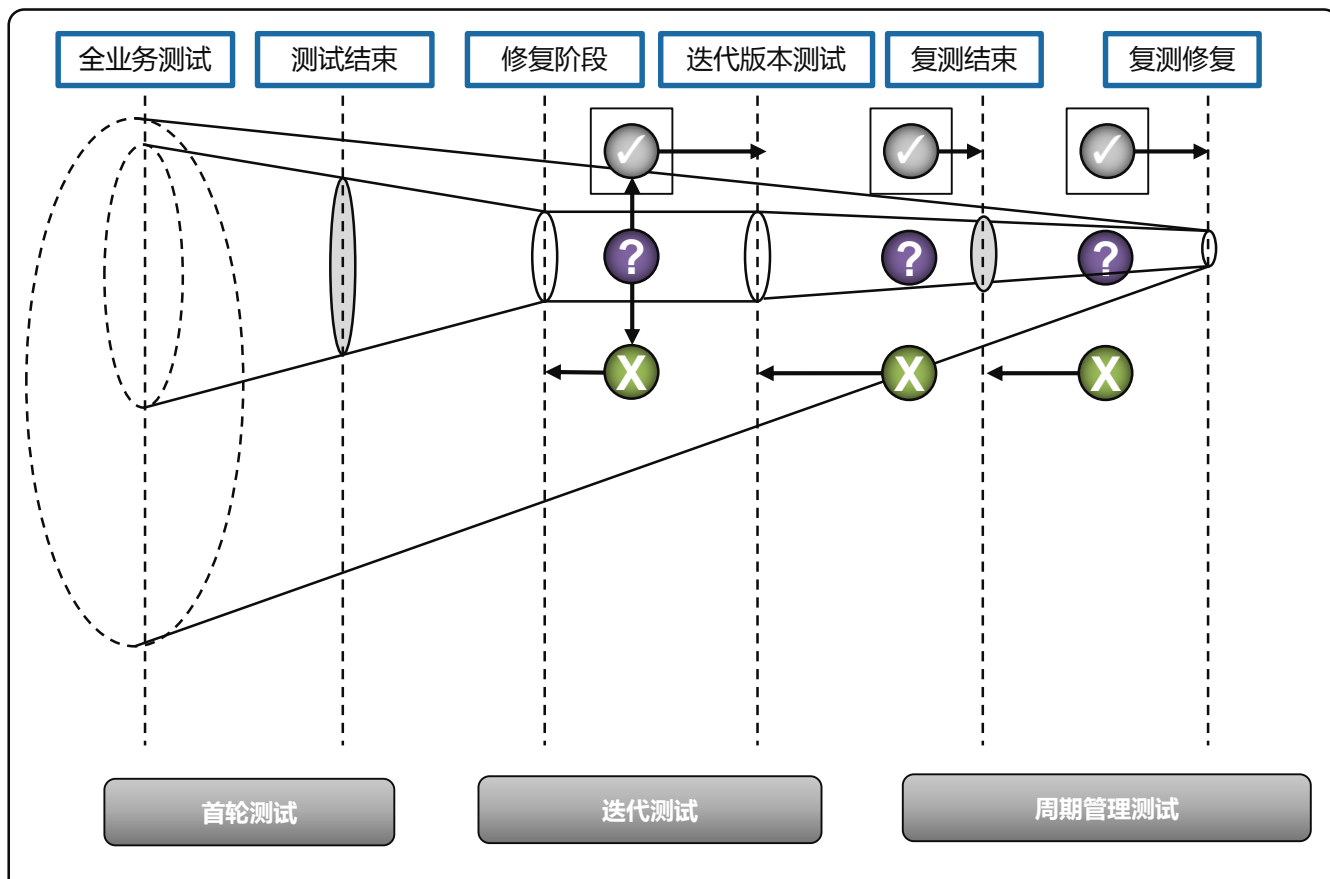


漏洞管理

全部	待审阅	待确认	待修复	已关闭	已公开
漏洞标题	风险级别	所属项目	白帽子	提交时间	当前状态
[REDACTED]	高	[REDACTED]	[REDACTED]	2015-01-27 20:29	待审阅
[REDACTED]	高	[REDACTED]	[REDACTED]	2015-01-27 20:17	待审阅
[REDACTED]	高	[REDACTED]	[REDACTED]	2015-01-27 19:53	待审阅
[REDACTED] 户密码漏洞	高	[REDACTED]	[REDACTED]	2015-01-27 19:48	待审阅
[REDACTED]	高	[REDACTED]	[REDACTED]	2015-01-27 19:31	待审阅
[REDACTED]	高	[REDACTED]	[REDACTED]	2015-01-27 19:30	待审阅
[REDACTED] 洞5	高	[REDACTED]	[REDACTED]	2015-01-27 18:00	待确认
[REDACTED] 披露	中	[REDACTED]	[REDACTED]	2015-01-27 18:00	待修复
[REDACTED]	高	[REDACTED]	[REDACTED]	2015-01-27 17:53	待确认
[REDACTED]	高	[REDACTED]	[REDACTED]	2015-01-27 17:43	待审阅

