



2024 WEST LAKE
DIGITAL SECURITY CONFERENCE
西湖论剑·数字安全大会

12th

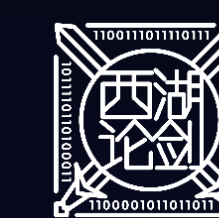
智绘安全X
INTELLIGENCE
ENHANCE SECURITY
ADVANCING
WITH DIGITALIZATION
乘数而上

《重大活动网络安全保障建设 及运营指南》解读

高丹 总裁助理

赛迪顾问股份有限公司

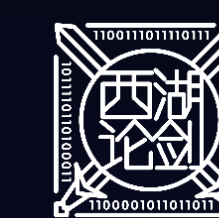




目录

CONTENTS

01. 重大活动网络安全态势及构建思路
02. 重大活动网络安全保障体系建设
03. 建议及展望



01

重大活动网络安全态势及构建思路

重大活动参与组织多、社会影响大，黑客攻击更加频繁，其安全保障尤为重要。重大活动期间因病毒传播、网络攻击、恶意入侵、信息泄露、服务宕机等网络安全事件频频发生，已成为全球性挑战。

重大活动定义

在中华人民共和国境内外组织举办的，对国家、行业、地方具有重大意义或者重要国际影响的大型活动。主要包括：

会议和论坛

通常是在政治、经济、科技、文化等领域举办的，汇集了国内外政要、专家学者、行业领袖等重要人士，旨在探讨重大议题、制定发展战略、促进交流合作。

会展和博览会

涵盖各个领域的展览会、贸易洽谈会、科技创新展等，是展示国家、地区产业实力、推动国际贸易、促进技术交流的重要平台。

赛事和盛会

包括体育赛事、文化艺术节庆、纪念活动等重要赛事活动，能够吸引大量国内外关注和参与，促进文化交流。

庆典和纪念活动

包括国庆阅兵、建党节庆祝、重要历史事件纪念等重要庆典及纪念活动，是彰显国家荣耀、传承历史文化、凝聚民心的重要方式。

国际合作与对话

涉及到国际重要议题、国际关系、全球治理等方面的高级别对话、峰会、会议等，展现国家外交实力和国际影响力。

伦敦奥运会期间网络安全事件

- 共发生**1.65亿次**网络攻击，产生**97次**严重的网络问题
- 开幕式当天奥运会场馆电力系统遭遇长达**40分钟**的大规模DDoS攻击

平昌冬奥会期间网络安全事件

- 开幕式期间网络屡次出现波动，甚至多次**直播画面中断**
- 奥运会**网站瘫痪数小时**，导致门票销售和下载被迫中断，部分观众无法打印门票进场

东京奥运会期间网络安全事件

- 奥组委计算机系统遭受勒索病毒攻击，导致**多台终端感染**
- 系统遭受多次网络攻击，造成门票购买者的登录ID和密码等**个人信息泄露**

俄罗斯世界杯期间网络安全事件

- 观众在使用场馆公共Wi-Fi时，**个人信息和账户遭到黑客窃取**
- 官方网站遭遇多次DDoS攻击，利用人们对赛事的兴趣通过钓鱼网站进行**欺诈活动**

重大活动期间发生网络安全攻击最直接的影响是造成活动中断、泄露个人隐私数据以及带来相应的经济损失等，此外，还会导致损害国家声誉、国家安全等间接影响。主要攻击方式包括网络钓鱼攻击、DDoS攻击、数据泄露、无线网络攻击、间谍软件/恶意软件攻击和漏洞利用攻击等。

网络钓鱼攻击

01

对活动参与者、赞助商或相关组织发送伪造电子邮件或消息，诱骗用户点击恶意链接或下载恶意附件，以**窃取资金、身份信息或其他重要数据**。

DDoS攻击

02

针对官方网站、在线投票系统等关键基础设施，通过大量合法的请求占用目标服务器的带宽或资源，**导致服务中断或性能下降**。

数据泄露

03

重大活动期间涉及大量的个人信息、交易数据和其他敏感信息，可能由于系统漏洞或外部攻击**导致个人隐私曝光、财务损失或声誉损害**。

无线网络攻击

04

通过破解无线密码、截取无线信号或进行中间人攻击，从而**窃取敏感信息或破坏无线网络连接**。

间谍软件/恶意软件攻击

05

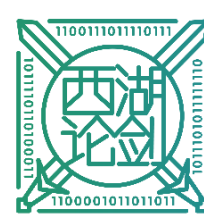
通过电子邮件附件、恶意广告等方式攻击活动的系统，**从而破坏系统或干扰活动的正常进行**。

