
2020 CTIC
网络安全分析与情报大会
共生
Symbiosis
共进
Success
共享
Sharing

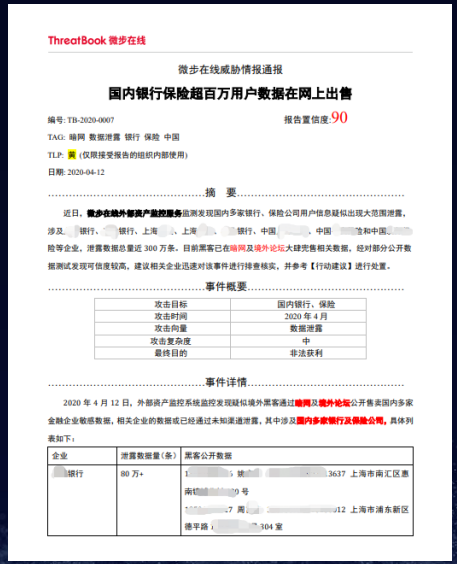
不容忽视的企业外部威胁

樊兴华

微步在线首席分析师

金融行业大规模暗网敏感数据泄露事件

- 十余家银行、证券、保险企业用户隐私数据泄露
- 通过暗网及地下黑客论坛售卖交易
- 涉及数据总量 300W条+
- 个别企业泄露数据至今仍在暗网售卖



ThreatBook 微步在线

微步在线威胁情报通报

国内银行保险超百万用户数据在网上出售

编号: TB-2020-0007　　报告置信度:90

TAG: 暗网 数据泄露 银行 保险 中国

TLP: 黄（仅限接受报告的组织内部使用）

日期: 2020-04-12

摘　要

近日，**微步在线外部资产监控服务**监测发现国内多家银行、保险公司用户信息疑似出现大范围泄露，涉及[redacted]银行、[redacted]银行、上海[redacted]、上海[redacted]、[redacted]银行、中国[redacted]、中国[redacted]洽和中国[redacted]险等企业。泄露数据总量近 300 万条，目前黑客已在暗网及境外论坛大肆兜售相关数据，经对部分公开数据测试发现可信度较高，建议相关企业迅速对该事件进行排查核实，并参考【行动建议】进行处置。

事件概要

攻击目标	国内银行、保险
攻击时间	2020 年 4 月
攻击向量	数据泄露
攻击复杂度	中
最终目的	非法获利

事件详情

2020 年 4 月 12 日，外部资产监控系统监控发现疑似境外黑客通过暗网及境外论坛公开售卖国内多家金融企业敏感数据，相关企业的数据或已经通过未知渠道泄露，其中涉及国内多家银行及保险公司，具体列表如下：

企业	泄露数据量（条）	黑客公开数据
[redacted]银行	80 万+	[redacted]3637 上海市南汇区惠南[redacted]9 号 [redacted]7 周[redacted]12 上海市浦东新区德平路[redacted]304 室

商品详情

交易市场 / 商品详情

(自动发货)3.5万个.[redacted]银行金卡名单

卖家:未激活隐藏

最后登陆:10分钟前

保障 平台担保 自动发货

无法联系卖家(您的账号还未激活)

类型 出售

分类 数据

收藏

已卖出 1

库存 99

3$(0.00032572BTC)

