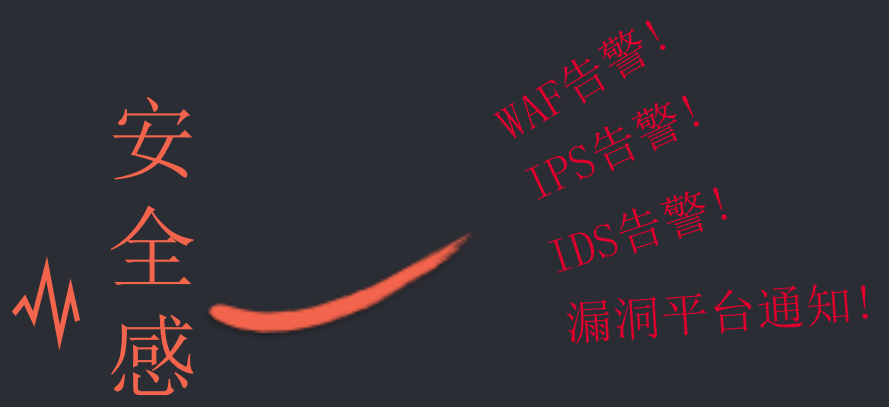
掌控企业安全威胁
企业安全2.0与威胁情报

默安科技． 聂万泉

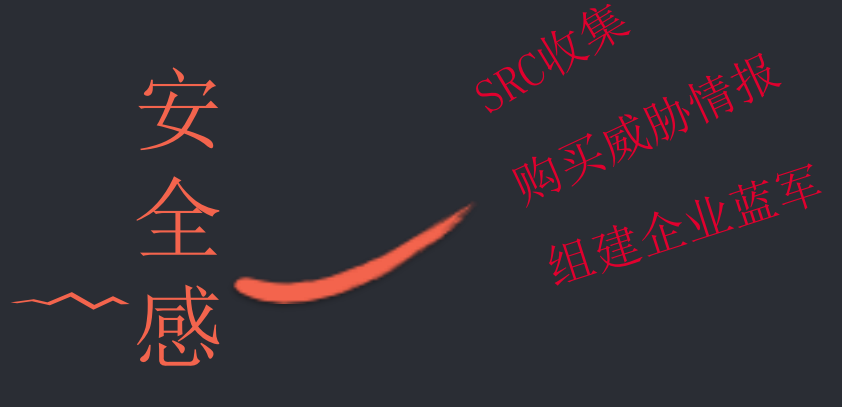
安全爱好者群体增长趋势

当不安全成为一种常态

企业如何找到安全感



以事件为中心-被动型



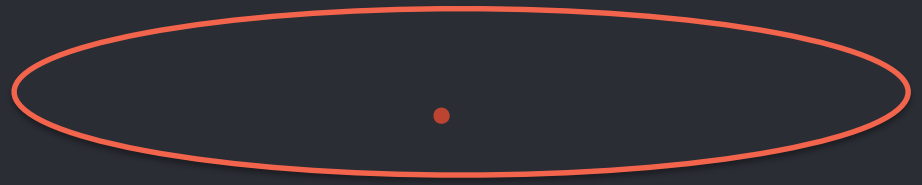
以威胁为中心-主动型

打造持续看见威胁的能力

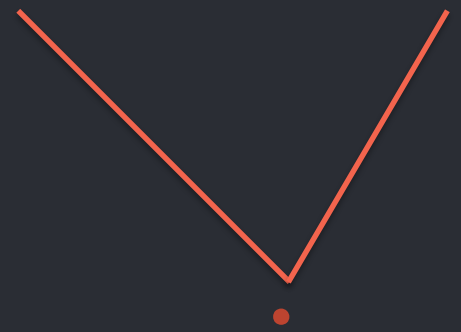
Security does not depend on God!

