安全大厂招聘技术栈

2020年6月3日 21:18

奇安信

- 熟练使用各种渗透测试工具（Burpsuite、Sqlmap、AWVS、Nmap、MSF、Cobalt Strike、Empire等）
- 掌握常见的攻防技术,对相关漏洞（web或二进制）的原理有深入的理解
- 熟悉常见Windows,Linux运维技术
- 熟悉操作系统原理，熟悉反汇编，逆向分析能力较强；
- 熟悉Fuzzing技术及常见漏洞挖掘工具；
- 挖掘过系统软件、网络设备等漏洞者（有cve编号）优先。
- 熟悉常见Windows&linux、Web应用和数据库各种攻击手段;
- 悉常见Web高危漏洞（SQL注入、XSS、CSRF、WebShell等）原理及实践,在各漏洞提交平台实际提交过高风险漏洞优先;
- 熟悉常见脚本语言,能够进行WEB渗透测试,恶意代码检测和行为分析;
- 熟悉病毒木马常用技术手段；
- 熟悉W32汇编语言，熟练使用OD，IDA等调试器（有逆向经验者优先）；
- 熟悉Windows操作系统原理和相关的熟悉
- PE结构，了解文件加载运行机制； 安全机制；
- 熟悉Cisco、华为、华三网络设备的配置和使用；
- 有至少CCNP同等级别或以上的网络知识；
- 具备大中型网络安全设计的能力，掌握常见网络安全防护手段，以及常见的安全攻击手法；
- 熟悉Windows或Linux常见系统机制与原理
- 熟练使用汇编语言、至少熟练使用C、C++、python、perl中的一种编写poc或辅助分析工具

- 对最新的 Web 类漏洞进行及时的研判、分析、复现、PoC/Exp 与技术文章编写

华为：

- 熟悉Linux/Android平台逆向技术，并能熟练使用IDA、JEB、GDB等调试逆向具，熟悉反调试、混淆、加壳等安全防护手段，熟悉DEP、ASLR、StackGuard、SeLinux、PXN等安全防御技术原理
- 熟练使用fuzzing工具，如AFL、syzkaller、libfuzz、trinity等。
- 熟悉ARMv7/ARMv8架构和TrustZone技术，熟悉ARM汇编。
- 精通Linux Kernel机制者优先。
- 有面向客户的安全解决方案设计、落地经验，有物联网、大数据安全、云安全等领域经验;
- 熟悉机器视觉产品安全攻防技术，精通主流安全漏洞原理，熟悉业界安全攻防动态；
- 熟悉软件及硬件的攻击和防御方案，能够进行软硬件结合的安全解决方案设计；
- 对网络功能进行分析、抽象，包括网络功能模型，各部件的功能要求，接口设计。通过网络功能和接口的设计，从而实现更高服务质量、更可靠、更安全，更加适合实现自动化的管理和维护
- 精通密码学与对称加密算法：3DES,IDEA,AES等
- 精通PKI及密码学应用：公钥与私钥、SHA、MD2、数字签名等
- 扎实的密码学基础，熟悉常用对称/非对称加密、哈希算法，基于密码的加密、认证、签名技术和产品； 掌握一种或多种高级密码学技术，如差分隐私、安全多方计算、隐私集合求交、全同态加密、保序加密、保留格式加密，具备工程落地能力；
- 具有海量数据的安全处理经验，熟悉网络安全、应用安全相关规范、技术、产品及方案，熟悉当前各种主流的网络、防火墙、UTM、VPN、加解密、身份管理 、认证授权和安全管理等安全技术及产品
- 拥有CISSP、CISA、ISO27001、ISO22301、IAPP等相关安全资质的优先；

