甲方SRC建设和运营之路

—— 董凯歌 智联招聘

第一篇章：SRC建设

SRC是什么?

SRC（Security Response Center，安全应急响应中心）

智联招聘SRC

智联招聘安全应急响应中心（Zhaopin Security Response Center） 诚挚邀请白帽子和各位安全爱好者同智联招聘一起保障广大用户的信息隐私、安全等问题。 本平台将收集智联相关业务及产品上存在的安全漏洞等相关情报， 并为各位参与者准备丰厚的奖励果实，等待卓越的白帽子前来采摘。 我们始终怀揣感恩的心，感恩每个关注智联招聘的人， 感恩所有为智联招聘的发展做出贡献的人

不同角色对SRC的看法

白帽子

验证思路(验证新工具/POC)

展示能力，寻求认同

通过挖掘安全漏洞赚取赏金，全职或者兼职

用户

企业重视安全问题

给用户带来安全感，B/C端用户放心将使用

安全团队

安全对外沟通的桥梁

扩大边缘感知范围，风险相对可控

优化企业安全建设策略，弥补安全漏洞

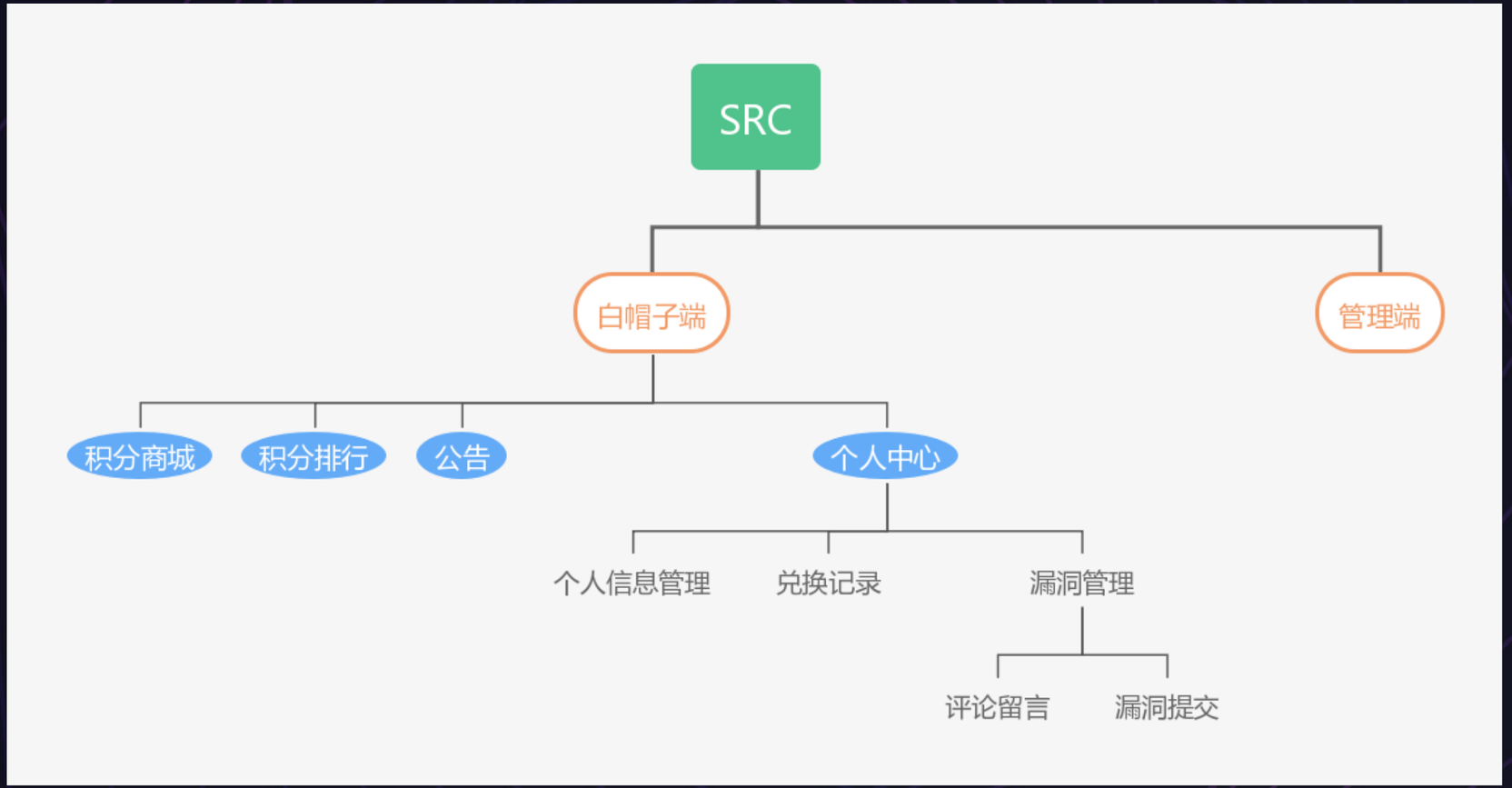
管理者

安全风险收敛投入

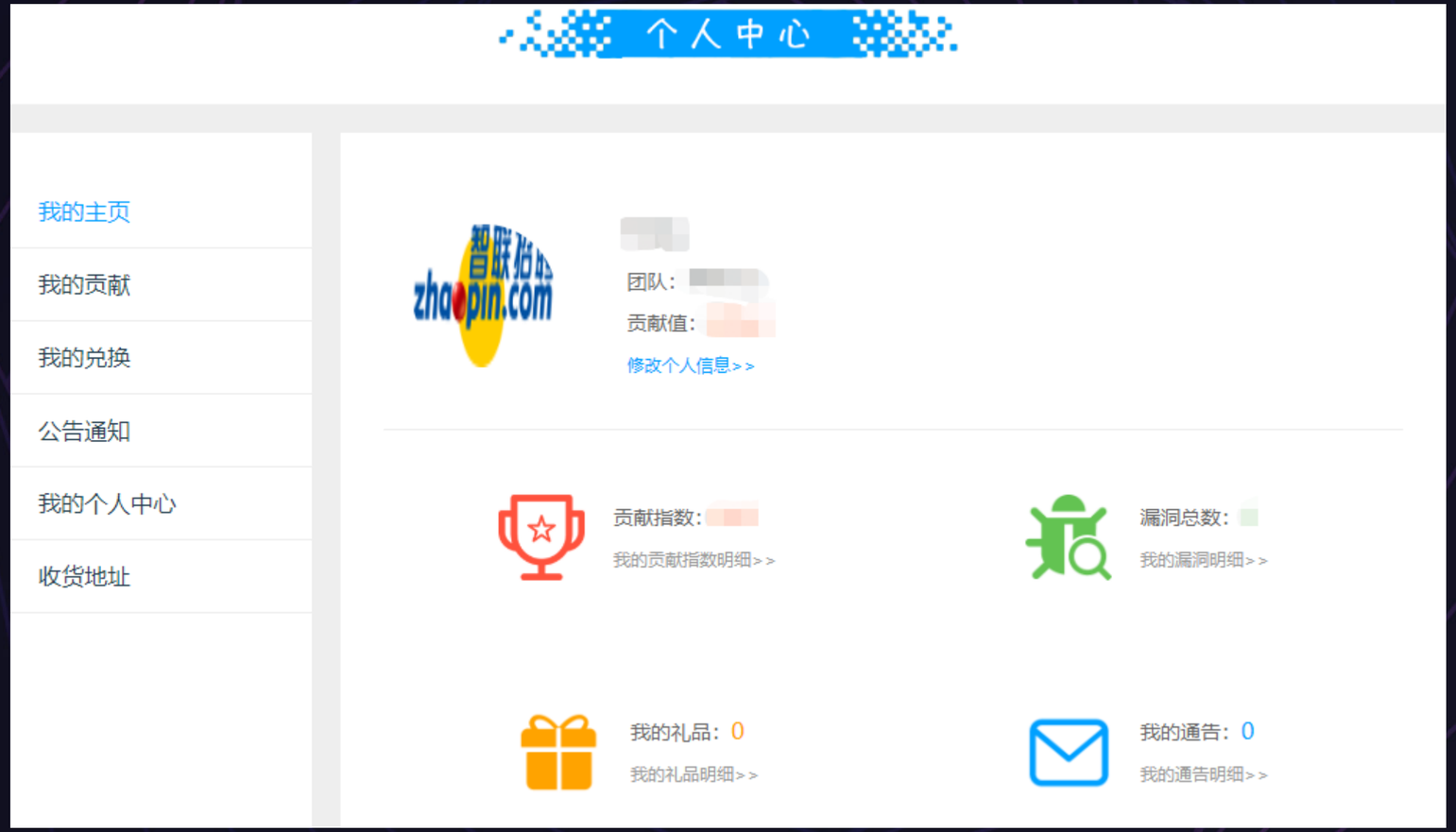
企业安全宣传渠道，提升公司品牌形象，增加产品安全口碑

安全人才储备

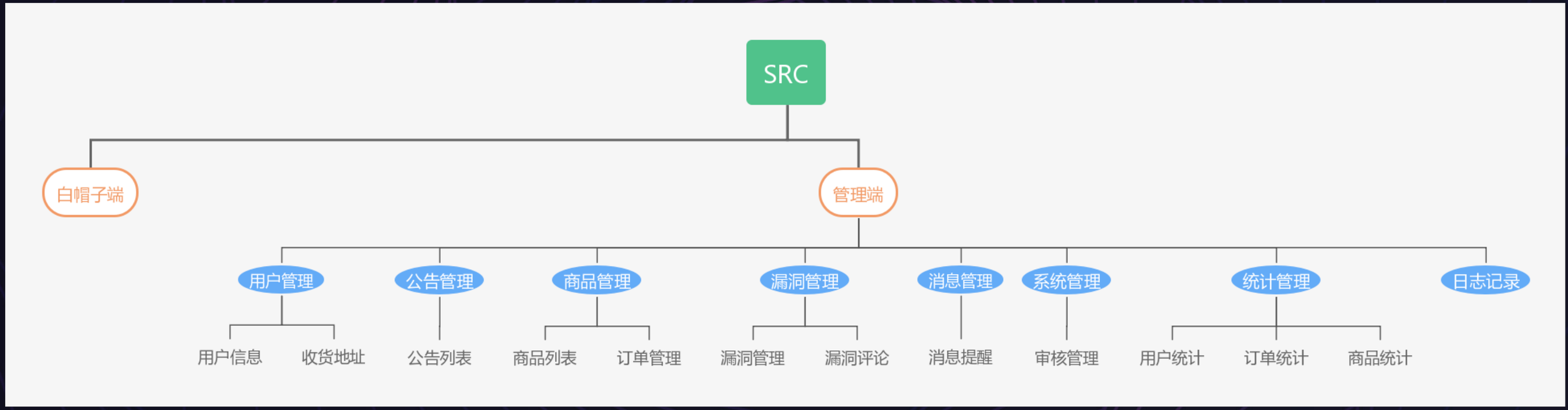
SRC白帽子端



SRC白帽子端


个人中心
我的主页
我的贡献
我的兑换
公告通知
我的个人中心
收货地址
zhaopin.com
团队：
贡献值：
修改个人信息>>
贡献指数：
我的贡献指数明细>>
漏洞总数：
我的漏洞明细>>
我的礼品：0
我的礼品明细>>
我的通告：0
我的通告明细>>