漏洞利用攻击

06

利用配置漏洞、操作系统漏洞、协议漏洞和应用程序漏洞等进行攻击，从而**造成数据泄露、系统瘫痪、经济损失等**。

重大活动网络安全保障的困难与挑战



2024 WEST LAKE
DIGITAL SECURITY CONFERENCE
西湖论剑·数字安全大会

12th

智能安全X
乘数而上
INTELLIGENCE
ENHANCE SECURITY
ADVANCING
WITH DIGITALIZATION

重大活动IT系统的复杂性较高，这是由于活动规模、多样性以及对信息处理的高度需求。此外，由于重大活动开放的网络环境、广泛的社会关注，网络安全风险也与日俱增。重大活动所需的信息化设备多来自赞助捐赠等方式，缺乏有效、整体的网络安全防护方案，因此具有设备临时性、场馆基础设施薄弱、受网络攻击频发等特点。

重大活动IT系统的复杂性

多模块和多系统集成

01

重大活动IT系统常由多个模块和子系统组成，包括注册系统、安保系统、媒体系统等。这些系统需要高度集成，以确保协同工作并共享数据。

大规模的数据管理

02

由于活动涉及大量的参与者、交易和其他相关信息，IT系统需要处理大规模的数据。这包括注册信息、参与者数据、安全数据、票务数据等，需要高效的数据库管理和数据处理。

实时性和高可用性需求

03

重大活动通常需要实时的信息流，包括安全事件、日程变更、媒体报道等。因此，IT系统需要具备高可用性和实时性，以确保信息及时传递和处理。

多渠道信息流

04

信息可能来自多个渠道，包括政府部门、媒体、社交媒体、参与者等。系统需要能够整合并处理来自不同渠道的信息，以提供全面的情报。

高度的安全性和隐私保护

05

由于涉及政治、经济、安全等方面的敏感信息，重大活动的IT系统需要具备高度的安全性和隐私保护机制，以防止数据泄漏和未经授权的访问。

用户体验设计的复杂性

06

系统可能服务于不同的用户群体，包括政府官员、组织者、参与者和媒体。因此，系统设计需要考虑到各种用户需求，以确保良好的用户体验。

应急响应和灾备计划

07

由于活动的重要性，系统需要具备应对突发事件的能力，包括灾难恢复计划和应急响应机制。

重大活动网络安全保障难点

网络攻击的多样化

重大活动因其关注度高，影响力大，其信息化往往易成为攻击首要目标，攻击者可能包括反华势力、黑客组织、利益组织以及敌对国家组织等。这些攻击组织根据不同的动机和目的，将使用特定的网络攻击，同时随着网络生态的发展，新的攻击方式也在不断涌现，网络攻击方式呈现多样化和复杂化趋势。



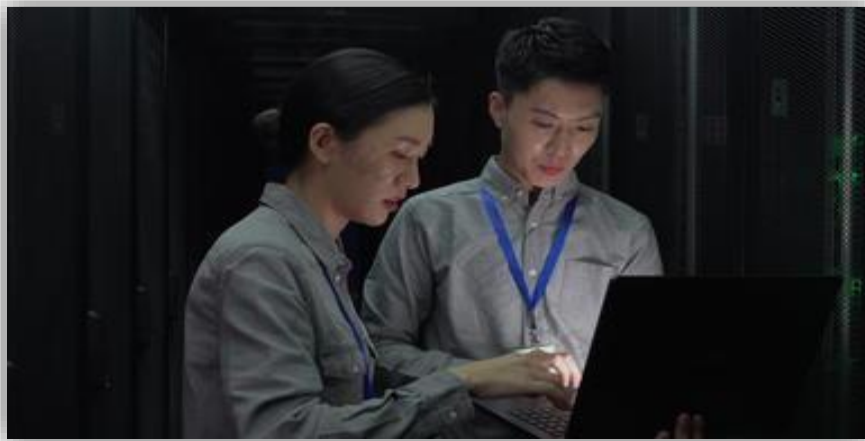
新技术的广泛应用

随着新技术的不断发展，如：物联网、人工智能(AI)、5G、大数据等，在重大活动中也得到广泛应用，这些新技术在给重大活动带来便利的同时，也可能引入新的安全风险，成为攻击者的窗口。



