奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

BCS2022系列活动-冬奥网络安全“零事故”宣传周

# 冬奥网络安全态势感知的探索与实践

常月 奇安信集团态势感知第一事业部总经理

奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

# 奥运历史网安威胁：攻击呈上升趋势

**2008年北京夏季奥运会**：
每天网络攻击告警高达1100万到1200万次。其中一些攻击具有政治动机，希望通过破坏性的攻击吸引对其政治诉求的关注。

**2012年伦敦夏季奥运会**：
记录约1.65亿“与网络安全有关的事件”。开幕当日，奥林匹克场馆电力系统遭受了40分钟大规模DDoS攻击。

**2018年平昌冬季奥运会**：
遭Sandworm组织攻击，开幕倒计时期间汉城数据中心的所有域控制服务器都被迫下线，互联网和广播系统中断。奥运会网站瘫痪数小时，门票销售下载中断，部分观众无法打印门票，场馆内出现大量空位。奥林匹克场馆周围Wi-Fi短时无法使用，开幕式直播信号中断。


**2021年日本夏季奥运会**：
共遭遇约4.5亿次网络攻击，日本奥委会遭到疑似勒索软件攻击，工作人员信息遭到窃取和泄露，开幕式前夕遭钓鱼攻击。

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

# 核心挑战：如何实现冬奥网络安全零事故？

## 目标：力保冬奥网络安全零事故

- 全面覆盖，数据全覆盖，信息全互通
- 实时展示，综合感知委内委外安全态势
- 精准识别，高位研判，充分整合优势资源合力
- 协调指挥，有效压制

战略目标

### 监测面

**背景：**226场站+公有云+供应链+万余终端

**挑战：**如何实现全面监测无遗漏？

### 研判面

**背景：**千亿（日均37亿）原始数据+2.4亿次攻击

**挑战：**如何及时消化，精确告警？

### 指挥面

**背景：**冬奥业务优先+国家级网空力量支撑

**挑战：**如何在冬奥业务及网络安全之间实现平衡？

**国家院士级分析研判思路 —— 准备期查漏补缺、战时精准打击**

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

# 网络安全与大数据的关系

■ 网络空间是一个高度复杂、贯穿了**虚拟**世界和**现实**世界的**复杂巨系统**

■ 被保护对象、攻击者、保卫者、支撑者，以及各种被利用的资源，在这个空间里**一刻也不停息地相互作用**。用数据来表达，则这些数据呈现典型的：**巨量**、**实时**、**多变**、**多维**、**相互关联**的特点

■ 要对这个巨型复杂系统进行：**深刻的洞察**、**实时的感知**、**精准的应对**、**保卫其安全**，就必须建立集：**感知**、**管理**、**预防**、**控制**、**打击**、**反制**能力**为一体**的大数据体系，来**有效**、**高效**地治理、保卫网络空间的安全

