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

揭秘冬奥背后的实时安全分析技术

韩鹏 奇安信集团技术合伙人

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

01 冬奥与网络安全

奇安信

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

冬奥网络安全中的大数据

1000+

- 1000+数据源，涵盖终端、服务器、网络设备、安全设备、应用系统、业务系统等所有核心资产
- 1000+安全分析模型，覆盖云上、云下所有核心资产的威胁、异常、违规监测场景

35亿

- 日均35亿日志，峰值超每秒10万条日志，接入云上网络、主机、数据、监控审计四大部分共18类数据源、30余类日志

7x24

- 保障冬奥网络安全零事故，监测上千起安全事件，冬奥期间无任何稳定性和功能问题

奇安信

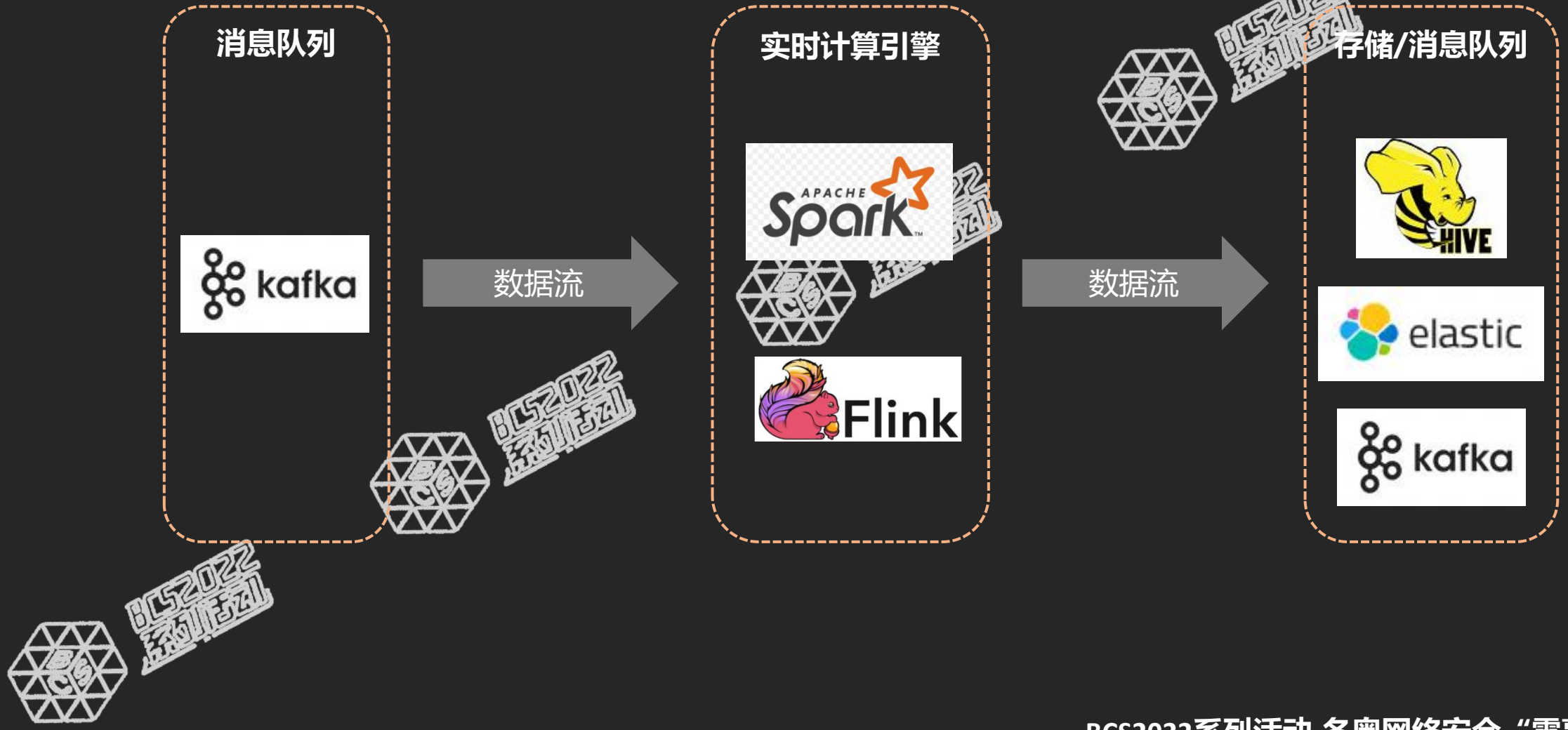
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

