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

北京冬奥会网络安全“零事故”中国架构分享

尹智清 奇安信冬奥保障总架构师

冬奥网络安全“零事故”宣讲团专家讲师

奇安信

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

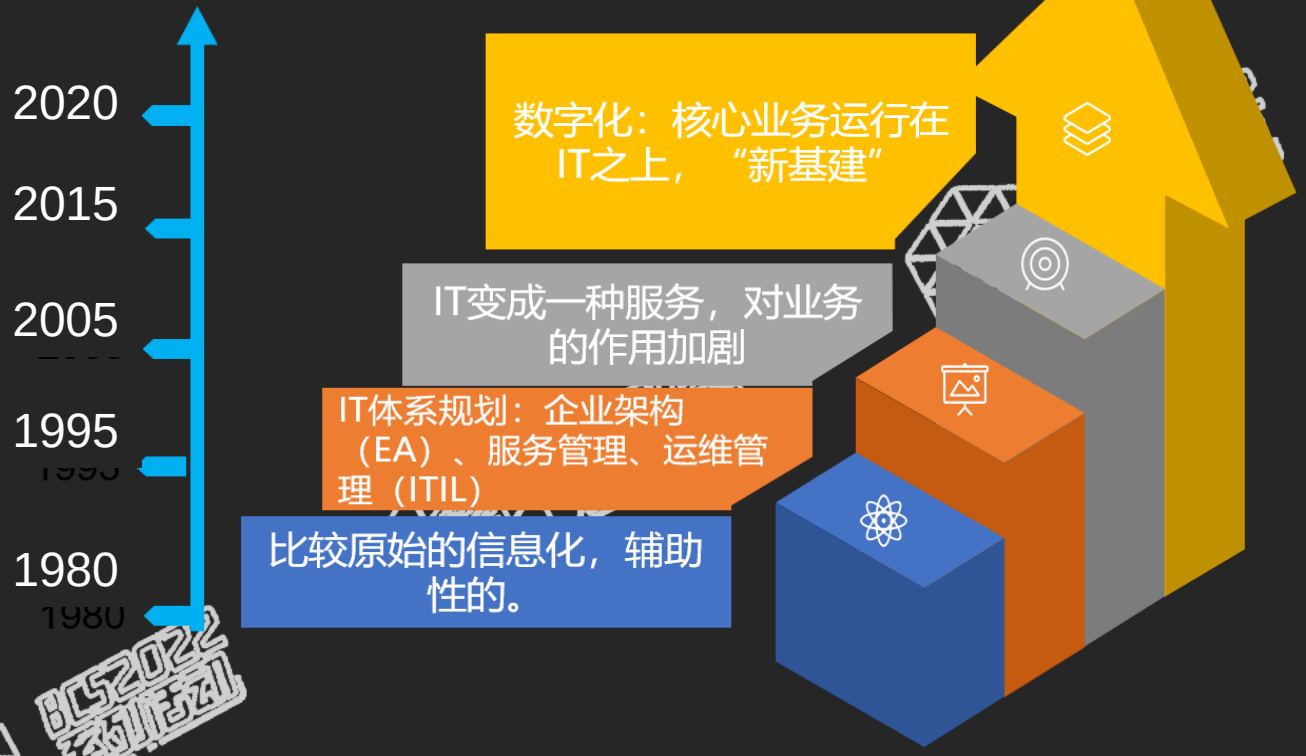
01 北京冬奥会网络安全体系架构设计方法

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

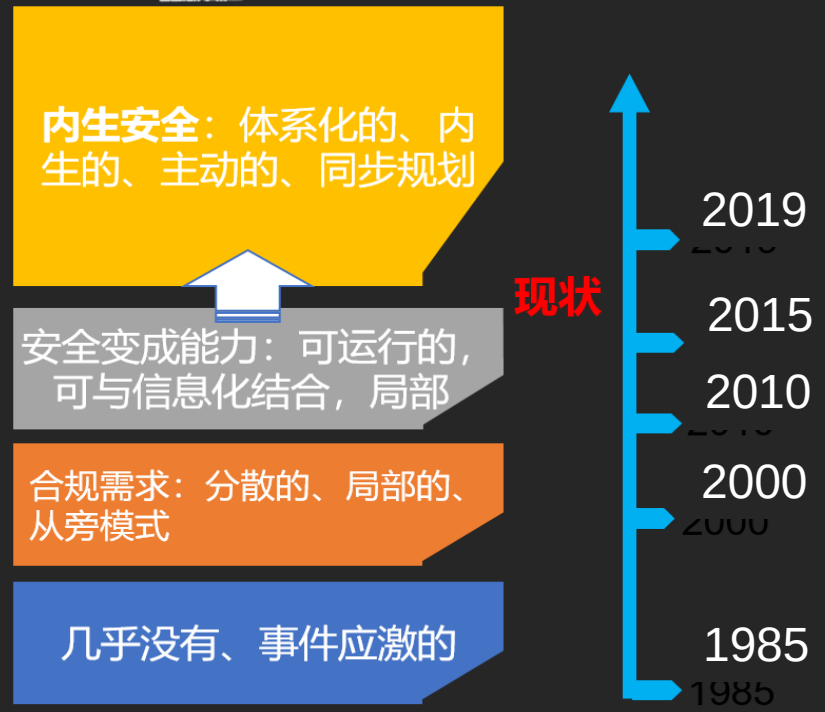
安全脱节于信息化发展，没有方法论

目前网络安全采用的是“局部整改”为主的建设模式
体系化缺失、碎片化严重，和信息化的系统化发展不匹配

信息化发展历程



网络安全发展历程



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

网络安全面临的六大风险

供应链攻击

20年底，黑客组织攻击IT管理软件SolarWinds，至少200家重要机构受害。其中，美国受害最严重，美国国土安全部、财政部、核安全管理局等多个重要机构都受到波及。
2021年7月2日，勒索组织利用IT软件供应商Kaseya发起供应链攻击，数千家企业受到影响。

APT攻击

“海莲花”组织对中国政府、科研院所、海事机构、海域建设、航运企业等相关重要领域展开了有组织、有计划、有针对性的长时间不间断攻击至少已持续8年。

内部威胁

FBI和CSI等机构联合做的一项安全调查报告显示，超过85%的网络安全威胁来自于内部，危害程度远远超过黑客攻击和病毒造成的损失。

勒索攻击

2019年5月1日至2021年6月8日，全球目前大约有2445个组织遭到勒索软件攻击。

系统漏洞

1990年-2019年，Windows平台提交漏洞总计6814个，平均每月发现漏洞27个。

国家级对抗

中美在科技领域竞争、对抗升级，以数字权力和科技利益争夺为目标，网络安全领域的对抗将成为重要手段。

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

网络安全只是技术问题吗？

在网络安全“新管理”模式下，强调**辩证统一的“七分管理三分技术”**。

安全体系的建设与运行是与企业安全策略、组织架构、企业架构管控、安全资源投入紧密相关。

面对数字化转型网络安全风险的高度不确定性，企业要把**网络安全工作模式**从“可选配合”升级为**“不可或缺的基础保障”模式**，要以**体系化、实战化、常态化**的理念加强顶层设计，构建网络安全基础设施，**面向安全成果进行评价考核，以数据分析结果牵引安全体系优化强化，**为数字化提供**“安全底板”**，夯实网络强国建设的网络安全基础。

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

体系化识别出网络安全存在的问题

安全建设从未停止但网络安全问题依然严重

普遍性问题

与业务融合度不高： 安全未能真正成为业务的一部分。安全与信息化的距离太远，与业务更远，对业务的价值不明显。

缺乏方法论指导： 未能像IT一样采用类似EA的系统工程方法论指导，安全建设不成体系，形成了零敲碎打、局部整改模式。

缺资源： 资源保障长期不充足。
因为规划里面没定义出来关键任务、技术路线，不知道在那些地方投入。
认为安全已经做得到位了，不需要再持续投入。

缺人： 因为大量工作没有显性出来，大量必要的工作缺相应的负责人。

缺运行： 运行不闭环。大量隐性工作，没有纳入运行；应急能力差；部门协同障碍。

缺技术： 广度不足、深度不深，落地不到位。

人防与技防结合不足： 非安全岗人员安全意识不足，觉得安全和自己无关，技术上缺乏足够的技术手段去控制，导致制度无法落实。

缺协同： 用了很多技术，整合不起来，碎片化、能力割裂，发挥不了作用。

缺应急： 安全资源、能力就绪度低

缺条令： 安全运行可持续性差。
大量隐形工作未显化，不知道干什么事情，没有人干。

缺基础： 安全体系基础设施不完备，IT资产管理混乱，基础较弱，不能完全知道要保护哪些IT资产？

缺深度： 与信息化各层次结合程度不高，不深入，两张皮

缺广度： 安全对信息化环境的覆盖面不全，盲点导致整个安全体系失效。（木桶效应）

缺乏全景框架： 看不清、看不全缺乏框架指导。

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

网络安全战略与管理理念的转变

数字化转型带来的业务运营与数字技术的深度绑定，以及国家网络安全监管要求的不断提升，对网络安全管理提出了更高的要求，驱动着网络安全管理理念的转变，**“网络安全管理”本身同样面临“数字化转型”的需要。**网络安全管理模式需要与数字化转型相适应，进而演进为网络安全的“新管理”模式。

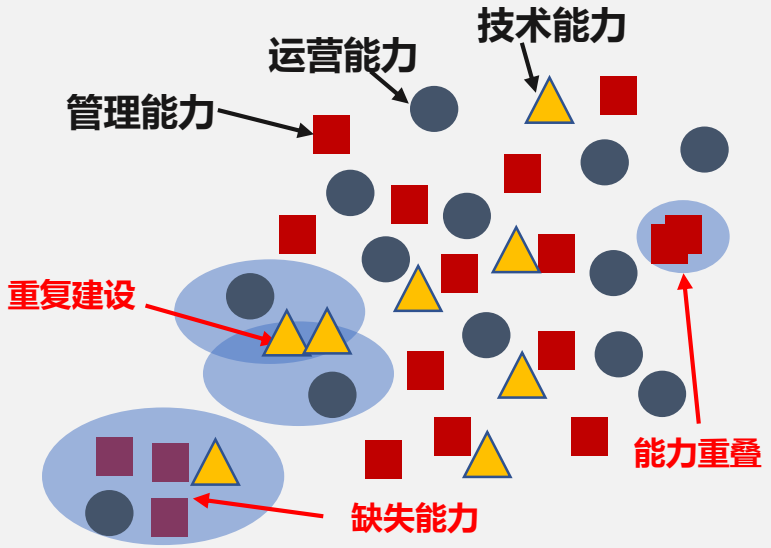
转变

安全损失	从“业务效率损失”到“企业运营停摆”
安全假设	从“边界内皆安全”到“新安全假设”
安全建设	从“被动建设”到“规划牵引”
安全能力	从“静态安全能力”到“动态安全能力”
安全姿态	从“事后应急姿态”到“事前防御姿态”
安全责任	从“安全部门责任”到“全员责任”
内部协同	从“零散割裂”到“体系化协同”
外部协同	从“单打独斗”到“企业-国家协同联动”

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

通过规划实现体系化建设

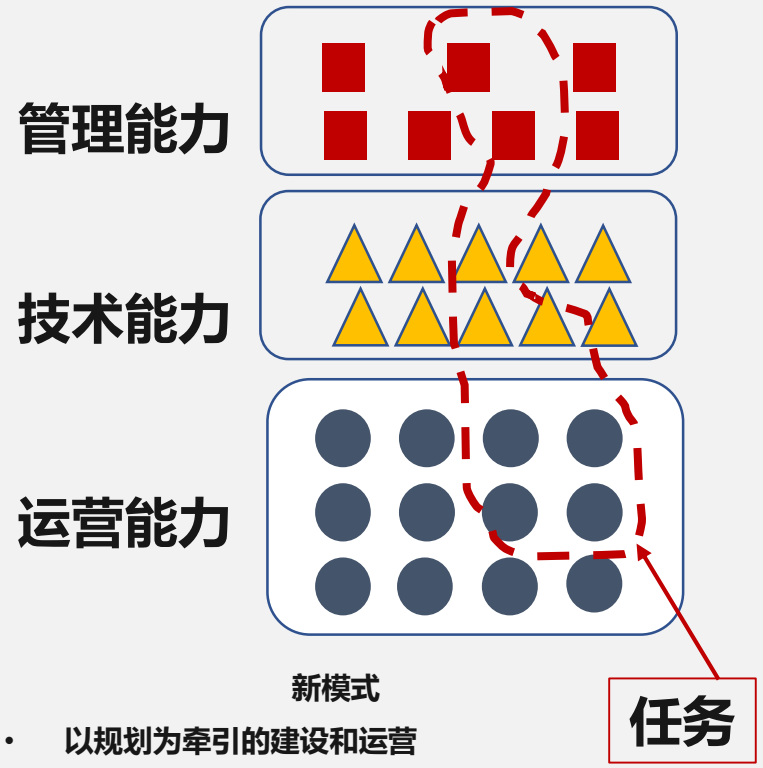
每一个任务设置要将管理、技术、运行等各方面的要素综合考虑，避免割裂。各任务之间相互关联、能力互补，形成有机的整体，具备体系化作战的能力。



旧模式

- 规划与建设、运行未统一
- 零散的项目设置
- 项目间相互独立、能力割裂、缺乏联动
- 关注短期建设

演进



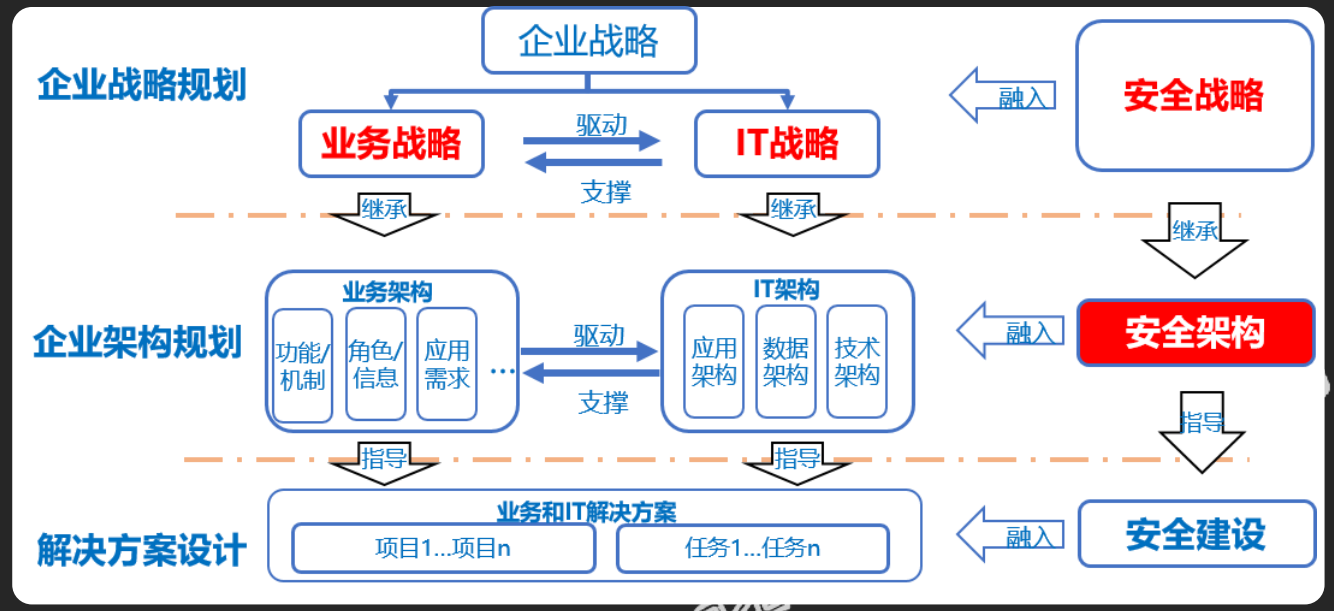
新模式

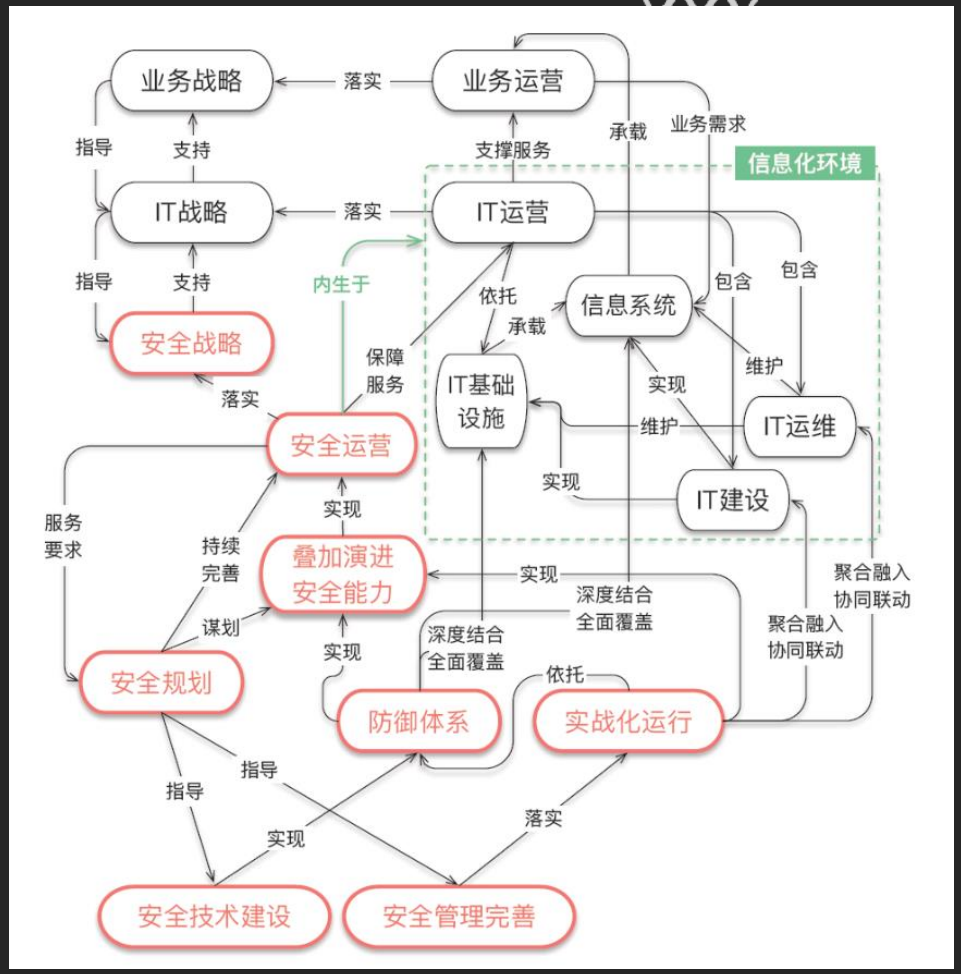
- 以规划为牵引的建设和运营
- 统一规划、分步建设
- 安全能力可扩展的、可集成、可协同
- 关注体系化作战、持续的安全效果