1386 1/139 1 2 3 4 5 6

平台中实时更新：当前测试进度、参与人员、漏洞报告、漏洞状态、修复状态



漏洞盒子安全测试收敛模型

■ 不仅发现问题，更注重解决问题

- ✓ 问题描述
- ✓ 漏洞分析
- ✓ 修复建议
- ✓ 样例代码
- ✓ 问题追踪
- ✓ 漏洞复测
- ✓ 输出测试报告（技术与管理版）
- ✓ 总结培训



服务贯穿于整个产品开发生命周期

■ 测试的人员多样化、手段现实、技能全面

■ 测试范围覆盖全面：

- ✓ Web网站、系统、应用
- ✓ 移动应用、APP (Android & iOS)
- ✓ 智能硬件设备、自助终端系统

■ 测试内容深入：

- ✓ 基于技术层面漏洞
 - OWASP TOP 10，CWE TOP 25：身份认证与授权，访问控制，数据输入/输出验证，安全配置，传输层安全，XSS，CSRF，SQL注入等
- ✓ 基于业务场景漏洞
 - 支付业务：交易数据泄漏、信用卡信息泄漏、数据篡改等攻击
 - 个人账户：账户盗用，越权查询敏感信息，自助缴费，转账汇款
 - 移动APP应用漏洞，导致的恶意交易，数据修改、终端数据泄漏等异常行为



安全威胁	扫描工具（程序）	传统渗透测试	漏洞盒子-互联网安全众测
漏洞入侵	<ul style="list-style-type: none">1、通过规则判断，给出报警，最终还是需要人工验证；2、误报率高；3、爬虫无法覆盖业务，尤其是需要交互的业务逻辑（这部分常常是关键业务）；4、无法识别数据是否核心；5、无漏洞关联检测能力	需要对业务及系统有足够的测试覆盖，传统安全测试人员数量有限（通常1~2人/项目），因此对测试人数及水平有较大要求	<ul style="list-style-type: none">1、可做到无条件限制能够直接接触目标核心数据；2、测试结果经过人工判断，保证有效性、可重现，威胁评级准确无误；3、识别漏洞最终威胁性，如是可获取关键数据或边缘数据
越权操作	无法检测	检测该类型漏洞对技术水平要求高，效果不理想	<ul style="list-style-type: none">1、可做到无条件限制能够直接控制业务逻辑；2、测试结果经过人工判断，保证有效性、可重现，威胁评级准确无误
数据泄露	<ul style="list-style-type: none">1、只能判断基本的调试信息、报错信息；2、误报率极高，无判断威胁的能力；3、漏报率极高，如人员敏感信息泄露、帐号密码信息，程序不具有识别能力；	需要对业务及系统有足够的测试覆盖，传统安全测试人员数量有限（通常1~2人/项目），因此对测试人数及水平有较大要求，效果不理想	<ul style="list-style-type: none">1、深度分析与发现信息泄露，覆盖每一个业务角落；2、精准判断，结合其他方法进行更深入测试
业务篡改	无法检测	检测该类型漏洞对技术水平要求高，效果不理想	<ul style="list-style-type: none">1、可做到无条件限制能够直接控制业务逻辑；2、测试结果经过人工判断，保证有效性、可重现，威胁评级准确无误

- 并发有效性
- 多因素认证有效性
- 暴力破解限制 (Username & Password 纬度)

登录模块

漏洞挖掘

商户模块

- 购物车模块权限测试 (查看、收藏、删除、修改等越权)
- 订单CSRF漏洞测试

- 个人信息权限测试 (查看、删除、修改等越权)
- SQL注入型测试
- 跨站挂马测试

结算模块

支付模块

- 银行支付网关测试 (积分、金钱、订单号等信息)
- 商品数量、价格、积分分数有效性测试
- 传输安全 (跳转

- 恶意评价测试 (跨站攻击、刷单评价)
- 订单越权测试 (查看、删除、修改等越权)

订单模块

并发请求1提现5000元

user

余额只有5000

WEB

DB操作未加锁

提现10000
user1帐号余额-5000

并发请求2提现5000元

提现记录 提现申请 我的银行卡

提现单号	申请时间	提现金额 (元)	目前进度	状态
TX20150109	2015-01-09 03:40	7626.00	等待银行处理	进行中
TX20150109	2015-01-09 03:41	7626.00	等待银行处理	进行中

提现申请 提现记录 我的银行卡

账户余额: -7626元

申请人: [REDACTED]

开户银行: 招商银行

银行卡号: 62 [REDACTED] 2

手机号: 186 [REDACTED]

