CCID 赛迪顾问

股票代码：HK02176

思 维 创 造 世 界

安恒信息

DAS-security 安全中国

西湖论剑
重磅战略成果
年度巨献

2024
重大活动网络安全保障建设及运营指南

DAS

参编单位

赛迪顾问股份有限公司

杭州安恒信息技术股份有限公司

前言

在当今高度数字化的社会中，各类重大活动如会议、展览、赛事及庆典等正面临着日益复杂和严峻的网络安全威胁。这些威胁不限于网络入侵或数据泄露，更涉及到对基础设施、关键信息系统和公众舆论的复杂攻击，需要国际社会的密切合作和长期关注。因此，为确保重大活动期间互联网相关服务的安全稳定运行，需积极开展网络安全保障的建设与运营工作。

重大活动网络安全保障工作需规划一套可实施性强、覆盖面广的保障方案。以实现重大活动网络安全“零事故”为目标，从重大活动的事前、事中、事后提供全方面、针对性的安全服务，帮助相关单位有效开展安全工作，顺利完成保障任务。其中，事前准备阶段主要是开展网络安全设计建设、安全加固、安全意识培训以及联合演练等工作。对涉及到的关键基础设施和重要网络设施等相关系统进行梳理，通过漏洞扫描、渗透测试等方式全面开展风险评估与自查整改工作，并基于评估结果部署相应的安全技术和设备。同时，通过安全意识培训和联合演练，检验保障方案是否切实可行并提高参与人员的安全处置能力。事中保障阶段是网络安全保障工作中的核心，主要开展网络检测与分析、事件应急处置、攻击溯源反制等工作。利用安全防护设备进行全流量监测和关联分析，准确甄别失陷事件，锁定攻击者并第一时间进行阻断，对攻击事件进行研判分析及验证，评估事件是否具有针对性、共性、以及是否可能引发全局性同步网络攻击等。总结阶段是对活动中所发生过的攻击事件进行复盘并形成报告。针对保障过程中系统的脆弱点开展整改工作，进一步提高目标系统的安全防护能力。同时，对网络安全数据进行整理和归档，为今后识别攻击者奠定基础。

《 重大活动网络安全保障建设及运营指南 》是业内第一份面向重大活动全方位技术建设与运营指导的权威性指南，充分且全面地考虑了重大活动可能面临的安全风险挑战。《 指南 》从设计理念、架构搭建等方面详实、系统地梳理了重大活动网络安全保障的建设与运营思路，围绕组织架构的搭建、管理制度的完善、技术保障体系的建立以及运营流程的规划等方面设计了一套全方位、立体的网络安全保障方案，为用户在重大活动网络安全保障时提供全面有效的实战型指导。在当今高度数字化的社会中，重大活动网络安全保障的重要性日益凸显，希望本指南的发布能够进一步推动重大活动网络安全保障工作的深入发展，为未来的重大活动的顺利举办注入更多的科技与安全力量。

《重大活动网络安全建设及运营指南》
构筑数字时代的安全堡垒

在全球数字化的今天，重大活动如国际峰会、体育赛事、以及各类大型攻防演练等，不仅是展示国家形象的窗口，也是网络安全风险的集中体现。**《重大活动网络安全建设及运营指南》**，为我们提供了一套系统全面的网络安全解决方案，它从重大活动的事前、事中、事后提供全方面、有针对性的安全服务，帮助相关单位有效开展安全工作，顺利完成保障任务，是一份保障国家利益和公共安全的重要参考。

本指南总结国内外重要会议活动保障经验，覆盖了从前期网络安全设计建设，到事中开展各类检测分析、响应处置等工作，再到事后对所发生的攻击事件进行完整复盘并形成总结报告的全流程，为重大活动网络安全保障工作提供了一份具有高水平、实战性、高价值的工作指南，帮助组织者快速构建起有效的网络安全防护体系。

而随着技术的快速衍进与迭代，网络安全威胁也在以新形态出现。本指南不仅关注当前安全挑战，更预见未来趋势，提出加强智能化安全防护手段应用等，实现多维度、长周期的安全保障。

本指南对于政府机构、有重大活动应急保障需求的各类单位组织者、IT专业人士以及所有关注网络安全的人士而言，是一份不可多得的宝贵资源。它不仅增强了我们在智能时代对网络安全重要性的新认识，更为我们提供了实现安全目标的明确路径。

宋皆荣

浙江省网络空间安全协会理事长

浙江省网络社会组织联合会副会长

浙江省委网信办原副巡视员

目录

CONTENTS

随着经济社会的快速发展，具有国际、国家或区域性重大影响的重大活动日益增多。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，会导致重大活动无法正常如期举行和顺利开展。

因此，为确保重大活动期间的互联网相关服务不被攻击和破坏，需开展网络安全保障建设及运营，从重大活动的事前、事中、事后提供全方面、针对性的安全服务，帮助相关单位有效开展安全工作，顺利完成安全保障任务。

重大活动的定义及特点

重大活动的定义

重大活动一般是指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会议、会展、赛事、纪念、庆典等大型活动。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，提升国家形象、增进民族团结、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。

除此之外，从网络安全角度来看，这些年国家及重点行业推动的重大攻防演练活动也具备重大活动的特点，也是应当重点关注的活动对象。**重大攻防演练活动**一般指的是由国家或行业主管机构组织的，集结攻防双方，以不限制手段、路径，进行获取权限并攻陷指定网络靶机为目的实战攻防演练。攻防演练的主要目标涵盖国家重要行业的关键信息基础设施，主要目的是通过真实网络中的攻防演练，全面评估目标所在网络的整体安全防护能力，检验防守方安全监测、防护和应急响应机制及措施的有效性，锻炼应急响应队伍提升安全事件处置的能力。

重大活动的举办有助于推动国家发展、增进民族团结、提升国际地位，是国家治理和外交工作的重要组成部分。因此，为保障国家、地方重大活动的顺利举行，针对可能存在的风险和影响，必须参照有关法律、法规采取预防性、临时性专项管理措施。

重大活动的特点

重大活动的举办往往需要大量的组织筹备工作、资源投入和宣传推广，对于各级政府、主办单位以及参与者都具有重要意义。重大活动通常具有以下几个特点：

高度的关注和影响力

重大活动往往能够吸引大量的关注和参与，无论是媒体报道、社会关注还是政府官员的重视程度，都可能会在全球或全国范围内产生广泛的影响。

政治意义和象征性

重大活动往往具有政治象征意义，可能与国家的政治方向、发展战略或领导人形象等相关联，可能会被用作政治宣传、国家形象展示的重要平台。

活动具有临时性

重大活动通常是在特定的时间段内举办，临时搭建场地，临时组织专门的组织机构或工作团队，参与活动的人员通常也是临时性的，当活动结束后相关场地、组织与参与人员均会被拆除或解散。

IT系统复杂度高

重大活动的IT系统复杂性通常较高，系统包含多个模块和子系统，需要处理大规模的数据，需要收集多渠道且实时的信息流等，需要在设计、开发和实施过程中充分考虑众多复杂因素，以确保系统的稳定性、安全性和有效性。

业务稳定性和安全性要求高

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，以防止网络攻击、数据泄漏等，保持活动业务的稳定性。

当前，重大会议论坛、赛事庆典等活动的数字化程度较高，以大数据、云计算、人工智能等为代表的新兴技术在重大活动中的应用愈加成熟。面向社会大众群体获取信息的途径也逐渐便捷，各类显示屏、App等载体应用的普及度迅速提升。智慧场馆、智慧交通、智慧餐饮等社会行业载体全面赋能重大活动，重大活动网络安全风险敞口变大，保障难度立方式增加。对于重大活动整体网络安全保障体系建设、统筹协调指挥、网络风险排查、网络安全保障队伍建设、网络安全事件应急处置，均提出较大挑战。因此，本章全面、客观、清晰的梳理了重大活动过程中可能面临的网络安全威胁挑战，能够帮助活动组织者预先识别风险，进而开展有针对性地处置措施来降低风险的可能性、减小后果的风险程度。

重大活动
网络安全威胁态势

重大活动网络安全威胁

在当今高度数字化的社会中，重大活动如会议会展、赛事庆典等面临着日益复杂和严峻的网络安全威胁。网络攻击者越来越善于利用先进的技术和策略，试图干扰、破坏或操纵这些活动，对社会稳定和公共信任造成重大威胁。这些威胁不仅仅是简单的网络入侵或数据泄露，还包括针对基础设施、关键信息系统和公众舆论的复杂攻击。当前，重大活动的网络安全攻击事件已经成为全球性挑战，需要国际社会的密切合作和持续关注来应对日益增长的威胁。过去十几年中，发生在重大活动期间的网络安全攻击事件有些并没有被大面积报道，但是有些事件也是引发广泛关注并造成重大后果的，以下列举一些重要事件。