体系化规划与建设的特点

① 消除安全能力重复、缺失、异构
② 能力体系完整、逻辑合理
③ 安全管理、技术、运营一体化设计、天然协同、避免割裂

将EA方法论应用在网络安全领域





- 以获得组织所需要的“能力”为目标
- 重点关注“巨系统、构成系统”的完整性、联系性、协同性
- 功能分配、系统对接、数据互通、平行扩展

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

内生安全理念

内生安全理念，是指将网络安全能力与信息化环境融合内生，
而不再是外挂和局部的，从而在数字化环境的内部，获得无处不在的“免疫力”

内生安全体系是实现在网络变革下，信息化建设和网络安全之间、安全公司和客户之间实现共赢选择。

构建内生安全体系有三个关键：

- 一是旨在面向政企数字化的网络安全体系化建设与工程化落地，坚持“三同步”原则，即同步规划、同步建设、同步运营；
- 二是运用三种聚合手段，即技术聚合、数据聚合、人才聚合；
- 三是以网络、身份、应用、数据、行为，以及数据驱动的安全运营，多维度技术与运行手段，构建支撑政企数字化业务运营的内生安全能力体系。

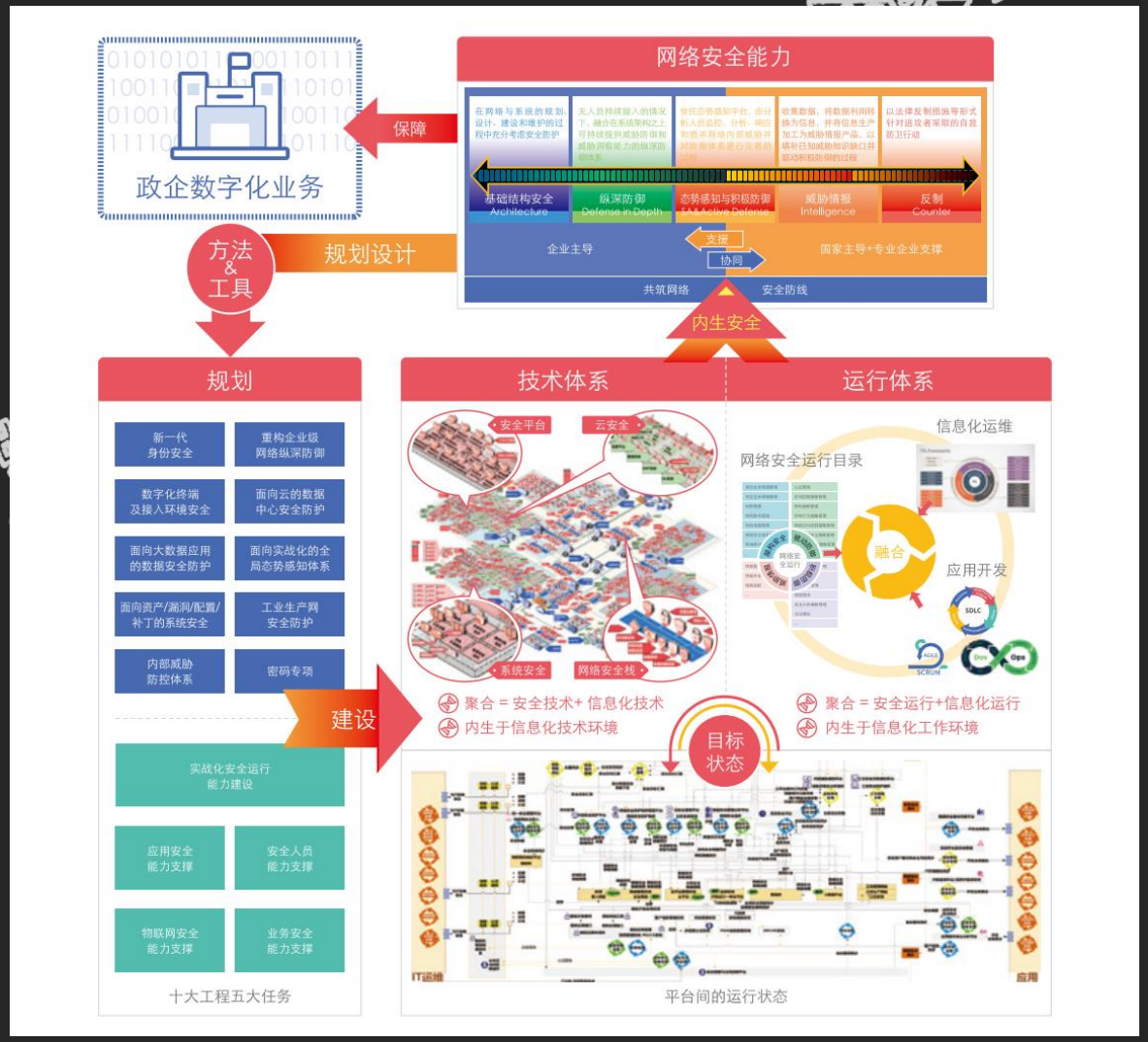
奇安信 | BEIJING 2022

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

实现内生安全是采用系统工程的方法实现网络安全体系化建设

内生安全系统工程，就是把安全能力内置到业务系统中，感知、响应对业务系统和数据的任何破坏行为，真正做到“事前防控”。

- **从局部整改、辅助配套的建设模式为主，走向深度融合的体系化建设模式；**
- **面向新基建建设、数字化业务，以系统工程方法论结合内生安全理念，形成新一代网络安全建设框架；**
- **以能力为导向的网络安全输出体系化、全局化、实战化的组件化安全能力，构建出动态综合的网络安全防御体系。**



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

内生安全框架落地的三个关键

内生安全框架以**系统工程方法论**结合内生安全理念，使得网络安全能力与信息化进行**内生融合**，从而在数字化环境内部产生“免疫力”。**网络安全能力**，从全局视角与信息化**“深度融合、全面覆盖”**，指导不同行业输出符合其特点的体系化、实战化的网络安全体系；从而产生1+1>2的“涌现”效果。在工程落地上，分为**“十大工程五大任务”**，满足新基建数字化、智能化的业务保障需求。

盘家底 01

- 体系化地梳理、设计出所需的安全能力
- 梳理时充分考虑所有可能涉及到的问题
- 设计时根据实际情况挑选、组合和规划

建系统 02

- 融合是建设的关键，深度结合全面覆盖
- 安全能力组件化，合理分配到正确位置
- 建设过程中，需要全景化技术部署模型

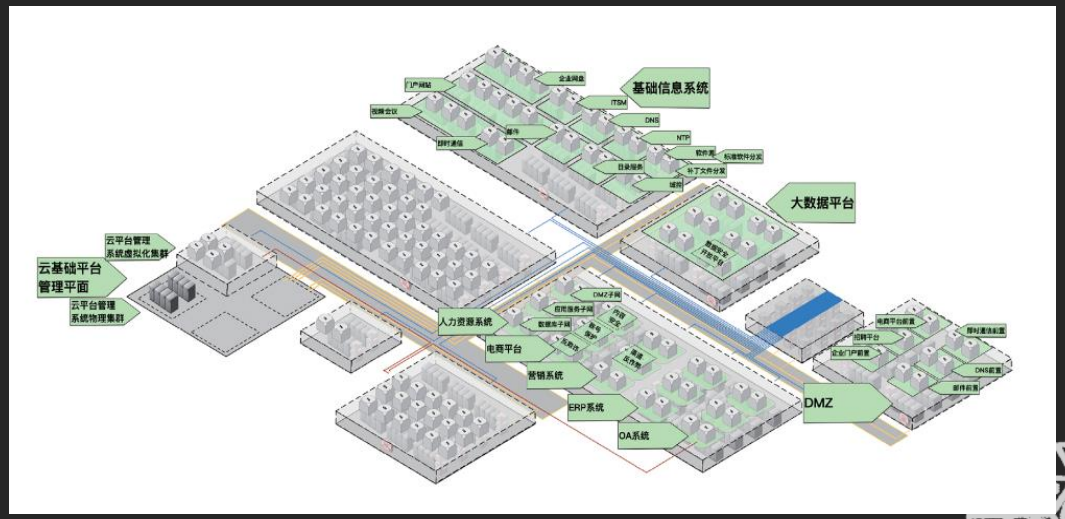
抓运行 03

- 缺乏安全运行的安全系统，相当于靠天吃饭
- 把管理作为关键，能跑赢漏洞、内鬼、黑客
- 确保安全运行可持续性，实现安全管理闭环

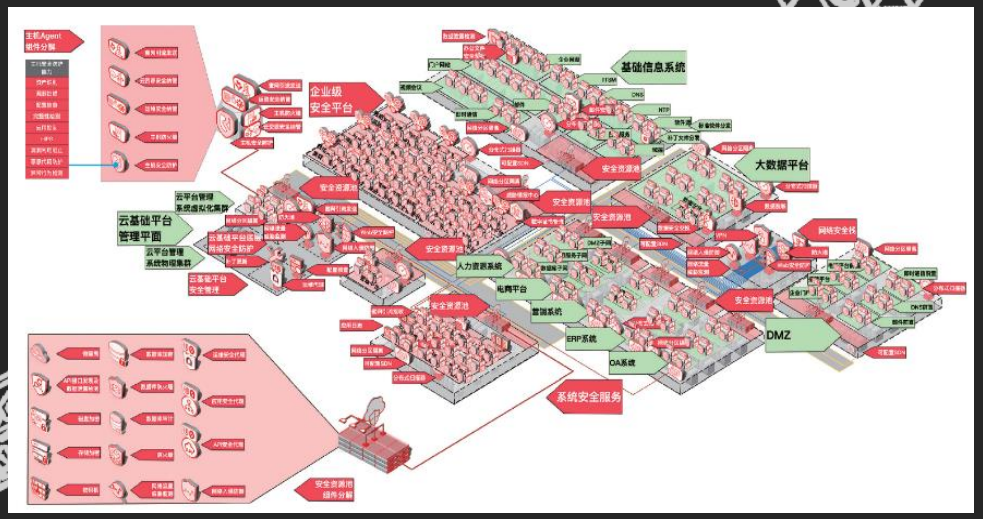
奇安信 | BEIJING 2022

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

盘家底：梳理并设计网络安全能力，梳理并设计信息化环境



理清信息化环境



理清安全能力

DNS安全防护	主机安全Agent	扫描器	Web安全防护	组件SDK	主机防火墙	零信任模式	资产测绘
API接口发现及数据泄露检测	网络准入	运维代理	恶意代码防范	安全开发包	数字证书	可配置	云抗D
密码机	日志审计	攻击诱捕	网络入侵防御	密钥管理中心	蜜网引流发送	软件源	靶场
智能选路	安全SD-WAN	数据脱敏	网络威胁监测	数字证书认证中心（CA）	白名单模式	安全工具	组件
邮件安全网关	日志采集	数据库防火墙	流量加解密	蜜网引流接收	定向流量采集	蜜罐	管理平台
流量复制	补丁更新服务	数据库审计	VPN	云资源安全纳管	IOT相关	蜜网	集群
微隔离	配置核查	数据泄露检测	网闸	API接口	工控相关	存储加密	系统
全流量监测	密钥管理	上网行为管理	入侵防御	应用日志	工控主机	磁盘加密	运行中心
安全代理网关	加密机	API安全代理	流量清洗	系统日志	可配置SDN	数据库加密	威胁情报落地中心
网络安全防护集群	沙箱	应用安全代理	数据安全交换	运维安全纳管	网络分区隔离	数据交换服务	

我们需要什么样的网络安全能力：滑动标尺、叠加演进

企业主导

国家主导

资产安全盘面	纵深防线盘面	威胁处置盘面	威胁情报
基础结构安全的防御姿态posture，主要就是解决“资产-漏洞-配置-补丁”问题的系统安全	纵深防御的防御姿态posture，是防护策略有效性，以构成坚实的防御“阵地”	积极防御的posture，是威胁发现能力和处置及时性有效	威胁情报的posture，是覆盖面、时效性和可执行水平

