甲方视角的情报体系

—从人的角度量化安全威胁

魏兴国（云舒）
默安科技CO-Founder & CTO

主办单位：杭州
Alibaba Group 阿里巴巴集团
战略合作伙伴：intel

目 录
content

- 为什么需要威胁情报
- 为什么需要甲方视角
- 甲方视角威胁情报的关键点
- 如何实现甲方视角
- 意见和建议

扫码观看大会视频

一、为什么需要威胁情报

1

内部：漏洞不足以描述风险的全貌

漏洞为中心到威胁为中心：评估现状、还原攻击、预测攻击

2

外部：黑客已经在使用威胁情报做攻击

github、Dropbox、邮件帐号、电话号码、社工库、钓鱼攻击。

二、为什么需要甲方视角的威胁情报

1

乙方视角的威胁情报更着重于全网趋势

全局情报与指定少量的公司资产关联，能匹配到多少全靠运气。

2

威胁情报需要与自身业务紧密结合，落地，取得最佳效果

不同的公司，不同业务，面临的威胁完全不同，需要的情报也不同。

三、甲方视角威胁情报的关键点

小王啊，我们作为宇宙最大的公司，数据损坏影响到宇宙的存在性，我们被人入侵了没有？数据被偷过没有？

老板，从目前部署的宇宙最强IDS报警来看，没有被入侵。但是M78星云和天顶星听说很厉害，不知道他们会不会绕过了我们的所有系统而我们不知道。

入侵还是没有入侵
这是个问题

报告老板，被攻击最多的TOP 10 IP地址是xxxxx，攻击来源最多的TOP 10 IP地址是ooooo，攻击来源TOP 10 地区是火星，over

搞不清楚入侵与否，那有攻击没有？攻击我们的是哪些人？那些是刻意盯着我们的，哪些是无意的？刻意盯着我们的，你们要抓一批！

抓不到黑客
不是我们无能
是黑客太狡猾？

扫码观看大会视频

Excuse me ?

老板，我们很辛苦的。昨天WAF受到666666次攻击，最近1小时受到2333次攻击。我们3个人查了3小时，发现一切正常。

误报和忙就是成绩？

1

是否已经被入侵了？

没有被入侵，还是入侵者技术太强，入侵了我们无法发现？这是一个悖论。需要明确的判断，并还原事件。

2

我们处于被攻击中吗？攻击者是谁？

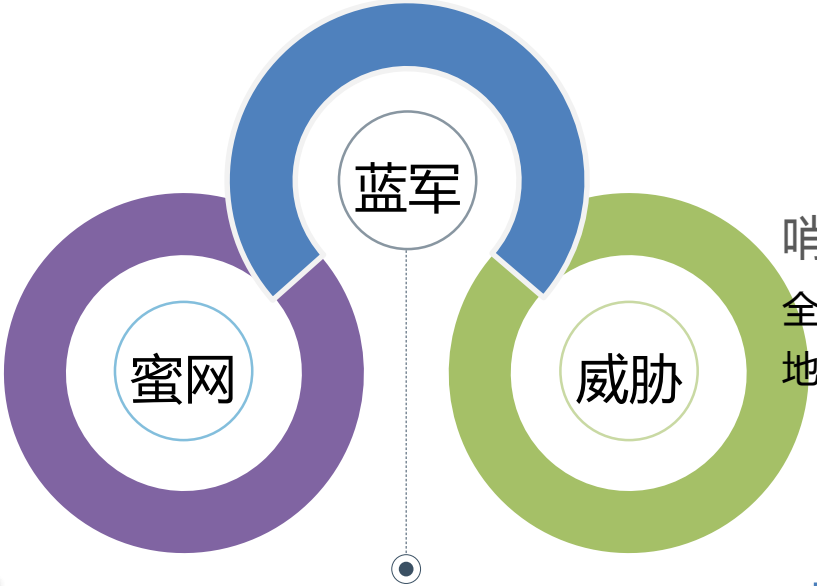
不要说攻击来源的TOP 10 IP是多少，被攻击的TOP 10 IP是多少。需要更高层次的人的语言，可以理解、可以做下一步动作的东西。