提现金额: [REDACTED] 元 * 金额不能为空

验证码: [REDACTED]

获取验证码

登录模块

- 登录凭证不安全数据存储（SQLite明文存储）
- 逆向分析（反编译，反汇编，动态分析）登录模块实现机制，测试APP登录加密算法实现
- 本地实现不当的安全加密（加密密钥泄露，不安全加密算法）
- 登录界面Activity劫持

传输模块

- 敏感信息明文传输
- 弱加密传输
- 无效SSL证书
- 忽略SSL证书异常，中间人劫持
- 常见OpenSSL安全测试（poodle攻击，Heartbleed攻击等）
- 请求与响应完整性检查

支付模块

- 订单越权查询
- 订单用户信息泄露
- 订单表单SQL注入，XSS攻击
- 支付金额篡改
- 积分逻辑问题
- 恶意评价商品
- 恶意刷单
- 越权订单收藏，删除，修改
- 支付请求并发测试



```
POST /ibp/toaMobile/iphone/qryAcctDetail.do?14213764 HTTP/1.1
Host: 
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 7_1_2 like Mac OS X) AppleWebKit/537.51.2 (KHTML, like Gecko) Mobile/11D257
X-Requested-With: XMLHttpRequest
Accept: application/json
Referer: https://218/index.html
Content-Type: application/x-www-form-urlencoded
Connection: close

Proxy-Connection: keep-alive
Content-Length: 165
Origin: https://
Accept-Encoding: gzip, deflate

accNum=62259&depSerialNo=00000&currType=RMB&busType=8101&FixedDepositSN=00000&channelType=1&responseData=JSON&jsVersion=150108&nativeVersion=2.1.8
```

```
HTTP/1.1 200 OK
Date: Fri, 16 Jan 2015 02:55:03 GMT
Content-Type: text/json; charset=UTF-8
Set-Cookie: 
X-OPNET-Transaction-Trace: a2_a10d65ee-173f-428f-bd20-b78f64dd00df
x-ua-compatible: IE=EmulateIE7
Connection: Close
Content-Length: 574

{"errMsg":"","responseBody":{"accNum":"62259","accNumFormat":"","accStatus":"41","accStatus1":"正常","accType":"002","agreementID":"","agreementNo":"","allias":"","avaliBalance":"","balance":"50577.46","currType":"RMB","depositDate":"","endDate":"","endOper":"","fixedDepositSN":"","00000","freezeAmt":"","hideFlag":"","interestRate":"0.42","noticeType":"","openAccBank":"","openAccDate":"20141009","pledgeeAmt":"","pureAvaiBalance"}}
```


漏洞盒子企业安全服务列表

安全测试	渗透测试（众测模式&私密模式） 源代码安全审计 脆弱性评估-应用程序&网络 移动APP安全测试 IoT及智能设备安全测试
安全培训	安全开发培训 安全测试培训 安全意识教育
安全咨询	风险评估 应用架构安全分析 安全开发、安全编码咨询 安全开发流程（SDL）体系构建咨询
其它	漏洞预警 应急响应

通过和公安部的深度合作，可提供信息安全认证培训服务

信息安全认证培训	
信息安全师 (初级)	使培训对象掌握基本安全管理技能，熟练应对常见安全事件，对复杂安全事件具有一定的分析、判断能力。
信息安全师 (中级)	使培训对象掌握高级安全管理技能，熟练应对复杂安全事件，能根据实际应用情景需求，设计安全体系架构，并利用主流安全产品部署安全策略，面对各种安全事件有较强的分析问题、解决问题的能力。
信息安全师 (高级)	使培训对象具备对大型系统的规划、设计、维护能力，对复杂安全事件具有较高的分析、判断能力，能够解决复杂安全问题能力。

- 国家级标准体系，获得了政府职能部门、行业协会、信息安全产业市场和人才市场认可。
- 企事业单位聘用信息安全人才的业界标准。
- 提高个人技能的同时，增加就业选择竞争力。