人员安全意识不足

通常重大活动人员涉及活动组织方、工作人员、供应商、志愿者、参会人员等，由于人员的复杂性，安全意识水平也可能存在不足，这些不足往往易遭受社会工程学手段攻击，如钓鱼攻击、电话诈骗，诱使泄露敏感信息或进行敏感操作，从而间接影响活动。



重大活动数据安全

重大活动信息化存储着大量的敏感数据，如：会议类参会领导人身份信息、体育赛事中的运动员身份信息、成绩数据。这些数据具有极高的价值，因此也容易成为攻击的重点，一旦发生数据泄露，将直接影响活动运行。



场馆基础设施脆弱

重大活动场馆主要以复用场馆为主，这些复用场馆基础设施可能未及时更新安全措施，存在安全漏洞和脆弱性，如网络设备、监控系统、门禁系统等，这些脆弱性可能被攻击者利用进行入侵和破坏。从而干扰活动举办。




供应链安全攻击

重大活动通常会招募合作伙伴或依赖于第三方服务提供商，例如网络服务提供商、云服务提供商、票务系统提供商等，攻击者可能通过恶意软件、社会工程学等手段渗透到这些提供服务的供应链当中，从而通过影响重大活动的关键供应商和合作伙伴，实现对活动的破坏和干扰。




重大活动网络安全保障要规划设计一套可实施性强、覆盖面广的网络安全保障方案，来确保重大活动顺利进行、防范网络安全风险。需要设置保障重大活动网络安全的组织架构，完善重大活动网络安全管理制度，建立重大活动的网络安全技术保障体系，提供全流程的网络安全保障服务，构建事前、事中、事后的多层次、全方位重大活动安全保障体系。