02 网络安全与实时计算

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

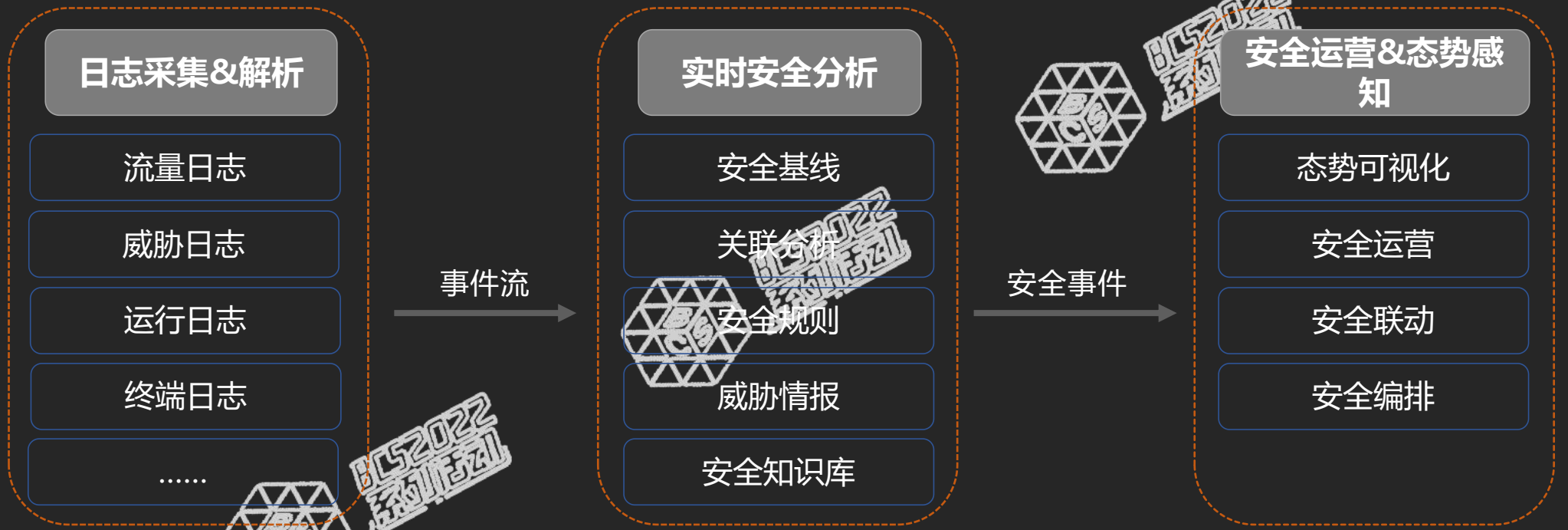
实时计算



