



大数据安全人才的选拔与培养

郑晓峰

奇安信集团羲和网络安全实验室

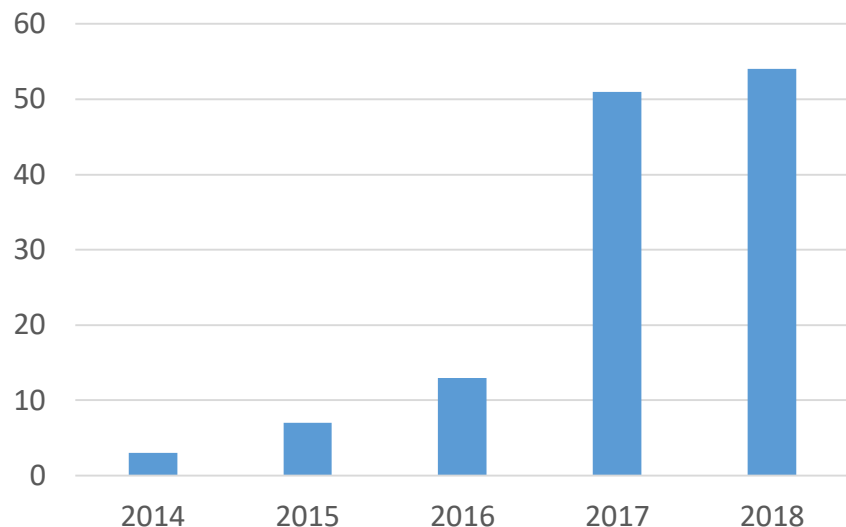
目录

国内安全人才培养现状

大数据安全人才培养

国内首届DataCon大数据安全分析比赛

“未知攻，焉知防”：CTF、漏洞挖掘赛事如火如荼



近年国内部分CTF公开赛事
(数据来源: XCTF社区)



THU NISL一景



CTF: 简历“标配”