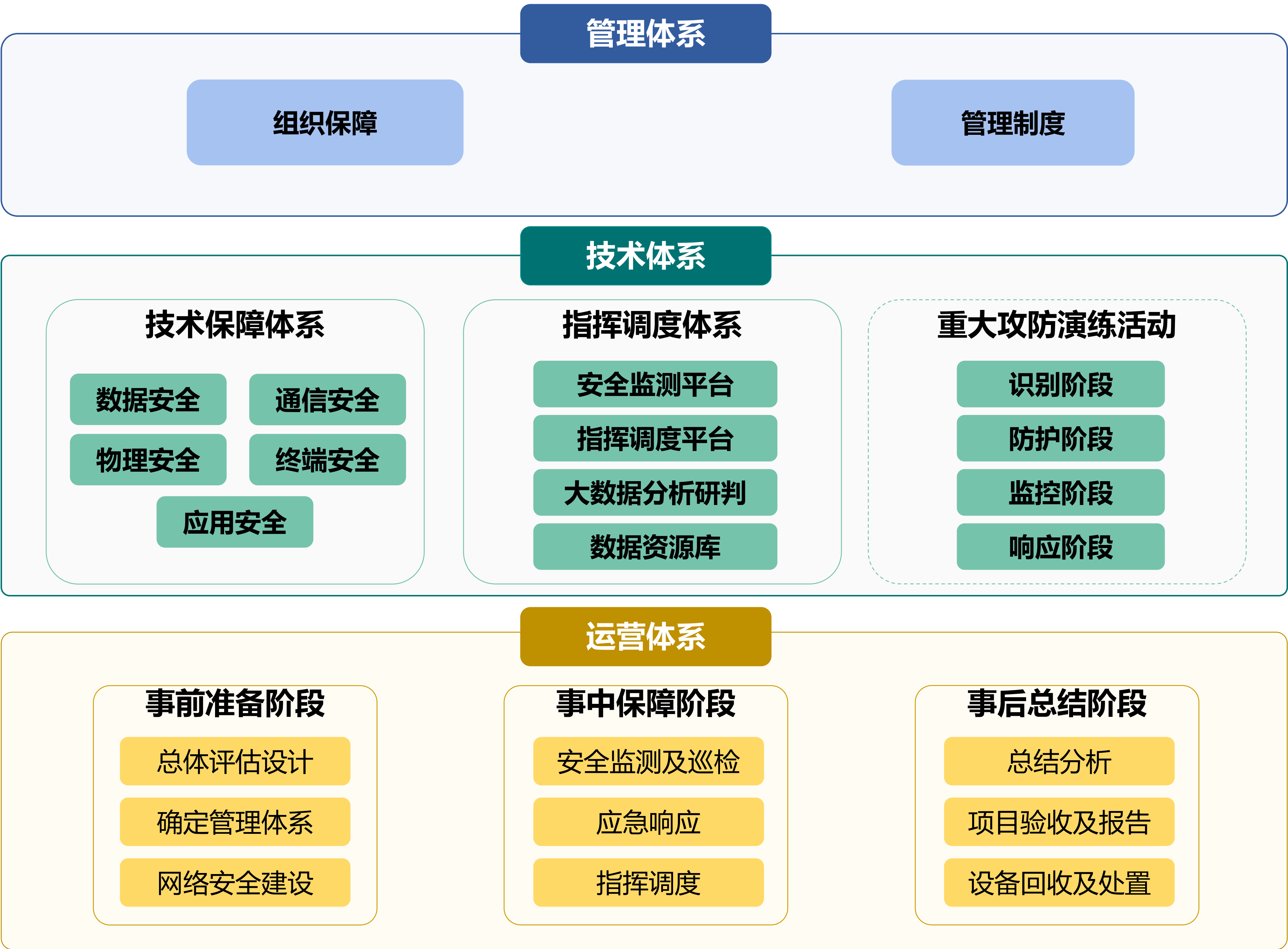
保障目标

- 保障系统稳定性和可用性
- 防御网络攻击
- 保护敏感数据安全
- 处理安全事件和应急响应
- 合规性和法律监管



保障原则

- 确保设计依据完整
- 设计原则切实有效
- 设计思路全面可行
- 方案框架结构完整
- 任务明确具体



01.管理体系

组织保障要设立权责对等的组织架构，由网络安全领导小组统筹整个重大活动过程中的网络安全保障工作。制度建设则制定实现重大活动网络安全保障的各项管理及工作制度。

02.技术体系

主要以重大活动活动前防护保障和检测监控、活动中态势感知、活动后应急溯源为基本框架思路，来构建网络安全总体防护能力。

03.运营体系

活动前以资产安全评估加固为主入手；活动中提供安全值守服务，通过态势感知平台进行威胁监测展示，及时处置安全风险；活动后进行长期防护优化及安全意识培训。



02

重大活动网络安全保障体系建设

网络安全保障是一项庞大且复杂的系统工程，须秉持整体与全局的安全观念来组织管理。统筹组织能力决定了网络安全团队在面对复杂安全威胁时，能否有效地协调各方资源、令各个安全要素形成合力，共同抵御网络攻击。在重大活动网络安全组织保障工作中，需要成立网络安全领导小组、网络安全决策小组以及网络安全工作小组，各小组协同工作，确保重大活动中网络安全保障工作的顺利进行。



