首先声明，这绝不是招聘广告，我们在设计这套技术定级体系的时候倒的确查阅了很多招聘信息，也发现有些渗透测试岗位的招聘信息算是千篇一律的内容，不管是初级安全工程师还是高级渗透工程师好像都是那么几条，而我们这篇文文章的内容有些的确比较适合用来设计不同级别的渗透测试岗位招聘信息的。

背景

在一个渗透测试团队建立之初，人员可能比较少，甚至说都有可能是一个人就是一个团队，这个时候只需要忙着做项目、做应急、写方案就行了，绩效什么的可能都没人单独去考核，工资也是领导根据你发际线高度大体就定了。

但随着人员越来越多，每个人擅长的方向和领域也有了不同，这个时候给每个人定一个薪资就有了一定难度。也有人说，技术岗位只要技术好那么薪资肯定就高，还说技术岗位的技术能力很好评定，但薪资不止是技术维度，还涉及积极性、饱满度、贡献度等，而且说技术能力好评定的估计也是没有细细考虑过的，比如你可以说在一个渗透测试项目里A挖的洞比较多比较突出，但你就这样来评定A的能力比其他人强就有点太牵强了。

基于这些考虑，我们团队内部制定了一套针对渗透测试团队的技术评级体系，供大家参考。

因为我们都是搞技术出身，没有任何薪资和人力相关经验，制定的评级体系也只是从技术角度去考虑，所以肯定有些不合理的地方，大佬们不要见笑~~

评级原则

我们制定评级体系的原则有如下几条：

1、透明原则

这是整个技术评级体系的设计核心。作为一个小型初创渗透测试团队（十来个人规模，而且水平都是比较水的那种，因此这一机制可能不适用于较大规模的团队或实验室），我们需要一个透明、自动化的机制来保证在技术评级这一敏感问题（直接挂钩薪资）上尽可能的公平。

2、引导技术为王的风气

毕竟还是初创团队，大家也都是在初级成长阶段，所以一个好的技术氛围也能引导大家能研究的更深能走的更远，尽量避免有些人在工作若干年后安于做项目，技术较为一般且成长较慢，但调薪时又会以资历老压住一些有能力的新人。

3、尽量保证所有项都能被量化

我们在设计每条考核指标的时候都讨论过该条款能否被量化，保证该内容不是非常模糊或者宽泛的内容，尽量能让大家在申请该级别的时候能根据自己的工作去匹配该考核项。

4、多套考核相结合

我们不仅只有这套技术评级来最终给团队成员定级，我们还会结合个人的绩效考核（主要涉及项目量、项目质量、报告质量、工作饱满度、工作积极性等）全年成绩，来确定该成员能否晋级。绩效考核是每月绩效工资的考核内容，也会对成员的每月收入有一定影响，不过不是我们今天讨论的重点。

适用范围

1、小型初创团队

团队处在快速成长期，成员能力和水平变动比较大，新员工赶超老员工的情况也比较常见，这时候就需要有一套比较好的技术评级标准来衡量考核相应技术提升。

2、上下均能认同该评级体系

每个级别都有不同的10个评定细则，这10个细则来衡量一个人的整体水平肯定比较片面，所以我们尽量挑选了一些比较有代表性、通用性的技术点，不管是领导还是员工也都认可：只要个人能力能达到该水平就代表能进行相应评级。

3、可以用来招聘

对每个级别的10条要求都是经过了认真赛选的，大家也算都能认可的，所以这些信息也可以用来设计招聘信息或者用来对不同技术层面的面试者进行面试。

评级方法

我们目前是要求成员在申请相应技术级的时候，每个级别下的10个评定细则中需要能满足7个及以上。另外，也允许越级适用条款，比如某成员在T2准备申请T3级时，可能有些T3的要求项不具备，但他具备T4的一些要求项，那么他也可以用T4的某一个或多个要求项来弥补T3申请时的不足。