律手段
制措施

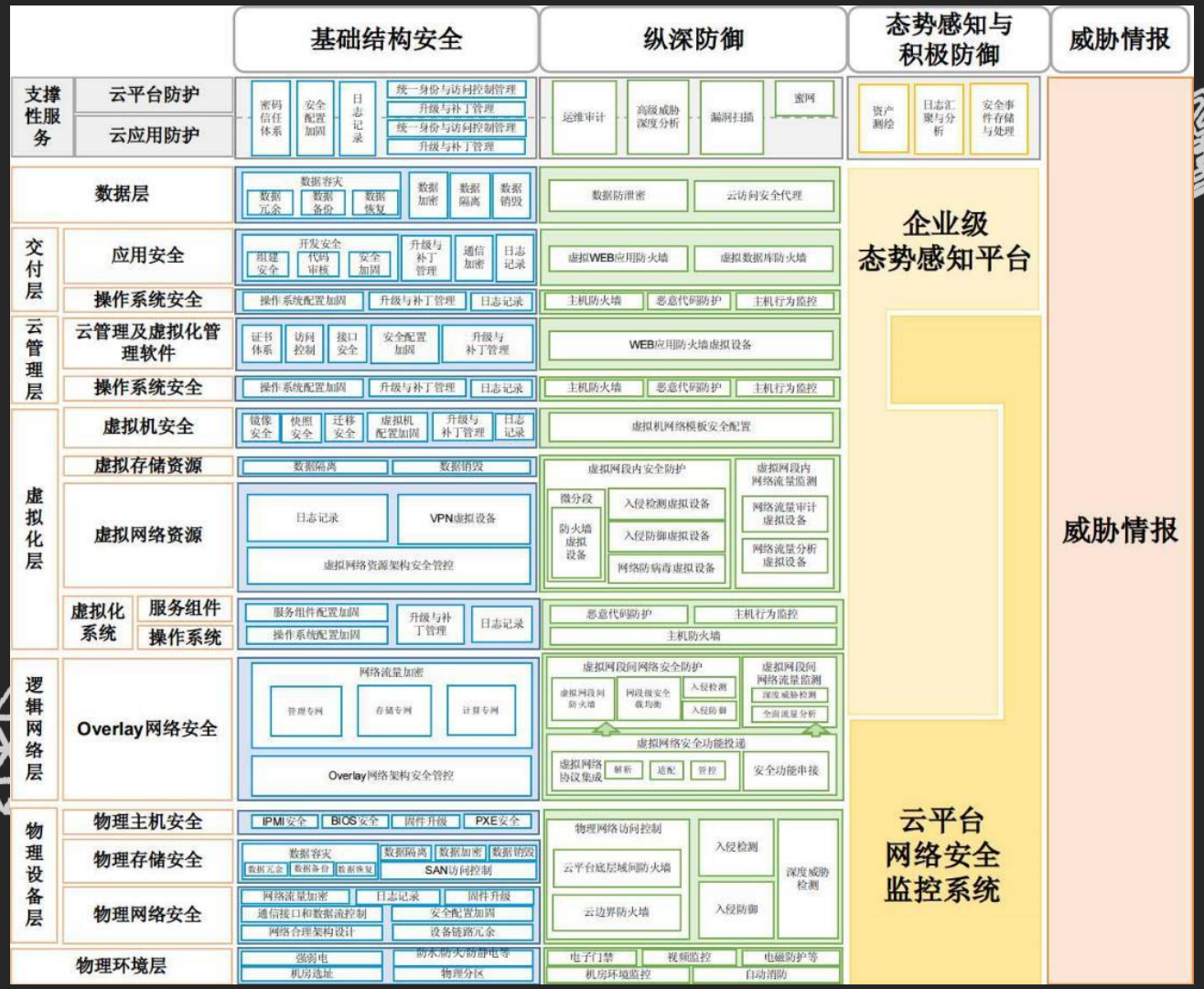
向部署
家威慑

处置支撑

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

从信息化视角看网络安全



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

建系统：基于全景化技术部署模型建设防御技术体系

在全景的网络覆盖区域融入纵深防御能力；

安全技术与信息化技术融合，安全能力全面融入信息化技术环境；

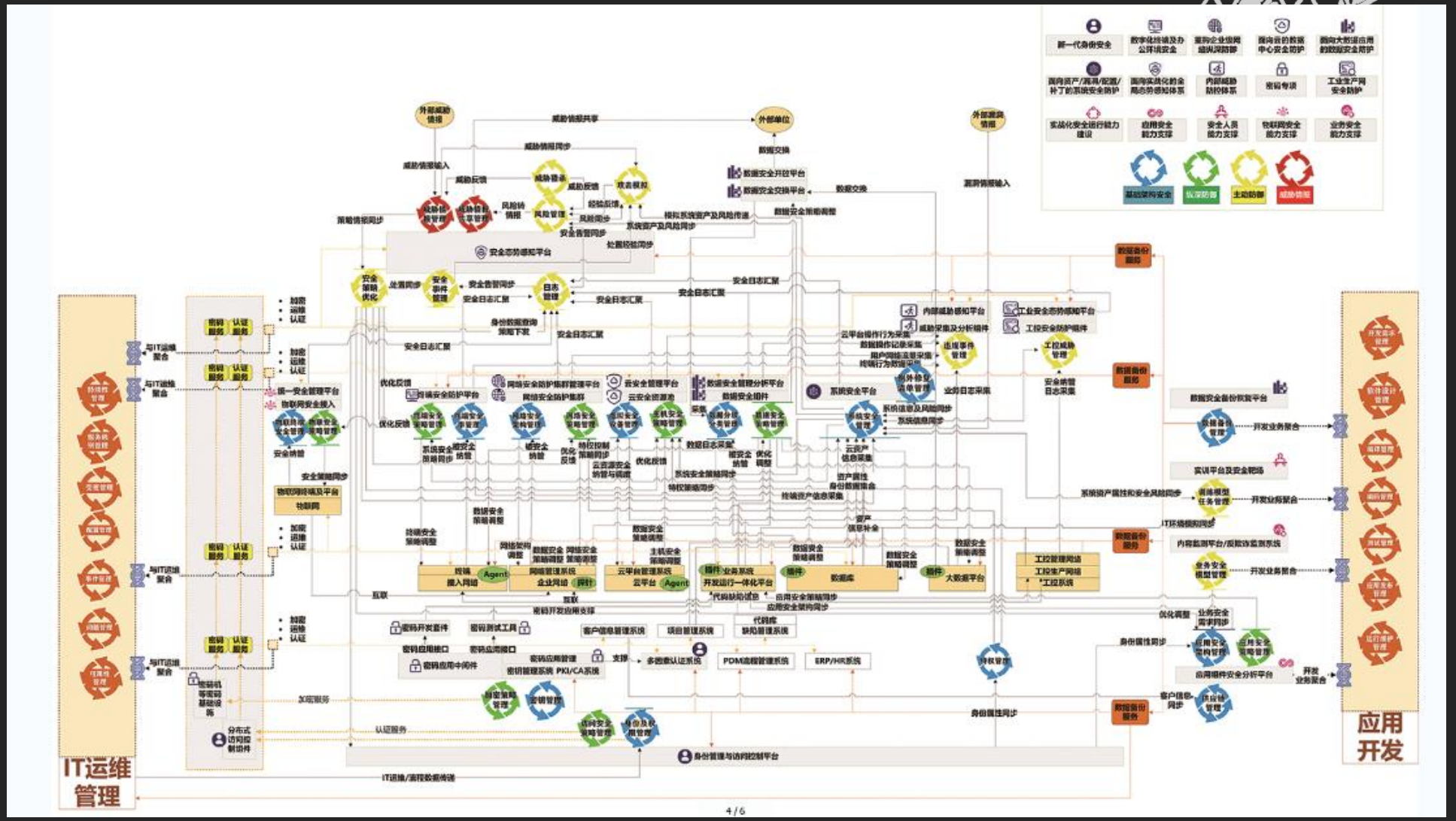
安全的全能力视图，覆盖整个信息化技术范围。

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

抓运行：基于内生安全框架构建安全运行体系全景图

通过安全与信息化技术聚合、数据聚合、人才聚合，构建一体化的协同运行能力。实战化的安全运行，要与信息化中的 IT运维、应用开发两大运行过程相协同。



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

“十大工程、五大任务”项目纲要库

甲方视角、信息化视角、安全全景视角，系统化的设计构建网络安全体系

十大工程

新一代身份安全

重构企业级网络纵深防御

数字化终端及接入环境安全

面向云的数据中心安全防护

面向大数据应用的数据安全防护

面向实战化的全局态势感知体系

面向资产/漏洞/配置/补丁的系统安全

工业生产网安全防护

内部威胁防控体系

密码专项

五大任务

实战化安全运行能力建设

应用安全能力支撑

安全人员能力支撑

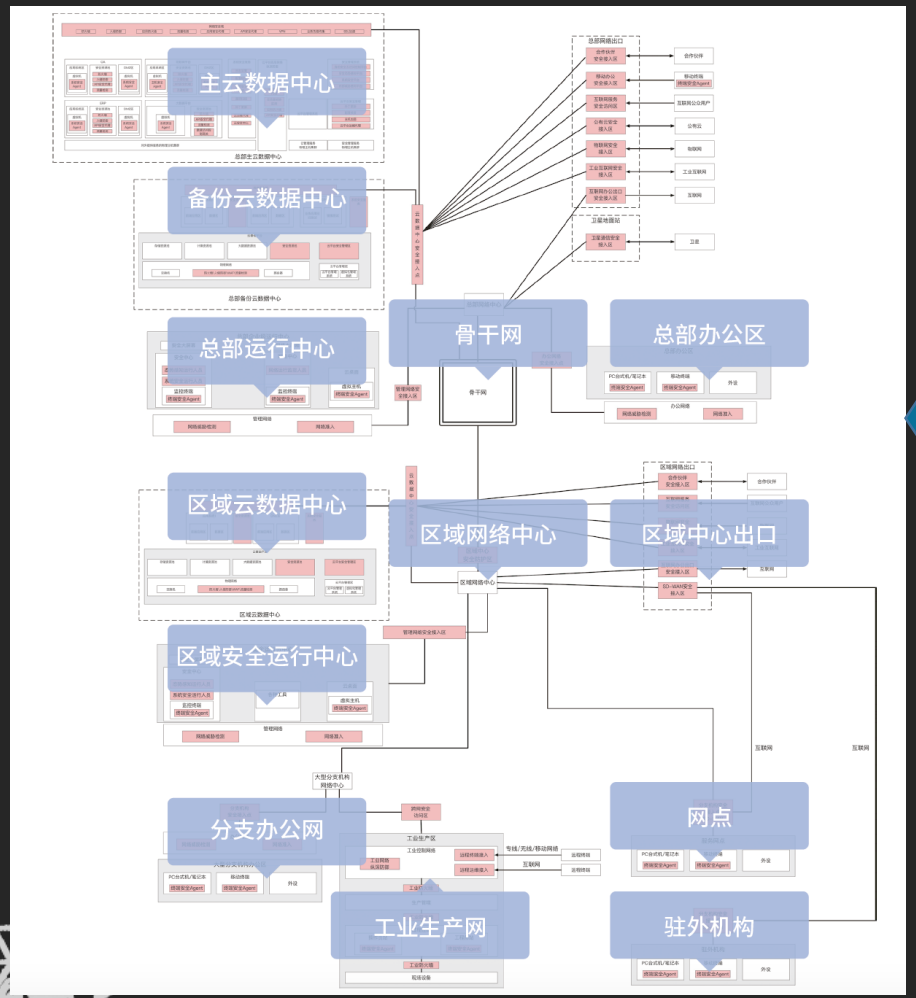
物联网安全能力支撑

业务安全能力支撑

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

安全能力与信息化技术体系融合全景



融入

十大工程

新一代身份安全	重构企业级网络纵深防御	数字化终端及接入环境安全	面向云的数据中心安全防护	面向大数据应用的数据安全防护
面向实战化的全局态势感知体系	面向资产/漏洞/配置/补丁的系统安全	工业生产网安全防护	内部威胁防控体系	密码专项

五大任务

实战化安全运行能力建设	应用安全能力支撑	安全人员能力支撑	物联网安全能力支撑	业务安全能力支撑

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 北京冬奥会网络安全保障体系总体设计和安全基础设施设计

奇安信

BEIJING 2022

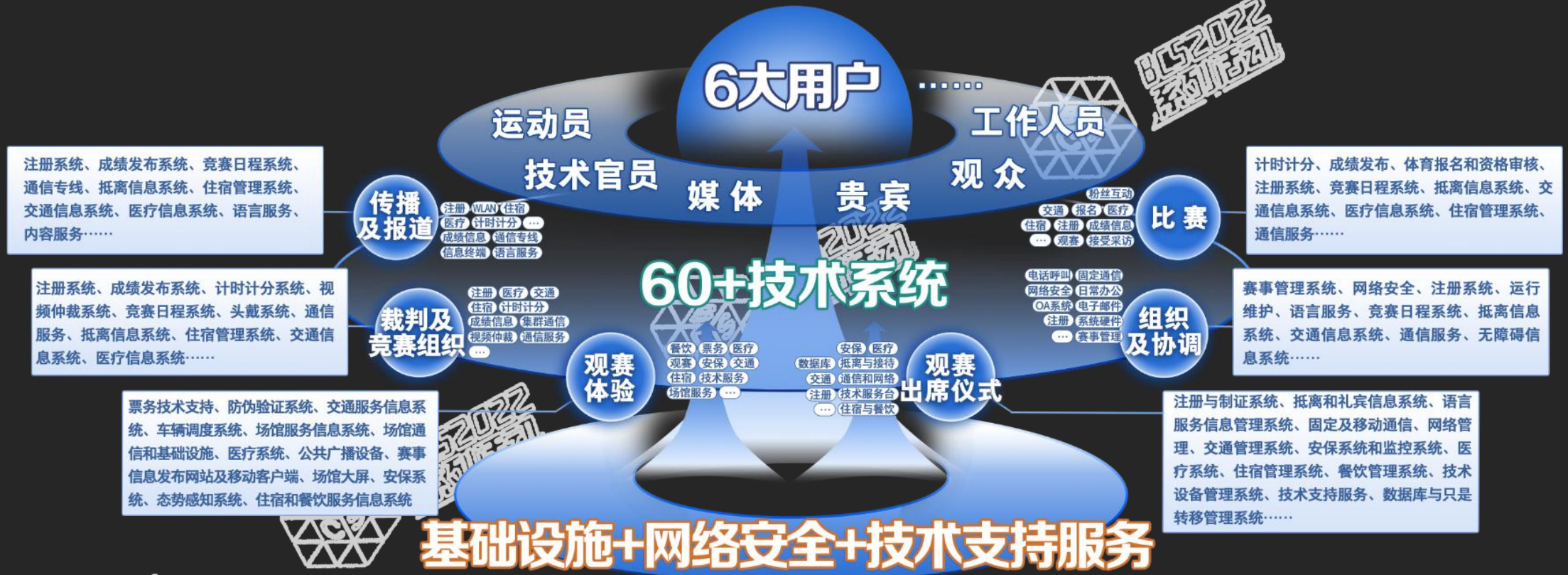
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

北京冬奥会网络安全保障体系总体设计

BCS2022系列活动-冬奥网络安全“零事故”宣传周

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

北京冬奥会涉及业务环境异常复杂



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

冬奥网络安全面临的威胁和风险

影响比赛的进行

- 运动员成绩不能准确记录、传递以及显示；
- 运动员成绩数据不能准确统计计算、传递以及显示。

影响比赛的传播

- 场馆现场解说员不能及时准确获得相关比赛信息；
- 新闻媒体、国家体育代表团、国际奥委会、国际单项体育联盟、国家体育代表团等不能及时准确获取相关比赛信息；
- 普通大众无法准确及时获取比赛信息和其他北京冬奥会相关信息。

影响比赛的组织

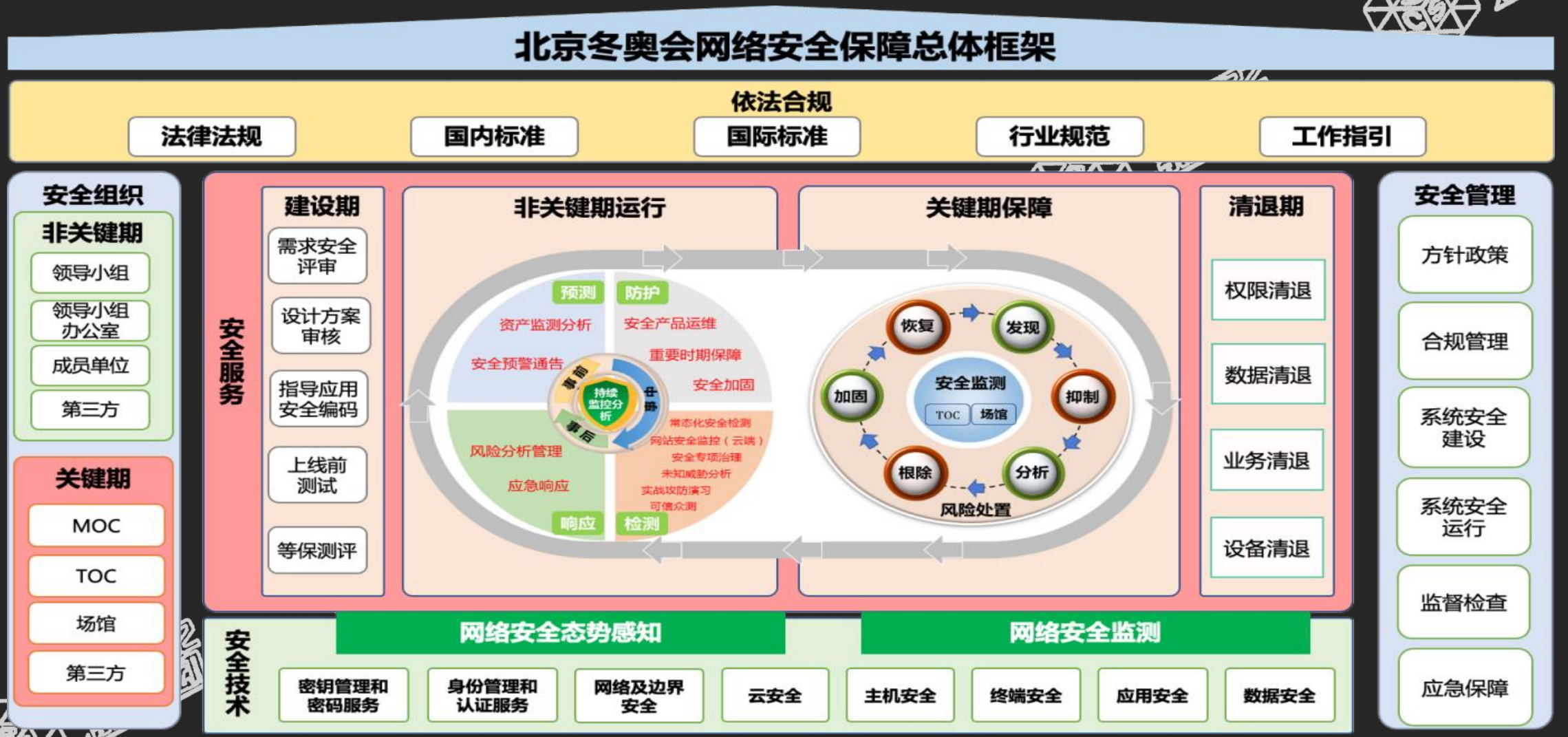
- 个人隐私数据泄漏，北京冬奥会参与人员（技术官员、媒体、体育代表团、志愿者、合作伙伴等）的注册、资格审核、赛事的日程管理、赛事人力资源管理、电子投票等；
- 北京冬奥会参与人员的酒店预定、医疗救治、交通出行受到影响；
- 北京冬奥会参与人员进出场馆、物流仓储、饮食、场馆运行等受到影响；
- 观众购票、用票收到影响等。

影响国家和组委会形象

- 除了以上问题的发生会影响到国家和北京奥组委的名誉之外，某些国家势力、黑客主义组织、网络恐怖主义组织对各种面向媒体和公众的带有北京冬奥会图标的网站、展示屏等非法篡改都可能造成名誉损失。

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

系统性、全局性统筹网络安全规划设计工作



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

网络安全管理架构设计

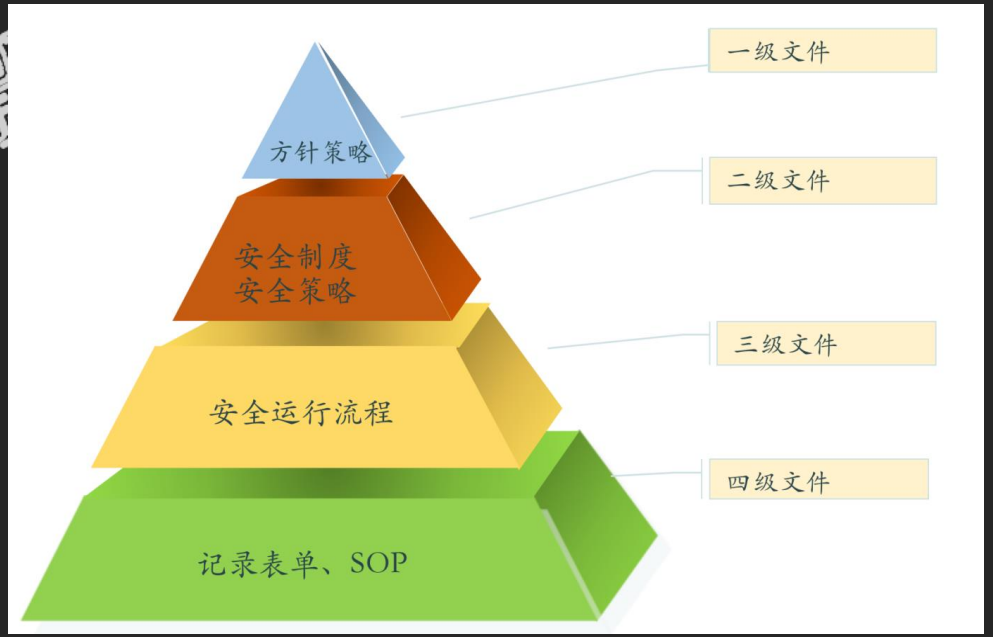
安全管理体系总体框架

网络安全组织机构

- 组织与岗位
- 安全协作
- 人员安全
- 安全培训

网络安全管理

- 方针政策
- 合规管理
- 系统安全建设
- 监督检查
- 应急保障
- 系统运行



奇安信

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

网络安全技术架构设计

网络安全运行架构设计

安全组织

“一个机构两块牌子”