网络安全领导小组

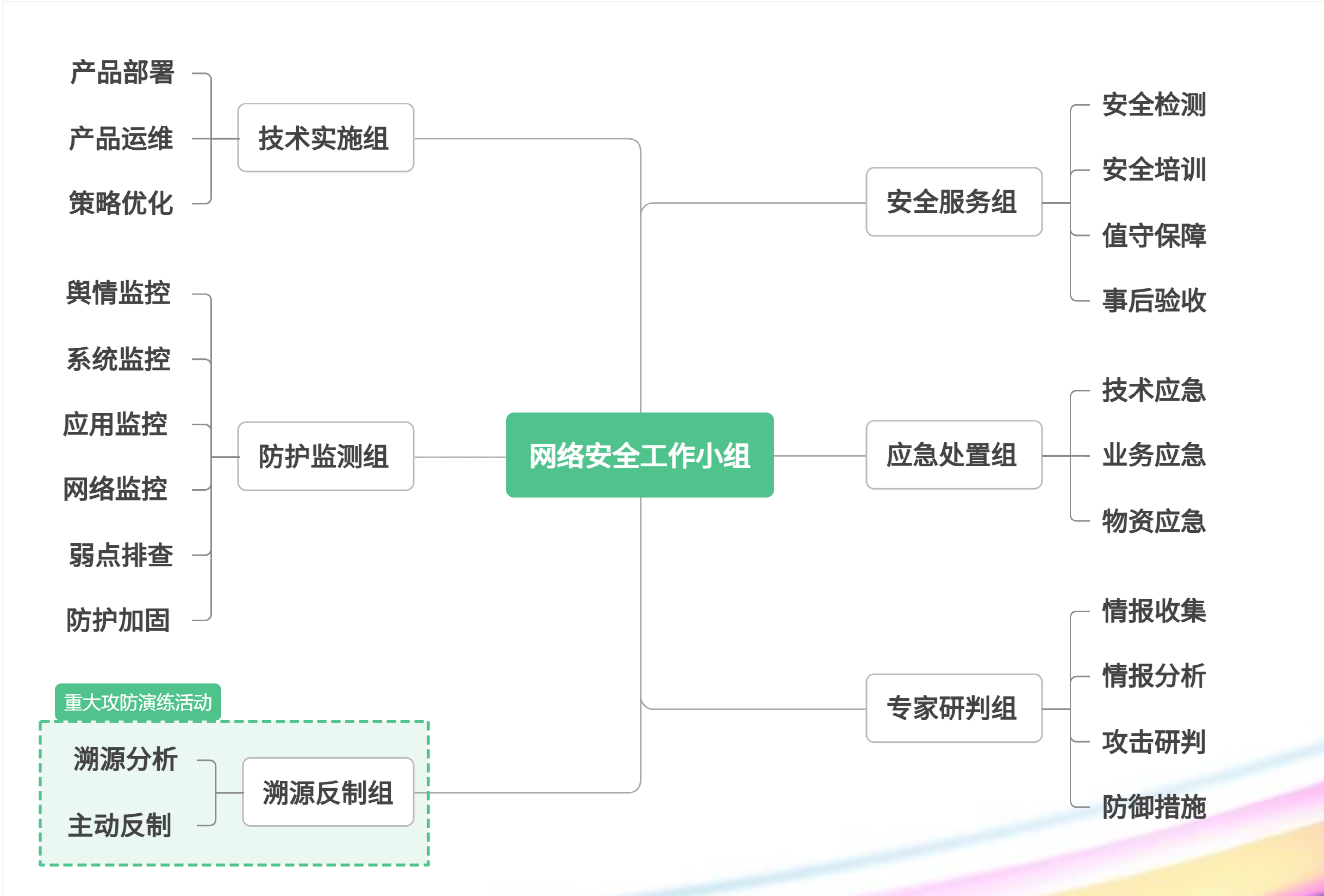
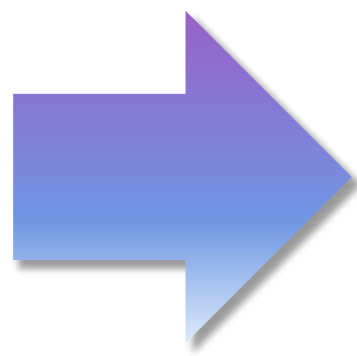
负责贯彻落实重大活动期间网络安全保障要求，领导、指挥并协调重大活动期间网络安全保障工作的开展，决策重大网络安全事件的应急处置，向上级主管部门上报重大网络安全事件发展以及应急处置情况。

