移动威胁情报安全生态实践分享

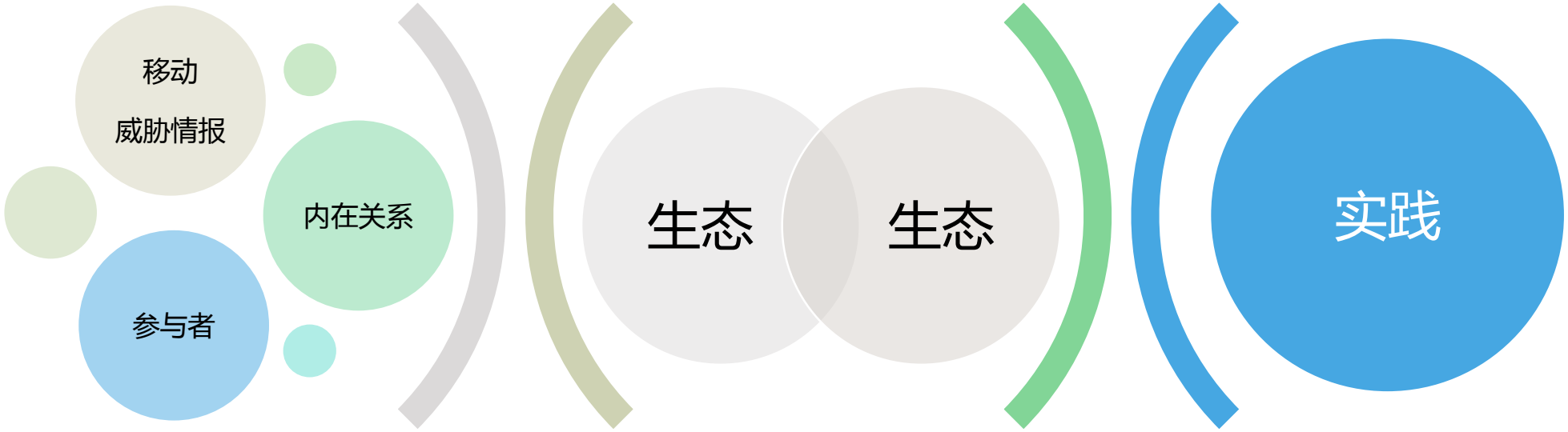
Tom:Pan（潘宣辰）

移动安全·安天

自我介绍——来自安天AVL移动安全

- 潘宣辰，Tom:Pan
  - 安天移动安全团队 Founder&Leader
- 技术涉猎较广，主攻手机恶意代码取证，手机反病毒引擎和自动化分析技术，以及移动网络安全。
- tompan@antiy.cn

标题的解读和提纲



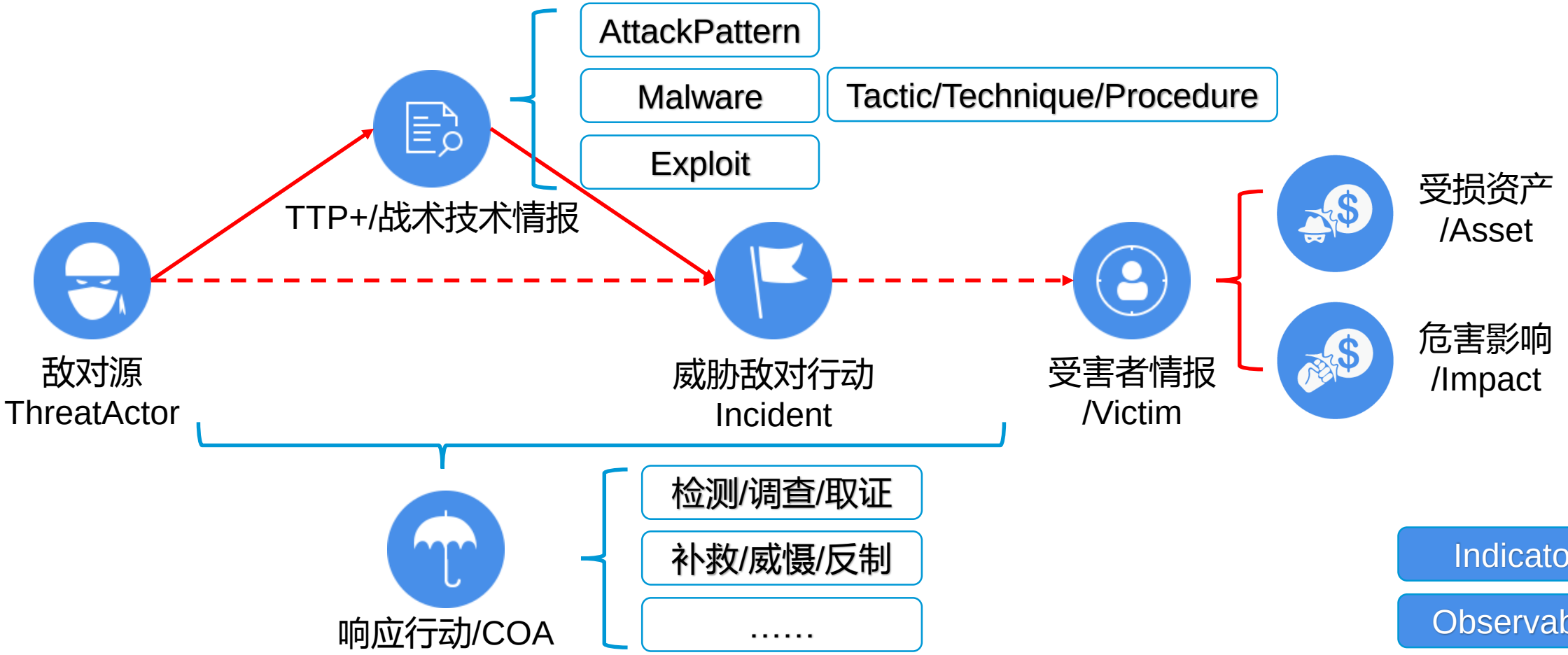
移动威胁情报视角　　生态的内在分析　　实践的分享

威胁情报视角

相关的概念体系	出现的背景
Threat/Risk/Exposure/Asset……	西方的IT管理和标准化的背景
DREAD,STRIDE,PASTA, Attack Tree……	微软和相关安全厂商所推出的风险管理模型
CAPEC,CWE,CVE,CVRF，MAEC，NVD……	对攻击模式，脆弱点，漏洞等各种基础的安全元素的标定和描述结构
Threat Modeling	各种威胁建模的方法论，工具，risk-centric，data-driven等等
Kill Chain,钻石分析,TTP……	面向Cyber和更高强度的攻击和对抗的场景的分析工具和分析方法
CybOX,TAXII，OpenIOC……	面向Cyber和信息交换的描述和标准体系
STIX	面向更完整的综合性的情报分析/作业/交换的体系

