2019第三届顺丰信息安全峰会

2019 THE 3rd SF INFORMATION SECURITY SUMMIT

找到那些躲在暗处的敌人

央视网威胁管理体系建设

黄乐

央视网 网络安全部 副总监

黑暗年代

痛点

入侵无感知

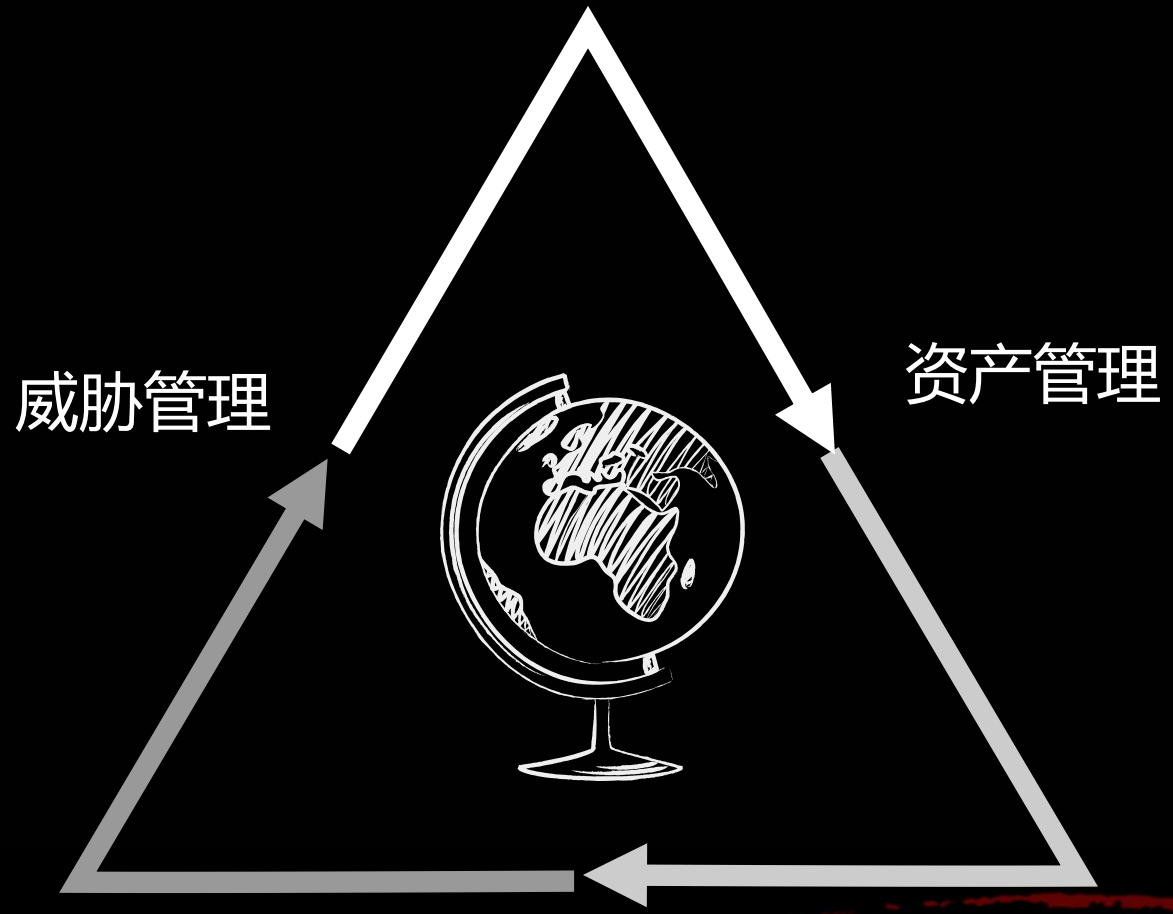
事后压力大

工作没数据

全年重保期

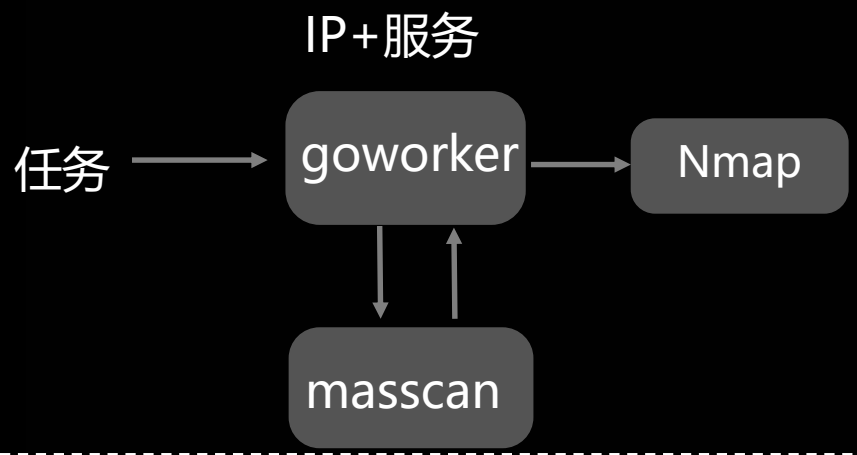
风险管理

风险管理



资产发现

主动



URL

改造Pholcus

被动

离线：DPI+kafka+ELK+策略

Or

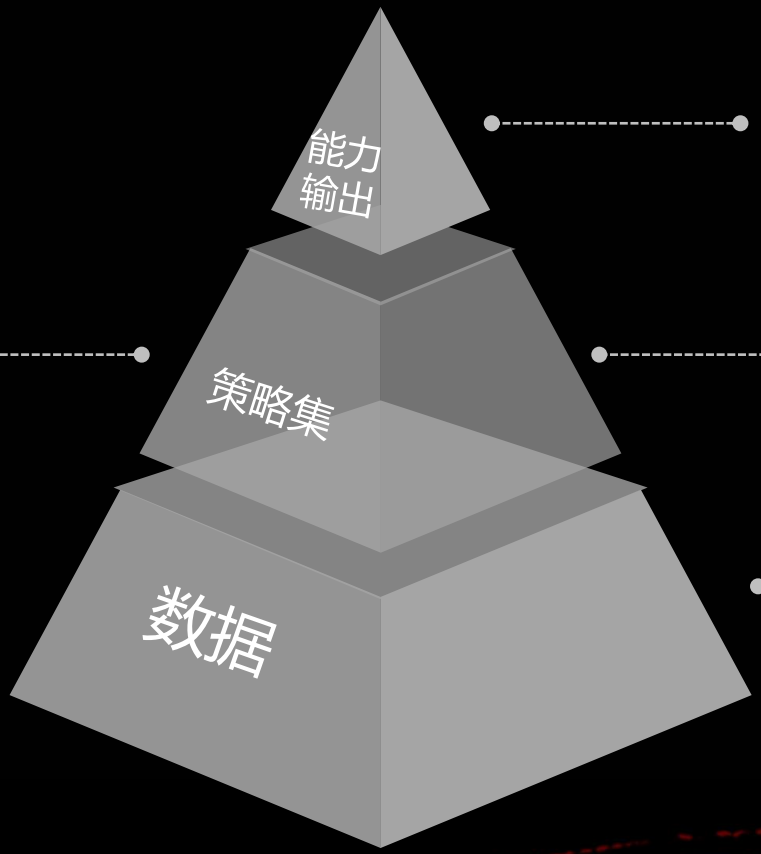
在线：流量+storm+策略

脆弱性管理


央视网漏洞治理系统
cctv.com vulnerability management system
1028
总发现漏洞数
72
紧急
407
高危
157
中危
383
低危
56
未修复漏洞总数
2
未修复:紧急
39
未修复:高危
8
未修复:中危
7
未修复:低危
漏洞平均修复时间分布
30-90天 (17.17%)
90-180天 (8.58%)
180天以上 (9.51%)
1-3天 (11.37%)
1天内 (4.87%)
3-7天 (11.14%)
7-30天 (37.36%)
未修复漏洞趋势图
紧急
高危
中危
低危
总数
100
80
60
40
20
0
03-07
03-09
03-11
03-13
03-15
03-17
03-19
03-21
未修复漏洞状态分布
整改未完成
整改中
复查中
未修复漏洞类别分布
TOP 10
A9-使用含有已知漏洞的组件
A5-安全配置错误
A2-失效的身份认证和会话管理
A4-失效的访问控制
A6-敏感信息泄露
A8-跨站请求伪造
A1-注入
A7-攻击检测与防范不足
0
5
10
15
20
25
30
未修复业务部门分布
紧急
高危
中危
低危
信息泄露
18个
15个
12个
9个
6个
3个
0个
移动开发中心
技术运维中心
用户数据运营中心
视频技术中心
平台技术中心
视影音开发运营中心
中视广信
韦画频道
康创联盟
IT支持组
党员网技术部
共产党员网事业部
国际传播事业群