网络安全决策小组

负责执行和落实网络安全领导小组下达的工作任务，组织协调网络安全事件的应急处置，确保各专业组间的顺畅沟通，并定期向网络安全领导小组汇报网络安全事件及应急处置情况。

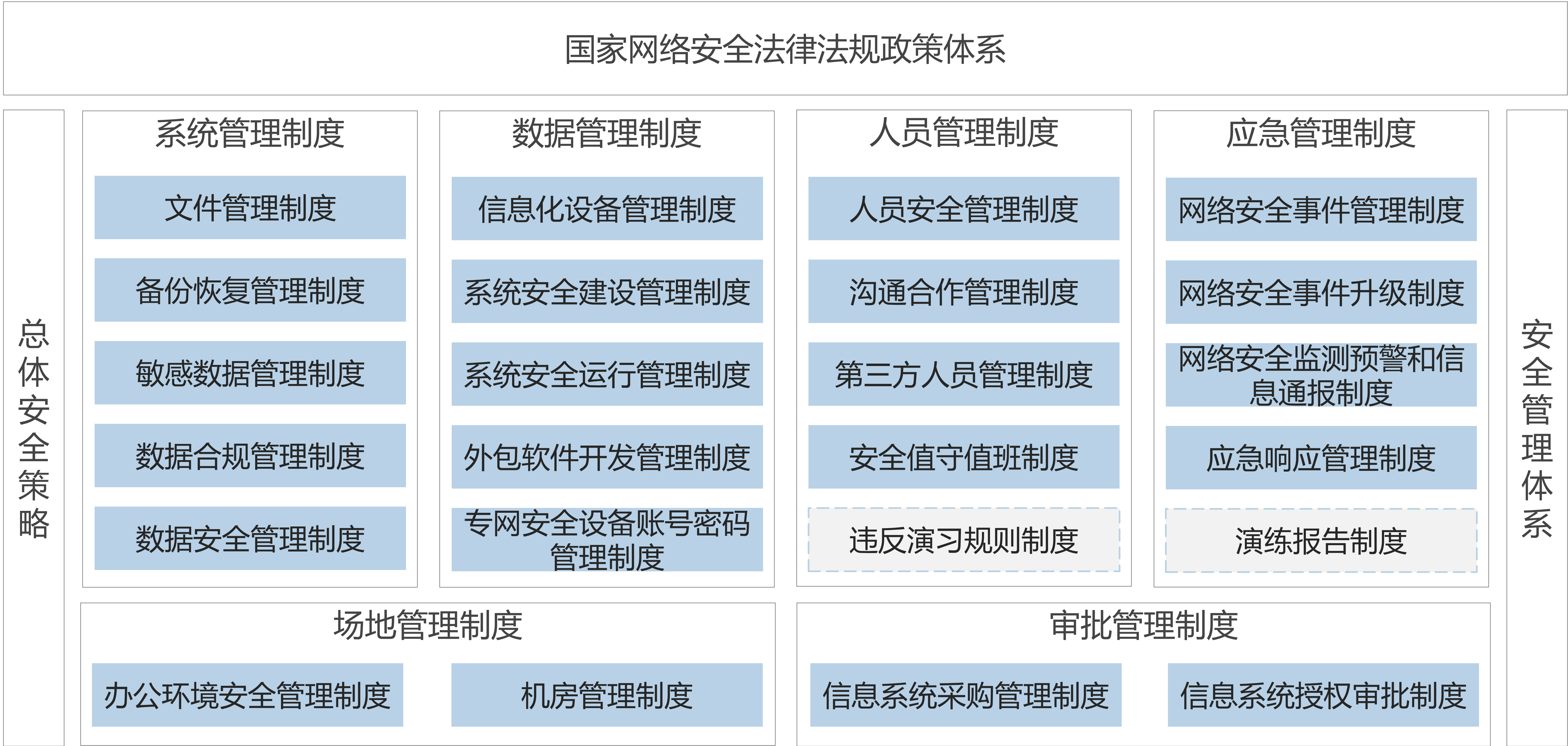
网络安全工作小组

负责重要活动期间的网络安全工作具体执行，并定期向网络安全决策小组汇报网络安全工作内容。各专业组设置如右图所示：



资料来源：赛迪顾问整理，2024.03

为确保重大活动网络安全保障工作有序展开，应构建完善的安全管理体系并明确总体安全策略。遵循国家网络安全法律法规政策体系，紧密结合重大活动的网络安全工作目标，制定全面的网络安全管理制度。