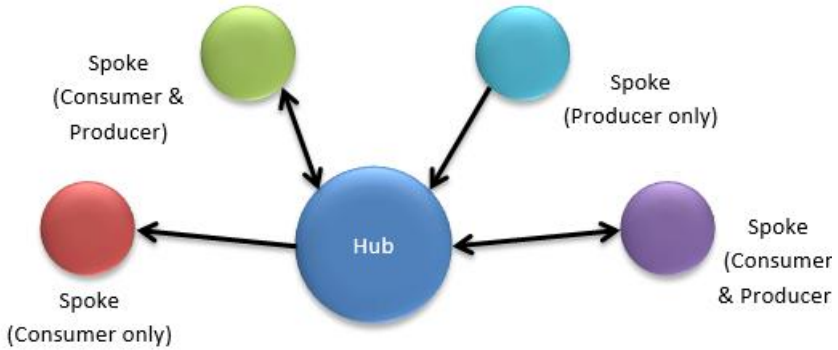
威胁情报视角之STIX

Structured Threat Information eXpression (STIX™)

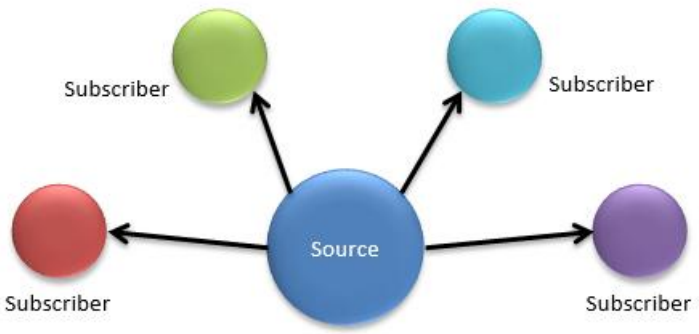


威胁情报视角之TAXII

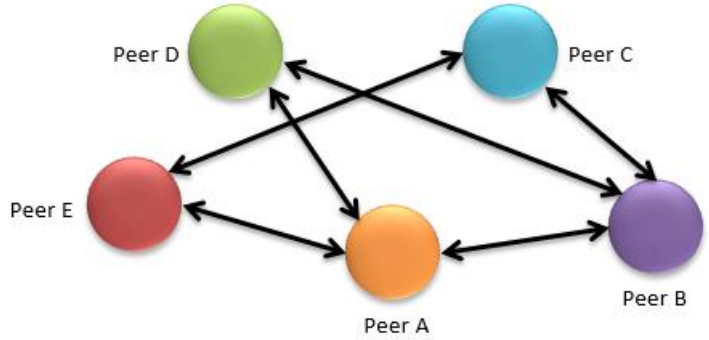
The Trusted Automated eXchange of Indicator Information (TAXII™)



