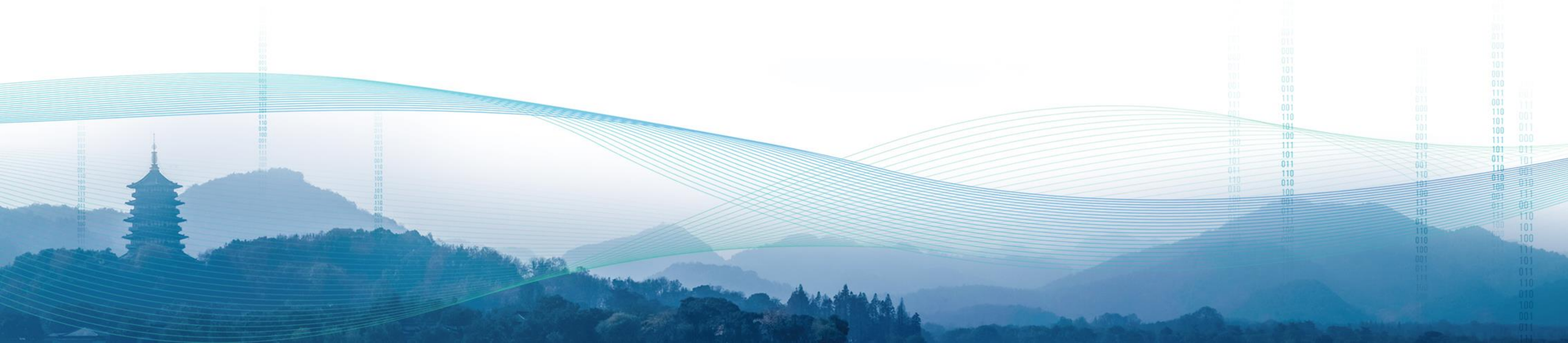
2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY CONFERENCE

城市安全运营中心AISCO平台

主讲人：李贵鹏

