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”[illegible]周

冬奥模式的实战化安全运行服务

顾鑫　冬奥项目组一线团队负责人
网络安全应急经理

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

兑现冬奥网络安全“零事故” 运行承诺

2019年12月26日，奇安信集团正式成为北京2022年冬奥会和冬残奥会官方网络安全服务和杀毒软件赞助商。官方赞助商应对北京冬奥会网络安全服务保障***承担全面的、彻底的、“端到端”***的责任。

目标：冬奥会网络安全***“零事故”！***

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

奥运会背后的网络安全战场

2012年 英国伦敦夏季奥运会

- 奥运会开幕前，黑客对伦敦奥运会的IT基础架构进行了约10分钟的漏洞扫描。
- 开幕当日，奥林匹克场馆电力系统遭受了约40分钟大规模DDoS攻击。此外，多家媒体机构遭到了攻击组织发动的针对性网络攻击。

2014年 俄罗斯索契冬季奥运会

- 索契冬奥会开幕式在10秒倒计时过程中，两块大屏幕都只数到5就黑屏。
- 低级别的网络安全事件在整个赛事筹备和举办过程中也层出不穷，包括：金融欺诈、虚假网站售票、黑客攻击行为导致网站暂时关闭等。

2016年 巴西里约热内卢夏季奥运会

- 黑客攻击行为，包括网站毁损，尽管其水平比2014年FIFA世界杯低得多。
- 来自政府和与奥运相关的组织（例如反兴奋剂机构）的数据泄漏；针对政府和赞助商网站的DDoS攻击，峰值为300Gbps-500Gbps。

2018年 韩国平昌冬季奥运会

- 2018年2月9日开幕式期间主办方遭遇身分不明的黑客攻击，服务器被入侵，互联网和广播系统影响。
- 奥运会网站瘫痪，无法打印门票，导致很多人无法参加开幕式。

2020年 日本东京夏季奥运会

- 2021年5月，负责东京奥运会网络安全的工作人员信息遭到窃取和泄露。
- 7月20日，开幕式前夕，东京奥组委发现伪装成为PDF图标的钓鱼恶意程序，试图钓鱼相关工作人员。

奥运会已经成为网络攻击的目标，无论是从经济利益为目的的黑客组织，还是国家级黑客，都是面临的巨大挑战

奇安信

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

两年精心建设和运行准备，兑现“零事故”运行承诺

设计期	▸2019年12月-2020年6月 ▸设计期同步开展应用系统全生命周期管理 ▸强调模块化、工程化设计
建设期	▸2020年3月-2021年10月，基础建设完成 ▸2021年11月，增补建设态势感知等专项任务
非关键运行	▸2021年2月-2022年1月，边建设，边运行；
关键期保障	▸2022年1月23日-3月16日，赛事保障，可用性优先
清退期	▸2022年3月-6月，数据清除、设备回收

韩子荣

北京冬奥组委专职副主席、秘书长

奇安信通过先进的技术、一流的服务、创新的模式，为北京冬奥会提供了全过程、全周期、全维度的网络安全保障，筑起网络安全的铜墙铁壁，**让北京冬奥会成为有史以来最安全的冬奥会！**

方滨兴

中央网信办冬奥会网络安全专家研判组组长，中国工程院院士

奇安信已经成功的完成了冬奥网络安保任务！做出这么好的成绩，非常值得祝贺，**对你们将来在市场上占有更高的制高点是好事，对国家更是大好事！**

喻红

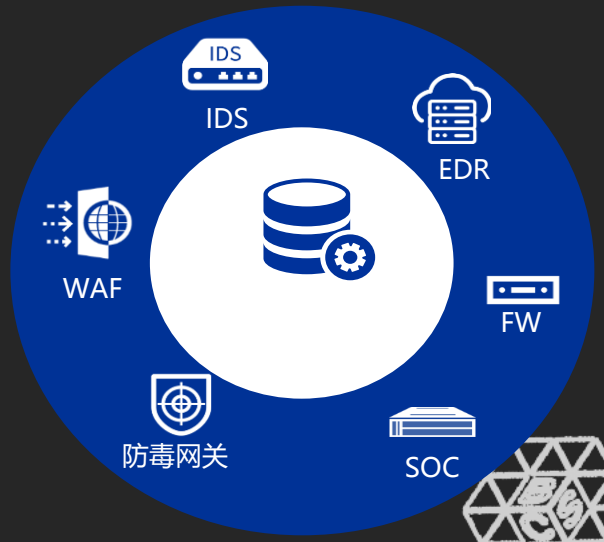
北京冬奥组委技术部部长

奇安信成为冬奥网络安全赞助商是首创，非常成功！“简约、安全、精彩”这个安全**没有网络安全就谈不上冬奥安全，这是奇安信对冬奥会做出的重大贡献！**

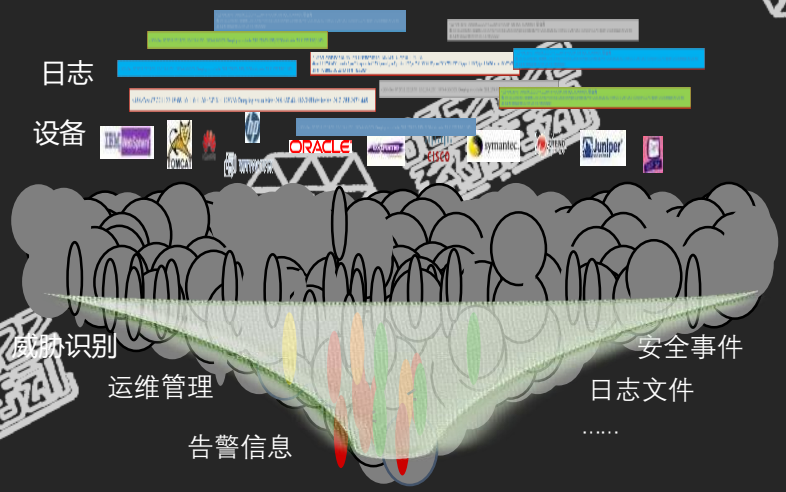
- 累计监测到各类网络攻击超**3.8亿**次（含社会面）；
- 跟踪、研判、处置涉奥事件**105件**；
- 发现恶意样本数量达**54个**，排查风险主机**150台**；
- 累计发现、修复漏洞**5782个**；
- 冬奥期间，日均监测日志超37亿条，监测日志数量累积达**1850亿条**；
- 投入、生产**威胁情报超过25000条**，基于情报内生体系，落地安全运行闭环。

挑战1：安全技术建设投资如何发挥能效

网络安全技术建设投资能效不显著，无法应对持续不断、隐蔽、多变的网络攻击



策略无法有效执行，安全运维效率低



海量日志导致麻木，风险处置不及时

资产不清，漏洞难管，应急难定位

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

挑战2：安全要求如何执行、效果如何保障

01
- 管理与运行脱节，“规矩”只是**挂在墙上**；

02
- 安全团队与信息化团队**扯皮多**，无法高效协同；

03
- 奥运会业务系统连续性要求，突发安全事件**无法快速决策，处置无序**；

04
- 规程众多，人员操作依靠个人经验或者临时查看操作手册，**效率低、有偏差**。

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

挑战3：如何应对网络空间的“不宣而战”

物理空间“作战”