进入TA的店铺

数量

1

支付密码

请输入您的支付密码

可用余额

0

立即购买

暴马古道警示：谨防诈骗，请拒绝任何方式的站外交易，否则将失去暗网和平台的安全保障！

本栏目需要激活账号以后才能交易，您的账号还未激活，不能进行交易

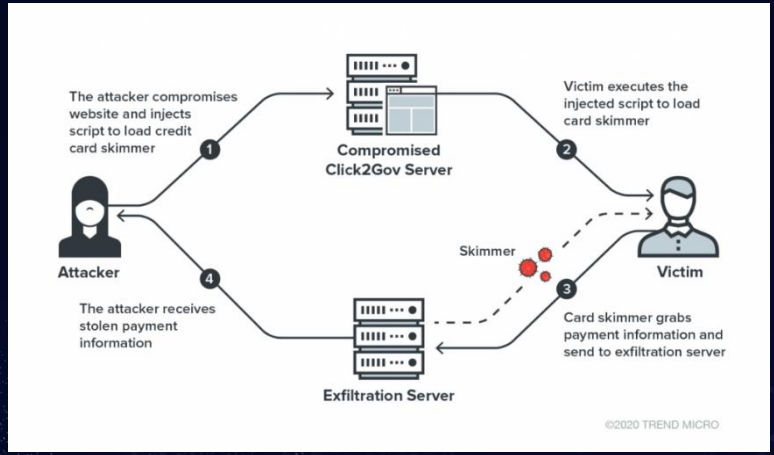
立即激活账号

产品详情

	A	B	C	D
1	开户银行	开户人	住所地址的	联系电话　通信地址
2	[redacted]银行	徐[redacted]	200120	13[redacted]7838 上海市临山路4
3	[redacted]银行	MA[redacted] A WA	200131	13[redacted]807 上海市张江高科
4	[redacted]银行	RO[redacted] SWIFT	200120	13[redacted]808 上海市浦东新区
5	[redacted]银行	王[redacted]君	201103	13[redacted]385 上海市嘉定工业

高级APT组织MageCart攻击活动

被攻击单位	攻击时间	备注
多个美国地方政府	2020.4	疑似经由**Click2Gov供应链入侵**
福布斯杂志	2019.5	疑似经由Picreel供应链入侵
美加200+校园商店	2019.4	经PrismRBS供应链入侵
新蛋网	2018.8	网站被篡改



备注：引用自趋势科技

某企业外部威胁分析

- 监控域名总量： 1.3k, 监控IP总量：814个；
- 待确认资产： 233个；
- 服务暴露事件： 6个；
- 数据泄露事件：48起；
- 暗网发现该企业用户的数据泄露事件4起；