CONTENTS
目 录

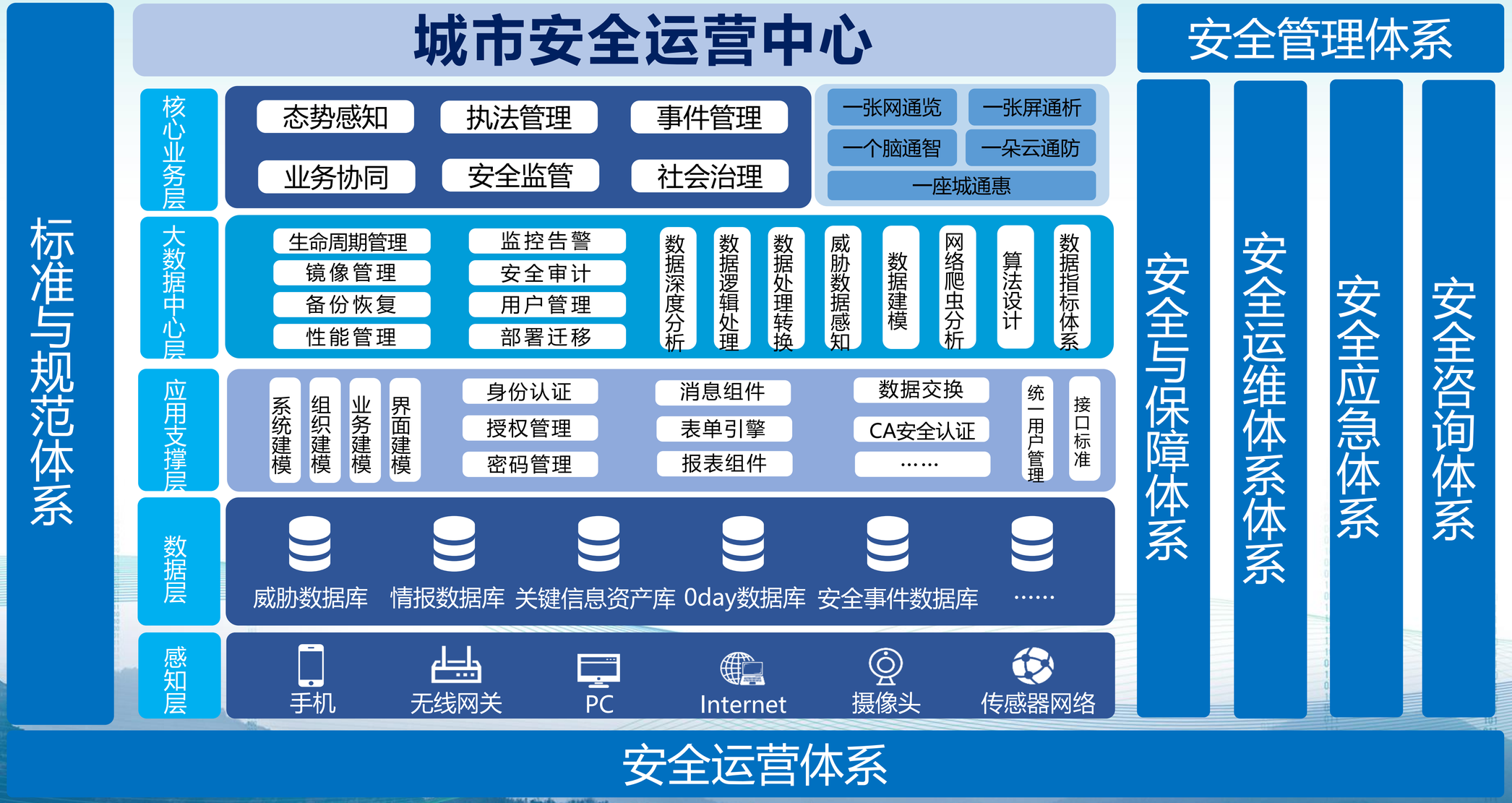
PART 01 城市安全运营中心介绍
PART 02 城市安全运营平台介绍
PART 03 城市安全运营应用介绍
PART 04 城市安全运营模式介绍



