



# 从基础大数据 到安全业务大数据的演进

鞠道霁

奇安信科技集团股份有限公司安全大数据中心数据运营部

## 目录


### 1.安全数据来源与利用方法现状

- 安全数据来源主要分类与特性
- 安全数据的利用思路与应用路线
- MASSIF框架

### 2.数据价值转换的阶段特性

- 基础大数据到安全业务大数据的演进方式
- 安全数据各阶段特性与业务价值转换
- 安全业务大数据的持续运营实现与应用场景



- 
- 数量抽离
  - 规则细化

## 大体量数据

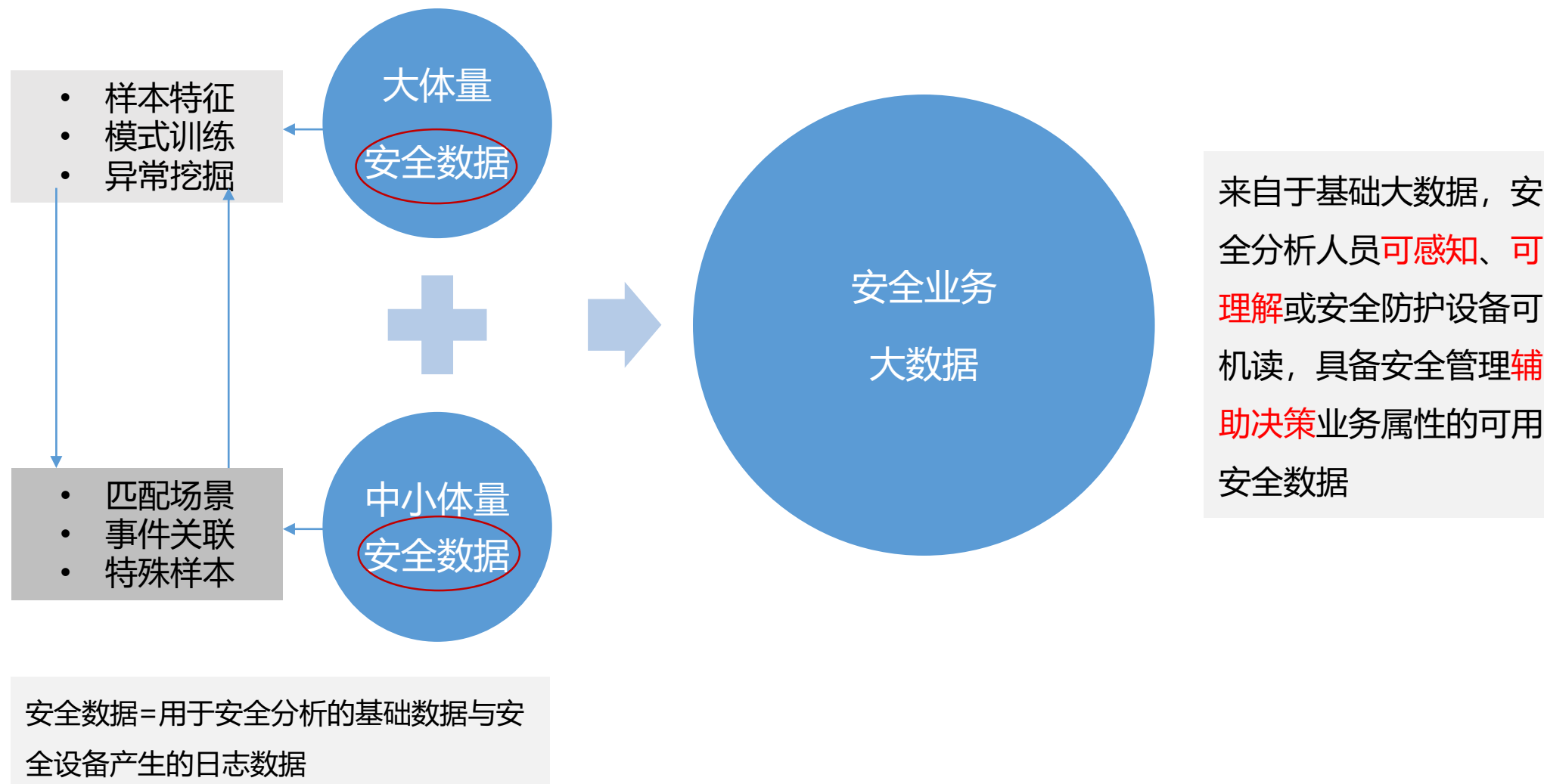
- 数量级大，数量大（条数多）
- 非关系型数据库存储，离线数据挖掘应用较多
- 数据采集点类型少
- 数据信噪比平衡问题难以解决
- 专用安全数据少，流量数据与业务数据类型居多，**C端数据除外**
- 典型：全流量镜像数据，运营商核心网设备数据