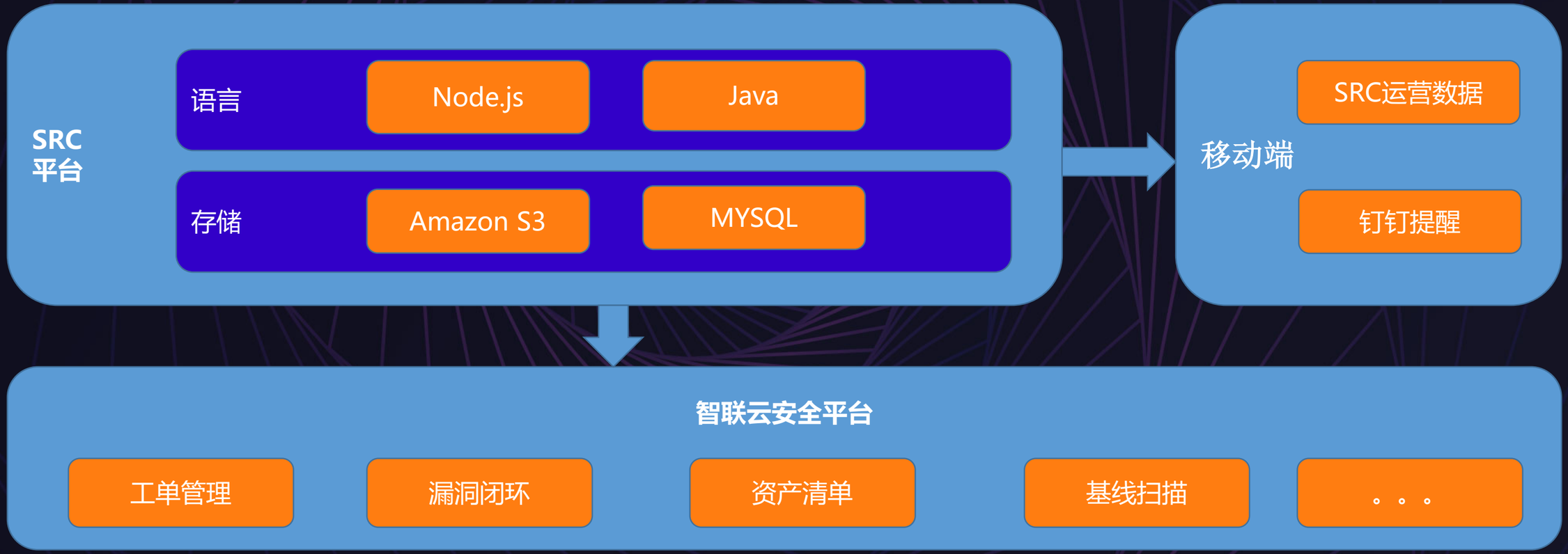
SRC管理端

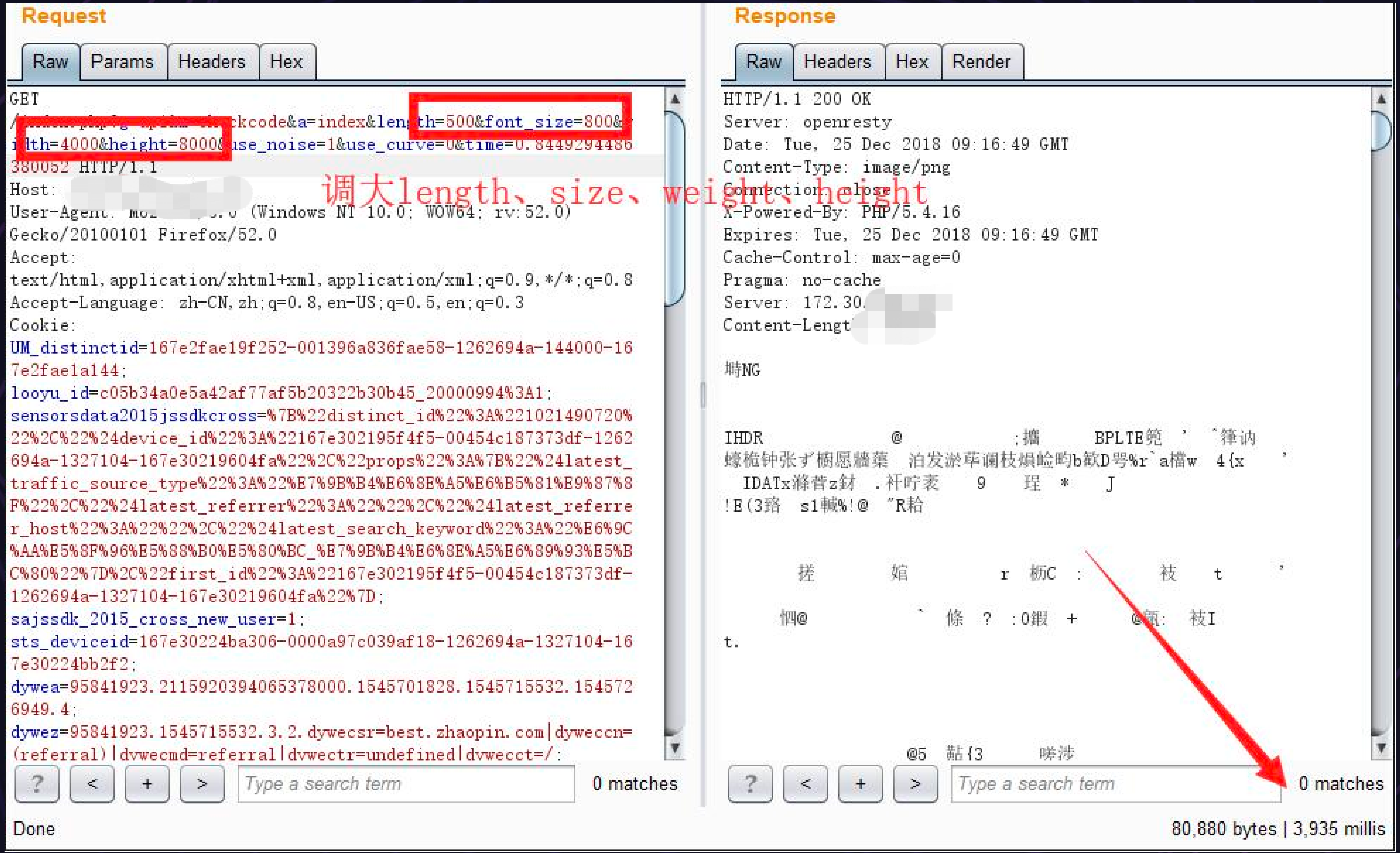

SRC
白帽子端
管理端
用户管理
公告管理
商品管理
漏洞管理
消息管理
系统管理
统计管理
日志记录
用户信息
收货地址
公告列表
商品列表
订单管理
漏洞管理
漏洞评论
消息提醒
审核管理
用户统计
订单统计
商品统计

SRC管理端


首页
用户管理
公告管理
商品管理
漏洞管理
消息管理
系统管理
统计
日志列表
首页
首页
快捷方式
漏洞列表
用户列表
公告列表
订单列表
漏洞消息
日志列表
数据统计
用户总数
380
今日在线
2
漏洞总数
商品总数
15
订单总数
102
漏洞指标
未解决漏洞
0
已确认漏洞
最久漏洞时长
2天
最快解决漏洞时长
1天
漏洞数量

SRC具体实现


SRC
平台
语言
Node.js
Java
存储
Amazon S3
MYSQL
移动端
SRC运营数据
钉钉提醒
智联云安全平台
工单管理
漏洞闭环
资产清单
基线扫描
。。。



Request
Raw
Params
Headers
Hex
GET
ckcode&a=index&length=500&font_size=800&
th=4000&height=8000&use_noise=1&use_curve=0&time=0.8449294486
380052 HTTP/1.1
Host:
User-Agent:
(Windows NT 10.0; WOW64; rv:52.0)
Gecko/20100101 Firefox/52.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Cookie:
UM_distinctid=167e2fae19f252-001396a836fae58-1262694a-144000-167e2fae1a144;
looyu_id=c05b34a0e5a42af77af5b20322b30b45_20000994%3A1;
sajssdk_2015_cross_new_user=1;
sts_deviceid=167e30224ba306-0000a97c039af18-1262694a-1327104-167e30224bb2f2;
dywea=95841923.2115920394065378000.1545701828.1545715532.1545726949.4;
dywez=95841923.1545715532.3.2.dywecsr=best.zhaopin.com|dyweccn=(referral)|dywecmd=referral|dywectr=undefined|dywecct=/;
0 matches
Type a search term
Done
调大length、size、weight、height
Response
Raw
Headers
Hex
Render
HTTP/1.1 200 OK
Server: openresty
Date: Tue, 25 Dec 2018 09:16:49 GMT
Content-Type: image/png
Connection: close
X-Powered-By: PHP/5.4.16
Expires: Tue, 25 Dec 2018 09:16:49 GMT
Cache-Control: max-age=0
Pragma: no-cache
Server: 172.30.
Content-Lengt
IHDR
IDAT
Type a search term
0 matches
80,880 bytes | 3,935 millis

