2017 中国互联网安全大会
China Internet Security Conference

高级威胁分析在安全运营中的应用

李中文

elknot@360corpsec
360企业安全集团观星实验室

目录

- 企业安全运营面临的挑战
- 企业高级威胁分析案例
- 高级威胁分析应用总结

ISC 2017 中国互联网安全大会

360互联网安全中心

企业安全面临的挑战

CHALLENGES OF ENTERPRISE SECURITY OPERATION

企业安全面临的挑战 - 老板我们被打了

Σ(° △ °|||)⁞ 只知道被DDoS了，其他的不知道。。。。

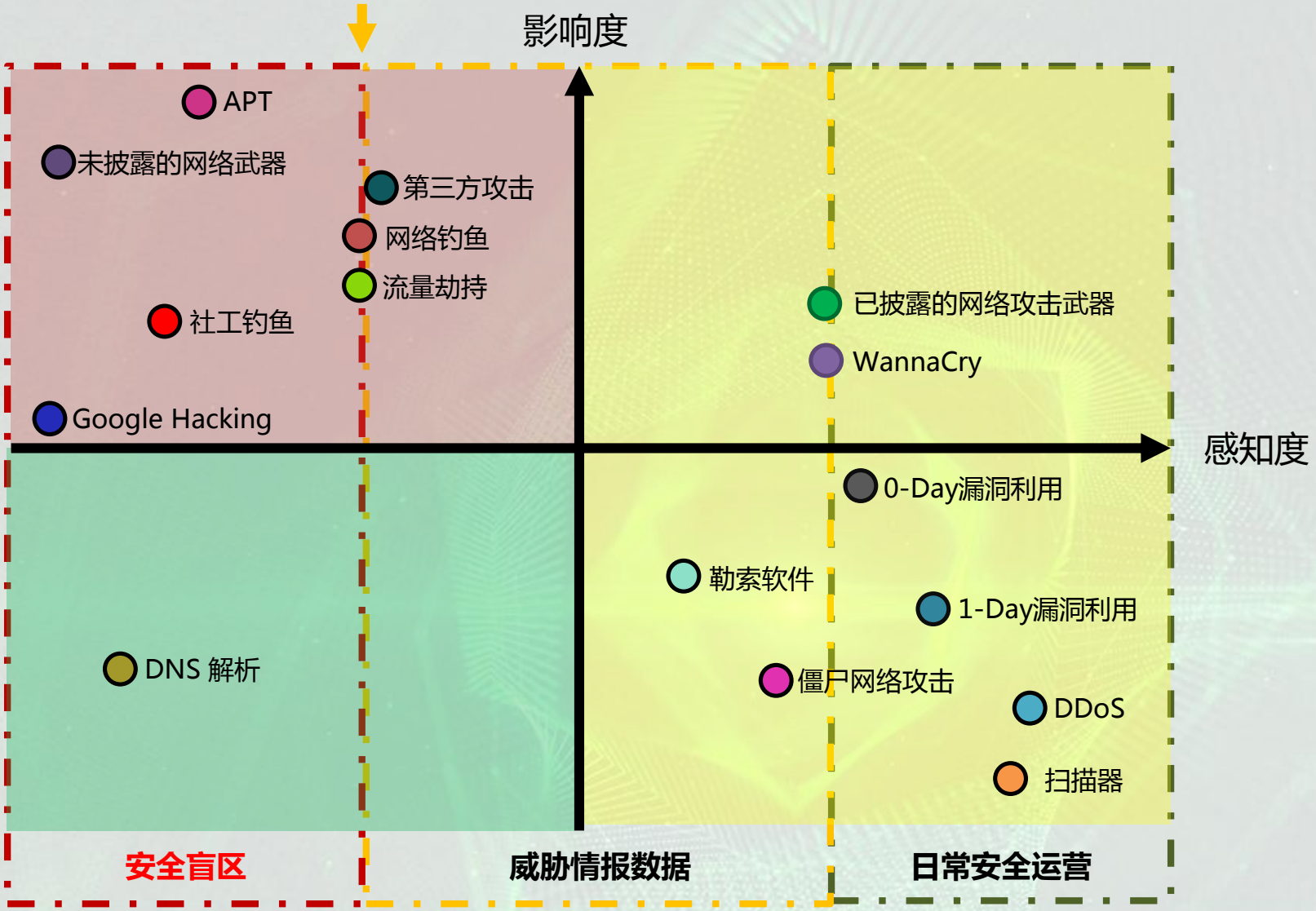
SOC Leader

(╬▔皿▔)，给我查！

(ノ｀Д´)ノ，查不出来扣你年终奖！

CTO

企业安全面临的挑战 - 安全运营的盲区



ISC 2017 中国互联网安全大会

360互联网安全中心

企业高级威胁分析案例

CASES OF ADVANCED THREAT ANALYSIS IN ENTERPRISE SECURITY OPERATION