企业面临的主要外部威胁

01 数据泄露

- Github敏感信息泄露
- 暗网论坛敏感信息泄露
- 网盘敏感信息泄露

02 未知资产

- 影子资产
- 资产变动

03 资产风险

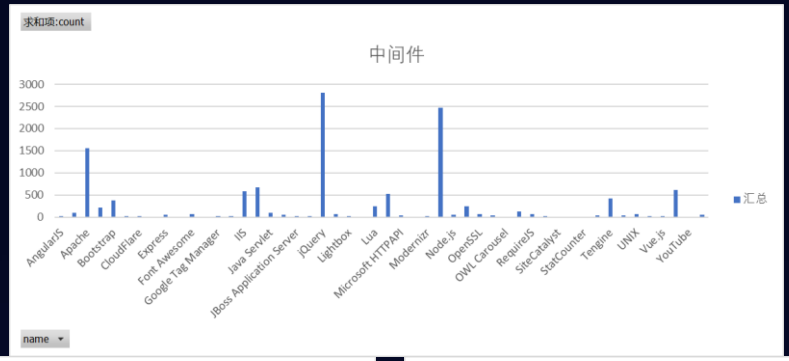
- 漏洞未修补
- 域名被仿冒
- 服务/端口开放公网

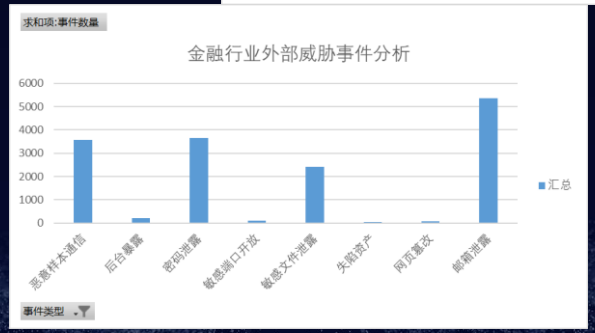
04 资产威胁

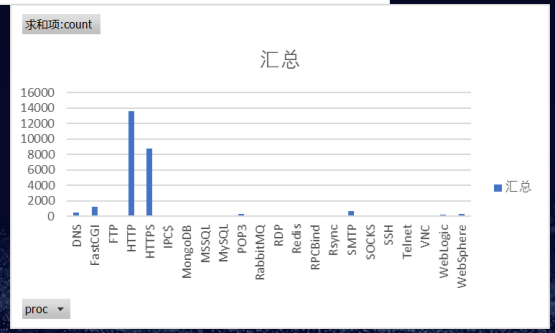
- 网站挂马&篡改
- 内网终端失陷

金融行业外部威胁态势分析

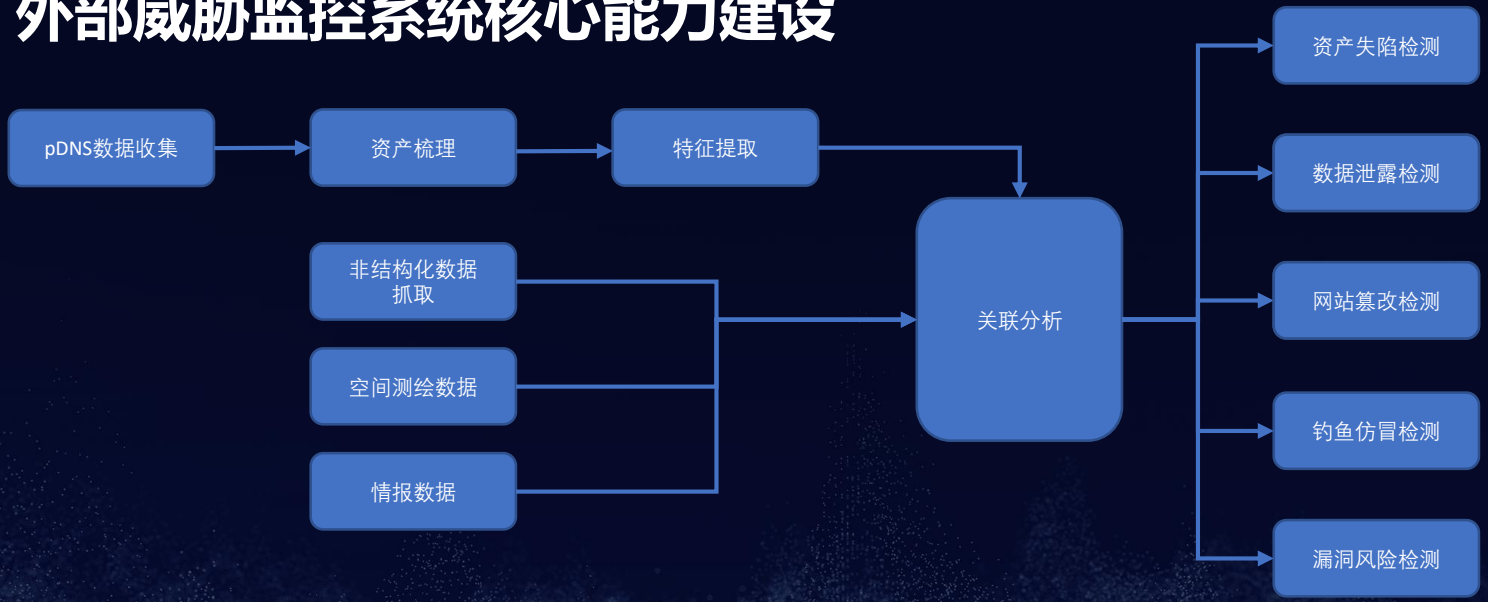
- 监控域名总量：400+， IP： 1W余个
- 威胁方面，数据泄露相关风险较为突出，比如暗网数据泄露、github敏感信息泄露以及邮箱泄露等问题
- 资产方面，中间件暴露较为突出，包括数据库类以及MQ、VNC等高危服务。