■ **态势感知**，就是这样的大数据体系，**也必须是**这样的大数据体系，才能发挥其应有的作用

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

# 因此，奇安信对态势感知的理解是

## 战略定位

将大数据技术应用于网络安全领域，应对日趋复杂、严峻的网络安全挑战，在网络空间安全保卫方面，进行社会治理体系与治理能力现代化的创新，实现网络空间的安全治理

## 机理定位

构建网络空间的免疫系统，第一时间感知威胁，产生有效的“抗体”，精准响应，必要时，可以实施主动反击，破敌于源头，实现从被动防御向积极防御的转化

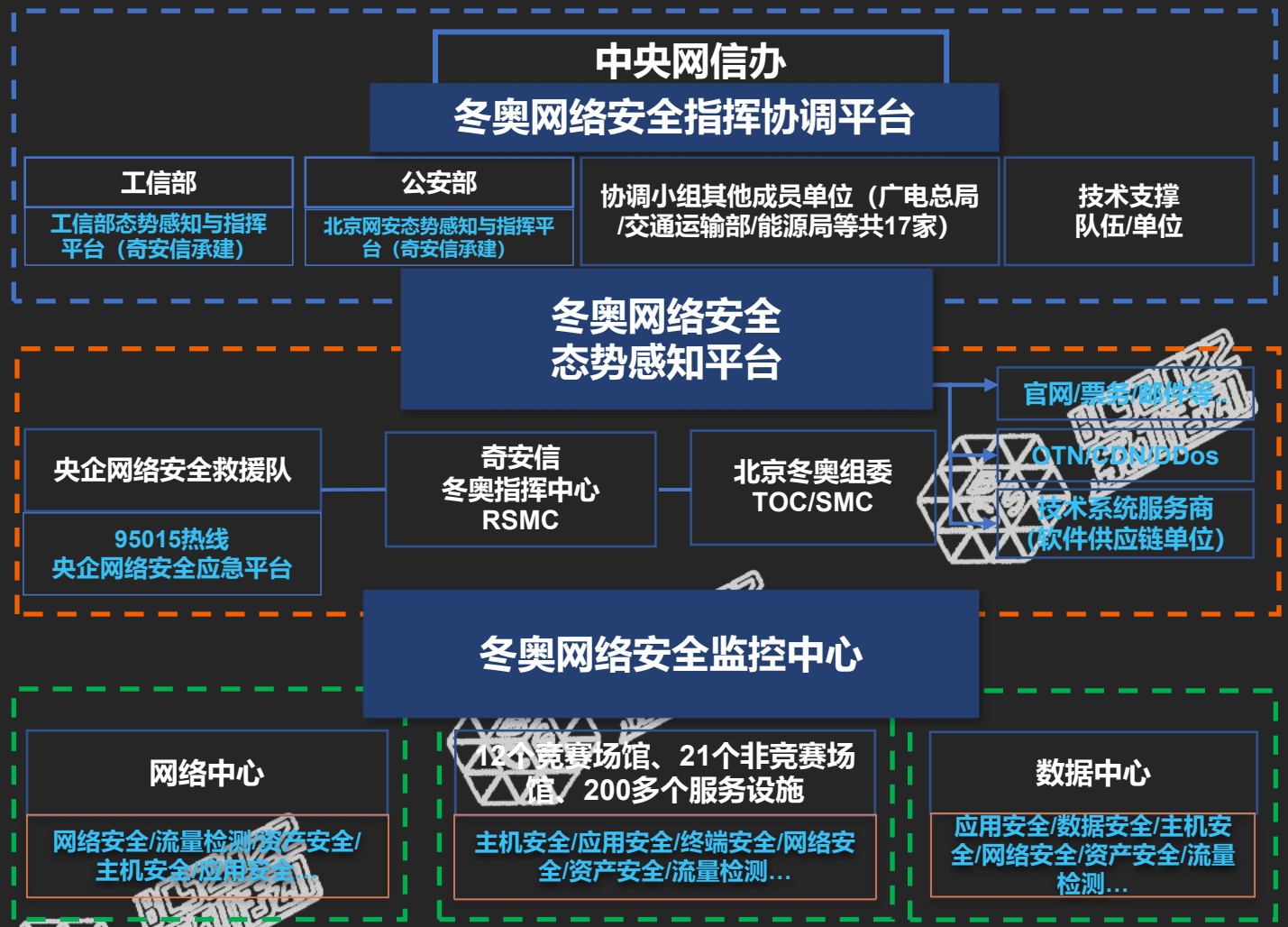
## 落地定位

以大数据体系建设的思路，建立智能开放、知行合一的网络安全治理平台，使其成为监管机构治理、保卫网络安全的核心抓手

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

# 体系保障 - 冬奥重保态势感知研判与指挥三级保障体系




**3级.研判指挥**
研判分析
国家网络安全力量资源协同
指令下达

**2级.态势感知**
拉通北京冬奥组委
奇安信、关键单位全局

**1级.安全监控**
全局监控、响应处置
事件上报、闭环运行

重保 决策 指挥 — 宏观态势

重保 分析 研判 — 中观态势

日常 安全 运营 — 微观态势

三级联动+各司其职+高速响应+闭环运行

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

# 设计理念 — 知行合一

**核心：建立网络空间安全治理的总抓手和总平台**

有效监管 决策指挥 协同联动 步调一致

## 知

- 知己
- 知彼
- 知威胁

## 行

- 通报预警 整改加固
- 情报共享 持续运营
- 应急指挥 重保指挥

总书记在4.19讲话中明确指出：

要全面加强网络安全检查，摸清家底，认清风险，找出漏洞，通报结果，督促整改。要建立统一高效的网络安全风险报告机制、情报共享机制、研判处置机制，准确把握网络安全风险发生的规律、动向、趋势。

奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

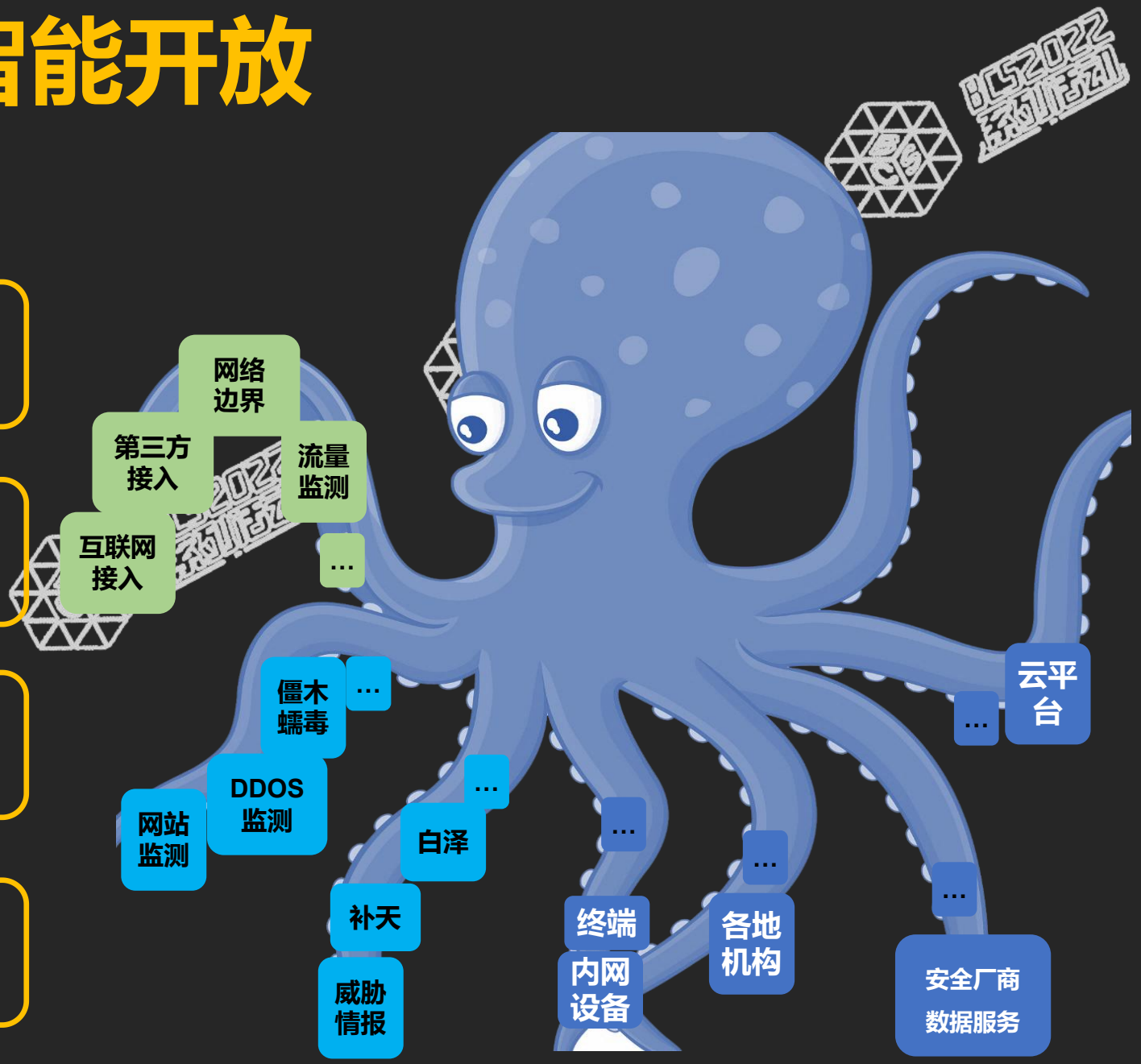
# 设计理念 — 智能开放

04 **大数据的思维与开放的平台**
平战结合的实战化“行动力”

03 **业务导向的大数据分析建模技术**
专家经验 + 机器挖掘

02 **CS-LDM业务驱动的数据治理融合技术**

01 **开放式、全类别数据源采集技术**
全要素、多源异构



奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

