网络安全创新大会
Cyber Security Innovation Summit

新形势下金融行业的安全能力演进-数据化和服务化

姓名　谢文博 阳光信保 信息安全负责人

自我介绍

- ✓ 自身的经历：从研发，攻防实验室，业务安全，数据安全，安全架构和开发一路走来，也是一种非常有意思的体验
- ✓ 技术方向：安全架构/开发，实时计算框架/数据处理

目录

挑战无处不在——工作职责

网络安全创新大会
Cyber Security Innovation Summit

基础安全岗

- 安全设备日常运维巡检
- 渗透测试
- 漏洞扫描
- 生产环境安全风险评估
- 桌面终端安全运维
- 系统上线前安全测试
- 安全漏洞告警修复跟踪
- 公司人员/外包入场离场审核
- VPN账户等多个账号访问权限审批

应用安全岗

- 安全需求评审
- 安全架构设计
- 代码审计
- 新旧基础组件评估
- 纵深防御体系设计
- 反羊毛党/恶意用户/恶意设备
- 安全开发/原型设计
- 数据/应用灾备方案评审

安全管理合规岗

- 等级保护、ISO27001相关测评工作
- 监管部门信息上报
- 每季度自查自纠相关工作表
- 相关法案草案标准的跟踪解读
- 人行征信相关安全检查工作
- 客户隐私保护
- 课题研究和撰写
- 应急演练组织及审核
- 灾备建设审核

安全开发岗

- 需求分析
- 架构设计
- 产品开发
- 测试上线
- 新技术的预研
- 业务需求沟通

数据安全岗

- 数据安全分级
- 数据安全提取
- 数据库账户权限审批
- 数据安全合规评价标准框架
- 持续开展数据安全评估
- 优化数据安全管理体系
- 数据脱敏方案流程制定
- 相关合作协议涉及审核（涉及客户数据授权等）
- 数据测试方案的制定
- 数据仓库/镜像库的创建访问安全审批