3

我们存在哪些问题？这些问题影响有多大？

不仅仅是漏洞，包括信息泄露、员工意识等一切可能导致风险产生的精确可量化的威胁。精确可以节省大量运营成本。

四、如何实现甲方视角威胁情报



幻盾

欺骗技术诱导攻击者，隔离攻击
行为分析模型，精确量化威胁
电子取证，设备指纹溯源黑客

哨兵云

全天候全面外部威胁发现
地下黑产情报采集

黑客化

影武者蓝军评估

发现任何可能的攻击路径
检验情报体系运营效果

常态化

扫码观看大会视频

1

基于行为，而不是特征

降低误报和漏报
降低运营成本

2

基于欺骗，控制黑客攻击的目标和链路

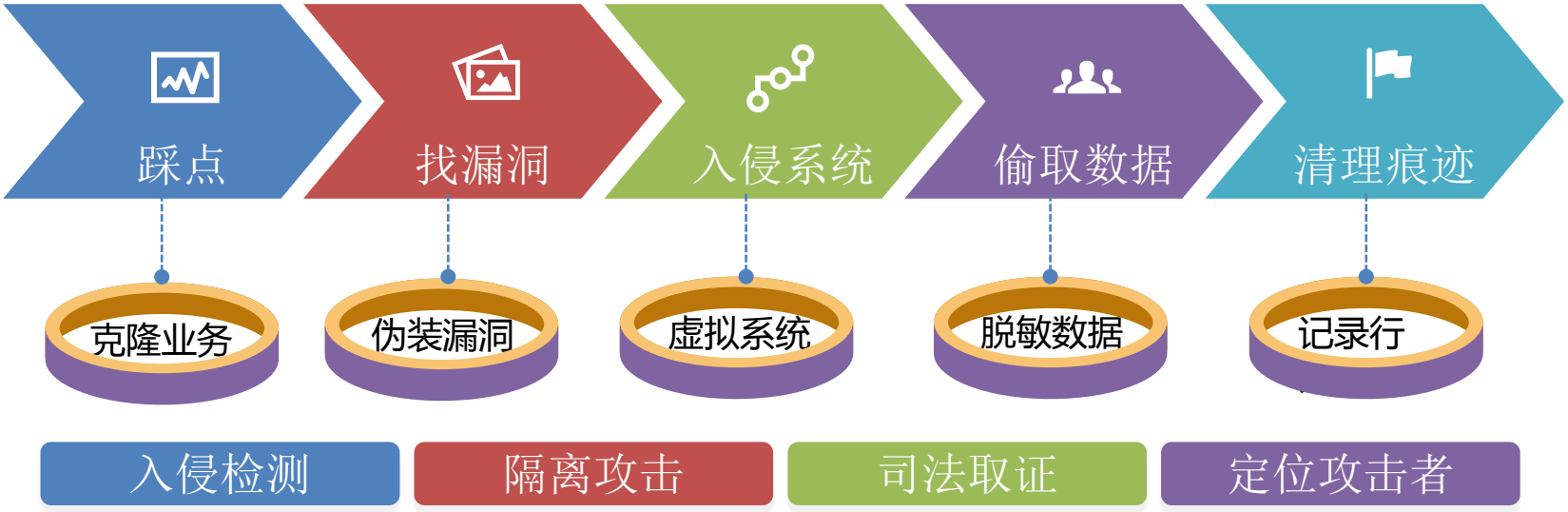
避免无休止的技术细节对抗
隔离攻击，消耗攻击者时间，增加攻击成本

3

建立黑客档案数据库

设备指纹，攻击行为建模

扫码观看大会视频


踩点
找漏洞
入侵系统
偷取数据
清理痕迹
克隆业务
伪装漏洞
虚拟系统
脱敏数据
记录行
入侵检测
隔离攻击
司法取证
定位攻击者

攻击者

网络ID:小卫

MID:GUYGUYGGI

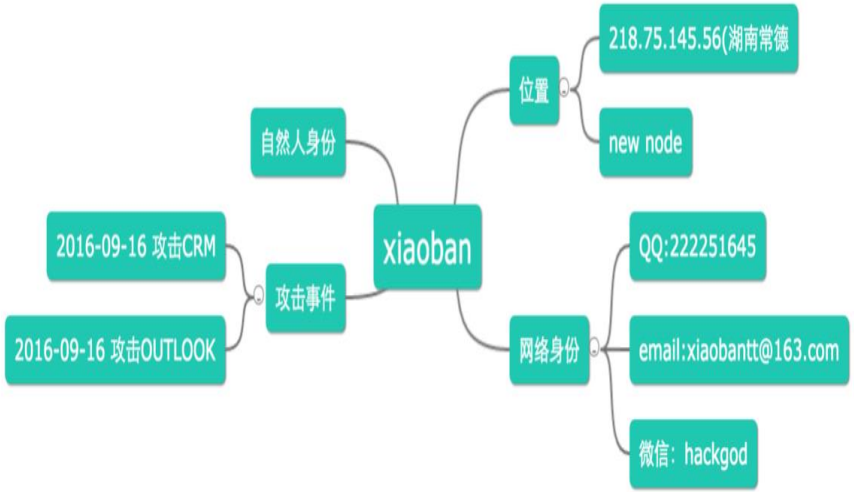
攻击目标:CRM蜜巢

物理位置:湖南常德

可溯源(增值)

真人概率:90%

经纬度:116.407395,39.904211



攻击记录

搜索

时间	来源	攻击目标	攻击手法
2016-09-16 12:32:45	218.75.145.56(湖南常德) 218.75.145.56(湖南常德)	CRM	POST crm.moresec.cn/upload.php 详情
2016-09-16 12:32:45	218.75.145.56(湖南常德)	CRM	cat /etc/passwd 详情

扫码观看大会视频

2016 The Computing Conference

THANKS

SANGFOR
深信服科技