“平时”日常态安全组织

领导小组

规划处 | 网络处 | 数据处 | 信息系统处 | 安全处

“战时”运行态安全组织

运行指挥部

值班主任 | 专业领域值班经理 | 值班人员 | 呼叫中心 | 专业领域安全专家 | 下属单位运行团队

安全管理

- 方针策略
- 管理制度
- 技术规范
- 工作流程
- 操作规程
- 记录表单

“平时”日常态工作

建设安全

监督检查

- 安全检查
- 安全检测
- 密码评估
- 等保测评
- 实战攻防演习
- 应急演练

教育培训

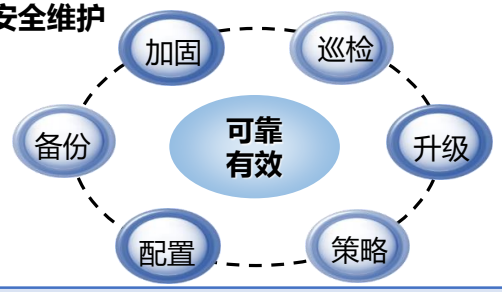
- 安全意识提升
- 技术技能提升

自检自查

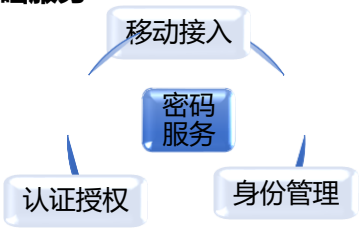
- 渗透测试
- 风险评估
- 蓝队评估
- 应急演练

“战时”运行态工作

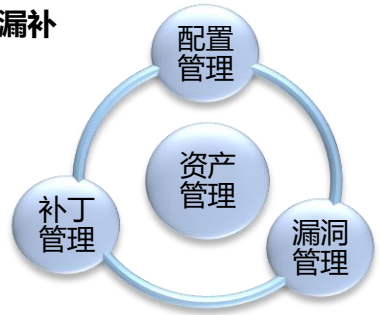
安全维护



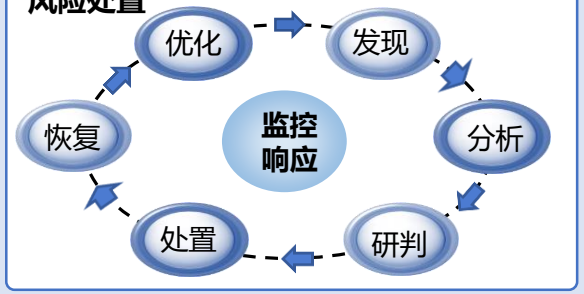
安全基础服务



资配漏补



风险处置



安全技术

应用安全 | 数据安全 | 主机安全 | 云安全 | 终端安全 | 网络及边界安全 | 密钥管理和密码服务 | 身份管理和认证服务 | 网络安全态势感知/网络安全运行监控平台

奇安信

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

北京冬奥会网络安全保障体系密钥管理和密码服务工程设计

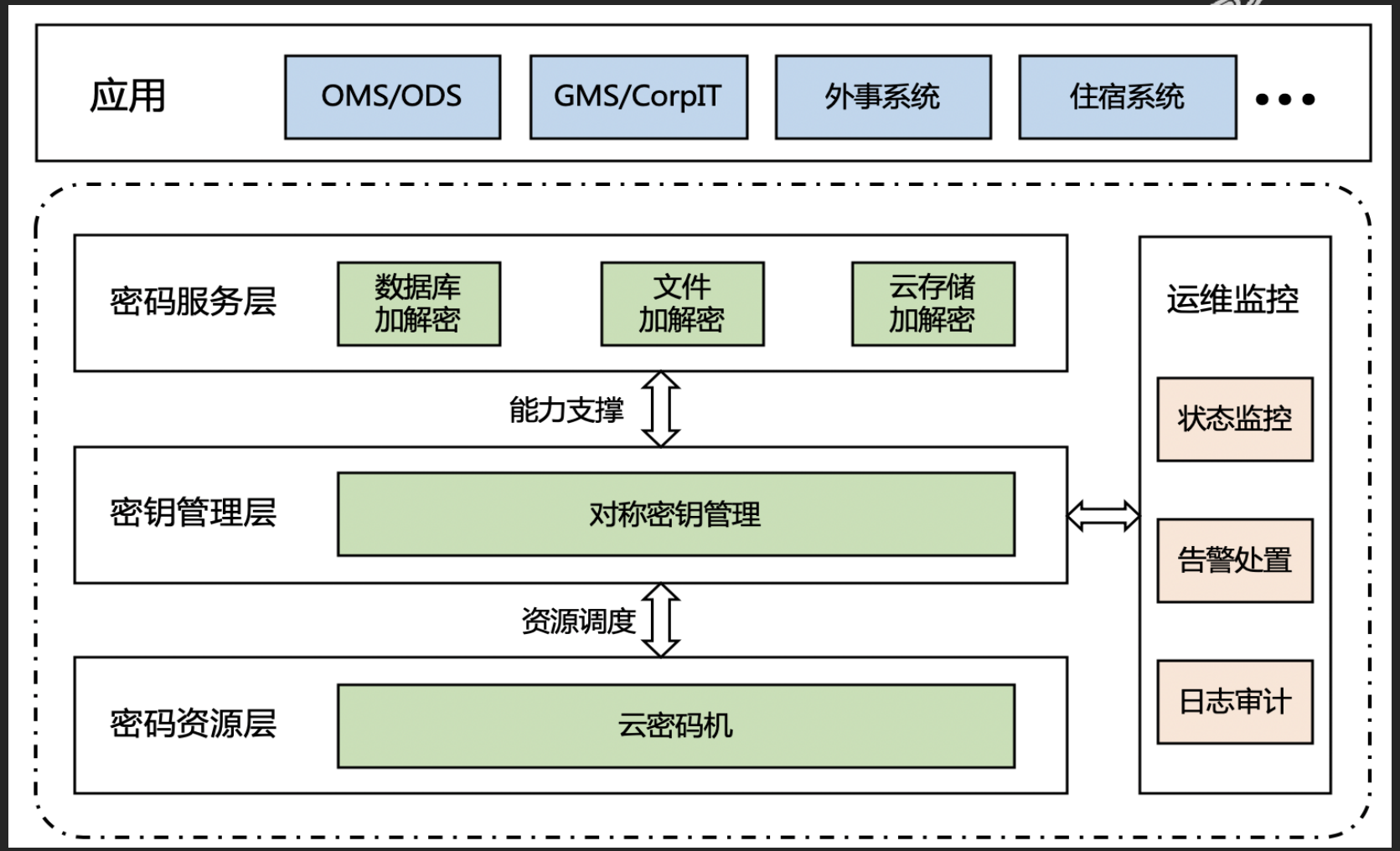
奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

密钥管理和密码服务工程建设目标

建设目标是：为确保冬奥会和冬残奥会网络运行安全与数据信息安全，遵循“同步规划、同步建设、同步使用”原则，建设由对称密钥管理系统、对称密钥密码服务等构成的冬奥会和冬残奥会密钥管理与密码服务体系，基于**国产密码**算法实现密钥集中统一管理、提供敏感数据加密等密码服务，**防止敏感数据泄露**，简化密钥管理工作，**符合国家密码管理要求**，为确保冬奥会和冬残奥会网络运行“零事故”的整体安全目标起到基础支撑作用。

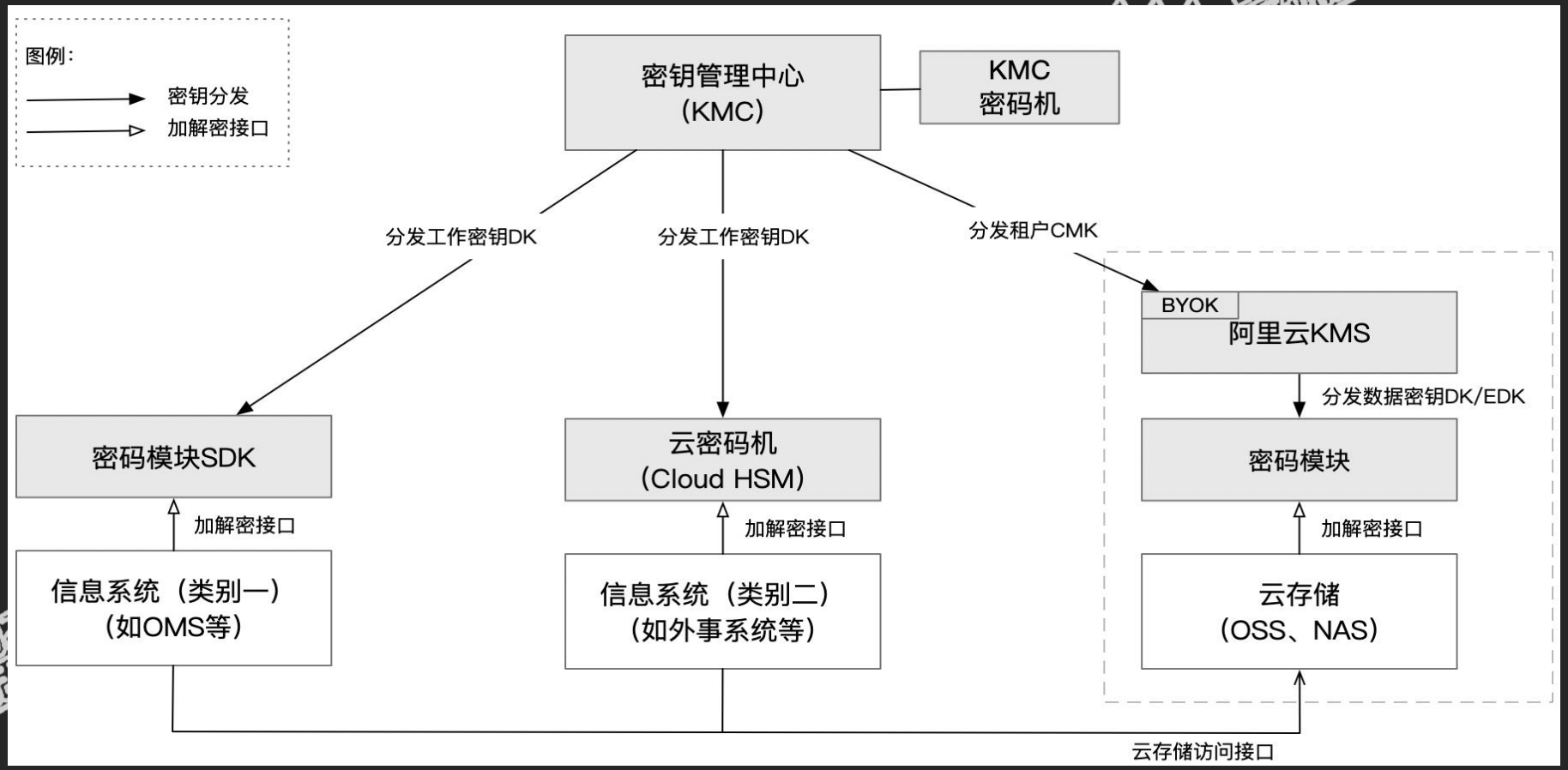
密钥管理和密码服务工程能力架构

冬奥会和冬残奥会密钥管理与密码服务系统总体上可以分为密码资源层、密钥管理层、密码服务层及运维监控层



密钥管理与密码服务集成架构

在对称密钥管理体系中，由密钥管理中心（KMC）提供集中的密钥管理能力，由密码模块SDK、云密码机（Cloud HSM）为信息系统提供数据加密服务能力。



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

密钥管理与密码服务高可用设计

云密码机备份与容灾

- 使用云密码机自身备份机制，将需要备份的所有密钥使用保护密钥加密导出，保护密钥以成分KEY导出，任意2个保护密钥成分KEY可以恢复出保护密钥，进而可以恢复所有加密的密钥

KMC系统备份与容灾

- KMC系统运行在阿里云ECS上，可通过快照或镜像方式对KMC系统盘、数据盘进行备份，如果存储在磁盘上的数据本身是错误的数据，如因应用错误或恶意读写导致的数据错误，此时就可以使用快照服务将磁盘上的数据恢复到期望的状态

RDS备份与容灾

- 阿里云RDS采用主备实例方式实现数据备份和高可用。主实例创建成功后，会在同一地区不同可用区内为该实例创建一个备实例；主备实例之间数据实时同步

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

北京冬奥会网络安全保障体系身份安全工程设计

BCS2022系列活动-冬奥网络安全“零事故”宣传周

奇安信

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

身份安全工程建设目标

认证

基于用户使用习惯提供扫码、短信、邮件等不同的认证方式，解决密码脆弱性问题(弱口令，默认密码，重复密码等问题)。

授权

统一管理分散的授权，解决访问安全隐患。

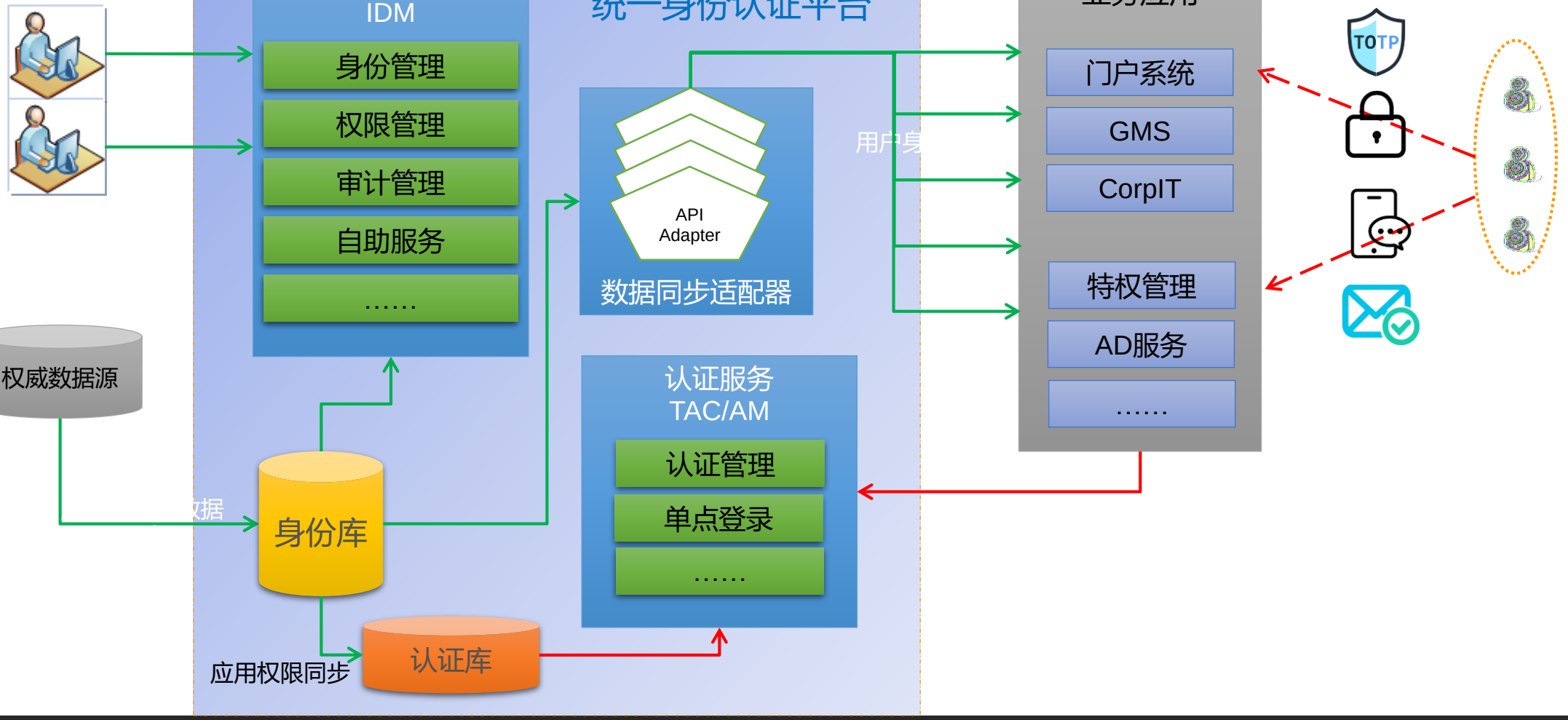
账号

奥运大家庭成员的身份生命周期维护，解决账户分散，生命周期管理不完整问题(停用账号在部分区域依然可用等)。

审计

审计合规，对外输出的标准接口，完善从端到业务的全链路访问日志记录。

身份安全工程技术架构


身份管理
IDM
身份管理
权限管理
审计管理
自助服务
……
2022冬奥
统一身份认证平台
API
Adapter
数据同步适配器
业务应用
门户系统
GMS
CorpIT
特权管理
AD服务
……
TOTP
权威数据源
身份库
认证服务
TAC/AM
认证管理
单点登录
……
认证库
应用权限同步