# 以平台化思维，构建大禹平台：整合数据、技术、服务能力，体系化输出安全能力

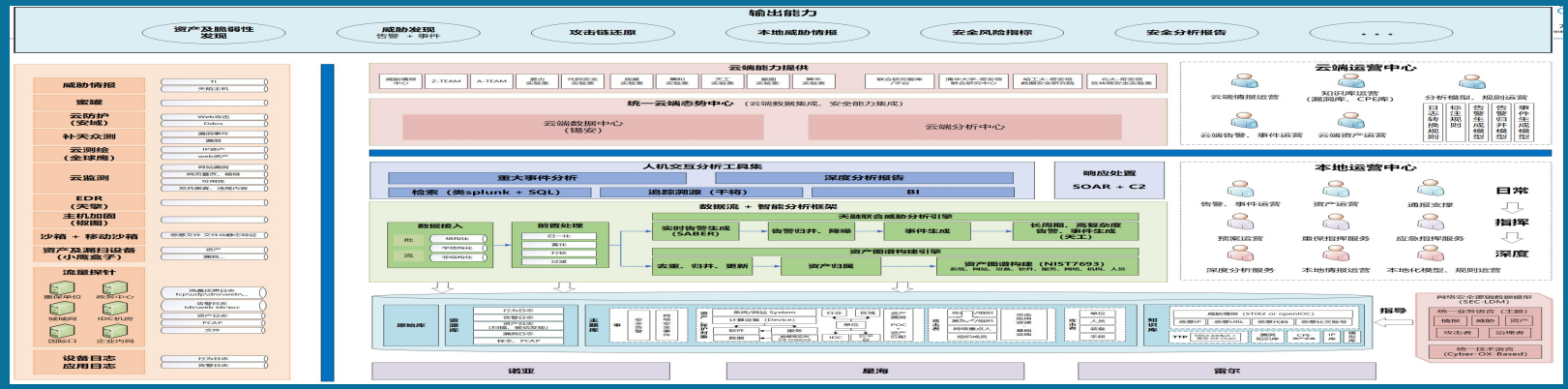
## 奇安信实战化态势感知（大禹版）

**决策层面**（3D可视化、N+场景、30+图层、80+要素）

**操作层面**（业务功能、分析功能、运营功能，10大中心，50+模块）

| | | | | |
|---|---|---|---|---|
| 态势中心 | 资产中心 | 威胁中心 | 通报中心 | 指挥中心 |
| 情报中心 | 分析中心 | 报告中心 | 监督考核 | 工作台 |

