

2022护网选手招募

山东万码奔腾信息技术有限公司

2022年2月



01

护网行动介绍

公安部护网行动

护网行动是国家应对严峻的网络安全形势所做的重要布局之一，是由公安部牵头，各地政府，公安，国安以及各大企事业单位、安全厂商协同参与的国内最顶级的网络安全国家行动。

- 护网行动是一场网络安全攻防演练。针对全国范围的真实网络目标为对象的实战攻防活动,旨在发现、暴露和解决安全问题,检验我国各大企事业单位、部属机关的网络安全防护水平和应急处置能力。
- 由公安、高校、安全企业等组成红队，对政府、金融、能源等目标单位进行网络攻击，由目标单位、安全企业等组成蓝队对攻击进行应急与防御。

参加护网行动，与国内顶尖的网络安全工程师并肩战斗

历年护网项目

护网单位

- 中国移动总公司(北京)
- 中国核电(山东)
- 中国烟草总公司
- 国家开发银行(北京)
- 南方电网
- 中国邮政(北京)
- 光大银行(上海)
- 中国人寿(北京)
- 其他重要基础设施单位

安全厂商



护网行业

政府 税务 电力 电信 银行 交通 财政
广电 教育 互联网 检察院 法院 石油 等

案例1：中国移动集团护网 2021 保障

在2021年公安部组织开展代号为“护网-2021”的网络攻防演习中，中国移动代表通信行业参加。



移动总部蓝队应急保障现场



事中阶段：提供7*24小时值守监控；告警事件的分析确认；提供处置建议
绿盟在监护期间，上报攻击事件数246个，被客户专家处置80个

移动集团护网参与厂商及角色分工



- ◆ 加固组做行动前的系统脆弱性检查，安全加固。
- ◆ 厂商监控组发现安全事件，按模板填写事件单，并按要求在规定时间内上报至外部专家组进行研判。
- ◆ 外部专家组中获取事件单后，进行攻击行为判断,并向处置组下达处置任务。
- ◆ 厂商处置组根据专家组的判断结果实施IP封堵。

移动集团护网2021 分组职责

□ 加固组（系统脆弱性检查，安全加固）

安天、梆梆安全、爱加密对集团互联网暴露资产进行WEB安全漏洞、弱口令检测、APP安全加固。

□ 监测组（通过设备平台对攻击事件进行监测、并上报至分析研判组）：

绿盟：IPS、WAF、ESPC（企业安全管理平台）

启明：IPS、WAF；亚信：IPS、WAF

360：天眼；中科院：沙箱；观安：蜜罐

□ 分析研判组（攻击事件的分析研判，下达处置命令）

信通院、CNCERT安全专家驻场，对集团、省公司监测发现的攻击事件进行研判，并将确认的攻击IP下发有处置组进行封堵。

□ 处置组（封堵IP）

鹏信：一键封堵（与防火墙联动）

天融信\宏达隆和\安华金和：防火墙IP封堵





护网工程师招募

人员需求

护网行动需要大量的蓝队值守工程师。初级蓝队工程师技术要求较低，培训即可参加。山东万码奔腾作为一家实力过硬的网络安全公司，参与护网行动多年。今年的护网工程师开始招募，我们期待着你的加入。本次招募培养的主要是初级防守工程师。