Hub and Spoke



Source/Subscriber



Peer to Peer

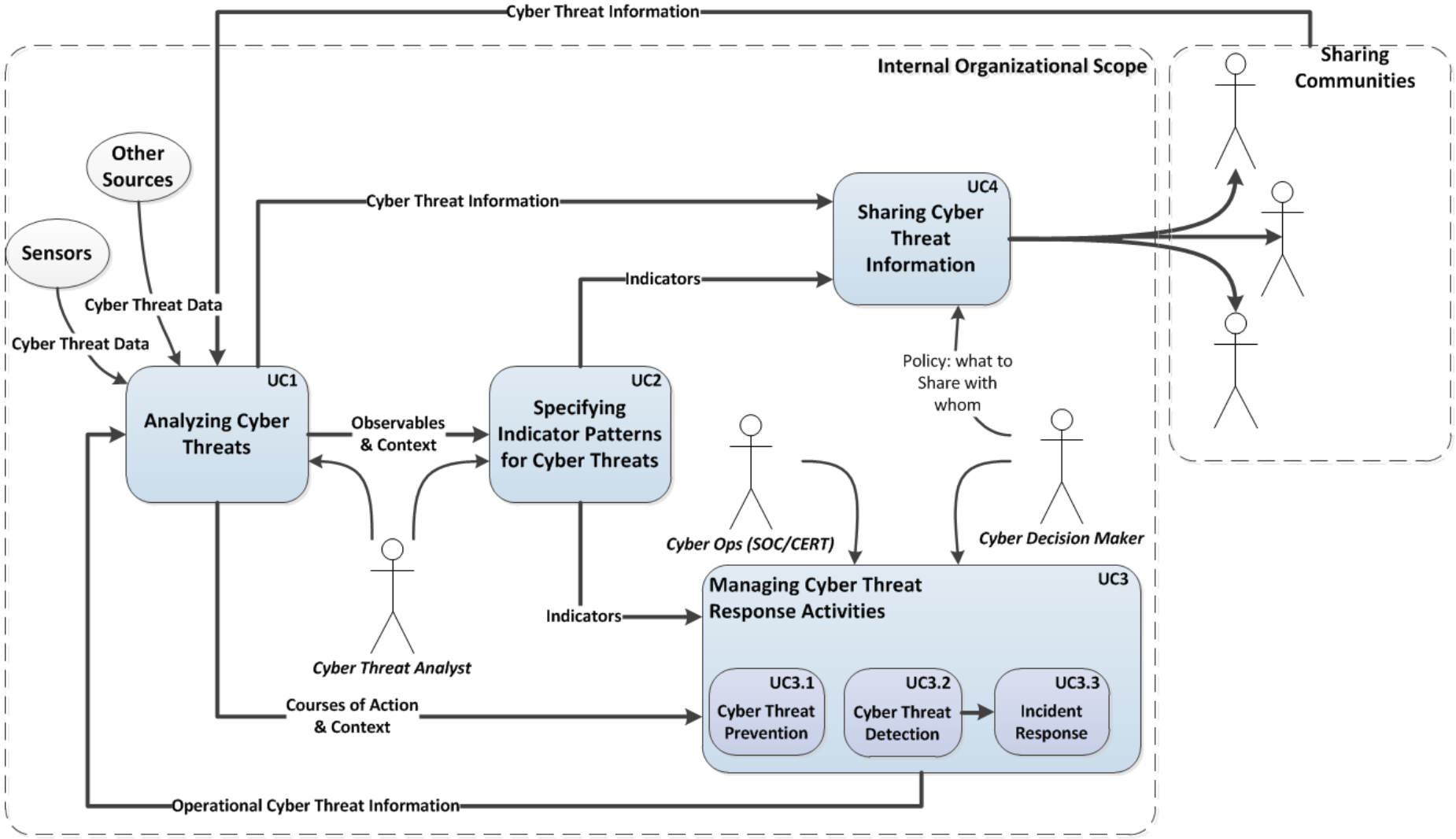
PULL → PUSH → DISCOVERY → QUERY

威胁情报视角来映射

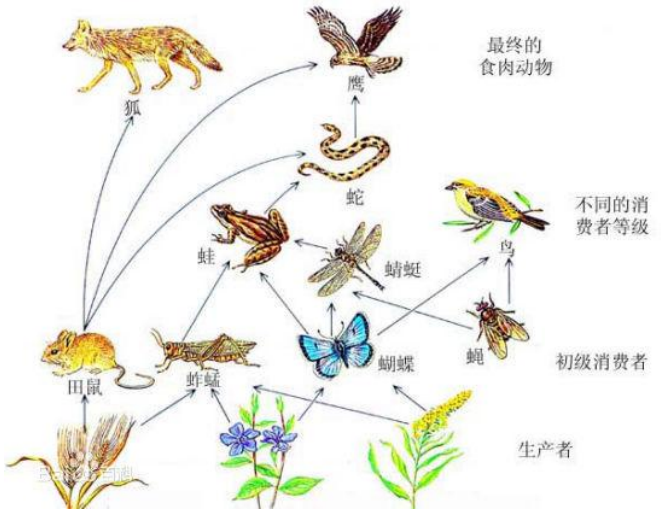
- STIX解决的是描述语言统一的问题
- TAXII解决的是交流习惯一致的问题

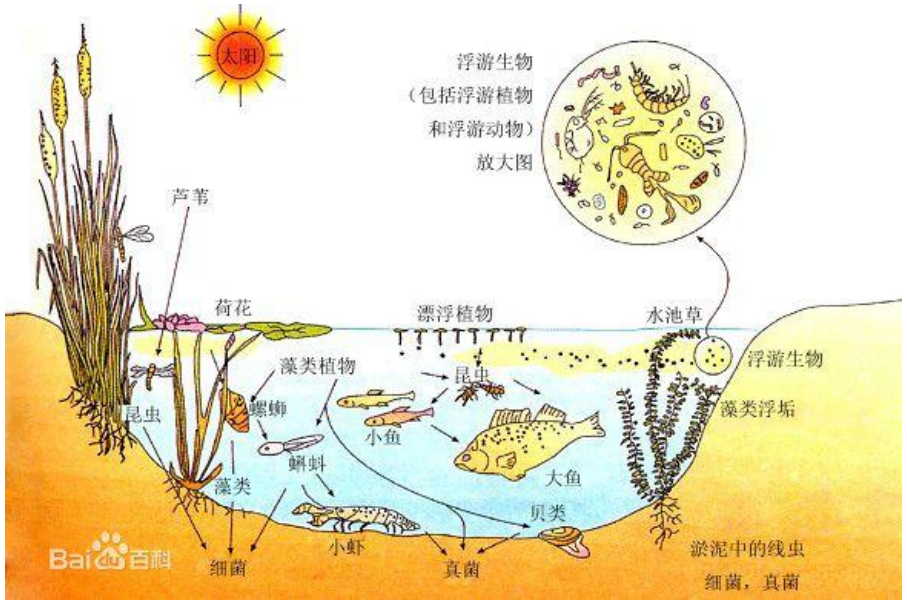
WHO：参与的角色？WHAT角色之间的关系和方式

威胁情报视角来映射


Cyber Threat Information
Internal Organizational Scope
Sharing Communities
Other Sources
Sensors
Cyber Threat Data
Cyber Threat Data
Cyber Threat Information
Indicators
UC4
Sharing Cyber Threat Information
Policy: what to Share with whom
UC1
Analyzing Cyber Threats
Observables & Context
UC2
Specifying Indicator Patterns for Cyber Threats
Cyber Ops (SOC/CERT)
Cyber Decision Maker
Cyber Threat Analyst
Indicators
Managing Cyber Threat Response Activities
UC3
UC3.1
Cyber Threat Prevention
UC3.2
Cyber Threat Detection
UC3.3
Incident Response
Courses of Action & Context
Operational Cyber Threat Information

