体育赛事
网络安全保障实践
蓝皮书
2024

联合发布单位
安恒信息 | 鹏城实验室 | 广州大学 | 哈尔滨工业大学（深圳）

蓝皮书编写组

编写指导

方滨兴　范　渊　袁明坤　贾　焰　田志宏　王　拓

刘秀超　张　超　韦国文　王　洁　顾钊铨　梁　浩

编写团队

冯文英　黄　涛　黄　曦　景　晓　姜　誉　刘嘉翼

李润恒　李伟伟　刘　园　林真引　苏　申　孙彦斌

谢敏容　向夏雨　王　科　王茂华　王梦娇　王奕超

杨建业　于天娇　张登辉　张桂文　张建盛　曾丽仪

邹铭津

（排名不分先后）

前言

随着信息技术的飞速发展，体育赛事已经高度依赖信息化技术，成为融合了信息技术、媒体传播等多领域的综合性活动。信息技术的引入不仅为体育赛事带来了便利和精彩，也伴随了新的网络安全的挑战。为此，保障体育赛事的网络安全不仅关系到比赛的顺利进行，更关系到参与者的权益及公众的信任。

从国际级综合体育赛事的视角看网络安全保障，可以分成赛前、赛中和赛间三个阶段，需要采取不同的网络安全保障模式。其中赛间是指运动会与残运会之间的转换期，如亚运会与亚残运会之间有两周的转换期。

赛前是赛事信息系统的准备阶段，采取的是自卫模式。在信息系统准备的同时，首先要进行安全管理，即需要检测信息系统自身的安全问题，需要确保信息系统符合安全基线，需要彻查信息系统的安全漏洞，需要进行风险测评，需要进行护网演练等；其次是要部署尽力而为的网络攻击应对手段，力保信息系统不因网络攻击而失效；再就是要部署必要的容灾备份系统，确保在系统承受不了攻击的时候可以切换应对。

赛中是赛事信息系统的运行阶段，采取的是护卫模式。这个时候继续挖掘安全漏洞已经没有意义，系统就算有任何瑕疵，也会因为“封网”的原因而不能再进行任何升级改造。因此，护卫模式的防御重点转向了发现攻击者、阻截攻击者的环节。在此期间，首先要利用蜜点等各种感知手段来感知攻击者的存在；其次是要通过IP碰撞、关联分析等研判手段来锁定攻击者；最终的目的是要知道谁是攻击者并将之阻断，同时还要反查攻击者都曾经渗透到哪些系统中，其风险程度如何。

赛间是赛事信息系统的休整阶段，采取的是迭代模式。在这期间，首先是要进行审计核查，即要分析信息系统的日志文件以检查攻击的蛛丝马迹，要对所发生过的攻击事件进行复盘以分析信息系统的脆弱点，要清除攻击者在攻击期间所埋的雷；其次是防御体系的迭代升级，要根据分析的结果对所出现的漏洞进行打补丁，要升级检测规则，要重构防御系统；再就是要进行攻击测绘，以便为今后识别攻击者奠定基础，包括对攻击者的IP、域名、代码风格进行画像留存。

安恒信息在鹏城国家实验室和广州大学的加持下，先后成功保障了第31届世界大学生夏季运动会、杭州第19届亚运会及杭州第4届亚残运会的网络安全，在面对大量网络攻击的情况下确保了赛事系统的正常运行。为了更好地应对赛事网络安全保障活动，作者根据多次国际体育赛事的保障经验，撰写了这本《体育赛事网络安全保障实践蓝皮书》。本书系统梳理了体育赛事网络安全的发展历程、国内外风险现状，以及全周期安全运营的理念和方法。通过深入分析亚运安全保障的具体实践，本书为读者提供了一套完整的体育赛事网络安全保障的理论框架和实践案例。

本书不仅是一本理论与实践相结合的专业书籍，更是体育赛事网络安全保障领域的一本重要参考资料。本书不仅为网络安全专业人员、体育赛事组织者、政策制定者提供了宝贵的参考，也为广大公众普及了体育赛事网络安全的重要性。随着信息技术的不断发展和应用，体育赛事网络安全保障的重要性日益凸显，希望本书的发布能够进一步推动体育赛事网络安全保障工作的深入发展，为未来的体育赛事注入更多的科技与安全力量。