- 用攻击者视角寻找问题
- 建造威胁预警系统
- 建设安全传感器网络
- 全局的威胁情报驱动

攻击者视角的重要性

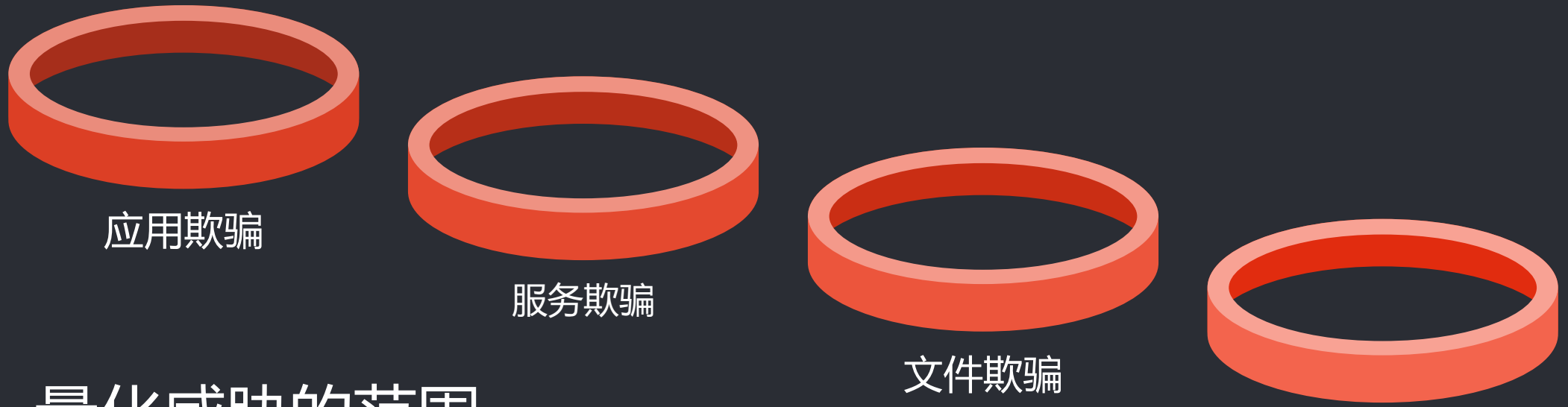


攻击者视角



防守者视角

用蜜网量化威胁



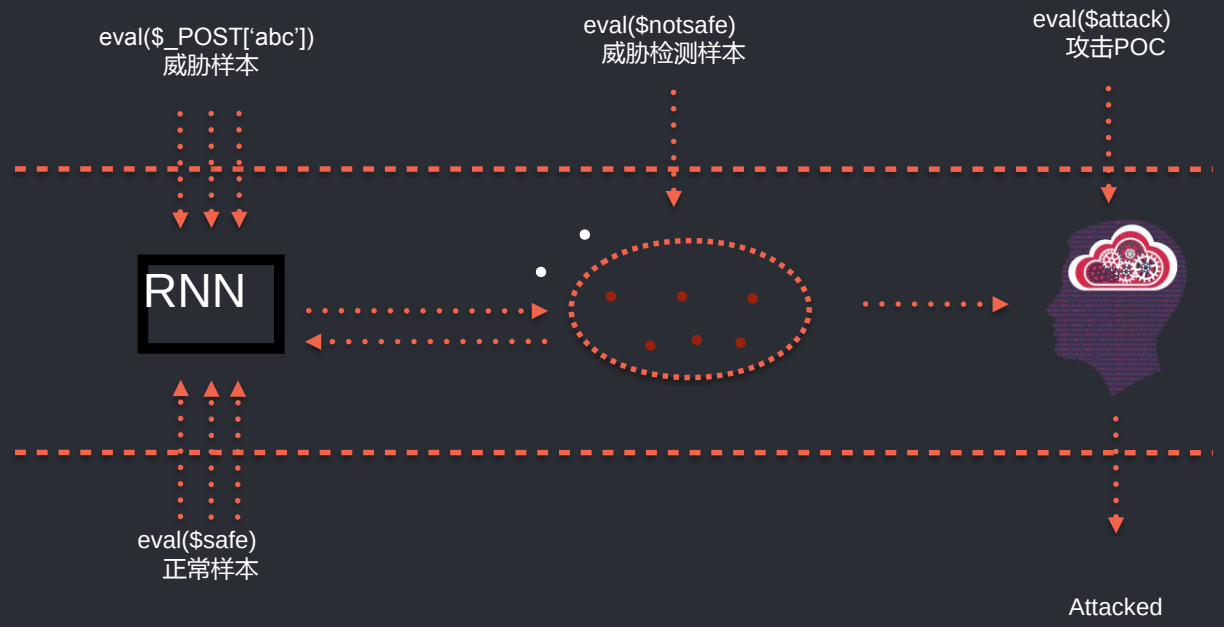
量化威胁的范围
感知威胁的深度

企业的安全传感器网络

感知安全脉博跳动

多纬度的联动响应

企业威胁识别的智能化


eval($_POST[‘abc’])
威胁样本
eval($notsafe)
威胁检测样本
eval($attack)
攻击POC
RNN
eval($safe)
正常样本
Attacked