威胁管理

逻辑



- 指导决策 、综合展示
- 应急处置、封堵

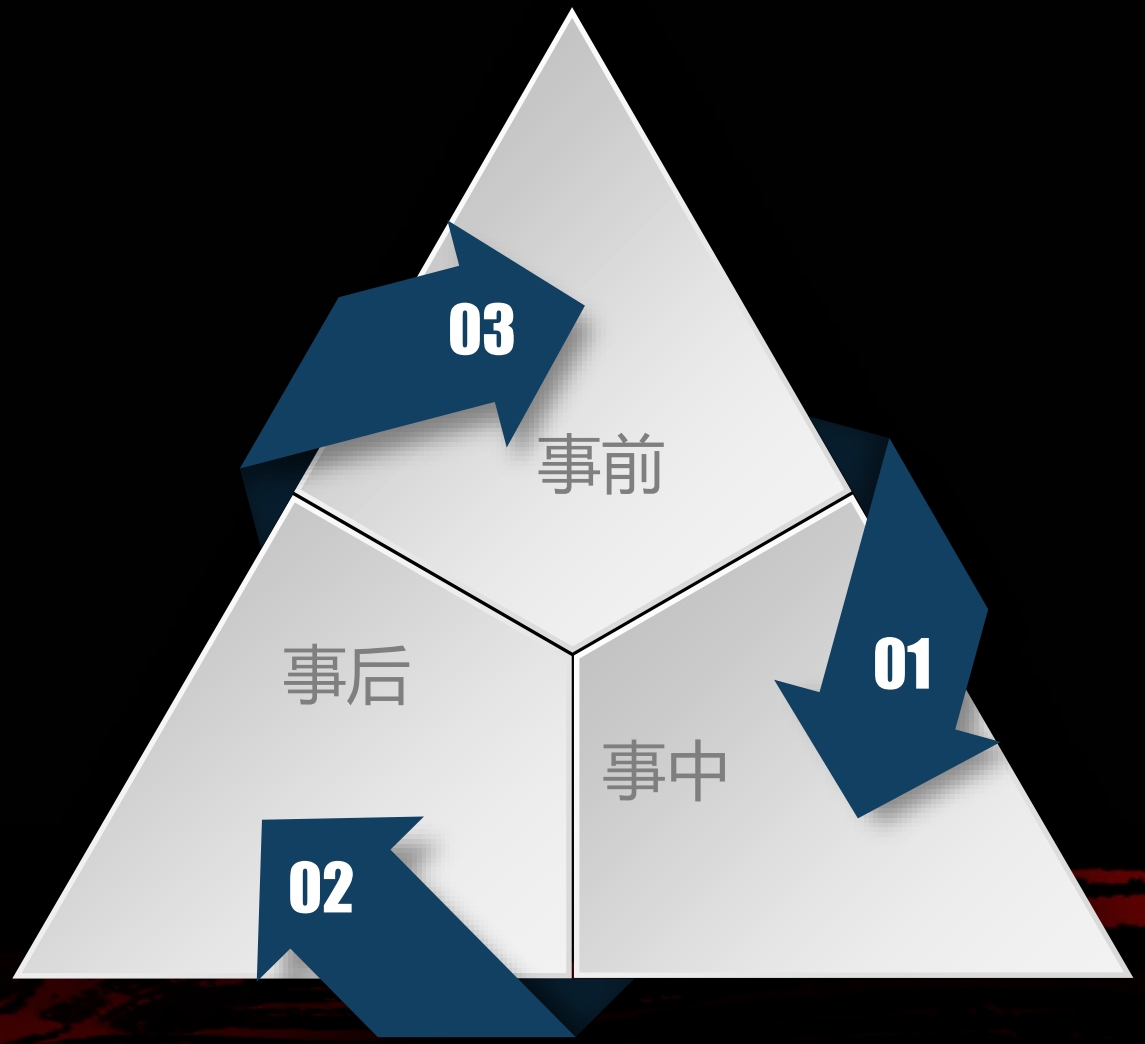
- 不浪费任何一次应急
- 安全服务落地

- 快速达到及格线
- 逐步完善

- 内部数据
- 外部情报

事前成本太高　　事后为时已晚

逻辑



数据

根据数据找需求 

根据需求找数据 

策略集--合作方式

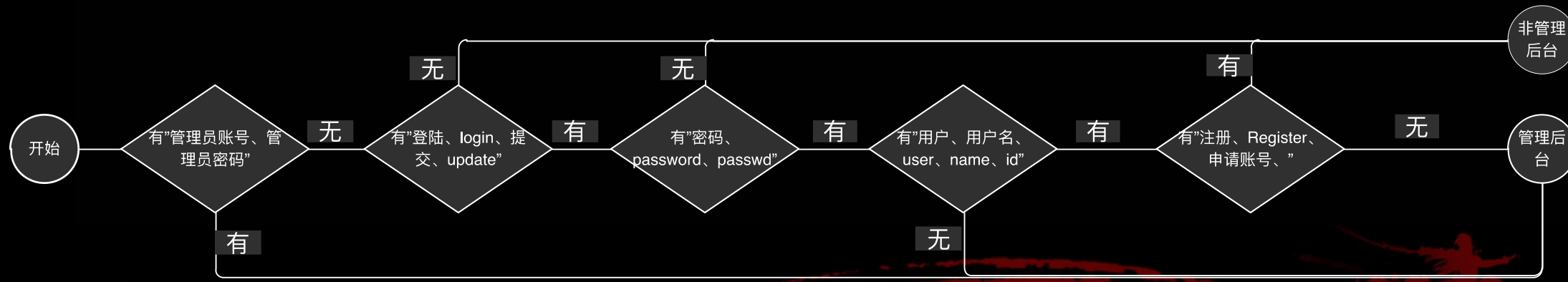
不能完全的买买买

也没有条件展开大规模自主研发

策略集举例--管理后台发现