目录

CONTENTS

体育赛事
网络安全保障实践
蓝皮书 > 2024

第一章
体育赛事信息安全发展背景

体育赛事信息化发展历程

自上世纪70年代以来，由IT技术引发的“第三次浪潮”席卷全球，对体育运动的影响日益强烈和深入，大型体育赛事信息设备和系统的建设成为必然。1972年的第二十届奥运会，因大量采用信息设备而名留史册。1992年巴塞罗那奥运会，开始引入成绩系统。瑞士天梭、法国源讯等都是国际大型赛事系统的技术解决方案提供商和集成商。例如：国际奥委会长期与源讯合作，从盐湖城冬奥会开始委托源讯统一负责IT信息化建设和成绩系统集成。近年来，借助举办杭州亚运会、成都大运会、陕西全运会以及广西学青会等大量国际国内综合性赛事，中国大型体育赛事信息服务业通过统一规划、高度模块化、集成能力强，且有利于业务流程优化再造的体育赛事信息化集成产品，已能更好的服务于体育赛事的竞赛、媒体、公众、指挥工作[1]。

信息化可以说是重大赛事的中枢神经，担负着比赛成绩的采集、整合、传输、发布工作，是赛事组织管理、指挥调度的重要技术手段。根据国际大体联（International University Sports Federation, FISU）、亚奥理事会（Olympic Council of Asia,OCA）等国际体育赛事管理机构发布的相关IT指导性文件，大型体育赛事信息系统主要由赛事成绩系统（Games Results System，GRS）、赛事管理系统（Games management system，GMS）、赛事支持系统（Games support system，GSS）三大系统组成，其中包括由竞赛报名系统（Sport Entries System，SES）、场馆成绩系统（Venue Results System，VRS）、中央成绩系统（Central Results System，CRS）、成绩发布系统（Results DistributionSystems，RDS）、竞赛视频系统（Competition Video Replay System，CVS）等子系统组成。场馆成绩系统由计时记分、成绩处理、技术统计、大屏控制、电视字幕、评论员等功能独立、数据互通的分系统构成。竞赛视频系统由仲裁录像、竞赛监控、竞赛闭路等分系统组成。云计算中心为信息系统提供计算、存储、网络出口等承载资源池。通信网络是信息系统采集、整合、发布信息数据的传输通道，主要包括竞赛专网、互联网、转播专网、设备网和物联网。

随着体育赛事的信息化程度越来越高，人们可以通过网络了解赛事，参与赛事；当代体育赛事的竞赛、媒体、公众服务与信息化已密不可分，体育赛事的成功举办离不开信息化的深度应用。然而，信息化技术在服务赛事的同时也有可能被不法份子利用，从而损害公共利益和破坏赛事安全、平稳运行。由此可见，对于体育赛事信息化网络安全的保障要求也越来越高。

[1] 赵海军 大型体育赛事场馆成绩系统方案设计与实现[D].北京：北京邮电大学计算机学院软件工程专业，2011:21-23.

国家监管层面的安全要求

重要性方面，2013年11月，习近平总书记在关于《中共中央关于全面深化改革若干重大问题的决定》的说明中指出“网络和信息安全牵涉到国家安全和社会稳定，是我们面临的新的综合性挑战。”2014年2月，中央网络安全和信息化领导小组宣告成立，习近平总书记亲自担任组长，再次指出“没有网络安全就没有国家安全，没有信息化就没有现代化”，反映出网络安全工作的极端重要性、紧迫性。2015年9月，习近平总书记在会见出席中美互联网论坛双方主要代表时指出“从老百姓衣食住行到国家重要基础设施安全，互联网无处不在。一个安全、稳定、繁荣的网络空间，对一国乃至世界和平与发展越来越具有重大意义。如何治理互联网、用好互联网是各国都关注、研究、投入的大问题。没有人能置身事外。”2016年4月，习近平总书记在网络安全和信息化工作座谈会上的讲话指出“我们一定要认识到，古往今来，很多技术都是‘双刃剑’，一方面可以造福社会、造福人民，另一方面也可以被一些人用来损害社会公共利益和民众利益。从世界范围看，网络安全威胁和风险日益突出，并日益向政治、经济、文化、社会、生态、国防等领域传导渗透。”之后多次在高层级会议上针对国家网络安全工作做出重要指示。