网藤风险感知

让安全无法撼动
Make Security Entrenched Still

2016年9月

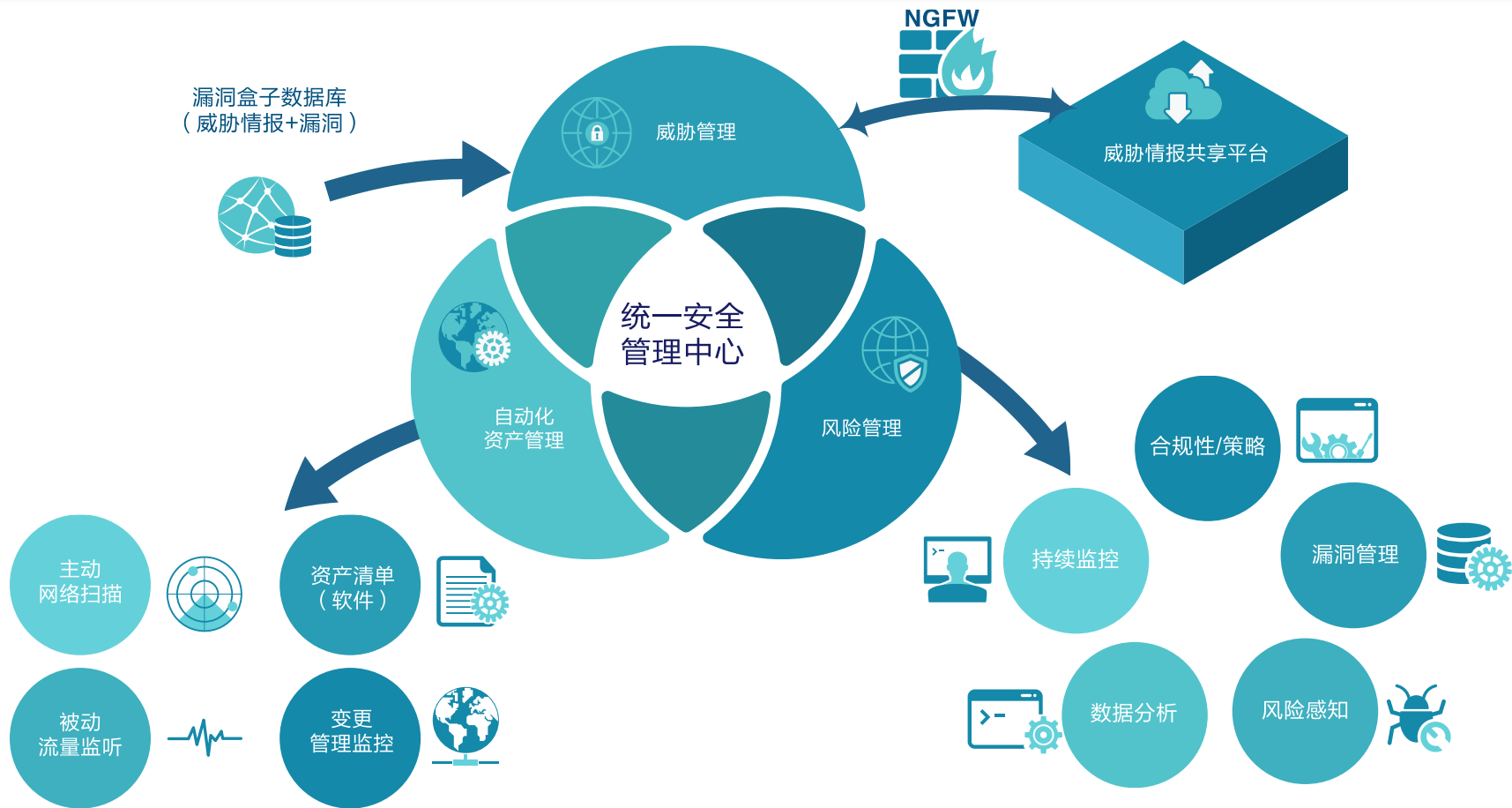
网藤 - 新一代企业级自动化安全服务

建立集中式安全监控与风险分析系统，运用下列关键技术，提供全方位安全解决方案

传感器：旁路式深度网络流量采集技术，可实时从用户活动、网络封包、网络设备等目标收集和汇总数据，支持OSI多层协议。

PRS(Passive Risk Sensor)：被动式风险感知，持续监控网络流量，深度预警与实时分析网络风险行为，消除周期性主动式风险监控的局限性，使视野更加全局完整。

ARS(Active Risk Sensor)：主动式风险感知，自动化发现企业关联资产，可对网络、WEB服务器、智能终端、应用程序进行深入的风险感知作业,帮助企业加强全网的风险管理。