评级细则

我们将渗透测试技术能力区分了7个级别，因为我们团队名是Tide，所以就用T来进行标识各级别了。

再次声明，因为我们属于初创团队，所以这种级别评定的水平和层次都比较低，大家觉得用得上的可以看看，薪资是我随手编的，大佬就当看个笑话就行了~~(>_<)~~

T1（助理工程师）

- [ ] 级别设计初衷：应届实习生、web安全初学者
- [ ] 年限要求：0-1年
- [ ] 薪资水平：6k-8k

> 能力描述：
> 1）有相关专业教育背景或从业经验；
> 2）对公司职位的标准要求、政策、流程等从业所必需了解的知识处于学习成长阶段；
> 3）能协助完成渗透测试项目。

能力要求：

- 1、熟悉Web安全、移动端安全等网络安全相关知识，了解网络安全法律法规与行业标准；
- 2、熟悉国内外主流安全产品和工具，如：Nessus、Nmap、AWVS、Burp、Appscan等；
- 3、能较好的完成渗透测试方案制定、文档编写等；
- 4、能根据测试用例进行逐项测试；
- 5、有较强的学习能力和钻研精神；

- 6、熟悉各类操作系统及数据库常见的安全漏洞和隐患，熟悉owasp top10；
- 7、熟悉各类网络安全设备、系统，如防火墙、VPN、IPS、WAF、防火墙、网页防篡改系统等；
- 8、具备一定编程基础，了解或熟悉C/C++/Perl/Python/PHP/Go/Java等开发语言；
- 9、具备良好沟通能力和语言表达能力；
- 10、拥有自己的博客、Github、安全圈等；

T2（初级工程师）

- [ ] 级别设计初衷：能独立完成项目，具有一定漏洞挖掘能力、应急响应能力
- [ ] 年限要求：0-1年
- [ ] 薪资水平：8k-10k

能力描述：
1）有相关专业教育背景或从业经验；
2）在专业领域中，对于本岗位的任务和产出很了解，能独立完成常规渗透测试项目，能配合完成复杂任务；
3）具有一定漏洞挖掘能力、应急响应能力。

能力要求：

- 1、熟悉主流的Web安全技术，掌握Web安全常规漏洞原理及防范措施，包括SQL注入、XSS、XXE、RCE等安全风险；
- 2、能对测试用例进行逐项深入测试，对测试备忘录中的所有漏洞都了解并能进行测试；
- 3、至少熟悉一门编程语言C/C++/Perl/Python/PHP/Go/Java等，能够进行脚本、漏洞验证的poc编写或改写；
- 4、熟悉Linux和UNIX主流操作系统和主流数据库（SQL、MySql、ORACLE等）并具备渗透测试能力；
- 5、能熟练搭建靶机并进行漏洞复现，并有文章总结输出3篇以上；
- 6、在各大安全漏洞平台、企业SRC平台提交漏洞；
- 7、处理过木马、病毒、入侵、网络攻击等突发安全事件经验；
- 8、分析高危漏洞原理和利用技巧，撰写相关技术总结文档；
- 9、具备WEB/APP（Android）渗透测试、数据隐私检测、安全评估、安全加固、应急响应、安全护航等实施和交付能力；
- 10、对CTF比赛中的web题目有一定的研究经验，了解加解密优先。

T3（中级工程师）

- [ ] 级别设计初衷：有擅长的安全领域
- [ ] 年限要求：1年及以上
- [ ] 薪资水平：10k-14k

能力描述：
1）在专业领域中，对公司职位的标准要求、政策、流程等从业所必需了解的知识基本了解，对于本岗位的任务和产出很了解，能独立完成复杂任务，能够发现并解决问题；
2）在中小型项目当中可以担任项目经理职责；
3）对逆向有一定了解，有自己擅长的安全领域。