攻防之辩

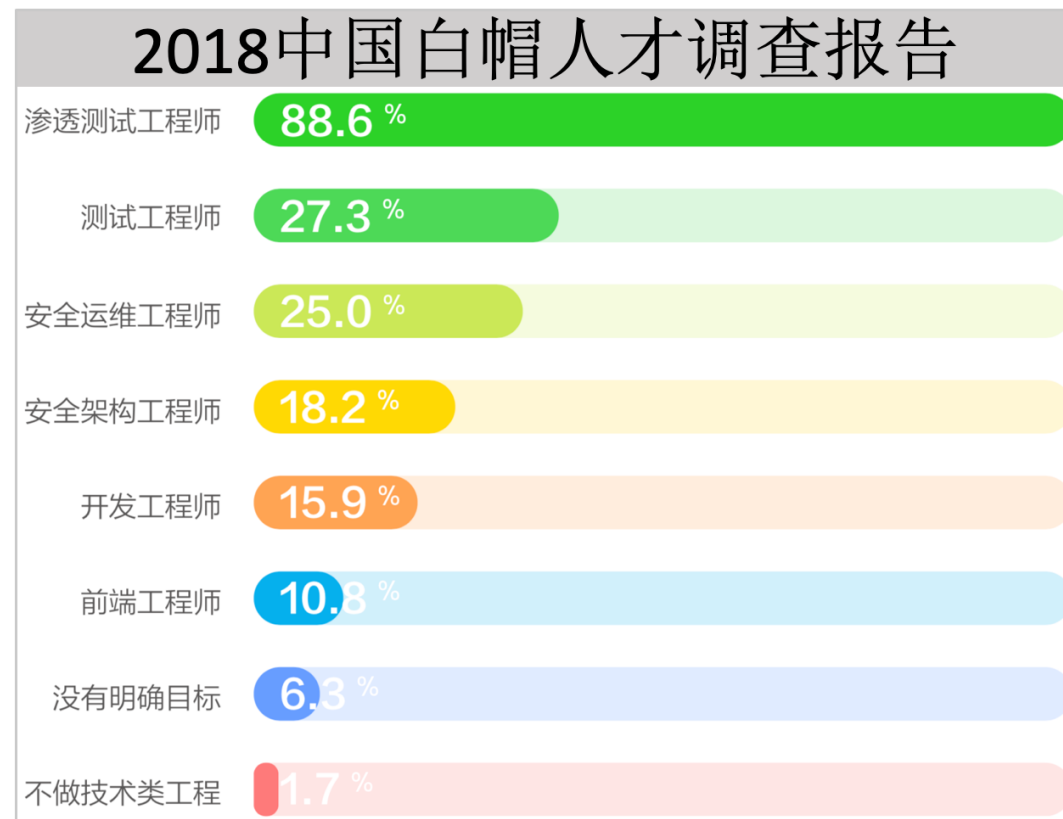
- 攻是防的必要非充分条件
- 攻已盛，防可待

大数据场景下，攻防对抗的1:99问题

- 攻击：成功率1%，厉害的攻击
- 防御：准确率99%，欠佳的防御

院校培养到企业人才的最后一块拼图

- 学院派 vs 工业派



数据来源：补天漏洞响应平台

需求、数据、平台

解决大数据应用的安全问题？

大数据场景下的安全问题

用大数据解决安全问题

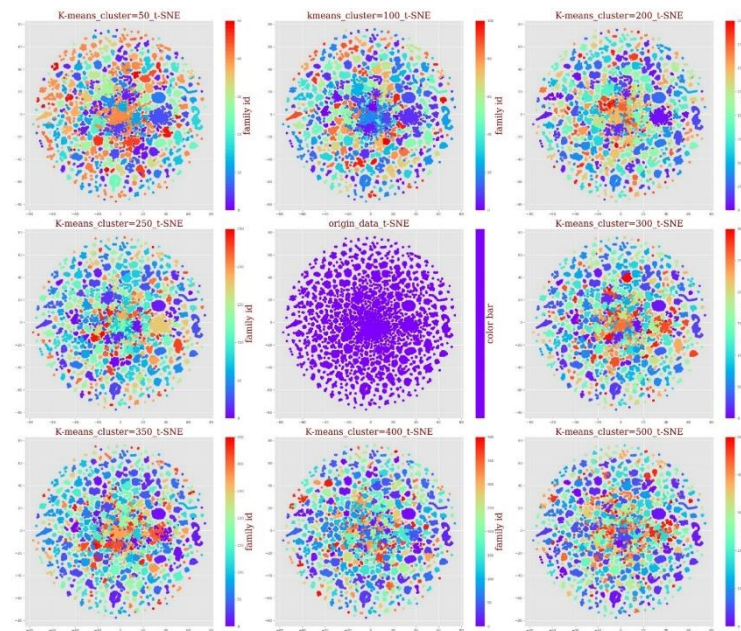
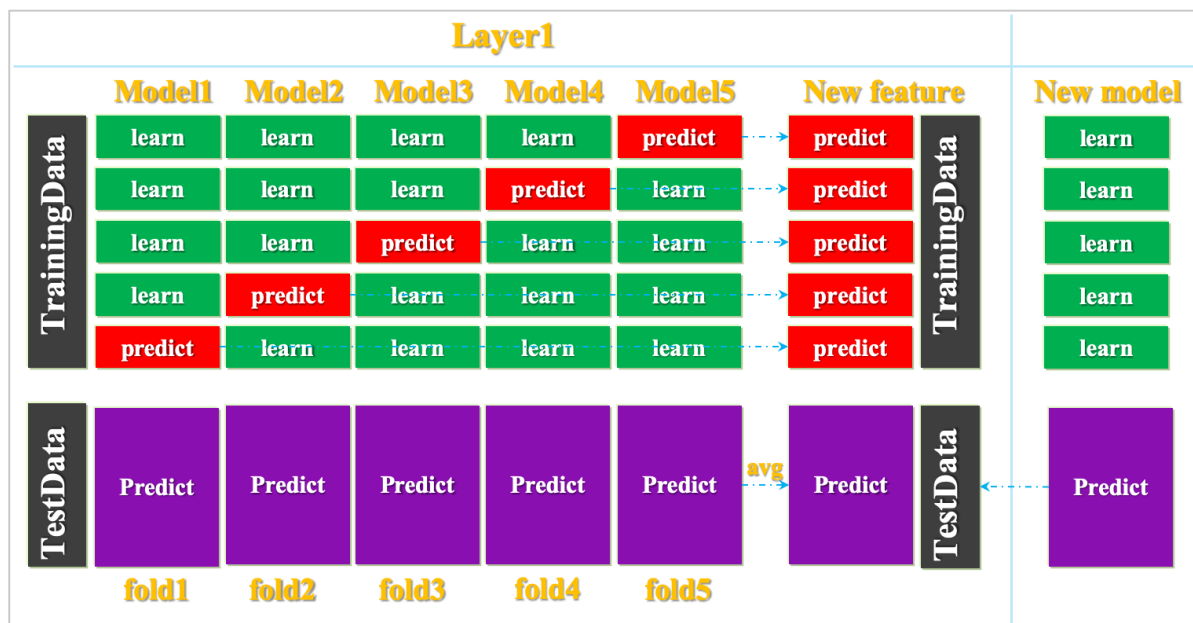
DataCon：国内首届大数据安全分析比赛