博彩情报

边缘业务被黑

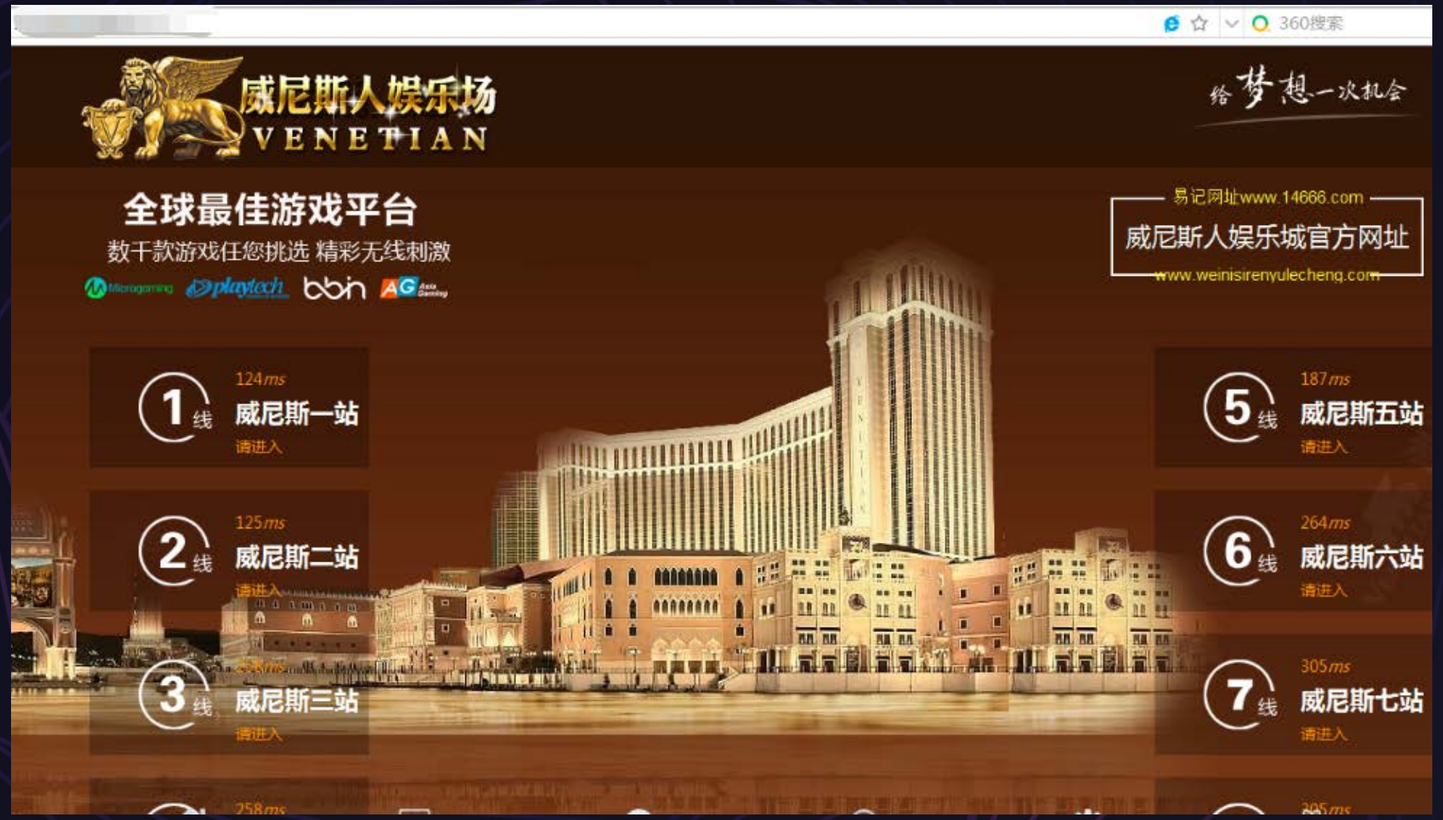
第三方外包

开源CMS

指纹收集

Waf防护缺陷

主机防护缺失



薅羊毛情报

安全上线流程规范

风控体系建设

威胁情报监控

APP算法破解

[技术专题] 智联招聘APP登录密码分析流程 [复制链接]

发表于 2018-7-17 01:45:20 | 只看该作者 | 只看大图

本帖最后由 Lunction 于 2018-7-17 01:59 编辑

话不多说,直接抓取登陆请求:

POST https://mi.zhaopin.com/android/My/LoginPostPassport?d=5677860f-ce3b-4bda-b2ae-9fd6454d6850&channel=360yingyong&v=7.91&key=135486907212185&t=1531747877&e=8abe76f88a49f281610

user_id:
user_location:
user_latlon: null;null
device_name: Nexus 5
device_platform: android
device_id:5677860f-ce3b-4bda-b2ae-9fd6454d6850
device_network: WIFI
device_resolution: 1080:1776
device_time: 2018-07-16 21:31:17
version_name: 7.91
version_code: 791
build_number: 0

password=a67266746b6568&userName=130xxxxx000

这里输入的密码是a123456

Apk没壳，直接拖入jadx反编译分析，最后确认它是使用SO里的encryptPwd方法进行加密的密码

```
package com.zhaopin.social.jni;

public class NdkTool {
    public native String encryptPwd(String str);

    public native String encryptUrl(String str, String str2);

    static {
        System.loadLibrary("_zhaopin_v1.0");
    }
}
```

APP算法破解

cpmain.cpp*

cpmain (全局范围)

```
1  #define _CRT_SECURE_NO_WARNINGS
2  #include "stdafx.h"
3  #include <iostream>
4  using namespace std;
5  int main(int argc, char **argv)
6  {
7      char* pwd = "a123456";
8      int pwdSize = 7;
9      char* constChar = "[redacted]367F6726FFA189370C0E9C3573AF4806B759773C4DD1ED6A";
10     for (size_t i = 0; i < pwdSize; i++)
11     {
12         unsigned char v6 = (unsigned char)pwd[i];
13         unsigned char v4 = (unsigned char)constChar[i];
14         printf("%2x", v6 + v4);
15     }
16     getchar();
17     return 0;
18 }
```

- APP反抓包
- APP加壳加固
- 密钥明文存储
- 接口防重放
- 接口签名效验

SRC不仅仅是收取漏洞平台

风险闭环

威胁情报

安全需求

SRC不仅仅是收取漏洞平台

第二篇章：SRC运营

上线前风险评估

漏洞跟踪闭环

zhaopin.com 智联招聘

见信好，该漏洞已修复，请安全团队验证，谢谢！

漏洞编号

ZL-VUL-20171212-154326

业务域名

[redacted]