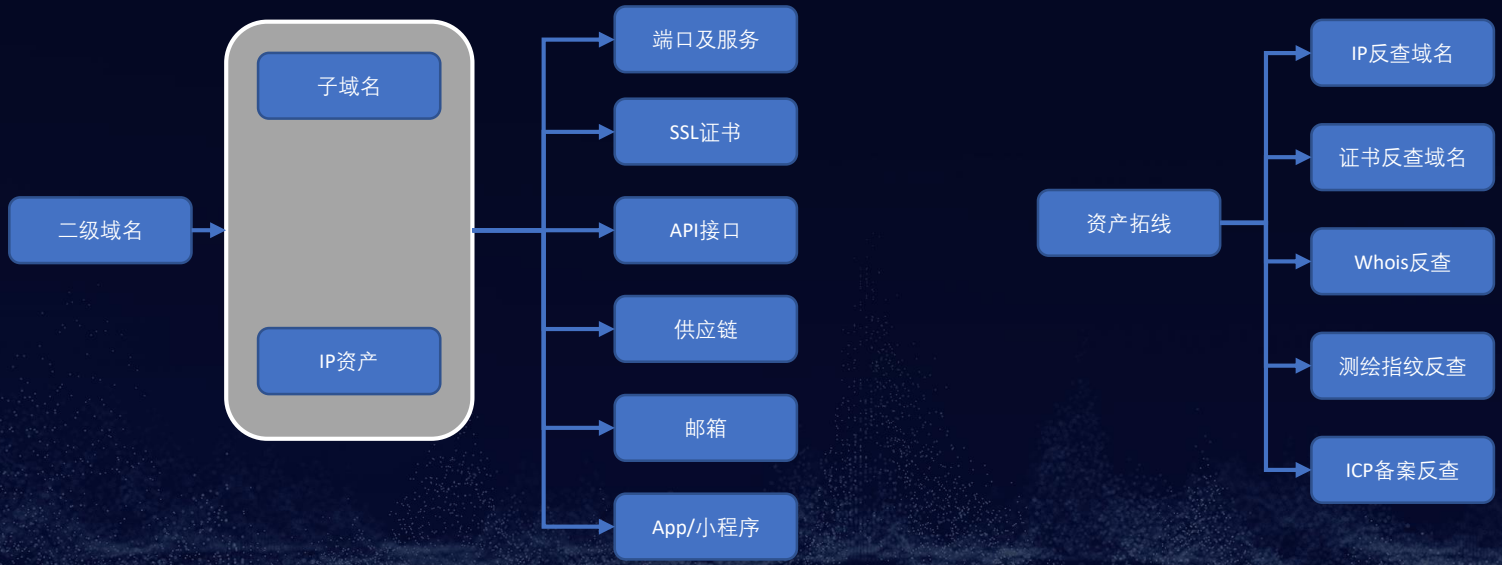




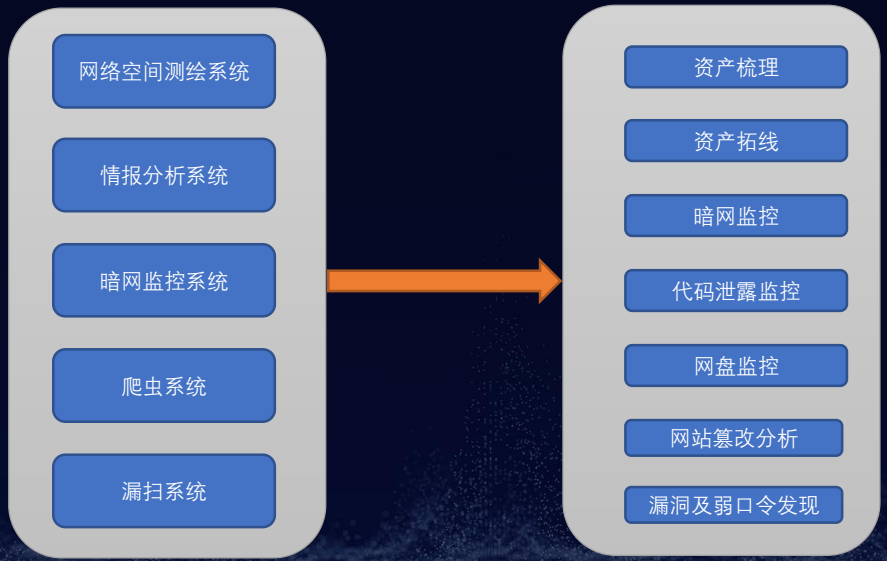
外部威胁监控系统核心能力建设



外部威胁监控系统核心能力建设 – 资产梳理

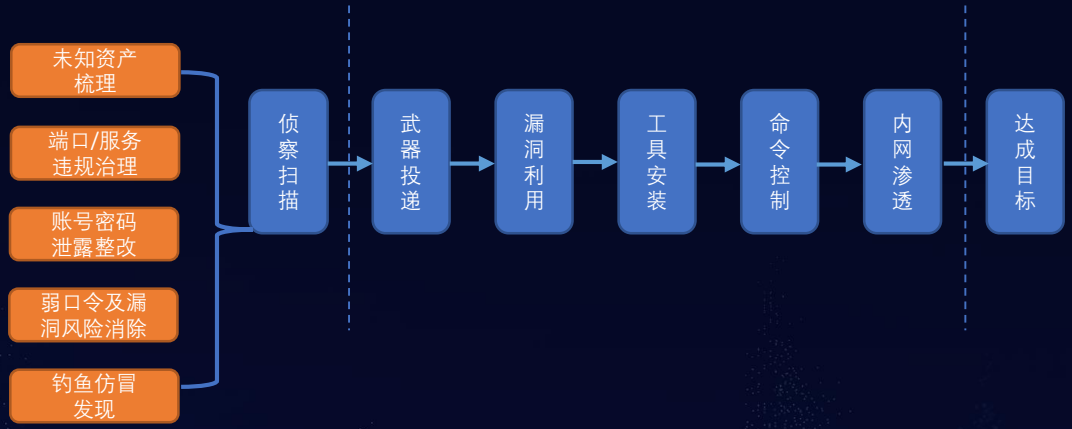


外部威胁监控系统核心能力建设 – 核心系统