政策法规方面，2016年11月，第十二届全国人大常委会第二十四次会议通过《中华人民共和国网络安全法》，自2017年6月1日起施行，指出“国家建立和完善网络安全标准体系”、“国家实行网络安全等级保护制度”。2019年5月，国家市场监督管理总局、中国国家标准化管理委员会发布《信息安全技术　网络安全等级保护基本要求》（GB/T 22239-2019），自2019年12月1日起施行。2019年10月，第十三届全国人大常委会第十四次会议通过《中华人民共和国密码法》，自2020年1月1日起施行。2021年6月，第十三届全国人大常委会第二十九次会议通过《中华人民共和国数据安全法》，自2021年9月1日起施行。2021年8月，第十三届全国人大常委会第三十次会议通过《中华人民共和国个人信息保护法》，自2021年11月1日起施行。2021年4月，国务院第133次常务会议通过《关键信息基础设施安全保护条例》，自2021年9月1日起施行。

随着信息化需求、设备、系统、网络规模的不断扩大和网络空间的一体化趋势，针对大型体育赛事网络安全的管控也愈加复杂。

中央网信办明确指出网络安全是事关国家安全的重大战略问题。信息安全与信息化技术的发展同等重要、相辅相成，信息安全和信息化是一体两翼，驱动之双轮，必须统一谋划，统一部署，统一推进，统一实施。

赛事与信息安全的关系

网络安全建设是维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展的需要。信息安全是赛事举办的重要保障，作为举世瞩目的体育赛事，网络安全形势复杂，主要面临以下五类网络安全风险，一旦出现数据篡改、数据泄露、勒索病毒等网络安全事件，轻则影响办赛形象，重则直接导致赛事无法顺利举办。需通过构建安全组织体系、安全技术体系和安全管理体系，建立权责清晰、分工明确、运行规范、监管有力的工作机制，形成合规、稳定、可靠的网络安全保障体系，建设一体化全天候网络安全屏障，实现赛前、赛时、赛后全方位的网络安全保障，为赛事成功举办保驾护航。

（一）国家间网络战愈演愈烈

世界正迎来百年未有之大变局，国际形势错综复杂，国家间的网络战争从未停止。互联网的便利在强化全球交流的同时，也引发了国家、民族间的文化交流冲突。体育赛事期间，相关信息系统及关键信息基础设施会成为重点攻击对象。

（二）境外敌对势力逢喜必闹

境外反华势力具有“逢喜必闹”的特点，多次针对我国重大活动发起网络攻击，甚至以重金悬赏方式企图对我国实施干扰，达到其卑劣目的。

（三）专业黑客组织攻击破坏

国内外存在着多个恶意黑客组织，一般都具有较强的技术实力、较严密的组织和较强的攻击能力。这些黑客组织或受极端思想侵害、或受非法利益驱动，经常在世界各国举办重大活动期间发起破坏性网络攻击，甚至投送专业网络攻击武器开展攻击活动。体育赛事关注度高、影响范围大，遭受攻击破坏的风险加大，需要对专业黑客组织团队进行重点防范。

（四）恶意网络攻击异常活跃

互联网每天存在大量尝试性攻击，这些攻击行为大部分无固定目标，每当新漏洞或新的利用方法出现时，网络攻击将明显上升，异常活跃。攻击者多为互联网漏洞探测平台，利用特定漏洞批量入侵。体育赛事信息系统庞大，技术复杂，存在大量的脆弱点，防御难度高，必然成为恶意网络攻击的重点攻击对象。

（五）网络黑产活动日益加剧

受巨大利益驱使，具备一定技术的个人或团体利用互联网谋取不正当利益，通过网络攻击获取目标数据，并通过利益关联的产业链进行变现，谋取非法所得，部分黑产使用暗网形成交易链。大型体育赛事信息敏感，数据价值高，极易成为网络黑产活动的精准攻击对象。

在此环境下，构建一个合规、有效的网络安全防护体系，在安全运营基础上，确保赛事信息化业务的连续性以及发生网络安全事件后的快速研判、处置能力，已成为体育赛事举办机构和安全服务商共同实现的目标。