生态的一些定义和概念

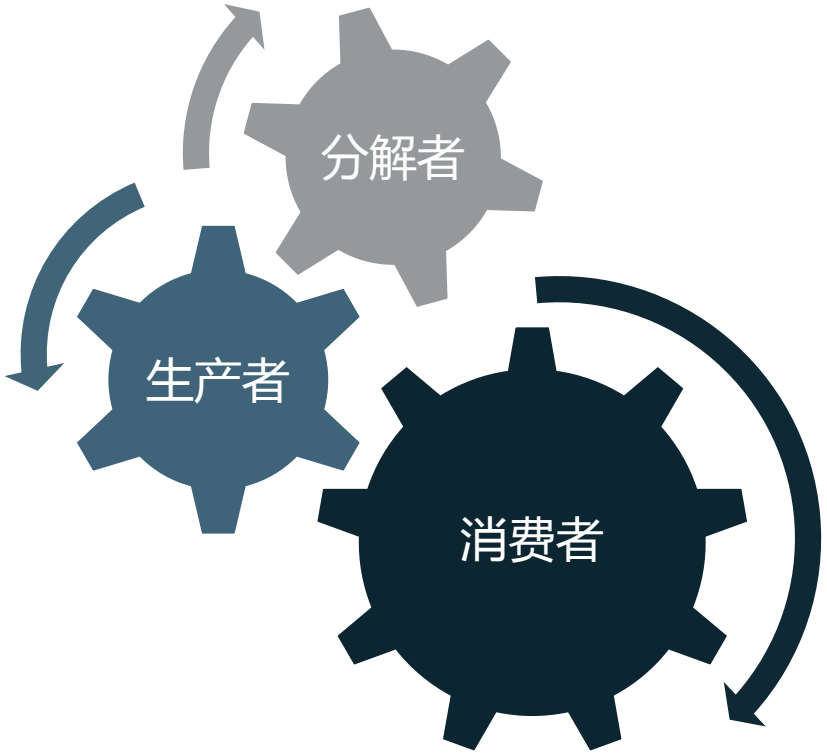


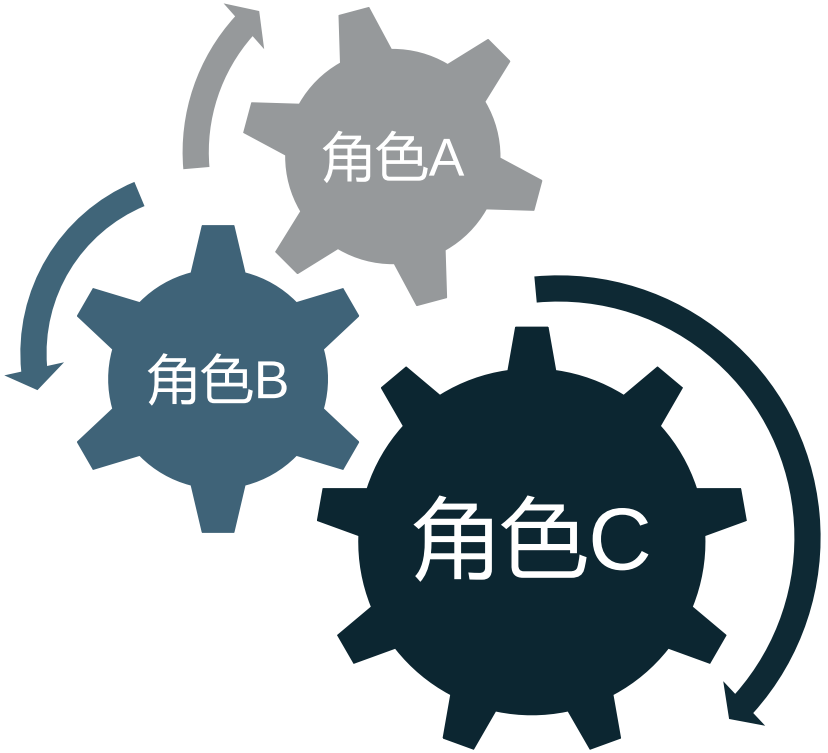


自然生态系统

人工生态系统

生态的一些定义和概念





多样性

动态平衡

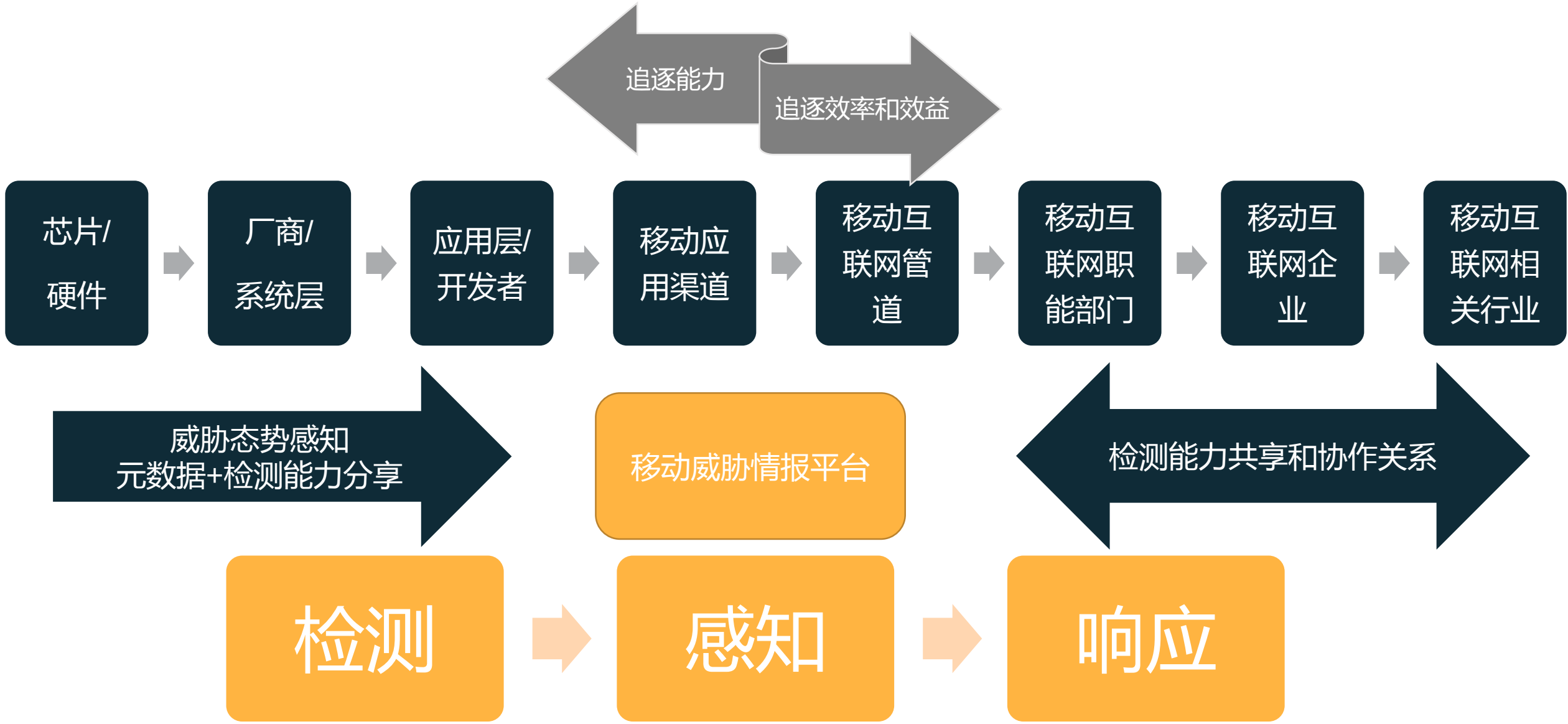
自然生态系统

人工生态系统

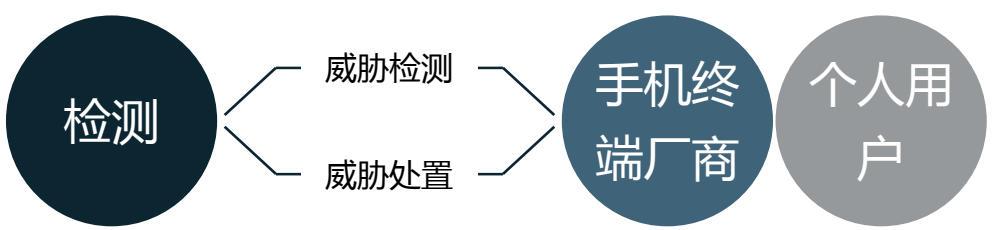