平时 → 训练 → 战备等级转换 → **战时** → 作战：攻+防

特点：
- 平时、战时界限分明
- 通过战备等级实现转化
- 战时攻防自主转换

网络空间安全防御=“战时”就是日常

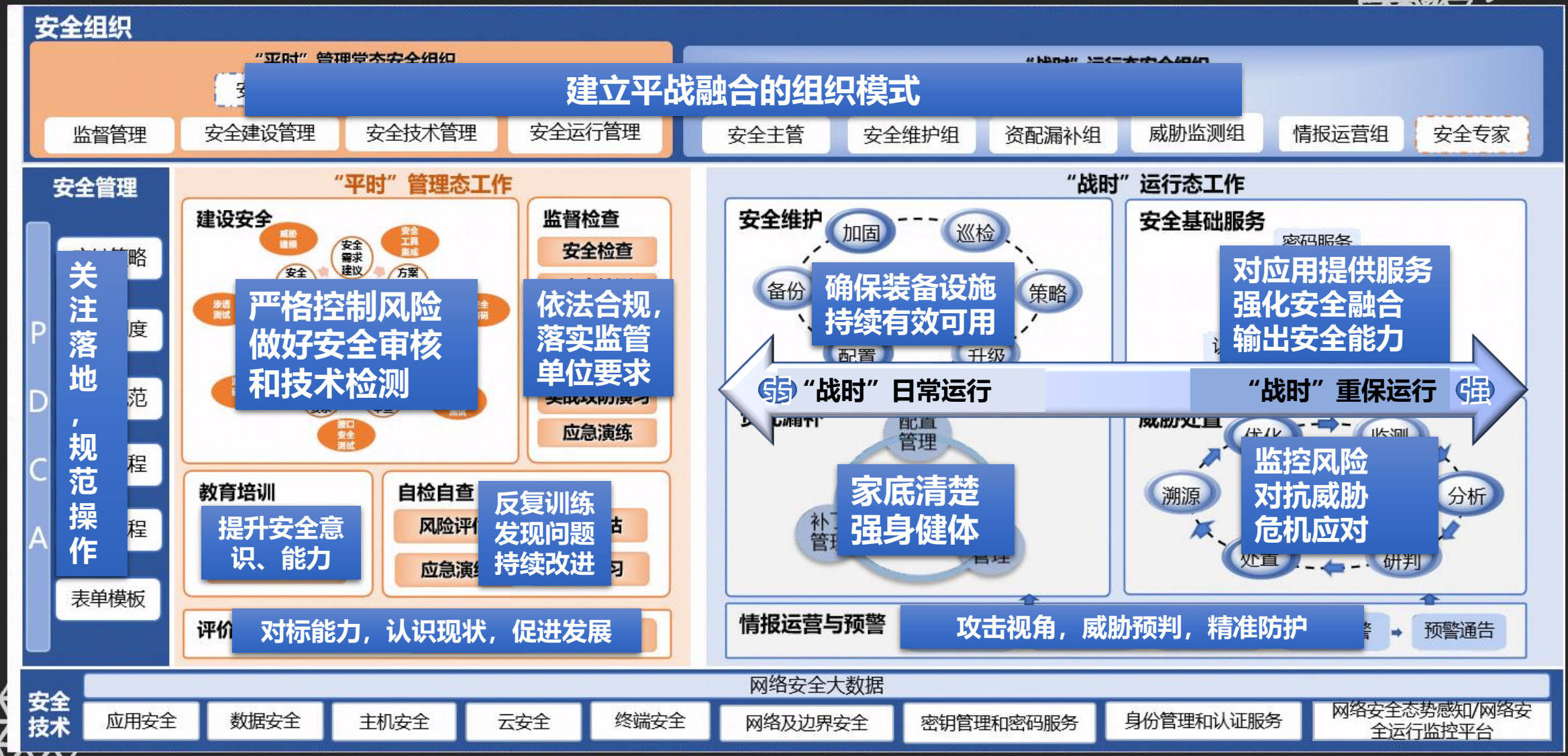
网络空间“作战”

“一般等级”战时 → 运行+溯源处置+训练 → 作战等级转换 → **“高等级”战时** → 高频次有限度反制

特点：
- 平、战融合，无界限
- 攻防兵种不同，特殊阵地
- 作战等级：时间点、不同等级威胁

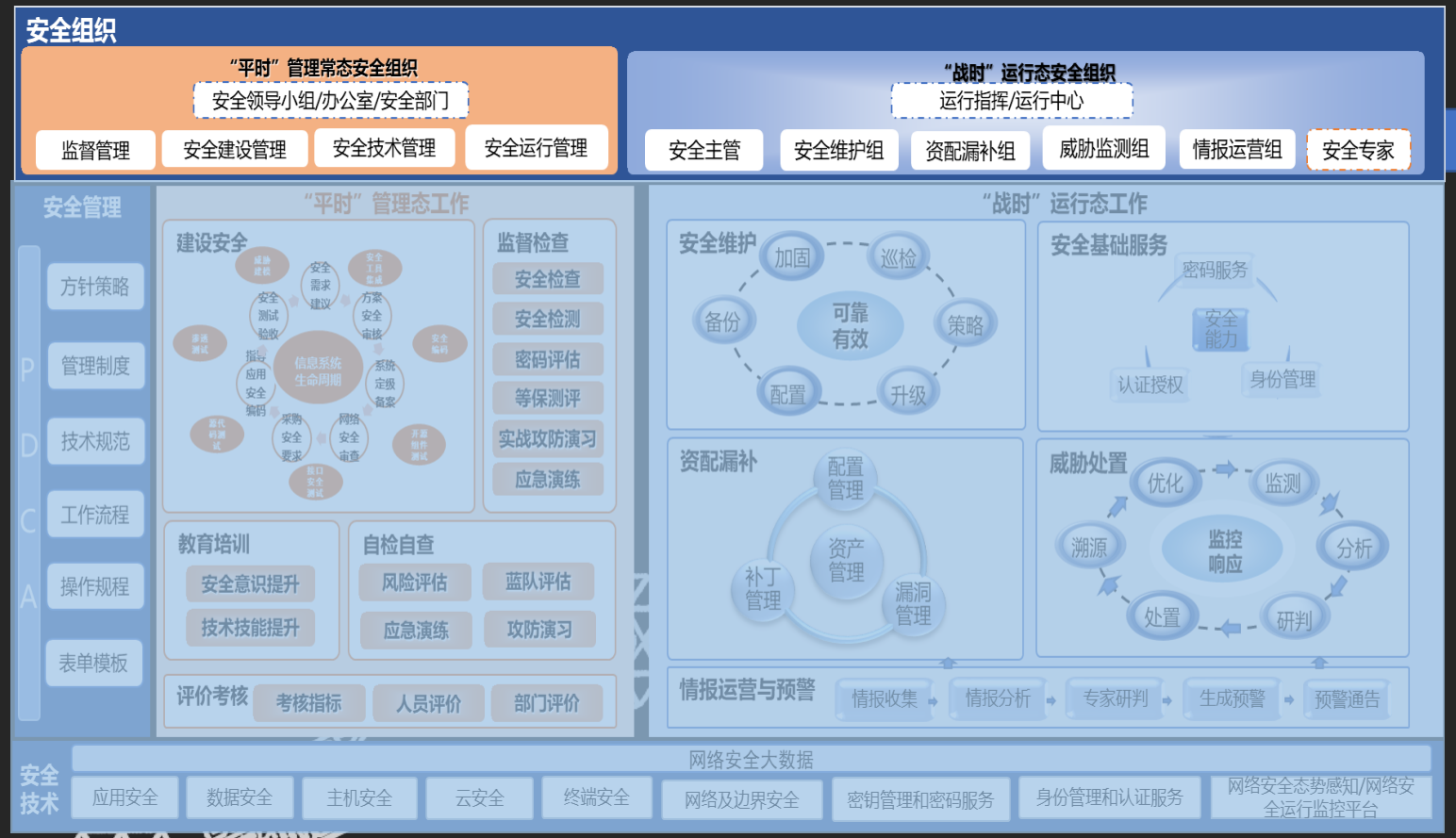
奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