主动扫描　　爬虫 + 字典 = 高准确率 + 高漏报

被动分析



展现

基于分析结果的多层展示，方便各个层面的员工和领导实用。

高层

能看懂

别炫技

中层

效率高

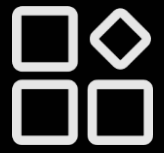
别造假

基层

可定制

别复杂

番外篇--联动



缩减时间

最大限度的缩减从威胁发现到封堵的时间。

避免误操作

威胁处置涉及到对设备大量的操作，避免误操作非常重要。

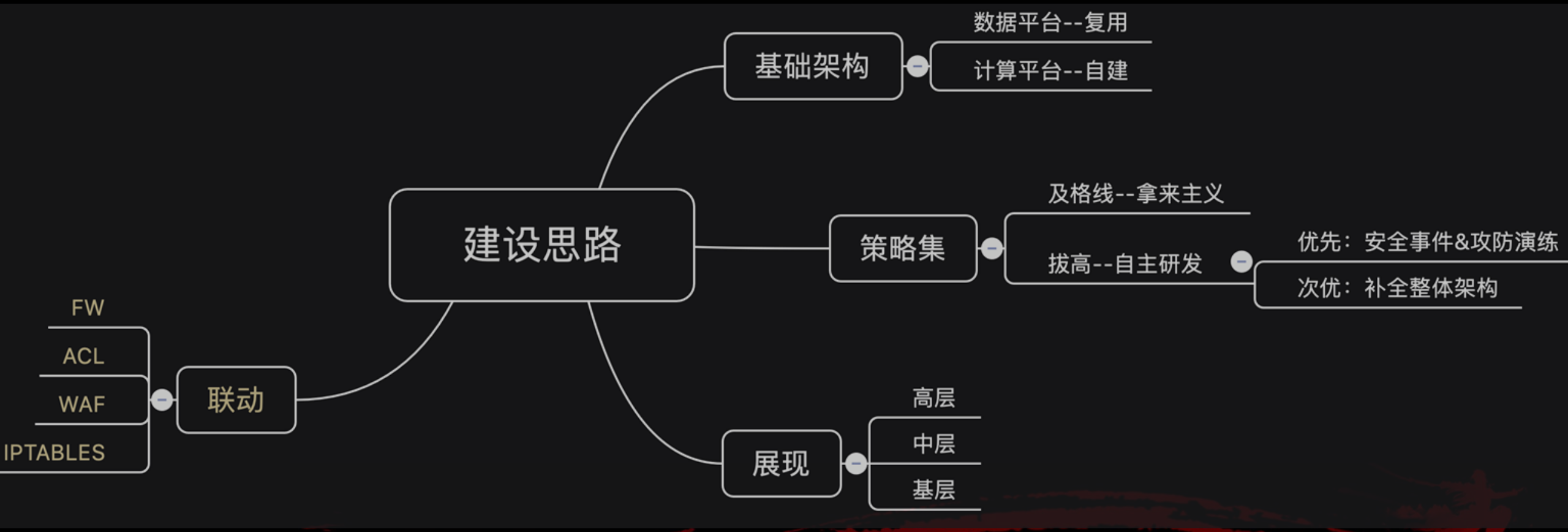