PREFACE

新一代的城市安全运营中心，安全运营平台是业界首个将SOC和安全服务业务融合的平台化化产品，采用创新SOAPA安全运营分析协作架构。为各城市与客户改善城市和公司安全运营情况，为城市安全运营市场以及建立安全运营相关标准提供助力。目前定位将安全数据从线下数码化转线上数量化，数字化，通过数模化建立展现出运营分析结果。安全资产将结合威胁情报/ EDR /机器学习等技术领域信息进行数用化应用处理让运营生态更加智能化。根据客户需求情况在监管机构、金融，能源，运营商，政府等多个重量级客户处部署，最终展示出城市安全与企业安全的综合安全管控和运营能力。

城市安全运营中心逻辑架构



城市盾安全运营中心核心特点

五大特点

01 安全健康度综合展示，对主要指标数据进行实时监控；

02 智能协助分析决策，数据的分析挖掘实现安全运行仿真和智能决策

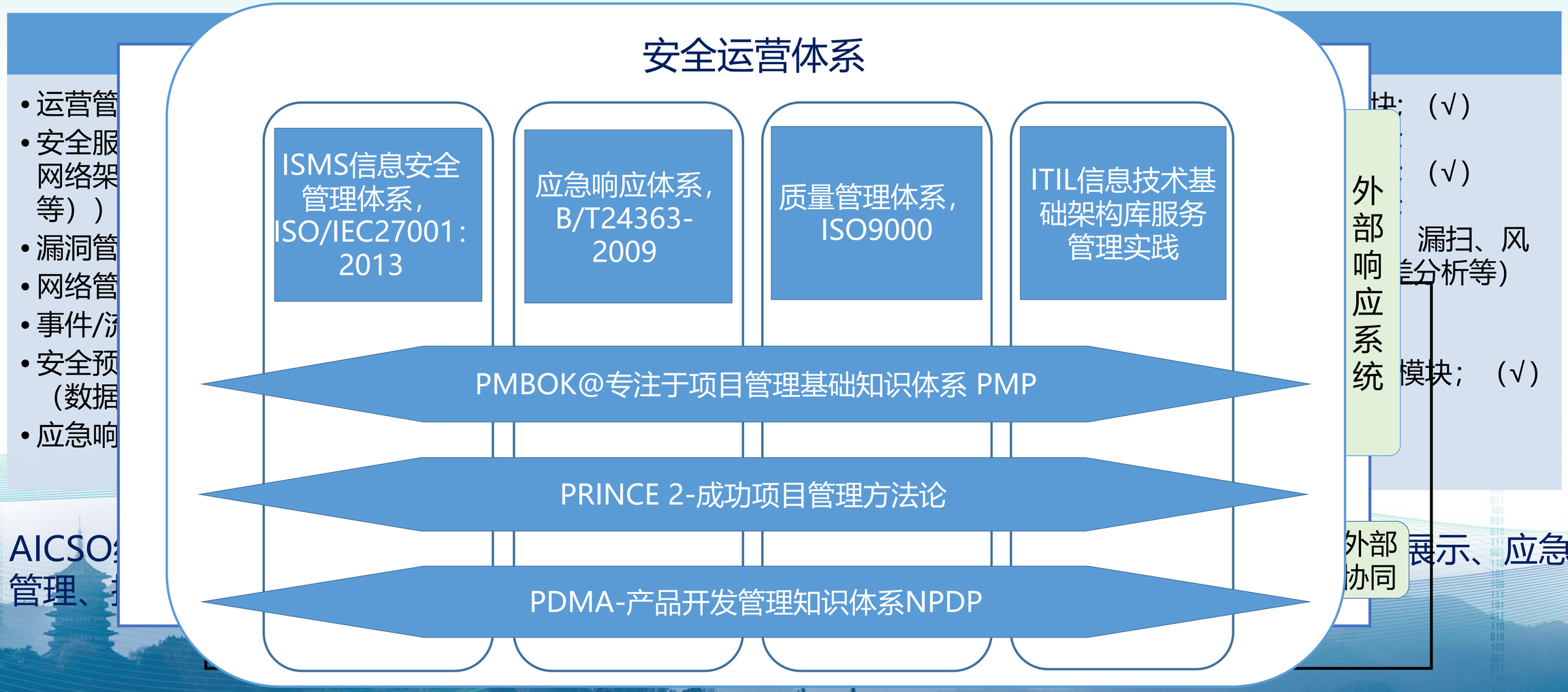
03 看板式事件管理，支持业务流程自定义设计，实现自动安全排程，高效的进行执行和解决问题；