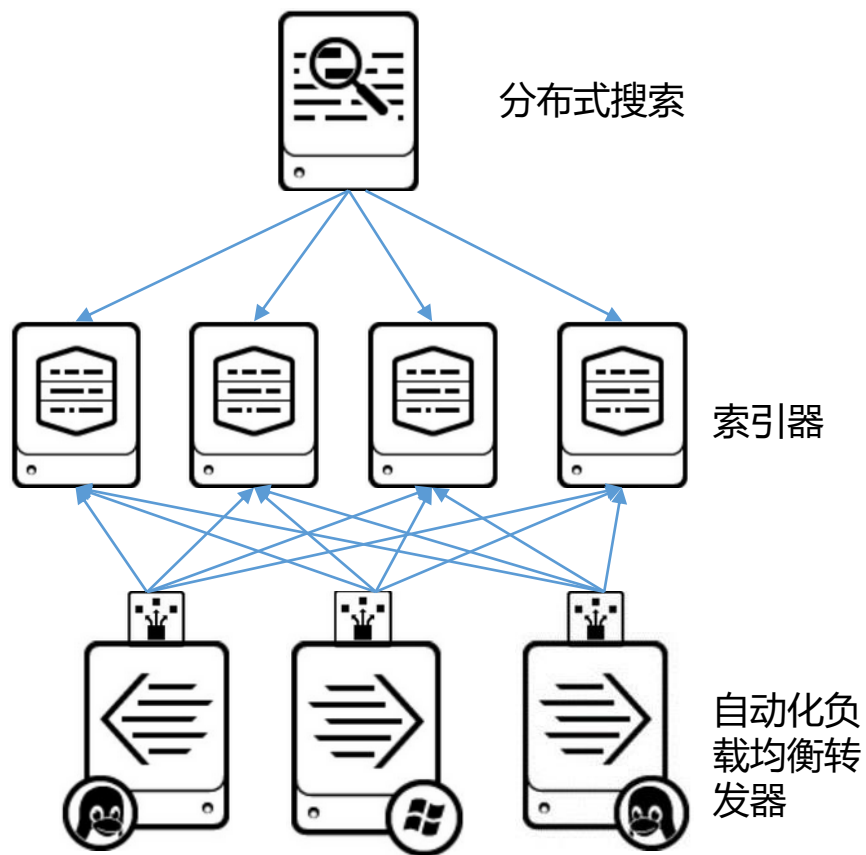
## 中小体量数据

- 数据量级相对较小，条数经预处理（合并，压缩）降低
- 关系型数据库存储，分析方法与表结构强相关
- 数据采集点类型多
- 专门用途设备日志居多
- 典型：单一业务系统日志，安全设备日志