- 非纯攻击/漏洞挖掘类比赛
- 非纯人工智能比赛
要AI，更要可用的AI
- 非固定命题比赛
开放式题目，共同探索
- 非一次性的比赛
面向学术研究数据开源、产生持续价值
- 贴近真实企业场景、数据驱动安全
货真价实的工业界一线需求

给需求！ 给数据！ 给平台！

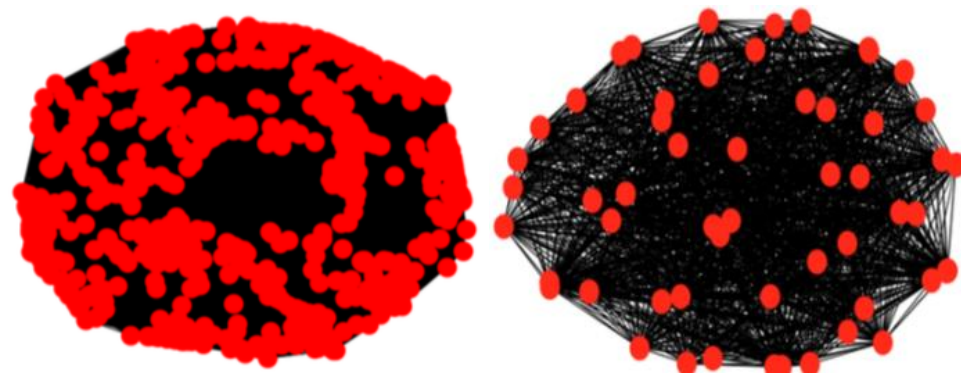
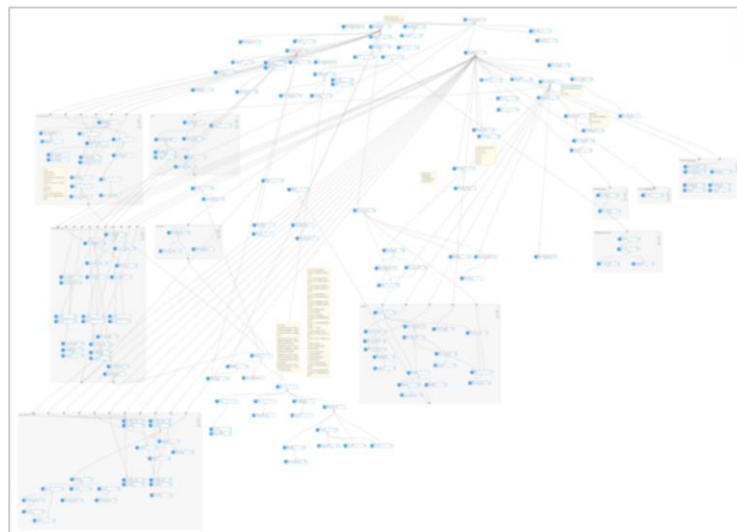
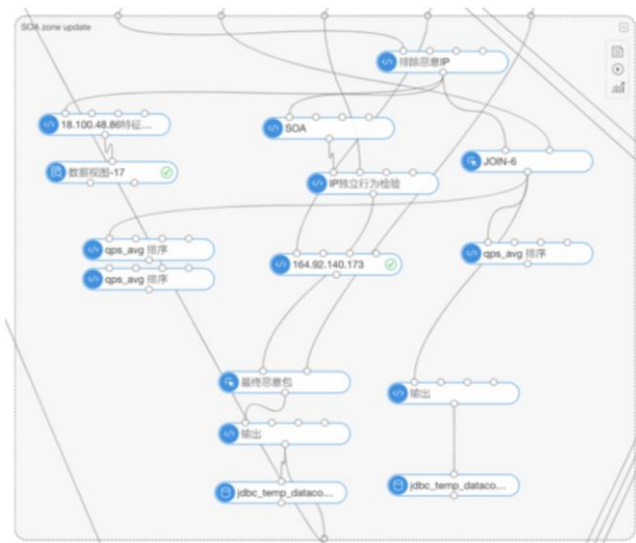
3万恶意代码动态行为序列