能力要求：

- 1、熟练使用Perl/Python/PHP/Go/Java中的一种，能快速独立完成poc开发，如爬虫、破解类脚本；
- 2、对waf等各种防护措施的绕过有一定了解；
- 3、在知名安全媒体上发表5篇以上较受关注的文章；
- 4、具有一定的源码审计（php/asp/jsp/python）能力，发现过通用漏洞或发表过文章；
- 5、熟悉汇编、smali代码，具有一定逆向能力，能对病毒、木马、APP等进行分析；
- 6、具备一定内网渗透、域渗透能力，有成功案例；
- 7、熟悉windows、linux平台渗透测试、后门分析、加固；熟悉各类攻击技术，能针对各种攻击类型进行入侵分析和取证；
- 8、具有CTF比赛经验、网络攻防竞赛经验，熟悉CTF技巧并能拿到一定分值；
- 9、独立挖掘过通用漏洞，具有CNVD原创证书或cve证书；
- 10、在工控、物联网、云安全、人工智能、大数据安全等领域有一定研究并有成果。

T4（高级工程师）

- [ ] 级别设计初衷：侧重于逆向技术，引导内外部贡献
- [ ] 年限要求：2年及以上
- [ ] 薪资水平：14k-20k

> 能力描述：
> 1）在专业领域，具备一定的前瞻性的了解，对公司关于此方面的技术或管理产生影响；
> 2）对于复杂问题的解决有自己的见解，对于问题的识别、优先级分配见解尤其有影响力，善于寻求资源解决问题；
> 3）在内网渗透、安全开发、逆向分析等方面有所研究

能力要求：

- 1、精通一种以上脚本语言，能独立完成中小型安全平台的开发或对接业务安全需求进行定制化开发；
- 2、对waf绕过等有较深入的研究，能自己编写waf规则，能绕过多种防护设备；
- 3、拥有NSATP、CCNP、RHCE、CISSP、CISA等证书之一；
- 4、具备较强内网渗透、域渗透能力，具有3个以上中型内网成功案例；
- 5、熟悉J2EE或php开发架构，熟悉主流web框架；具有JAVA/php开发经验或代码安全审计能力（白盒测试）并有成果输出；
- 6、每年在专栏或公众号发表文章5篇以上，论文/期刊1篇；
- 7、熟悉x86/x64系列汇编语言、c/c++语言，熟练使用IDA、Windbg、Ollydbg、Immunity Debugger等分析工具，熟悉静态分析、动态调试、代码跟踪方法，具备较强的逆向分析能力；
- 8、参加国内较高水平CTF比赛，取的较多分值协助团队取得较好名次，熟悉通用加密算法、逆向或pwn优先；
- 9、有独立提交3个以上高风险漏洞，如补天或SRC等，SRC累积赏金一万以上；
- 10、具有cnvd原创证书或cve证书3个以上。

T5（安全研究员）

- [ ] 级别设计初衷：专精某一领域，研究较为深入
- [ ] 年限要求：3年及以上
- [ ] 薪资水平：20k-35k

能力描述：
1）在某一专业领域中，对于公司及业界的相关资源及水平比较了解；
2）开始参与部门相关策略的制定；对部门管理层的在某个领域的判断力产生影响；
3）是专业领域的知名人士。

能力要求：

- 1、熟悉逆向知识，具备多平台逆向经验(iOS/Android/Windows)，模拟器检测对抗研究等，能对病毒、木马进行深入分析；
- 2、熟悉浏览器、office、adobe以及flash等软件内部工作原理以及相应软件漏洞分析与利用技术；
- 3、对CTF比赛中的pwn、reverse题目有较深的研究经验；熟悉对称及非对称密码体系常见加解密算法；熟悉流量分析、数据隐写、取证等技术；
- 4、在阿里、蚂蚁金服、腾讯、360、百度等知名SRC排名前三；
- 5、每年在专栏或公众号发表文章10篇以上，论文/期刊累计3篇及以上；
- 6、能掌握一门或几门以下技术：PHP/Python/Shell/JavaScript/Ajax进行系统开发，至少精通一种数据库应用，如mysql、redis、mongodb等；
- 7、对业界前沿攻击和防御手法进行研究跟踪，能单独处置常见信息安全事件及热点事件跟踪，针对最新的安全漏洞及安全事件进行响应处理；
- 8、对内网渗透、APT攻防、黑灰产分析等有较深入研究并有成果输出，拥有反欺诈 / 反爬虫 / 业务风控 / 威胁情报分析能力；
- 9、对操作系统（win/mac/win）、移动端、工控、物联网等方面之一的安全技术有较为深入的研究并有成果输出；
- 10、能精通一门语言的主流框架，如php的tp5、yii或python的flask、django，掌握框架的安全漏洞及利用。