- ✓ 抽样深度分析（恶意样本提取）
- ✓ 具体业务全量分析（DNS解析记录）
- ✓ 离线分析 > 实时分析

- ✓ 全量日志分析
- ✓ 多种类数据关联分析
- ✓ 实时分析 > 历史分析

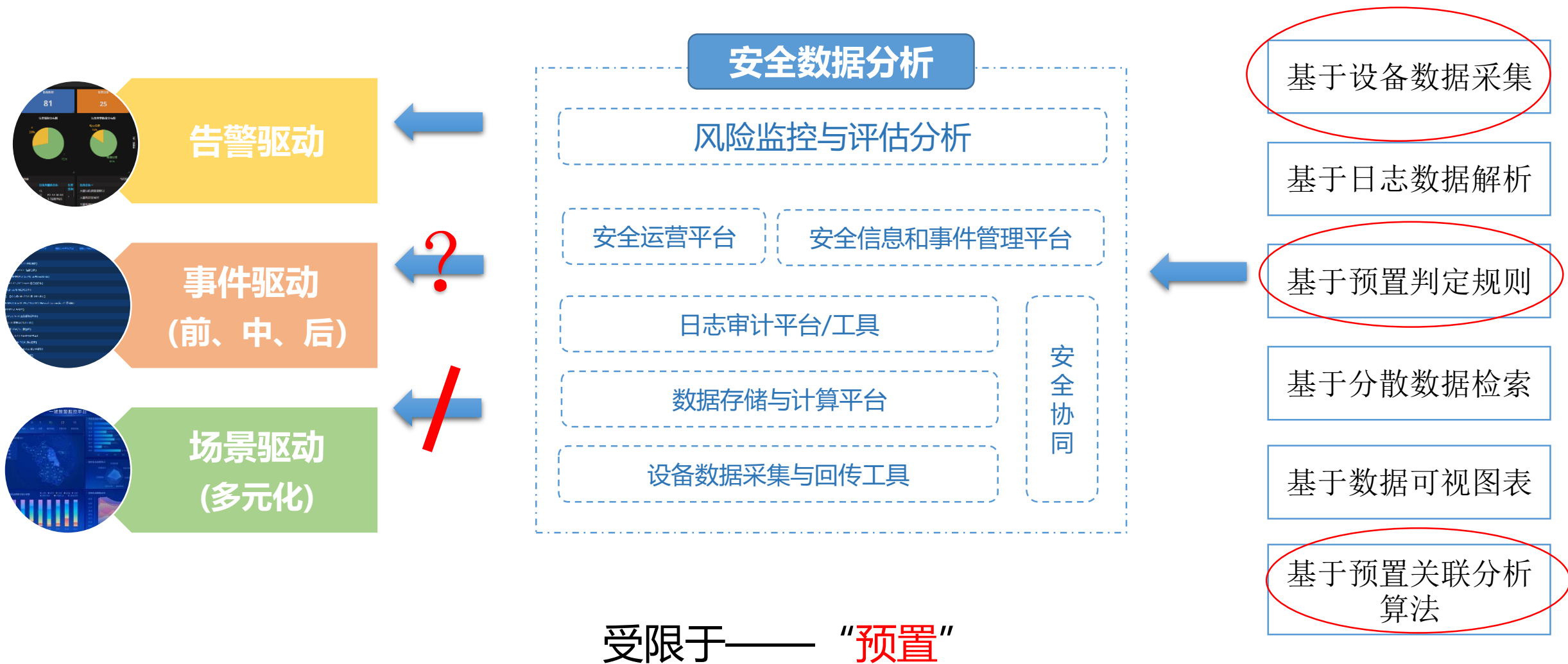