04 监控预警，基于大数据、机器学习等技术实现安全运营的监控和智慧化预测，提前识别风险，并触发预案；

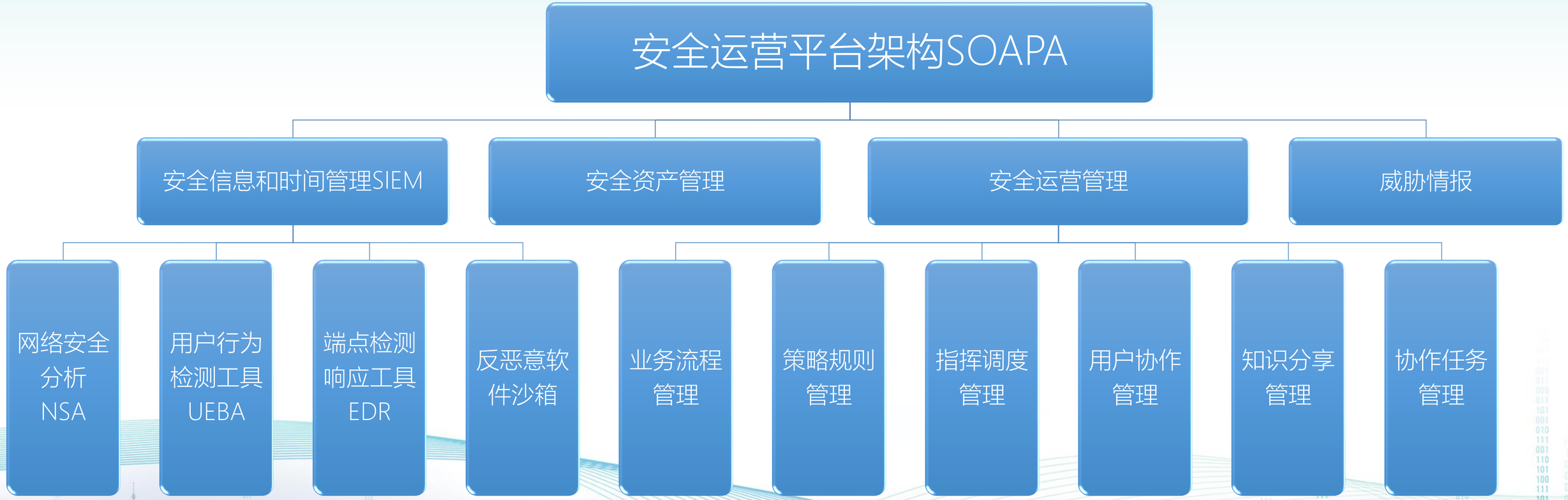
05 指挥调度，联合决策与整合平台实现跨部门资源协调联动指挥。

安全运营平台介绍

AICSO采用最新SOAPA动态的架构，整合六大体系由七个能力核心十大功能模块组成；



安全运营平台架构介绍


安全运营平台架构SOAPA
安全信息和时间管理SIEM
安全资产管理
安全运营管理
威胁情报
网络安全分析 NSA
用户行为检测工具 UEBA
端点检测响应工具 EDR
反恶意软件沙箱
业务流程管理
策略规则管理
指挥调度管理
用户协作管理
知识分享管理
协作任务管理