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

身份安全工程功能架构

认证服务

- 主认证
- 多因子认证
- SSO接口
- OAuth2.0/ OIDC
- 权限列表
- 密码修改

管理

- 系统管理
- 工单管理
- 工作流

自服务

- 工单申请
- 密码服务

认证管理

- 认证策略管理
- 多因子认证
- 单点登录
- 集成配置

身份管理

- 用户管理
- 分组管理
- 组织机构管理
- 设备管理
- 应用帐号管理
- 应用管理
- 资源管理

权限管理

- 角色管理
- 授权策略管理
- 权限访问矩阵
- 权限视图

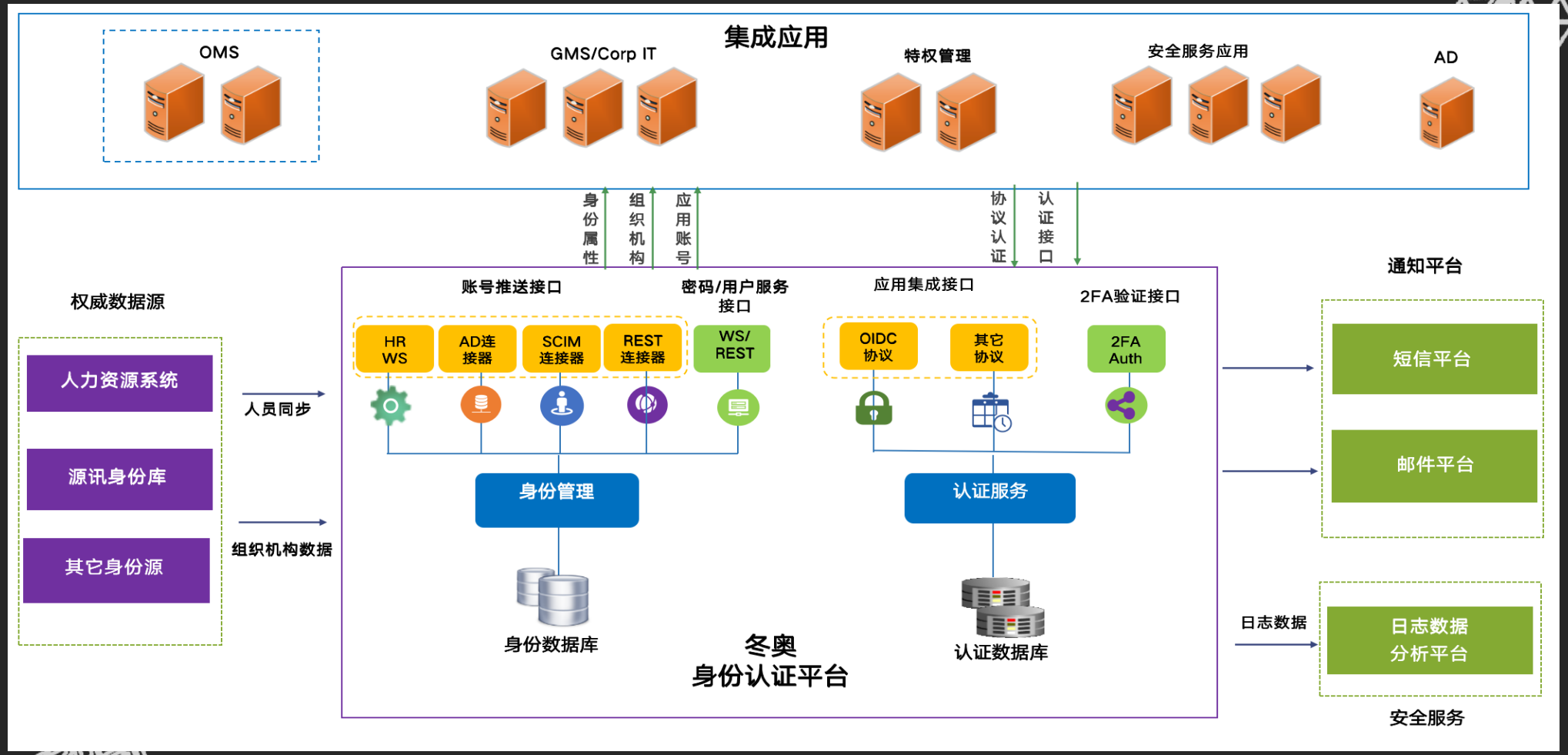
身份源服务

- 用户供给
- 组织机构供给
- 权限分发
- AD适配器
- SCIM连接器
- 其它连接器

基础服务

- 日志审计
- 数据存储
- 高可用
- 灾备

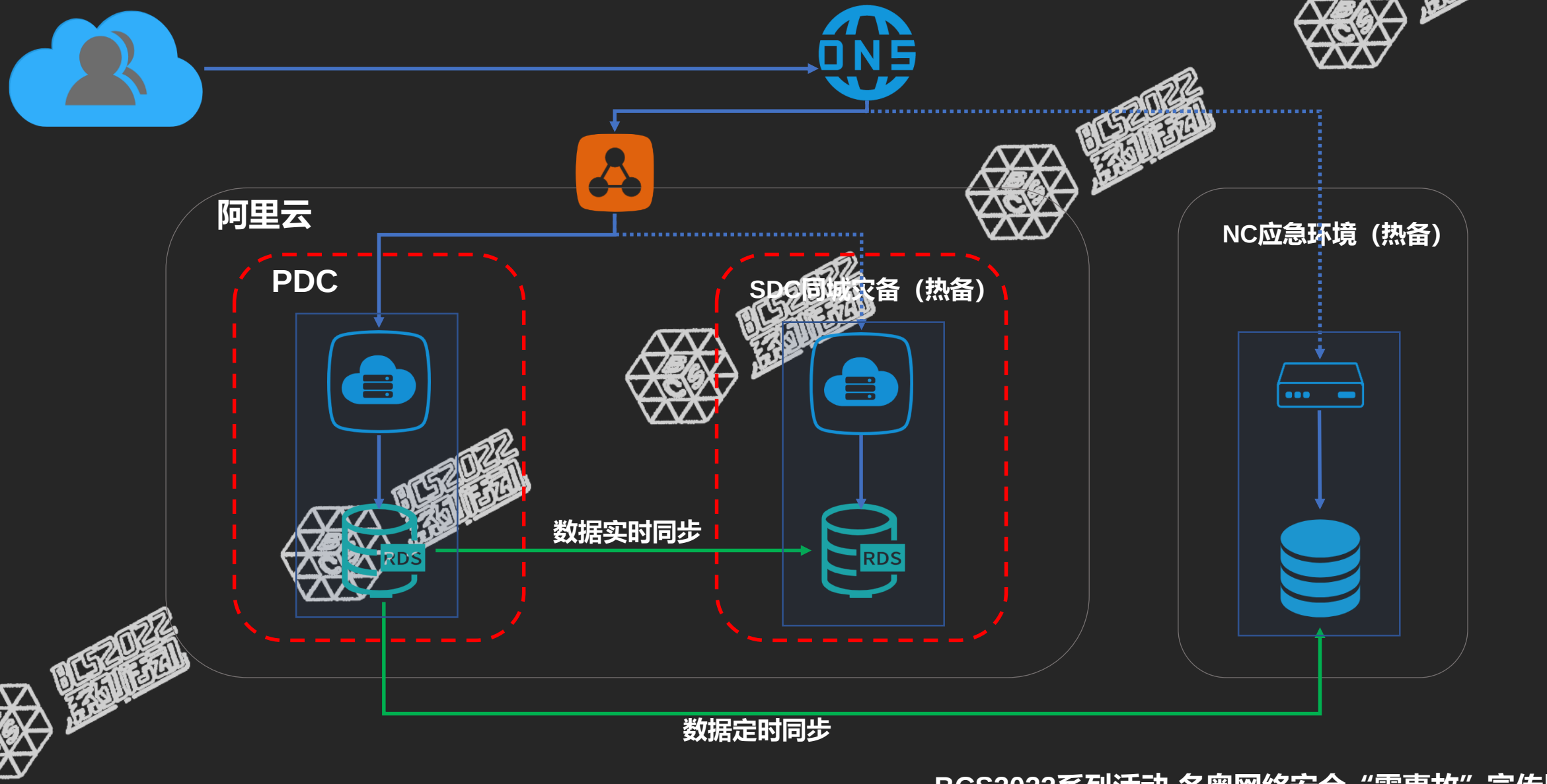
身份安全工程集成架构



- ✓ 针对冬奥进行场景化梳理，形成身份的管理、认证、权限控制多层级安全需求
- ✓ 设计参照奥组委身份安全的建议、要求、大赛经验，设计业务逻辑
- ✓ 结合我司在身份安全、零信任领域的安全能力，完善安全设计

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

身份安全工程高可用设计



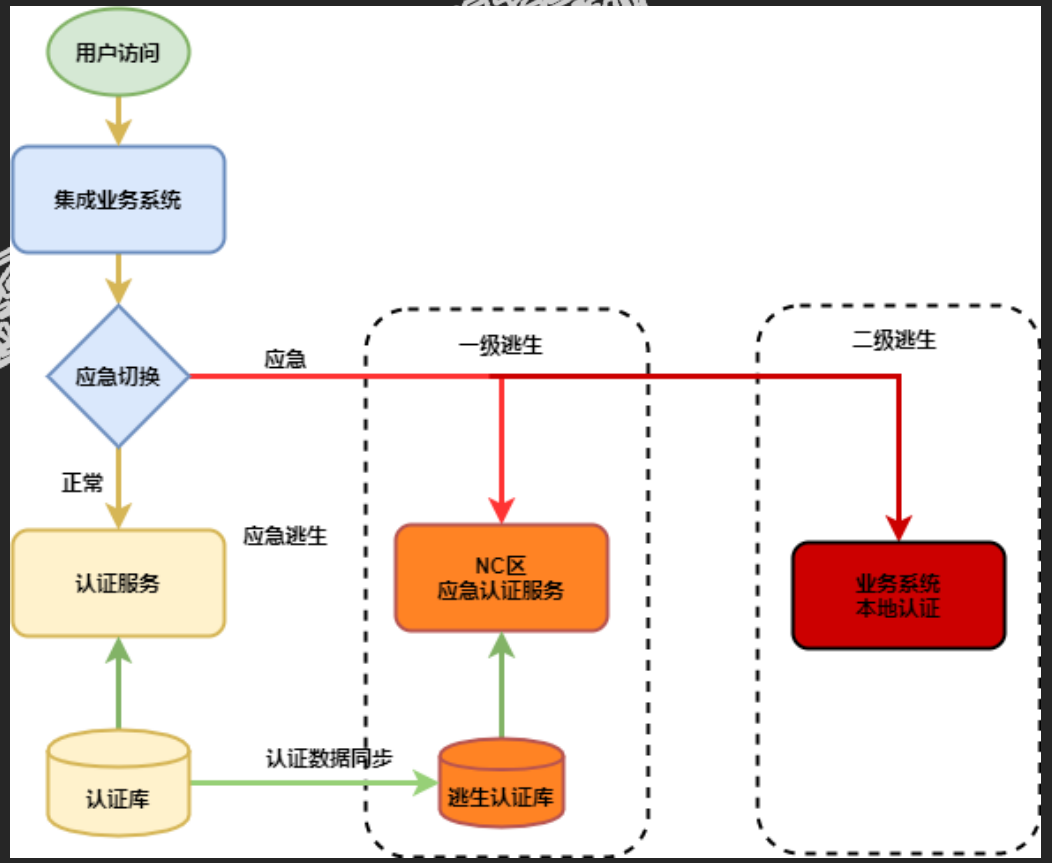
身份安全工程高可用设计

一级逃生：

- 认证服务域名DNS切换至NC认证服务地址（DNS支持）。
- 集成业务系统切换认证服务至NC应急认证服务（DNS不支持）。

二级逃生：

1. 集成业务系统切换认证至本地认证服务。
2. 用户口令通过管理员重置或本地找回方式进行重置，用户使用重置后的口令认证。



奇安信

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

03 北京冬奥会网络安全保障体系基础工程设计

奇安信

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

北京冬奥会网络安全保障体系
终端安全工程设计

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

终端安全工程建设目标

保护对象

- **赛事终端**：
  - OVR终端
  - 解说员终端
  - 信息查询终端
  - 其他赛事专用终端
- **办公终端**
- **运维终端**
- **证件查验终端**
- **打印机**：
  - 网络打印机
  - 扫描复印打印一体机等

安全建设目标与重点策略

1. 非奥组委的终端不能入网
2. 持续维持终端及其承载应用程序的可用性，不影响赛事活动的正常开展和运行；
3. 确保竞赛终端的高可用性，办公和运维终端的安全性；
4. 为使用者提供安全便利的操作环境；
5. 快速发现威胁，并进行有效处置防止威胁扩散，避免终端成为攻击其他目标的跳板；
6. 保护终端上的敏感数据，防止数据丢失或外泄。

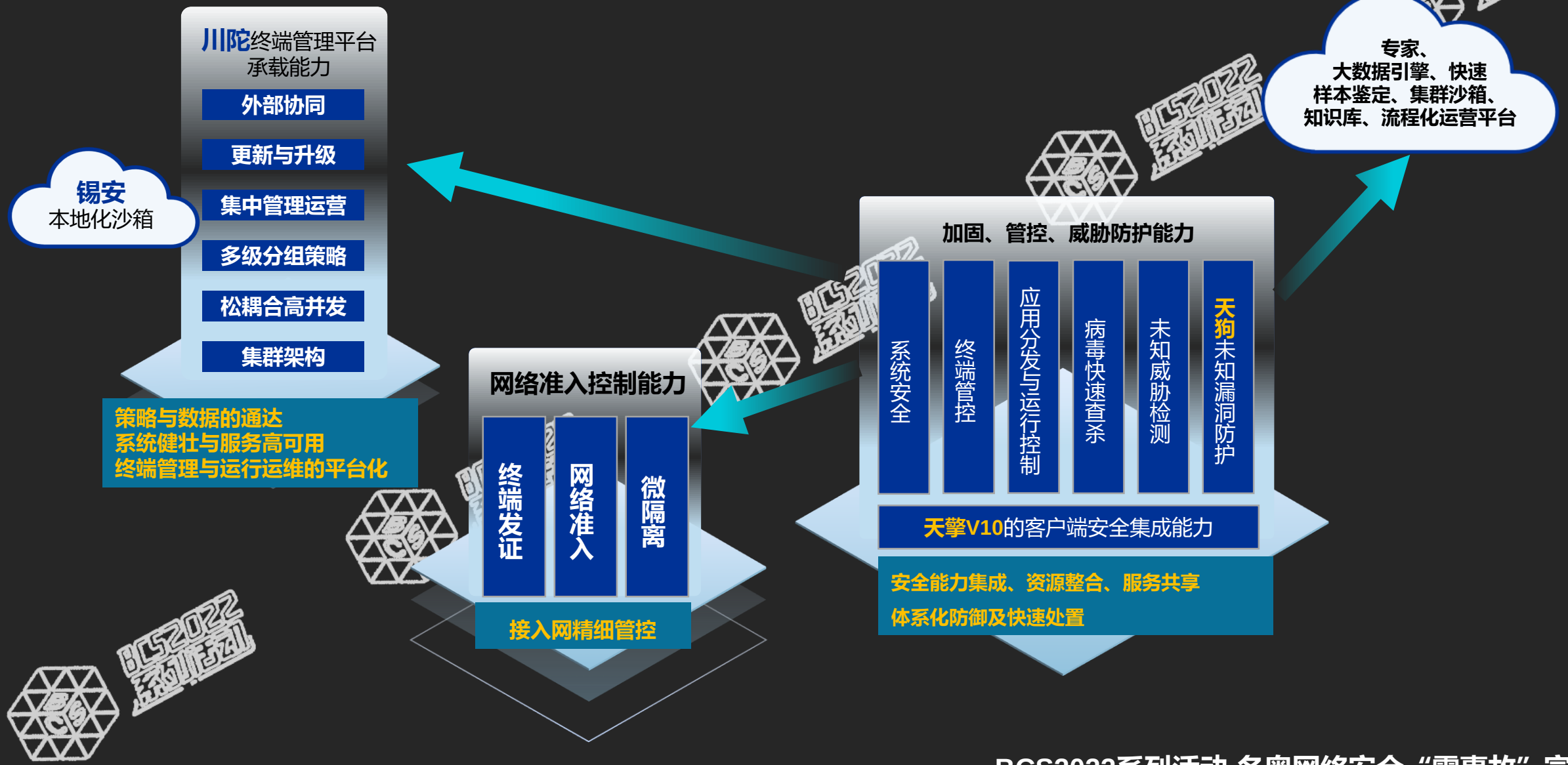
奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