奇安信 BEIJING 2022

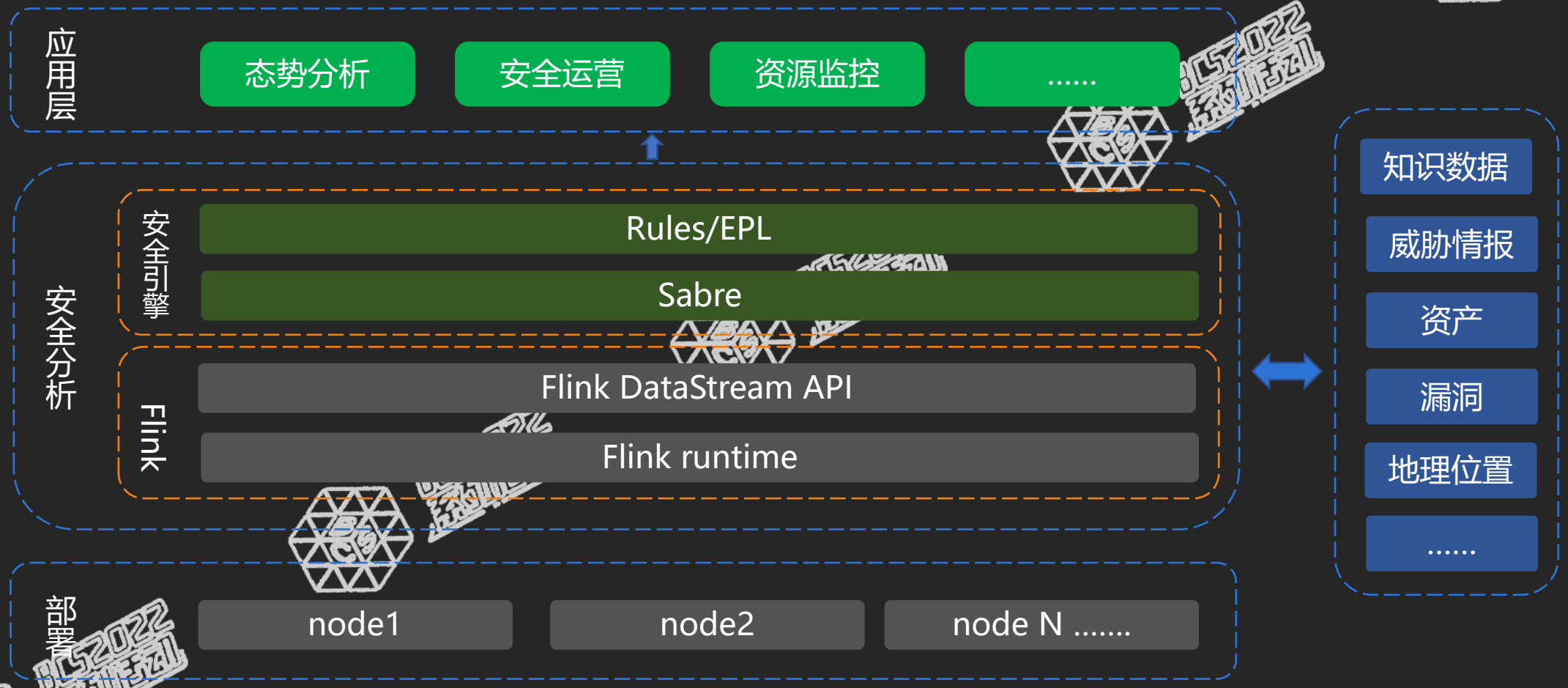
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