某企业撞库事件分析

企业高级威胁分析案例 - 某企业撞库事件分析

客户

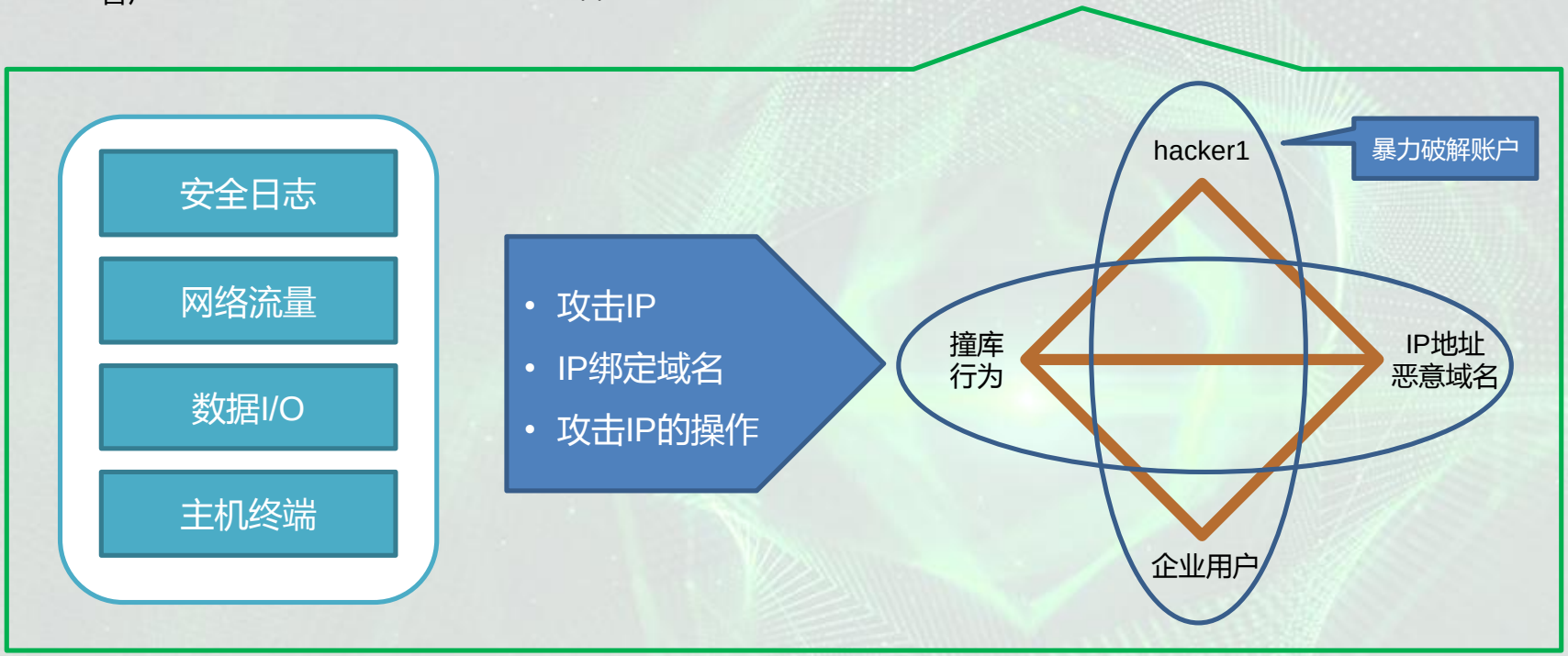
投诉

客服

反馈

SOC团队

- ~~怎么搞我们？~~
- 为什么搞我们？
- 撞库的数据哪儿来的？



企业高级威胁分析案例 - 某企业撞库事件分析

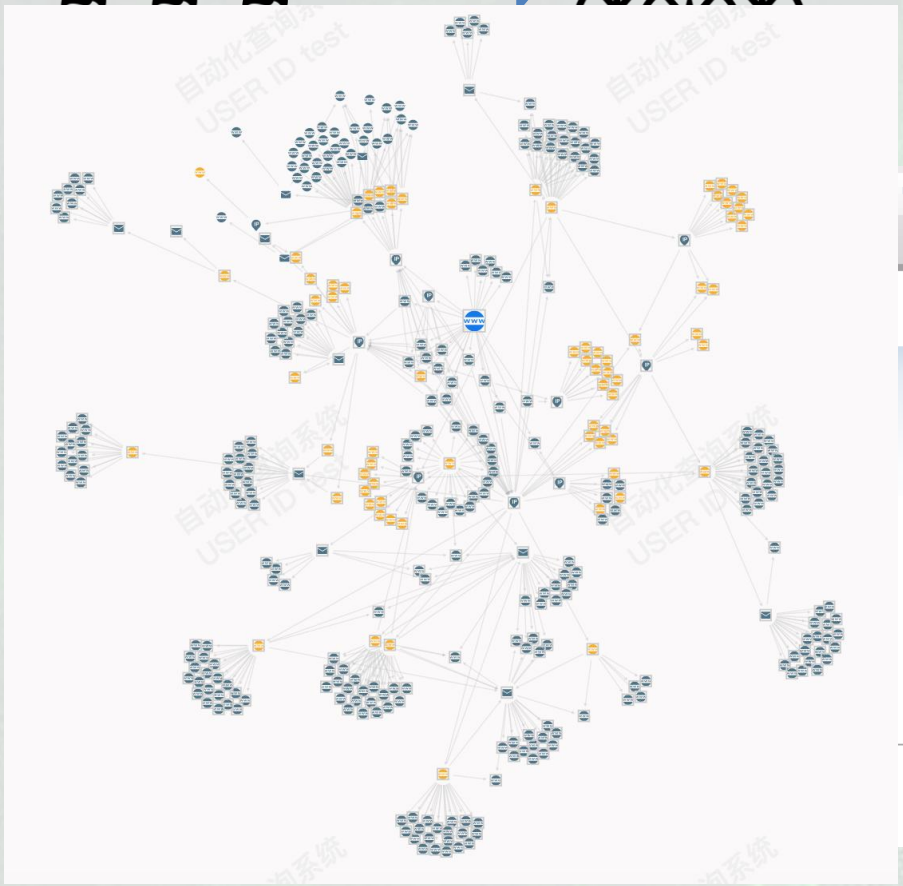
投诉

反馈

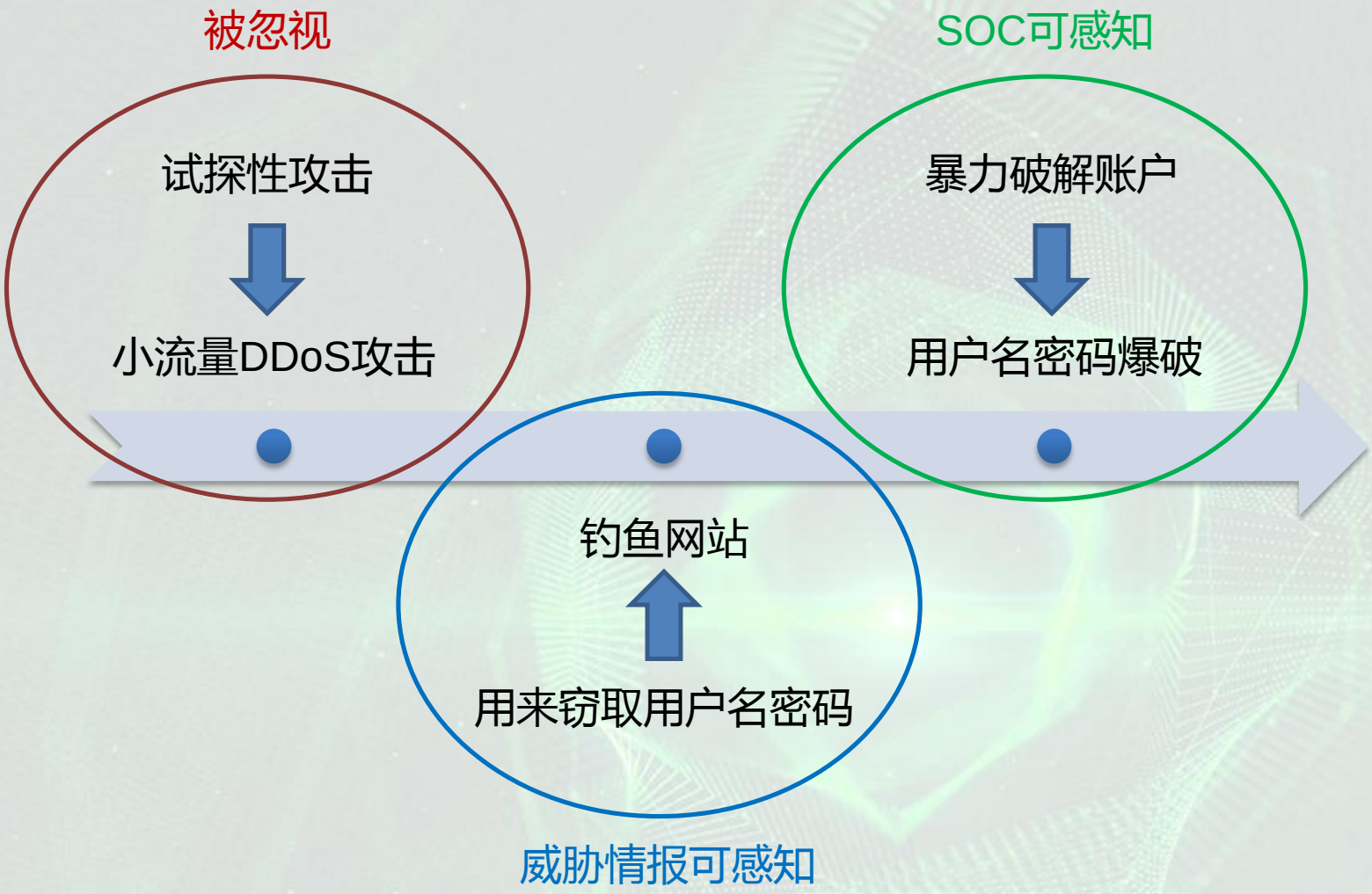