干预&易变&依赖

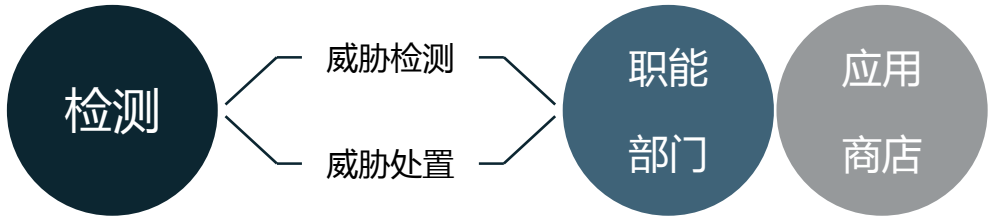
目的性

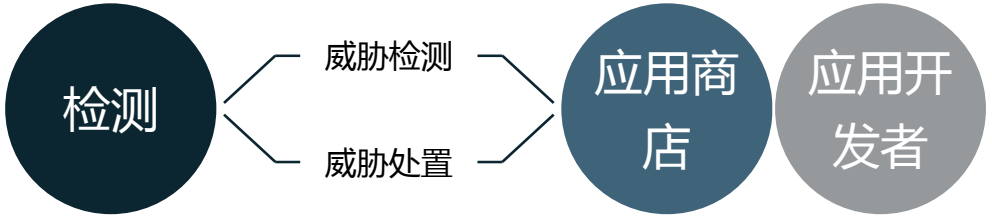
移动安全生态实践的分享

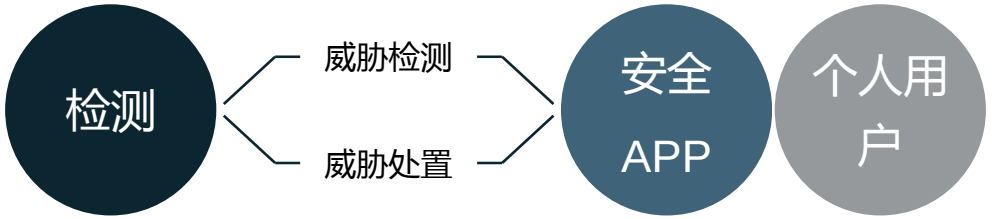


移动安全生态实践的分享









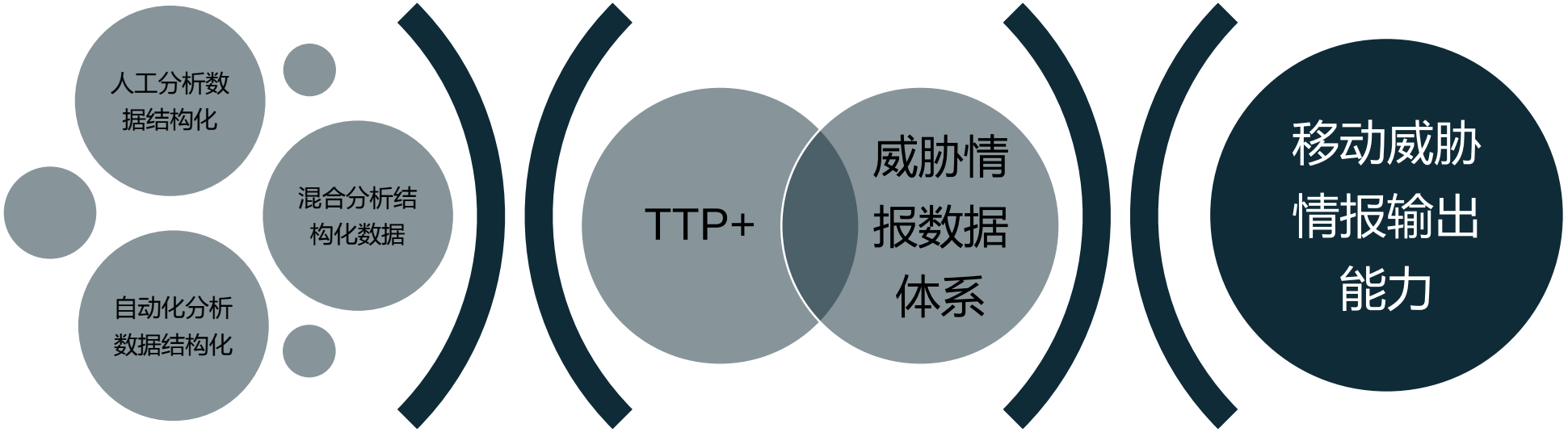
移动安全生态实践的分享