终端安全工程建设思路

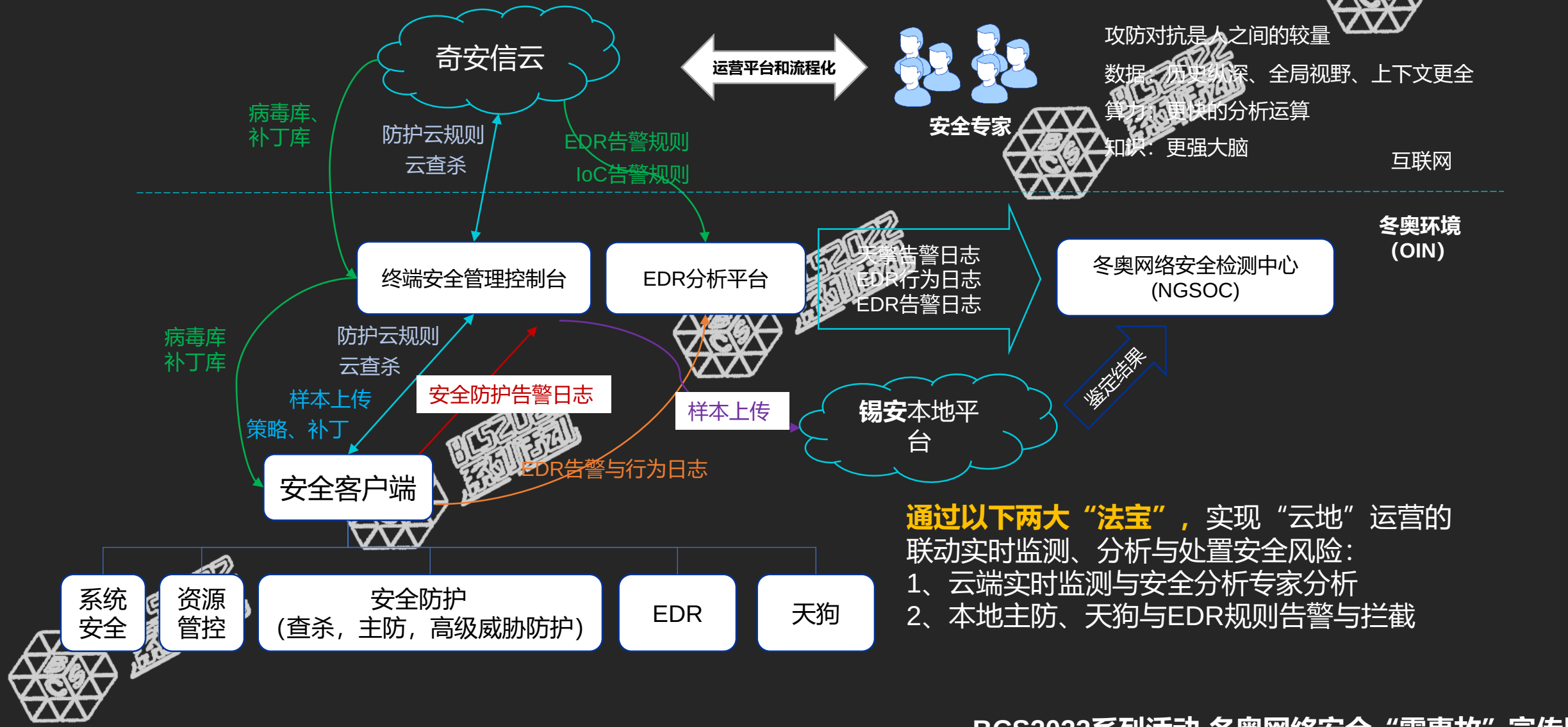
- 建设**集中式终端安全管理平台**，提高**管理运行效率**，减少中间环节提高策略时效性和处置响应速度以应对终端数量大、位置分散带来的挑战。支持**精细化防控**适应灵活多变的场景和突发事件；**统一管理客户端安全能力**和访问入口，**节约终端资源，提高终端性能**；
- 构建**体系化防御**能力：
  - **终端加固**：管理终端资产的**系统安全配置、补丁修复**提高终端自身稳健壮性；
  - **安全管控**：加强威胁入侵渠道的管控**收缩终端攻击面，包括系统完整性、账户权限、外设访问、网络外联、应用程序；**
  - **入网控制**：建立可信的**终端数字化身份，对接入网逻辑细分**，对入网进行强管控**核实终端身份与安全基线配置**情况实现可信终端安全入网。
  - **威胁防御**：构建**多层威胁防御**体系，快速进行威胁感知、检测、识别、处置，保护系统和关键应用。
- **精细策略：分类管控、分级防护，**精细化的定义**场景**相关终端的**安全策略**
- **监控运营**
  - **运营监视：**动态监视全网终端的漏洞、补丁、病毒、威胁等告警与事件，利用大数据技术和Ioc情报进行风险分析，辅助安全决策；
  - **三级协同：场馆巡视、现场运营中心**实时监视运营、**公司奥运中心**监视应急支撑，形成三级协同保障、运营及应急相结合的安全流程闭环。

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

终端安全工程能力架构



终端安全工程技术架构



通过以下两大“法宝”，实现“云地”运营的联动实时监测、分析与处置安全风险：

1、云端实时监测与安全分析专家分析

2、本地主防、天狗与EDR规则告警与拦截

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

终端安全工程运行架构

	场馆运维团队	本地安全运维团队	本地安全分析团队	云端专家团队
地	场馆		技术运行中心	奇安信公司
物	客户端安全工具	终端安全管理平台	锡安本地化高级威胁分析平台	奇安信云
事	• 场馆巡检与支持 • 受害机器应急处置 • 管控效果验证与反馈 • 紧急事件处理	• 策略定义与下发 • 策略优化调整与效果评估 • 监控补丁推送状态 • 规则库更新 • 系统升级	• EDR分析运营 • 告警分析与研判、主动威胁狩猎 • 安全防护告警分析 • 常规木马病毒事件确认 • 可疑样本分析	• 云端行为日志分析 • 云端可疑样本分析

① ② ③ ④

冬奥网络安全监测中心 (NGSOC)

- 与天擎EDR联动
- 与天狗联动
- 全景数据接入与分析（终端、流量、样本信息）
- 关联分析模型
- 告警分类
- 团队协作运营体验

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

北京冬奥会网络安全保障体系高级威胁检测工程设计

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

高级威胁检测工程建设目标

1.建设网络威胁全感知能力

- 建设基于网络流量检测分析技术的高级威胁发现能力
- 建设面向主机和终端安全威胁检测防御技术能力
- 建设恶意文件未知威胁检测能力
- 建设威胁情报匹配验证能力

2.云上云下网络流量全覆盖

全流量采集覆盖全网2个云数据中心、2个网络中心及33个重要场馆的网络流量

3.建设主机/终端安全防御能力

建立业务主机系统、终端系统的威胁入侵、非法访问、非法外连行为的发现防护

4.形成云上安全能力补位

业务访问首先会经过基础安全设备FW、WAF等的流量过滤，但过滤后缺少查漏补缺手段，一旦被APT突破，则无法有效防御，让建设的高级威胁检测防御能力与冬奥云上基础安全能力形成安全互补

5.补充详实的网络访问日志

安全事件分析需要全量网络数据的支撑，缺失则会对威胁事件溯源分析取证造成较大障碍，补充解析记录全网全量网络访问日志解决这一问题

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

高级威胁检测工程能力架构-网络侧

冬奥云上云下流量采集

- 冬奥云数据中心流量
- 冬奥网络中心流量
- 冬奥场馆流量

智能引擎处理

- **天眼自研引擎(QNA)**
  200多种协议解码+DPI
- **NBT机器学习引擎**
  机器学习算法识别检测
- **智能分析引擎**
  优化提升告警精度
- **SQLparser引擎**
  Sql语句识别检测

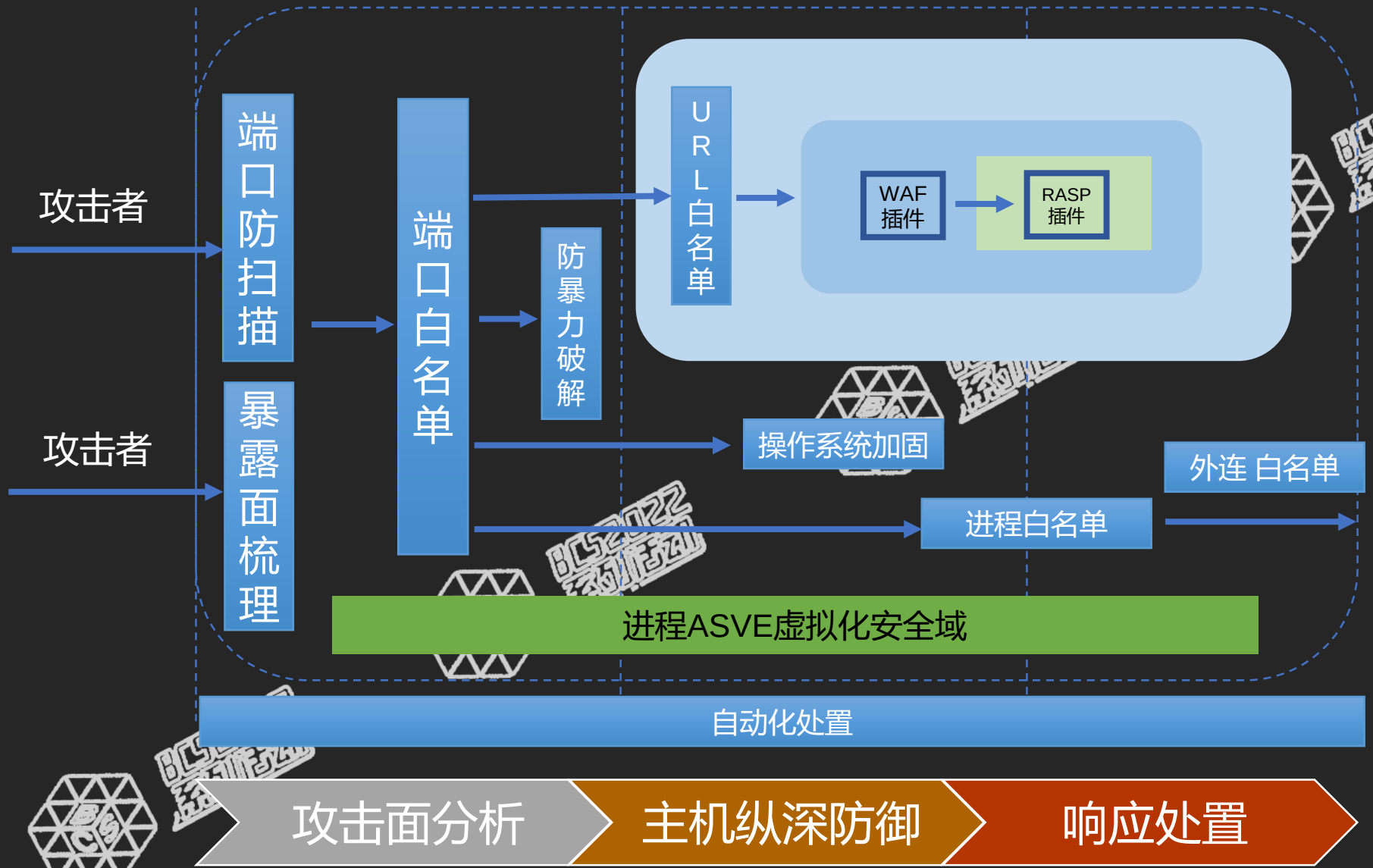
自动化威胁检测分析

威胁规则检测	**威胁情报** 300w+IOC情报
	规则检测 10000+检测规则 100+缺陷分类
文件还原检测	**沙箱** 6+静态特征检测引擎 40多种深度动态分析环境
行为提取检测	**异常行为分析** 30多种机器学习 行为分析模型

可视化事件监测

- **APT攻击事件**
  Web攻击、漏洞攻击
  邮件攻击、恶意软件
  …
- **新型事件线索**
  异常行为
  未知威胁
  0day攻击

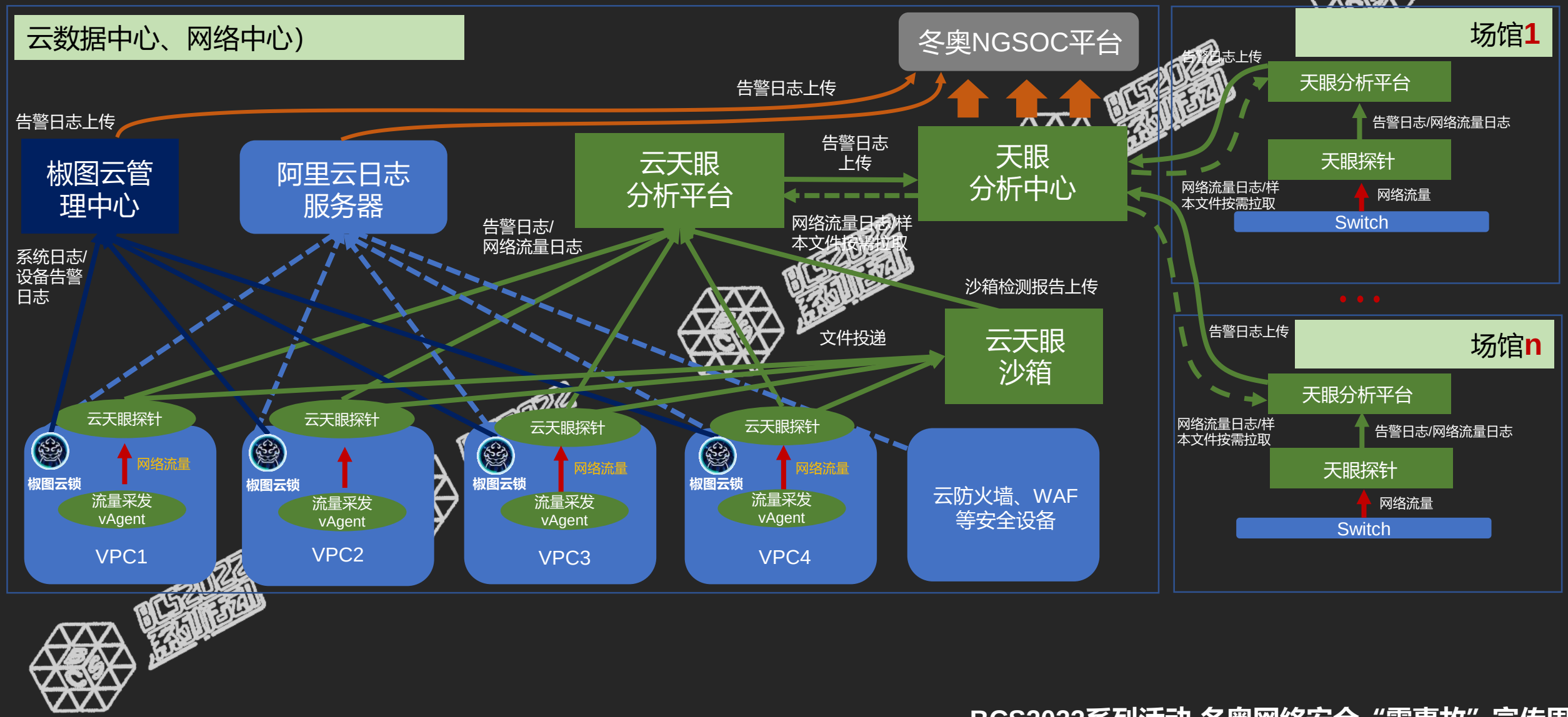
高级威胁检测工程能力架构-主机侧



针对冬奥业务主机系统的主机侧安全防护，主要通过椒图云锁端口白名单、URL白名单、外联白名单、进程白名单等功能，限制非法访问和非法外连行为，对出入流量进行管控，实现主机侧威胁入侵和非法进程外连行为的有效阻断拦截。

攻击面分析 → 主机纵深防御 → 响应处置

高级威胁检测工程技术架构



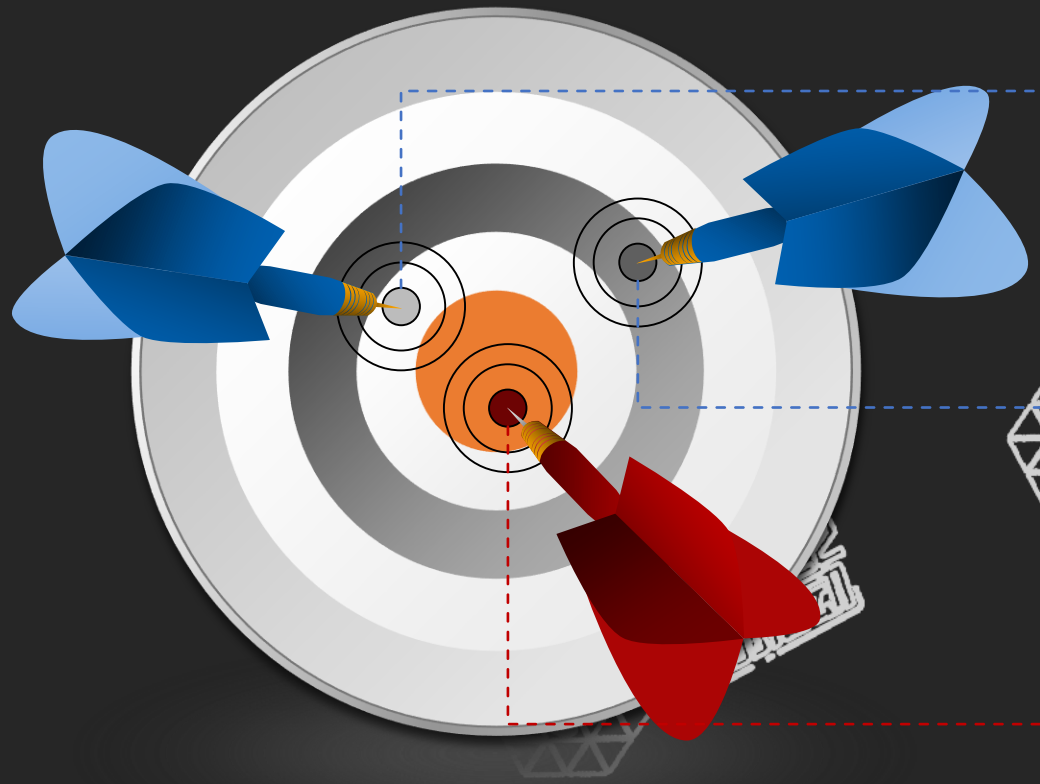
奇安信

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

北京冬奥会网络安全保障体系纵深防御工程设计

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

纵深防御工程建设目标



基于业务访问关系的精细化控制，在满足业务可用性的前提下，构建权限最小化的安全访问策略

能防御、能发现、能控制的纵深防御能力，提供针对性的边界控制措施，将安全控制能力深度融合、全面覆盖

以保障赛事业务顺利进行的安全运行工作模式：承接安全战略及制度策略，应对高级威胁，开展策略梳理和优化工作，保障赛事顺利进行

纵深防御工程建设分区分域

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

纵深防御工程安全能力设计

分类	网络边界	网络安全威胁分析								
		拒绝服务	网络攻击	恶意代码	泄密	越权滥用	误操作	篡改	仿冒	抵赖
PNC SNC	互联网边界	高	中	中	中	低	低	低	低	低
	Server farm	低	中	中	中	中	中	中	中	中
	DC接入	低	中	中	中	低	低	低	低	低
	PNC-SNC	极低	极低	极低	极低	极低	极低	极低	极低	极低
场馆	场馆边界	低	中	中	低	低	低	低	低	低
	VDC room	低	中	中	低	低	低	低	低	低
	OVR room	低	中	中	低	低	低	低	低	低
	CIS	低	中	中	低	低	低	低	低	低
	Back office	低	中	中	低	低	低	低	低	低