挑战无处不在

网络安全创新大会
Cyber Security Innovation Summit

海量数据

终端安全

层出不尽的新技术

安全运维

合规要求

永远不够的资源

数据/日志标准化

高频的发版

复杂的业务

数据安全

沟通交流

SDLC-C落地

新的攻击手法

如何应对

层出不尽的新技术

- 不断的学习
- 了解技术的发展和演进
- 合理引入新技术，将其工程化

永远不够的资源

- 安全能力自动化，平台， 数据化
- 交流沟通
- 安全能力的下沉和前置
- 数据能力提升

复杂的业务

- 贴近业务
- 了解产品
- 了解行业
- 轮岗

合规要求

SDLC-C 落地

安全能力的下沉和前置

数据安全/客户隐私保护

- 法规规范的解读
- 行业特性和规范的了解
- 业务系统与数据的关系
- 数据安全分类分级
- 数据安全评估
- 数据安全管理体系
- 数据生命周期

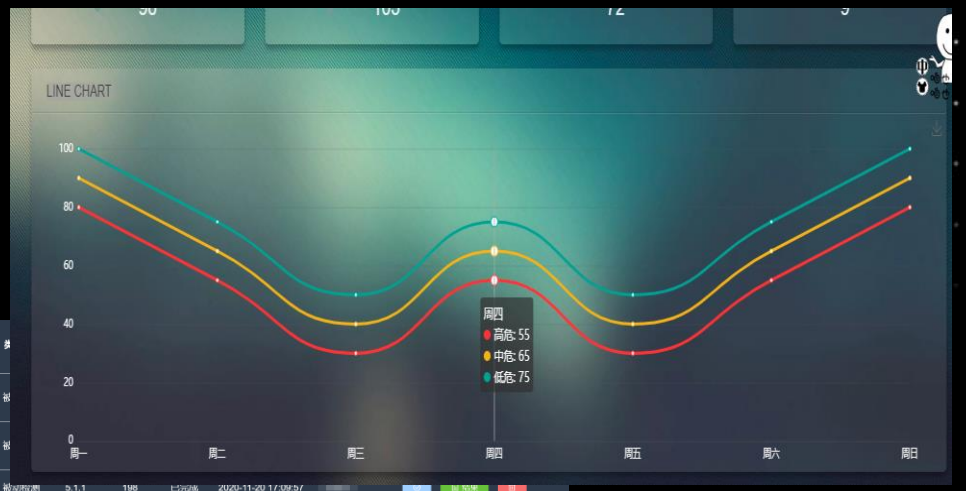
终端安全

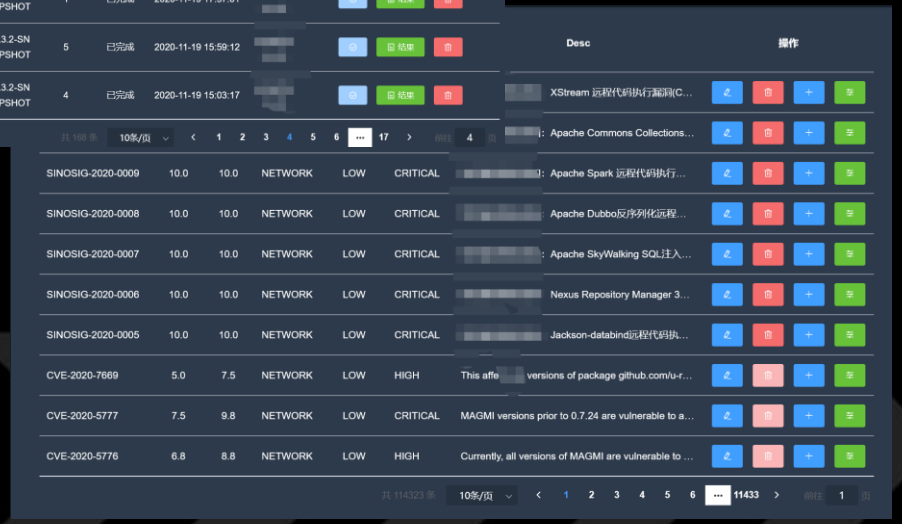
安全网关平台

- 多云环境下系统的区域隔离，访问控制，降低业务系统风险；
- 通过黑白灰关名单键词路径等（全局/局部），灵活限制用户或系统对业务系统的访问；
- 通过不同的策略组合实现对业务系统的快速止损，并对系统实现限流/降级/熔断等功能；
- HTTP/TCP/UDP 流量的任意复制放大转发；
- 业务系统参数可视化配置，支持集群模式业务分组；
- 后期与Kubernates Ingress-nginx 整合；
- 与数据平台的整合；