安全运行体系设计思路：平战融合、可对抗、可持续运行



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

组织|冬奥“平战融合”的组织体系



面临问题：

1、日常态（平时）与运行态（战时）并存，岗位、人员有限，如何同步开展工作；

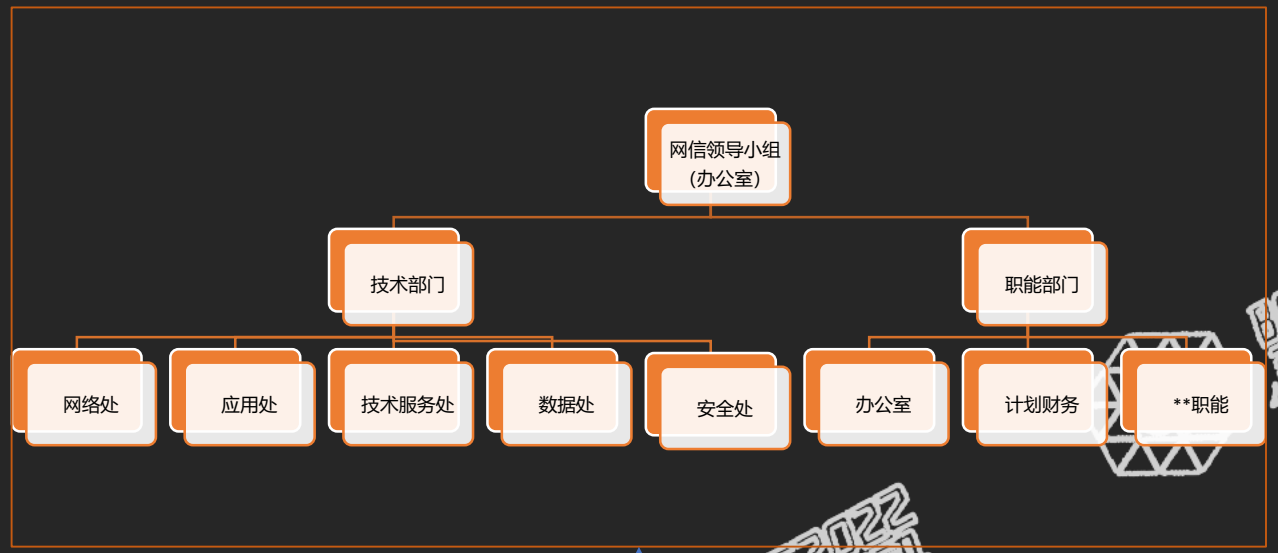
2、网络安全涉及所有IT相关横向部门，如何协同处置；

3、安全岗位错综复杂、涉及广泛，如何制定合理的岗位、职责与配合机制；

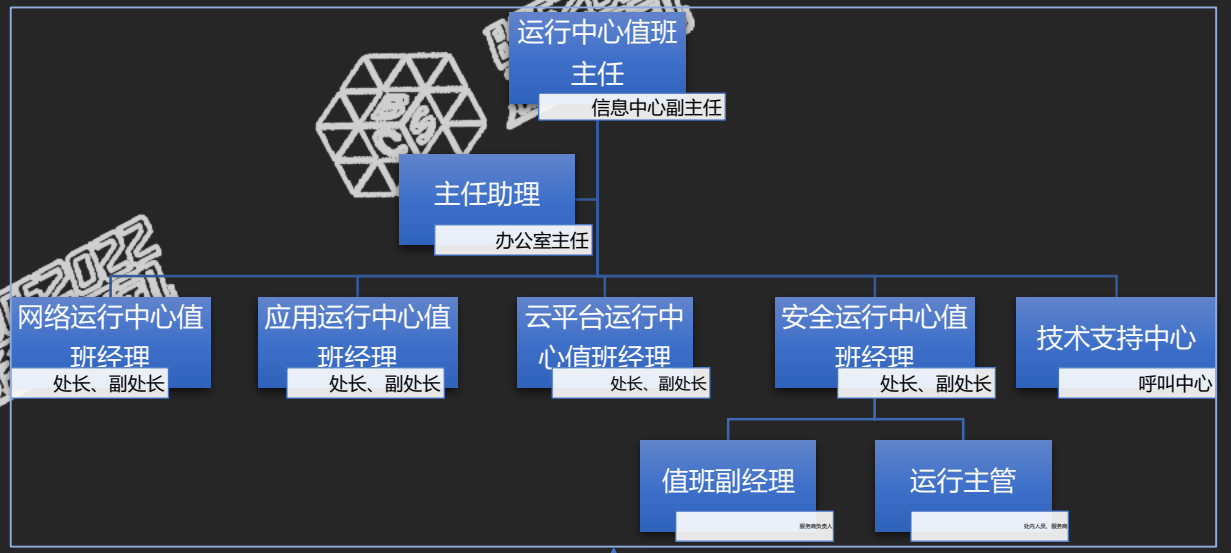
……

组织|冬奥“平战融合”的组织体系

日常态（管理态）网信组织架构示意（行政组织）



运行态网信组织架构示意（运行中心）



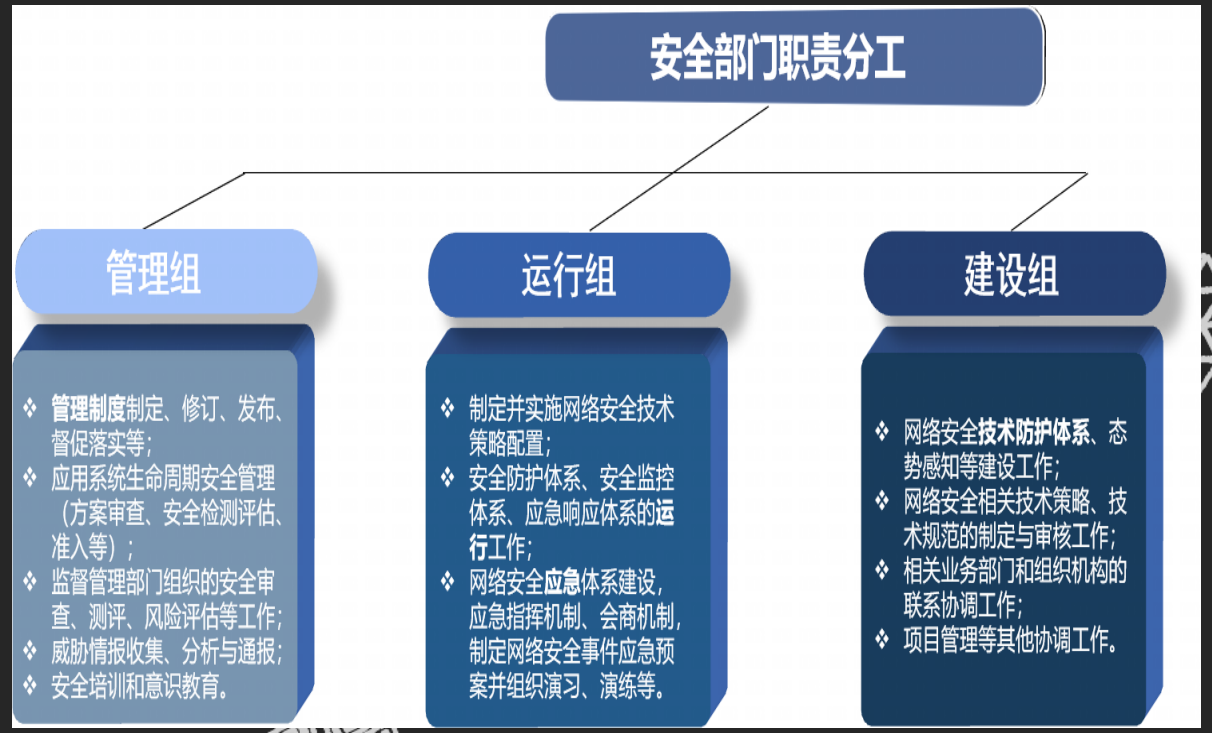
同一班子人员（组织并行、职能切换）

- 日常态（管理态）和运行态组织并存
- 日常态（管理态）按照行政架构和工作流程执行（统筹规划、同步建设、建章立制、依法合规、能力提升）
- 运行态按照运行中心（中枢协调联络、全天候监控响应、处理突发）的运行管理流程执行