- 对网络安全知识有较为全面的了解和认知，熟悉安全合规要求，精通至少1到2项国内外的产品安全认证，或者主流的云安全认证；
- 有较为丰富的安全设计经验，熟悉主流的加密算法以及算法应用，了解网络安全协议
- 主导过产品FIPS认证，有密码算法开发或者测试经验者优先
- 精通安全设计原则、典型攻击和防护原理，有成功产品安全架构设计经验
- 熟悉云安全、内核安全、主机安全、芯片/硬件安全等安全技术。
- 熟悉IoT、AI等解决方案安全技术。
- 有边缘计算产品安全架构设计和开发经验者优先。
- 网络基础扎实，熟悉TCP/IP协议，二层转发和三层路由的原理，及常用的应用层协议；
- 熟悉公司一个以上领域产品的技术或业务（华为云、终端云、电商、数据通信、网络安全产品、各类软件平台等）优先；
- 具备大型软件平台的架构设计和开发经验，熟练掌握云化、弹性、多租户的软件架构技术精通微服务架构的设计原则、约束、治理的技术和方法。
- .对行业安全管理和身份治理具有丰富经验，熟悉应用安全、数据安全、Web安全等安全治理，熟SAML、OAuth2、OpenID、CAS等认证技术；
- 熟悉常见安全防护设备（WAF、IPS、IDS等）的原理和安全方案；熟悉国内外网络安全标准（BSIMM、OWASP等）和认证（如CC认证、FIPS认证等）；
- 服务器系统（Wi各种入侵检测系统（漏扫/防护墙/WAF/抗DDos/RASP/病毒防护/舆情监测等）原理及使用，有开发和设计安全防护系统经验优先；ndows/Linux/Unix）及数据库（mysql/oracle）安全策略加固
- 攻击溯源、安全（日志）审计、风险评估流程；
- 蜜罐技术，有实际搭建及使用经验；
- 负责华为IT产品线存储服务器、安防摄像头、MDC、服务器系统、数据库和硬件的安全加固、安全评估、安全检测、响应取证溯源，发现IT产品线产品面临的安全漏洞、安全风险、安全防护短板，促进产品整体安全防护水平及产品线产品安全能力的提升
- 熟练掌握安全测试工具，抓包工具，如CodeDeX / Burpsuite / Appscan / Nesssus / Nmap / Wireshark/ fiddler等，可独立面向解决方案开展安全漏洞挖掘与测试；
- 掌握Linux/Android系统知识和安全机制，熟悉DEP、ASLR、StackGuard、SeLinux、PXN等安全防御技术原理；
- 熟悉ARMv7/ARMv8架构和TrustZone技术，熟悉ARM汇编，具备汇编编写程序和反汇编能力。

- 负责AOSP/HOSP框架、HMS、MAPLE、工具链（方舟编译器）、关键应用（如浏览器）等核心部件的攻防技术规划和安全研究，对相关核心部件的安全竞争力和安全表现负责；
- 病毒样本分析；
- 熟悉Verilog编程语言，并了解C语言
- 熟悉ASIC、FPGA芯片的端到端开发流程，并掌握相关的EDA工具。
- 熟悉ARM、X86、PowerPC等一种或以上处理器体系架构与工作原理;
- 熟悉车载产品/电机的EMC/防护/安全/认证/可靠性/NVH端到端交付流程及要求，具有持续优化流程的能力。
- 具备如下任一领域的经验或实践：硬件、芯片、操作系统、数据库、Web领域安全技术；密码学、CA、身份认证技术；云安全、可信计算、安全认证；形式规约、形式验证等；
- 有智能边缘产品安全架构设计和开发经验者优先
- 熟悉数通IP通用知识和运营商、企业网典型解决方案；
- 熟悉业界开源漏洞解决和管理流程、网络安全技术；
- 了解隐私保护相关法规和技术；
- 掌握ASTRIDE等安全设计方法，熟悉安全质量活动，守护版本基础安全设计质量；
- 深度了解KVM/Docker架构与核心原理。
- 深度了解KVM/Docker的安全机制，熟悉KVM/Docker曾爆出严重漏洞及修复方法
- 具备网络安全产品安全渗透测试经验，熟悉Struts，Spring等框架，能够独立完成常见web漏洞的攻击利用，熟悉云安全、IoT安全者优先。
- 三年以上安全从业经验，了解国内外及各行业信息安全相关政策与标准（如等级保护、ISO27001、CSA-CCM、SOX、GDPR等），有安全风险评估、安全管理体系咨询、大型组织信息安全规划经验。
- 熟悉网络及系统技术，能根据不同网络环境，对信息安全项目进行规划和设计；熟练掌握云计算知识，具备OpenStack，KVM，vmware相关经验
- 熟悉网络安全、主机安全、应用安全、数据安全等技术，熟悉PKI、加解密原理、防火墙、VPN、SOC、入侵检测系统、终端安全系统、安全审计系统、身份认证、负载均衡、网闸等信息安全产品基础原理和应用部署方案
- 熟悉微服务架构设计模式和实践、微服务2.0技术栈；