平台特点

业务安全服务运营

1

1、实现跨系统追踪定位问题。

2、实时监控业务安全表现，全渠道业务监控管理，完善数字化KPI。

3、实现业务运维和安全管理双向驱动。

1、多方位、细粒度、实时监控，并实现故障定位和告警响应。

2、动态展示用户网络拓扑及节点的运行状态，与业务安全服务运营联动，加快应急响应。

2

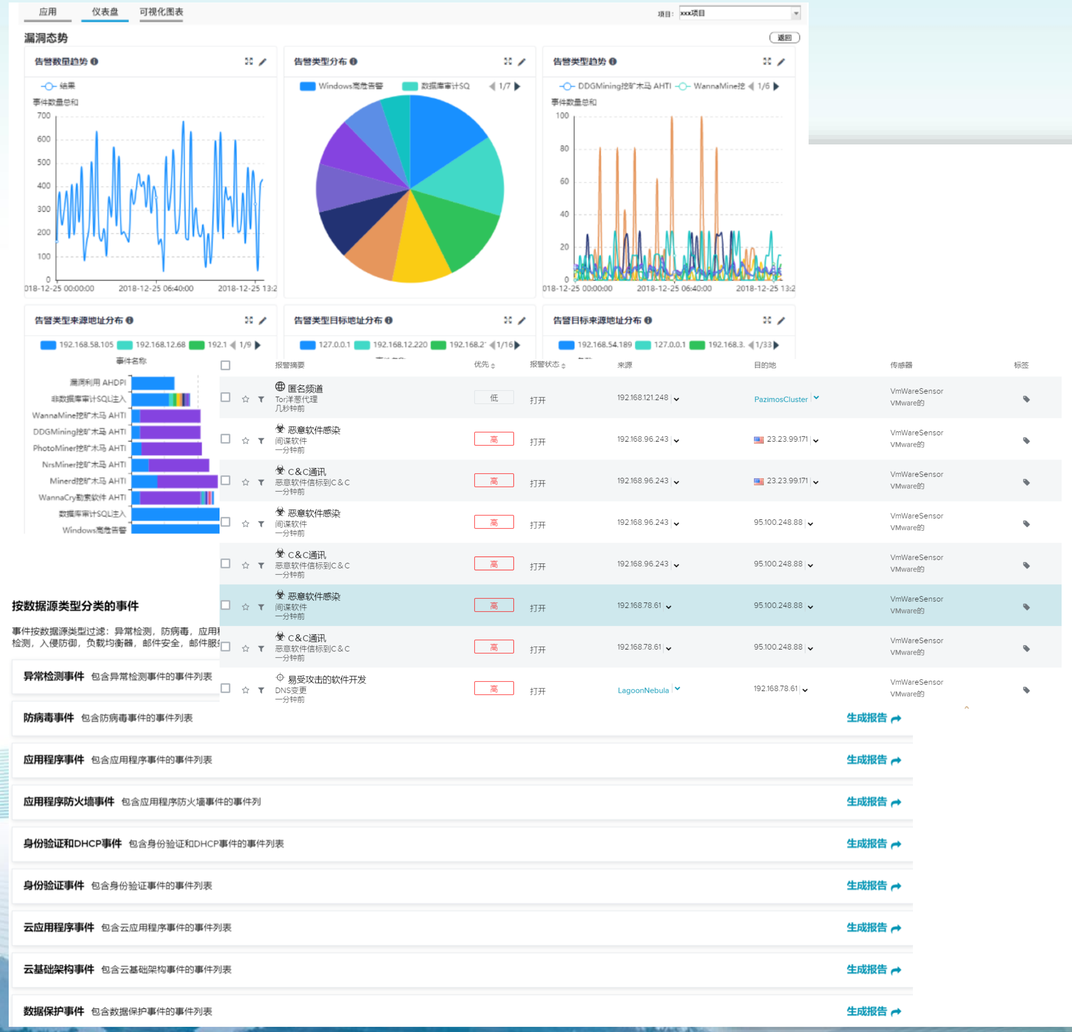
安全运维监控服务

应用场景——智慧城市

将政府和企事业单位的网络安全业务进行集中托管，为客户提供有效的整体安全服务，通过专业的安全运维人员、业务领域专家和安全运营分析团队为客户提供7*24小时的安全监测、情报感知、响应处置和运营管理能力。并在各城市间区域安全运营中心建立横向联动机制，结合漏洞与情报，制定运营中心的应急响应体系，保障各政府机构和企事业单位的信息系统正常与可持续运行。