招募流程

人员报名

计算机、网络、信息安全、
信息工程相关专业，在职/在
校毕业生均可报名

1



2



3



4



5



6



技术培训

公司组织高级安全工程师
进行一个月的线上/线下的
免费技术培训

项目安排

根据个人技术能力及项目
需求，安排工程师进入不
同的项目组

项目实施

工作时间为4月或5月的2-3
个星期，工作地点为北京、
山东、上海等甲方单位

工资结算

包住宿和差旅，具体工
资按照实际工时结算

工作推荐

表现优秀的工程师可留
任本公司或内推网络安
全企业工作

人员培训



网络安全基础培训



网络安全项目培训



项目及面试培训



安排到护网项目



培训过程完全免费，高级攻防安全工程师精心筹划课程。



自研的网络攻防演练平台，实战化练习，掌握基本的企业网络安全运维能力

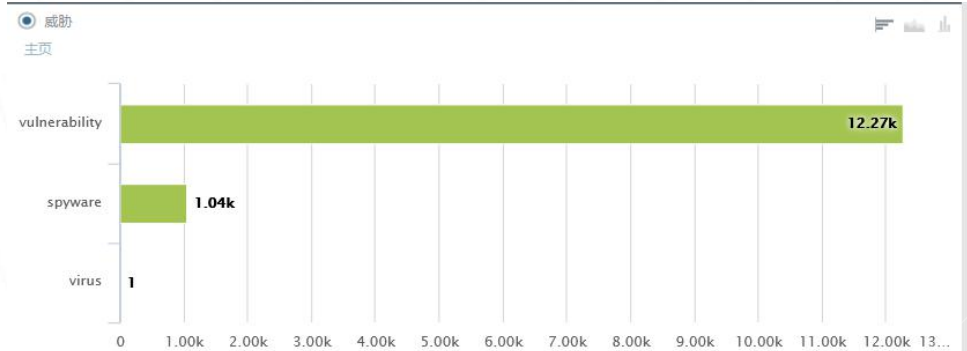
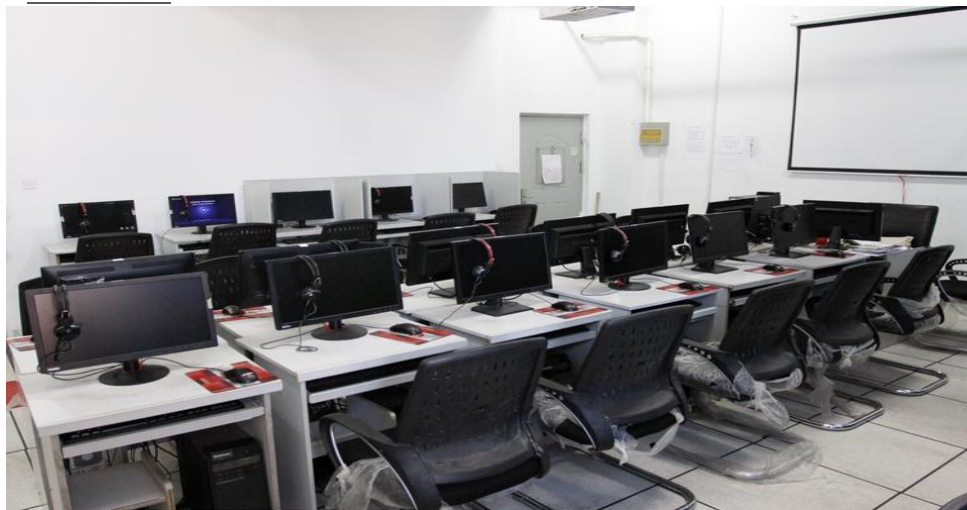