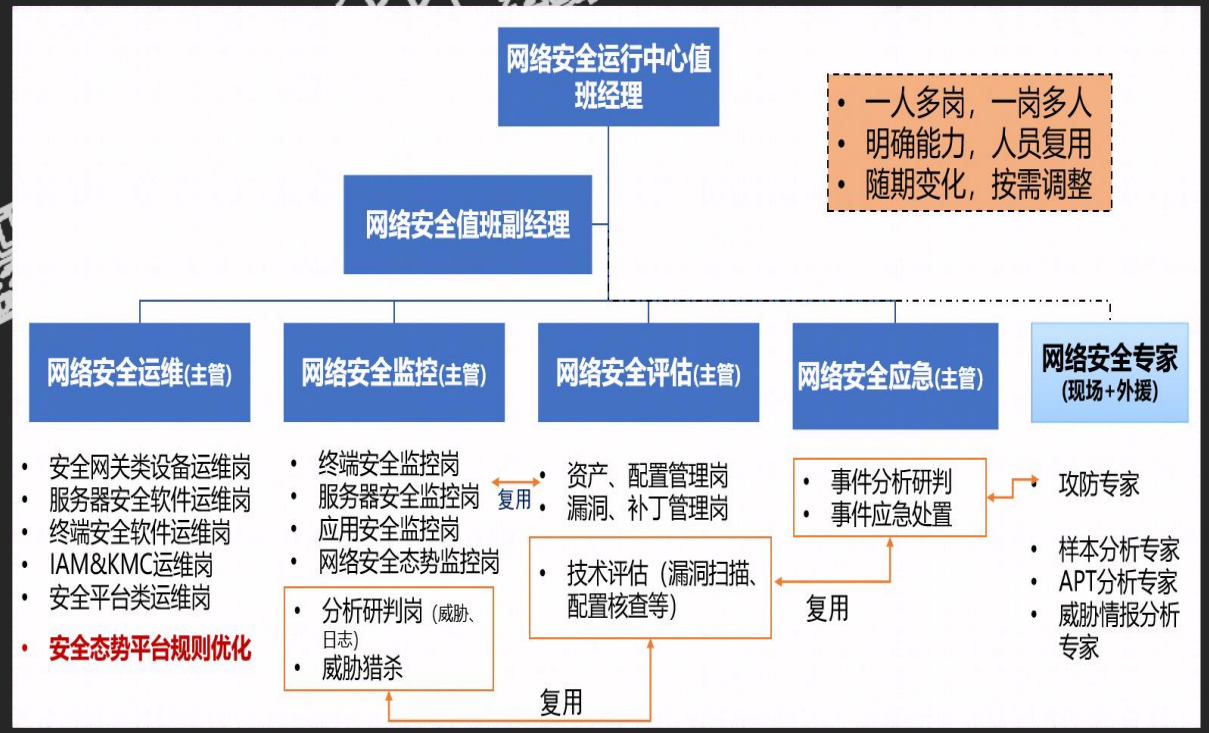
奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