现已应用于“一带一路”网络安全感知防御云运营中心方案

应用场景——监管部门



实时监控大屏

- 支持多厂家安全设备
- 多方位、细粒度、实时监控，并实现故障定位和告警响应。
- 动态展示用户网络拓扑及节点的运行状态

全流程管理

- 自动生成报告
- 通告平台：分配、跟踪、修复完验证

数据分析

- 自定义画板
- 35种分析模块

应用场景——企业集团中的安全部门

安全运营管理

•提供运营管理支撑：整合本地服务数据、远程服务数据和威胁情报为运营管理人员运营管理数据支撑

•提供部分场景运维自动化工具支撑

•提供异地人员能力支撑

业务流程管理

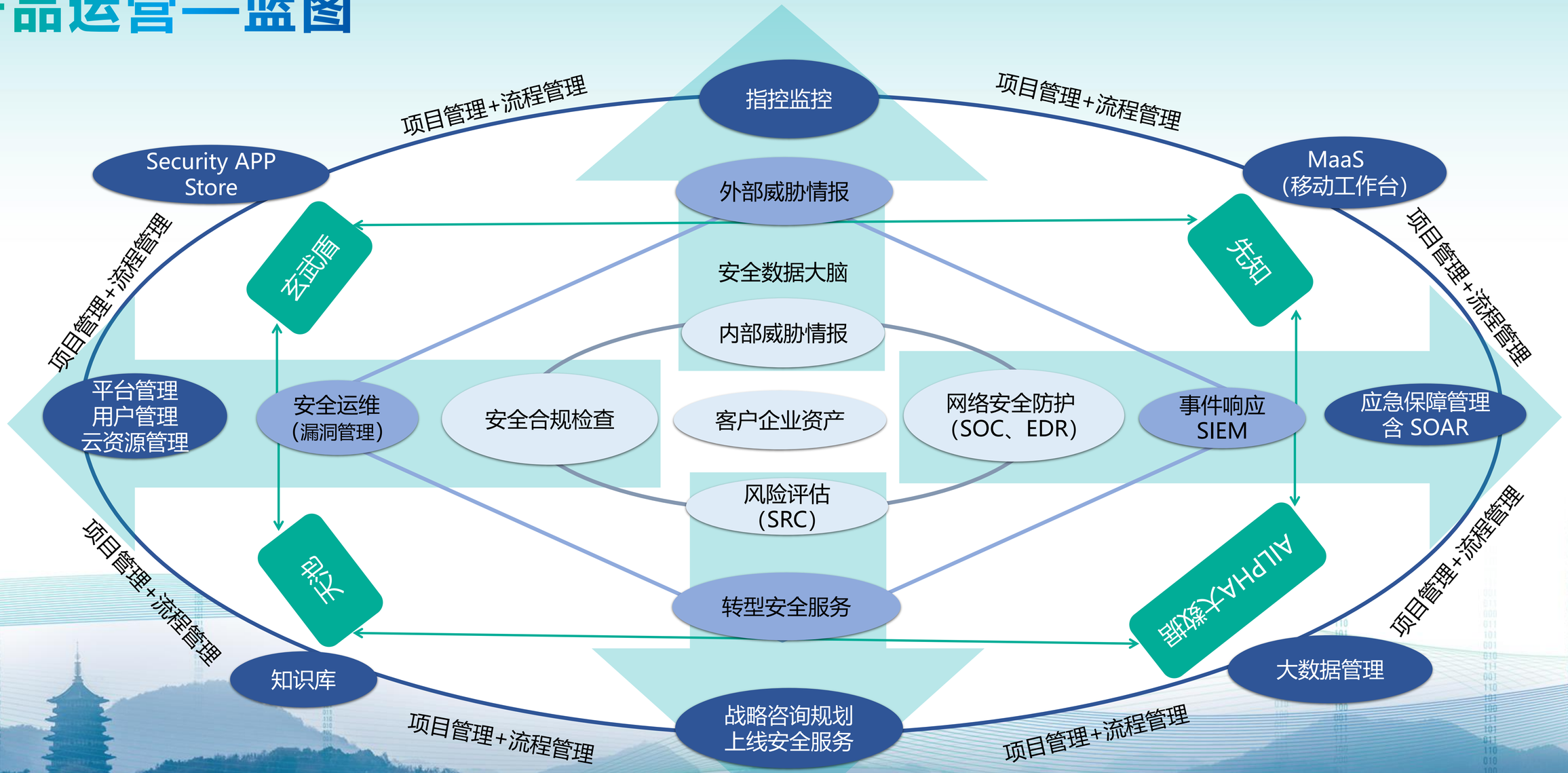
•包括流程引擎、集成引擎、规则引擎、报表引擎、流程门户等

•解决了重复录入造成的数据错误或缺失、效率低下问题，降低管理成本

应急响应

•提供自适应应急响应机制，基于平台漏洞库、威胁数据库、外部威胁漏洞情报信息及标准的应急响应流程，结合专业的情报组、运维团队、研究与分析团队等，实现快速的分析及处置。

产品运营—蓝图


指控监控
项目管理+流程管理
项目管理+流程管理
Security APP Store
MaaS（移动工作台）
项目管理+流程管理
项目管理+流程管理
外部威胁情报
玄武盾
先知
安全数据大脑
内部威胁情报
平台管理
用户管理
云资源管理
安全运维
（漏洞管理）
安全合规检查
客户企业资产
网络安全防护
（SOC、EDR）
事件响应
SIEM
应急保障管理
含 SOAR
风险评估
（SRC）
项目管理+流程管理
项目管理+流程管理
天眼
ALPHA大数据
转型安全服务
知识库
大数据管理
项目管理+流程管理
项目管理+流程管理
战略咨询规划
上线安全服务

