**蓝盾信息安全技术股份有限公司**

**技术研发岗位招聘信息**

1. **测试工程师**

职位描述：

1. 负责公司产品的软件测试；

岗位要求：

1. 网络基础：熟悉TCP/IP，局域网广域网相关知识等；

2、程序语言：熟悉其中一种或多种语言（C/C++、Java）；  
 3、数据库：熟悉其中一种或多种数据库的查询、修改、添加、删除数据库操作（SQL、 Oracle、Mysql、Sybase）；  
 4、操作系统：熟悉Windows，Linux系统的各种常用服务的搭建；  
 5、测试工具：熟悉操作一种或多种测试工具（IXIA、LoadRunner、QC、QTP、jmeter）。

职能类别：软件测试 系统测试

1. **Pyhon开发工程师**

职位描述：  
1、参与产品需求的讨论，编写相应的设计文档  
2、参与产品控制管理功能模块的开发和代码维护  
3、严格测试，保证代码的可靠，安全  
岗位要求：  
1、1年以上python的开发经验。  
2、有1年以上的web开发经验  
3、能够熟练使用python的web框架设计网站，例如django等  
4、熟练掌握各种web前端技术，包括html，js，jquery等  
5、熟练掌握mysql等常见数据库  
6、熟悉Linux操作系统，了解Linux下shell编程；  
7、拥有良好的代码习惯，结构清晰，命名规范，逻辑性强，代码冗余率低

职能类别：软件工程师 高级软件工程师

1. **安全攻防专家**

职位描述：  
1、负责系统渗透测试、漏洞分析及处理、组织攻防比赛（出题、环境搭建、评分）等工作；  
2、安全事件的应急处理、分析、回溯；  
3、业内安全交流；  
4、负责跟踪和分析国内外安全事件、发展趋势和解决方案，引入或开发安全工具；  
5、负责研究与挖掘漏洞；  
6、跟踪业界漏洞风险信息，并且及时进行通告；  
岗位要求：  
1、对某一领域的攻防、渗透技术非常精通，包括但不限于Web,Linux,Windows,Database,Openstack，Xen等；  
2、熟练使用各种渗透工具，有丰富的安全渗透经验并能能独立完成渗透测试；  
3、熟悉网络攻防的各类技术及方法，对各类web应用的弱点有较深入的理解，有实战经验；  
4、熟悉常规脚本语言，能够进行WEB渗透测试，恶意代码检测和代码审计；  
5、关注和了解最新web的漏洞，有良好的漏洞获取资源，并能熟练利用这些漏洞，具备漏洞挖掘的能力；  
6、主动性强，责任感强，具有良好的培训沟通能力和文档编写能力；  
7、 有大型安全会议演讲经验者优先，在业内有影响力优先；  
8、 具有较强的责任性，工作耐心、细致，可出差，能承受一定的工作压力。

职能类别：其他

1. **网络渗透测试工程师**

职位要求：   
 1.计算机或相关专业本科以上学历（能力突出者学历和专业不限）；   
 2.有Unix、Windows系统知识经验，能熟练使用Unix、Windows系统平台下各种应 用系统，如：MSSQL、Oracle、Exchange等；   
 3.熟悉相关网络安全产品，如防火墙、IDS、防病毒，漏洞评估工具等；   
 4.能够独立完成各种系统（主机、网络、数据库等系统）的安全评估和加固；   
 5.处理过网络攻击；   
 6.敬业、正直、诚实，喜欢学习新知识、乐于接受新事物；   
 7.良好的沟通能力与事件处理能力。   
 优先考虑的条件：   
 1.精通多种安全技术，掌握或熟悉各种攻击与防护技术；   
 2.具有一定的编程能力，可以自己编写简单的攻击和检测程序；   
 3.精通应用系统安全架构设计和攻防技术精通SQL注入、跨站脚本攻击；   
 4.理解多种Web应用技术（ASP.NET、PHP、JSP），并熟悉相关的安全问题；