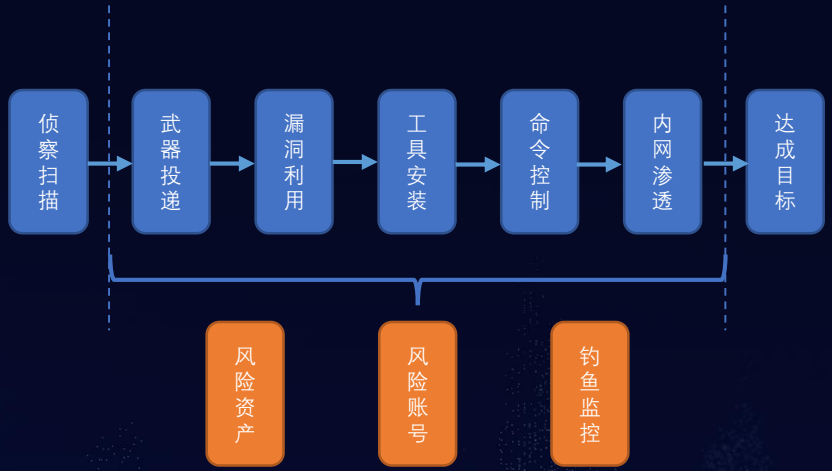


外部威胁监控能力是企业安全体系不可或缺的组成

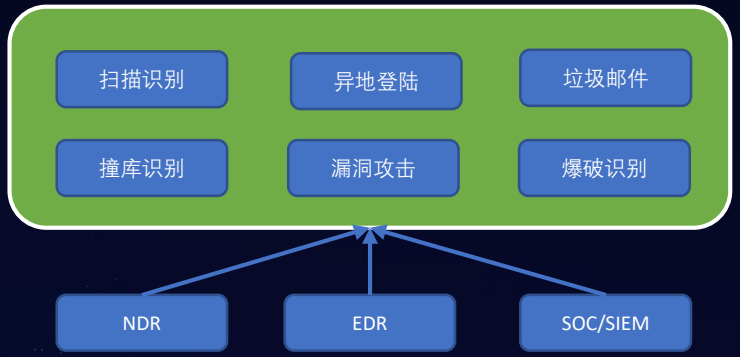
外部威胁监控能力是企业安全体系不可或缺的组成



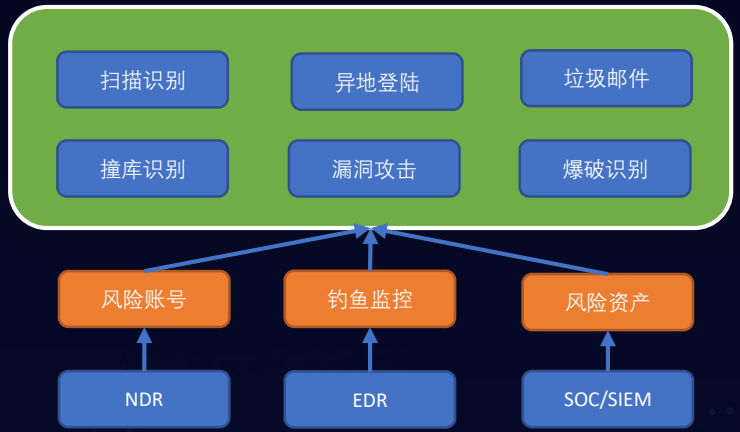
外部威胁监控能力是企业安全体系不可或缺的组成