组织|冬奥“平战融合”的组织体系

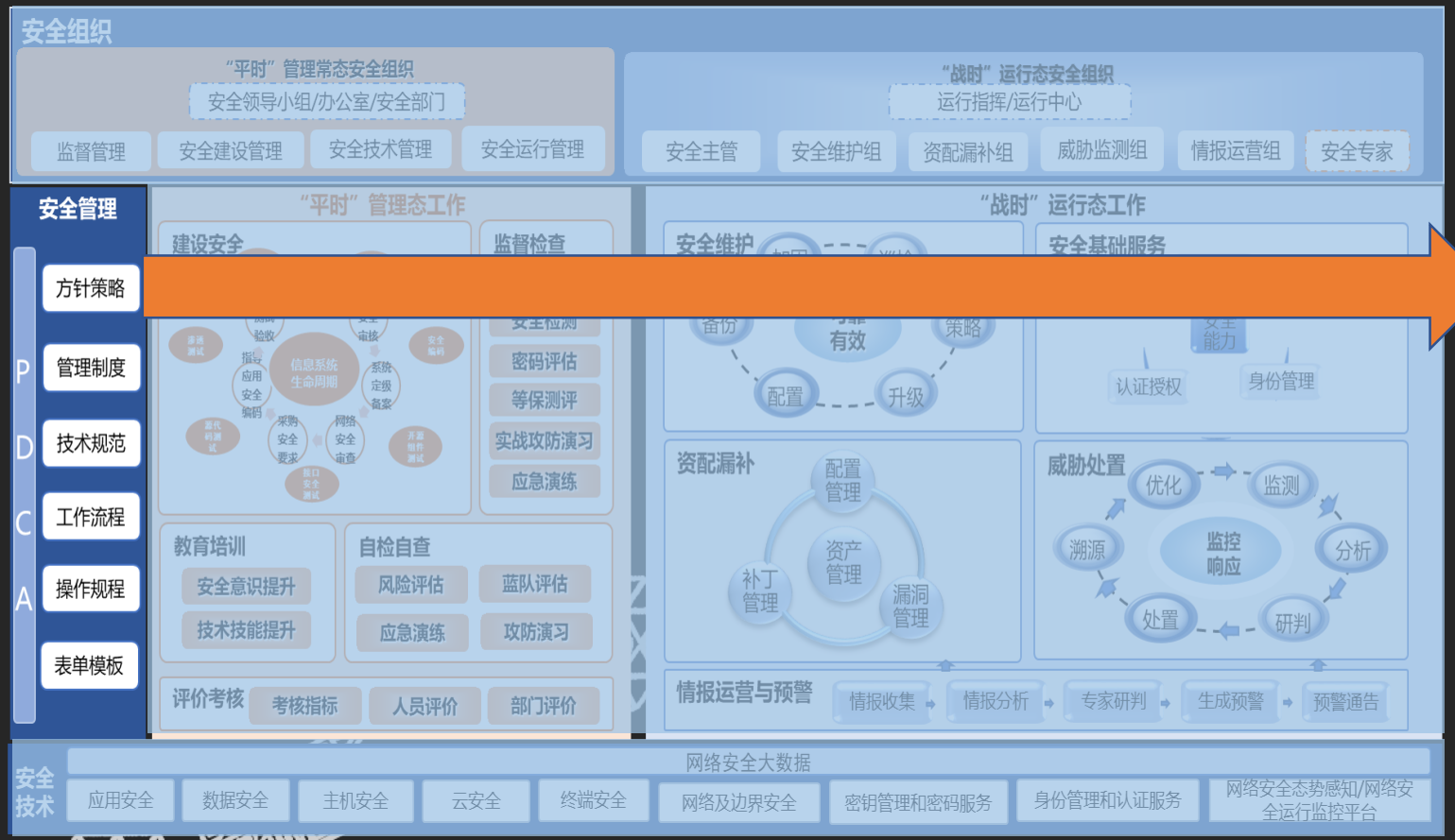
日常态（管理态）安全职责示意



运行态安全职责示意



管理|可落地的安全管理制度体系



面临问题：

1、网络安全战略、规划高高在上，与具体执行之间存在断层；

2、安全制度只提要求，不告知如何落地，不可执行；

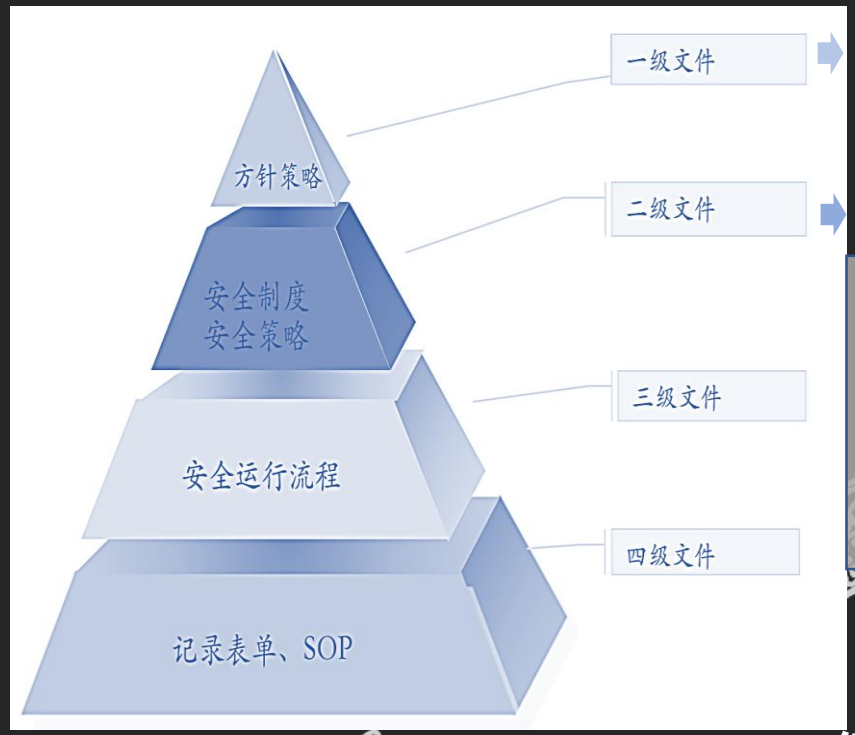
3、网络安全制度和IT运行制度有冲突，或三不管；

……

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

管理|从实战出发，制定并落实标准化文件



IT安全战略、信息系统总体规划

网络安全管理办法、 IT安全策略、IT安全架构

网络安全守则	IAM账号管理和使用安全要求	服务器运维安全策略
网络行为管理策略	应用程序安全编码指南	网络安全策略
用户账号和密码管理策略	[illegible]	软硬件资产安全管理策略
邮件安全策略	网络安全漏洞管理策略	服务桌面安全策略
终端技术设备安全管理策略	[illegible]	信息系统生命周期网络安全要求
计算机终端用户安全要求	中间件安全配置策略	数据安全保护策略
打印机安全管理策略	web服务器安全配置策略	应急预案概述
哑终端安全管理策略	linux服务器安全配置策略	总体应急预案
VPN账号申请和安全使用要求	网络设备和安全设备安全运维策略	专项应急预案.....

用策略代替制度，
策略要有技术控制点来支撑！
没有技术体系支撑的策略，是挑战人性！

一级文件：

结合IT规划，同步设计、同步落实。

二级文件：

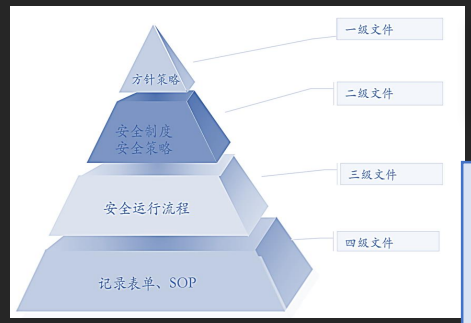
自上而下：落实框架，解决全面性问题；

自下而上：找问题，解决具体实际风险。

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

管理|底数清、运维明、流程严、处置灵



规范化、流程化确保安全策略、要求有效落实

三级文件：
明确工作流程，确保工作流通畅

四级文件：
通过SOP（操作规程）、表单、保障工作可标准化落地，并有证可查

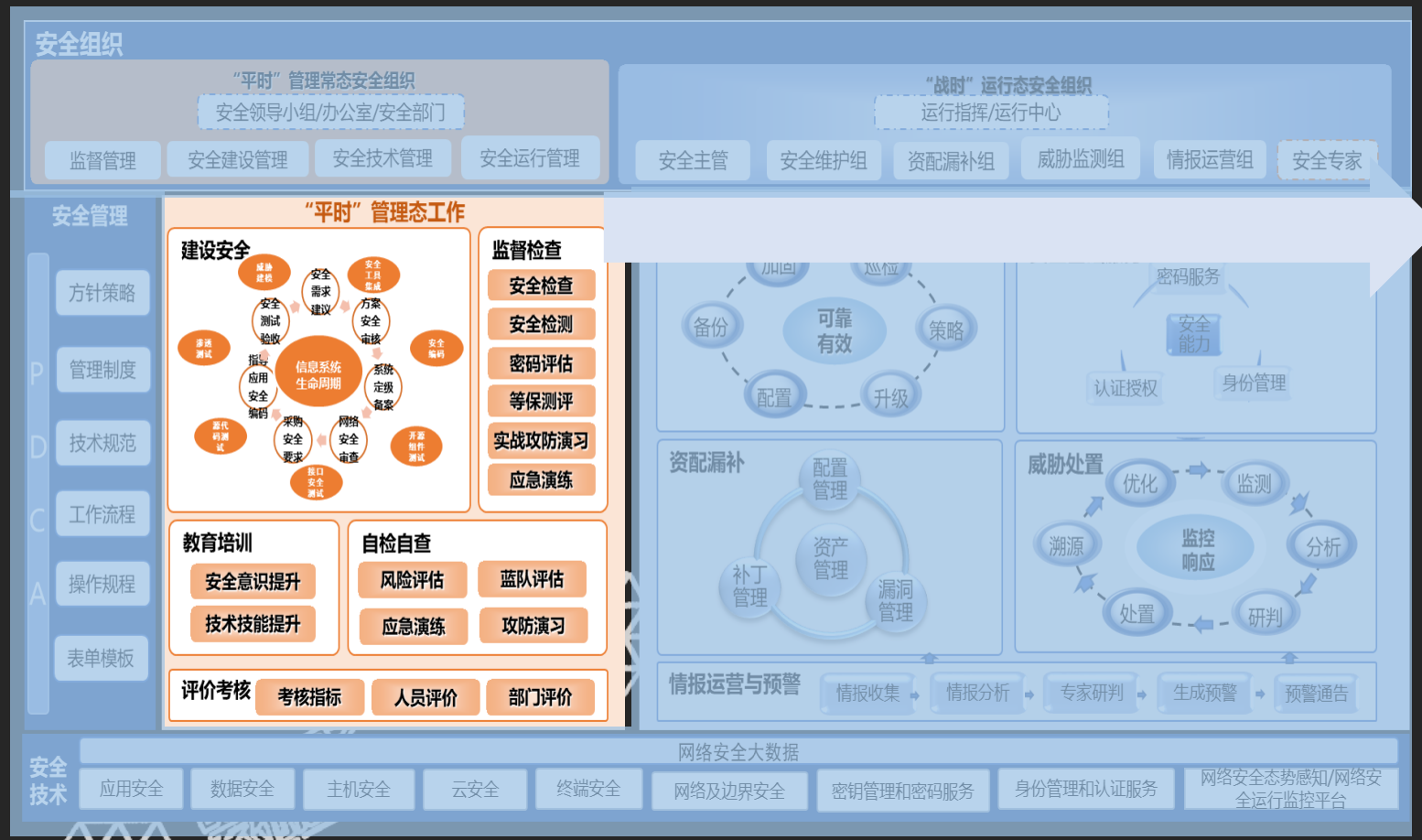
安全维护	资配漏补	安全支撑业务	风险处置
设备巡检流程 工作汇报流程 工单管理流程 策略变更流程 配置备份流程 版本升级流程 补丁&hotfix升级流程 故障处置流程 备机替换流程 样本提取流程	资产入网流程 资产核实流程 配置变更流程 配置维护流程 漏洞扫描流程 漏洞修复流程 补丁更新流程 补丁维护流程	VPN账号申请流程 IAM账号申请使用流程 IAM账号变更流程 保险柜账号开通流程 堡垒机账号变更流程 密码密钥使用申请流程 密码密钥管理监控服务流程	安全告警及预警排查处置流程（总）、日常告警监测流程、日常告警分析流程、钓鱼攻击排查流程、恶意样本排查处置流程、供应链风险预警流程、勒索病毒事件处置流程、流量劫持事件处置流程、恶意代码攻击事件处置流程、信息篡改事件处置流程、信息泄露事件处置流程、供应链攻击事件处置流程、DDOS攻击事件处置流程
日常巡检SOP、工单系统SOP、策略变更SOP、配置备份SOP、版本升级SOP、补丁&hotfix升级SOP、故障处置SOP、通报SOP、终端问题处置SOP、安全事件协同SOP、备机替换SOP、交接班表单、设备巡检表单、变更申请表单	资产登记记录单 资产信息变更记录单 资产核实记录单 配置变更SOP 配置维护SOP 漏洞扫描SOP 深度/广度漏洞SOP 补丁操作规程 补丁更新记录	VPN账号开通申请单 VPN变更申请单 VPN账号开通申请汇总单 IAM账号开通申请单 密码密钥使用申请单 密码密钥使用汇总单 密码密钥使用操作SOP	监控每日报告、监控事件汇总表、分析数据汇总表、交接班要点记录单、每日报告、勒索病毒应急人员操作手册SOP、流量劫持应急人员操作手册SOP、恶意代码攻击应急人员操作手册SOP、信息泄露事件应急人员操作手册SOP、供应链攻击事件应急人员操作手册SOP、DDOS攻击事件应急人员操作手册SOP