2012年伦敦奥运会期间网络安全事件：共发生1.65亿次网络攻击，其中产生了97次严重的网络问题，必须交由技术运营中心进行紧急应对。开幕式之前就发现有黑客组织对奥运会IT基础架构进行了约10分钟的漏洞扫描；开幕式当天奥运会场馆的电力系统遭遇长达40分钟的大规模DDoS攻击；此外，假冒网站、钓鱼链接、电信诈骗团伙更是不计其数。

2016年里约奥运会期间网络安全事件：虽然有2014年巴西世界杯的经验教训，对本次网络系统进行了严密监控，但依然出现了许多低级别的网络安全事件。比如多次遭受黑客攻击造成官方网站损毁；当地官方和奥组委信息发生数据泄露事件；当地官方和奥林匹克赞助商网站遭遇DDoS攻击，峰值达到300-500Gbps。

2018年平昌冬奥会期间网络安全事件：开幕式之前，网络安全部门工作人员就发现大批黑客盯上了这届冬奥会，奥组委各部门也遇到各种恶意钓鱼网站；开幕式期间，网络屡次出现波动，甚至多次信号中断，导致直播画面多次中断；此外，由于黑客攻击，奥运会网站还瘫痪数小时，这不仅导致门票销售和下载被迫中断，还导致一些观众无法打印门票，最终导致很多观众无法进场观看赛事。

2018年俄罗斯世界杯期间网络安全事件：针对世界杯官方网站或赞助商网站的DDoS攻击，以及钓鱼网站和恶意软件攻击，试图利用人们对赛事的兴趣进行欺诈活动；此外，也有一些球迷在使用公共Wi-Fi时，个人信息和账户遭到黑客窃取。

2020年东京奥运会期间网络安全事件：在东京奥运会延期举办前，东京奥组委及其合作伙伴就曾遭受过网络攻击和网络钓鱼攻击，虽然没造成严重损失，但引发了广泛关注；在东京奥运会举办期间，东京奥组委的计算机系统遭受勒索病毒攻击，导致多台终端感染；此外，还遭受了多次网络攻击，包括门票购买者的登录ID和密码等个人信息在互联网上被泄露。

世博会期间网络安全事件：上海世博会期间曾监测到假冒世博会寄出的电子邮件中含有恶意程序，利用Adobe Acrobat and Reader已知的软件缺陷夹带名为TROJ_PIDIEF.ACV.的恶意程序来发动进攻。

重要经济论坛期间网络安全事件：世界经济论坛等经济类重大活动期间，也曾发生过网络安全事件。例如，2015年达沃斯世界经济论坛期间，一些参会者的个人信息和行程安排被黑客窃取并在网上出售。

重大活动网络安全攻击意图及手段

攻击意图

攻击者发起重大活动网络安全攻击的目的主要包括经济意图和政治意图。经济意图方面，攻击者通过非法赌博、活动操纵或勒索等来获取金钱。比如，利用内幕信息赚取大额赌注或者窃取体育赛事敏感信息以勒索体育组织机构；攻击者受悬赏刺激，使用暗网形成交易链，接受悬赏任务，对重要会议、赛事庆典等实施精准攻击，达到利益最大化。政治意图方面，攻击者利用重要会议会展活动以及重大比赛庆典活动等作为政治宣传的平台，试图损害活动举办国家或政府的形象，干扰重大活动的顺利举行。此外，攻击者还会出于好奇心或技术挑战进行黑客活动，试图通过攻击重大活动来获取名誉和声誉，以提高其社会地位或吸引更多关注。无论是上述哪种意图，攻击者的最终目的都是通过攻击有影响力的重大活动来干扰其正常运行，从中牟取经济利益或达到其政治企图。

攻击方式

重大活动期间发生网络攻击的主要攻击方式包括网络钓鱼攻击、DDoS攻击、数据泄露、间谍软件/恶意软件攻击、无线网络攻击和漏洞利用攻击等。

网络钓鱼攻击

这种攻击方式通常通过发送伪造的电子邮件或消息，诱骗用户点击恶意链接或下载恶意附件，从而获取用户的敏感信息或执行恶意代码。在重大活动期间，网络钓鱼攻击可能会针对活动参与者、赞助商或相关组织进行，以窃取资金、身份信息或其他重要数据。

DDoS攻击

分布式拒绝服务（DDoS）攻击是一种通过大量合法的请求占用目标服务器的带宽或资源，使其无法处理正常请求的攻击方式。在重大活动期间，DDoS攻击可能会被用来针对官方网站、在线投票系统或其他关键基础设施，导致服务中断或性能下降。

数据泄露

由于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，数据泄露的风险也会相应增加。数据泄露可能是由于内部人员疏忽、系统漏洞或外部攻击导致的，一旦泄露可能会导致个人隐私曝光、财务损失或声誉损害。

间谍软件/恶意软件攻击

间谍软件/恶意软件可能会被用来窃取敏感信息、破坏系统或干扰活动的正常进行。这些软件可能会通过电子邮件附件、恶意广告或其他途径传播，一旦感染，可能会对活动参与者或相关组织的计算机系统造成损害。

无线网络攻击

在重大活动期间，无线网络可能会被广泛使用，但同时也面临着被攻击的风险。黑客可能会尝试破解无线密码、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网络连接。

漏洞利用攻击

漏洞利用攻击主要通过利用配置漏洞、操作系统漏洞、服务漏洞、协议漏洞和应用程序漏洞等进行攻击，对重大活动的影响包括但不限于数据泄露、系统瘫痪、经济损失等。

影响分析

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。

影响活动正常进行

网络安全攻击可能导致活动网站或系统瘫痪，使活动参与者无法正常访问或使用相关服务。例如，DDoS攻击可以通过大量请求拥塞服务器带宽，导致网站无法访问，从而影响活动的正常进行。

损害品牌形象和声誉

网络安全事件可能导致活动组织者的品牌形象和声誉受到损害。一旦发生数据泄露、恶意攻击等事件，公众对活动组织者的信任度可能会下降，进而影响其未来的业务发展和合作伙伴关系。此外，攻击事件可能会受到媒体的广泛报道，从而进一步损害其声誉。

造成经济损失

网络安全攻击可能导致活动组织者面临经济损失。例如，数据泄露可能导致需要支付高额的赔偿金，而系统修复和恢复也可能需要大量的资金投入。此外，由网络安全事件导致的业务中断也可能造成收入损失。

泄露敏感信息

网络安全攻击往往伴随着敏感信息的泄露风险。这些信息可能包括个人信息、交易数据、商业机密等，一旦被泄露，可能会对活动参与者、赞助商或相关组织的隐私和利益造成损害。

影响公众信任和参与度

网络安全事件可能导致公众对活动的信任度下降，从而影响其参与度和积极性。如果公众认为活动存在安全隐患或个人信息可能被盗取，他们可能会选择不参与或避免使用相关服务。

国家安全和政治影响

如果攻击事件与国家安全或政治事件相关联，它可能对国家的安全产生严重影响。这可能会引发政府的回应，包括对攻击者的起诉、制定新的网络安全政策或进行网络战略调整。此外，攻击事件可能会影响国际关系，导致不信任和紧张局势的加剧。

法律责任和合规风险

在发生重大网络安全事件时，活动组织者可能面临法律责任和合规风险。例如，他们可能需要遵守相关法律法规，对事件进行报告和调查，并可能需要承担因未能保护用户数据而产生的法律后果。

当前，网络安全事件频发，来自互联网的黑客攻击持续不断，内部人员和第三方人员的威胁也存在挑战，多元化的网络安全威胁对重大活动的安全保障带来巨大的挑战。《国家网络安全事件应急预案》明确提出“国家重要活动、会议期间要加强网络安全事件的防范和应急响应，确保网络安全。加强网络安全监测和分析研判，及时预警可能造成重大影响的风险和隐患，重点部门、重点岗位保持24小时值班，及时发现和处置网络安全事件隐患”。因此，需要依据各种重大活动的具体情形制定一整套完整的重大活动网络安全保障方案。

重大活动网络安全保障体系建设思路

保障目标及对象

重大活动网络安全保障的目标是保障重大活动中涉及的IT系统的稳定性、安全性和可用性，以防止各种网络威胁对活动的影响。保障工作主要是确保在活动期间，保障目标的安全稳定运行，及时发现并消除系统的高危安全隐患，降低安全事件发生的可能性，高质量完成网络安全重保工作任务。

保障的重点对象包括包括服务器、路由器、交换机等网络设备， IT信息系统的各个组成部分，还要确保数据在传输和存储过程中的安全性，包括加密传输、数据备份等措施。

重大活动网络安全保障面临的挑战

重大活动IT系统的复杂性

随着信息技术的广泛深入应用，重大庆典活动、赛事、政务活动等各类重大活动越来越高度依赖于信息技术。而重大活动的IT系统复杂性通常较高，这主要是由于活动的规模、多样性以及对信息处理的高度需求，这就要求活动组织方在设计、开发和实施过程中充分考虑IT系统的复杂性，以确保系统的稳定性、安全性和有效性。