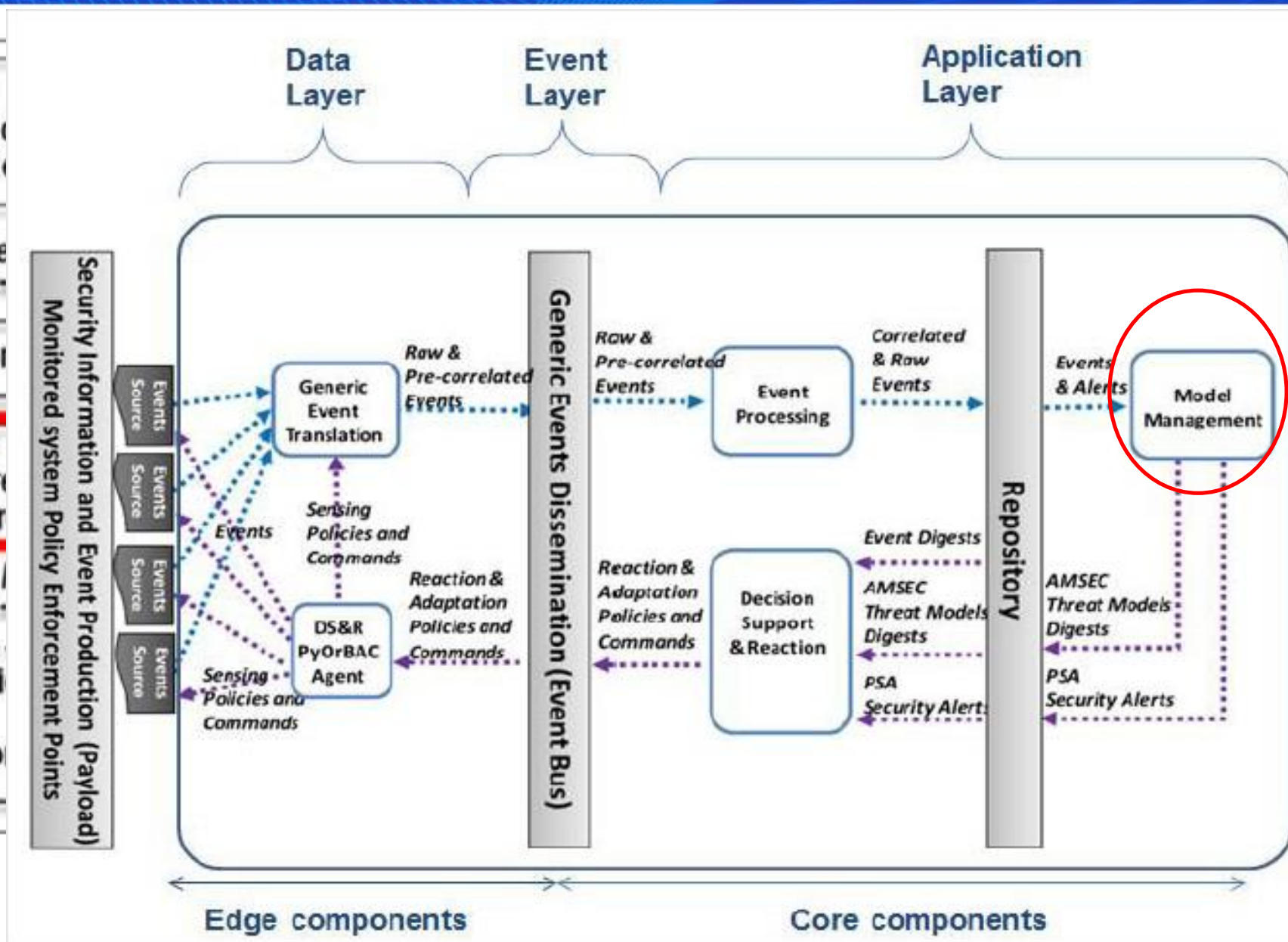
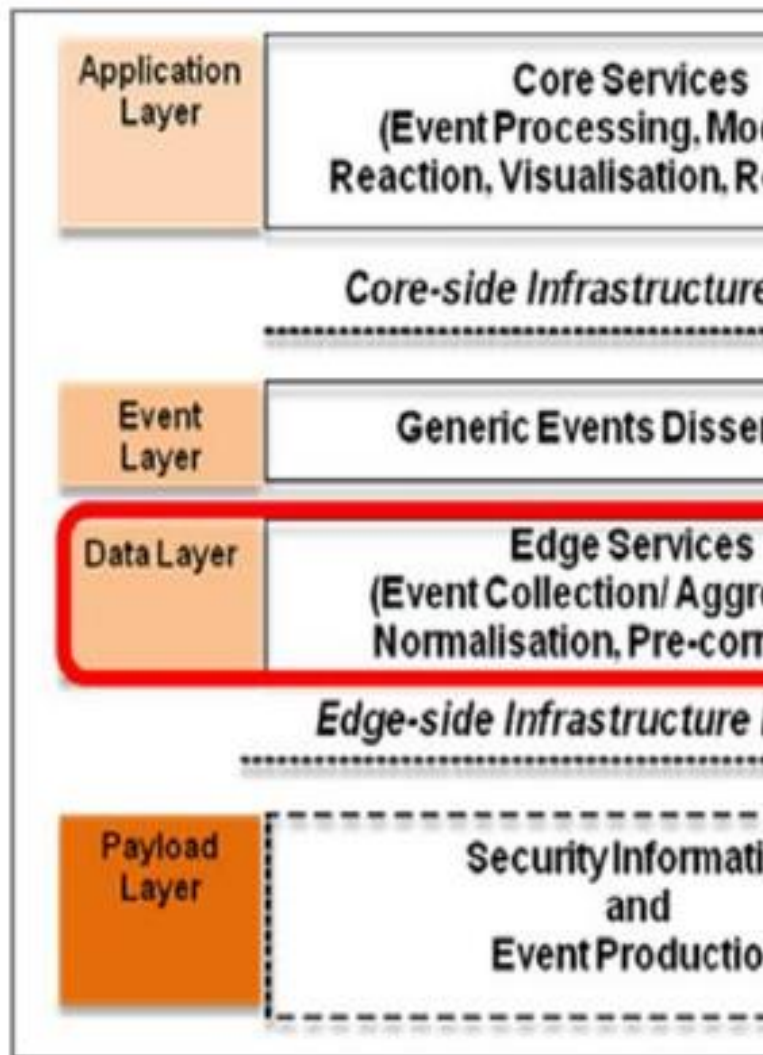
企业内部运维级安全数据分析体系