漏洞名称

zabbix存在SQL注入

漏洞等级

高危

漏洞简介

zabbix存在SQL注入，通过构造payload可获取登录密码。

提交人

kaige.dong

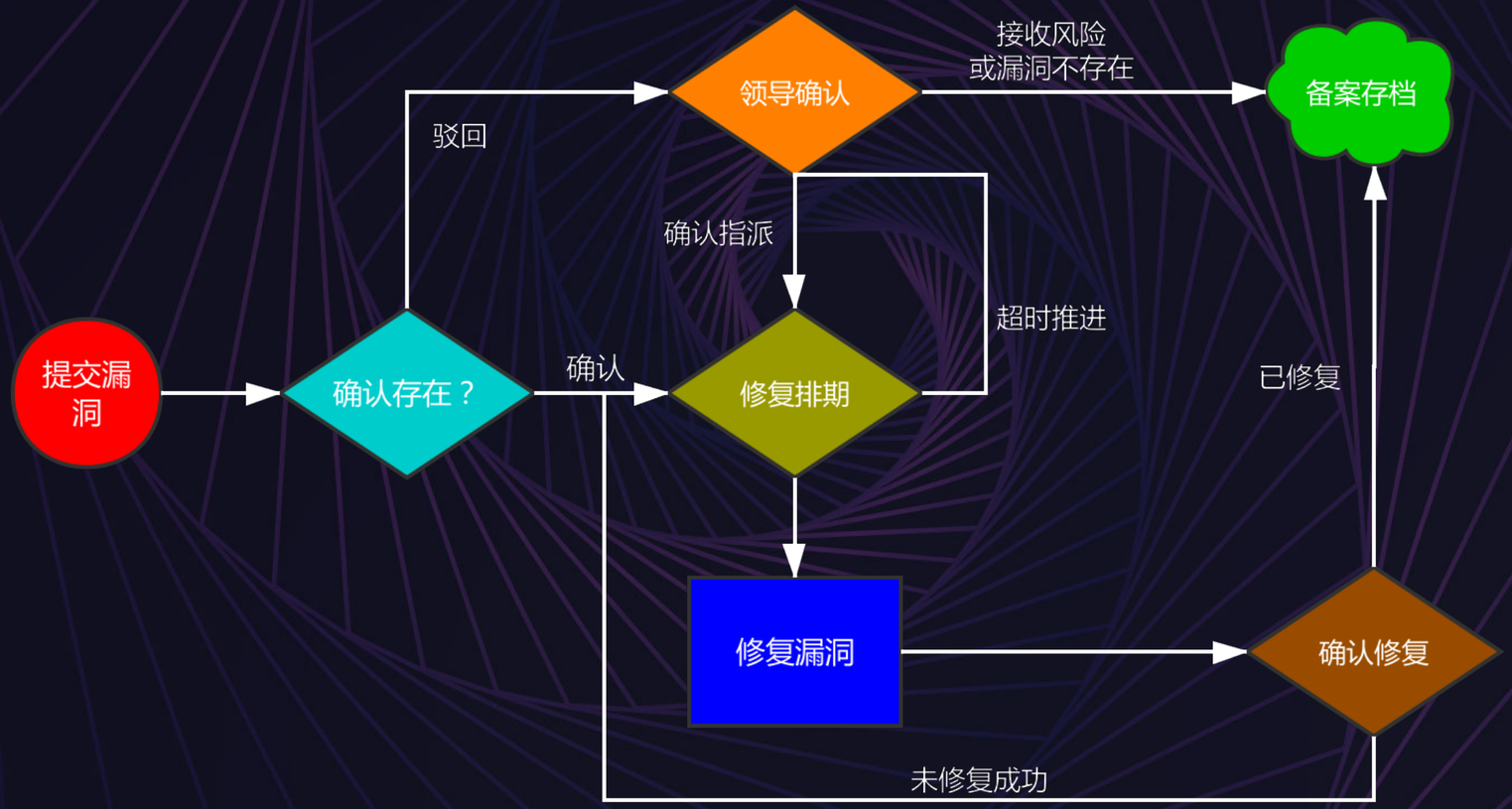
备注

已升级到最新版

漏洞超时机制：
高危漏洞：1天
中危漏洞：7天
低危漏洞：15天

一级提醒：漏洞负责人、漏洞协作人
二级提醒：直系领导
三级提醒：CTO、业务VP

漏洞跟踪闭环


提交漏洞
确认存在？
驳回
领导确认
接收风险
或漏洞不存在
备案存档
确认
确认指派
修复排期
超时推进
已修复
修复漏洞
确认修复
未修复成功

漏洞和威胁情报评估规范

漏洞奖励规则

智联招聘采用漏洞积分作为漏洞奖励，按资产的重要性及漏洞的影响来计算每个漏洞的积分(1积分=10RMB)：

核心及重要业务，包括：智联招聘主站、校园招聘主站、卓聘主站，包括个人端、HR端、企业端、通用型接口如登录等。

一般业务，包括：职Q、智联教育、智联测评等。

边缘业务，包括：临时活动页、已废弃活动页、已废弃的未及时下架的APP等。

不收取业务，包括：xue.zhaopin.com、e.zhaopin.cn、非智联业务

不同的安全漏洞和威胁情报，积分奖励不同，具体见表1-1：

	严重	高危	中危	低危
核心应用	150~300	50~150	20~50	5~20
一般业务	50~100	20~50	10~20	3~10
边缘业务	15~20	10~15	3~10	1~3