T6（安全专家）

- [ ] 级别设计初衷：技术专家，引导团队内技术走向
- [ ] 年限要求：5年及以上
- [ ] 薪资水平：35k-60k

能力描述：
1）是公司某一领域中的资深专家；
2）对公司某一专业方向的规划和未来走向产生影响；
3）对业务决策产生影响；
4）使命感驱动。

能力要求：

- 1、挖掘浏览器、Office、Adobe Reader、flash等客户端软件以及网络协议常见漏洞；熟悉操作系统的相关安全机制，掌握绕过漏洞缓解措施的基本方法；
- 2、在某领域出版过电子书籍或实体书，具有一定影响力；
- 3、熟悉常用算法和数据结构，精通C/C++/Java/Go/Python/Shell/Perl语言中的一种或多种，能够进行漏洞扫描器、网络爬虫架构设计与产品开发；能独立完成自动化安全扫描或者防御框架；
- 4、发表过有深度的技术Paper或独立挖掘过知名开源应用/大型厂商高危漏洞经历；
- 5、熟悉病毒木马，内核Rootkit的原理和行为，并对其做深入技术分析和逆向；
- 6、参加过geekpwn、xcon等大型安全会议的演讲；

- 7、精通防火墙、入侵防御、病毒防护、漏洞扫描、审计系统、身份认证等信息安全产品基础原理、安全部署，根据客户需求提供解决方案；
- 8、进行事件调查/追溯攻击者经历，IoC大规模处理经验，具备APT攻击和防御能力；具备从流量、日志、事件等数据中发现威胁的能力和威胁情报分析能力；
- 9、精通各类常见漏洞的原理、测试方法以及解决措施，具有分析研究安全漏洞的能力；且有丰富的攻击渗透实战经验、Fuzzing测试能力；
- 10、有大型CTF比赛(DEFCON、XCTF等)或国内顶级赛事获奖经历。

T7（首席安全官）

- [ ] 级别设计初衷：业内知名专家，基本无所不能
- [ ] 年限要求：8年及以上
- [ ] 薪资水平：60k-1000000k

> 能力描述：
> 1）业内知名，对国内/国际相关领域都较为了解；
> 2）对公司的发展做出重要贡献或业内有相当的成功记录；
> 3）所进行的研究或工作对公司有相当程度的影响；
> 4）使命感驱动；坚守信念；对组织和事业的忠诚。

能力要求：

- 1、参与国家地方或行业相关部门的信息安全标准制定；
- 2、主导过大中型网络、互联网应用等安全建设；
- 3、前沿安全攻防技术研究与利用，熟悉业界安全攻防动态，掌握国内外最新安全攻防技术；
- 4、对大数据、人工智能、物联网、工控安全、区块链等新兴技术具有较深研究，能够熟悉该行业最新攻击方法、渗透技术以及防御技术；
- 5、具备极为丰富的应急响应，事件调查经验，能利用技术进行事件调查/追溯攻击；
- 6、对安全体系的构建，安全架构的规划与设计、以及开发生命周期安全规范的落地具有丰富经验；
- 7、熟悉通用信息安全风险管理流程与框架，对国际国内信息安全标准如ISO27001，等级保护标准等有着较为深入的理解，并具有丰富的标准融合、体系落地及推广经验；
- 8、对代码虚拟化、反调试、反Hook等具备一定造诣，具备较强的逆向分析、攻防对抗、脱壳、反混淆相关能力；
- 9、对各类操作系统、应用系统的漏洞有较深理解，具有安全加固、渗透测试、应急响应等安全服务的实施经验；
- 10、拥有自己的研发专利、知识产权；出版过相关领域评价度较高的书籍。