所有的安全工作、安全技术控制点的落实，都要通过标准化流程来固化，形成闭环与团队协同！

具体操作要标准，提高效率、降低人力成本。
一般性、普适性工作，不依靠个人经验，减少犯错误的几率。

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

平时|“管理态”网络安全工作



面临问题：

1、应用系统自身安全没有把控，先天不健康，后天弥补难度大，导致带病运行；

2、疲于应对安全监督检查，自身没有得到实质性提升；

3、人员安全意识薄弱，一旦突破，体系破防，对重要系统及数据带来极大风险；

……

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

平时|“管理态”网络安全工作

建设期网络安全风险管控

需求调研 → 立项采购 → 设计阶段 → 开发阶段 → 测试集成 → 交付阶段 → 运行阶段

建设期安全风险管控工作

需求调研	立项采购	设计阶段	开发阶段	测试集成	交付阶段	运行阶段
安全需求建议	安全经费纳入项目预算	设计方案要通过评专家评审和网络安全审查	源代码审计	配置安全策略	生产环境安全检测、渗透测试、漏洞扫描、配置核查	等级保护测评
确定信息系统保护等级	采购合同中明确安全要求	完成等级保护定级备案	渗透测试	查找安全漏洞	组织资产核验、安全验收测试	资配漏补
				配置运维账号权限		风险评估
				确认资产信息		应急预案
				开源组件安全评估\源码审计、渗透测试		应急演练

- 安全部门信息部门之间建立敏捷、高效的沟通机制；
- 提前制定并发布信息系统生命周期安全管理办法，配套安全技术策略、安全需求建议模板、安全编码规范、安全测试规范和相关报告模板；
- 建设期工作要和运行期工作衔接，做好资产、策略、配置、权限、漏洞等相关工作；
- 管控过程要能够同步落实国家网络安全审查、等级保护制度等相关要求。

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

平时|“管理态”网络安全工作

落实监督检查

- 《网络安全法》
- 《数据安全法》
- 《关键信息基础设施安全保护条例》
- 《密码法》
- 《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》
- 《党委党组网络安全工作责任制实施办法》

要求

监督检查机构（国家网信部门、公安机关）	网络（关基）运营者
安全检查	安全自查
安全检测	渗透测试
密码评估	风险评估
等保测评	蓝队评估
关基风险评估	应急演练
数据安全评估	
实战攻防演习	
应急演练	