职能类别：软件测试

1. **等级保护测评工程师**

职位描述：  
1、负责全国等级保护安全服务项目实施（尤其是政府、大型企事业单位项目实施），负责安全漏洞扫描、技术评估、人工访谈、整改建议、安全加固等工作；  
2、负责支撑方案编写、安全网络规划和设计；  
3、负责对客户/合作伙伴/内部员工进行信息安全技术培训；  
4、撰写项目相关文档报告，促进项目优质验收；  
5、完成领导交办的其它工作；  
岗位要求：  
1、信息安全专业或计算机相关专业，专科及以上学历，1年以上信息安全相关领域工作经验；  
2、熟悉计算机网络、通信网络、数据网络等基本原理，熟悉常见主流厂商的网络设备和安全设备基本工作原理；  
3、具有较强的沟通能力、团队合作能力、学习能力、文档撰写能力，工作态度认真负责；  
4、熟悉国家信息安全等级保护相关政策和标准，熟悉ISO/IEC 27000系列等信息安全管理标准／规范；  
5、具有等级测评师／CISSP／CISP／CCNP／CCIE或相关认证资质者；

职能类别：网络工程师

1. **安全攻防专家**

职位描述：  
 1、负责系统渗透测试、漏洞分析及处理、组织攻防比赛（出题、环境搭建、评分）等工作；  
 2、安全事件的应急处理、分析、回溯；  
 3、业内安全交流；  
 4、负责跟踪和分析国内外安全事件、发展趋势和解决方案，引入或开发安全工具；  
 5、负责研究与挖掘漏洞；  
 6、跟踪业界漏洞风险信息，并且及时进行通告；  
 岗位要求：  
 1、对某一领域的攻防、渗透技术非常精通，包括但不限于 Web,Linux,Windows,Database,Openstack，Xen等；  
 2、熟练使用各种渗透工具，有丰富的安全渗透经验并能能独立完成渗透测试；  
 3、熟悉网络攻防的各类技术及方法，对各类web应用的弱点有较深入的理解，有实战经验；  
 4、熟悉常规脚本语言，能够进行WEB渗透测试，恶意代码检测和代码审计；  
 5、关注和了解最新web的漏洞，有良好的漏洞获取资源，并能熟练利用这些漏洞，具备漏洞挖掘的能力；  
 6、主动性强，责任感强，具有良好的培训沟通能力和文档编写能力；  
 7、 有大型安全会议演讲经验者优先，在业内有影响力优先；  
 8、 具有较强的责任性，工作耐心、细致，可出差，能承受一定的工作压力。

职能类别：其他

1. **网络攻防环境模拟研发工程师**

职位描述：  
 1、统招大学本科及以上学历，计算机，信息安全等相关专业，2年以上工作经验；  
 2、熟悉网络攻防的各类技术及方法，熟悉Web应用，掌握常见的Web漏洞入侵与防范方法或技巧（SQL注入、XSS跨站脚本、CSRF跨站伪造请求、文件上传、文件包含、命令执行），并有实战经验；熟练掌握各种渗透测试工具，包括kali，metasploit等工具的使用并有实战经验；  
 3、熟悉C/C++、JAVA、ASP.NET、PHP、JSP、Python中至少两种编程工具，熟悉脚本技术；  
 5、具有良好的沟通表达能力，责任心强，能承受较强的压力；  
 6、有项目研发工作经验优先。

职能类别：高级软件工程师

1. **高级研究员**

职位描述：  
 1、配合项目申报工程师，依据项目申报要求，分析本项目所处行业及技术研究工作，编写项目可研报告等资料；  
 2、落实项目验收的答辩工作。  
 岗位要求：  
 1、硕士以上学历，计算机相关专业；  
 2、从事相关工作3年以上；  
 3、熟悉计算机、软件行业相关技术；  
 4、有良好的写作分析能力，能独立撰写可研报告等；

职能类别：科研人员