国泰海通
GUOTAI HAITONG

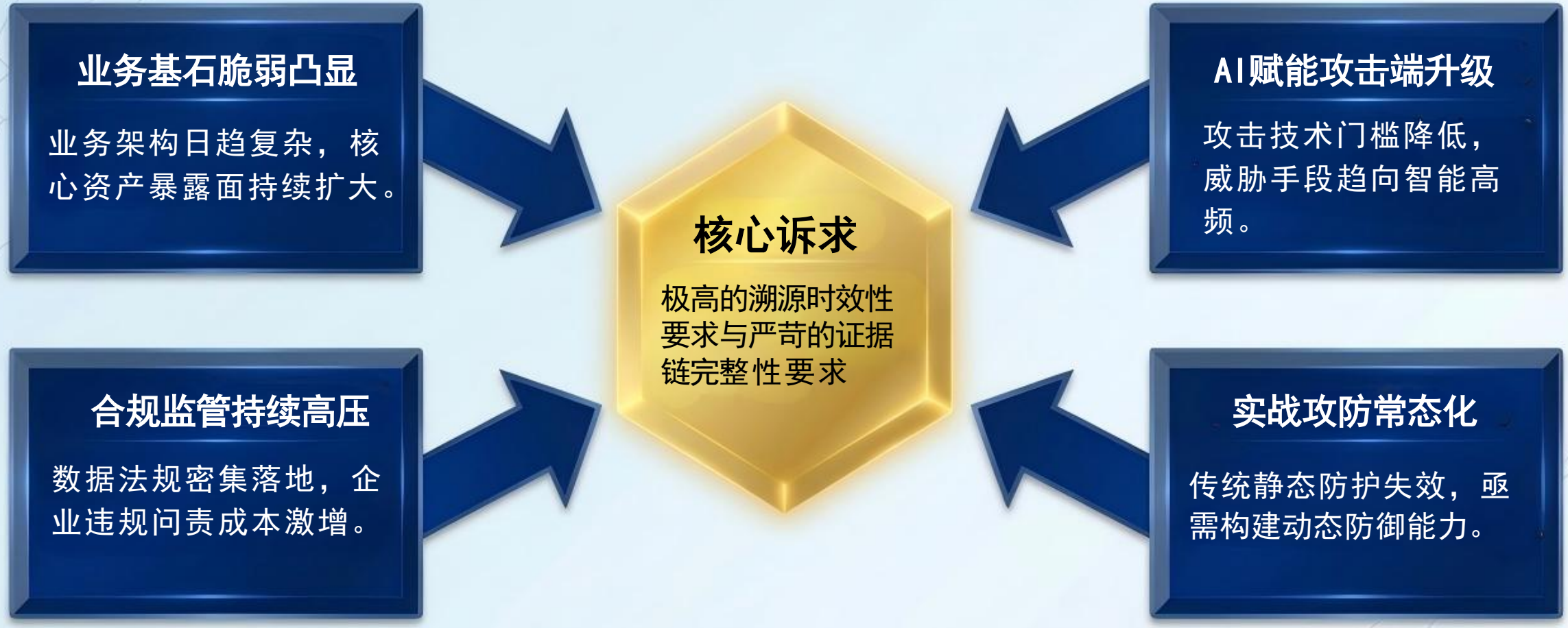
2026金融业大模型与智能体应用研讨会

基于大语言模型的全流量安全智能体研究与实践

国泰海通证券 侯亮
2026年4月10日

目录

一、背景：证券面临的多重压力



一、现实瓶颈：运营体系的三大挑战

数据支撑断层

跨设备告警难聚合，缺乏完整攻击链视图与溯源证据链。

响应时效极低

高度依赖人工关联回溯，复杂事件分析耗时4–6小时起步。

高级威胁发现难

对抗技术门槛高，严重依赖少数安全，专家，无法低成本、规模化应用。

二、破局之道：全流量安全智能体