开展攻防演习

组织、协调

组织单位

攻击队

成立若干攻击小组，以竞赛或合作的方式展开真实的网络攻击，发现安全漏洞，获得服务器权限。

实战攻防演习平台

可视化展示，所有攻击行为安全可控，攻击录屏，视频监控

防守单位

成立防护工作小组，实时监控网络，进行实时阻断，应急响应等工作。

开展应急演练

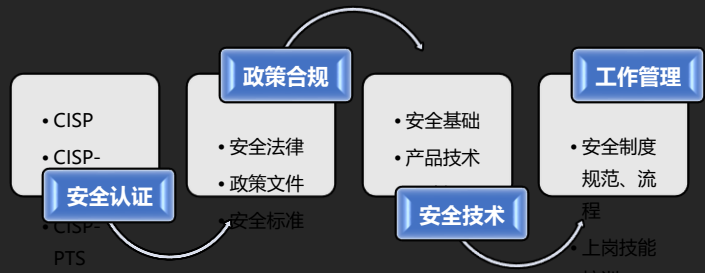
- 桌面演练
- TR演练
- 攻防演习

- 关注应急响应组织、流程、响应时效、流转配合等
- 关注应急响应的事件监测发现、分析、响应和处置能力

提升人员能力

安全意识提升

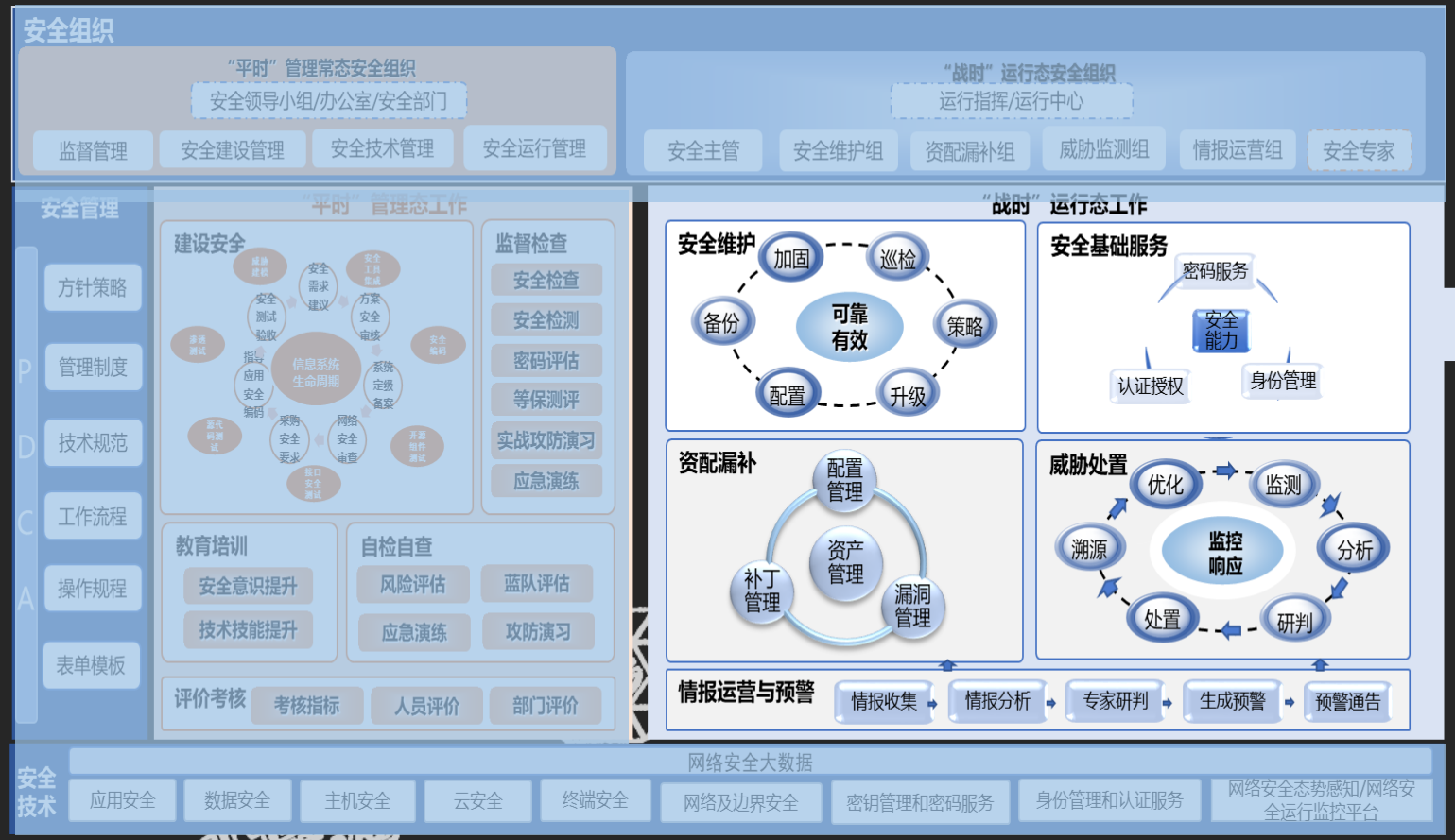
安全能力提升



安全意识专项测试-钓鱼邮件测试

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

战时|“运行态”网络安全工作



面临问题：

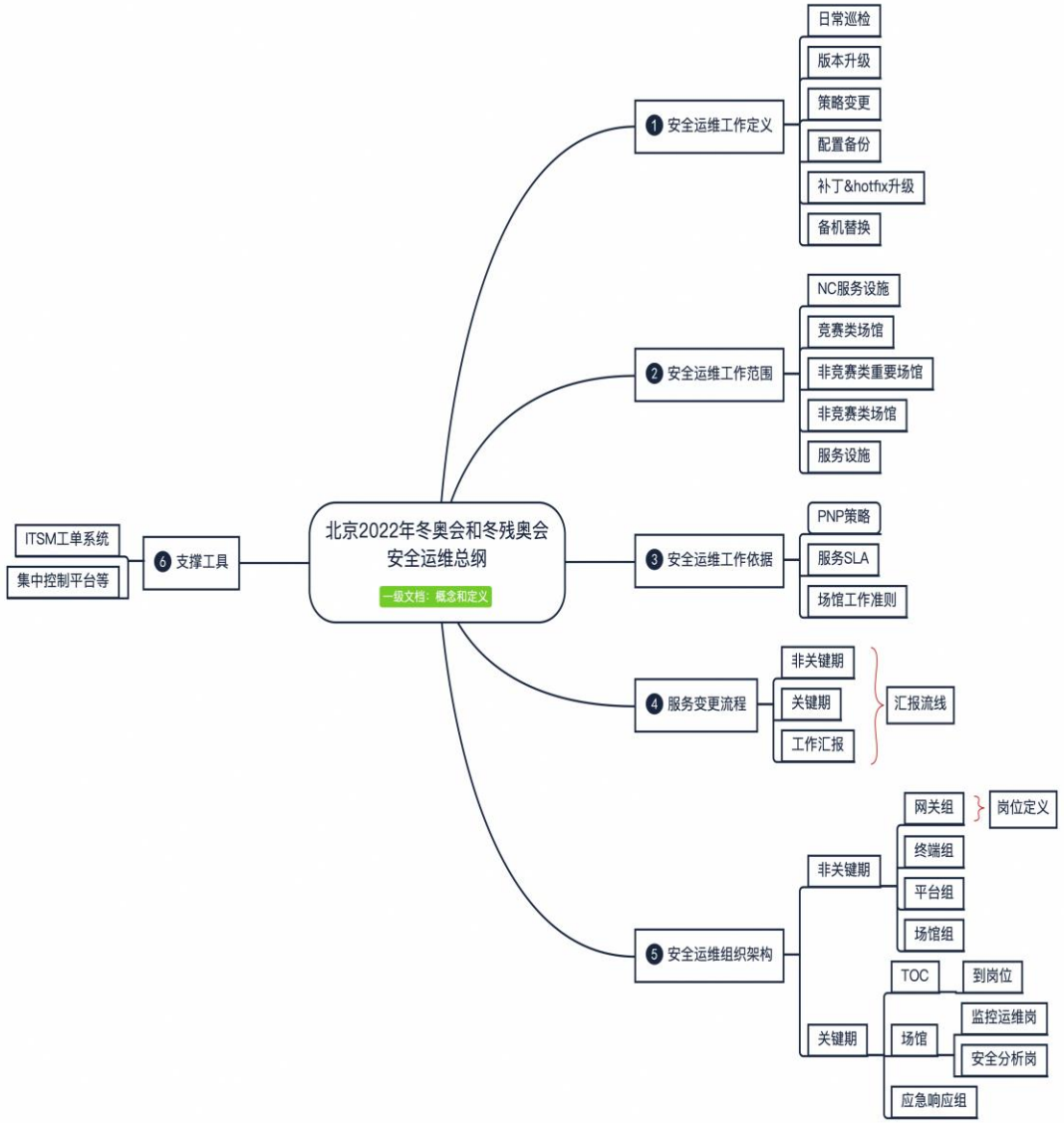
1、策略设计、落实、清理等环节管控不严，历史策略无人维护，导致策略失效；

2、家底不清、漏洞不补、配置不管，导致系统资产脆弱不堪；

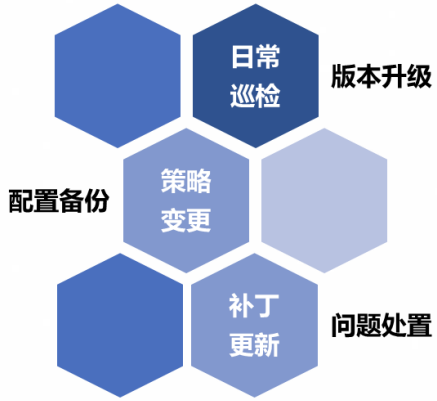
3、海量告警数据，淹没真实事件，安全监测设备沦为事后溯源工具；

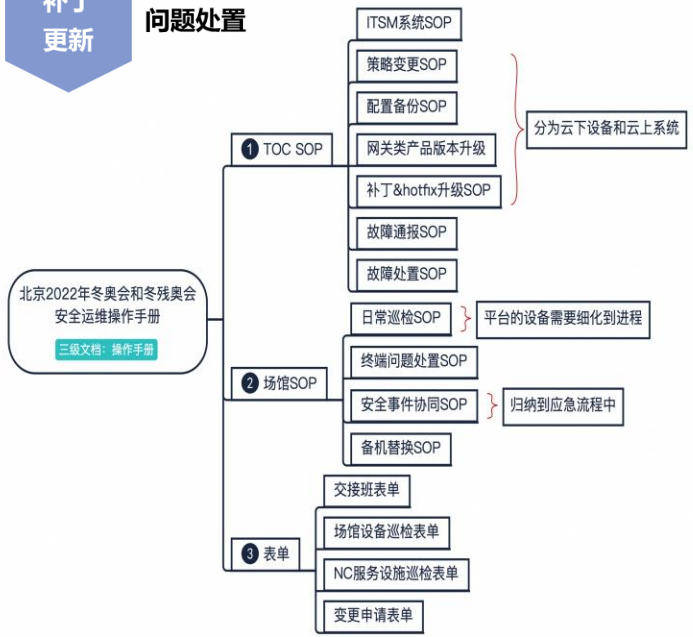
……

战时|“运行态”网络安全设备/系统维护



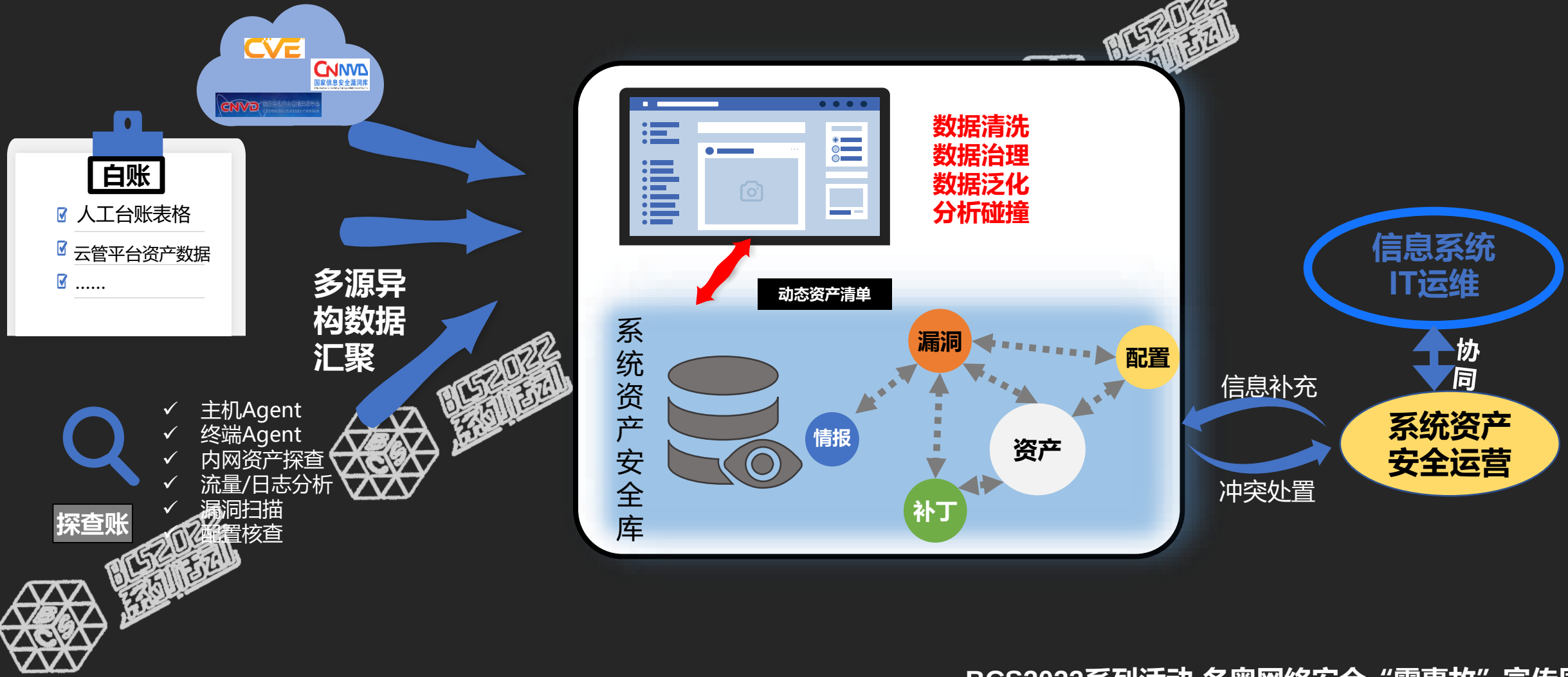
1、按照时间线，分为关键期和非关键期，将流程嵌套到两个期中；
2、落到某个具体流程或动作的时候，直接指到某个文档的某个内容；





安全产品运维关注标准化、流程化、规范化，运行人员能够按照规范、流程、操作指南等标准化要求操作，动作不变形

战时|“运行态”-资配漏补，保障运行流程闭环



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

战时|“运行态”-风险处置

百分七十的告警并不能直接认定为攻击！
百分之一的攻击不会直接产生告警！

37亿

数据源
- 防火墙
- 流量监测
- 主机防护
- 终端安全
- IDS
- VPN
- 上网行为
- 云平台监控
- 操作系统/数据库/应用

数据集成
- 数据接入
- 数据采集
- 数据清洗
- 数据富化
- 数据融合

告警关联规则
- 恶意软件事件：勒索软件、电脑病毒
- 入侵类事件：漏洞利用
- 失陷类事件：横向移动、外联
- 破坏类事件：DDOS、流量劫持、网页篡改
- 数据泄露事件：数据泄露
- 社工类事件：网络钓鱼
- 威胁情报事件：供应链攻击
- 合规类事件：弱口令、违规操作、违规外联
- 故障类事件：设备离线、网络连通性
- 监控类事件：资源占用

978

- 告警描述
- 告警场景
- 告警对应设备