- 本质是日志集成搜索系统
- 对大数据架构日志系统支持乏力
- 商业化软件成本高
- 封闭式架构扩展性较差
- 基于搜索结果进行分析，分析行为后置
- 字段提取、合并、统计与建模行为分离
- 分析能力取决于分析师个人能力或外部团队支持

受限于—— “后置”

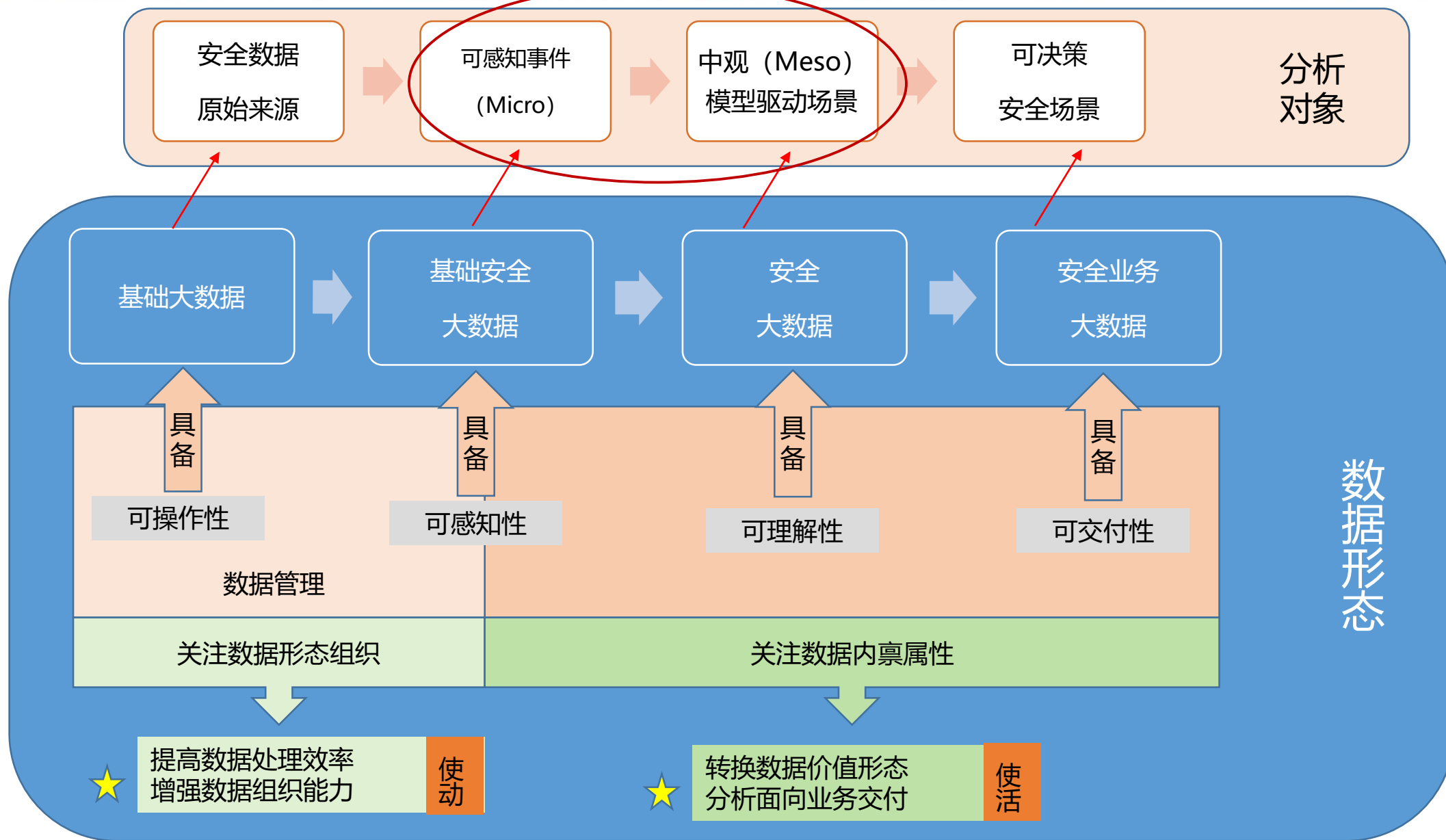






# 安全数据核心价值转换——数据“活动”

2019 北京网络安全大会  
2019 BEIJING CYBER SECURITY CONFERENCE





（微观）事件：组成基础安全大数据的元素对象，由基础大数据中的原始日志经安全业务导向的事件模型构造，具备**最细粒程度**的安全属性。

大数据环境存储的原始日志  
(Something happened)

