长亭科技
CHAITIN.CN

智能化校园网络安全解决之道

北京长亭科技有限公司

简介

长亭科技 CHAITIN.CN

陈宇森 D3AdCa7

- 北京长亭科技有限公司联合创始人
- 免试保送进入浙江大学竺可桢学院求是科学班计算机方向，浙江大学信息安全研究团队AAA创始人，美国西北大学访问学者。
- 曾获得大量网络安全攻防比赛冠军，其中包括360杯大学生安全竞赛总决赛冠军、CNCERT中国网络安全攻防大赛冠军、首都网络信息安全日攻防竞赛冠军等。
- 曾在2015阿里巴巴安全技术峰会、2015华为安全沙龙等做技术演讲，美国 BlackHat 2015 Arsenal 做技术展示。

校园网络安全现状

长亭科技 CHAITIN.CN

- 业务线长，漏洞数量多且类型复杂，修复漏洞通常不及时（**工作量太大**）
- 本身承担着很多运维相关的工作，难有专门负责安全的人（**人员匮乏**）
- 每天有处理不完的业务需求时，没有时间跟进最新安全趋势（**难以应对千变万化的攻击**）

校园网络安全现状

导致的后果就是大量的校园网站被入侵、长期控制

- 暴露出来的问题只是冰山一角
- 随着信息化的推进，网络安全防护无法跟上的话，问题会越来越严重

人生苦短，我用 Python

人生苦短，我要智能

可能的解决思路

- 智能化
  a. 节省人力
  b. 自动化处理大量工作
  c. 应对日新月异的攻击
- 和高水平学生合作
  a. 节省人力
  b. 应对日新月异的攻击

现在的时代：一点也不智能化时代

长亭科技 CHAITIN.CN

- 安全产品
  a. 规则集（老生常谈：**绕WAF**）
  b. 死板
  c. 大量的配置项，一台设备没有一个专人负责，几乎等于没有用
  d. 漏报率误报率高，不敢拦截只敢检测
  e. 设备之间互为信息孤岛，即使有SoC，也只是收集统计，并不能做进一步的工作

我们想带来的改变，智能化 1.0 时代

长亭科技 CHAITIN.CN

- 安全产品
  a. 去规则化，用高准确率召回率的算法引擎分析
  b. 几乎零维护，即插即用
  c. 产品之间数据互通，关联分析揪出入侵者
  d. 机器学习，处理海量数据

简单介绍一下我们——长亭科技

长亭科技 CHAITIN.CN

- 顶尖的安全团队
  - 2016年，公司多位成员参与组成的 b10op 战队获得全球顶尖网络安全攻防赛 Defcon CTF 全球决赛第二名，同时长亭科技几乎垄断了国内网络安全攻防比赛的冠军
  - 在物联网安全领域，发现了众多国际知名路由器如思科、华为以及众多国际知名摄像头的高危安全漏洞。其中2016年315晚会展示的智能摄像头漏洞是我们的研究成果。
- 业界领先的防护算法
  - SQL 注入无规则防护引擎登上国际顶级黑客会议 Blackhat USA 2015

雷池 / SafeLine

长亭科技 CHAITIN.CN

- 传统WAF的困境
  - 传统WAF产品依赖规则（正则表达式匹配）来进行Web攻击防御
    - 规则维护麻烦，且容易出错，费力
    - 规则越多速度也越慢，费事
    - 误报率和漏报率都很高，且难以跟踪未知漏洞，费心
  - 传统硬件WAF产品主要以单台硬件设备形式部署
    - 对于使用云服务器的公司无法支持

欢迎访问我们的官方网站了解详情，申请试用：https://chaitin.cn

雷池 / SafeLine

长亭科技 CHAITIN.CN

- 雷池的优势
  - 无规则
    - 精细化处理的智能语义理解的检测引擎代替传统规则集
  - 支持水平扩展
    - 支持大数据、大流量、云环境

欢迎访问我们的官方网站了解详情，申请试用：https://chaitin.cn

雷池 / SafeLine

长亭科技 CHAITIN.CN

- 雷池能达到的效果
  - 快
    - 检测速度快
  - 准
    - 攻击检测准确率高、召回率高
  - 省
    - 省时、省力、省心

欢迎访问我们的官方网站了解详情，申请试用：https://chaitin.cn

从数据泄漏事件到银行大劫案，多数企业在事件爆发时才知道自己被黑。

——接受攻防不对等的现实，着力提升感知能力，形成防护闭环

谛听 / DSensor

长亭科技 CHAITIN.CN

- 现状：黑客进入大多数企业内网之后，如入无人之境，畅通无阻

- 解决安全内网最后一公里的困境
  - 使用基于真实服务的伪装欺骗技术
  - 适配业务场景
- 目的
  - 准确、快速的发现入侵行为
  - 迷惑攻击者，为后续的应急响应争取宝贵的事件

欢迎访问我们的官方网站了解详情，申请试用：https://chaitin.cn

高级渗透测试

长亭科技 CHAITIN.CN

- 不止局限于覆盖功能点的合规性测试
- 尝试从多种角度进行渗透
  - 无线网络
  - 社会工程学
  - 网络设备
  - 安全设备
- 最大限度的帮客户提前发现漏洞，提出修复建议，减少攻击面

长亭安全巡检

长亭科技 CHAITIN.CN

- 建立企业资产列表，及时了解对外资产状态。
- 企业资产信息监控，及时发现资产异常状态。
- 企业资产漏洞管理，及时跟进漏洞修复状态。
- 安全漏洞事件预警，及时获取漏洞事件信息。

展望未来，智能化 2.0 时代

长亭科技 CHAITIN.CN

- 安全产品
  a. AI
  b. 自动化的人机对抗
  c. 像 google 的机房用机器人换硬盘一样，让 AI 来和入侵者对抗

关于人才的一点小想法

长亭科技 CHAITIN.CN

- 暂时来看，安全归根到底是人与人的对抗。
  a. 毕竟距离实现出好用的AI还需要些时间。
- 高校的安全课程体系比较缺乏实践环节和业界前沿资讯。
  a. 校企合作，共建课程
  b. 设置挑战，良性引导
  c. 立足长远，重视基础
  d. 学生助力，更加安全