安全威胁发现平台——组件检测

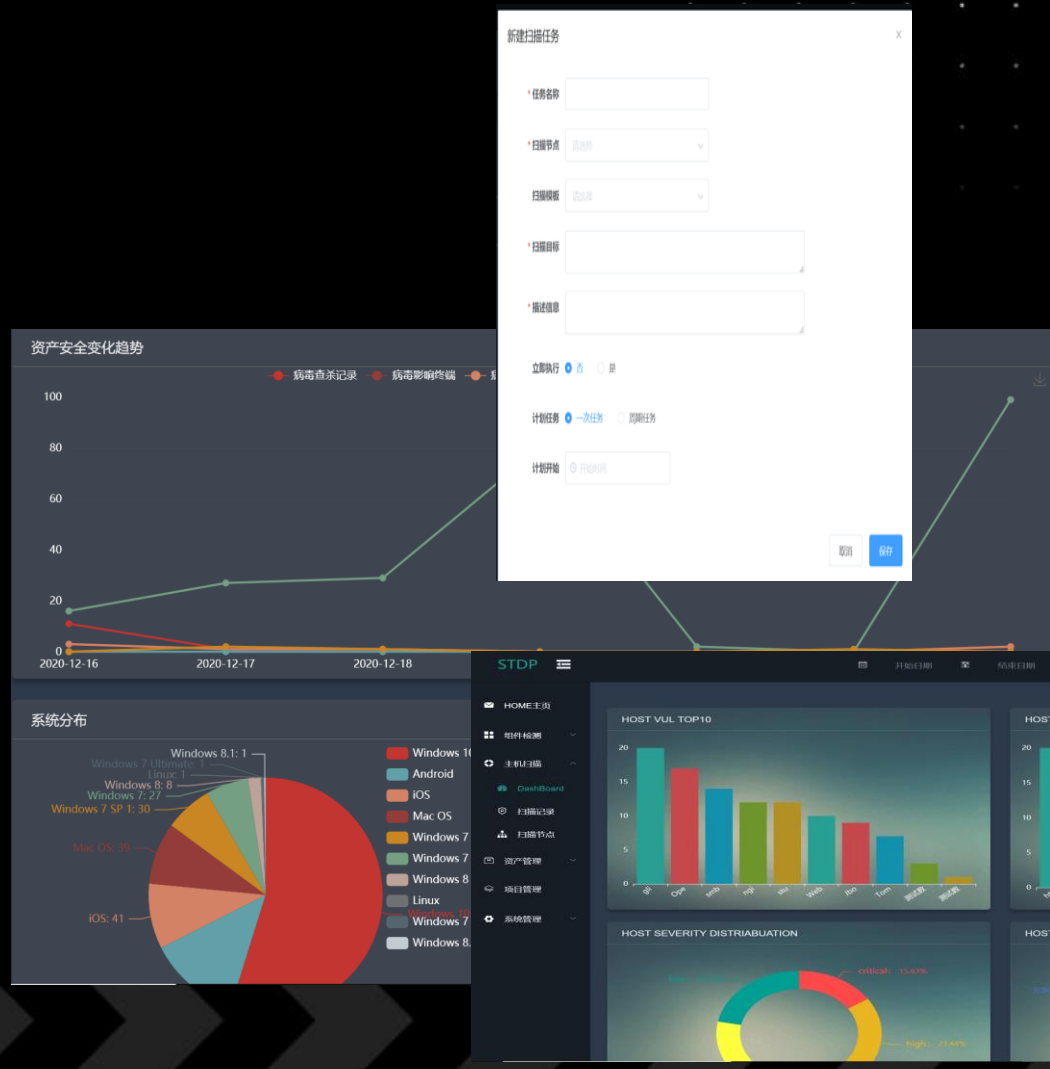
- 直观明确的 DASHBOARD；
- 快速检测项目中各类组件漏洞，漏洞追踪定位到项目/个人；
- 可灵活配置的私有组件漏洞库；
- 与CI/CD的整合；
- 后期与Findbugs/PMD 的整合；





安全威胁发现平台——主机/终端风险检测

- 外部安全扫描系统的灵活接入管理；
- 主机内部风险识别和控制；
- 各类系统资产信息识别；
- 结合数据平台各类威胁事件的降噪；
- 各类系统资产信息识别；
- 终端资产的迅速隔离止损；
- 软件正版化管理；
- 终端漏洞风险评估管理；
- 恶意入侵识别与防御；
- 高风险地址访问识别监控；
- 内部用户威胁行为识别发现；



未来

- ✓ 动态安全网关；
- ✓ 数据能力前置；
- ✓ 安全能力更加自动化；
- ✓ 应用弹性部署和自动调度；
- ✓ 风险自动治愈；
- ✓ 更多新技术工程化引入自研项目；

- ✓ 传统岗位新挑战：信息安全之路

https://www.freebuf.com/articles/network/232341.html

网络安全创新大会
Cyber Security Innovation Summit

THANKS