漏洞严重性分级

【严重】

【高危】

【中危】

【低危】

【无危害】

贡献榜

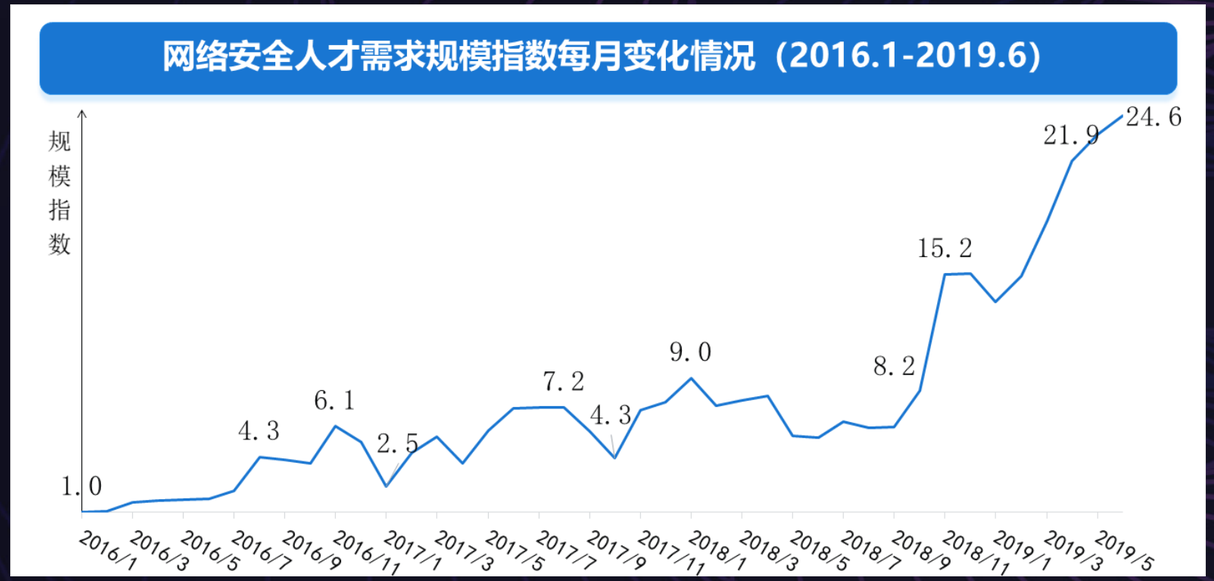
贡献榜

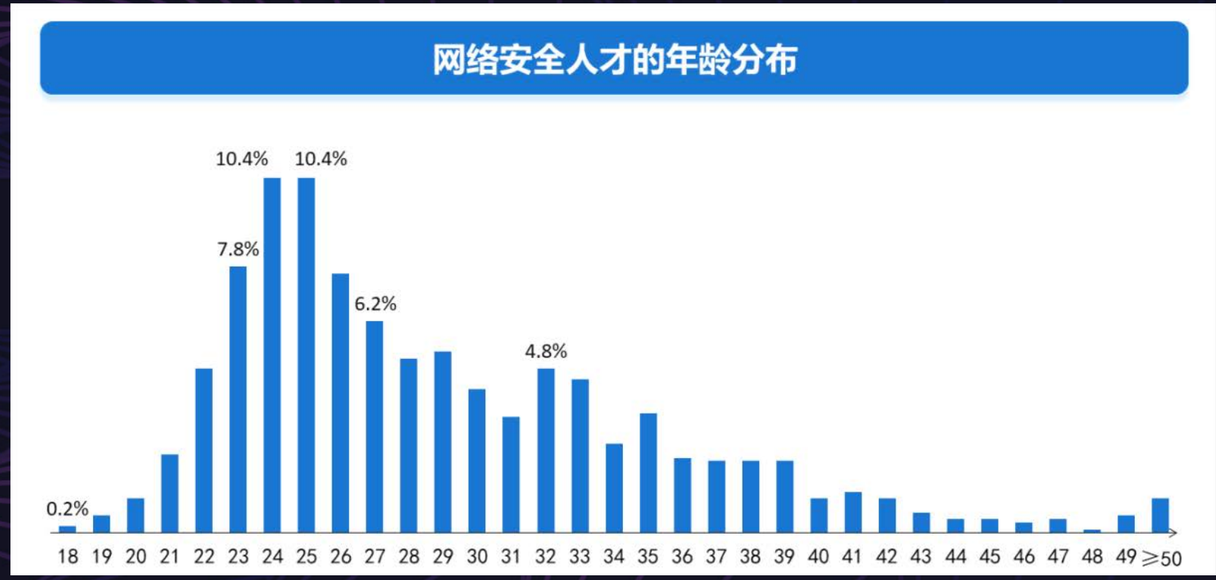
月度英雄榜 | 年度英雄榜 | 季度英雄榜 | 总排行榜

2019-12

排名	头像	昵称	团队	荣誉头衔	贡献值
1		龙腾至尊		安全师长	2140
2		黑色键盘	网络尖刀	安全团长	720
3		Ttstcy	NSTL	安全团长	647
4		HeartSky今天锻炼了吗	米斯特安全团队	安全团长	470
5		Wpel		安全团长	445