- 告警分析SOP

安全告警分析

- 安全告警预警流程
- 安全告警处置流程
- 安全事件应急响应流程

基于攻防：真实攻击、关联分析
基于业务：理解业务、规则建模
→ 持续规则运营

基于情报：研判前置、情报融合
→ 前置分析研判

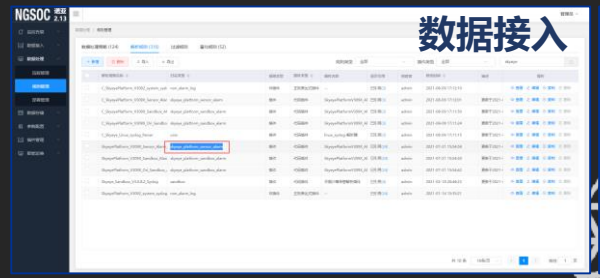
奇安信 | BEIJING 2022

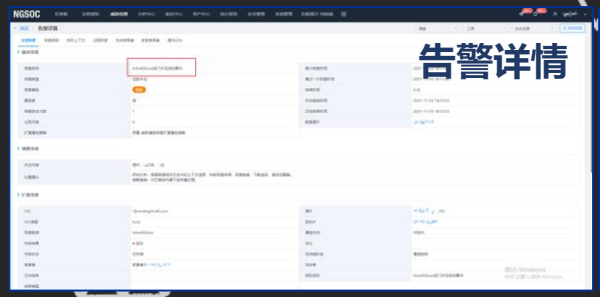
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

战时|“运行态”-统一运行平台实现核心业务全场景安全运行

全局视角

技术视角





实现：

1. 数据全打通关键低位数据全获取，威胁分析不断链；
2. 海量告警中提取高价值数据，避免被数据淹没；
3. 对”隐形“攻击进行建模分析；
4. 攻击链规则关联，实现标准化分析研判，更少依赖专家。

奇安信

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

冬奥实战化安全运行主要目标

家底清、责任明

装备“持续保障”

策略“全面有效”

隐患“动态清零”

告警“动态清零”

基于情报“精准防护”

对抗能力持续提升

安全零事故

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

结合冬奥实成果经验，推出战化安全运行咨询服务

	现状调研	安全运行体系总体设计	安全运行组织设计	安全运行制度样例设计	安全运行工作内容和机制设计	安全运行工具和平台建议
服务内容	① 梳理现有的安全运行组织、制度和技术措施情况； ② 调研现有安全运行体系的主要需求和管理层期望； ③ 调研安全运行体系的阶段性发展需求。	① 网络安全运行体系框架设计； ② 网络安全运行体系目标设计； ③ 网络安全运行体系阶段目标和重点任务设计。	① 制定网络安全运行组织框架； ② 设计网络安全运行组织岗位、职责； ③ 设计网络安全运行各岗位人员能力。	① 制定日常态“建设安全”管理制度和流程； ② 制定运行态“威胁检测处置”工作流程； ③ 结合项目和客户实际需求制定网络安全运行相关的制度、规范、流程和sop等。	① 日常态安全运行内容和机制设计； ②运行态安全工作内容和机制设计； ③结合项目和客户实际情况对部分工作内容、机制进行细化	① 制定数据安全分级管控与防护策略； ②结合数据使用场景制定场景化数据安全方案； ③制定数据安全体系建设路线与能力提升方案
关键交付	• 《网络安全运行体系现状调研和需求分析报告》	• 《网络安全运行体系总体设计方案》	• 《网络安全运行组织设计方案》	• 网络安全运行制度样例； • 结合项目交付具体的制度、规范等成果	• 《日常态和运行态网络安全运行内容和机制设计方案》	• 《网络安全运行工具和平台建议书》

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