多模块和多系统集成

重大活动的IT系统通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。这些系统需要高度的集成，以确保它们协同工作并共享数据。

大规模的数据管理

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

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

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

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

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

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紧急响应机制。

重大活动网络安全保障的难点

在保障活动正常运行的同时，由于其开放的网络环境、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，缺乏有效的、整体的网络安全防护方案，因此具有设备临时性、受网络攻击频发等特点，从而导致高开放性、低集成性的特点以及高可用性的需求。

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体系设计思路

重大活动安全保障体系的目标

重大活动网络安全保障方案设计能力是指导和引领整个保障工作的顶层设计，是网络安全保障任务成果完成的基础。以实现重大活动网络安全“零事故”为目标，用顶层设计来指导安全风险防范和应急处置工作，保障系统网络安全稳定运行。

保障系统稳定性和可用性。重大活动的网络系统需要保证在活动期间始终稳定运行，以防止因为网络故障或攻击而导致的服务中断。

防御网络攻击。建立完善的安全防护系统来防御来自各种渠道的网络攻击。

保护敏感数据安全。采取措施确保重大活动的网络系统中的大量敏感数据的安全性，如个人信息、财务数据等。

处理安全事件和应急响应。建立健全的安全事件响应机制，及时应对各种安全威胁，降低损失。

合规性和法律监管。网络安全保障措施符合相关法律法规的要求，同时积极配合监管机构进行安全审查和监督，以确保网络安全保障工作的合规性和有效性。

重大活动安全保障设计原则

重大活动安全保障体系建设从系统建设开始，同步规划、同步建设、同步运营，提供可操作的安全指导，协助构建安全保障基础。主要的设计原则如下：

确保设计依据完整。网络安全保障方案设计需要符合国家相关网络安全政策和要求，参考并依据国际网络安全相关标准，确保重大活动网络安全保障方案遵循国家法律、符合国家政策，适应国际相关标准。

设计原则切实有效。为实现重大活动网络安全保障服务项目的总体目标，结合信息安全体系建设的实际情况和需求。

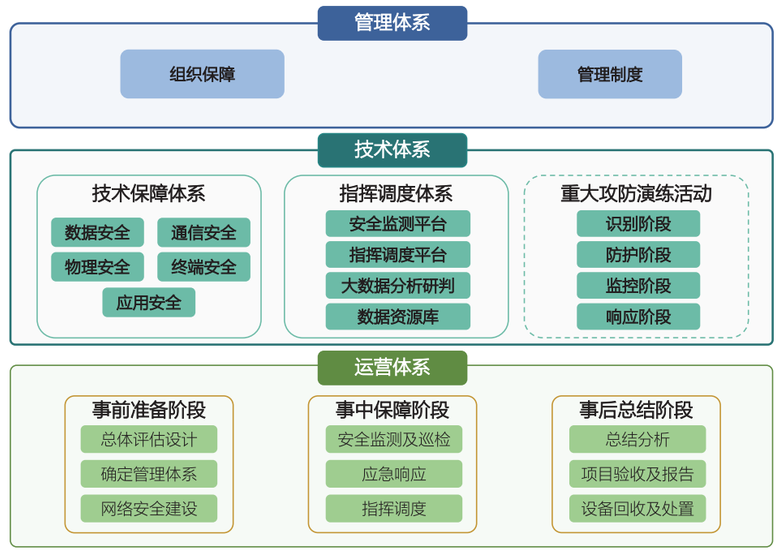
设计思路全面可行。遵循“总体设计、分步实施”原则，根据重大活动特征，分析网络安全风险点，确定适用性强、操控性强、创新性强的技术路线，保证保障对象、保障地点、指挥架构、保障内容等全面可行。

方案框架结构完整。整体工作方案框架结构完整，包括重大活动安全管理体系、重大活动安全技术保障体系和重大活动安全运营保障体系三大体系。

任务明确具体。方案中要明确不同组织的分工和具体工作任务，对于事前、事中、事后都有完备的任务安排。

重大活动网络安全保障整体架构

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，形成一套完整的网络安全保障工作流程，确保重大活动顺利进行、防范网络安全风险。主要内容包括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、全方位的重大活动安全保障体系。



数据来源：赛迪顾问整理，2024,03

图 1　重大活动网络安全保障整体架构

重大活动网络安全保障的管理体系建设主要包括重大活动网络安全组织保障和重大活动网络安全管理制度建设。其中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各项活动。制度建设则是结合国家法律法规及重大活动目标，制定的全面实现重大活动网络安全保障的各项管理及工作制度。

重大活动网络安全技术体系建设包括网络安全技术保障体系、网络安全指挥调度体系等，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、活动后分析复盘为基本框架思路，来构建网络安全总体防护能力。

重大活动网络安全运营服务体系主要分为活动前、活动中、活动后三大阶段，活动前从资产安全评估入手，结合物理、网络、应用和安全管理等方面的评估进行安全加固，通过态势感知平台进行威胁展示和监测。活动中提供安全值守服务，对发现的安全风险及时处置，组织和协调全体保障人员，共同分析研判和封堵网络攻击行为。活动后通过时间和事件维度进行总结分析，并进行整体长期防护优化建议及安全意识培训。

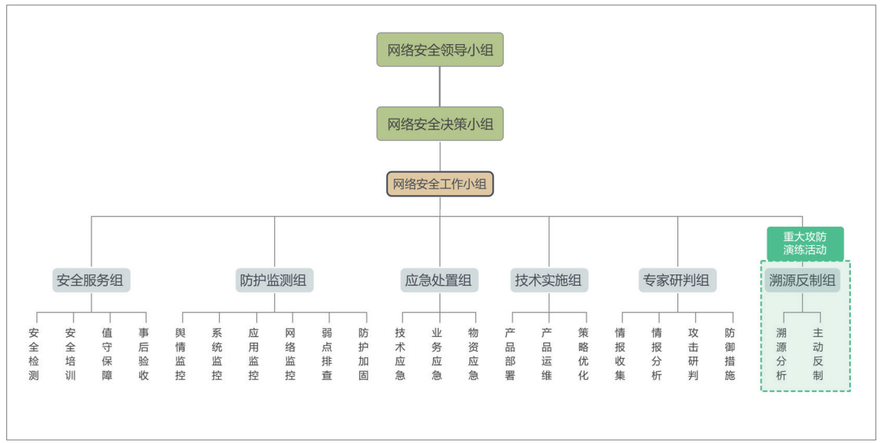
近年来，网络安全环境日益严峻。随着云计算、大数据、物联网、人工智能等技术的不断发展，网络威胁呈现出攻击对象扩大化、攻击方式多样化、攻击常态化和攻击影响深远的特征，给网络安全带来了更为严峻的挑战。要在当前形势下实现重大活动的网络安全保障目标，首先应明确网络安全保障是一项庞大且复杂的系统工程，须秉持整体与全局的安全观念来组织管理网络安全，而不能仅仅聚焦于其中的某个环节、某种防护手段或单个防护设备。在这个过程中，统筹组织保障显得尤为重要。它考验着网络安全团队在面对复杂多变的网络安全威胁时，能否有效地协调各方资源、令各个安全要素形成合力，共同抵御网络攻击。因此，只有具备优秀的组织保障能力，才能在重大活动中形成一个坚不可摧的安全防护体系。

重大活动网络安全保障的管理体系

重大活动网络安全保障的组织设置

重大活动网络安全保障的组织架构

网络安全工作需要统筹管理、统一规划。为确保重大活动期间的网络信息安全保障任务有条不絮的进行和圆满完成，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。根据重大活动中涉及到的网络安全工作任务，网络安全工作小组可下设安全服务组、防护监测组、应急处置组、技术实施组以及专家研判组，各小组协同工作，确保重大活动中网络安全工作的顺利进行。对于重大攻防演练活动，组织设置可划分为演习网络安全领导小组和网络安全工作小组。除重大活动中各专业组的设置外，还应设立专门的攻击溯源反制组，负责对演练中出现的攻击行为进行溯源分析、诱捕和反制工作。组织架构图如下所示。



数据来源：赛迪顾问整理，2024,03

图2 重大活动网络安全保障组织架构

重大活动网络安全保障的各部门职责

网络安全领导小组

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。网络安全领导小组成员应涵盖各相关部

门负责人，组长可以由活动组委会或执委会负责人担任，副组长则至少由分管负责人或负责人的联系人担任。职责上，网络安全领导小组需组建网络安全工作的具体执行部门，向参与重大活动网络安全工作的相关人员传达网络安全标准，明确网络安全责任，并部署相应任务。此外，领导小组还需明确重大活动中网络安全工作相关的预算、人力等资源如何配置，网络安全管理制度体系如何制定等工作。为有效监控和管理网络安全工作，领导小组应定期召开网络安全专项工作会议，听取网络安全决策小组和网络安全工作小组的汇报，并对重大网络安全事项做出决策。