安全分析



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

实时安全分析



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

03 实时安全分析技术

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

数据源和数据类型

阿里云

Linux

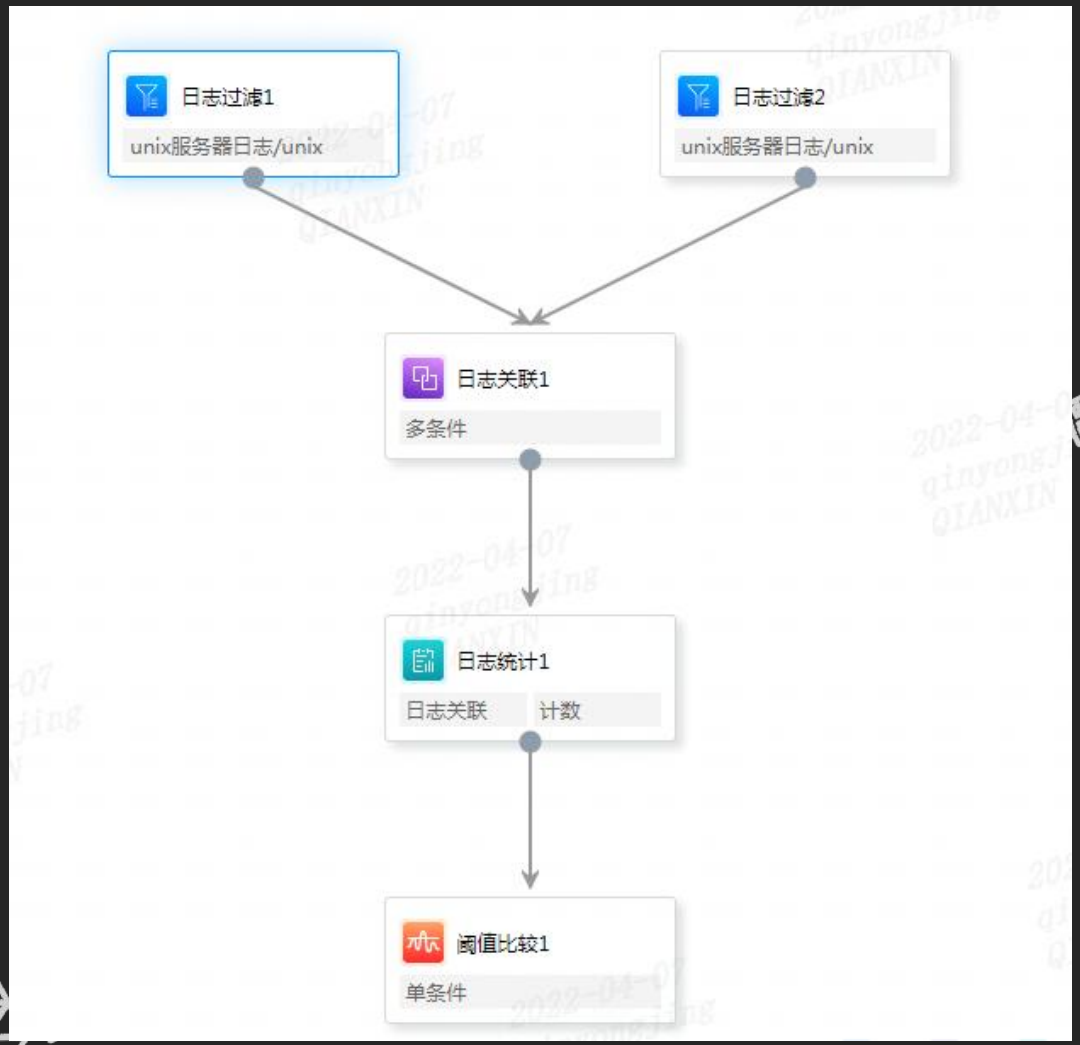
Microsoft

NGINX

网络中心、数据中心、云上系统以及众多场馆

云上网络、主机、数据、监控审计、EDR、NDR等30多类日志类型

分析工具-可视化建模



规则属性配置

计算单元配置

日志过滤名	日志过滤1
数据来源（日志类型）	unix服务器日志/unix

过滤条件 如何创建过滤条件？

AND

简单条件：事件类型 = (忽略大小写) PATH

简单条件：文件路径 匹配(忽略大小写) \/proc\/\d+\/maps

规则响应配置

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

统计分析

实时计算

- 实时时间窗口
