朱柯余

个人介绍

性别：女	**出生日期：2000年**
联系方式：15600178595	求职意向：安全开发工程师
邮箱：kyre0@outlook.com	工作经验：4年
博客: Kyre0ee.github.io	教育: 西安财经大学
专业：软件工程	毕业时间：2020.07

技能与专长

- 熟悉常见的web、主机等方面的相关漏洞，并了解其原理和防御措施;
- 熟悉基础网络知识;
- 熟悉各类安全产品维护、规则调优;
- 对常见Web安全漏洞的原理、危害、利用方式及修复方案有较深入理解;
- 熟练掌握MSF、CS等工具的使用

工作经历

- 奇安信科技集团，2019-07 - 至今
- 职位：安全开发工程师
- 工作内容：
  - 负责安全产品（WAF、IDS、IPS、防火墙等）的运维和优化
  - 及时处理安全事件及告警，进行合理的应急处理
  - 参与WAF和DNS检测系统架构设计与优化
  - 设计和优化Webshell检测模块

项目经验

- IPS、IDS送测入围项目,2020-2023
  - 项目描述
    - 该项目旨在评估和测试IPS、IDS确保其在实际环境中的有效性和可靠性。针对不同攻击场景进行测试评估对各种网络攻击的检测能力和响应速度。预期结

果包括发现和修复潜在的系统漏洞和性能瓶颈，并为客户提供定制的安全解决方案，从而提高其网络安全水平和抵御能力。

    - 角色与贡献
        - 负责确保控制规则的检出率和误报率满足项目要求
        - 制定及优化IPS规则
        - 与引擎开发团队合作，改进后台检测逻辑
- 冬奥、重保、HW、nox应急响应,2020-至今
    - 项目描述
        - 通过制定详细的应急响应计划以及持续监测和分析，及时发现并应对各类安全威胁，确保网络的安全稳定运行。
    - 角色与贡献
        - 负责漏洞分析以及规则维护优化。
        - 应急响应及时分析漏洞。
        - 提升安全检测能力。
- WAF防火墙产品开发,2022-至今
    - 项目描述
        - 实时监测和拦截针对Web应用的各类攻击，包括SQL注入、跨站脚本等常见漏洞攻击，保障Web应用的安全性和可用性。
    - 角色与贡献
        - 设计WAF产品检测逻辑及规则语法。
        - 增加Webshell的防御检测规则，并负责规则优化。
        - 提升Web防火墙的安全能力。
- DNS流量检测产品，2023-至今
    - 项目描述
        - 实时监测和分析DNS请求，识别恶意域名、异常行为和潜在威胁，提升网络安全防御能力。
    - 角色与贡献
        - 负责样本分析和收集，深入研究DNS流量检测技术。
        - 调研分析DNS隧道样本，并提出检测思路。
- Botnet样本逆向分析，2023-至今
    - 项目描述
        - 通过对Botnet样本的逆向分析，识别其通信协议、C&C结构和恶意功能，为防御和应对Botnet攻击提供关键信息。
    - 角色与贡献
        - 逆向分析botnet/malware样本，提出检测思路。
        - 分析常见家族的流量特征。
        - 开发自动化工具，实现对已知C2连接流量的实时分析。
- IPS、IDS安全能力运维，2019-2023
    - 项目描述

        - 通过持续的安全运维工作，有效提升IPS和IDS系统的安全防御能力，以严谨的安全运维流程和规范，确保安全规则及时更新。
    - 角色与贡献
        - 负责规则开发与实现
        - 优化系统性能
        - 协助团队进行项目进度控制和质量保证

自我评价

- 对安全技术有浓厚兴趣和持续学习动力
- 具备良好的问题分析与解决能力