扩展安全防护能力

提升应急响应能力

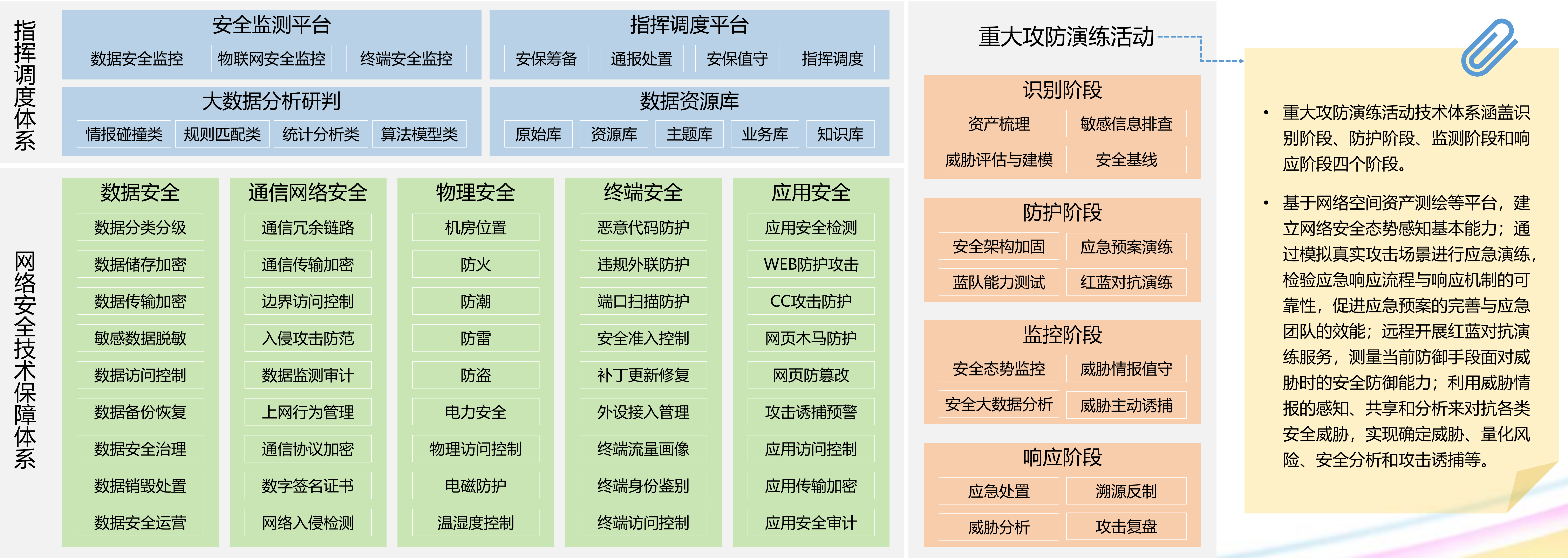
加强安全监管能力

图例

重大活动制度

重大攻防演练活动制度

重大活动的网络安全体系设计，以覆盖“一平台、两张网（活动专网、管理专网）、多应用”的框架构建网络安全总体防护能力，以重大活动的活动前防护保障和检测监控、活动中态势感知、活动后应急溯源为基本框架思路，建立重大活动的网络安全技术保障体系、网络安全指挥调度体系，实现事前、事中、事后全方位、立体性的安全保障体系。



现代重大活动的场所化运行特点让网络安全保障工作呈现出典型的“一个中心、多点接入”的架构，重大活动网络安全运营保障工作也表现出全生命周期性，具有动态变化和挑战等特点。重大活动网络安全运营保障工作涵盖“事前准备、事中保障、事后总结”三个阶段，每个阶段都有明确的目标和任务。通过对不同阶段进行划分，明晰不同阶段、时间的工作重点，制定好工作计划和工作预期来统筹管理重大活动的网络安全运营保障工作。



重大攻防演练活动网络安全保障体系——运营建设



2024 WEST LAKE
DIGITAL SECURITY CONFERENCE
西湖论剑·数字安全大会

12th

智绘安全X
INTELLIGENCE
ENHANCE SECURITY
ADVANCING
WITH DIGITALIZATION
乘数而上

重大攻防演练活动是一项系统性、综合性任务，每个阶段都包含一系列关键工作流程和要素。其中，事前准备阶段通过资产梳理、暴露面收敛、安全检测加固以及联合演练等一系列流程，为演练活动的顺利开展奠定坚实的安全基础；事中保障阶段则注重现场监测值守与快速响应，强调对安全事件的及时处理和有效指挥调度；事后总结阶段则是对整个攻防演练过程的回顾总结与整改提升。