网络安全决策小组

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，确保各专业组间的顺畅沟通和协同合作。决策小组的核心职责之一是制定网络安全保障策略、应急方案以及网络安全技术方案。此外，决策小组还负责组织和协调网络信息事件的应急处置。通过统筹协调，确保在发生网络安全事件时各专业组能够迅速启动应急响应机制，最大程度地减少损失和影响。同时，网络安全决策小组负责评估网络安全事件的影响，对事件进行评级，定期向网络安全领导小组汇报网络信息安全事件及应急处置情况。

网络安全工作小组

网络安全工作小组负责重要活动期间的网络安全工作开展，制定网络安全技术方案，并定期向网络安全决策小组汇报网络安全工作内容。各专业组具体职责如下：

安全服务组

安全服务组工作内容涵盖了安全检测、安全培训、值守保障以及事后验收等多个方面，为重大活动中的网络安全提供了坚实的保障。一是负责安全检测工作。采用渗透测试、源代码安全审计、众测与钓鱼测试、红蓝对抗等技术手段和检测方法来保障目标系统的安全性。二是负责安全培训工作，根据各专业组成员的不同背景和安全保障目标，制定相应的培训计划，包括重大活动的网络安全保障策略、应急预案以及活动中网络安全管理等各项制度，提高各专业组应对突发情况的能力。三是负责值守保障工作。需熟悉重大活动网络安全防护范围内的网络、系统等目标，熟练掌握应急处置和指挥调度系统功能，能够协助建立安全支撑响应的规范和流程，建立健全防御体系。四是在重大活动结束后负责事后验收工作。针对活动中的网络安全保障工作进行深入分析与总结，完成撤离前技术处理和处置工作。同时，协同开展验收与审计事务。在验收与审计工作完毕后，执行数据清除、设备下架回收等后续任务。

防护监测组

防护监测组负责全面监控和管理网络环境中的各个层面，确保活动的顺利进行，包括舆情监控、网络监控、弱点排查、防护加固等工作内容。首先是通过舆情监控，实时监测社交媒体、论坛等渠道与重大活动相关的舆情信息，识别可能引发负面影响的因素，并制定相应的应对策略。此外，防护监测组的主要工作内容是对网络环境进行全面的监控和分析，包括异常行为检测、网络攻击监测等。及时发现网络攻击和异常行为，保障网络安全稳定。通过对网络设备、操作系统、数据库、应用程序等各个组成部分的全面扫描，以及对网络流量和日志数据的实时分析，重点关注那些可能对系统安全构成严重威胁的漏洞，并对其进行详细的分类、定级和风险评估。评估过程中，需要综合考虑漏洞的严重程度、影响范围、修复难度等因素，以制定合理的安全策略和修复计划，并定期对安全策略进行审查和更新，确保防护措施的有效性和适应性。

应急处置组

应急处置组负责重大活动中网络信息安全事件的应急处置，包括技术应急、业务应急以及物资应急三大任务。团队负责评估网络信息安全事件所产生的影响、根除相关事件、恢复相关设备及系统等工作，并向网络安全决策小组汇报网络信息安全事件应急处置结果，并编写网络信息安全事件应急处置报告。应急处置组需具备快速响应和解决问题的能力。重大活动往往涉及多个业务领域，如票务、安保、宣传等，且IT系统复杂性通常较高，团队需对活动业务流程有深入了解，密切关注技术设备和系统的运行状态，以确保能够在业务层面、技术层面迅速应对突发情况。此外，重大活动中的物资需求量大且种类繁多，例如通信、能源、设备等。应急处置组还需提前制定详细的物资保障计划，确保各类物资能够在需要时及时调配和使用。应急处置组可分为内部组织和外部组织两大部分。内部组织主要由活动中负责网络安全保障的内部成员或干系供应商构成，主要负责攻击监测、研判、分析和处置，能够在

网络安全事件发生时迅速作出反应，提供技术应急支持和业务应急支持。而外部组织则主要由外部专家、合作伙伴和相关机构组成，能够在网络安全突发事件中为网络安全部门调配外部资源，以提供支援和协助。例如，在应对DDoS流量型攻击时，一旦攻击达到一定量级，可以申请外部组织（如通信管理部门）协助处置和资源调配，共同应对网络安全威胁，帮助组织迅速恢复网络安全。应急处置组需明确指定主要负责人，确保在突发情况下能够迅速响应并进行紧急处置及事后恢复工作。在应急处置组中可以考虑人员兼任或复用。鉴于应急响应任务的突发性，应急处置组的主要负责人应设置A/B角，以确保重大活动期间实现7/24的全面保障。

技术实施组

技术实施组负责重大活动期间网络安全产品的实施、部署、运维、升级、策略优化等工作，保障网络安全产品在重大活动期间稳定运行，以及在遭遇产品故障时迅速响应。具体工作内容一是对网络安全产品进行全面评估，确保产品满足高并发、低延迟等性能要求。二是根据网络安全领导小组批准的安全策略和计划，部署相应的硬件设备、软件支持以及网络环境，如防火墙、入侵检测系统、数据加密设备等。根据实际需求进行资源配置，确保在活动期间不会出现因为硬件或软件问题而导致的网络安全事故，且各项安全措施能够有效覆盖重大活动的各个环节，实现全方位、无死角的网络安全防护。三是负责产品运维与升级。密切关注产品运行状态，定期开展性能检测。根据活动进展和网络安全形势，及时对网络安全产品进行升级和优化。此外，在应急响应方面，技术实施组需要具备快速响应和处置网络安全事件的能力，向网络安全决策小组汇报安全防护体系现状及下一步改进计划与措施，编写相关服务方案及报告。

专家研判组

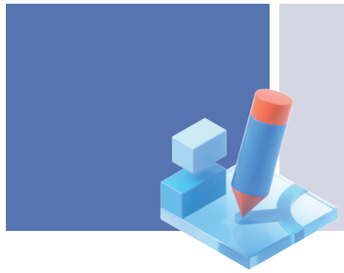
专家研判组负责收集活动期间的网络安全威胁情报，对可能影响活动举办的风险进行评估和预警，同时对活动期间发生的各类复杂情况进行深入研究和分析，提供专业的意见和建议。首要任务是与防护监测组协同，对需要重点关注的潜在威胁、恶意行为、漏洞信息等网络情报进行采集研判。在此基础上，识别出可能对活动造成影响的潜在风险。这些风险可能来自于网络攻击、数据泄露、系统瘫痪等多个方面。专家研判组的工作重点之一是针对各类网络威胁，提出切实可行的防御措施建议、准确评估风险的可能性和影响程度，并提前参与相应的防御措施和应急预案的编写工作。针对重大活动中所面临的复杂安全挑战，如漏洞利用攻击、间谍软件/恶意软件攻击等，专家研判组参与制定安全设备部署方案，并负责指导团队开展漏洞扫描、渗透测试、基线检查等工作。同时，专家研判组还要进行包括异常行为分析、攻击告警分析、日志检索分析在内的情报分析工作。通过分析得出网络中的异常流量、异常访问等行为，及时发现针对活动的网络攻击、可能存在的安全漏洞和攻击痕迹等，为响应处置提供及时、准确的信息。

溯源反制组

重大攻防演练活动中的溯源反制小组负责对演练中发生的攻击事件进行溯源，并整理攻击者画像及对攻击者进行反制。当目标网络被攻击后，通过主机日志、网络设备日志等信息对攻击行为进行分析，区分出攻击方式和来源以判断是否为演练组织的攻击者。在确认为演练攻击者后，对网络攻击事件的进行成功溯源，提交有效证据材料构成证据链并还原完整攻击路径，证实攻击者的攻击行为。此外，溯源反制组能够通过在终端上部署蜜罐，将红队攻击者的攻击流量主动诱捕到蜜罐中，从而实现对攻击者的主动诱捕。基于Web、MySQL、Git 等溯源手段获取攻击者账号、手机号等信息，甚至通过主动反制支持 Windows、Linux 平台可执行程序反控攻击主机。

各类型重大活动组织保障的区别

根据活动性质和目的、参与的人员类型、组织保障关注的对象不同，各类型重大活动的组织保障也不同。国家级会议类主要是通过会议进行政治合作、知识分享、合作交流、决策制定等，其参会人员主要是各国领导人、政府官员等，其组织保障通常根据会议的级别决定其安保组织，一般分为部委组织和地方组织。赛事类活动主要是给运动员提供竞技的平台，其参会人员主要是运动员、裁判、工作人员等，其组织保障主要根据赛事的级别、规模、类型决定其安保组织。通常会成立赛事组织机构执委会或组委会。组织机构成员主要由地方政府、各委办局、社会招聘等人员组成。重要时期攻防演练活动主要由公安部或省市监管单位组织，对参演单位模拟真实网络安全攻击,检验参演单位网络安全防护水平，各参演单位网络安全保障组织由各单位自行组织。