广度

层次

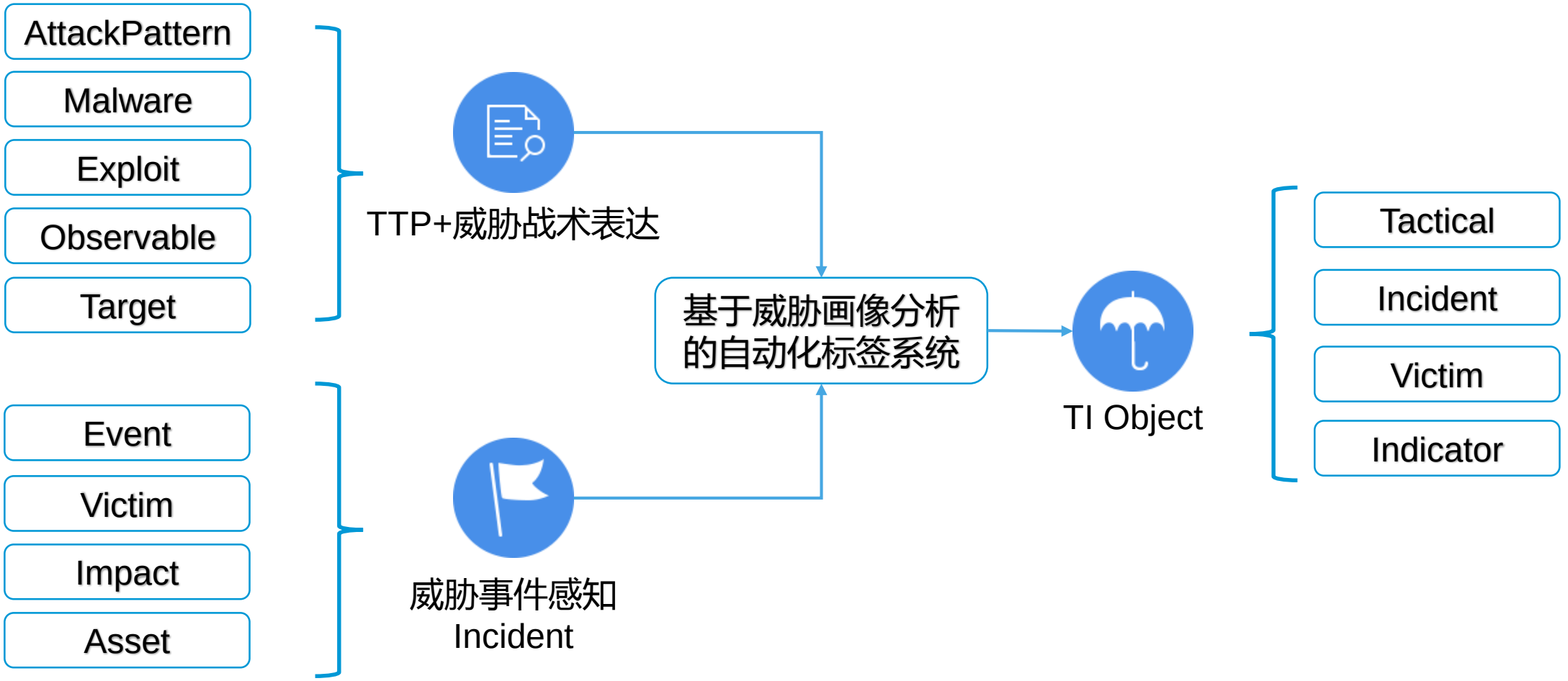
质量

移动安全生态实践的分享——数据体系

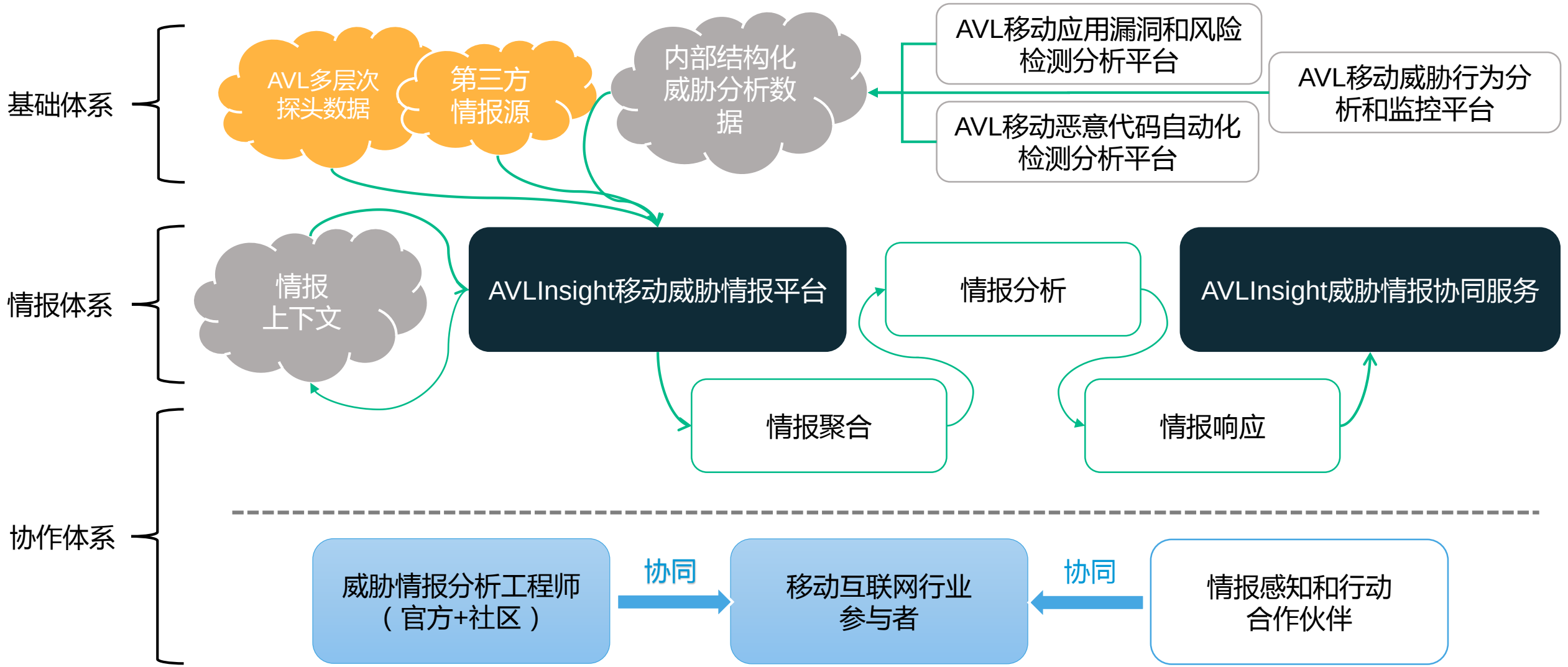


AVML	AEngLog	TTP+	TI Object	TI Service
2010年开始 全库样本集合范围	2013年开始 终端引擎范围	2015年开始 高级或针对性威胁范围	2015年末开始 面向情报输出和服务能力定制化输出	