资产梳理

- 关联域名
- 资产指纹
- 开放端口
- 敏感信息等

暴露面收敛

- 端口扫描
- 指纹识别
- 网络边界检查
- 服务器核查等

隐患排查

- 漏洞扫描
- 渗透测试
- 基线检查
- 攻击路径分析
- 敏感信息排查等

安全加固

- 补丁更新
- 代码修复
- 病毒查杀
- 数据备份等

安全预警

- 失陷事件
- 0day/Nday漏洞等

分析研判

- ATT&CK 框架
- 机器学习
- 多维度关联分析等

监测值守

- 异常流量
- 恶意文件
- 木马远控
- 弱口令
- 漏洞利用攻击等

响应处置

- 应急响应计划
- 备份恢复计划等

溯源反制

- 攻击者源IP地址
- 攻击服务器IP地址
- 邮件地址等

复盘总结

- 攻击方复盘总结
- 防守方复盘总结

整改提升

- 技术总结整改
- 流程总结整改
- 人员总结整改

重大攻防演练活动安全加固工作清单

分类	工作项	工作内容
服务器操作系统安全加固	系统补丁更新	将服务器系统重要补丁升级至最新。
	服务器端口核查	清理服务器开放端口,关闭非不要端口。
	服务器日志审计	开启服务器日志审计, 包括保存本地日志同时发送到日志审计服务器, 日志留存时间不小于6个月。
	服务病毒查杀	对服务器进行一次全面杀毒查杀。
	WEB应用层防护	web应用服务器前端应部署应用防火墙 (WAF) 。
	安全策略梳理	梳理服务器安全策略包括但不限于密码策略、登录策略、防火墙策略等。
网络与安全设备加固	梳理操作系统账号	清除非必要的管理员账号, 更改后的口令必须符合安全基线中对于口令强度的要求。
	账号与弱口令核查	清除非必要账号, 开展弱口令扫描。
	非必要服务关闭	关闭路由器交换机WEB管理、智能安装页面。
	安全基线配置	1.禁用Telnet进行远程管理。 2.SNMP只允许网管系统、公司网管、安全检查项目组的设备只读配置。 3.检查管理员账号和权限, 关闭不必要的账号和不合理的账号权限,保证密码强度符合安全基线要求。 4.限制可以远程管理的IP地址。
	网络设备日志审计	开启日志审计, 包括保存本地日志同时发送到日志审计服务器, 日志留存时间不小于6个月。
	安全策略梳理	检查所有网络设备及安全设备的策略,删除无用策略, 保证安全防护策略有效且处于使用状态。
数据库安全加固	配置备份	所有网络设备及安全设备全部要做好配置备份, 确认备份有效可以恢复。
	补丁更新	将数据库系统重要补丁升级至最新。
	数据备份	做好数据备份,确认备份有效可以恢复。
	数据库权限梳理	以最低权限的原则梳理数据库访问权限。
	访问策略管理	通过操作系统防火墙和数据库配置限制数据库管理员账号可登陆的IP地址。
	禁用函数	在数据库中禁用可以执行系统命令的函数(如MySQL数据库的system函数SQL Server数据库的xp_cmdshell函数等)。
中间件安全加固	安全策略梳理	开展数据库安全策略梳理。
	默认配置修改	中间件后台默认路径修改、中间件默认端口修改、中间件默认账号口令修改。
	口令权限加固	删除控制台存在默认的账号密码、删除无用账户、禁止管理员权限运行中间件。
	补丁增补	中间件已知漏洞补丁增补, 增补不了的关停或人员重点监测。
	敏感信息泄露加固	自定义每个站点的404、403和500错误页面信息。
	脚本映射关闭	删除不必要的脚本映射。
互联网安全加固	目录加固	各站点的目录部署应用分区;各站点的目录配置严格权限。
	日志开启	中间件日志存放在数据分区。
	账号安全	配置帐户锁定时间和会话超时时间。
	删除多余的测试账号。	
	账号安全	同一用户会话限制在两台机器上用同一个账号进行登录;启用超时帐户自动退出。
	上传限制	限制上传类型和上传文件大小。
互联网安全加固	数据传输加密	登录密码在传输中加密, 应用系统密码是采用密文的方式存储在数据库中。
	WEB应用层防护	web应用服务器前端应部署应用防火墙 (WAF) 。

资料来源：赛迪顾问整理，2024.03

资料来源：赛迪顾问整理，2024.03



03

建议及展望

随着云计算、人工智能等新技术的不断发展与加深应用，网络安全面临的威胁与挑战也更加的复杂化。未来，重大活动网络安全保障将朝着智能化、多维度、协同化和个性化的方向发展，我们应当利用新技术和新理念不断提升网络安全保障水平，确保重大活动中网络系统的稳定性、安全性和可用性。





2024 WEST LAKE
DIGITAL SECURITY CONFERENCE
西湖论剑·数字安全大会

12th

智绘安全X
INTELLIGENCE
ENHANCE SECURITY
ADVANCING
WITH DIGITALIZATION
乘数而上

谢谢