SOC团队

寻求帮助

威胁分析师

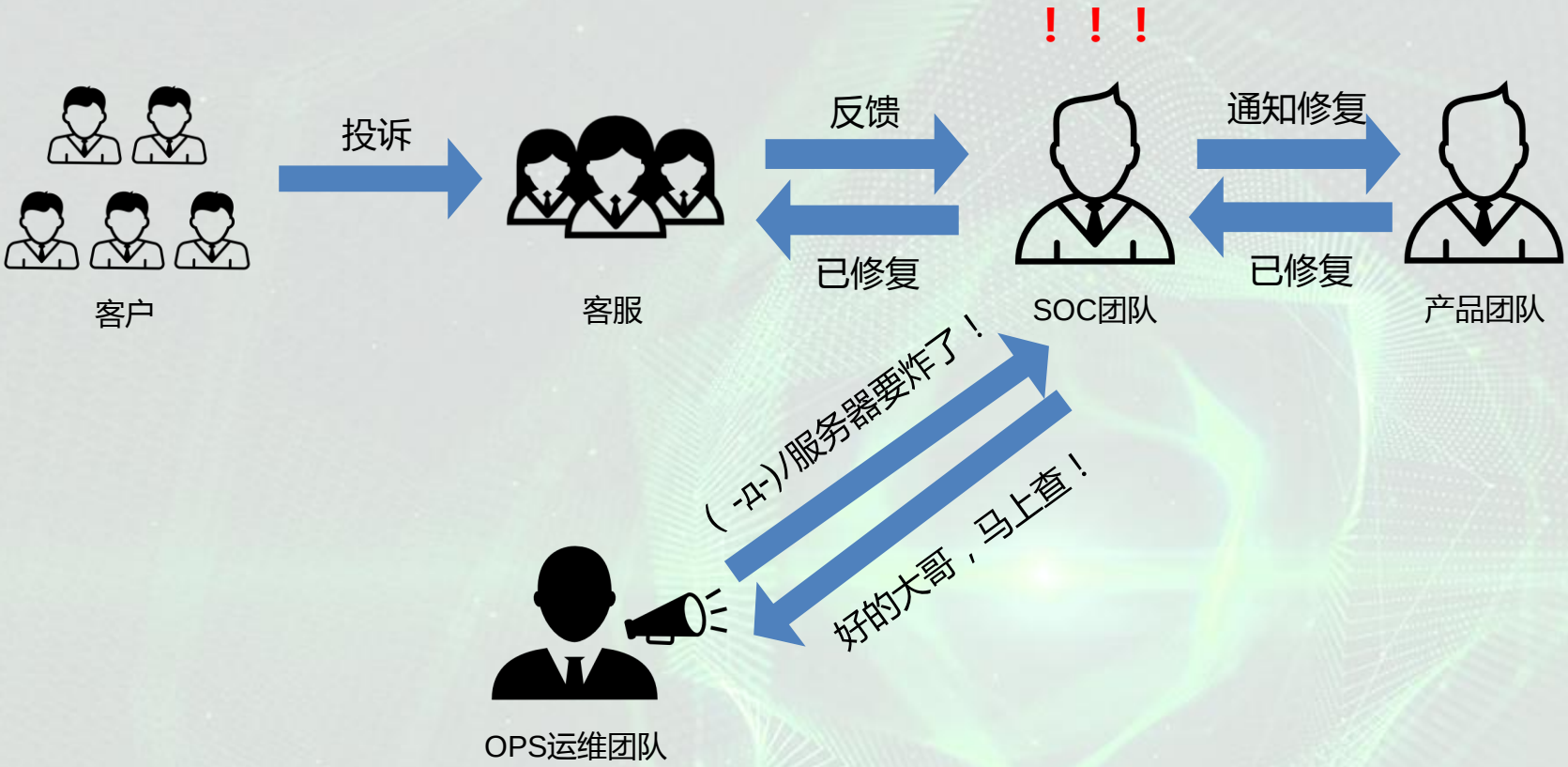


企业高级威胁分析案例 - 某企业撞库事件分析



某企业短信平台事件分析

企业高级威胁分析案例 - 某企业短信平台事件分析



企业高级威胁分析案例 - 某企业短信平台事件分析

SOC团队

- 这么多都是一个请求而且有好几个都被情报标记了——从经验上来看一定是CC攻击！
- (*￣∇￣*)，我就是这么聪明！喂，老大，问题解决了，确实是CC攻击，赶紧封锁IP！
- ヾ(o◕∀◕)ﾉ，响应这么及时而且这么准确，出任CTO迎娶白富美指日可待！

企业高级威胁分析案例 - 某企业短信平台事件分析

企业高级威胁分析案例 - 某企业短信平台事件分析

威胁分析师

- 短信平台存在的漏洞没有彻底修复导致大量无效请求仍然会发送至服务器处理
- 这个短信平台接口之前被黑产收录了，封装进了短信轰炸机程序
- 不只是你们，很多其他的企业的问题接口也在这个目录里，你们都是被黑产坑了的受害者
- 整改建议——重新修复漏洞，然后烧高香，等黑产 release 一个新版本把你们的接口删掉