- 具备一定的应用密码学实践经验，熟练掌握密码算法的使用及openssl等开源库、SSL等安全协议、熟悉PKI体系、CA系统、密钥管理、可信计算、安全启动、随机数熵池等，熟悉应用密码技术在区块链技术中的应用；

深信服：

- 熟悉主流的安全产品如防火墙/WAF/AC/堡垒机/CASB/SOC等；
- 具备实际信息安全方案规划和实施经验，如DLP、防病毒、网络安全边界和访问控制
- 熟悉安全日志数据分析（IPS日志、EDR日志等），掌握 python/shell/perl 等至少一门脚本语言；
- 具备渗透测试实战经验，熟悉常见web漏洞/系统漏洞/业务逻辑漏洞利用方法，如：sql注入、webshell上传、越权漏洞、远程命令执行漏洞等；长期跟踪业界新爆发的漏洞，如：struts2系列漏洞、java反序列化漏洞等；
- 有虚拟补丁开发经验者优先
- 熟悉Windows驱动开发、应用程序开发
- 熟悉病毒、木马的原理，熟悉恶意文件的逆向分析优先
- 有病毒处置经验者优先
- 熟悉国内外信息安全标准，如GBT20984、等级保护、ISO27001；
- 了解OWASP Top 10，熟练国内外各大漏洞库，熟练渗透与反渗透（取证、溯源等），有强烈的安全洞察能力，有逆向能力者优先；
- 能熟练使用Kail、BT5、Metsploit等集成环境和自动化渗透测试工具；
- 熟悉物联网相关接口协议，如MQTT和CoAP
- 制定并维护SIEM基础架构的战略规划、路线图和设计流程
- 基于当前的威胁、漏洞、协议、工作任务或其他客户环境中的特点，制定并实施监测系统的初始检测内容（IDS特征，SIEM应用场景等），并响应安全威胁情报负责人提供的输入
- 定期评估SOC的有效性，以及从中获取的经验。
- 深入了解SIEM工具（规则创建、关联等）

- 熟悉ELK、Flink、Kafka等大数据相关开源组件，具有相关使用经验的人士优先。
- 了解安全趋势，包括：机会主义威胁攻击者、有组织的网络犯罪团体以及国家层面的攻击者所用的攻击策略、流程及技术；
- 了解数据分析流程及工具，了解威胁数据的传输及存储架构（例如， OpenIOC, CybOX, CRITS, Threat Connect等）；
- 了解常见的挖矿病毒、勒索病毒、后门病毒的等场景的惯用手法；
- 熟悉Windows内核原理，研究过WRK或者ReactOS；
- 熟悉常用Hook技术，系统各种回调机制；
- 熟悉各种DLL注入技术原理；
- 熟悉文件过滤驱动框架，sfilter或者MiniFilter，两者熟悉一种即可，开发过文件过滤驱动
- 熟悉网络过滤驱动框架，TDI或者WFP，两者熟悉一种即可，开发过网络过滤驱动优先考虑；
- 负责病毒IOC特征提取；
- 负责病毒行为分析，提取病毒扩散传播使用的攻击技术。
- 有流行病毒分析经验，熟悉加解密、脱壳、常见可执行文件格式，并且熟悉如脚本类、宏病毒类的病毒分析；
- 熟悉恶意软件分析、木马/rootkit分析、僵尸网络、安全事件调查等相关专业知识，可以对安全事件进行应急及溯源分析

同盾科技：

- 追踪互联网黑产攻击、分析攻击手法、攻击目标、攻击工具、上下游产业链等；
- 熟练使用原型工具Axure、使用Visio 、Xmind或其他工具制作流程图
- 熟悉常用建模方法及模型评估指标，如LR / GBDT / XGboost等，有信用风险全流程建模经验优先
- 移动安全，设备指纹，二进制，虚拟机，加固，前端安全，加解密，js

- 精通 IOS调试工具和方法，可以应付各种IOS复杂问题
- 精通IOS框架及原理