裁剪

关联

聚合

微事件 (What happened)

## 事件模型示例

审计设备日志

登录对象日志

流量/会话日志

根据  
模型  
抽取

有  
意义  
的  
**最小**  
字段

ETL

登录行为  
事件

衍生为规则

异常登录  
行为事件

尝试登陆次数  
超过阈值，账  
户锁定，不再  
记录登陆行为，  
如何识别异常

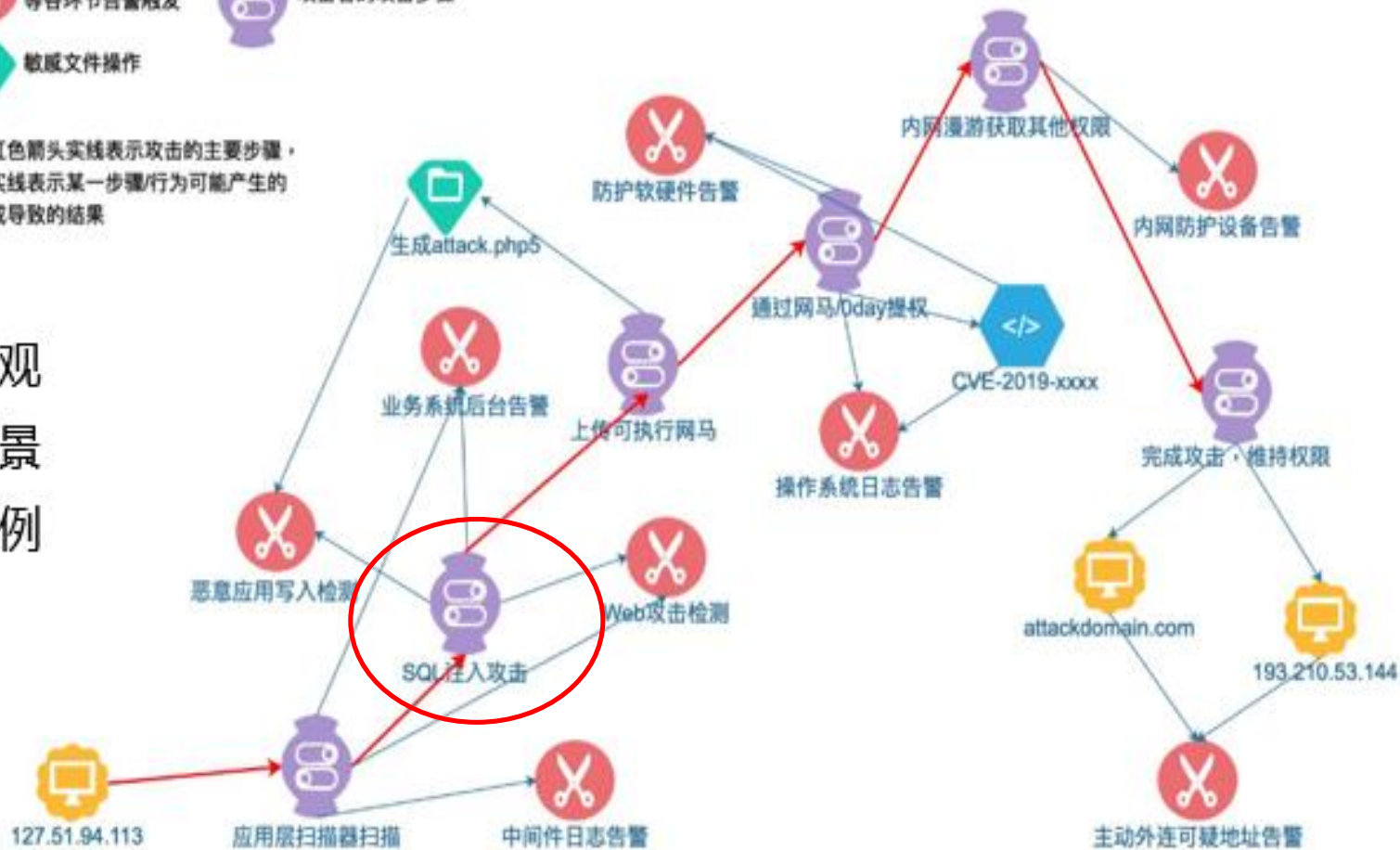
登录行为关联的原始日志

1. 在原始数据来源稳定情况下，固化关联模型，减少取数资源消耗，尤其适应列数据库环境；
2. 多源数据关联避免单点数据造成的I型与II型错误；
3. 为场景建模提供可感知的建模元素形态与数据通道；
4. 降低分析人员工作难度与专业度要求。



