甲方视角威胁情报

——欺骗的力量

默安科技联合创始人兼CTO
云舒

几个小问题

我们最近没有被入侵吧？

昨天WAF受到66666次攻击，办公网IPS报警23333次，我们3个人分析了5个小时，发现一切正常。应该没有入侵吧？除非攻击者太厉害

那攻击有没有?
知不知道是谁在盯着我们?
我们要抓人，威慑一下他们!

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

漏洞呢？有多少个？有没有暂时还不知道的漏洞？

扫描器说oracle服务器可能存在一个不明细节的漏洞，还不知道怎么处理。不知道的漏洞，既然不知道，我怎么知道……

- 厂商互比追求数据全面，大量误报运营成本极高
- 厂商和客户语言不通，双方各说各话
- 完全的硬碰硬正面防御，纠缠于技术细节对抗

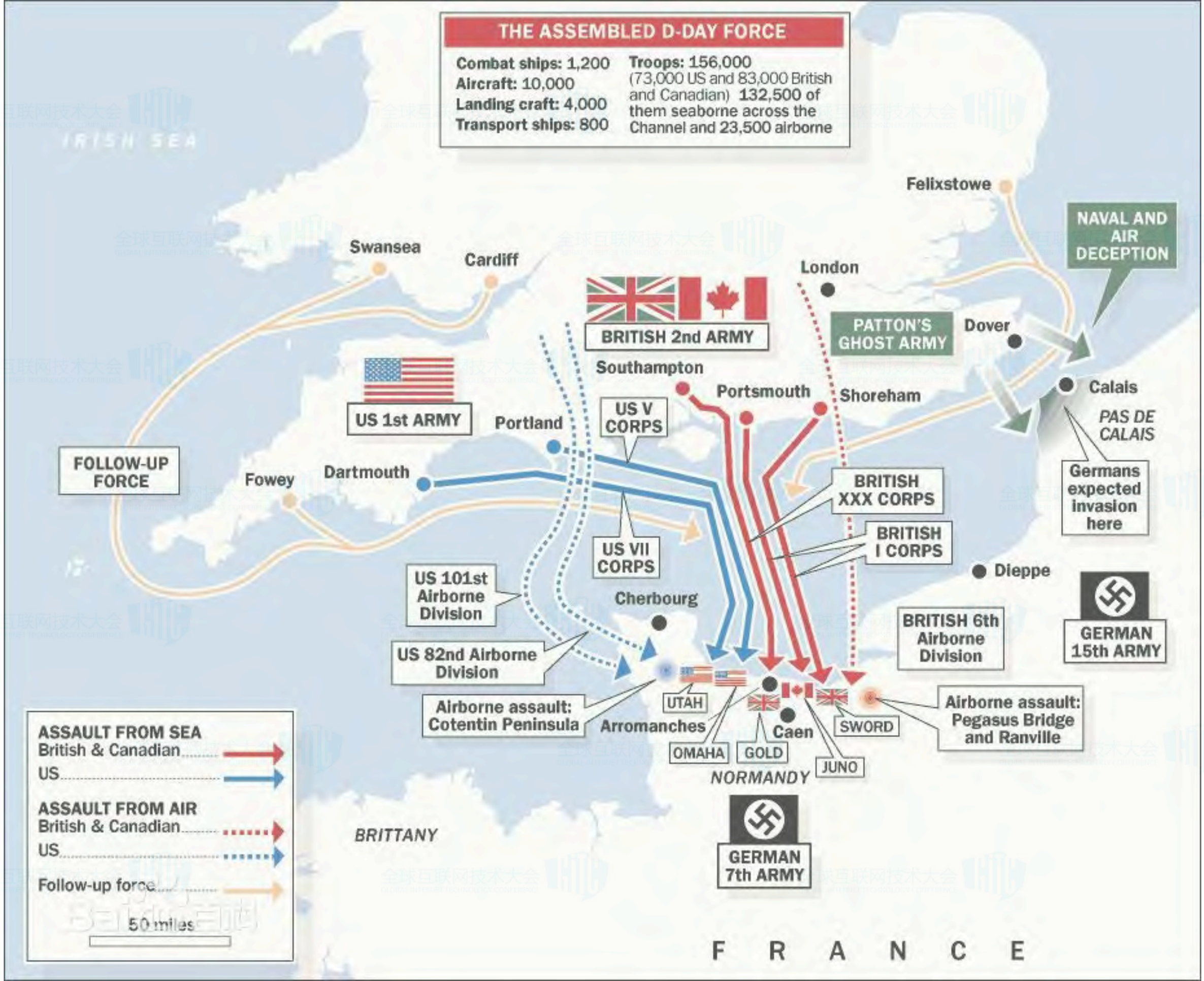
没有真正站在

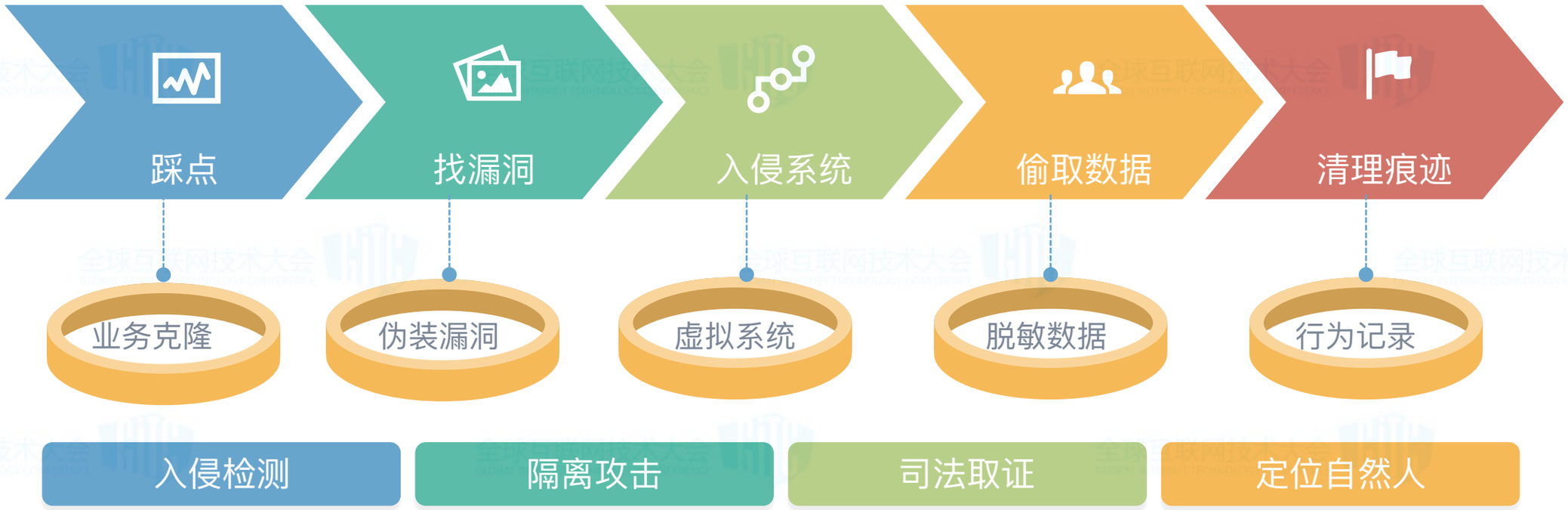
甲方角度思考安全

甲方想要什么?

- 我已经被黑了吗？是谁黑的？目的是什么？
- 有人正在尝试黑我们吗？他们是谁？用什么方法？
- 我们存在黑客也没有发现的安全问题吗？在哪里？

甲方视角威胁情报：5W1H


THE ASSEMBLED D-DAY FORCE
Combat ships: 1,200
Aircraft: 10,000
Landing craft: 4,000
Transport ships: 800
Troops: 156,000 (73,000 US and 83,000 British and Canadian) 132,500 of them seaborne across the Channel and 23,500 airborne
IRISH SEA
Felixstowe
NAVAL AND AIR DECEPTION
Swansea
Cardiff
London
BRITISH 2nd ARMY
PATTON'S GHOST ARMY
Dover
Southampton
Portsmouth
Shoreham
Calais
PAS DE CALAIS
US 1st ARMY
Portland
US V CORPS
FOLLOW-UP FORCE
