| **岗位编号** | **岗位名称** | **职责简介** | **任职条件** | **具体岗位要求** | **特殊**  **要求** |
| --- | --- | --- | --- | --- | --- |
| 1101 | 软件漏洞  分析师 | 1、软件代码缺陷检测和漏洞分析；   2、软件安全漏洞分析技术研究和开发。 | 1、硕士及以上学历；   2、计算机、通信、网络安全、电子等信息类相关专业。 | 1、熟悉C、C 、Objective C、Java、C#、PHP等常见编程语言中的两种以上，具有一定的编程开发经验；   2、熟悉软件编译相关技术；   3、具备较强学习能力；   4、对软件安全具有浓厚的兴趣。 |  |
| 1102 | 信息技术产品 漏洞分析师 | 1、网络信息技术产品或系统的漏洞检测与分析；   2、网络信息技术产品漏洞分析技术研究和开发。 | 1、硕士及以上学历；   2、计算机、通信、网络安全、电子等信息类相关专业。 | 1、熟悉网络设备、网络络技术和网络协议。   2、具备较强学习能力；   3、对网络信息安全具有浓厚的兴趣。 |  |
| 1103 | 漏洞消控  工程师 | 漏洞消控技术研究 | 1、硕士及以上学历；   2、计算机、通信、网络安全、电子等信息类相关专业。 | 1、软件、计算机、网络、通信等基础知识扎实；   2、熟悉网络信息安全相关法规、政策、标准；   3、具备较强学习能力；   4、英文听说读写能力突出；   5、文字表达能力强，有一定的组织协调能力。 |  |
| 2407 | 信息系统风险评估工程师 | 1、进行安全评估服务项目的实施，包括安全评估项目的用户系统调研、安全评估方案编写，现场安全评估项目实施、项目后期的安全风险评价及项目报告的编制等。   2、现场安全评估项目实施需承担安全管理核查评估、安全技术配置核查评估、安全渗透测试、入侵痕迹分析、无线安全测试等技术测试工作中的至少两项。 | 1、硕士及以上学历；   2、网络与信息安全相关专业。 | 1、熟悉信息系统安全风险评估、等级保护测评方面的基本知识理论、安全标准和工作流程；   2、熟悉网络设备、安全设备、操作系统、中间件、数据库及Web应用等相关的安全技术及安全检测，至少精通其中两项。   3、有较强的动手能力，能够熟练使用常用的安全测试工具，如扫描测试工具、渗透测试工具等；具备一定的开发能力，可自己开发安全测试工具者优先。 |  |
| 2408 | 云计算安全 测评及研究  工程师 | 1、 实施云计算安全测评项目及安全审查工作；   2、 进行云计算特性相关安全技术方面的科研工作。 | 1、硕士及以上学历；   2、计算机及信息安全相关专业。 | 1、熟悉国内外云计算及云安全的发展情况；   2、熟悉云安全审查的相关国家政策及国内外安全标准等；   3、对云计算特性相关的安全技术（如虚拟化资源隔离技术、云计算环境下数据安全保护技术）有较为深入的研究；   4、熟悉对常见虚拟化技术和主流云计算平台，如Openstack、VMWare、KVM等。 |  |
| 2509 | 安全大数据  挖掘师 | 针对海量安全数据，开展数据建模、分析和挖掘，发现网络空间虚拟主体及可疑行为之间的关系，从中抽象出可推广的数据安全产品；根据网络安全态势编写需求，提供相应的数据支持方案。 | 1、硕士及以上学历；   2、计算机、统计学、数学、运筹学、信息处理专业。 | 理解机器学习基本算法的设计思想，掌握常用的数据挖掘和机器学习算法，有较强的算法实现能力；熟悉Hadoop、Spark或其他开源数据挖掘项目，具有实现分布式机器学习算法的经验者优先。 |  |
| 2510 | 大数据平台 运维工程师 | 负责大规模服务器的大数据存储、计算、分析平台的运维及优化工作，支撑漏洞挖掘、舆情分析、威胁监测等大数据业务。 | 1、硕士学历；   2、计算机相关专业。 | 熟悉Linux操作系统、云平台、Hadoop/Spark生态系统组件（HBase、Hive、storm）的使用，良好的团队合作及沟通能力，较强的责任心。 |  |
| 2511 | 大数据安全体系研究员 | 跟踪国内外云计算和大数据技术发展，研究信息安全技术发展趋势和政策；研究大数据环境下的关键安全技术，参与相关科研项目、行业标准的起草和编制；为大数据安全保障体系建设提供技术支撑。 | 1、硕士及以上学历；   2、信息安全、计算机、自动化和电子信息相关专业。 | 具有深厚的信息安全理论功底，较强的科研能力，参与和指导相关课题和项目；熟悉云平台、Hadoop/spark生态系统的安全机制，以及业界典型防火墙、入侵检测、防病毒等安全产品原理；具备较强的文字组织、语言表达能力和组织协调能力。 |  |