体育赛事
网络安全保障实践
蓝皮书 > 2024

第二章
体育赛事安全保障国内外风险现状

网络安全建设是维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展的重要举措。国际性、综合性体育赛事网络与信息系统安全是赛事举办的重要保障，需通过构建安全组织体系、安全技术体系和安全管理体系，建设一体化全天候网络安全屏障。

为防止网络及信息系统遭到恶意的（包括并不限于）拒绝服务、数据篡改与泄露以及设施破坏等攻击，保障体育赛事网络与信息系统的可用性、完整性与保密性。需结合业务需求，通过网络安全技术防护手段及安全管理措施，并遵循国家相关法律法规的要求，例如《中华人民共和国网络安全法》、网络安全等级保护2.0体系、关键信息基础设施相关保护条例等。同时，使网络与信息系统符合相关体育赛事国际组织的业务系统安全要求来设计安全防护方案。

国外赛事信息安全案例

2012年伦敦奥运会，开幕前东欧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40分钟大规模DDoS攻击，但未成功。2016年里约奥运会，APT28组织对奥运会相关的反兴奋剂组织发起了攻击，获取并公开该组织账号、运动员测试结果、相关人员隐私等数据；出现大量针对奥运会的邮件欺诈、网站篡改及仿冒、伪造Wi-Fi网络、勒索病毒的网络安全事件；针对奥运会相关网站、巴西和里约政府相关网站、赞助商相关网站的DDoS攻击，流量高达300～500Gbps。2018年平昌冬奥会组委会受到网络安全攻击导致WI-FI无信号，场内数千台电视机黑屏，安检门失效，12个冬奥会设施开始瘫痪，冬奥会官方客户端以及购票系统无法接入等严重网络安全事故。2021年5月，为应对东京奥运会期间可能出现的网络攻击，日本国家网络安全中心召集约170位安全管理人员参与演习，但上述人员个人信息均遭泄露。从大型国际综合性运动会影响范围大、涉及国家多的大型活动特点看，络攻击态势呈现“逐届加剧，危害倍增”的趋势。

攻击即服务模式的风险

攻击即服务模式（Attack as a Service，AaaS）的风险加剧是一个严重的网络安全问题，给赛事带来了诸多挑战。这种模式允许攻击者以服务的形式提供恶意活动和攻击工具，使攻击变得更加简单和普及化。以下是一些攻击即服务模式带来的风险：

技术门槛降低：攻击即服务模式降低了网络攻击的技术门槛，使得即使是没有专业知识的攻击者也能利用这些服务发动攻击。这导致了攻击的频率和规模的增加。

扩大攻击范围通过攻击即服务模式，攻击者可以更容易地接触到各种攻击工具和恶意软件，从而能够针对不同的系统和应用程序展开攻击。这增加了受攻击的目标范围，包括个人、场馆和赛事组织机构。

提高攻击效率：攻击即服务模式提供了成熟的攻击工具和基础设施，使攻击者能够更快速、更有效地发动攻击。这增加了防御的难度，因为安全团队需要迅速应对不断变化的威胁环境。

匿名性和追踪困难：攻击即服务模式通常提供匿名性，使攻击者难以被追踪和定罪。这增加了攻击者的嚣张气焰，降低了他们发动攻击被发现的风险。

为了应对攻击即服务模式带来的风险，以下是一些建议：

提高安全意识：加强员工的安全意识和培训，使他们能够识别和应对网络攻击。培养一种安全文化，鼓励员工报告可疑活动和威胁。

强化安全防护措施：采用多层次的安全防护措施，包括入侵检测系统、防火墙、反病毒软件等，以检测和阻止潜在的攻击。定期更新和升级安全设备和软件，以应对新的威胁和漏洞。

威胁情报共享：与其他组织和企业建立威胁情报共享机制，及时交换有关网络攻击的情报和最佳实践。通过合作和信息共享，共同应对网络安全挑战。

加强法律执法力度：加强网络安全法律法规的制定和执行，打击网络犯罪活动。加大对攻击即服务模式的打击力度，追究攻击者的法律责任。

研发新技术和解决方案：投入更多的资源研发新的网络安全技术和解决方案，以应对不断变化的网络威胁环境。利用人工智能、机器学习和大数据分析等先进技术来检测和预防网络攻击。