Fowey
Dartmouth
BRITISH XXX CORPS
Germans expected invasion here
BRITISH I CORPS
US VII CORPS
Dieppe
US 101st Airborne Division
Cherbourg
GERMAN 15th ARMY
BRITISH 6th Airborne Division
US 82nd Airborne Division
Airborne assault: Cotentin Peninsula
UTAH
Arromanches
Caen
SWORD
Airborne assault: Pegasus Bridge and Ranville
OMAHA
GOLD
JUNO
NORMANDY
ASSAULT FROM SEA
British & Canadian
US
ASSAULT FROM AIR
British & Canadian
US
Follow-up force
50 miles
BRITTANY
GERMAN 7th ARMY
F R A N C E


踩点
找漏洞
入侵系统
偷取数据
清理痕迹
业务克隆
伪装漏洞
虚拟系统
脱敏数据
行为记录
入侵检测
隔离攻击
司法取证
定位自然人

不是蜜罐，是思维升级

- 基于黑客攻击习惯，模拟一切会遭受攻击的目标
- 可以与核心业务互相嵌入，悄无声息转移攻击
- 节点间错综复杂，自动生成关联性，消耗攻击者时间

- 更积极的防御，让黑客主动暴露自己
- 以黑客的眼光看问题，从漏洞为中心到威胁为中心
- 第一次看清安全现状，可度量的精准威胁分析
- 精确响应，低运营成本，自动分析、取证、溯源

甲方安全的三个基本问题

- 我已经被黑了吗？是谁黑的？
- 有人正在尝试黑我们吗？他们是谁？用什么方法？
- 我们存在黑客也没有发现的安全问题吗？在哪里？

- 智能识别企业暴露资产，扫描发现漏洞和异常
  - IP、域名、业务系统、SEO关键词
  - 员工邮箱、手机、云盘、代码仓库
- 监控黑产群动态
- 监控业务舆情

和普通威胁情报有什么区别

- 不要全网范围打来打去的宏观层面的地图炮
- 不要呆萌的外部蜜罐捕获的大范围攻击的蠕虫病毒
- 根据企业业务量身定做的、精确量化企业自身威胁的、人能看懂的、可以采取下一步行动的情报

Q&A