1 破局切入点

从网络全流量入手，保障底层数据100%无死角。

2 核心理念

智能调度+专业分工+多智能体协作。

终极目标 3

摆脱人力瓶颈，夯实“AI化”安全运营底层基础。

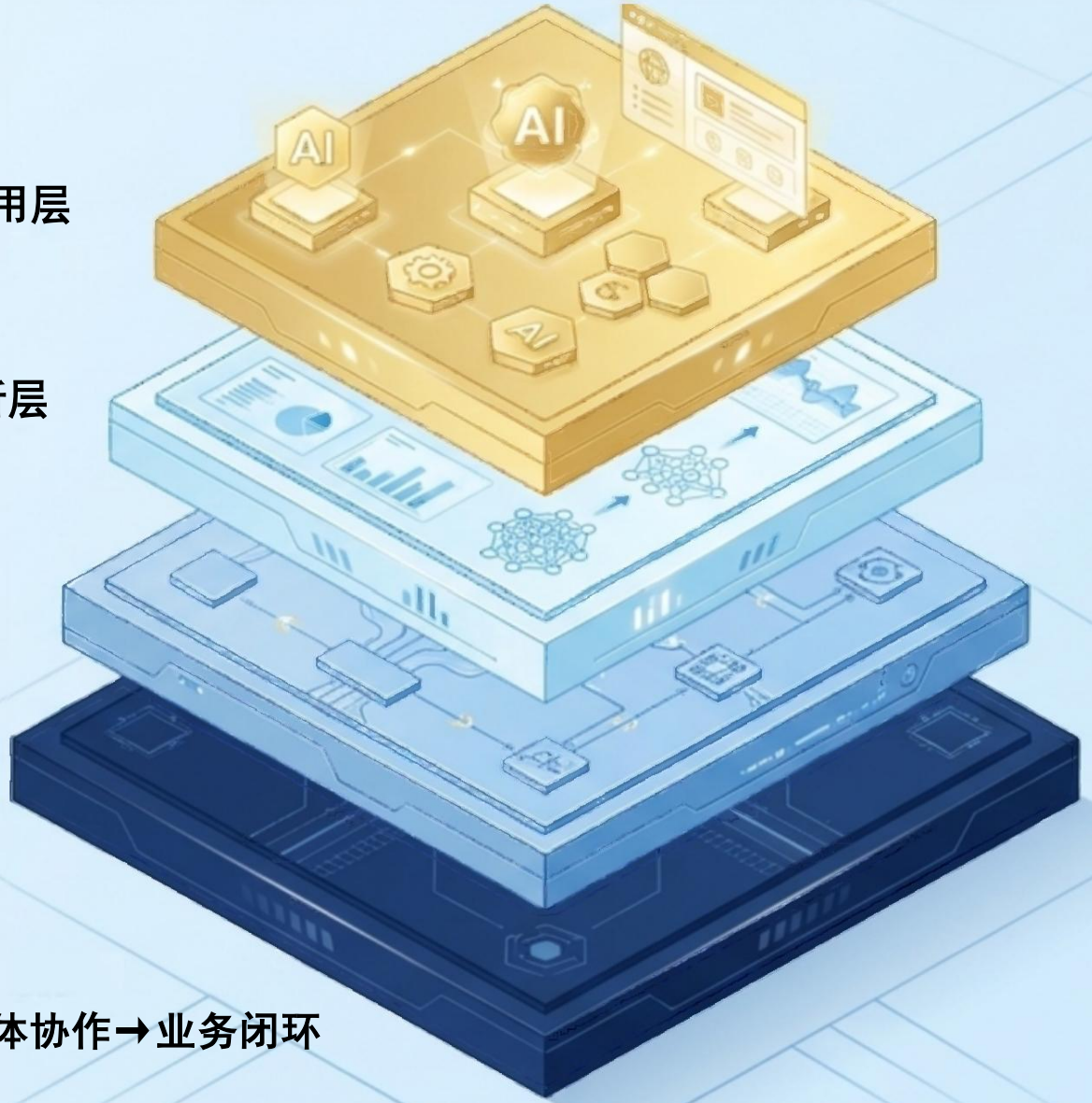
二、系统总体架构概览

第四层：AI应用层

第三层：数据分析层

第二层：核心调度层

第一层：数据接入层



技术路径：

数据驱动→模型推理→智能体协作→智能体协作→业务闭环

二、架构详解：底座与大脑

核心调度层(智能大脑)

模块A
集成多模型(千问/DeepSeek/Kimi)