丰富实践经验，从实际项目中学到真正第一线的技术。

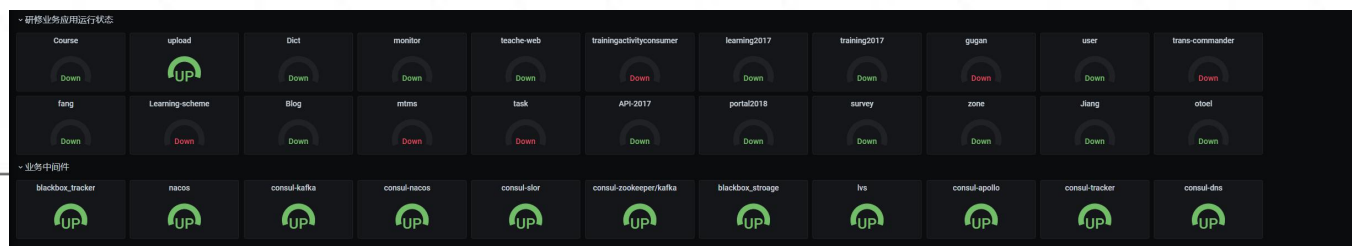
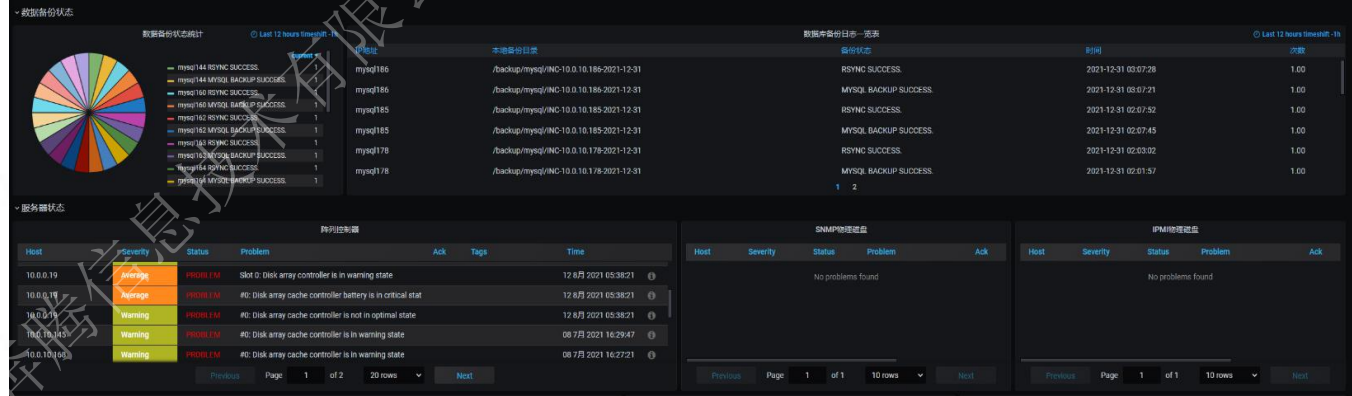
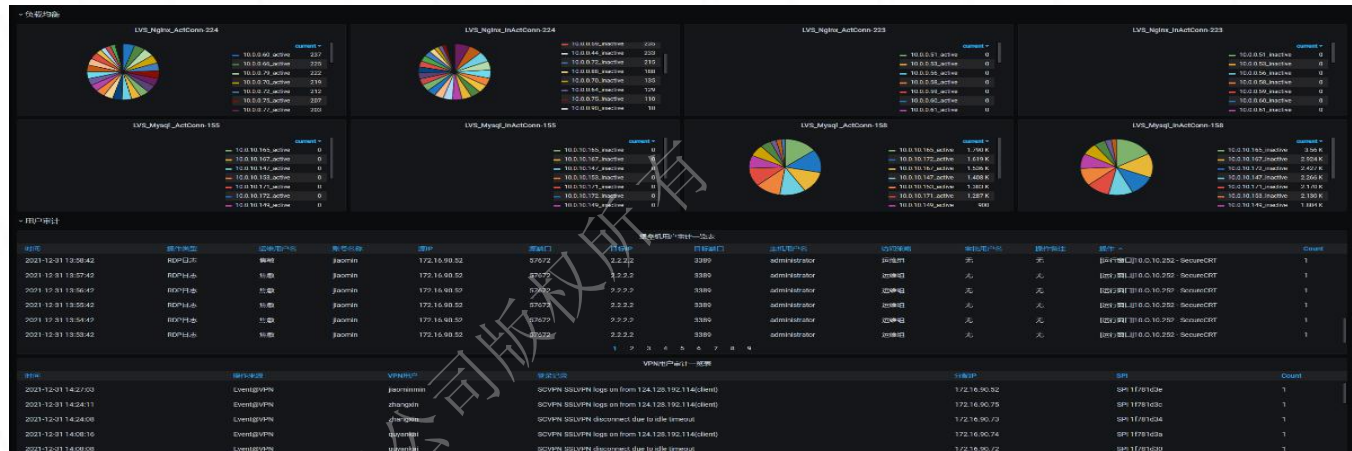


推荐一二线安全公司实习及就业

攻防设备实战



威胁名称	ID	严重性	威胁类型	威胁类别	计数
Oracle WebLogic Server File Upload Vulnerability	55542	medium	vulnerability	code-execution	6.2k
Microsoft IIS Escaped Characters Decoding Command E...	30444	high	vulnerability	code-execution	1.6k
HTTP Directory Traversal Request Attempt	30844	medium	vulnerability	info-leak	1.5k
Webshell.JSP.tenncc.Cmd_JSP File Detection	80819	medium	spyware	webshell	941
Apache Shiro Improper Authentication Vulnerability	58132	critical	vulnerability	info-leak	289
ZGrab Application Layer Scanner Detection	57955	medium	vulnerability	info-leak	273
HTTP /etc/paswd Access Attempt	35107	high	vulnerability	info-leak	241
Microsoft Windows win.ini Access Attempt Detected	30851	high	vulnerability	info-leak	233
VPN: Palo Alto Networks SSL VPN Authentication Brute...	40017	medium	vulnerability	brute-force	212
HTTP Directory Traversal Vulnerability	54701	high	vulnerability	info-leak	175
others	others	others	others	others	1.6k