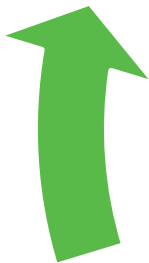
Monitoring

Discovery

动态、持续

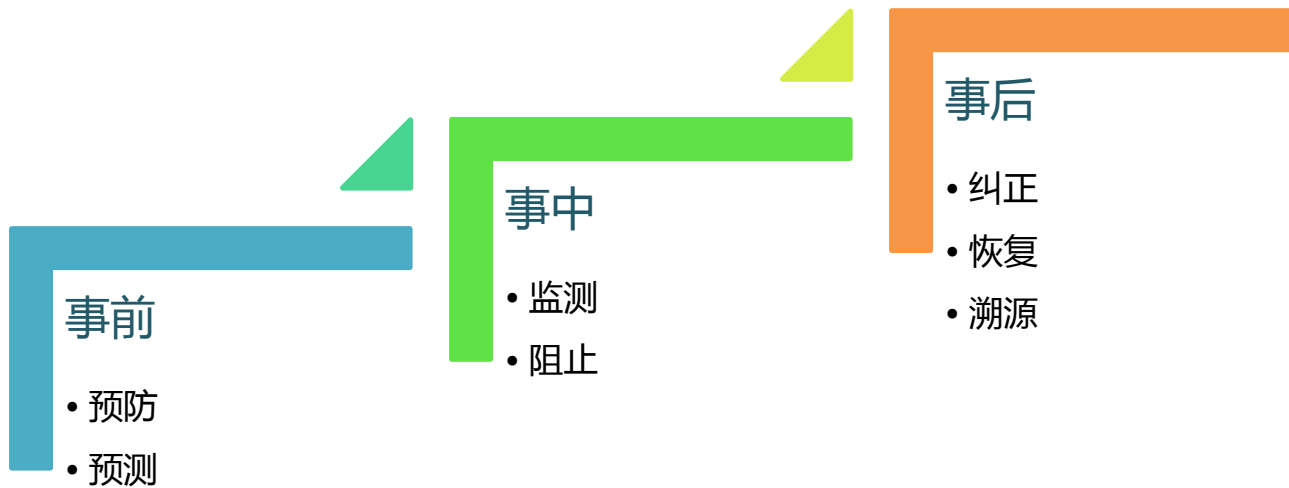
Remediation

Analysis





解决哪些问题？



网藤-资产管理，资产自动化发现、建模及变更监测，助企业便捷管理

资产发现



资产模型

- 自动化清点IT资产及遗忘资产
- 灵活修改资产模型
- 资产标签化、业务结构拓扑化
- 对发现每一资产建立基线模型

资产监测

- 对IT资产监测及变更管理
- 深入发现暴露在外面的设备、端口、应用程序，降低整体攻击面
- 及时发现资产变更带来的风险，如挂马、暗链
- 第一时间有针对性的发现安全风险，如0-Day漏洞

资产透视

您当前位置: 首页 / 资产透视

资产透视

资产拓扑

拓扑图

资产构成

子域

IP

关联IP

资产识别

登录入口

测试文件

功能组件

白名单

将从检测中删除

ch.com



域名 128



IP地址 57



服务 215

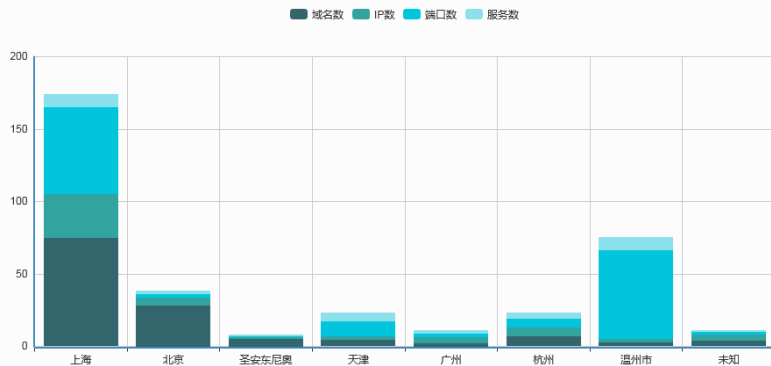


端口 215

网站 请选择网站

时间范围 请选择日期

各城市资产统计



资产分布城市



新增资产

IP	域名	服务	端口	来源
112.90.78.157	email.nq-sky.net	http,http,un...	80,443,843	系统发现
112.90.77.178	email.nq-sky.net	http,http,un...	80,443,843	系统发现
183.60.15.173	mail.ch.com	http,http,un...	80,443,843	系统发现