- 恶意代码检测
- 恶意家族聚类



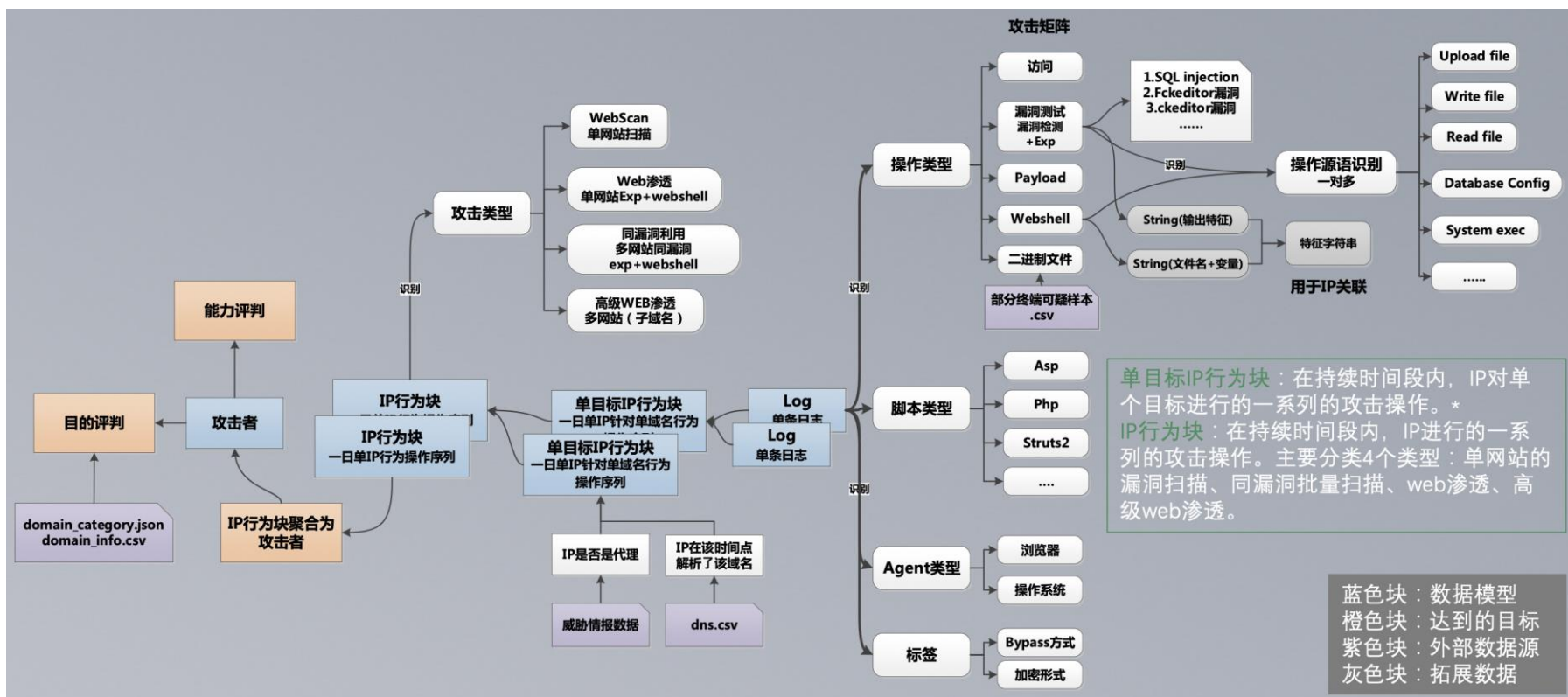
1000万条DNS原始数据

- 检测DNS攻击
- 检测DGA恶意域名
- 恶意域名家族聚类



DGA域名社区发现 (Louvain)