两个问题

- 公开薪酬标准不怕其他公司来挖人吗

说到底对于大部分初创团队来说，市场上更有钱、更土豪的公司都大有人在。对于大部分小公司来说没有办法光靠钱引进人才。所以我们认为通过好的团队氛围、工作环境，搭配合适的、有竞争力的薪酬水平，是比较好的争取人才的方式。再说了我也没公开薪酬，上面薪资纯粹靠编。。。

- 靠10个要求项来判定一个人是否不合适

肯定不合适的。前面也说了，这10条只是一个水平标准线，是一个引导性的方向，是代表能达到相应技术水平层次的能力，包括而不限于这些项，我们也相信当你达到相应水平的时候也绝不会只会这几条。另外我们还有绩效考核，会对技术之外的更多维度进行评定。

电子版下载

关注下方微信公众号，回复“技术评级”可获取电子版资料。

Tide安全团队技术评级方案

级别	称谓	能力描述	能力要求	年限要求	薪资
T1	助理工程师	1）有相关专业教育背景或从业经验； 2）对公司职位的标准要求、政策、流程等从业所必需了解的知识处于学习成长阶段； 3）能协助完成渗透测试项目。	1、熟悉Web安全、移动端安全等网络安全相关知识，了解网络安全法律法规与行业标准； 2、熟悉国内外主流安全产品和工具，如：Nessus、Nmap、AWVS、Burp、Appscan等； 3、能较好的完成渗透测试方案制定、文档编写等； 4、能根据测试用例进行逐项测试； 5、有较强的学习能力和钻研精神； 6、熟悉各类操作系统及数据库常见的安全漏洞和隐患，熟悉owasp top10； 7、熟悉各类网络安全设备、系统，如防火墙、VPN、IPS、WAF、防火墙、网页防篡改系统等； 8、具备一定编程基础，了解或熟悉C/C++/Perl/Python/PHP/Go/Java等开发语言； 9、具备良好沟通能力和语言表达能力； 10、拥有自己的博客、Github、安全圈等；	0-1年	6k-8k
T2	初级工程师	1）有相关专业教育背景或从业经验； 2）在专业领域中，对于本岗位的任务和产出很了解，能独立完成常规渗透测试项目，能配合完成复杂任务； 3）具有一定漏洞挖掘能力、应急响应能力。	1、熟悉主流的Web安全技术，掌握Web安全常规漏洞原理及防范措施，包括SQL注入、XSS、XXE、RCE等安全风险； 2、能对测试用例进行逐项深入测试，对测试各忘录中的所有漏洞都了解并能进行测试； 3、至少熟悉一门编程语言C/C++/Perl/Python/PHP/Go/Java等，能够进行脚本、漏洞验证的poc编写或改写； 4、熟悉Linux和UNIX主流操作系统和主流数据库（SQL、MySql、ORACLE等）并具备渗透测试能力； 5、能熟练搭建靶机并进行漏洞复现，并有文章总结输出3篇以上； 6、在各大安全漏洞平台、企业SRC平台提交漏洞； 7、处理过木马、病毒、入侵、网络攻击等突发安全事件经验； 8、分析高危漏洞原理和利用技巧，撰写相关技术总结文档； 9、具备WEB/APP（Android）渗透测试、数据隐私检测、安全评估、安全加固、应急响应、安全护航等实施和交付能力； 10、对CTF比赛中的web题目有一定的研究经验，了解加解密优先。	0-1年	8k-10k