全局威胁情报的意义

上下游风险

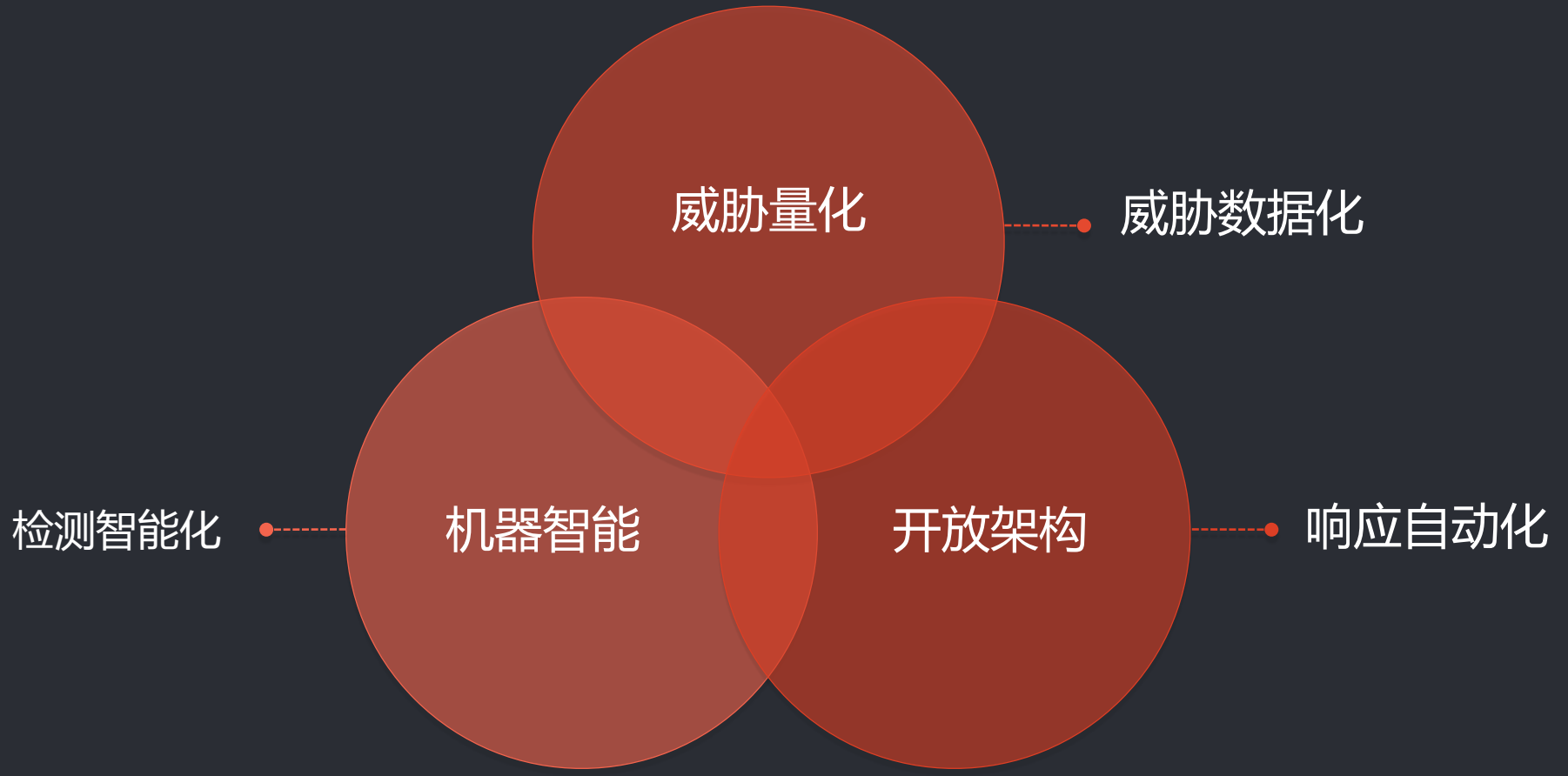
高危漏洞

同行的问题

竞争及法务风险

什么是万物互联时代的安全体系

企业安全体系2.0



谢谢!