2019“宁聚创新成果，共创无限未来”

单位参会岗位信息

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 单位名称 | 博智安全科技股份有限公司 | | | | |
| 单位规模 | 300人 | | | | |
| 工作地点 | 南京市雨花区软件大道168号润和软件园C幢5层 | | | | |
| 单位介绍 | 博智安全科技股份有限公司总部设在南京，坐落在软件大道润和软件园园区，属国家高新技术企业和双软企业。 博智主要专业从事信息安全领域，服务于军工、政府、金融，教育，国企。公司“安全御”产品线的系列产品连续多年进入国家和江苏省保密局政府采购推荐目录，服务于全国600多家政府、军工和企业用户。         博智是江苏省保密协会常务理事单位、南京市保密协会副会长单位，江苏省计算机安全专委会副主任委员单位、江苏省信息安全联盟成员单位。         博智十分重视人才队伍建设，目前拥有“江苏省双创人才”、“江苏省333高层次人才”、“南京321计划人才”组成的经营和技术骨干团队。为了更好的实现技术创新，公司聘请华东师范大学何积丰院士作为首席安全顾问，并聘请国家级信息安全专家——“中国反黑客第一人”许榕生研究员作为公司的首席科学家，带领技术团队进行信息安全领域技术攻关。         博智与多所重点大学和科研机构开展产学研合作，依托中科院高能所计算中心、中科院信息工程研究所国家信息安全重点实验室、北京邮电大学信息安全中心、华东师范大学软件学院和南京大学国家保密学院，力争共创国内一流的信息安全产品和解决方案的孵化基地。         博智知识产权体系完备，拥有数十项软件著作权和发明专利。公司多项产品和技术获得省市科技进步奖和金慧奖，并有多项产品获得省高新技术产品认定和省高价值发明专利认定。         凭借深厚的技术积累、持续的技术创新、先进的服务理念和专业的服务团队，博智立志成为国内一流的信息安全研发基地、产品供应商和技术支持与服务中心，成为中国信息安全领域的领军企业 | | | | |
| 联系方式 | 联系电话：13951826045 王老师  联系邮箱：[wangcui@elextec.com](mailto:wangcui@elextec.com)  （简历以附件形式发送，邮件主题及附件命名格式为：应聘岗位-学校-专业-学历-姓名） | | | | |
| 岗位信息 | | | | | |
| 序号 | 岗位名称 | 任职要求 | 岗位职责 | 所属部门 | 汇报对象 |
| 1 | web前端 | 1、了解Bootstarp，Echart，iview或elementUI, 等前端框架或类库；2、熟练使用Vue.js,了解其工作原理及内部组件使用，包括webpack等构建工具；  3、有数据可视化相关项目经验或web单页开发经验优先；4、熟悉任意一种后端开发语言python、jav或nodejs即可； | 1、参与PC端页面布局及开发，配合后端开发人员实现页面、交互相关功能；  2、负责数据可视化呈现等相关前端功能开发；  3、良好的编码规范，具备良好的表达能力和沟通能力。 | 技术研发部 | 部门经理 |
| 2 | Linux Python开发 | 1.参与过扫描器、协议分析等相关项目，2.工作尽职尽责，能完成领导安排的其它工作。 | 1.参与工控态势感知系统产品功能维护与迭代（后端开发）  2.参与工控运维管理系统后端维护 | 技术研发部 | 部门经理 |
| 3 | LinuxC开发 | 1.有流量深度检测、流量还原、流量特征分析经验优先2.有过wireshark协议解析插件源码优先3.熟练掌握linux c编程，进程间通信、消息队列、网络编程经验 | 1.参与工控审计系统、工控防御系统、入侵检测相关系统开发  2.参与工控攻击指纹特征提取，协议深度解析，及检测插件编写 | 技术研发部 | 部门经理 |
| 4 | 安全攻防专家/工程师 | 1.熟悉各种网络协议和网络架构，熟悉多种类型的网络攻击和防御手段；  2..熟悉各种攻防技术以及安全漏洞原理，具备独立分析或挖掘漏洞的经验；掌握漏洞利用方法，能够了解漏洞原理以及修复方法；  3.熟悉Linux操作系统，熟练掌握C、Python等语言的使用；  4.熟练掌握Web渗透手法，如SQL注入、XSS、CSRF、文件上传、目录遍历、获取Webshell等攻击技术等，熟悉攻防常用工具；  5.参与国内CTF比赛并且拿到较好名次或曾经有过举办比赛经验者优先;  6.有过实际漏洞挖掘案例、有各安全平台漏洞编号优先；  7.有网络安全或工控安全工作经验者优先；  8.熟悉软件逆向静态分析、动态调试、代码跟踪等，熟悉脱壳者优先；  9. 较好的逻辑思维能力和沟通能力，学习能力强，热爱技术，能独立解决问题；  以上满足几项即可。 | 1.具体从事信息系统安全漏洞的发现、挖掘、检测、分析和研究工作；  2.网络及应用入侵攻击和防护加固方法的研究，渗透性测试、软件源代码安全测试、安全工具研究等方面的工作；  3.熟悉安全攻防对抗技术，能从攻击者视角看问题，不断提升公司产品安全检测、防御、预警能力，指导安全研发团队研发安全检测、监控或防御方案；  4.参与安全事件应急响应，能对攻击进行溯源安全并给出改进方案；  5.CTF靶场、网络安全攻防比赛等的设计、赛题和技术培训工作； | 技术研发部 | 部门经理 |