资产来源占比

系统发现 自主添加

自主添加



网藤-风险管理，提供持续性监测&分析技术，找出安全漏洞、降低安全风险，确保合规审计

Continuous Monitoring

- 深度流量监听、行为监控
- 纵深监测（文件、主机、网络）
- 入侵检测、恶意软件

Vulnerability Management

- 应用漏洞扫描、评估、安全配置
- 脆弱性智能分类、整治与监控
- 支持通用策略、漏洞规则库及时升级

Data Analysis

- 日志集中式管理、分类、搜索
- 异常侦察与事件关联分析
- 可视化风险报表、报告

Compliance / Policy

- 协助合规审计
- 等级保护
- PCI-DSS

Risk Sensor

- APT感知
- 异常&潜在危险行为
- 攻击路径预测&分析



通过网藤主动感知引擎，对企业关联资产进行安全风险感知



安全风险

漏洞检测

全面的漏洞规则库：OWASP-TOP10、CVE、CNVD
支持最新漏洞检测：漏洞盒子最新漏洞及0-Day高效转换

SQL注入、命令注入

跨站脚本攻击-XSS

失效的认证和会话管理

不安全的直接对象引用

跨站伪造请求-CSRF

安全配置错误

尚未验证的重定向和转发

运维风险

配置文件核查

权限过大

控制宽松

内部端口对外

弱口令

敏感数据外泄

开发后门

人为弱点

威胁情报

互联网漏洞平台

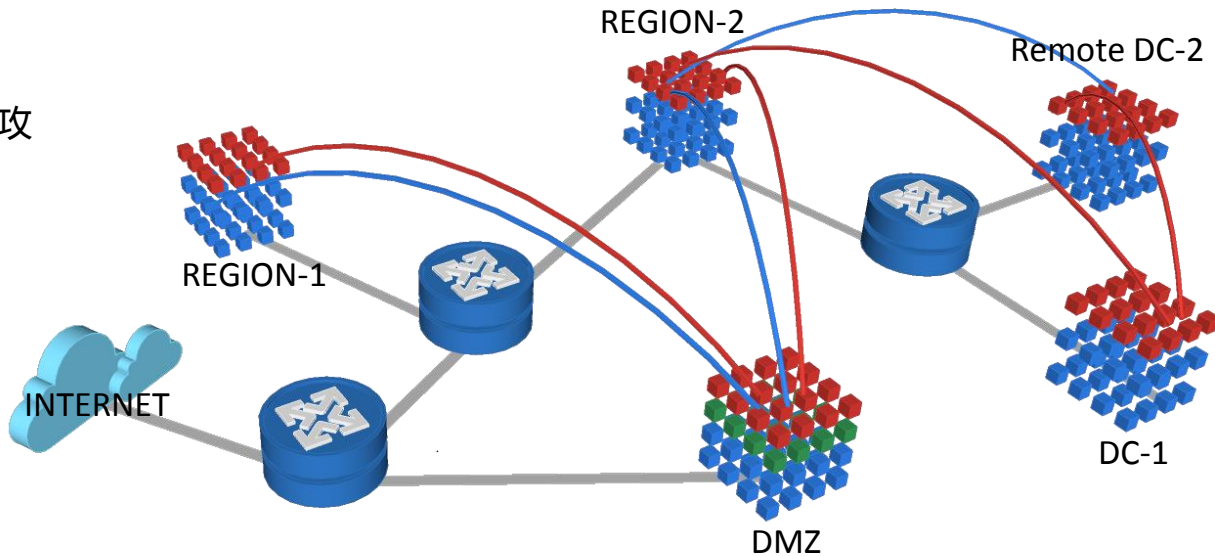
全网数据侦查

最新安全动态

数据联动分析

网藤-攻击路径预测 (Predicting Attack Paths)

- ❑ 漏洞矩阵
- ❑ 可利用矩阵，评估攻击向量
- ❑ 对外开放端口汇总
- ❑ 资产互联关系
- ❑ 应用服务



PRs

您当前位置： 首页 / 控制台

贴内保 添加任务 Sensor prsadmin

控制台

弱项

攻击事件

资产

报警

系统

风险管理

批量操作

所属任务 请选择所属任务 所属网站 请选择所属网站 风险名称 请选择风险名称

级别 全部 攻击事件

风险名称

XSS防御设置检测

OpenSSL组件漏洞

OpenSSL组件漏洞

OpenSSL组件漏洞

OpenSSL组件漏洞

应用攻击 暴力破解

被攻击应用 请输入被攻击的应用 攻击时间

服务器IP 请选择服务器IP 服务器端口 请选择服务器端口 攻击来源IP 请选择攻击来源IP

类型 全部 4920 SQL注入 2581 XSS攻击 2336 代码/命令执行 0 文件本地包含 0 远程文件包含 0 脚本木马 0 上传漏洞 0 路径遍历 0 拒绝服务 0 越权访问 0 CSRF 0

导出EXCEL

攻击事件	开始时间	结束时间	攻击特征	服务器IP	攻击来源IP	操作
------	------	------	------	-------	--------	----

风险工单

您当前位置： 首页 /

3 待处理工单 1 已关闭工单 0 已移交工单

工单编号	工单标题	提交时间	最近处理时间	执行者	状态	操作
20160575	CVS-2016-05-554193	2016-05-11 10:39	2016-05-11 10:39	cvstest	处理中	查看 删除
20160574	CVS-2016-05-554194	2016-05-11 10:39	2016-05-11 10:39	cvstest	处理中	查看 删除
20160573	CVS-2016-05-554195	2016-05-11 10:39	2016-05-11 10:39	cvstest	处理中	查看 删除



发现异常行为与潜在威胁	监控安全威胁和态势，发现安全薄弱环节
监控内部风险	发现员工发送机密的设计文件
协助合规审计	实时监控所有的网络行为，协助PCI等合规
精准捕捉	基于行为识别的机器学习，不断对内部业务行为学习建模，最大限度降低误报和漏报率
依据资产的风险定级	基于资产建模和等级划分，进行智能风险定级，协助企业快速修复风险
Open API – 无缝对接	提供RESTful Web Services API接口，可满足企业定制化需求