总之，攻击即服务模式的风险加剧是一个紧迫的网络安全问题。通过提高安全意识、强化安全防护措施、威胁情报共享、加强法律执法力度和研发新技术等手段，可以更好地应对这一挑战，保护赛事的网络安全。

应用上云带来的安全挑战

因赛事需确保数据的安全性和可靠性，以避免数据泄露、篡改或丢失等风险。同时，由于云作为赛事应用集中承载资源池的的性质，云安全解决方案还需要考虑到网络攻击、DDoS攻击、恶意软件等网络安全威胁。以下是针对赛事的云安全挑战与解决方案的一些建议。

虚拟化环境的安全性

虚拟化是云计算的核心技术之一，但虚拟化环境安全性却是一个重大挑战。虚拟机之间的隔离和访问控制需要得到充分的关注和管理，以防止未经授权的访问和数据泄露。

虚拟化环境的安全性是一个重要问题，因为虚拟化技术广泛应用于赛事基础设施中，以下是一些与虚拟化环境安全性相关的考虑因素：

虚拟机的隔离：确保虚拟机之间的适当隔离是维护虚拟化环境安全性的关键。虚拟机之间的隔离可以防止潜在的攻击者从一个受损的虚拟机扩展到其他虚拟机或宿主机。

虚拟化管理程序的安全性：虚拟化管理程序（Hypervisor）是虚拟化环境的核心组件，其安全性至关重要。必须确保虚拟化管理程序本身没有漏洞，并采取适当的安全措施，如访问控制和安全更新。

资源分配和管理：虚拟化环境中的资源分配和管理也可能对安全性产生影响。必须确保虚拟机的资源分配受到限制和监控，以防止资源耗尽或拒绝服务攻击。

数据保护和加密：在虚拟化环境中，数据保护和加密也是重要的安全性考虑因素。应采取适当的数据保护措施，如磁盘加密和备份，以保护虚拟机中的数据。

访问控制和监控：实施严格的访问控制和监控机制，以确保只有授权的人员能够访问和管理虚拟化环境。这包括对虚拟机的创建、修改和删除等操作进行监控和审计。

安全更新和漏洞管理：及时应用安全更新和修复漏洞是保持虚拟化环境安全性的关键。应定期检查和更新虚拟化环境中的组件，包括虚拟化管理程序、操作系统和应用程序。

物理安全性：虚拟化环境的物理安全性也需要注意。应确保虚拟化环境的物理访问受到限制，并采取适当的安全措施，如物理安全控制和机房安全。

需要注意的是，虚拟化环境的安全性是一个复杂的主题，具体的安全策略和控制措施应根据云上承载应用的业务逻辑和风险状况进行定制。

数据安全

运动员和观众的数据需要进行加密和保护，以避免数据泄露和篡改。云安全解决方案需提供强大的数据加密和保护措施，包括数据备份、恢复和访问控制等。同时，需确保云资源池满足严格的数据保护政策和合规性要求。具体来说，数据安全包括以下几个方面：

数据加密：通过加密算法和密钥对数据进行加密，确保数据在传输和存储过程中不被未经授权的人员获取。

访问控制：设置访问控制策略，限制对数据的访问权限，确保只有授权人员能够访问和操作数据。

数据备份：定期对重要数据进行备份，以防止数据丢失或损坏，并确保在需要时可以恢复数据。

安全审计：对数据进行安全审计，发现和记录数据的访问、修改和删除等操作，以便及时发现和处理安全事件。

防止恶意攻击：采取必要的安全措施，如防火墙、入侵检测系统等，防止恶意攻击和数据泄露。

合规性：遵守相关的法律法规和标准，如《 数据安全法 》等，确保数据的合法性和合规性。

网络攻击

赛事可能成为网络攻击的目标，因为攻击者可以通过网络攻击获取敏感信息、干扰比赛结果或进行恶意宣传等。云安全解决方案需要提供实时监测、防御和响应机制，以应对各种网络攻击。同时，需确保云资源池具备强大的网络安全防护能力和经验。云计算网络攻击的挑战可以归纳为以下几点：