序号	网络安全威胁	威胁应对措施
1	拒绝服务	流量清洗、网络访问控制
2	网络攻击	网络结构隔离、网络访问控制、网络入侵防范、Web应用防护、高级威胁检测、攻击诱捕
3	恶意代码	恶意代码防范、高级威胁检测、网络访问控制
4	泄密	上网行为管理、传输加密、数据泄露检测
5	越权滥用	网络安全审计、网络访问控制
6	误操作	网络安全审计
7	篡改	网络安全审计
8	仿冒	网络安全审计
9	抵赖	上网行为管理、网络安全审计

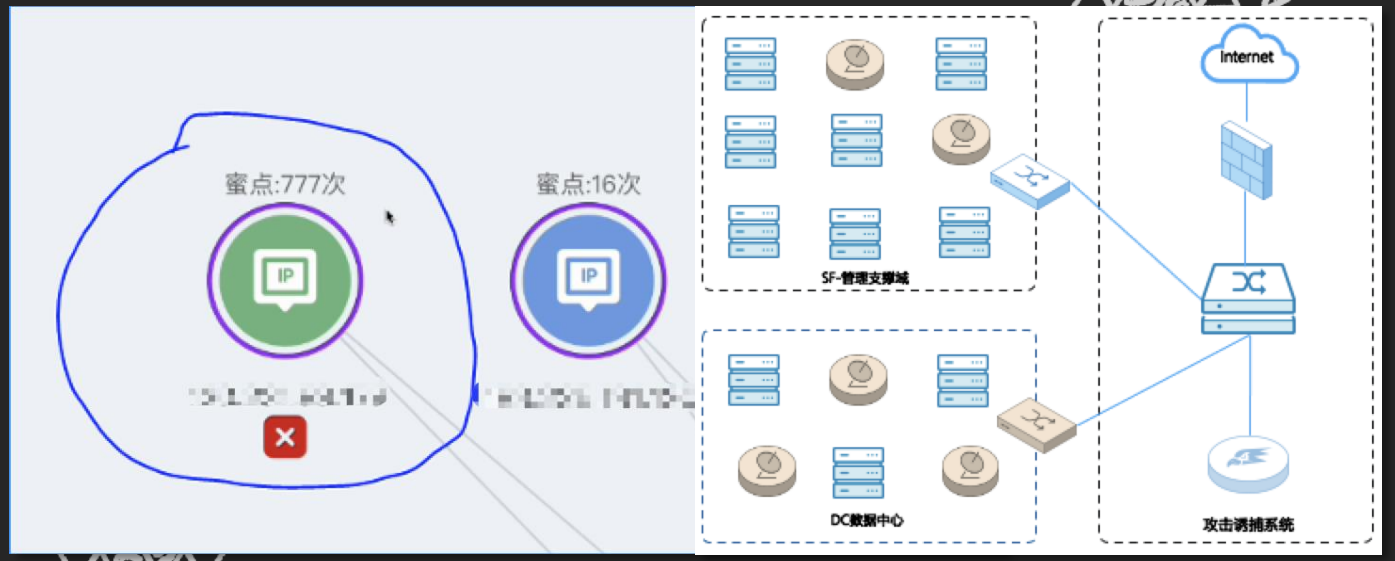
备注：部分网络安全威胁的防护涉及到身份认证、数据加密、运维管控等措施，在其它专项中有详细设计。

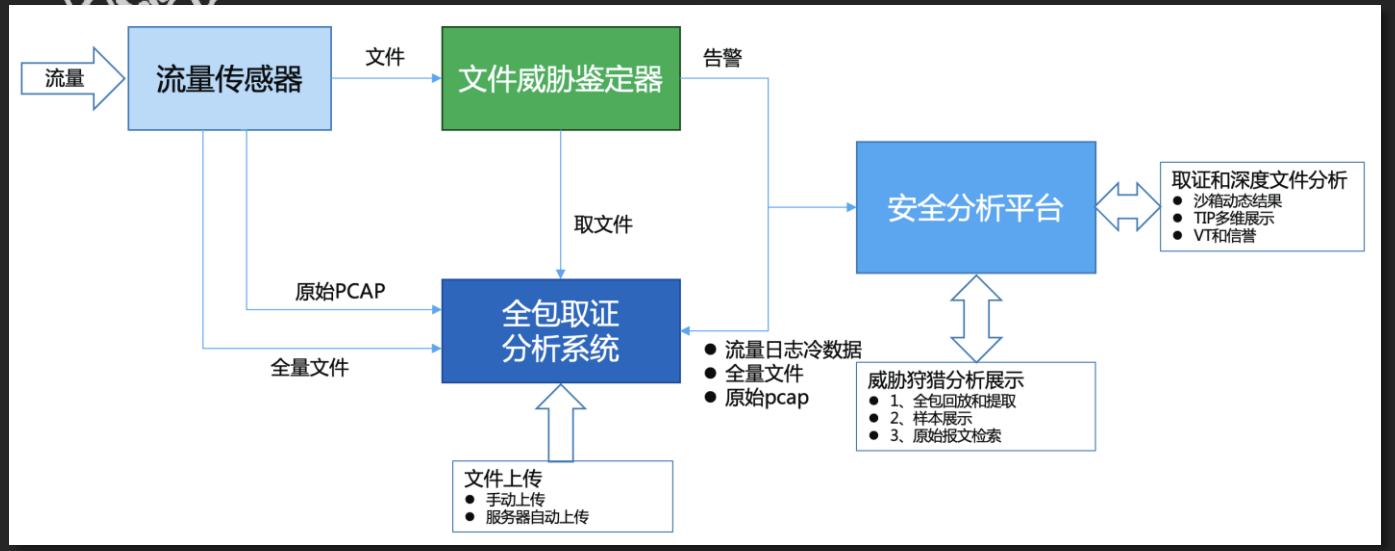
分类	网络边界/节点	安全防护措施									
		网络访问控制	通信传输加密	网络入侵防范	恶意代码防范	高级威胁检测	Web应用防护	上网行为管理	数据泄露检测	网络安全审计	攻击诱捕
PNC SNC	互联网边界	√	√	√	√	√		√	√		
	Server farm	√		√		√	√		√	√	√
	DC接入	√		√		√	√		√		
	PNC-SNC	√									
场馆	场馆边界	√		√	√	√					
	VDC room	√		√		√	√				
	OVR room	√		√	√						
	CIS	√		√	√						
	Back office	√		√	√						

纵深防御工程安全安全能力设计

蜜点诱捕：在系统中某些特殊的、正常用户不可能访问到的位置，部署的一系列微型蜜罐。蜜点设计的关键不在于对系统的仿真程度，而在于部署的位置。通过这种方式可以直接捕获各路黑客的各种“踩点”行为，即使这些潜在的攻击者并没有做出任何真实的攻击动作；

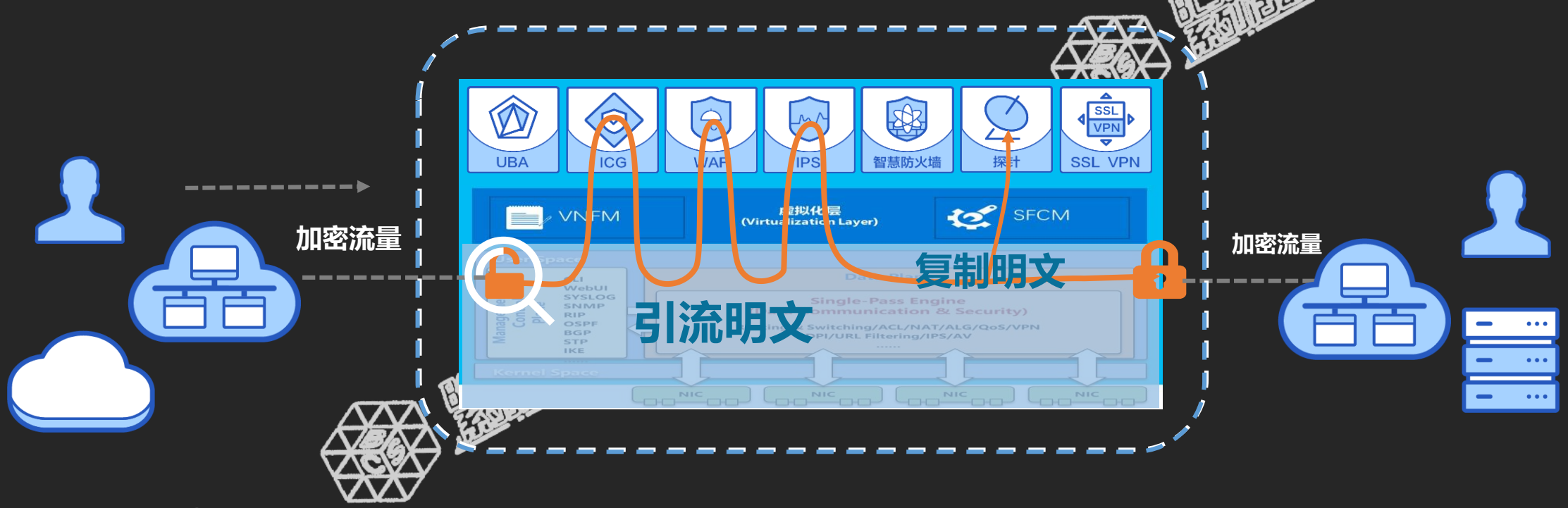
全包取证：提供全量数据对安全事件进行回溯和调查，分析人员可以在攻击之前、期间和之后检查特定的网络数据包和会话，能够重建和可视化触发高级威胁攻击事件，使安全团队能够快速和有效地响应。





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

纵深防御工程安全安全能力设计



奇安信

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

04 北京冬奥会网络安全保障体系运行保障工程设计

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

北京冬奥会网络安全保障体系特权管理工程设计

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

特权访问工程建设目标

建设由堡垒机+统一管理平台构成的特权访问安全服务体系。

- 特权账号安全保存：对部署在OIN网络中NC区域和场馆区域的主机、网络设备、安全设备的后台特权账户进行统一托管，设置高强度密码，并定时改密；
- 特权访问安全：为部署在OIN网络中NC区域和场馆区域的主机、网络设备、安全设备、重要系统提供安全运维通道与可控变更通道，实现实时监控运维操作、全程录屏变更行为，并对高危命令进行拦截与告警。

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

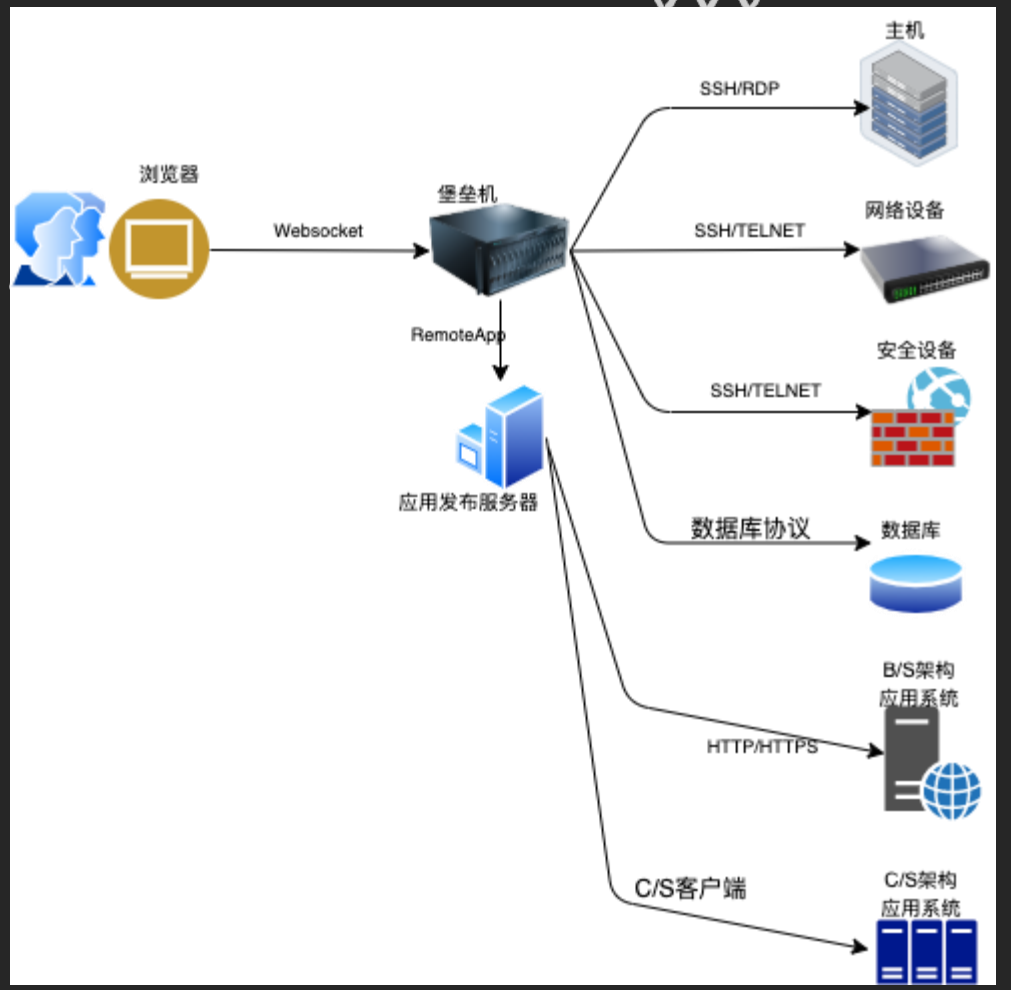
特权访问堡垒服务

1、堡垒机

- SSH、RDP、TELNET、VNC等协议代理，为主机、网络设备、安全设备提供安全的运维通道，实时监控，全程录屏，高危指令拦截。
- MySQL、Oracle、SQLServer等数据库协议代理，为数据库提供安全的运维通道，进行库表细粒度访问控制、协议级数据操作拦截、敏感数据动态脱敏、数据库操作审计。

2、应用发布服务

- 为应用系统、核心桌面应用提供可控的使用通道，实时监控，全程录屏。
- 运维水印：将当前操作用户的登录名作为水印背景，如果通过截图发生了数据泄露，可快速追溯相关人员，并迅速寻找到传播的源头。
- 控制文件上传下载、上下行剪贴板，做到数据不流出
- **操作审计：**对所有的操作进行录屏审计，支持实时监控与事后回放



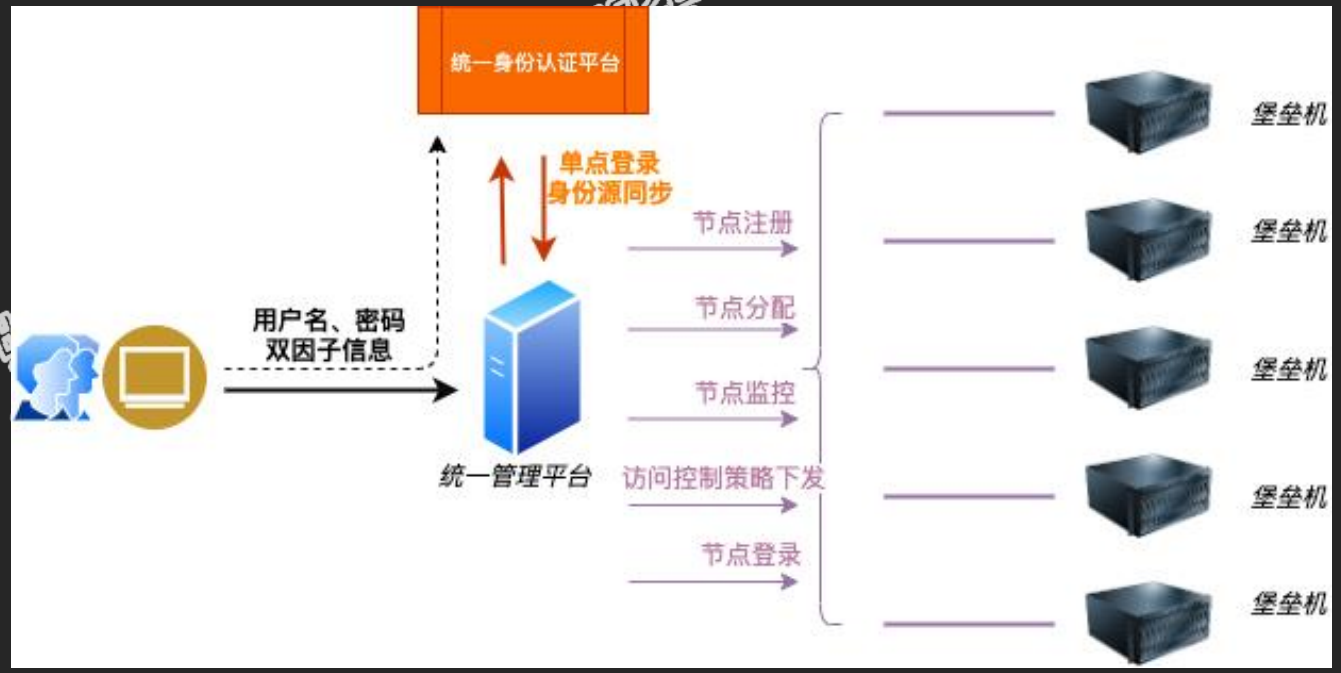
特权访问管理

统一管理平台

- 为部署在NC区域和场馆区域的堡垒机提供一站式管理，是用户登录堡垒的唯一入口。
- 与IAM实现单点登录：用户登录统一管理平台需要通过IAM进行认证，认证信息包括**用户名，密码，双因子**
- 与IAM进行身份同步：IAM会定时向统一管理平台同步用户信息，统一管理平台再向堡垒机同步用户信息。