T3	中级工程师	1）在专业领域中，对公司职位的标准要求、政策、流程等从业所必需了解的知识基本了解，对于本岗位的任务和产出很了解，能独立完成复杂任务，能够发现并解决问题； 2）在中小型项目当中可以担任项目经理职责； 3）对逆向有一定了解，有自己擅长的安全领域。	1、熟练使用Perl/Python/PHP/Go/Java中的一种，能快速独立完成poc开发，如爬虫、破解类脚本； 2、对waf等各种防护措施的绕过有一定了解； 3、在知名安全媒体上发表5篇以上较受关注的文章； 4、具有一定的源码审计（php/asp/jsp/python）能力，发现过通用漏洞或发表过文章； 5、熟悉汇编、smali代码，具有一定逆向能力，能对病毒、木马、APP等进行分析； 6、具备一定内网渗透、域渗透能力，有成功案例； 7、熟悉windows、linux平台渗透测试、后门分析、加固；熟悉各类攻击技术，能针对各种攻击类型进行入侵分析和取证； 8、具有CTF比赛经验、网络攻防竞赛经验，熟悉CTF技巧并能拿到一定分值； 9、独立挖掘过通用漏洞，具有CNVD原创证书或cve证书； 10、在工控、物联网、云安全、人工智能、大数据安全等领域有一定研究并有成果。	1年及以上	10k-14k
T4	高级工程师	1）在专业领域，具备一定的前瞻性的了解，对公司关于此方面的技术或管理产生影响； 2）对于复杂问题的解决有自己的见解，对于问题的识别、优先级分配见解尤其有影响力，善于寻求资源解决问题； 3）在内网渗透、安全开发、逆向分析等方面有所研究	1、精通一种以上脚本语言，能独立完成中小型安全平台的开发或对接业务安全需求进行定制化开发； 2、对waf绕过等有较深入的研究，能自己编写waf规则，能绕过多种防护设备； 3、拥有NSATP、CCNP、HDCE、CISSP、CISA等证书之一； 4、具备较强内网渗透、域渗透能力，具有3个以上中型内网成功案例； 5、熟悉J2EE或php开发架构，熟悉主流web框架；具有JAVA/php开发经验或代码安全审计能力（白盒测试）并有成果输出； 6、每年在专栏或公众号发表文章5篇以上，论文/期刊1篇； 7、熟悉x86/x64系列汇编语言、c/c++语言，熟练使用IDA、Windbg、Ollydbg、Immunity Debugger等分析工具，熟悉静态分析、动态调试、代码跟踪方法，具备较强的逆向分析能力； 8、参加国内较高水平CTF比赛，取的较多分值协助团队取得较好名次，熟悉通用加密算法、逆向或pwn优先； 9、有独立提交3个以上高风险漏洞，如补天或SRC等，SRC累积资金一万以上； 10、具有cnvd原创证书或cve证书3个以上。	2年及以上	14k-20k
T5	研究员	1）在某一专业领域中，对于公司及业界的相关资源及水平比较了解； 2）开始参与部门相关策略的制定；对部门管理层的在某个领域的判断力产生影响； 3）是专业领域的知名人士。	1、熟悉逆向知识，具备多平台逆向经验(iOS/Android/Windows)，模拟器检测对抗研究等，能对病毒、木马进行深入分析； 2、熟悉浏览器、office、adobe以及flash等软件内部工作原理以及相应软件漏洞分析与利用技术； 3、对CTF比赛中的pwn、reverse题目有较深的研究经验；熟悉对称及非对称密码体系常见加解密算法；熟悉流量分析、数据隐写、取证等技术； 4、在阿里、蚂蚁金服、腾讯、360、百度等知名SRC排名前三； 5、每年在专栏或公众号发表文章10篇以上，论文/期刊累计3篇及以上； 6、能掌握一门或几门以下技术：PHP/Python/Shell/JavaScript/Ajax进行系统开发，至少精通一种数据库应用，如mysql、redis、mongodb等； 