  事件触发计算
  实时更新结果

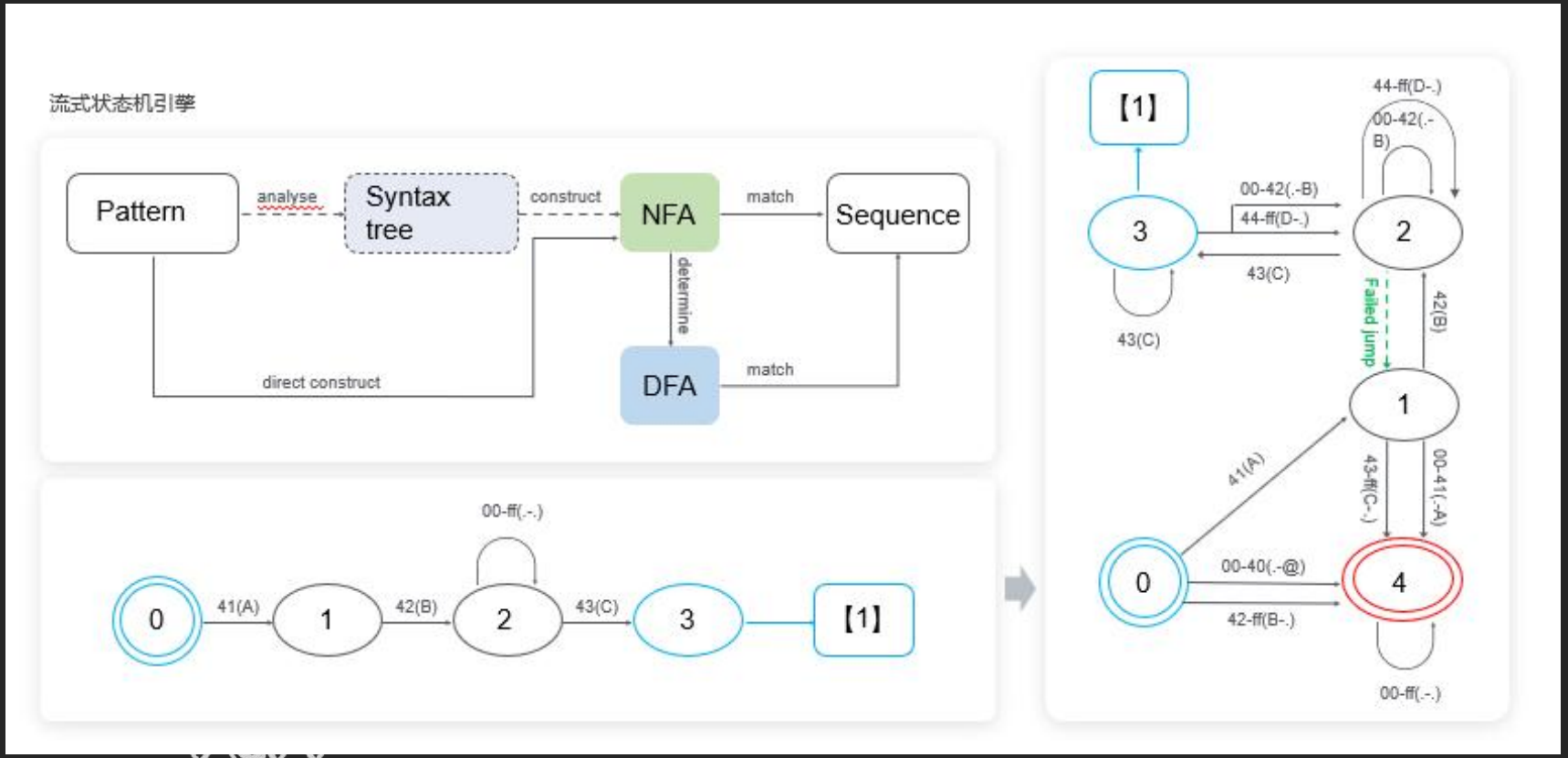
事件存储

- 存储当前活跃事件集
  实时删除无效/过期事件
  标记已使用事件

统计方法

- 最大值
  最小值
  平均值
  总和/乘积
  均方差
  统计机器学习
  序列

序列分析



重复匹配消除 → 局部乱序纠正 → 流式序列状态机

奇安信

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

关联分析

实时关联

- 时间线追踪
- 事件触发计算
- 实时更新/删除中间状态

安全场景增强

- 事件流时间线对齐
- 多流关联
- 重复关联消除

性能优化

- 条件前推
- hash join

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

行为分析

安全基线

- **统计类安全基线**
  - 时间类安全基线
  - 频率类安全基线
  - 空间类安全基线
  - 范围类安全基线
  - 多级统计类安全基线
- **序列类安全基线**
  - 指数平滑类安全基线
  - 周期类安全基线
- **机器学习类安全基线**
  - 聚类安全基线
  - 决策树类安全基线