重大活动网络安全保障的制度建设

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。在此基础上，遵循国家网络安全法律法规政策，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，包括操作规程制度、系统管理制度、数据管理制度、人员管理制度、场地管理制度以及审批管理制度等。网络安全制度建设如下图所示。

数据来源：赛迪顾问整理，2024,03

图 3 重大活动网络安全制度建设

系统管理制度

系统管理制度应进一步明确系统安全建设的标准和流程，从系统配置、系统策略制定以及安全漏洞的修复等，都应有明确的指导和规范。同时，应明确系统运行的各项标准和要求，例如稳定性、安全性以及故障处理流程等，保障系统持续稳定地提供网络服务。对于在重大活动中会涉及到的外包或第三方系统，应规范外包软件的开发流程和质量要求，确保外包软件的安全性和稳定性，避免因软件漏洞或缺陷而引发的安全风险。在系统运行过程中，系统变更管理制度同样重要。它应明确系统变更的流程和审批程序，确保系统变更的合规性和安全性，避免因变更不当而带来安全风险。最后，专网安全设备账号密码管理制度应严格规范账号和密码管理，确保账号和密码的安全性和保密性，防止账号和密码被非法获取或滥用。

数据管理制度

为保障重大活动中的数据安全，应制定涵盖数据在收集、存储、传输和销毁等全流程的管理制度，确保数据的安全性和完整性。制度应包括文件管理制度、备份恢复管理制度、敏感数据管理制度、数据合规管理制度、数据安全管理制度等。首先需保障数据的来源、使用目的、共享范围等方面的合法性和合规性，以及数据泄露、篡改等事件的处置机制，如数据脱敏最小化、注销业务及时下线、禁止跨域访问数据、一人一账号等相关规范。同时，须建立完善的备份恢复机制，对备份的频率、周期、存储等进行规定，以及备份数据的测试、恢复和验证流程，确保在数据丢失或损坏时能够及时恢复。此外，对敏感数据的访问和传输需制定相应制度进行严格控制，防止敏感数据被泄露或滥用。

人员管理制度

人员管理制度应明确网络安全人员的职责和权限，强化网络安全意识和技能培训，提高人员的网络安全防护能力。具体而言，人员安全管理制度应详细规定各岗位人员的职责，确保在紧急情况下能够迅速响应。同时，加强沟通合作管理制度，促进网络安全人员间的信息交流与协作。对于第三方人员，应制定专门的管理制度，进行必要的网络安全培训和监管，防止其成为安全隐患。此外，实施安全值守值班制度，确保关键时刻有专人值守，能够迅速应对网络安全突发事件。 在重大攻防演练活动中，应制定更为严格的人员管理制度，明确参与人员的职责、权限以及安全保密规定。对于违反演习规则的行为，应有明确的处理机制。任何擅自更改演练流程、未经许可擅自行动等行为都应受到严肃处理，根据违规行为的严重程度分级处理，包括扣分、公开通报、终止个人或队伍本次资格、个人或单位加入黑名单、行业禁入等。

应急管理制度

重大活动中的网络安全保障工作应构建一套完善且明确的应急管理制度，详细规定各项网络安全事件的响应与报送机制，确保在发生网络安全事件时，能够迅速、有效地进行应对和处置。此制度应涵盖网络安全事件应急管理的各个环节，明确网络安全事件的分类、定级、处置流程以及责任主体的清晰界定。同时，对于可能引发连锁反应的事件升级情况，应明确具体条件、程序以及相应的处置措施。依据不同攻击的严重程度，制定并执行相应的响应流程，确保对应级别的人员能够及时介入并妥善处理。通过构建高效的信息通报机制，并经过演练对信息通报机制进行备案，确保在网络安全事件发生时相关部门和人员能够迅速获取关键信息。在制度构建中，还应详细规定应急响应的具体流程、措施以及保障条件，确保在网络安全事件突发时，能够迅速启动应急响应机制，最大限度地减少损失。

在重大攻防演练活动中，为确保演练的有序进行需制定详尽的演练报告制度。该制度应清晰规定在攻击方对目标实施攻击后，值守人员需按照设定的条件和步骤，使用统一的加密通讯工具向演练指挥部报告相关情况。基于制度规范值守人员的报告机制，防止因未经指挥部批准擅自行动而产生的不利影响。

场地管理制度

场地管理制度应确保网络设备的安全运行环境，明确办公区域的布局、设备摆放以及人员出入等要求，以确保办公环境的整洁、有序和安全。此外，机房作为网络设备的核心存放和运行场所，应设立严格的机房出入登记制度，确保只有授权人员能够进入机房。同时，对设备的放置、供电、防火、防水等方面进行规范，以防止因环境问题导致的网络安全事故。

审批管理制度

审批管理制度是确保信息系统授权、采购等关键操作得以规范执行的重要保障机制。通过严格的审查和批准制度，确保操作符合重大活动中网络安全保障工作的要求。首先，审批管理制度应明确具体的审批流程，包括申请提交、初步审查、深入评估、审批决策以及结果通知等各个环节，以及每个环节对应的责任人和执行标准。此外，制度应明确申请通过的标准，如授权申请需符合企业的安全策略和授权管理要求，或采购申请需确保所采购的产品或服务的性能、安全性、兼容性等方面满足网络安全保障需求。

重大活动网络安全保障的技术体系建设贯穿于活动的整个生命周期，包括活动前实施、活动时保障、活动后验收三个阶段。网络安全总体设计遵循网络安全事件的客观发展规律，充分考虑重大活动的特殊性和重要性，总体技术保障方案按照“总揽全局、纵深防御、严抓实施、重在保障”覆盖重大活动的系统安全、基础设施安全、活动运行安全等各个方面。

重大活动网络安全保障的技术体系建设

重大活动网络安全保障的技术体系建设思路

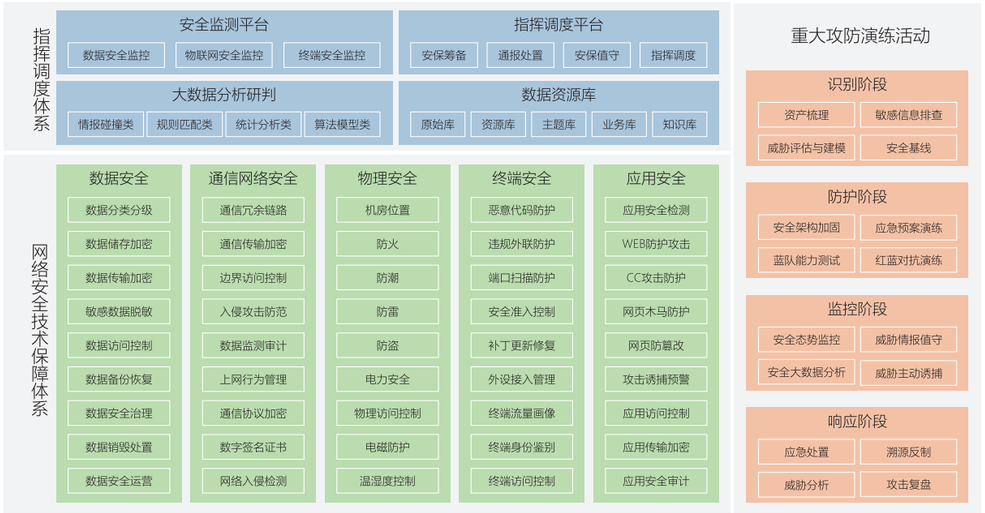
重大活动网络安全技术保障体系的建设主要从保障重大活动基础设施安全和业务系统安全两方面着手进行。重大活动基础设施分为活动举办场所、非活动举办场所，活动举办场所用于活动举办，非活动举办场所用于服务和保障活动的顺利举行。活动举办场所网络安全保障包括场所的系统、网络（活动专网、管理专网）、应用、终端、数据等，非活动举办场所包括网络安全、系统安全等。重大活动基础设施安全建设应按照不同场所情况、特点，提供差异化设计，为活动主办方、活动参与方、媒体、观众等提供安全高效的保障。

重大活动业务信息系统是活动的核心组件，是完成重大活动各项组织工作、具体活动工作以及管理工作的基础。业务信息系统包括核心业务系统、承载业务信息系统的云计算平台和网络系统等。重大活动业务信息系统安全建设应采用“多层防护、横向扩展”的安全设计思路，充分考虑物理安全、网络安全防护、应用安全保障、数据安全冗余、终端可信可控等实际要求，因地制宜，在网络安全保障和业务平稳运行中找到最佳平衡点。

重大活动网络安全保障的技术体系建设内容

重大活动网络安全保障技术体系的总体设计应建立在成熟的等级保护体系基础上，选取适宜的网络安全模型思想，突出重点保障和立体防护，构建全方位主动防御、动态监测、整体防控和精准防护。设计时要坚持管理与技术并重，使信息保障的策略、过程、技术和机制在整个重大活动的活动前、活动时、活动后三个阶段均得以落实，从而在整体上提升网络安全保护能力，切实维护和保障重大活动的网络与信息系统整体安全。