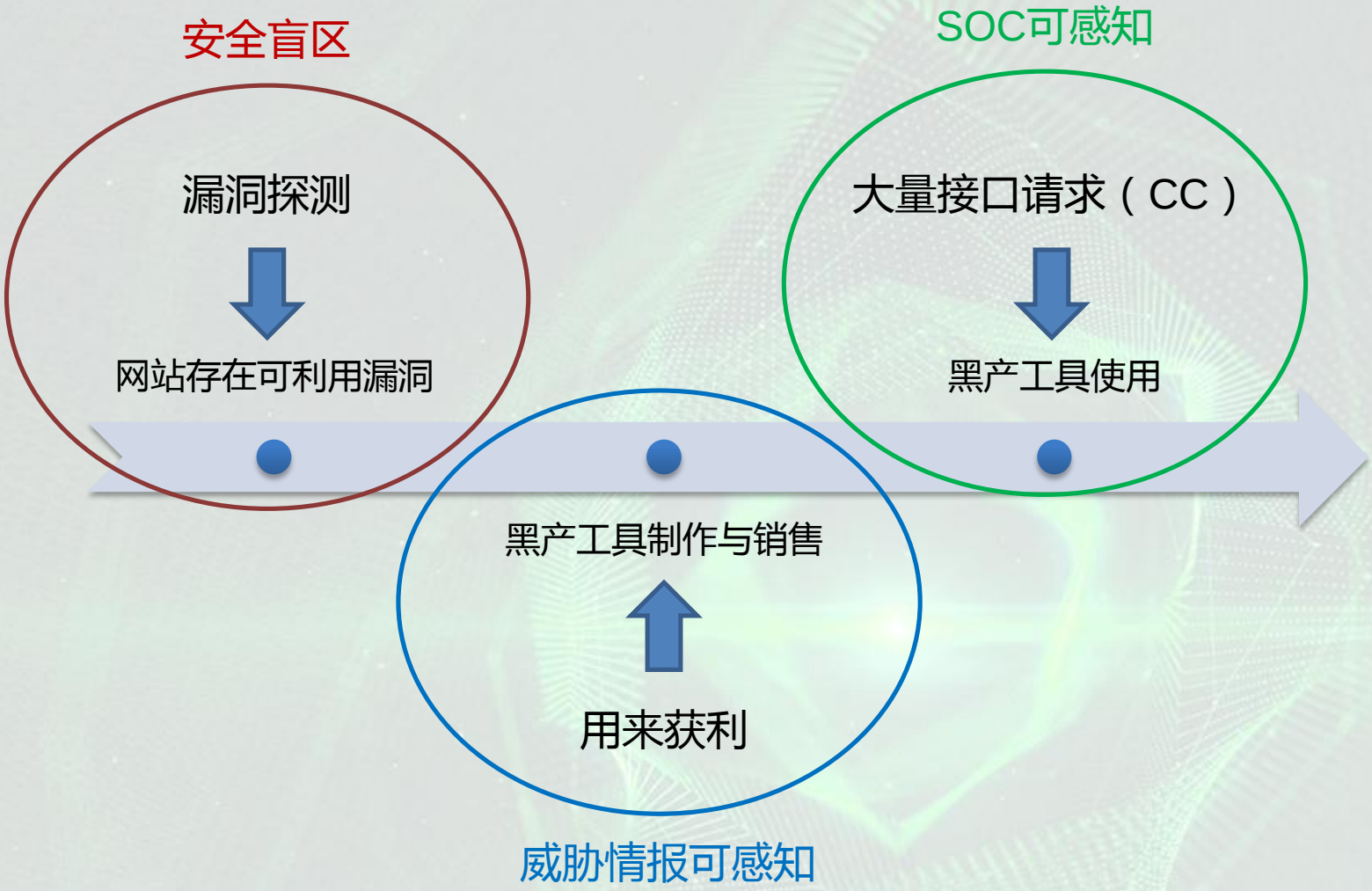
攻击者的行为

攻击者基础设施

攻击目的

攻击工具集 top3
短信轰炸机（75%）
扫描器（12%）
注入工具（6%）

企业高级威胁分析案例 - 某企业短信平台事件分析



ISC 2017
中国互联网安全大会

360互联网安全中心

高级威胁分析对于安全运营的意义

SIGNIFICANCES OF ATA IN ENTERPRISE SECURITY OPERATION

高级威胁分析对安全运营工作的意义

- ✓ 使用更多威胁情报数据能缩小安全运营盲区
- ✓ 威胁情报 + 高级威胁分析方法 = 真正的攻击目的和攻击者画像
- ✓ 新时代下的安全面前，经验往往是靠不住的
- ✓ 可能是攻击的攻击不一定是攻击，不太可能是攻击的往往是攻击的源头

总结

- ✓ 安全盲区对于安全运营的影响
- ✓ 分析高级威胁攻击事件的方法
- ✓ 高级威胁分析对于安全运营的意义

谢　谢