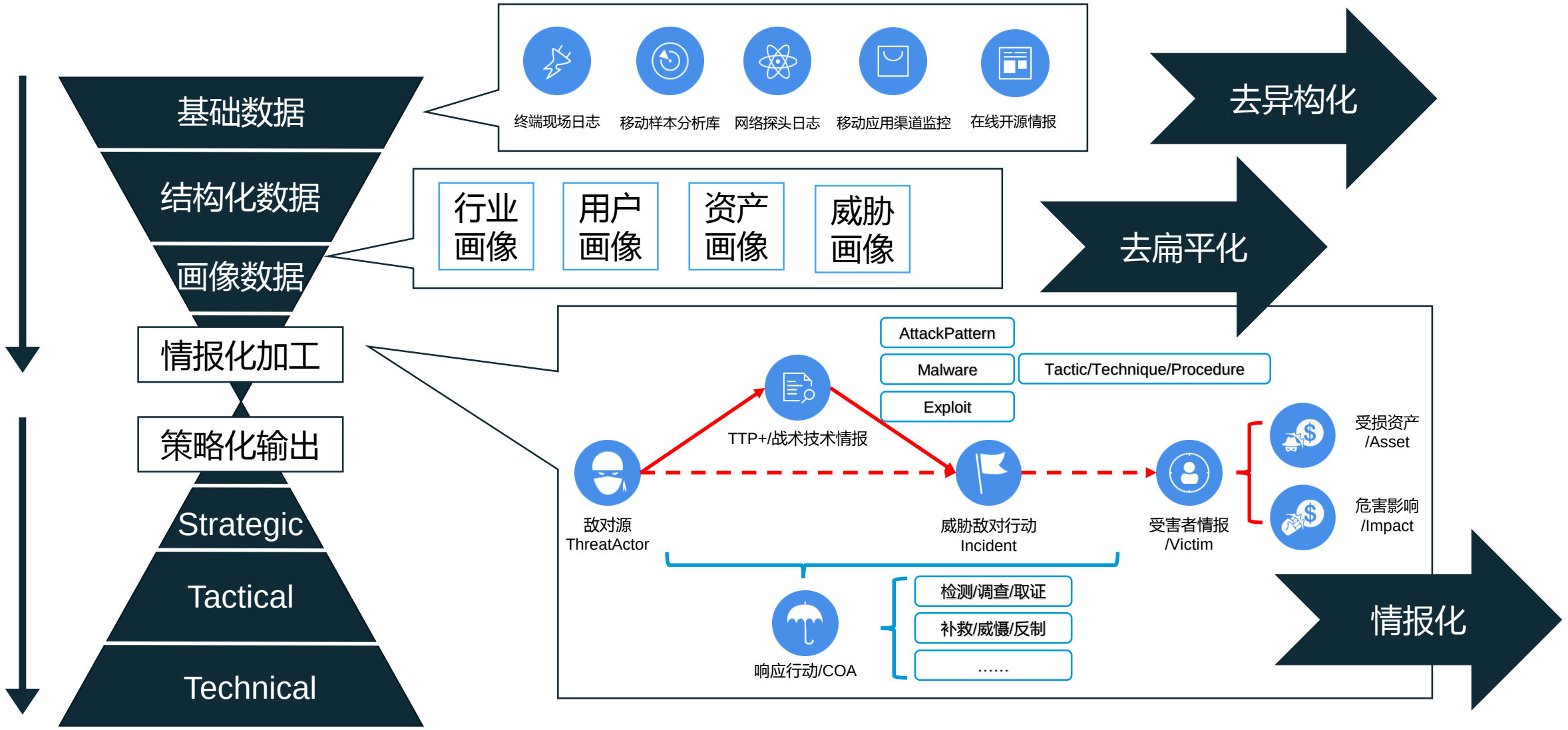
移动安全生态实践的分享——计算体系



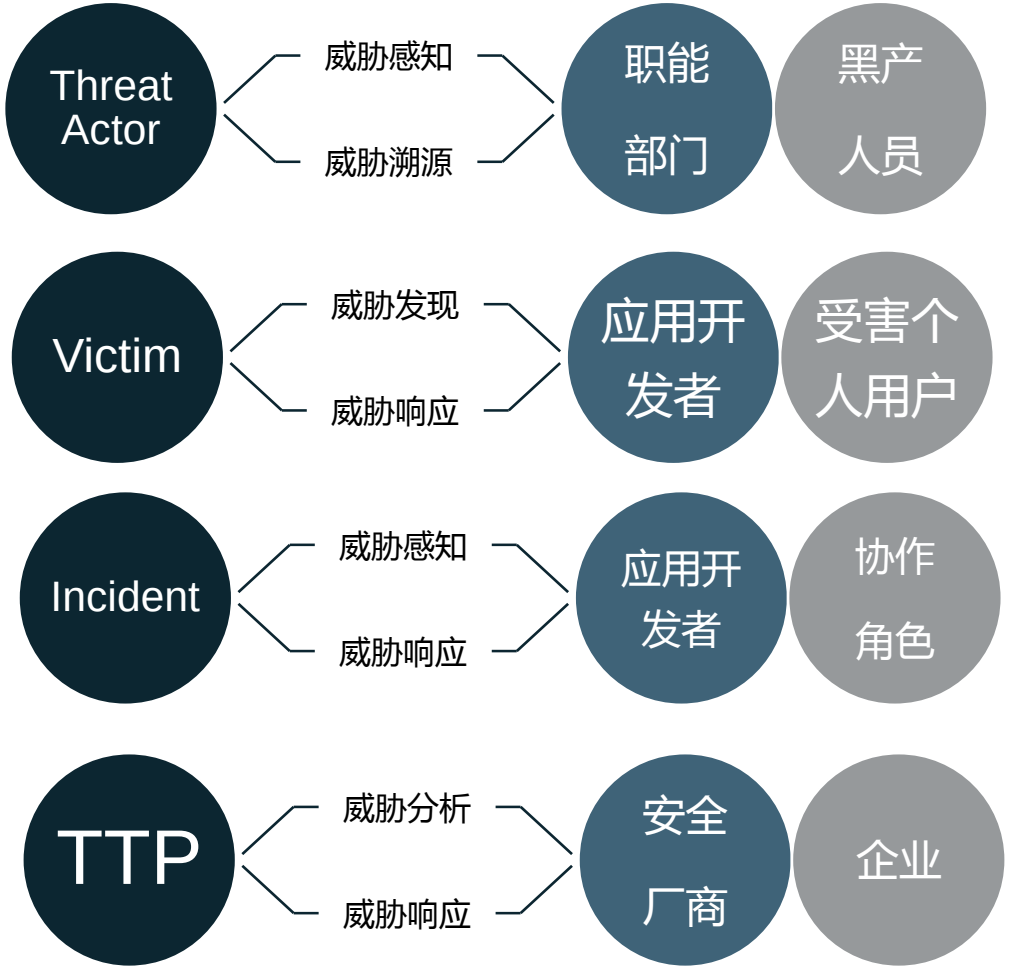
移动安全生态实践的分享——协作体系