| 2714 | 大数据分析  工程师 | 分析网络行为数据，建立相关领域模型；设计分析算法，利用大数据技术进行实现；验证分析结果，定位安全事件。 | 1、硕士及以上学历，博士研究生优先考虑；   2、信息安全、计算机等相关专业。 | 1.相关业务/研发经验，专业技术背景；   2.熟悉大数据架构，了解SPARK，Storm，HIVE等，一项或多项者优先考虑；   3.具有系统开发能力；   4.具有机器学习，统计分析计算基础。 |  |
| 2715 | 网站安全分析工程师 | 从事Web安全研究，对安全事件进行分析及响应。 | 1、硕士及以上学历；    2、信息安全、数据分析、软件工程、通信工程等相关专业。 | 1.熟练掌握Web安全漏洞及解决办法；  2.具备一定的安全渗透测试能力；  3.具备一定的报告编制能力；    4.热衷于安全攻防技术研究。 |  |
| 2716 | 安全监测分析工程师 | 从事恶意代码、攻击样本的分析研究，日常网络流量的安全监测，网络流监测工作的前端工具研发等相关工作。 | 1、硕士及以上学历；   2、信息安全、数据分析、软件工程、通信工程等相关专业。 | 1.熟练掌握网络安全，大数据分析，网络协议分析，恶意代码分析，软件编程，渗透测试等一项或几项技能者优先；   2.具有较强实践动手能力，具有相关领域科研和工程工作经验；   3.具有团队合作精神和组织能力；   4.同等条件下，独立主持过大型科研和工程项目经历者优先考虑。 |  |
| 1204 | 信息技术产品安全测评  工程师 | 1、依据相关标准的要求对信息技术产品进行穿透性测试；   2、对主流信息技术产品进行深度安全检测；   3、对国外信息安全产品检测技术、攻防技术进行动态跟踪和研究。 | 1、硕士及以上学历；   2、信息安全、计算机、通信等相关专业。 | 1、熟练掌握操作系统、网络协议和信息安全相关技术，熟悉信息安全攻防知识，具备较好的攻防技能和经验；   2、具有较强的动手能力、分析问题和解决问题的能力，以及良好的文字表达能力；   3、有漏洞检测或分析经验者优先考虑。 | 仅限京籍应届毕业生报名 |
| 1305 | 移动安全技术研究员 | 负责Android/ios 系统及应用的安全性分析与测试，并参与移动安全前沿技术和国家级科研项目研究。 | 1、硕士及以上学历；   2、计算机、信息、电子类相关专业。 | 1、熟练掌Android/ios平台移动应用安全测试技术；   2、具有较强的逆向分析能力、有手机应用测试经验者优先考虑；   3、能力突出者，可不限专业，放宽到本科及以上学历。 | 仅限京籍应届毕业生报名 |
| 1306 | 工控安全技术研究员 | 1、对工控软件、通信协议、固件进行漏洞和隐患分析；   2、对工控系统及产品进行安全测评。 | 1、硕士及以上学历；   2、计算机、自动化相关专业。 | 1、至少掌握一种编程语言，熟悉网络协议等；   2、熟悉逆向分析、渗透测试等技术，对漏洞和网络攻击有深入了解和研究；   3、熟悉工控系统，有过组态编程经验。 | 仅限京籍应届毕业生报名 |
| 2612 | 攻防技术  研究员 | 1、国际前沿攻防技术与实战研究；   2、 科研项目规划与承担。 | 1、博士学历；   2、计算机相关专业，网络专业优先。 | 1、需要有实习或实践经验，包括理论科研课题承担；   2、在攻防技术方面有一定科研成果或心得。 | 仅限京籍应届毕业生报名 |
| 2613 | 渗透测试员 | 从事渗透测试与技术攻坚等相关工作。 | 1、硕士学历；   2、计算机相关专业，网络专业优先。 | 1、需要有实习或实践经验，不包括理论研究；   2、熟悉PYTHON编程；   3、熟悉网站建设和维护技术。 | 仅限京籍应届毕业生报名 |
| 3817 | 综合研究员 | 1、持续跟踪信息安全态势的发展变化；   2、开展信息安全综合分析研究；   3、开展信息安全专项课题研究。 | 1、硕士及以上学历；   2、国际关系、国际政治、新闻与文化传播等专业。 | 英语六级以上 | 仅限京籍应届毕业生报名 |
| 3818 | 分析通报员 | 1、开展信息安全漏洞与隐患信息的整编通报；   2、对漏洞和隐患信息进行综合研究。 | 1、硕士及以上学历；   2、国际关系、国际政治、新闻与文化传播等专业。 | 英语六级以上 | 仅限京籍应届毕业生报名 |
| 3919 | 高级网络舆情分析师 | 负责对互联网公开信息进行汇总、分析、研判，撰写大型综合分析报告和深度分析报告 | 1、硕士及以上学历；   2、新闻学、传播学、国际政治、情报学等相关专业。 | 1、熟悉互联网媒介中信息传播规律，具备良好的事件综合关联分析能力，文字功底扎实；   2、具有相关工作经验者优先。 | 仅限京籍应届毕业生报名 |