

honeypot

360网络安全研究院杭州开点招聘



Genshen Ye

Sep 8, 2020 • 6 min read

团队简介

360网络安全研究院（360Netlab）于2014年成立。不同于传统网络安全主要基于规则，数据分析是团队的主要方向。团队持续专注于DNS和僵尸网络领域，并在领域内保持领先地位。

从2014年开始，团队在DNS方向上建设了国内历史最久、覆盖范围最广的PassiveDNS基础数据库，及其附属其它基础数据库，持续分析产出威胁情报并应用于360网络安全大脑，并在多个DNS领域内的技术会议上做公开报告。在僵尸网络领域内，团队多年来持续致力于发现跟踪僵尸网络活动，披露了包括Mirai、Satori在内的若干重大安全威胁，并因为其中针对Mirai僵尸网络的持续分析工作得到美国FBI、美国司法部的致谢。

360网络安全研究院计划在杭州新成立一个产品团队，把我们的安全数据和技术产品化，探索网络安全行业未知威胁检测难题，为360安全大脑添砖加瓦。

从一次平凡的网络扫描，到漏洞、样本、安全事件分析，再到0-day漏洞检测、未知恶意软件检测、高级威胁追踪，我们致力于通过数据驱动安全，构建网络安全看得见的能力。

更多信息：<https://netlab.360.com>

简历投递

yegenshen@360.cn

工作地点

杭州（文一西路998号海创园）





招聘岗位：前端开发工程师（实习生走校招内推流程）

职责说明

- 参与数据可视化系统WEB端的开发

岗位要求

- 精通 JavaScript/CSS/HTML
- 熟悉 React/Vue/Angular 任一前端框架
- 了解 Webpack/Gulp 等前端打包发布工具
- 熟悉 Python，且熟悉 Flask/Tornado 任一服务端框架
- 了解基本的Linux命令
- 有基本的美学判断能力和设计能力
- 良好的团队合作能力

加分项

- 熟悉 Typescript
- 熟悉数据可视化，及D3/Vega/G2 任一可视化框架

招聘岗位：后端开发工程师（实习生走校招内推流程）

职责说明

- 参与蜜罐产品化工作

岗位要求

- 计算机相关专业本科及以上学历，精通Java、C/C++或Python，3年以上开发经验，熟悉常用数据结构和算法，具有良好的编程和工程实现能力
- 学习能力强，有良好的较好的创新能力和逻辑思维能力，善于主动思考，对技术有强烈激情
- 有良好的沟通能力，跨团队协作能力，具备出色的计划和执行力，强烈的责任感
- 熟悉一种以上海量数据处理平台/框架，如ClickHouse、Hadoop、Storm、Spark、HBase，Elasticsearch等开源系统者优先
- 有网络安全大数据处理方面经验者优先

招聘岗位：安全研发工程师（实习生走校招内推流程）

职责说明

- 负责蜜罐、沙箱产品研发

岗位要求

- 计算机相关专业本科及以上学历，精通Java、C、C++或Python，3年以上开发经验，熟悉常用数据结构和算法，具有良好的编程和工程实现能力
- 学习能力强，有良好的较好的创新能力和逻辑思维能力，善于主动思考，对技术有强烈激情
- 有良好的沟通能力，跨团队协作能力，具备出色的计划和执行力，强烈的责任感
- 有过开源蜜罐或沙箱项目研发经验者优先

招聘岗位：产品经理

职责说明

- 主导360Netlab安全数据产品化工作，参与安全分析系统设计工作
- 把控安全项目进度，紧跟客户和市场需求

岗位要求

- 3年以上互联网产品工作经验，对网络安全数据有产品经验者优先考虑
- 负责产品需求沟通、需求分析、需求设计、原型设计、交互设计等
- 负责项目团队的进度把控、产品迭代质量、交付版本验收，对结果负责
- 有较强的学习能力，为实现产品期望而砥砺前行
- 良好的沟通能力和团队合作精神，有一定的组织协调能力和决策能力
- 敏锐的洞察力和超强的分析与解决复杂问题的能力

招聘岗位：安全工程师（实习生走校招内推流程）

职责说明

- 负责高级恶意软件威胁分析，并撰写分析报告
- 从常规的网络安全数据和恶意样本提炼特征，为安全系统提升检测能力
- 热爱研究网络空间中不断出现的攻防对抗技术

岗位要求

- 热爱网络安全工作，具有安全漏洞/恶意代码分析和检测经验者优先考虑
- 熟悉x86/ARM/MIPS汇编指令，精通ELF/PE文件逆向分析
- 掌握C/C++、Python、Go等一门或者多门语言，具备开发自动化分析程序能力
- 熟悉网络攻防技术和常见攻击手法，能快速识别常见的网络攻击
- 善于主动思考，具备独立分析和解决问题的能力
- 有较强的学习能力，具备良好的团队合作精神和沟通能力

招聘岗位：算法工程师（实习生走校招内推流程）

职责说明

- 深度理解360Netlab网络安全数据，应用机器学习算法，为安全系统提升检测能力
- 在工作中能够主动发现各种策略的问题并提出优化方案，并推进优化方案落实

岗位要求

- 热爱数据分析工作，对网络安全数据（恶意代码、恶意流量、恶意软件行为）有分析经验者优先考虑
- 熟悉一种或多种常用机器学习模型，具有相关项目经验
- 熟悉一种或多种常见的机器学习/深度学习工具，有实际使用经验
- 掌握C/C++、Python、Go等一门或者多门语言，具备开发自动化分析程序能力
- 善于主动思考，具备独立分析和解决问题的能力
- 有较强的学习能力，具备良好的团队合作精神和沟通能力

薪酬范围

上述JD级别不限，薪酬范围20~45K，如果感兴趣，欢迎联系：yegenshen@360.cn



Start the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name



Share

Best Newest Oldest

Be the first to comment.

Subscribe

Privacy

Do Not Sell My Data

— 360 Netlab Blog - Network Security Research Lab at 360 —
honeypot



Spring4Shell在野漏洞传播分析

What Our Honeypot Sees Just One Day After The Spring4Shell Advisory

Day 10: where we are with log4j from honeypot's perspective

IoT

幽灵在行动： Specter分析报告

背景 2020年8月20日，360Netlab未知威胁检测系统捕获了一个通过漏洞传播可疑ELF文件(22523419f0404d628d02876e69458fbe.css)，其独特的文件名，TLS网络流量以及VT杀软0检出的情况，引起了我们的兴趣。经过分析，我们确定它是一个配置灵活，高度模块化/插件化，使用TLS，ChaCha20，Lz4加密压缩网...

QNAP

In the wild QNAP NAS attacks

Author:Yanlong Ma, Genshen Ye, Ye Jin From April 21, 2020, 360Netlab Anglerfish honeypot started to see a new QNAP NAS vulnerability being used to launch attack against QNAP NAS equipment. We noticed that this vulnerability has not been announced on the Internet, and the attacker is cautious in the

See all 49 posts →



Sep 25,

2020

11 min

read



Aug 31,

2020

4 min