大规模规则优化方法-规则计算优化

公共表达式优化

- 对EPL中相同语义逻辑进行优化

引用数据表优化

- hash匹配
  大规模IP匹配优化
  大规模正则匹配优化

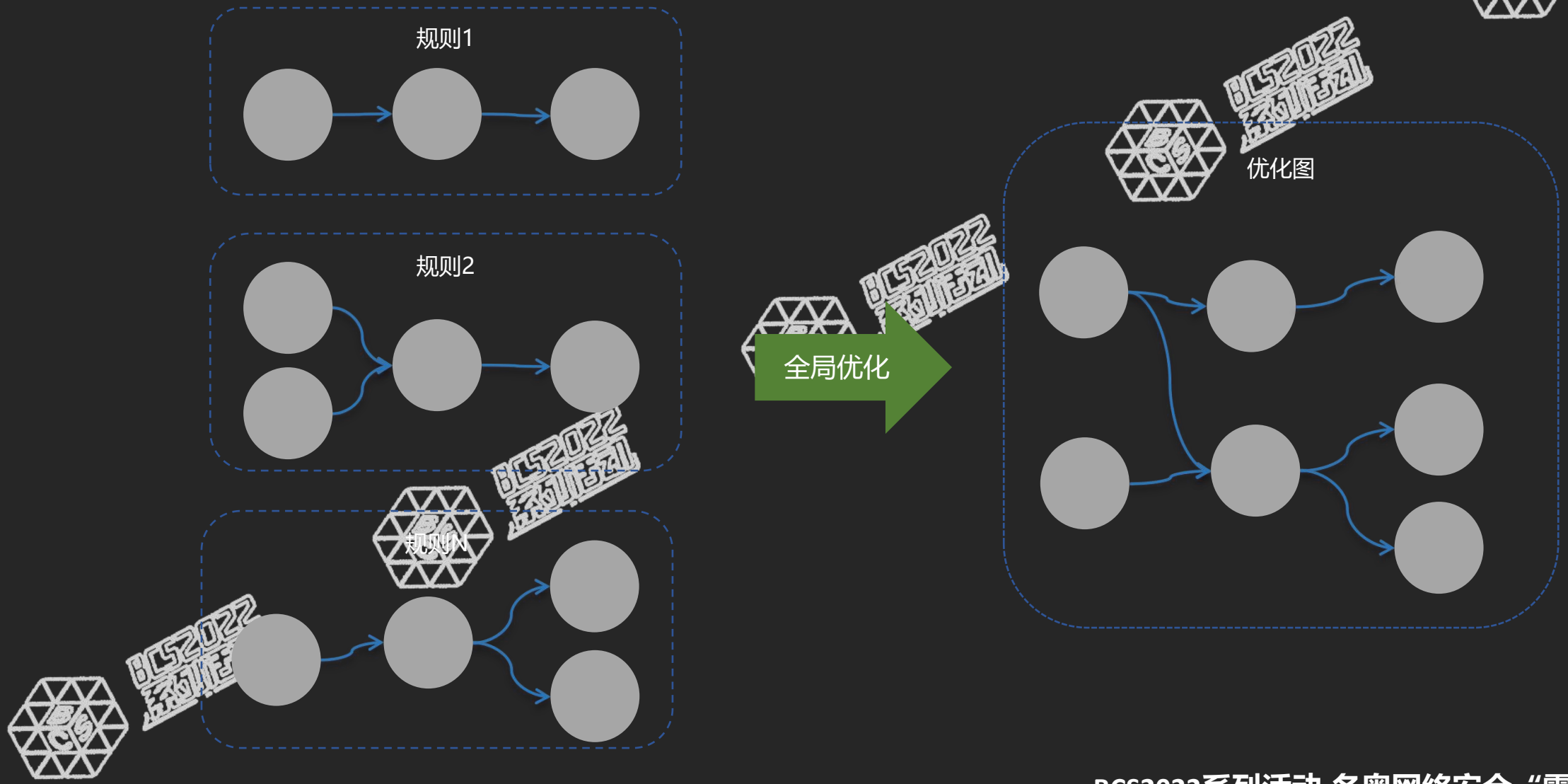
常量表达式优化

- 预计算各种常量表达式

表引用优化

- 引用实例归并
  引用语义归并

大规模规则优化方法-全局规则优化



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

图优化方法

图融合

- 子图融合
  图节点语义融合
  时间窗口归并
  公共资源优化

数据流优化

- Key前置
  语义等价节点融合
  网络吞吐均衡
  节点归并

字段裁剪

- 图上字段推导、裁剪
  字段归并

代码生成

- DSL代码生成
  图代码生成
  执行图映射
  DataStream API

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

大规模数据检测的优化方法

大规模串匹配优化

- 超大规模串正则匹配引擎（100w+）
- hash匹配

大规模IP匹配优化

- 精确匹配
- 范围匹配
- 模糊匹配

大规模知识库存储和匹配优化

- 威胁情报、资产、漏洞
- Bloom Filter
- 内存+磁盘多级计算

资源监控和保护

稳定性增强

- 计算内存监控
- 计算内存保护
- 资源优先级管理
- 计算资源保护
- 慢路径发现
- 子图隔离

状态监控

- 图节点状态跟踪
  CPU、内存、磁盘、输入、输出、运行状态
  逻辑&处理延迟监控
- 图状态跟踪
  大规模图状态报告优化
  图状态->规则状态映射

流量控制

- 主动流量控制
  被动流量控制
  时间窗口控制

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