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、活动后分析复盘为基本框架思路，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。



数据来源：赛迪顾问整理，2024,03

图4 重大活动网络安全技术保障总体架构

重大活动网络安全技术保障体系构成

重大活动信息系统是活动举办的重要保障，特别是国际综合性、有影响力的重大活动，必须依照国家相关法律法规，按照网络安全等级保护2.0标准及《关键信息基础设施安全保护条例》的要求设计网络安全技术保障体系，建立一体化全天候网络安全防护屏障。重大活动网络安全技术保障体系是围绕着云计算中心和场所两大业务应用场景进行保障的，因此要将重大活动信息系统的整个安全防护抽象成物理安全、通信网络安全、应用安全、终端安全、数据安全几个维度，形成信息系统全方位立体防护体系。在信息系统安全防护的每一个维度，利用综合信息系统安全保障的技术管理和人员服务要素对信息系统进行安全保障。

物理安全

云计算中心和场所承载着重大活动最为重要和核心的业务。云平台和云上业务防护安全要求云供应商应按照规范化要求进行安全防护设计、建设和运维。重大活动的主办部门应对云计算中心的运行进行监管，并根据监管需要补充缺失的安全能力。场所的网络安全按照不同场所情况和特点进行差异化设计，以提供良好的网络安全保障服务。每一个承担业务系统单元的安全建设，应按照不低于等级保护三级要求标准来完善网络安全技术服务和技术手段。

通信网络安全

重大活动整体的通信网络主要覆盖活动专网和管理专网，包括两张专网的骨干网、场所和云计算中心。针对互联网开放的网络重点部署防御DDoS攻击、入侵攻击等网络恶意攻击事件，基于等级保护三级的建设要求采用冗余链路、通信加密、流量监测、上网行为管理等安全措施，保障重大活动通信网络的安全生态环境。

应用安全

重大活动信息系统的应用安全涉及应用安全域划分建议、应用系统上线、安全评估流程建议、等级保护定级等四个环节，从各方面完善重大活动的应用安全防护体系，形成应用系统的安全闭环运营，全面构建重大活动应用系统运行的安全防护能力。

终端安全

重大活动信息技术建设涉及的设备数量庞大、种类繁多，需要设计一整套互为补充且能够共同协作的终端安全解决方案。通过防病毒软件、主动威胁防护、系统防护、网络防护、外设管理、文件审计等防护手段，保障活动举办期间整个主机及终端的可用性和业务连续性。

数据安全

重大活动信息化业务开展过程中会采集（产生）、存储和处理大量的敏感数据，需要建立整体的数据安全治理保障体系，包括数据安全管理制度、数据全生命周期的安全防护、数据安全咨询服务等。通过数据安全风险监测和运营，从风险的发现、响应、决策，直到处置，不断地迭代和优化数据安全保障能力，逐步实现从“单点的被动保护”向“整体的主动防护”转变，为保障重大活动举办期间的数据安全保驾护航。

重大活动网络安全技术保障体系要构建安全稳定、可控可信的网络运行环境，重点加强应用与数据安全保护，做好入网终端设备的安全管控，用先进的技术和手段，识别潜在的安全风险和隐患，提供全面的技术保障措施。

网络安全指挥调度体系

网络安全指挥调度体系是重大活动的“安全大脑”，总体架构设计应充分利用大数据的处理能力，统筹规划各场所数据资源，实现多元异构数据的接入，以资产管理、安全监测、分析研判、指挥调度为核心建设网络安全指挥调度平台。平台通过采集活动专网、管理专网及各场所中的网络资产数据、应用安全数据、流量监测数据、系统日志数据、恶意攻击样本数据、终端安全数据、威胁情报数据、等级保护检查数据等，构建既能管理全域安全数据又能支撑多层次网络安全业务分析与计算需求的大数据基础支撑系统，形成标准的原始库、主题库、资源库、知识库和业务库。在此基础上，利用多源异构数据融合、关联分析可视化、溯源分析可视化等技术，实现大数据智能分析研判，达到安全事件的精准感知，实时通报预警以及高效响应处置，提升重大活动网络安全保障团队的人工研判能力，以及平台与国家、城市监管机构之间的网络安全事件联动处置能力。

重大攻防演练活动技术体系建设主要内容

针对重大攻防演练活动的技术体系主要围绕识别阶段、防护阶段、监测阶段和响应阶段四大模块进行建设。识别阶段主要基于网络空间资产测绘等平台，结合敏感信息排查、威胁评估和安全基线建立等服务，测绘信息资产安全暴露面，建立网络安全态势感知基本能力。防护阶段主要通过分解业务场景、绘制数据流图、评估风险点等步骤划定攻击路径，形成威胁模型；基于当前网络拓扑存在的安全风险进行安全评估，输出安全布防图；针对性开展安全意识和应急预案培训，通过模拟真实攻击场景进行应急演练，检验应急响应流程与响应机制的可靠性，促进应急预案的完善与应急团队的效能；远程开展红蓝对抗演练服务，有效测量当前防御手段面对威胁时的安全防御能力。监测阶段通过整合终端、网络链路、应用系统等各类数据源，利用威胁情报的感知、共享和分析来对抗各类安全威胁，实现确定威胁、量化风险、安全分析和攻击诱捕。响应阶段主要提供包括应急处置、溯源反制等，并实现全面攻击复盘总结。

重大活动网络安全运营体系是确保重大活动安全顺利举办的关键所在。根据重大活动特点和活动运行的要求，结合对重大活动面临的风险分析、安全需求分析，重大活动网络安全运营服务规划了事前准备阶段、事中保障阶段、事后总结阶段三个阶段的网络安全运营保障计划，设计了重大活动网络安全运营服务体系，确保能够按照预期安全、高效、稳定地保障重大活动举办的各项安全。

重大活动网络安全保障的运营体系建设

重大活动网络安全保障的运营整体思路

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。由于所有准备工作、设计规划和保障服务都是为了重大活动的安全、稳定运行，因此事中保障阶段成为重大活动网络安全工作中的重要环节。

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。

	事前准备阶段		事中保障阶段		事后总结阶段	
重大攻防演练活动	网络安全设计	网络安全管理体系	网络安全巡检	网络安全应急响应	总结分析	配合项目验收
	网络安全评估	网络安全应急演练	网络安全监测	网络安全值守保障	项目报告	配合项目审计
	网络安全建设	网络安全检测加固	网络安全运维	网络安全攻击处理	数据清退	设备回收
	联调联试	网络安全联合演练	网络安全分析	网络安全指挥调度	项目验收准备	遗产处置
	编制整体防守方案	组件防守演练团队	实战场景推演	安全攻击实施	攻击复盘总结	防守复盘总结
	常见风险排查验证	深度安全评估服务	安全防守实施	攻击溯源反制	防守报告编制	风险持续整改

数据来源：赛迪顾问整理，2024,03

图 5 重大活动网络安全运营服务总体架构

针对不同类型重大活动的差异性需求，网络安全运营保障会采取不同的策略。例如，体育赛事和重大会议在网络安全运营流程上的不同之处主要体现在安全保障重点、风险评估、预案制定和实施等方面。首先，体育赛事的网络安全工作重心在于确保赛事的顺利进行和参赛人员、观众的人身安全。因此，网络安全流程保障涉及到对赛事场馆、住宿设施、交通路线等环节的风险评估，以识别潜在的网络威胁。此外，大型综合类体育赛事组织具有周期长、投入精力大等特点，大型综合类体育赛事的网络安全保障实质上是考验承办城市的网络安全综合保障水平，因此，赛后的总结将会赋能城市的网络安全建设，为后续的城市网络空间保护提供借鉴。而重大会议的网络安全工作则更注重政治敏感性、国家安全和数据安全等。在会议筹备阶段，网络安全运营保障需要更多关注针对会议的主题、议程、参会人员等信息的审查，以确保不会出现政治敏感词句和不良信息。同时，在会议期间，网络安全团队要对与会人员的电子设备进行安全检查，以防窃取国家机密和会议敏感信息等。

重大活动网络安全保障的运营服务重点内容

网络安全运营保障是一项系统性、综合性的任务。构建一套完整的网络安全运营流程是确保重大活动顺利进行、防范网络安全风险的先决条件。重大活动的网络安全保障工作贯穿“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，共同构成了全面、系统的网络安全运营保障体系。

重大活动的网络安全运营工作的每个阶段都包含一系列关键流程和要素，以确保网络环境的安全性和稳定性。其中，事前准备阶段通过网络安全设计、网络安全建设、网络安全检测加固以及网络安全联合演练等一系列流程，为活动的顺利进行奠定了坚实的网络安全基础。事中保障阶段则注重实时监控与快速响应，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保障过程的回顾，为未来的网络安全工作提供宝贵经验。