**能力底座 - 大禹平台**（整合数据、技术、服务能力，体系化输出安全能力）



奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

# 能力基座-大禹平台总体架构

SAAS

| | | | | | |
|---|---|---|---|---|---|
| 挂图作战 | 实体画像 | 报告管理 | 信息共享 | 重保指挥 | 应急指挥 |
| 告警管理 | 事件管理 | 事件分析 | 场景化分析 | 追踪溯源 | … |
| 全局检索 | 高交互分析 | 云查 | 知识库 | 情报管理 | 资产管理 |

**安全应用平台( dayu-secapp-platform)**

**安全应用平台（应用超市）：**

提供资产、告警、事件、情报、检索等核心应用，支撑业务快速产品化。

DAAS

| | | | | |
|---|---|---|---|---|
| 网络安全逻辑数据模型（QAX-SEC-LDM） | | | | |
| 诺亚 | 玄机 | 天工引擎 | 联合分析引擎 | BI引擎 |

**安全大数据平台 ( dayu-secdata-platform)**

**安全大数据平台：**

基于安全数据模型，提供数据接入、治理及工具集，为数据驱动的安全业务开发提供支撑

| | | | | | |
|---|---|---|---|---|---|
| 权限管理 | 运维监控 | 配置管理 | 许可证 | 审计管理 | 升级管理 |
| 备份还原 | 数据监控 | 消息中心 | 字典管理 | 标签管理 | 级联管理 |