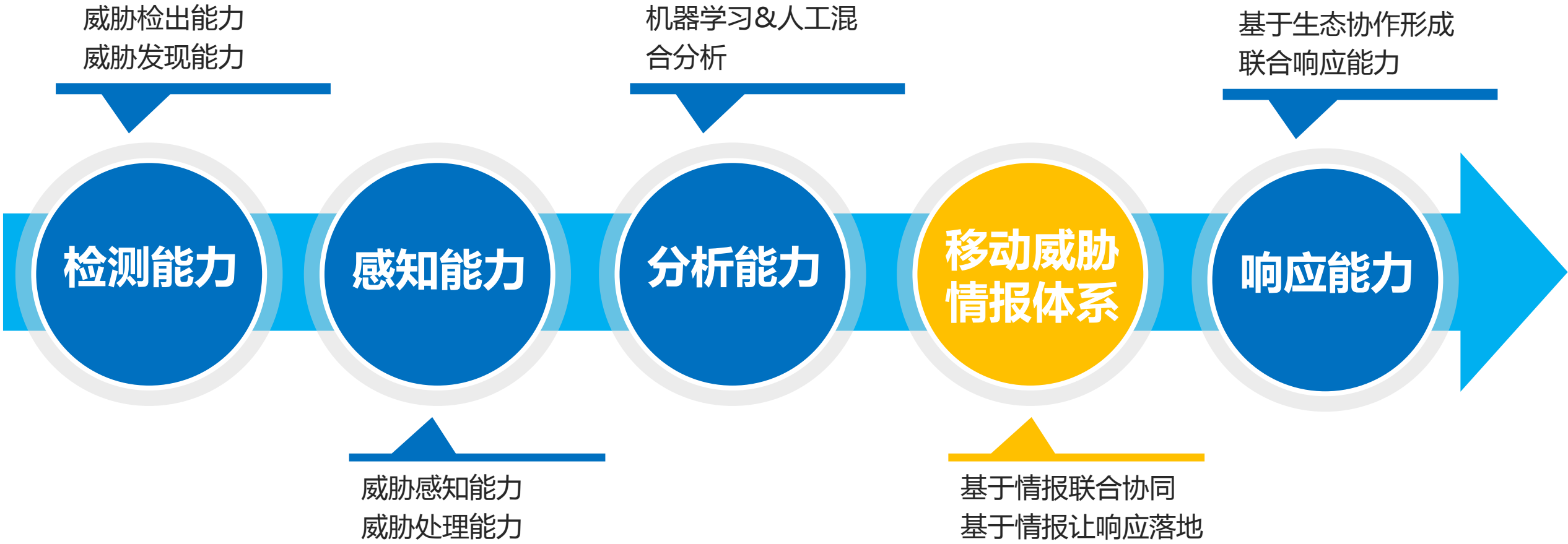
移动安全生态实践的分享——整体架构



移动安全生态实践的分享——生态能力升级



移动安全生态实践的分享



THANKS!

AVL 移动安全·安天