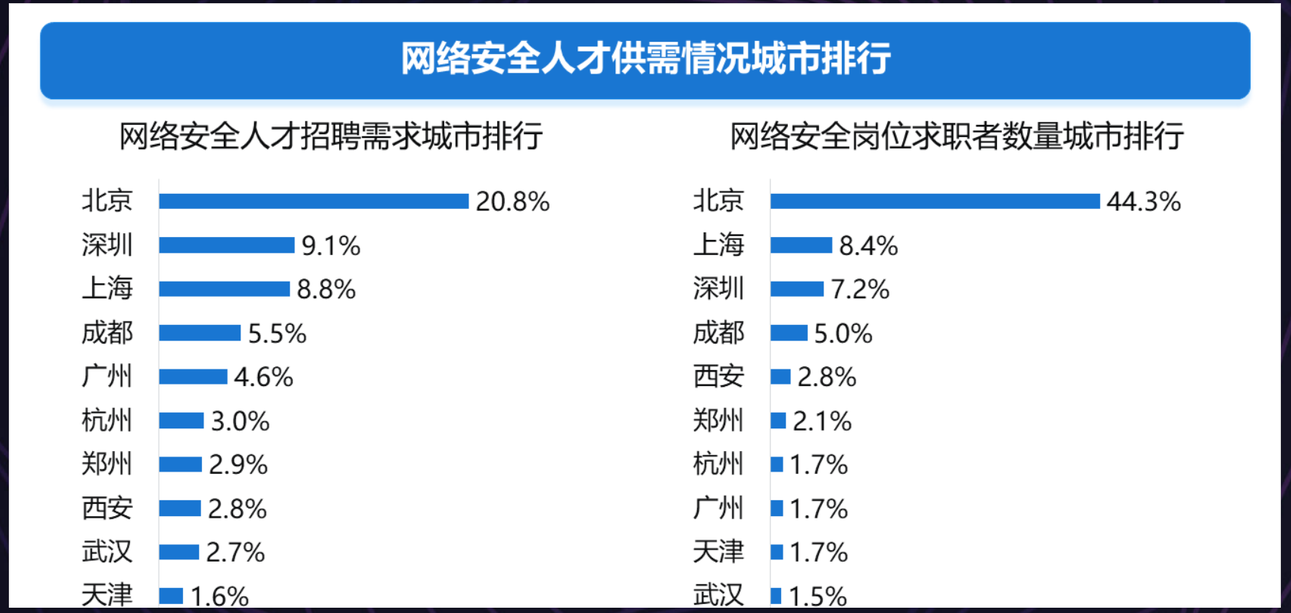
网络安全人才相关统计





网络安全法、等保2.0、密码法、个人信息保护法

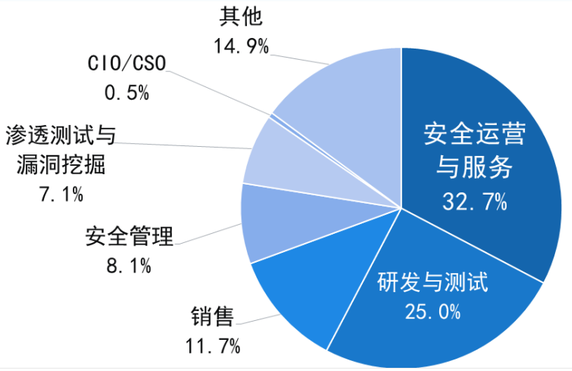
网络安全人才相关统计


网络安全人才供需情况城市排行
网络安全人才招聘需求城市排行
北京 20.8%
深圳 9.1%
上海 8.8%
成都 5.5%
广州 4.6%
杭州 3.0%
郑州 2.9%
西安 2.8%
武汉 2.7%
天津 1.6%
网络安全岗位求职者数量城市排行
北京 44.3%
上海 8.4%
深圳 7.2%
成都 5.0%
西安 2.8%
郑州 2.1%
杭州 1.7%
广州 1.7%
天津 1.7%
武汉 1.5%

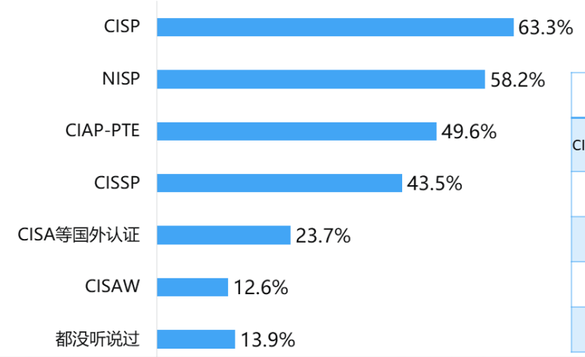
政企需要什么样的安全人员

2019年5月21日，揭阳网警工作发现违法嫌疑人苏某有涉嫌非法侵入计算机系统的行为。经深入调查发现，违法嫌疑人苏某于2019年5月13日，利用“御X”软件等对网站进行漏洞扫描，后用弱口令测试某中医院网站的后台并成功登陆，在未经授权的情况下擅自修改管理员账号密码，同时将该网站的漏洞提交给“漏洞盒子”网站。据其本人交代，其违法行为只是为了获取相应积分，有利于其以后找工作。违法嫌疑人苏某的行为构成干扰他人网络正常功能和非法侵入他人计算机系统，根据《中华人民共和国网络安全法》第六十三条，揭阳警方对其作出行政拘留五日的处罚。

政企机构网络安全人才的岗位类型分布



新晋网络安全人才了解或熟悉的资质证书



CISAW	信息安全保障人员认证
CISA等国外认证	注册信息系统审计师、Secutity+等认证
CISSP	注册信息系统安全专家
CIAP-PTE	CISP渗透测试工程师
NISP	国家信息安全水平考试
CISP	注册信息安全专业人员

智联招聘SRC愿景

一份工作就是一个饭碗，一个饭碗就是一个家庭的幸福

安全从业者关注求职者的信息安全，我们关注从业者的工作和幸福

THANKS