**安全运行框架（dayu-runtime-framework）**

**安全运行框架：**

可扩展、高可用、高性能、强安全的服务运行框架：

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

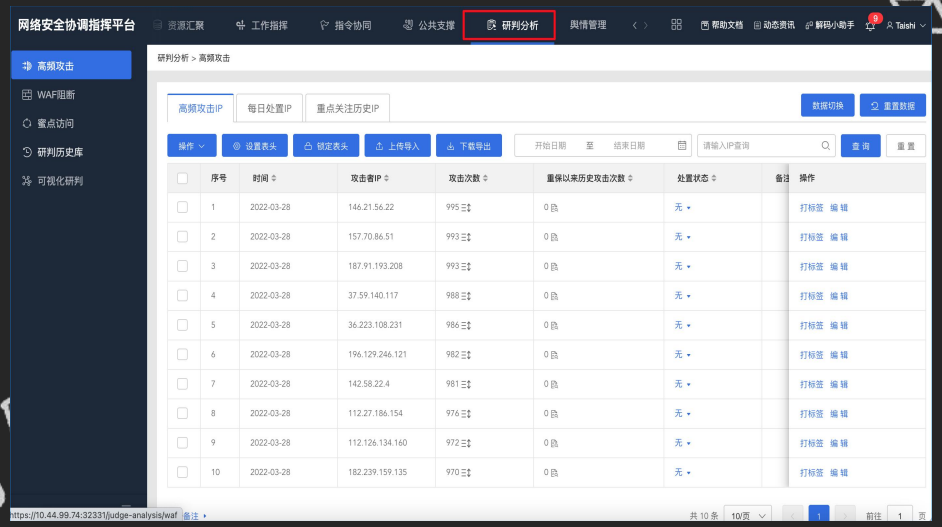
# 操作层面（业务功能、分析功能、运营功能，10大中心，50+模块）

奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

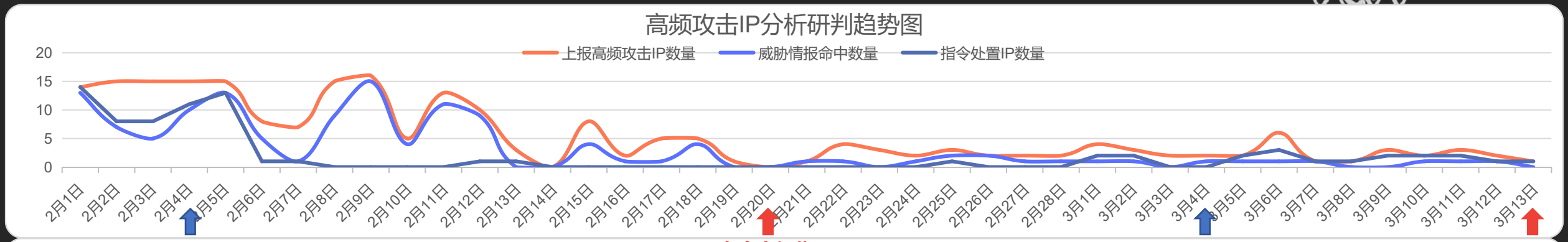
# 系统展示（部分）

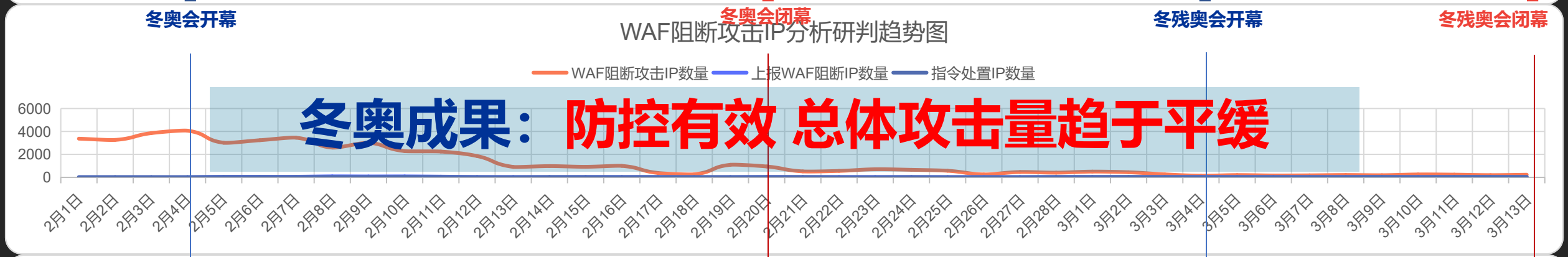




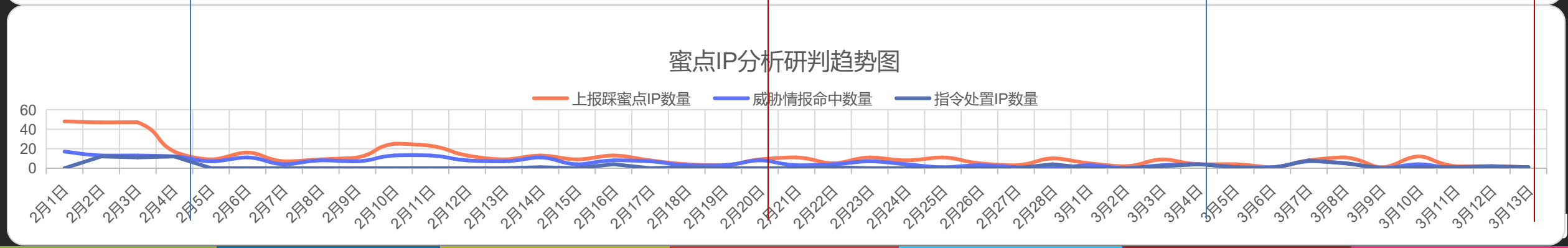

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

# 冬奥成果：攻击量受压制，实现零事故承诺




**冬奥成果：防控有效 总体攻击量趋于平缓**



奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

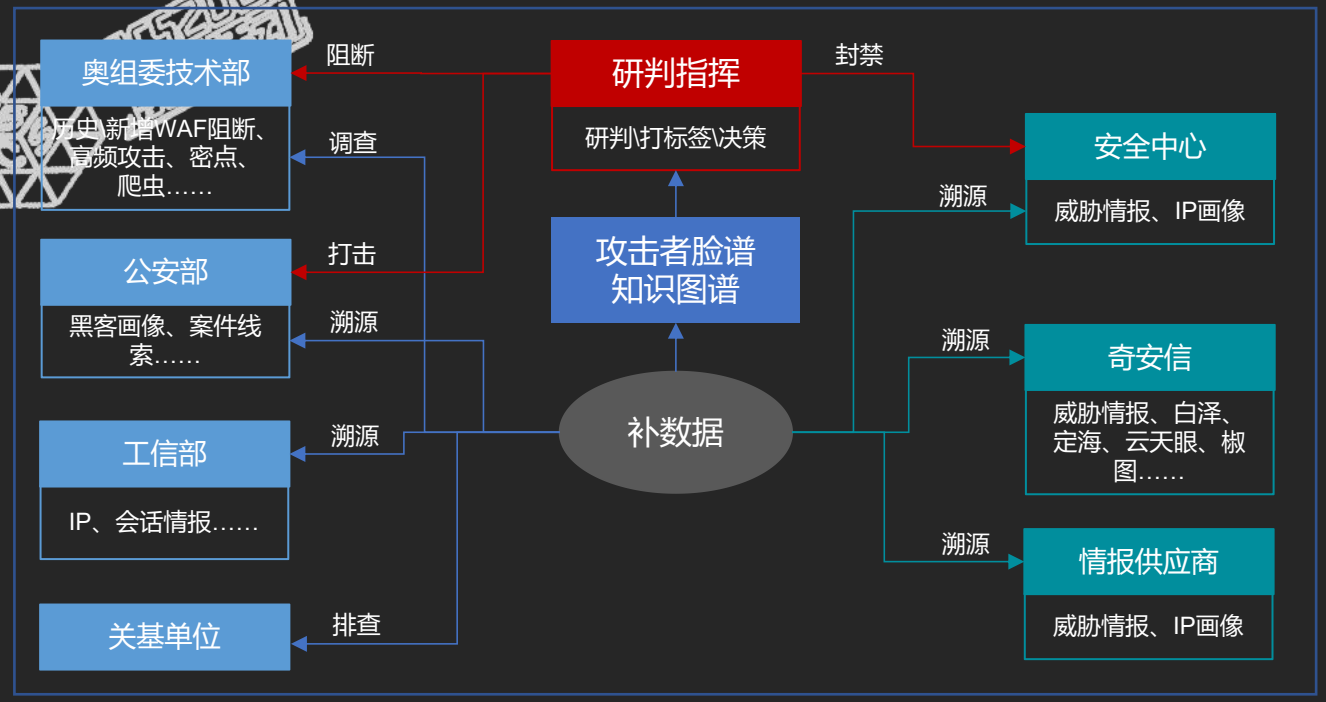
# 冬奥成果：基于六步法的关口前置研判指挥模式

1.汇数据 → 2.去噪音 → 3.找异常 → 4.补数据 → 5.做研判 → 6.下指令

**【传统被动】**
- ■被动防守
- ■阈值-触发式
- ■应急为主
- ■保下限

＋

**【新型主动】**
- ■主动出击
- ■脸谱-预案式
- ■控制打击为主
- ■提上限




**冬奥战略：主被结合，先发制人，降低不确定性，御敌边界之外！**

奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

# 实战体会

平台须具备**业务**、**数据**、**技术**、**服务**、**安全**、**呈现**、**交付**七大能力

这些能力，需要用**平台化**的思路进行**整合**，才能从**散碎**走向**体系化**

**实战化**的指挥平台，**必然是**一个庞大的工程体系，不可能一蹴而就

否则，**数据**能力、**资金**能力、**运营**能力、**人员**能力都很容易跟不上

但**顶层设计**很重要、**基因**很重要、**整体架构**很重要，否则伤筋动骨

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

BCS2022系列活动-冬奥网络安全“零事故”宣传周

# THANKS