产品运营—服务模式

云上 SAAS 服务

用户无需在本地部署系统，只需在自助云端门户选购产品、服务或不同的会员套餐。基于云端平台及在线服务，提供运营管理、安全服务、监控展示、应急响应等功能。

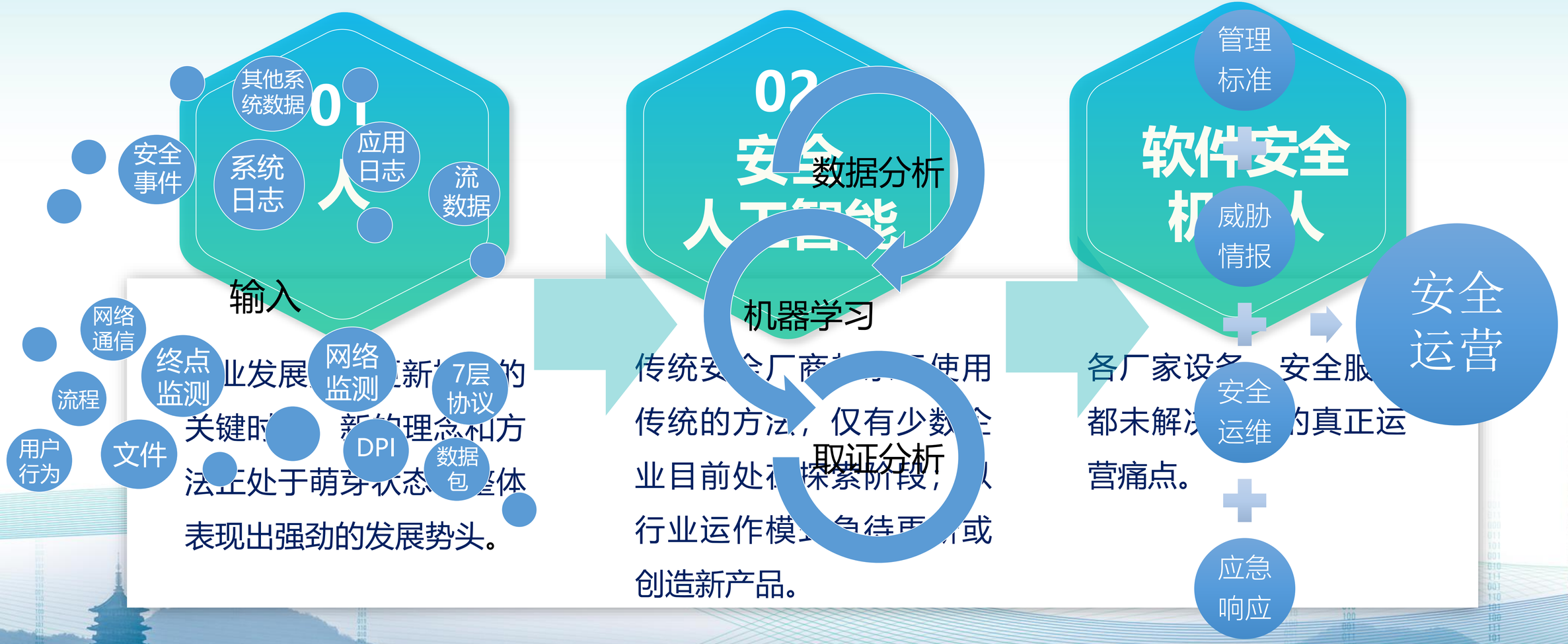
异地 联合运营 SAAS+EPAAS

用户按年租用安全运营平台，可在私有云部署，用户可通过安全运营平台与安恒的安全服务工程师协同工作，联合运营。

本地部署 运营服务 LAAS+EPAAS+SAAS

用户购买整套平台，在本地部署，安恒可提供现场安全服务人员。基于AILPHA大数据分析平台实现数据采集、存储、分析，并提供运营中心组织建设、运营中心规则制度建设。

未来发展



输入

业发展[illegible]新[illegible]的关键时[illegible]新的理念和方法正处于萌芽状态，整体表现出强劲的发展势头。

传统安全厂商[illegible]使用传统的方法，仅有少数企业目前处在探索阶段，从行业运作模[illegible]急待更新或创造新产品。

各厂家设备[illegible]安全服[illegible]都未解决[illegible]的真正运营痛点。

THANK YOU

谢　　谢　　观　　看