注：红色箭头实线表示攻击的主要步骤，  
蓝色实线表示某一步骤/行为可能产生的  
告警或导致的结果

## 中观 场景 示例



## 中观攻击行动

行为步骤1

行为步骤2

行为步骤3

行为子步骤1

行为子步骤2

行为子步骤3

行为M级子步骤1

事件1

事件2

事件3

...

事件N

## 安全场景 ER建模

- 确定安全场景各主题、实体
- 确定主客体属性及相关关系

## 安全场景逻辑建模

- 使用标准业务元数据字段名，将安全场景ER模型映射为安全场景维度表
- 使用事件模型构建安全场景事实表，并与维度表关联

## 安全场景物理建模

- 基于逻辑模型已建立的各事件模型关系，建立索引
- 根据事件模型算法，生成ETL脚本，提供提数接口

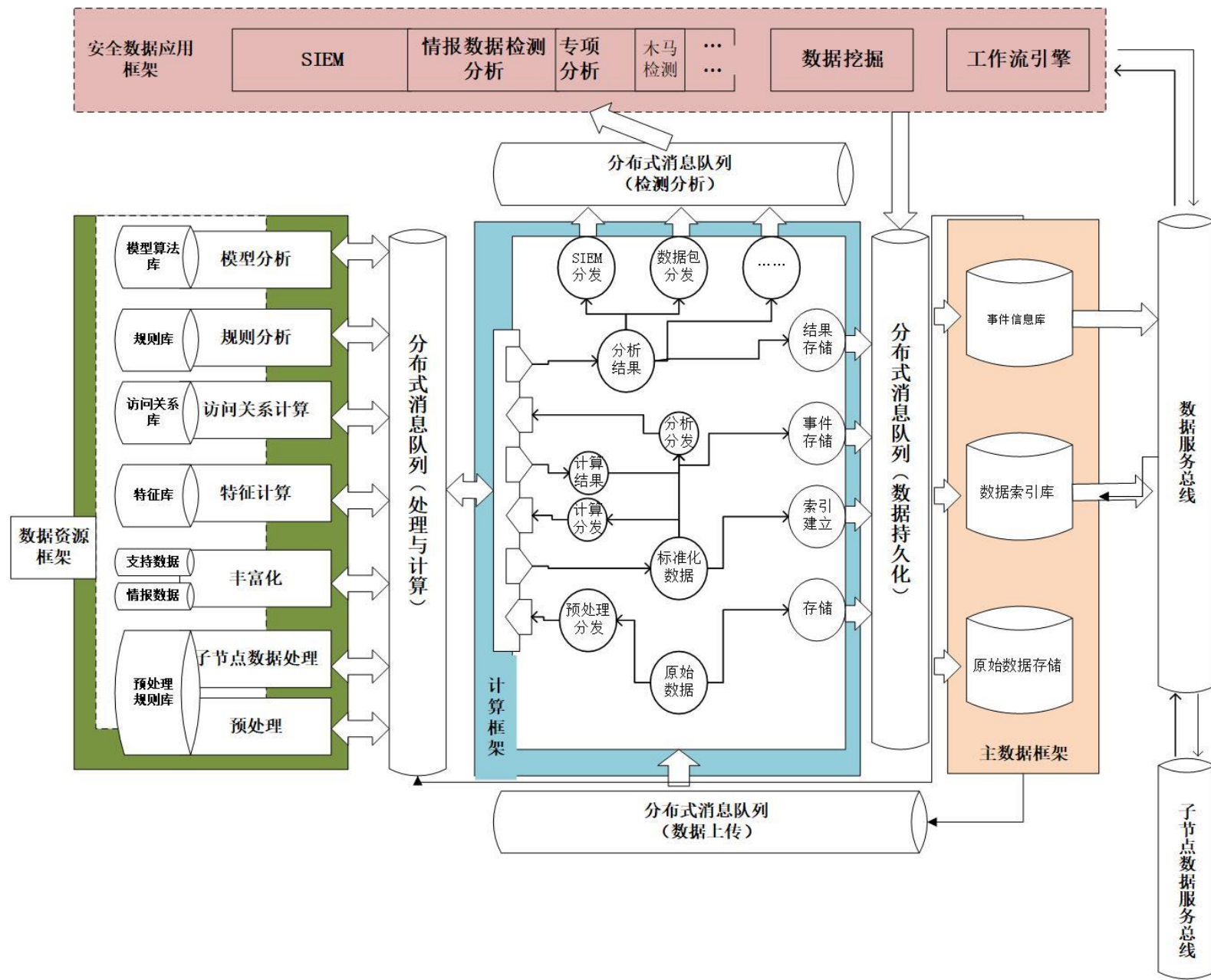
Permissions	Privilege Evaluation	Defense Evade	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
OS Search Order Hijacking			Brute Force	Account Discovery	Windows Remote Management		Automated Collection	Automated Exfiltration	Command and Control
Legitimate Credentials			Credential Dumping	Application Window Discovery	Third-party Software		Clipboard Data	Data Compressed	Communication Through Removable Media
Accessibility Features	Binary Patching			File and Directory Discovery	Application Deployment Software	Command Line	Data Staged	Data Encrypted	Custom Command and Control Protocol
AppX/DLL	Code Signing	Component Manipulation		Exploitation of Vulnerability	Execution Through API	Graphical User Interface	Data From Local System	Data Transfer (See Note)	Custom Cryptographic Protocol
Local Port Monitor	Component Hijacking		Credentials In Files	Local Network Configuration Discovery	Logon Scripts	PowerShell	Data From Network Shared Drive	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
New Service	OS Side Loading		Local Network Connections	PowerShell	PowerShell	PowerShell	Data From Removable Media	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel
Path Interception	Disabling Security Tools	Input Capture	Network Sniffing	PowerShell	PowerShell	PowerShell	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel
Scheduled Task	File Deletion		Network Sniffing	PowerShell	PowerShell	PowerShell	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel
Service File Permissions Windows	File System Logical Offsets		Two Factor Authentication Interception	PowerShell	PowerShell	PowerShell	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel
Service Registry Permissions Windows	File System Logical Offsets		Two Factor Authentication Interception	PowerShell	PowerShell	PowerShell	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel
Web Shell	Indicator Blocking			PowerShell	PowerShell	PowerShell	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel
Basic Input/Output System	Exploitation of Vulnerability			PowerShell	PowerShell	PowerShell	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel
BasicIO	Remote User Account Control			PowerShell	PowerShell	PowerShell	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel
Change Default File Association	OS Injection			PowerShell	PowerShell	PowerShell	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel
Component Firmware	Indicator Removal from Tools			PowerShell	PowerShell	PowerShell	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel
Hypervisor	Indicator Removal on Host			PowerShell	PowerShell	PowerShell	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel
Logon Scripts	Indicator Removal on Host			PowerShell	PowerShell	PowerShell	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel
Modify Existing Service	Indicator Removal on Host			PowerShell	PowerShell	PowerShell	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel
Redundant Admin	Indicator Removal on Host			PowerShell	PowerShell	PowerShell	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel
Registry's Run Key / Task Folder	Indicator Removal on Host			PowerShell	PowerShell	PowerShell	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel
Security Support Provider	Indicator Removal on Host			PowerShell	PowerShell	PowerShell	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel
Shutdown (Modification)	Indicator Removal on Host			PowerShell	PowerShell	PowerShell	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel
Windows Management Instrumentation Event Subscription	Indicator Removal on Host			PowerShell	PowerShell	PowerShell	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel
Windows Remote DLL	Indicator Removal on Host			PowerShell	PowerShell	PowerShell	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel	Exfiltration Over Command and Control Channel

基于ATT&CK模型的中观攻击行动业务模型






1. 形成基础大数据到安全业务大数据持续转换生产的技术支撑能力；
2. 解决大数据安全应用场景下，安全大数据挖掘与实时业务系统“取数难”的问题；
3. 解决安全分析师在数据分析建模能力的短板问题，降低安全数据分析认知难度；
4. 数据形态转换各阶段均可自定义，避免先验认知误差问题。





The background is a solid blue color with a subtle, abstract pattern of thin, light blue lines that form a grid or mesh-like structure, creating a sense of depth and movement.

# THANKS

**2019 北京网络安全大会**  
2019 BEIJING CYBER SECURITY CONFERENCE