工作名称	工作子项	工作内容	配合内容
事前准备阶段	团队组建	> 组建重大活动网络安全保障的组织管理团队	> 确定并布置指挥部、分析组、处置组工作地点及监控大屏 > 全员安全意识培训，尤其是社会工程学攻击防护意识
	隐患自查	> 资产梳理，暴露面检查 > 网络拓扑结构梳理 > 账户与弱口令检查 > 漏洞与基线检查 > 泄露信息与入侵痕迹排查 > 渗透测试	> 协同收集和确认资产 > 确认资产赋值方案 > 重要信息资产价值
	防护措施落地（评估与加固）	> 安全运维策略优化 安全检测与防护设备部署（慧眼检测平台、应急处置装置、安全态势感知）	> 协调网络运维人员、业务系统运维人员现场配合设备上线及策略优化
	攻防演练（应急预案）	> 模拟攻击演练，发现问题解决问题	> 协调相关人员全程参与
事中保障阶段	应急值守	> 安全态势监控分析 > 入侵事件行为分析，包含扫描、破解行为，漏洞利用行为，木马上传与利用行为，横向肉机利用行为 > 多产品联合策略优化分析 > 安全应急响应处置	> 协调相关人员全程参与
事后总结阶段	汇报总结	> 活动总结汇报，通过时间和事件维度同时分析 > 防护整改优化建议，包含防护策略优化建议，网络安全域改进建议，防护设备确实补充建议，安全服务能力提升建议 > 安全意识培训	> 协调相关人员全程参与

数据来源：赛迪顾问整理，2024,03

表 1 重大活动网络安全运营服务流程表

事前准备阶段

网络安全设计

在网络安全工作启动阶段，需要咨询设计组、运营管理组等事前实施组织整理需求，明确活动的具体范围、目标、参与人员，以及活动期间的重点保障对象，制定整体保障方案。保障方案应围绕上级单位要求和自有系统的关键保障资产清单，由安全保障领导小组统筹安排，明确保障人员，并签订网络与信息安全保障承诺书。

安全保障领导小组向下级组织发布保障方案后，各部门需根据规定，细化各自的保障工作方案与应急预案。根据国家对关键信息基础设施安全保护和网络安全等级保护等相关要求，结合活动的整体工作安排，将保障方案、应急预案中的总体要求不断细化。在此过程中，各组织应详尽列出重大活动保障期间所有需执行的相关工作、存在的问题和可能遇到的困难，并明确各项任务的责任人、完成时限以及达标要求等。针对所列出的各项问题和任务清单，逐一下发到对应责任人，落实闭环销项。

网络安全建设

在任务明确后，事前实施组织成员需开展核查工作。首先要依据重大活动的类型和网络安全保障重点，进行全面的网络安全风险评估。这需要对涉及到的关键基础设施和重要网络设施等相关系统和资产进行进一步梳理，特别是对互联网暴露面资产和关键基础设施进行潜在威胁的识别，并评估这些威胁可能对活动造成的影响。事前实施组织需基于风险评估结果，部署相应的安全技术和设备，包括加固网络基础设施、数据加密与传输安全部署、配置安全策略和访问控制等。

网络安全检测加固

通过逐一排查、逐一整治的方式，对部署的重要系统开展全面自查整改工作，对各组织负责的重要网站、系统和业务实施监督检查。在此过程中，安全保障领导小组将发挥关键作用，负责监督并推动检测加固的落实。同时，领导小组还需建立起安全事件监测后的事件上报流程和信息共享机制，以便各成员单位及时报告和处理安全事件。当各项活动前准备任务完成后，责任人需上报结果，由安全保障领导小组对各项工作的完成情况进行确认与审核，形成闭环反馈机制，确保整个网络安全加固工作的持续改进。

网络安全联合演练

在各个筹备环节均已完成的情况下，事前实施的关键步骤是通过真实模拟保障任务的过程来检验保障手段是否切实可行。为此，领导小组需组织全体将参与重大活动网络安全保障工作的人员开展联合演练活动，全面、深入地评估当前安全策略的实际成效及其可行性。如果在模拟保障任务过程中发现任何潜在的安全漏洞，必须严格按照闭环处理流程进行调整和优化，确保网络安全防护水平的提升。

事中保障阶段

网络安全监测与分析

活动运行保障期间是网络攻击的高发阶段，也是网络安全保障工作中的核心。因此，本阶段的核心任务是对各类安全事件的实时监测与研判。为确保网络安全事件的及时响应，网络安全部门需指派专门的值守团队，全天候待命，并建立7*24小时监测预警与防护机制。同时，事中保障组织将全面负责关键网络设备、系统及应用的巡检工作，实施全面的网络安全监测措施，包括网络流量监测、安全事件监测、恶意代码监测等。一旦发现任何异常行为或潜在威胁，将立即触发报警机制，并通知值守工程师进行处置。

网络安全攻击处理

由于网络安全攻击或事件处置的时效性要求较高，及时处理有助于遏制扩散或降低入侵成功率。因此，一旦发生报警机制被触发，现场保障人员应第一时间依据预先制定的方案进行处置，启动应急响应流程。在完成网络安全事件的应急处理后，网络保障人员需及时

通过系统报告处置情况。随后，专家研判组将对每起上报的网络安全事件进行深入分析，评估事件是否具有针对性、共性，以及是否可能引发全局性同步网络攻击，同时预测攻击者是否会转移目标，病毒是否存在无限传播扩散的可能性等。领导小组将根据研判结果、活动进展和整体安全状况分析，决定是否调整安全措施和策略。

网络安全指挥调度

在事中保障阶段，网络领导小组发挥着核心作用，需要与活动组织方、技术支持团队等各方保持密切协调和沟通，并建立网络安全信息共享机制，及时收集和分析各方提供的网络安全情报。同样也能确保各方在网络安全事件发生时迅速响应并形成合力，共同应对可能出现的网络安全事件。

事后总结阶段

总结分析

在事后总结阶段，各小组应就值班状况、安全防护措施、监测手段、响应和协同处置等方面，形成总结报告并向有关部门汇报。报告内容应涵盖网络安全事件的全貌，如事件起因、影响范围、处置过程等。同时，应形成对整个活动的网络安全保障工作的总结与评估，并分析安全事件的原因和教训，对活动保障过程中存在的脆弱点，提出改进措施和建议，为未来类似活动提供借鉴。在此基础上，对继续沿用的系统开展整改工作，以提升目标系统的安全防护水平。

配合项目验收

在活动结束后，事后验收组织需要继续发挥重要作用，配合数据清退、遗产处置以及项目审计等工作。首先，事后验收组织需要负责整理和归档所有与活动相关的网络安全数据，包括监控日志、事件报告、威胁情报等。在确保数据完整性和安全性的前提下，按照相关规定和程序进行数据清理工作，删除或脱敏不再需要的数据，确保不会泄露敏感信息。对于需要长期保存的数据，保障小组需要制定存储方案，并确保数据的安全性和可访问性。同时，如果需要将数据移交给其他团队或机构，保障小组需要确保移交过程中的安全性和合规性。

重大攻防演练活动运营体系建设主要内容

准备阶段

重大攻防演练活动事前准备阶段主要开展隐患排查、安全加固、安全防护设备优化、安全意识培训等工作。隐患排查针对无法关闭的信息资产开展漏洞扫描、渗透测试、基线检查、攻击路径分析、敏感信息排查、Webshell专项检查、弱口令扫描、策略梳理等工作，以评估信息资产的安全性，确保活动前安全问题发现和解决。安全加固根据前期发现的问题，通过补丁更新、代码修复、关闭不必要的服务、调整安全策略等方式进行安全加固。安全意识培训针对本次活动参与人员进行安全意识培训，提高参与人员的安全处置能力。

资产梳理

通过使用自动化平台或工具，探测组织内网和外网资产，发现相关资产信息，包括关联域名、服务类型、资产指纹、协议类型、开放端口、人员敏感信息等数据。

暴露面收敛

通过端口扫描、指纹识别、网络边界检查、服务器核查等方式对资产梳理出的资产进行识别，识别当前暴露面，并梳理相关高风险暴露面进行收敛。

工作项	工作内容
出口收敛	减少互联网、广域网、专线、“一张网”、VPN等连接通道，归拢外网访问出口。
互联网资产清理	通过互联网出口IP段全端口扫描、搜索引擎搜索关键字、NAT策略和已有的互联网应用台账。
内网资产清理	开展内网IT资产扫描，更新或创建IT资产表，关停清退未知IT资产。
网络边界梳理	清理网络防火墙、区域防火墙、VPN设备策略、账号。
网络拓扑检查	梳理并更新网络拓扑,部署安全设备，整改过宽的策略。
服务器端口核查	服务器开放自身提供服务相关端口，关闭不必要的端口和对外服务，减少暴露面，建立白名单。
服务器非法软件核查	服务器应采用最小化系统安装原则，只安装与自身业务相关的操作系统组件及应用软件。