外部威胁监控能力是企业安全体系不可或缺的组成

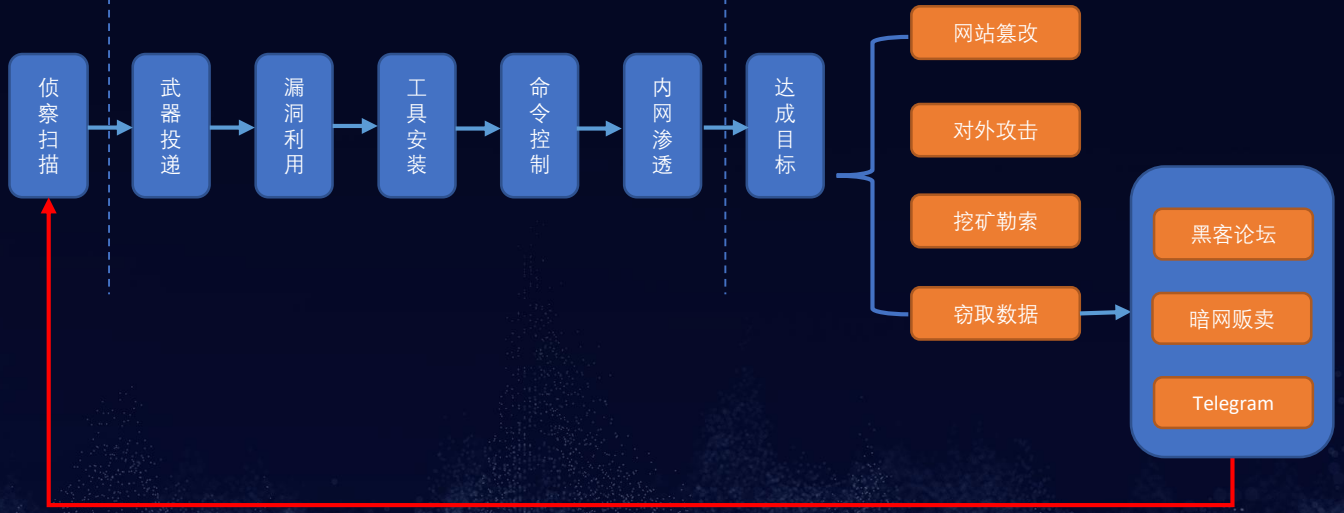


误报高

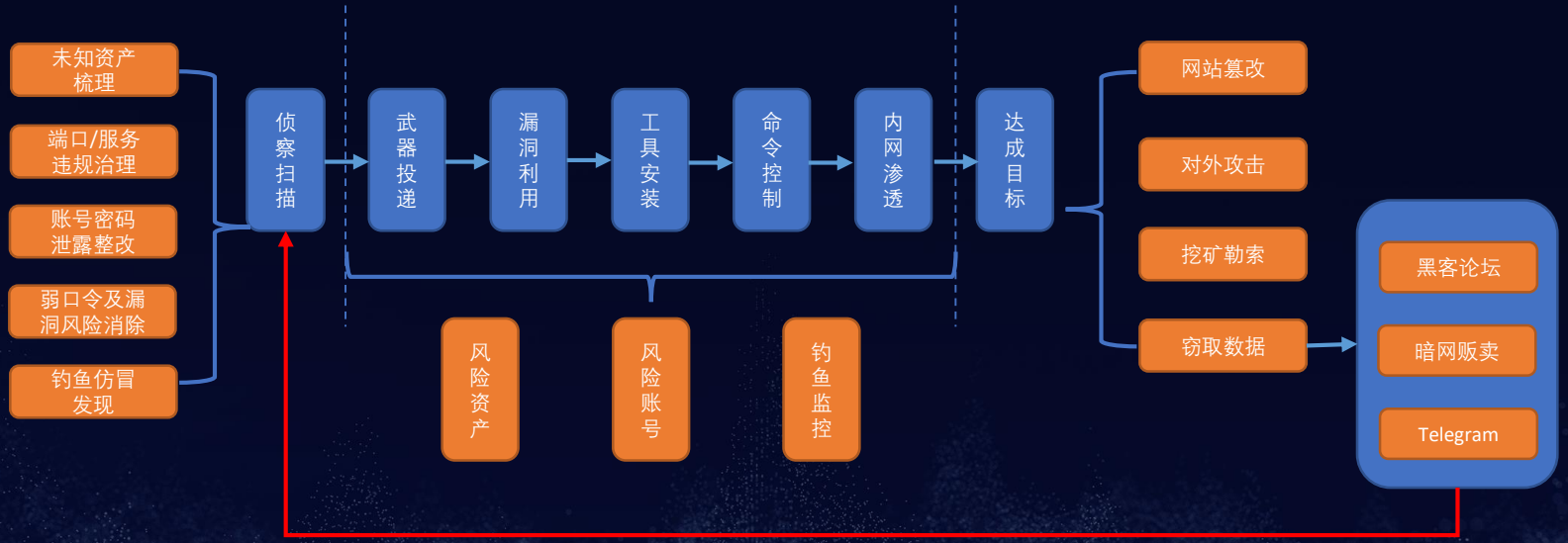


误报低

外部威胁监控能力是企业安全体系不可或缺的组成



外部威胁监控能力是企业安全体系不可或缺的组成



Thank you