超越合规性转到以风险为基础的策略

定制架构，实现对组织真正风险的策略性评估，同时强调网络安全的优先级。



增加与企业最高管理层的协作

使用架构作为有效的沟通工具，以更为易用的方法，将网络安全策略传达给利益相关者，以获得支持。



运用架构驱动的网络全洞察

运用正确的技能、第三方情报和业界最佳做法，以实现源自架构的指导。

网藤风险感知



网藤SaaS云平台提供7x24小时安全监测

- 企业仅需提供域名，无需给出服务器IP
- API接口模式，灵活部署
- 可定制安全可视化、安全报告、预警服务

及时发现企业Internet应用安全漏洞
识别网站后门、黑客挂马、异常代码
发现企业应用系统异常状况提供安全预警

Internet

交易传输

入侵和破坏

安全威胁：
1、帐户失窃
2、钓鱼攻击
3、恶意代码

应用服务器群

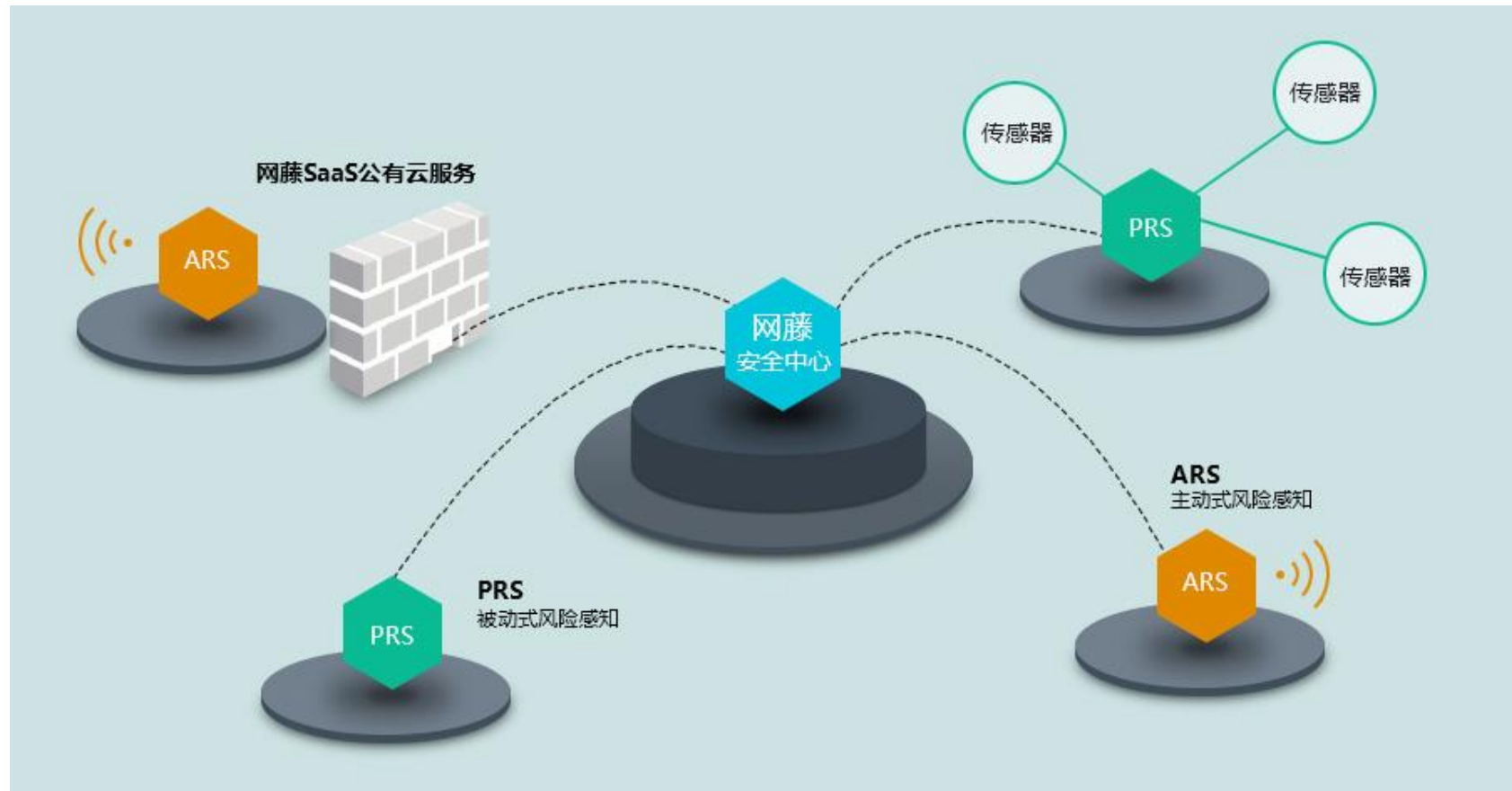
安全威胁：
1. SQL注入，命令注入
2. 跨站脚本-XSS
3. CSRF
4. 暴力破解
5. WEB页面篡改
6. 替换文件
7. 直接针对服务器的攻击
8. 窃取数据库数据
9. 新增业务或资产威胁