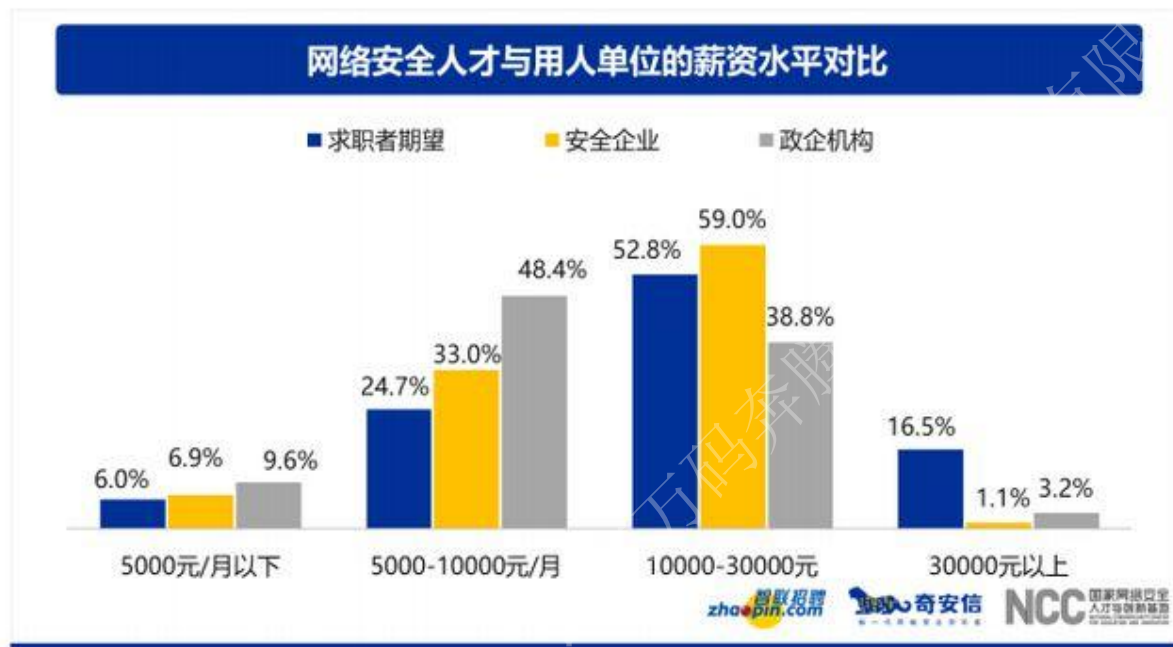
03

为什么参加护网

网络安全产业人才缺口大

我国网络安全专业人才缺口超140万人。今年上半年，网络安全产业人才需求总量较去年增长39.87%，安全研究、应急响应等岗位需求很高。

网络安全人员就业薪资：



网络安全人员需求缺口：



就业优势

▶ 与国内一线厂商合作，优秀的护网工程师可内部推荐：奇安信、安恒信息、深信服、天融信、360等国内一线安全厂商。

▶ 网络安全岗位选择丰富：

研发类：网络安全研究工程师、网络安全设备开发、攻防安全研究员等

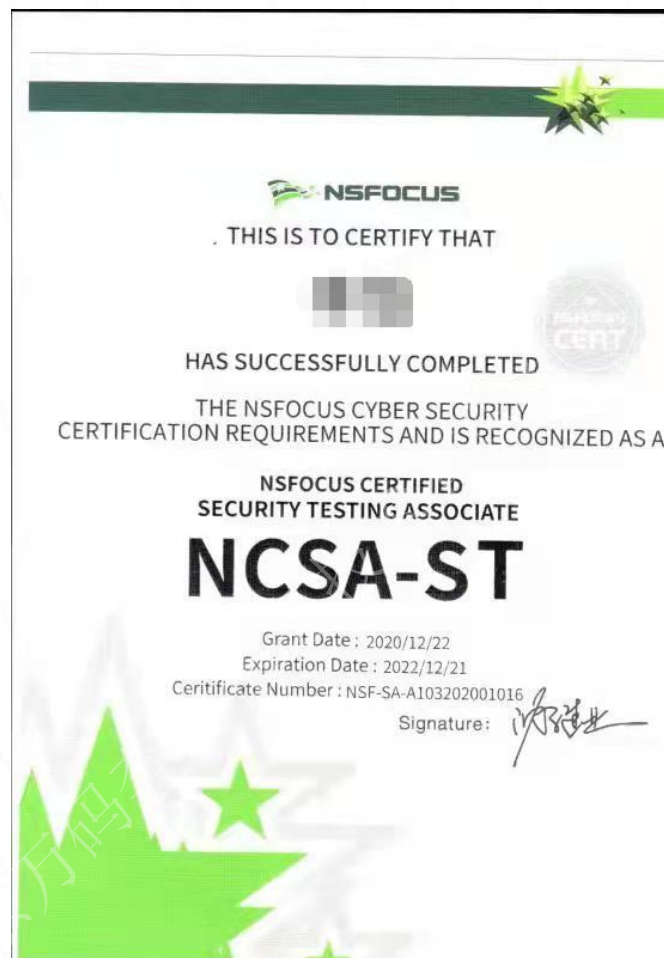
安服类：安全服务工程师、渗透测试工程师、反病毒工程师、代码审计工程师，风险评估分析师，网络安全建设工程师，等保测评师等