7*24小时工作

不知道黑客什么时间工作，我们需要不用睡觉的机器人。

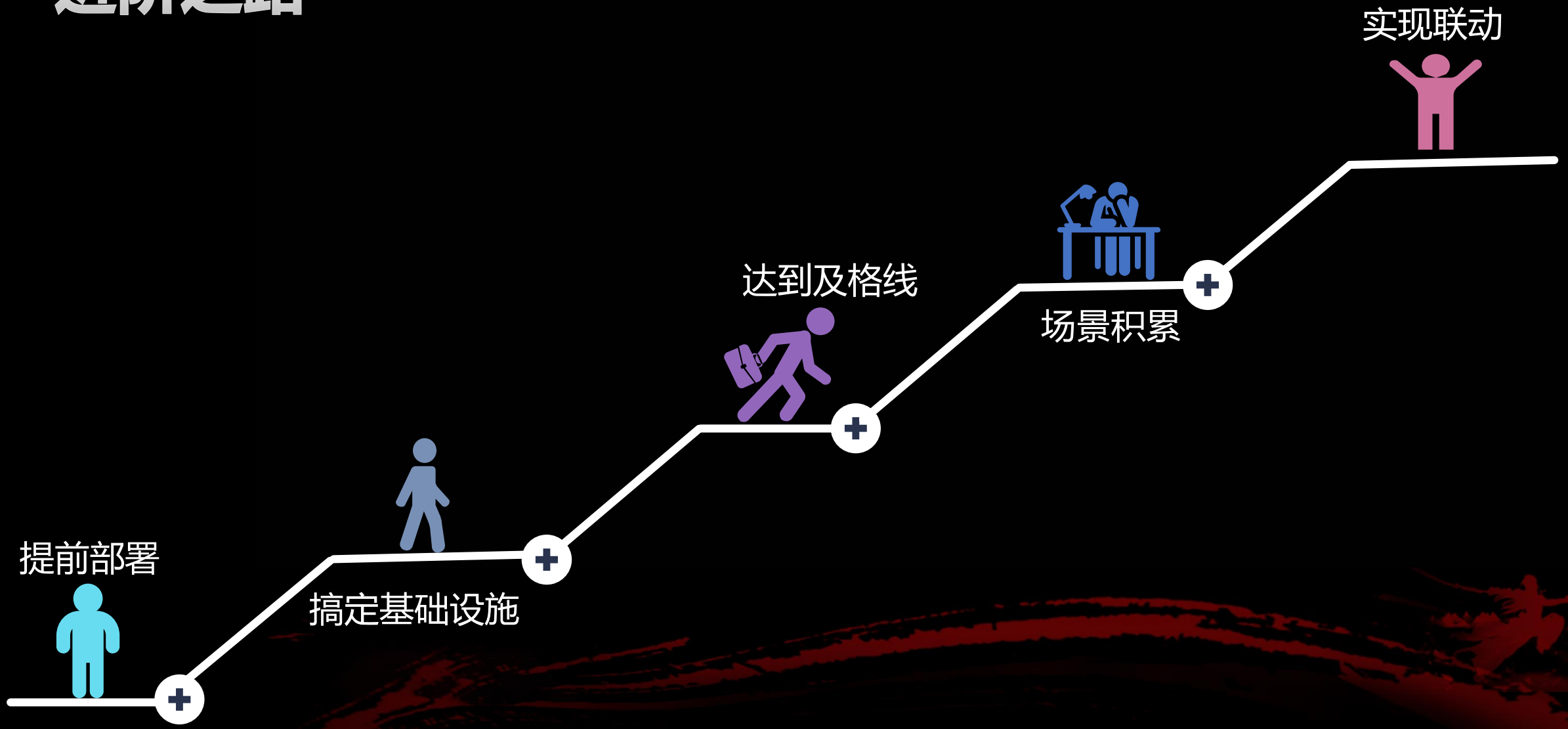
联动严格上不是威胁感知体系内的能力模块，但没有联动威胁感知就变成了镜花水月。

回看

建设思路


建设思路
基础架构
数据平台--复用
计算平台--自建
策略集
及格线--拿来主义
拔高--自主研发
优先：安全事件&攻防演练
次优：补全整体架构
联动
FW
ACL
WAF
IPTABLES
展现
高层
中层
基层

进阶之路



THANK YOU