长亭科技牧云安全研发工程师招聘

牧云是什么

牧云是长亭科技“攻防知查抓”安全防护体系中的重要一环，为主机安全方向，介绍信息可见 https://www.chaitin.cn/zh/cloudwalker。

下面是安全相关功能的一个粗略分类：

资产收集	风险感知	入侵检测
• 主机基本信息 • 软件应用、Web 框架等 • Web 站点 • docker 镜像、容器、网络等 • 启动项、内核模块、用户、端口、进程等 • ……	• 漏洞扫描 • 补丁管理 • 弱口令 • 合规基线 • 安全扫描 • ……	• 反弹 shell • Webshell • 命令审计 • 恶意文件 • 本地提权 • 网络异常 • 暴力破解 • ……

安全研发在牧云项目中的角色

牧云项目组的结构

- 产品经理、设计师、测试、前后端等常见的岗位。
- 系统研发工程师，主要是牧云探针研发，提供安全检测插件运行环境、调度、系统底层 api 封装整合等功能。
- 安全工程师（其他的招聘网站上有时候也称为安全策略工程师）
    - 偏安全研究方向，专注几个小方向，提供检测思路，可能写代码较少。
    - 偏安全研发方向，也就是我所在团队，目前五六个人，为小型化的团队。这是本招聘的重点所在。

安全研发在做什么

目前的招聘方向偏研发，你能熟悉安全就更好了，两个方向都有合适的事情去做。

如果你偏向做安全

安全研究方向的同学也只是覆盖一部分的主机安全场景，比如 Webshell 检测、Windows 安全相关等等， 上面模块划分的表格中剩下的绝大多数功能还是安全研发方向的同学在做，所以可以理解安全研发会更偏向写代码一些，但是并不是完全不去思考检测思路。

做过的事情举例如下：

1. 很多文档方案中，检测反弹 shell 都是基于命令行特征和简单网络关系的粗糙处理，漏报会多一些，而我们将这些思路进行了非常精细化的处理，补充了一些新姿势，目前效果挺不错的。
2. 从集成第三方杀软到自己编写很多 yara 规则到基于 `api` 调用关系的恶意文件检测，而且能进行打标和给出详细说明。我们专注于黑客软件和 exploit 的检测，这是对企业安全最大的威胁之一。
3. 命令审计，简单理解就是对命令行信息的匹配，比如 ssh 后门 `ln -sf /usr/sbin/sshd /tmp/su; /tmp/su -oport=12345`，堆规则大家都会，如何让这个插件性能和效果更好呢？我们设计开发了自定义表达式规则、基于 bash session 关系的黑客操作习惯检测、命令行中 ip、域名等威胁情报检测、反弹 shell 记录全量命令等等功能。
4. 弱口令识别不是对服务直接进行暴力破解，而是基于数据文件分析得到哈希值进行爆破的，比如 Linux 用户密码在 `/etc/shadow` 文件中存储，获取哈希比较简单，但是对于数据库类型（比如 MySQL+多种存储引擎、Oracle、PostgreSQL 等），如何分析一个用户表数据文件得到哈希就需要对存储引擎进行深入的理解和研究了，我们都已经基本搞定了。
5. 用户配置的密码字典可能比较小，需要按照攻击者的思维进行自动化的信息收集来生成一个新的字典供用户参考。

如果你偏向研发，不怎么懂安全

这个也没有关系，我们也维护多个安全检测服务，偏向后端方向，而且我们认为转安全方向也并不难。

做过的事情举例如下：

1. 同步 nvd、cnnvd 等漏洞情报数据、应用资产描述、oval 漏洞匹配规则、一些自行维护的漏洞匹配规则、系统补丁信息，将这些数据进行整合和编辑，输出为数据库，支撑漏洞匹配、漏洞情报、补丁管理、补丁情报等功能。
2. 上述的漏洞和补丁相关功能为一个单独的服务，基于数据和规则文件进行扫描和匹配，和后端使用 rpc 通信，服务可以热更新。

3. 恶意文件检测也是一个单独的服务，需要管理文件的分发规则，封装第三方杀软、自研引擎的接口，统一多种接入方式（因为这是一个通用项目，可能对接多种队列、数据上报 rpc 等），管理检测缓存，提供类似 VirusTotal 一样的内部扫描界面，管理引擎更新，引擎监控等。
4. 弱口令识别中，需要类似彩虹表一样去缓存哈希运算的结果，但是又不能无限制的存储，需要去压缩和淘汰低频访问数据。
5. 检测插件是 Lua 写的，但是这种语言对大型项目非常不友好，我们参考了已有的一些开源项目，最终选择了一种带类型的 Lua 方言，但是开源项目并不完全满足需求，我们又对其进行了修改和增加了一些配套工具，比如构建工具、lint 工具等。

其他要求

- 计算机基础扎实，熟悉常见编程语言。
- 做事认真，有创新能力，思维活跃。
- 工作中不要被推着往前走，能积极的贡献自己的想法，推动想法去实现和落地。

工作环境 / 薪资待遇

- 没有比较紧急的事情不会要求加班，2020 年周末加班次数小于五次。
- base 北京 / 杭州，优先北京。
- 工作时间大概为 10:00 - 19:00，保证总工作时间的基础上，可以浮动。
- 薪资待遇与多种因素相关，比如面试结果、评估的职级等，但是可以保证的是，不会低于对应职级在互联网公司中的常见薪资。如果你是大佬，什么都可以谈。

投递简历

可以将简历发送到 `virusdefender@outlook.com` 或者 `yang.li@chaitin.com` 。

也可以加我的微信 ID `virusdefender`
来聊一聊其他感兴趣的问题，二维码见右图。

不局限于安全研发，对长亭的所有研发岗位感兴趣也可以通过上述渠道联系，会帮你初筛简历和内推。