- 事件分析
- 攻击者溯源



全球551支战队、3000多名选手参赛

多个高校将此次比赛纳入计算机相关课程学分考核体系

15家500强企业招聘直通车



中国石油



中国石化
SINOPEC



国家能源集团
CHN ENERGY



中国交通建设
CHINA COMMUNICATIONS CONSTRUCTION



GREE 格力



港中旅
CTS



中国平安
保障·银行·投资

平安银行
PINGAN BANK



北汽集团
BAIC GROUP



长江证券
CHANGJIANG SECURITIES

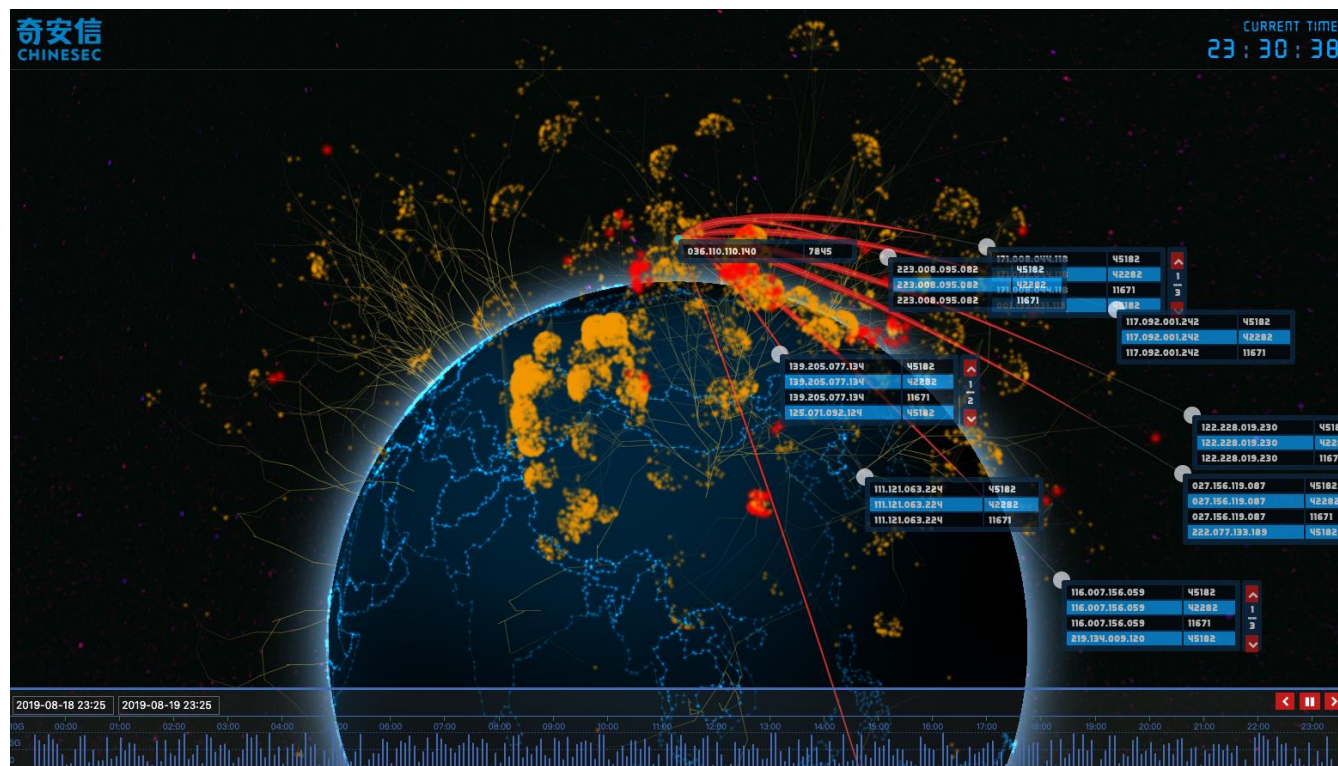
OCT 华侨城


专题赛

- 聚焦专项数据
- 加密流量、邮件、APT、暗网

行业赛

- 聚焦行业数据特点、需求痛点
- 高校、金融、电力、运营商...



The background is a solid blue color with a subtle, abstract pattern of thin, light blue lines that form a grid-like structure, possibly representing a network or data flow. The pattern is more dense in some areas and more sparse in others, creating a sense of depth and movement.

THANKS

2019 北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE



2019北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE

网络安全人才论坛

多源化、实战化、行业化