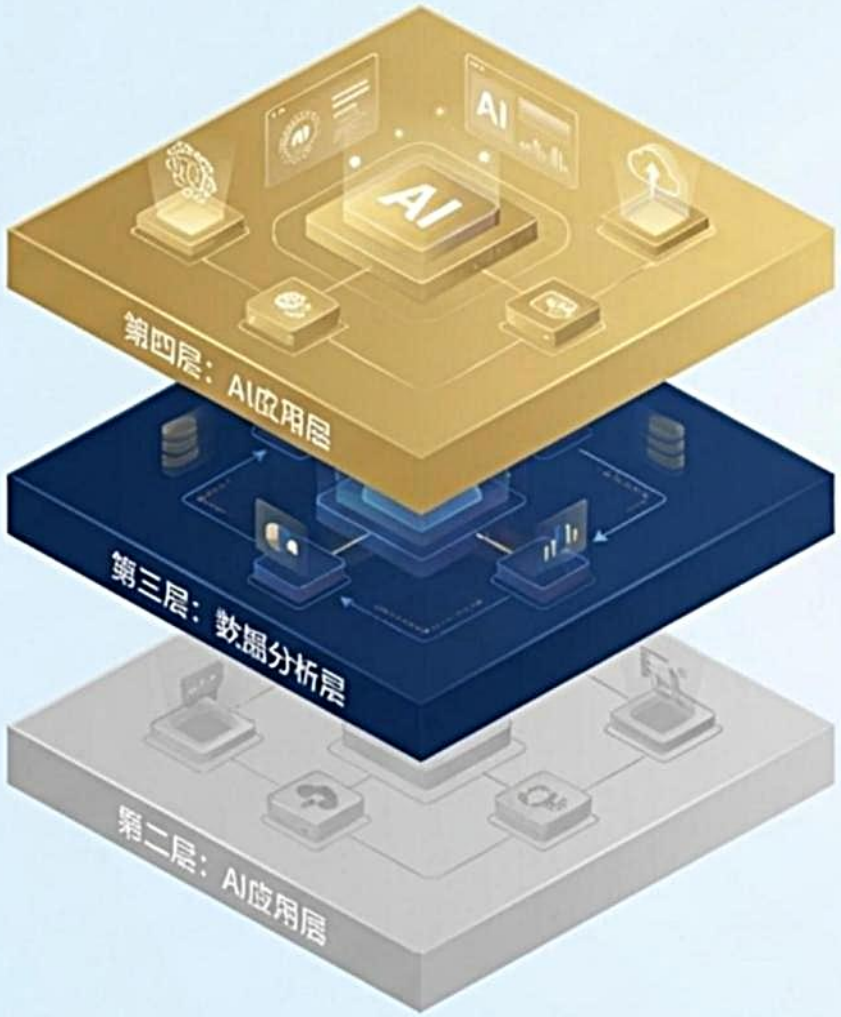
模块B
引入RAG（检索增强生成)与DAG(有向无环图)任务编排

模块C
动态匹配最优模型推理能力

数据接入层(统一底座)

接入全流量、告警、知识库等多源异构数据，标准化数据底座。

二、架构详解：中枢与闭环



AI应用层（业务闭环）

线索自动化调查溯源。

“分析-决策-响应” 安全运管全闭环。

Webshell智能专项分析。

数据分析层（协作中枢）

5类专业智能体（分析师、流量、研判、路径、专家）通过发布-订阅机制松耦合运作。

三、核心功能1:统一接入与极速溯源

线速采集不断连

10-100Gbps探针线速处理，彻底避免丢包，保障底层证据链 。

海量极速检索

时序列引擎+五元组复合索引，实现

90天历史流量

PB 级数据

秒级溯源。

语义级关联

全协议解码上下文，标准化告警构建“资产-漏洞-威胁”知识图谱。

三、核心功能2:大模型安全推理(感知到认知)

认知跃升

不仅能“看到”攻击特征，更能“看懂”攻击意图，推断未知高级威胁。

代码深度解析

表面特征

```
eval(base64_decode("aWYoJHXitIw%h%B(%8Sb%&
%EIsMHyC:...IOHB CoMtNde%tzogoLAxYvtav3DpyPs
c%IkSGmPƏ%HA(^g__W!:IorniiEMfnsBbtiVFnB%zWhpk
us(AFiDJW&stasWUW%wS #HivG%ng&gtrINplDE(
eW!%T:JH..."));
function x()(return y);
var a = "0a4S'
var ':::=('"%dd%94: :nvnop%hrixahütavT&E% GJ?atit:
8tWuBT(AB&Dn%mw))ntP?axt=snepCH%9:?tV0f8.ü%
");
```