7、对业界前沿攻击和防御手法进行研究跟踪，能单独处置常见信息安全事件及热点事件跟踪，针对最新的安全漏洞及安全事件进行响应处理； 8、对内网渗透、APT攻防、黑灰产分析等有较深入研究并有成果输出，拥有反欺诈 / 反爬虫 / 业务风控 / 威胁情报分析能力； 9、对操作系统（win/mac/Win）、移动端、工控、物联网等方面之一的安全技术有较为深入的研究并有成果输出； 10、能精通一门语言的主流框架，如php的tp5、yii或python的flask、django，掌握框架的安全漏洞及利用。	3年及以上	20k-35k
T6	安全专家	1）是公司某一领域中的资深专家； 2）对公司某一专业方向的规划和未来走向产生影响； 3）对业务决策产生影响； 4）使命感驱动。	1、挖掘浏览器、Office、Adobe Reader、flash等客户端软件以及网络协议常见漏洞；熟悉操作系统的相关安全机制，掌握绕过漏洞缓解措施的基本方法； 2、在某领域出版过电子书籍或实体书，具有一定影响力； 3、熟悉常用算法和数据结构，精通C/C++/Java/Go/Python/Shell/Perl语言中的一种或多种，能够进行漏洞扫描器、网络爬虫架构设计与产品开发；能独立完成自动化安全扫描或者防御框架； 4、发表过有深度的技术Paper或独立挖掘过知名开源应用/大型厂商高危漏洞经历； 5、熟悉病毒木马，内核Rootkit的原理和行为，并对其做深入技术分析和逆向； 6、参加过geekpwn、xcon等大型安全会议的演讲； 7、精通防火墙、入侵防御、病毒防护、漏洞扫描、审计系统、身份认证等信息安全产品基础原理、安全部署，根据客户需求提供解决方案； 8、进行事件调查/追溯攻击者经历，IoC大规模处理经验，具备APT攻击和防御能力；具备从流量、日志、事件等数据中发现威胁的能力和威胁情报分析能力； 9、精通各类常见漏洞的原理、测试方法以及解决措施，具有分析研究安全漏洞的能力；且有丰富的攻击渗透实战经验、Fuzzing测试能力； 10、有大型CTF比赛（DEFCON、XCTF等）或国内顶级赛事获奖经历。	5年及以上	35k-50k
T7	首席安全官	1）业内知名，对国内/国际相关领域都较为了解； 2）对公司的发展做出重要贡献或业内有相当的成功记录； 3）所进行的研究成工作对公司有相当程度的影响； 4）使命感驱动；坚守信念；对组织和事业的忠诚。	1、参与国家地方或行业相关部门的信息安全标准制定； 2、主导过大中型网络、互联网应用等安全建设； 3、前沿安全攻防技术研究与利用，熟悉业界安全攻防动态，掌握国内外最新安全攻防技术； 4、对大数据、人工智能、物联网、工控安全、区块链等新兴技术具有较深研究，能够熟悉该行业最新攻击方法、渗透技术以及防御技术； 5、具备极为丰富的应急响应，事件调查经验，能利用技术进行事件调查/追溯攻击； 6、对安全体系的构建，安全架构的规划与设计、以及开发生命周期安全规范的落地具有丰富经验； 7、熟悉通用信息安全风险管理流程与框架，对国际国内信息安全标准如ISO27001，等级保护标准等有着较为深入的理解，并具有丰富的标准融合、体系落地及推广经验； 8、对代码虚拟化、反调试、反Hook等具备一定造诣，具备较强的逆向分析、攻防对抗、脱壳、反混淆相关能力； 9、对各类操作系统、应用系统的漏洞有较深理解，具有安全加固、渗透测试、应急响应等安全服务的实施经验； 10、拥有自己的研发专利、知识产权；出版过相关领域评价度较高的书籍。	8年及以上	50k-1000000k