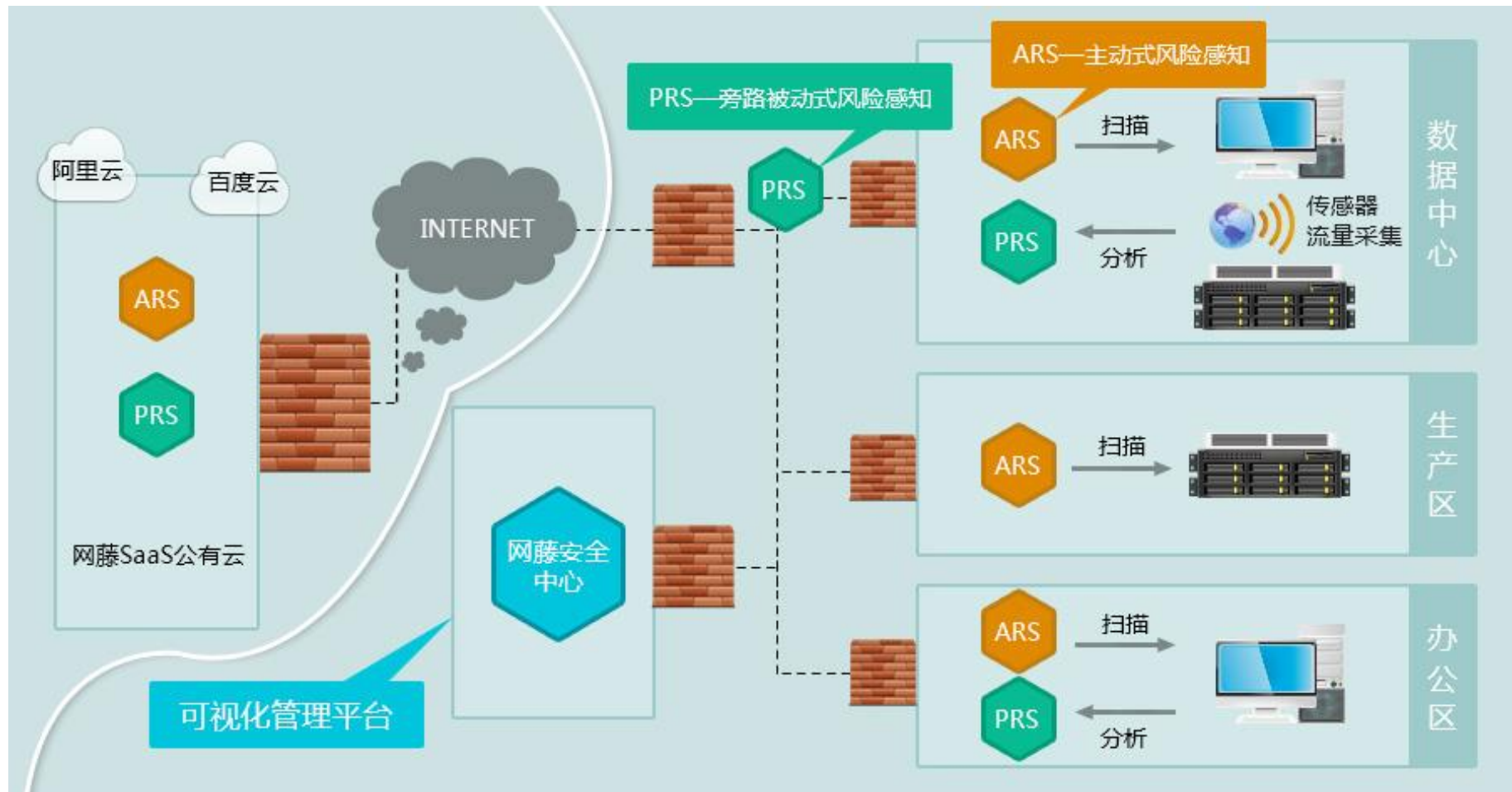
数据库群

安全威胁：
1、信息泄露
2、信息窃取
3、APT攻击

实时监测

分布式部署监测设备，ARS+PRS高精度风险感知







漏洞盒子

WWW.VULBOX.COM



网藤风险感知

www.riskivy.com



www.vulbox.com



www.freebuf.com



上海斗象信息科技有限公司

Email : mkt@vulbox.com

电话 : 400-156-9866

地址 : 上海市浦东新区碧波路690号7号楼7F