AI Translation Layer

AI

深度解析

Deep Analysis Tree

无视表面混淆(如精准识别eval本质)。

- Identifies core logic
- Bypasses obfuscation

精准推断加密算法数学特征。

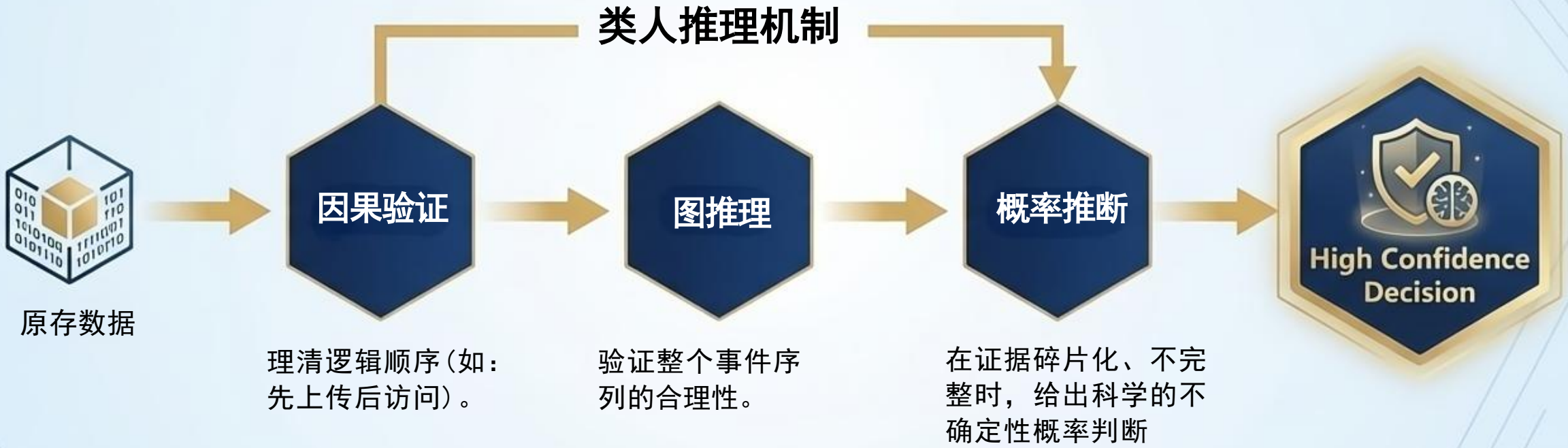
- Recognizes patterns
- Determine algorithm type

自动提取动静态密钥并生成解密脚本。

- Extracts keys
- Generates decryption tools

三 、核心功能2:大模型安全推理(类人决策)

底层支撑：基于RAG 与CoT （思维链)技术。



三、核心功能3:多智能体协作机制

三、核心技术4：AI专业工具函数库(一)

Webshell分析

- TB级流量骤降至MB级
- 大模型语义检测高危调用
- 动态提取加密通信密钥

反序列化检测

- 递归解码与反序列化解析
- 多语言Gadget链精准匹配

三、核心技术4：AI专业工具函数库(二)

外联扩散分析

- 基于全局狩猎构建通信关系图
- 图遍历算法识别内网横向移动
- SIR模型预测威胁扩散趋势

异常行为检测

- 流量建立协议头白名单基线
- 大模型语义判定偏离合理性

四、实践案例：红蓝对抗初期响应

实战背景

Webshell疑似植入 → **服务器出现异常外联** → **探测到横向端口扫描**

接力处置（上场）

T+0

下发任务

分析师智能体第一时间归纳告警，统筹全局。

极速解密（耗时5分钟）

流量智能体提取冰蝎RSA/AES密钥，还原出被隐藏的完整攻击指令。

四 、实践案例：路径重构与效能提升

接力处置（收网）

重构路径（耗时15分钟）

成功串联“漏洞利用→Webshell→横向移动→窃取凭证→数据外传”完整链条。

定损出报

精准评估影响网段与敏感数据，输出全景图证据链报告。

效能提升

传统人工耗时（8-12小时）

全流程闭环仅需 **30分钟**

94%

响应效率大幅飙升

五、总结与未来展望

现状总结

跨越至“认知”安全运营，溯源从数小时降至分钟级，彻底摆脱高级专家单点依赖。

实战深化

持续推进多智能体在更复杂安全运营场景下的落地应用。

技术前沿

探索引入具身智能(Embodied AI)，全面提升自动处置覆盖率与精准度，构建敏捷、高效的新一代防御体系。

国泰海通
GUOTAI HAITONG

AI是对人类学习过程的阐释，对人类思维过程的量化，对人类行为的澄清，以及对人类智能边界的探索。AI将是人类认识自我这一历程的“最后一公里”。

《AI未来进行式》