运维类：安全运维工程师、技术服务工程师等

▶ 有护网相关的项目实践经验，为以后的就业选择开拓一条新的道路

技术提升

- 由从业多年的攻防演练工程师进行培训，助你掌握主流的安全设备的使用。
- 在项目中直接参与到大型企业网络的维护管理之中，为自己未来的就业积累宝贵的经验
- 在于厂商的合作中，将有机会获得诸如360，绿盟等安全厂商的技术认证证书。



The background features a complex network of thin grey lines connecting various sized grey dots, creating a mesh-like structure that is denser on the left and right sides and sparser in the center. The overall color palette is light grey and white.

04

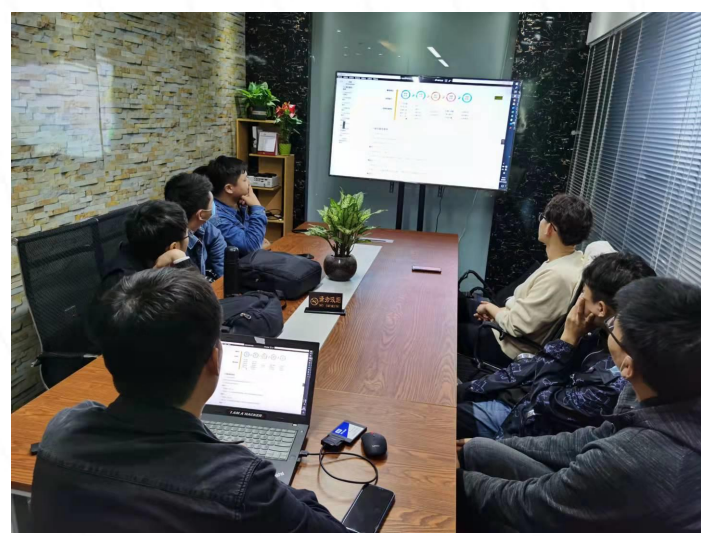
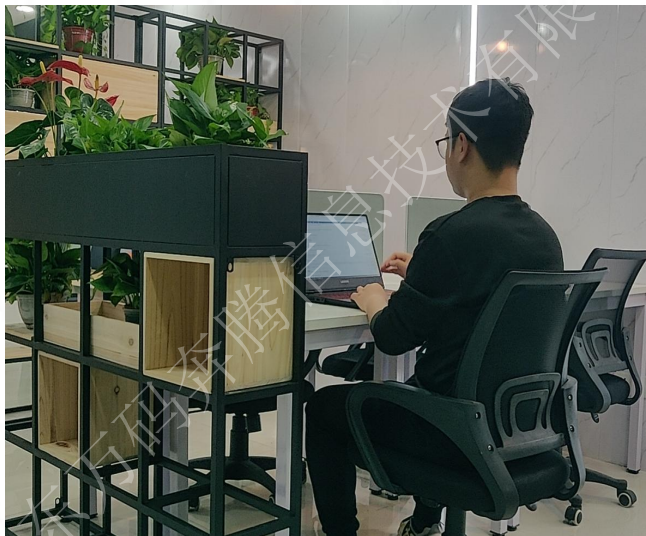
关于我们

公司简介

山东万码奔腾信息技术有限公司是专业的安全服务/安全软件产品供应商，致力于为合作伙伴提供优质的网络安全产品和服务。

公司总部位于泉城济南，人员总数50+，其中技术人员占比超90%，拥有攻防实验室、开发安全实验室两个实验室。

万码奔腾已服务合作伙伴超过百家。依托专业的攻防能力、资深的技术服务专家团队、丰富的交付经验，为合作伙伴带来高质量的安全服务交付能力，并在业内积累起了良好的服务口碑。



= code-gallop

参加网络安全护网行动，
为国家网络安全贡献一份力量

