

基于社区的持续风险管理平台实践

乌云 · 章华鹏 · boooooom

从Spring Boot的0day漏洞说起

Spring Boot

Spring 是Java的三大框架之一，广泛应用与Java Web 的网站开发， Spring Boot是Spring的一个核心子项目。目前国内各大互联网公司都在使用的一个新的微框架。



每一个企业都很关心的问题

-  企业是否遭受这个漏洞的影响？
-  如何定位我们在互联网上的业务是否使用了这项技术？
-  我们使用该技术的业务是否遭受该漏洞的影响？
-  这会造成什么样的风险？如何修复？
-  未来如何应对可能再次出现的安全风险？



企业业务系统是否使用了这项技术？



全网业务系统梳理



应用系统指纹识别



使用该技术的业务系统是否遭受影响？



基于指纹识别结果的风险检测



这会造成什么样的风险？如何修复？



进行风险演示



详细的修复方案



未来如何应对再次出现的安全风险？



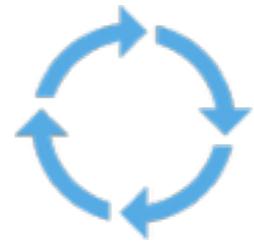
全面资产识别



深度风险管理



快速风险修复



持续风险管理

解决问题的秘诀=优秀的方案+高效的实现

基于社区的持续风险管理平台实践



全面资产识别



子域名遍历



DNS数据



DNS域传送漏洞



爬虫抓取



域名



IP



应用



服务



安全是一个整体



来自社区贡献的指纹识别策略



深度风险检测

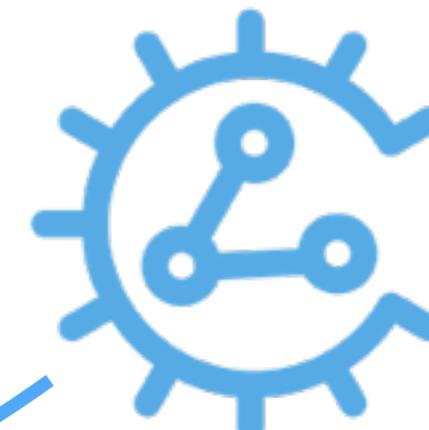
- ☑ 自研应用程序风险检测「SQL注入/XSS/命令执行等」
- ☑ 第三方应用程序漏洞 「WP/OA/Discuz/Struts2等」
- ☑ 网站内容安全风险 「挂马/博彩/恶意内容/黑链等」
- ☑ 基础服务漏洞 「服务配置错误/通用漏洞等」
- ☑ 员工安全意识风险 「Github代码泄露/弱口令等」



深度风险检测



指纹&插件



平台引擎



命中分红



监测报表



企业

社区两万白帽子
二十万漏洞积累



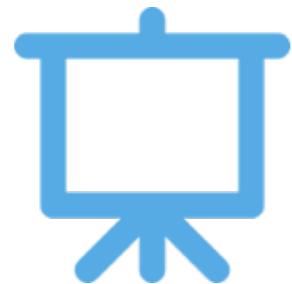
快速问题修复



业务不懂安全漏洞，一脸懵逼



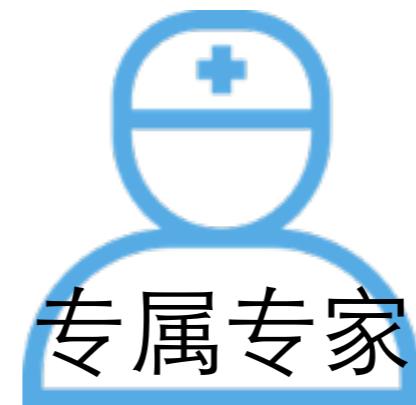
快速问题修复



人工风险演示



详细的修复方案



专属专家



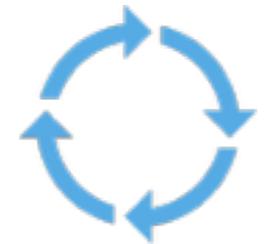
100%准确率



专家风险预警



持续风险管理



周期性安全监测



风险趋势分析



唐朝安全巡航
TangScan.com



谢谢