堡垒机管理功能

- 节点注册
- 节点分配
- 节点登录
- 节点监控
- 访问控制策略下发



奇安信

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

北京冬奥会网络安全保障体系安全监控工程设计

BCS2022系列活动-冬奥网络安全“零事故”宣传周

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

安全监控工程建设目标

安全“无死角”监控

1. 云上、云下资产全接入
2. 各类日志数据全接入
3. 数据源、资产数据动态管理

实现安全运行全流程闭环管理

1. 安全事件可监测、可分析、可溯源、可处置
2. 承载冬奥安全运行流程（工单流转闭环管理）
3. 实现安全运行降本增效（ 标准化SOP ）
4. 多角色、全岗位运行工作覆盖

基于冬奥场景安全监测、可视化

1. 结合冬奥运行场景构建安全监测关联规则
2. 分场馆进行安全可视化
3. 持续优化关联规则、降低告警噪音

平台稳定，高性能、高可用

1. 保障安全告警的时效性
2. 保障7*24小时持续运行

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

安全监控工程能力设计—数据全面采集

PDC/SDC

阿里云
云主机、云安全中心、WAF、云防火墙、OSS、NAS、
应用系统等

流量探针
流量分析平台

场馆…

防火墙，流量探针，IDS，交换机，终端设备等

日志
资产

日志
资产

PNC/SNC

安全监控平台

1. 接入安全日志、告警日志、审计日志、应用系统日志
2. 接入主机资产、网络资产、终端资产数据
3. 基于攻防场景驱动数据质量优化：接入终端进程日志、DNS解析日志、终端security日志等。

日志
资产

安全监测
防火墙、WAF、上网行为管理 、漏洞扫描、资产探查系统、流量分析平台、流量探针、文件沙箱、SOAR、锡安平台等

终端安全
天擎、EDR、椒图、虚拟化、身份签发服务器、准入控制台服务器、天狗、Linux主机、Windows终端

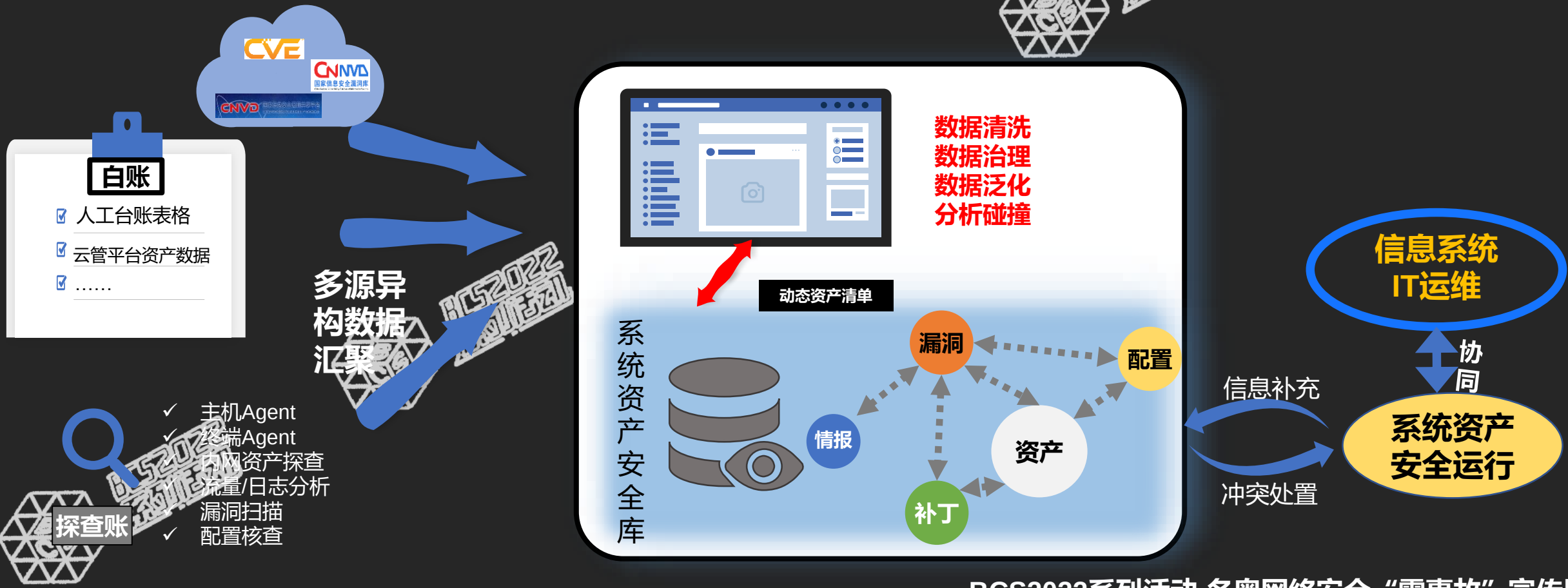
网关设备
负载均衡、堡垒机、蜜罐、SWG代理服务器、SDWAN管理中心、SDWAN中心节点、IPSEC VPN、SSL VPN、密码机、SMAC防火墙统一管理平台、堡垒机统一管理平台、流量解密防火墙等

奇安信 | BEIJING 2022

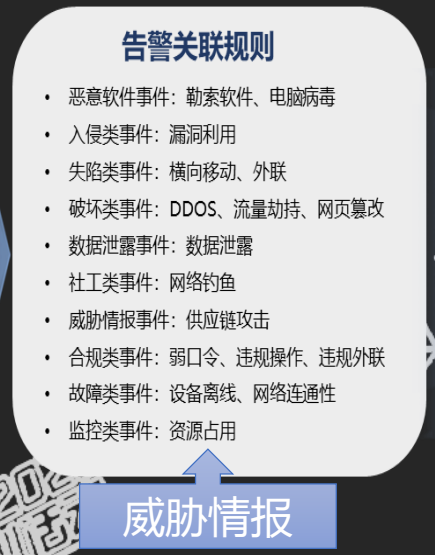
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

安全监控工程能力设计—资产闭环管理

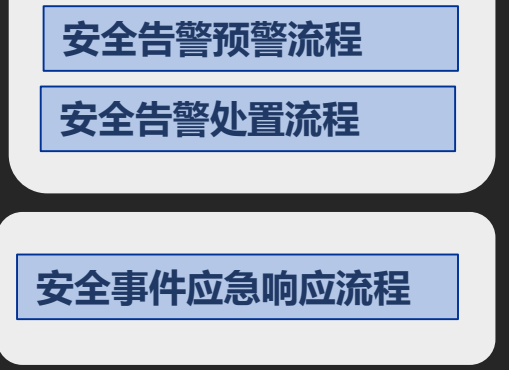
汇聚冬奥资产**“白账”**与**“探查账”**数据，结合漏洞情报，对**云上/云下资产**及其**配置、漏洞、补丁**等安全状况数据进行**数据治理**与**数据碰撞**分析，发现“白账”中**未登记的资产**及**登记错误**的数据，人工运行补全“探查账”中**未核实的**资产信息，判定**资产安全状况**与**脆弱性缓解优先级**，形成冬奥信息系统的**动态资产清单**——**“系统资产安全库”**！



安全监控工程能力设计—规则有效



安全告警分析



- ✓ **常态化关联规则优化：**SMC威胁建模专家不断优化关联规则逻辑、不断优化参数设置，使告警精准、有效、可控。
- ✓ **安全告警分析：**当出现关联规则构建逻辑分歧、不确定性异常等复杂问题时，安全分析专家、威胁建模专家会不定期召开安全告警分析会，及时讨论关联规则优化方案。

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

终端安全工程技术架构

NGSOC

10+种设备联动，实现处置命令、策略下发
快速响应，处置闭环

SOAR
告警数据对接
支撑SOAR溯源取证分析

WAF
阻断外部攻击IP的访问
阻断对恶意域名/IP的访问

天擎/EDR
办公终端失陷终端隔离
恶意文件隔离

NGFW
阻断外部攻击IP的访问
阻断对恶意域名/IP的访问

第三方防火墙
阻断外部攻击IP的访问
阻断对恶意域名/IP的访问

椒图
服务器端的失陷终端隔离，恶意文件隔离

NAC
禁止问题/失陷账号入网

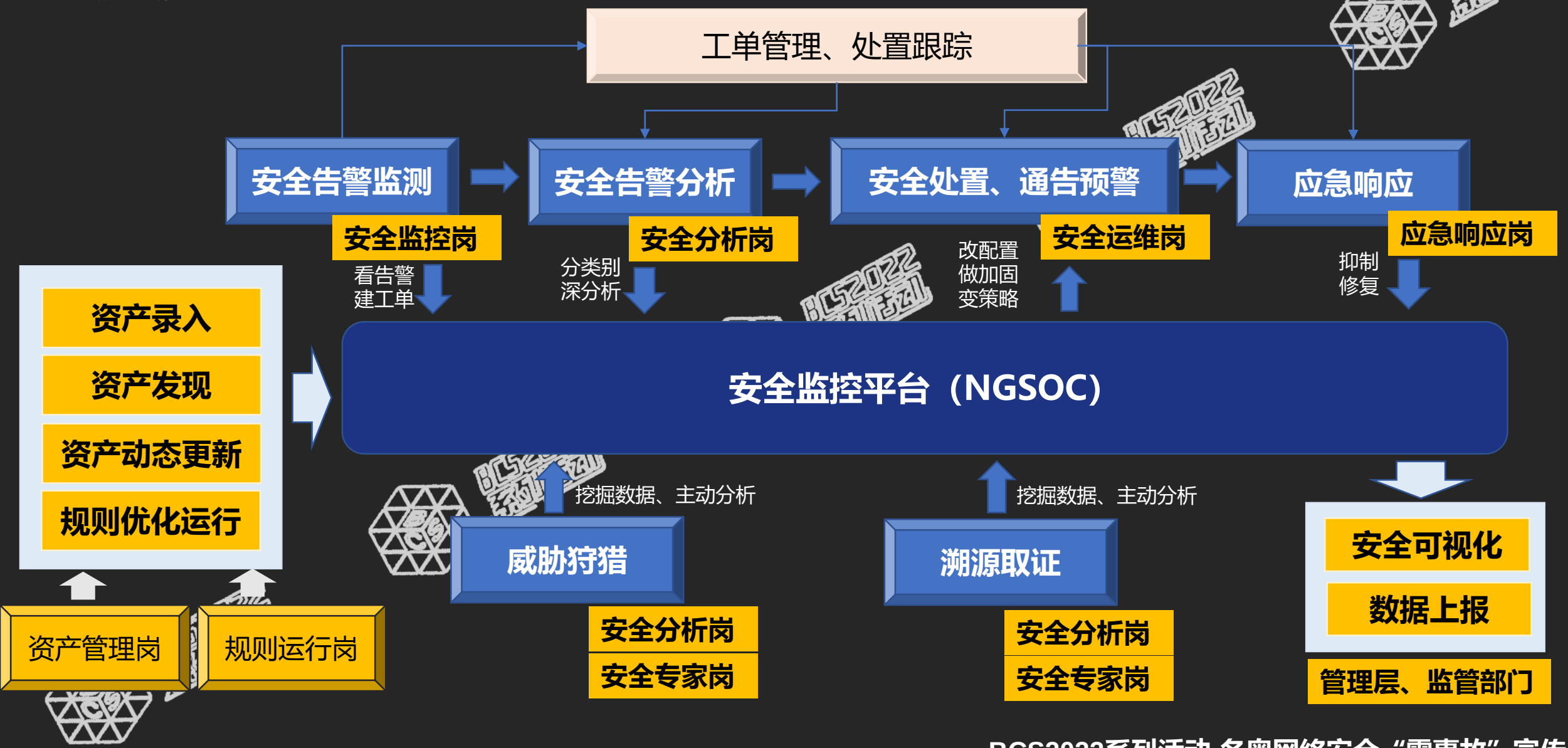
ICG
阻断外部攻击IP的访问
阻断对恶意域名/IP的访问

漏扫
下发漏扫任务
漏扫报告对接
漏扫报告导入

资产探查
下发探查任务
全网资产动态同步

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

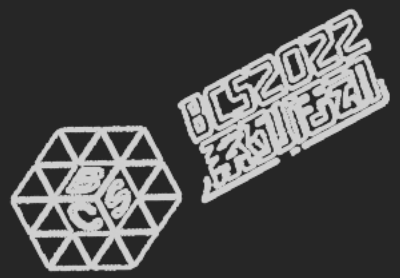
安全监控工程运行架构



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

北京冬奥会网络安全保障体系态势感知工程设计



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

态势感知工程建设目标

平台定位

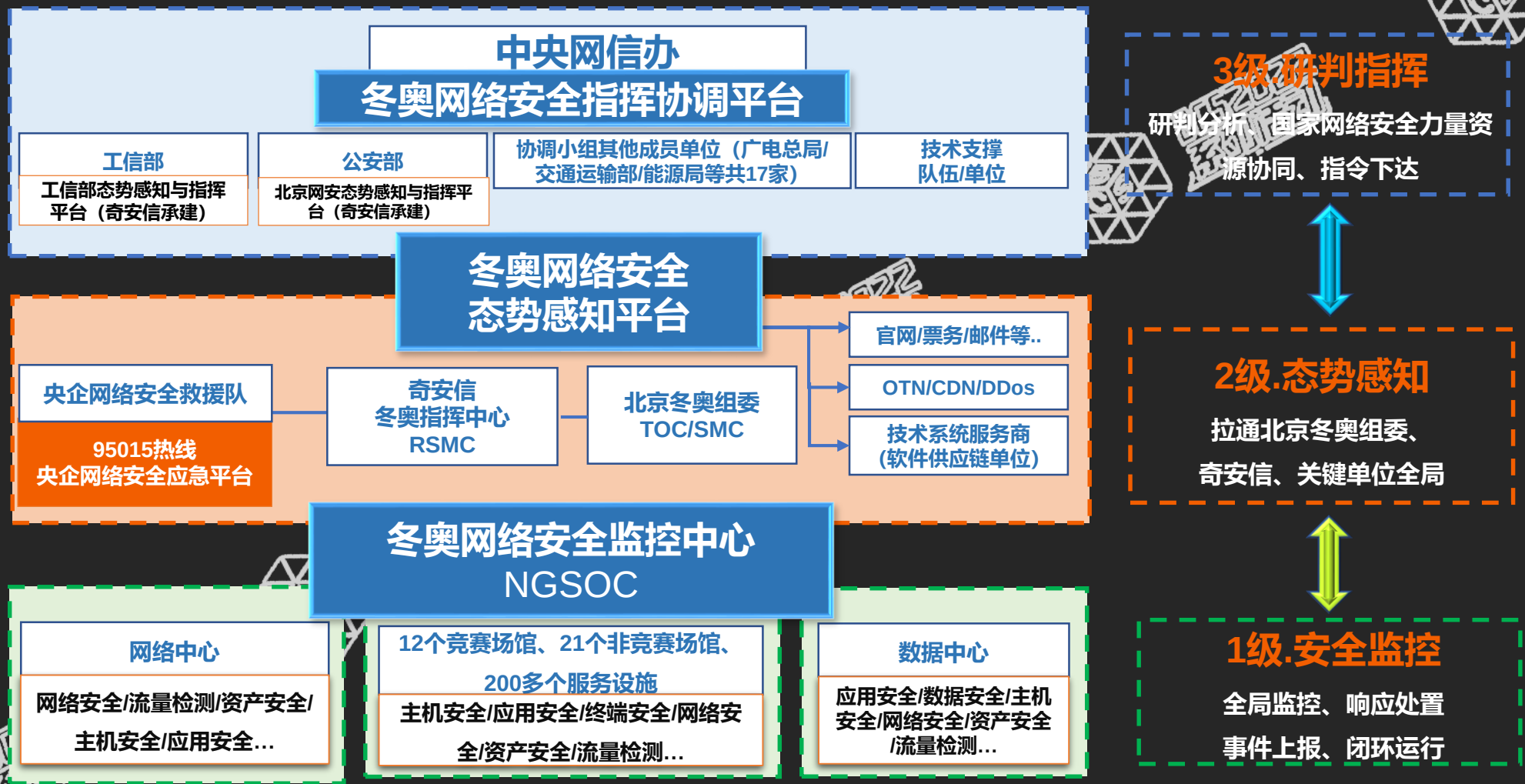
实时汇聚纷繁复杂的安全事件、外部相关部门提供的安全情报、安全预警等信息进行统一分析，通过可视化的方式，支撑冬奥会安全管理团队做出研判，进行事件决策、管理并调度相关资源进行快速响应提供全面、准确的决策数据支撑。最大程度降低、消除安全事件引起的负面影响，保障赛事安全、顺利的进行。

建设要求

- 掌握赛事相关信息系统网络安全监测
- 建立健全网络安全事件应急预案和响应流程
- 加强外部防御和内部管控，提高突发事件应对能力和处置效果
- 建立和健全信息资源共享机制

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

态势感知工程定位



态势感知工程功能架构


平台接口
业务协同接口
数据服务接口
系统通讯接口
统一接口管理
业务应用
态势展示
冬奥整体安全态势
场馆安全事件态势
事件处置态势
协同资源态势
指挥协同
安全监测
协同调度
信息共享
安全运营
研判决策
综合事件研判
综合审核
决策呈报
资产管理
冬奥合作伙伴管理
人员管理
资产管理
情报信息管理
数据治理和融合
数据服务
全文检索
统计分析
关联分析
标签服务
日志服务
字典服务
配置服务
资源中心
原始库
日志库
告警库
安全事件库
资产信息库
治理资源库
地址信息库
情报信息库
漏洞库
数据治理
网络安全领域数据模型
数据采集
数据清洗
数据融合
数据富化
数据调度
数据源
安全监控平台
OTN
冬奥官网
邮件系统
云端监测数据
CDN
第三方合作情报
大数据基础平台
平台支撑
运维管理
运营管理
数据监控
系统管理

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