数据来源：赛迪顾问整理，2024,03

表 2 重大攻防演练活动暴露面收敛工作清单

隐患排查

针对无法关闭的信息资产开展漏洞扫描、渗透测试、基线检查、攻击路径分析、敏感信息排查、Webshell专项检查、弱口令扫描、策略梳理等工作。以评估信息资产的安全性，确保重大攻防演练活动前安全问题及时发现和解决。

安全加固

根据前期资产梳理、隐患排查工作发现的问题，通过补丁更新、代码修复、关闭不必要的服务、调整安全策略等方式进行安全加固。

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。
	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。
网络与安全设备加固	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。
	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。
数据库安全加固	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)。
	安全策略梳理	开展数据库安全策略梳理。
中间件安全加固	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。
	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。
互联网安全加固	账号安全	删除多余的测试账号。
		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。
		对用户的登录登出、重要操作以及应用系统的重大变更进行审计，开启安全审计功能。
	上传限制	限制上传类型和上传文件大小。
	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）。

数据来源：赛迪顾问整理，2024,03

表 3 重大攻防演练活动安全加固工作清单

安全意识培训

面向本次演练参与人员进行安全意识培训，明确演练工作中应注意的安全事项；提高本次演练参与人员的安全意识；提高本次演练参与人员的安全处置能力，针对演练攻击中可能用到的技术手段和应对措施进行培训。

演练阶段

重大攻防演练活动事中演练阶段主要开展攻击检测与分析、事件应急处置、攻击溯源反制等工作。攻击检测与分析主要分析网络流量和日志，识别可能的攻击行为，如恶意流量、异常登录尝试等。安全事件应急处置对发现的安全事件进行及时响应，采取必要措施阻止攻击并减少损失，针对攻击成功的系统进行快速恢复，确保业务连续性和服务可用性。攻击溯源反制分析攻击者的行为和攻击路径，确定攻击者入侵系统的方式和方法，提出改进建议和修复措施。

专项情报推送

利用多种渠道，采用多样化的技术手段，采集大规模碎片式的异常数据以及其他相关威胁信息。通过集中的深度挖掘、提练、融合、归并以形成与信息系统核心资产有关的威胁线索集合，并结合恶意特征进行分析，得出有价值的威胁信息，为后续分析、预判、决策提供基础。通过威胁情报的评估、关联分析、以及智能推演完成海量情报分析，通过支撑网络空间安全防御的计划、执行、检查及处理，形成安全防护的闭环。

安全监测值守

利用安全防护设备（全流量监控、大数据平台、WEB　防火墙、数据库审计）等进行全流量监测和大数据关联分析，及时发现异常行为，如外连远控、横向非法访问等，第一时间发现安全威胁，并进行分析研判。实时监测分析安全设备告警日志，主要监测分析异常流量、恶意文件、木马远控、弱口令、漏洞利用攻击等，第一时间发现安全威胁，并进行分析研判。

安全分析研判

针对网络攻击告警事件进行深入分析，研判攻击造成危害和影响，准确有效甄别疑似和真实失陷事件。基于ATT&CK 框架，利用安全运营平台日志检索分析模块工具对海量日志进行人工检索、多维度关联分析，深度挖掘潜在和未知安全威胁。

网络安全预警

针对已遭受成功入侵的安全事件进行预警，预警内容包括受害IP、攻击时间、攻击类型、可能的攻击路径、下一步处置建议等，快速预警各类疑似和真实失陷事件，为响应处置提供技术支撑。针对0day/Nday 漏洞进行预警，包括漏洞名称、影响范围、危害和安全整改加固措施等，快速预警0day/Nday 漏洞，并采取整改和加固措施，防止攻击继续利用漏洞突破网络边界。

应急响应处置

对发现的安全事件进行及时响应，采取必要的措施阻止攻击并减少损失。针对不同类型的攻击，制定相应的应急响应计划和操作指南。发现违规情况第一时间阻断，上报领导小组。对攻击事件进行研判分析及验证，确定漏洞存在的真实性。针对攻击成功的系统进行快速恢复，确保业务连续性和服务可用性。实施备份和恢复计划，还原受损的系统和数据。

攻击溯源反制

对演练中发生的攻击事件进行溯源，整理攻击者画像，并对攻击者进行反制。当目标网络被攻击后，通过主机日志、网络设备日志、

入侵检测设备日志等信息对攻击行为进行分析，找到攻击者源IP地址、攻击服务器IP地址、邮件地址等。溯源目的是要区分攻击方式和来源以判断是否为演练组织的攻击者，在确认为演练攻击者后，防守团队立即上报，演练结束将完整的溯源流程记录在演练报告中。对网络攻击事件进行溯源，提交有效证据材料构成证据链，还原完整攻击路径，证实攻击者的攻击行为。

总结阶段

重大攻防演练活动事后总结阶段主要通过全面总结本次演练活动各阶段的工作情况，包括组织队伍、攻击情况、防守情况、安全防护措施、监测手段、响应和协同处置等，形成总结报告并向有关单位汇报。针对演练结果，对演练过程中存在的脆弱点，开展整改工作，进一步提高目标系统的安全防护能力。

攻击复盘总结

针对攻击事件进行综合分析，从攻击视角检视网络安全监测和防护体系，为持续提升安全能力提供依据。主要包括攻击方法、攻击时间、攻击目标分布及攻击成功事件等方面。

防守复盘总结

防守复盘总结主要从攻击干扰、威胁情报获取、攻击发现、攻击阻断、应急处置、追踪溯源等方面开展总结，针对整个防守过程进行全面复盘，分析实际工作中的得失，评估威胁发现能力、应急处置能力、策略优化能力、安全加固能力在本次演练中的能力级别。同时针对得分点进行总结分析，提炼攻防技战法。

风险持续整改

基于复盘进行攻防演练后的总结改进提升。对不足的部分提出安全整改建议，强化现有安全防护能力。通过对技术漏洞问题和管理流程问题的梳理，进行技术总结整改、流程总结整改、人员总结整改内容评估工作，最终组织专业技术人员和专家，汇总、分析所有攻击数据，汇总发现的突出问题，形成全面整改报告。

安全能力提升

通过攻防复盘、培训、会议等方式，进行攻防技能经验交流分享，积累实战经验，针对技术人员进行相应攻防技能培训，同时针对非技术人员进行相关基础安全意识赋能，全面提升人员的技术水平。全面更新攻防知识库，提升攻防技战术，由攻防演练向常态化安全运营过渡。优化安全运营流程与工作，尤其针对在演练过程中提炼出的监测及处置手段，应用于安全运营中，将相关流程标准化，进一步提升日常安全保障水平。

重大活动期间的网络安全保障依赖于网络安全从业者们平时长期深厚的积累，才能应对突发情况下的安全威胁。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。为应对这种日益复杂、不断变化的安全挑战，重大活动的网络安全保障建设内容和工作方法需要随之变化与升级。未来，重大活动网络安全保障必将朝着智能化、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。

建议及展望

加强智能化安全防护手段的应用

随着人工智能和大数据技术的发展，重大活动的网络安全防护将使用更多智能化的手段。自动化的安全监控系统能够实时识别和应对各种安全威胁，提高安全防护的效率和准确性。利用大数据和机器学习等技术，能够对安全风险进行更加精准的分析和预测，及时采取措施防范安全威胁。利用安全大模型提升重大活动网络安全保障的威胁检测能力、运营效率等。

实现多维度的安全保障

未来的网络安全保障将更加注重多维度的安全防护，包括网络安全、应用安全、数据安全等多个方面。保障包括对应用程序的开发、部署和运行过程进行安全审查和监控，防止应用漏洞和恶意代码攻击；保障数据的安全传输和存储，包括加密传输、访问控制、数据备份、数据恢复等措施，防止数据泄露和篡改；保障物理设施的安全，包括机房、服务器等设备的物理安全防护，防止未经授权的人员进入或损坏设备；此外还要保障人员以及供应链各环节的安全性，有效降低重大活动的网络系统遭受安全威胁的风险。

加强协同防御和威胁情报共享

重大活动网络安全保障要更加注重协同防御和共享安全情报。各相关部门、机构和组织之间建立合作机制，共同应对网络安全威胁。建立安全信息共享平台，用于各方之间共享安全情报、攻击事件信息、威胁情报等，及时获取最新的威胁情报，做出更有效的应对措施。通过加强协同防御和威胁情报共享，能够有效整合各方的资源和力量，提高网络安全的整体防御能力和应对能力，降低网络安全威胁带来的风险和损失。

提供个性化安全服务

根据重大活动不同组织和用户的需求和特点，提供定制化的安全解决方案和服务，更好地满足各方的安全需求。针对会议的级别、重要性以及类别等，部署不同的网络防御设备，提供个性化的身份验证与访问控制策略，制定应对各种紧急安全事件的应急响应计划、数据保护措施等。通过提供这些个性化的安全服务，可以帮助确保重大会议活动的网络安全，并保护参与者的隐私和敏感信息免受威胁。

2024

重大活动网络安全保障建设及运营指南

扫码下载电子版指南