多样化的攻击途径：在云计算环境，攻击者可以从多个方面入手，如虚拟机的操作系统、网络设备、云中间件、云服务等等，呈现出多样化、变异性、模式化的趋势。

复杂的云安全管理：由于云计算环境的多样化和复杂性，安全策略及其管理难度大大增加。如何正确地配置云系统，选择适当的安全策略并建立有效的安全体系结构，将云环境下的复杂安全问题切实解决，成为了需要攻克的难题。

API 漏洞和违规：很多应用程序中，API安全性通常都落后于Web安全应用程序，这使公共开发人员和合作伙伴可以进入其应用程序的生态系统和软件平台。事实证明，API安全是最薄弱的环节，它可能导致原生云威胁，并使用户的隐私和数据面临风险。

管理和访问控制问题：在云计算环境中，管理和访问控制是两个重要的安全问题。用户可能希望在云端保留对数据的完全控制权，同时还需要确保云服务提供商能够提供必要的安全措施来保护数据。

综上所述，云计算网络攻击的挑战包括多样化的攻击途径、复杂的云安全管理、API漏洞和违规、管理和访问控制问题的挑战以及不断变化的威胁环境等多个方面。为了应对这些挑战，云服务商需采取综合性的安全措施，包括加强网络安全防御、建立完善的安全管理制度、使用加密技术和安全访问控制等措施来保护云计算环境的安全。

DDoS攻击

DDoS攻击是一种常见的网络攻击方式，通过发送大量无用的请求来耗尽服务器的资源，使其无法响应正常的请求。云安全解决方案需要提供专业的DDoS防御服务，以保护赛事的网站和服务器免受攻击。云计算环境面对DDoS攻击的挑战主要来自于以下几个方面：

大规模流量攻击：DDoS攻击可以通过制造大量的网络流量来淹没目标服务器，使其无法响应正常请求。云计算平台需要具备足够的网络带宽和防御能力来应对这种大规模的流量攻击。

多样化攻击方式：DDoS攻击可以使用多种方式来攻击目标，如UDP洪水攻击、TCP洪水攻击、ICMP洪水攻击等。云计算平台需要具备识别和防御这些不同类型攻击的能力。

伪造IP地址：DDoS攻击可以使用伪造的IP地址来隐藏攻击者的真实地址，这使得追踪和防御攻击变得更加困难。云计算平台需要具备识别和防御这种伪造IP地址的能力。

加密流量攻击：DDoS攻击可以使用加密流量来隐藏攻击内容，这使得传统的防御手段无法有效防御。云计算平台需要具备解密和分析加密流量的能力，以应对这种加密流量攻击。

混合攻击：DDoS攻击可以与其他类型的攻击相结合，如SQL注入、XSS等，以实现更复杂的攻击。云计算平台需要具备应对这种混合攻击的能力。

管理和访问控制问题：在云计算环境中，管理和访问控制是两个重要的安全问题。用户可能希望在云端保留对数据的完全控制权，同时还需要确保云服务提供商能够提供必要的安全措施来保护数据。

虚拟化技术的挑战：虚拟化技术是云计算的核心技术之一，但也带来了新的安全挑战。例如，虚拟机可能遭受更严重的攻击，因为它们共享物理资源并处于同一网络中。

为了应对这些挑战，云计算平台需要采取综合性的安全措施，包括加强网络安全防御、建立完善的安全管理制度、使用加密技术和安全访问控制等措施来保护云计算环境的安全。同时，也需要不断更新安全策略和技术来应对不断变化的威胁环境。

恶意软件

恶意软件可能会感染赛事信息化设备，从而获取敏感信息或者进行破坏活动。云安全解决方案需要提供恶意软件检测和防御服务，以保护设备和数据的安全性。云计算恶意软件挑战主要体现在以下几个方面：

感染范围扩大：由于云计算环境的共享性和开放性，恶意软件可以在云内部快速传播，并感染更多的虚拟机和应用程序。这增加了恶意软件的感染范围和传播速度，使得清除和隔离恶意软件变得更加困难。

持久性攻击：一些恶意软件采用持久性攻击策略，在云环境中长期潜伏，并等待合适的时机进行攻击。这些恶意软件可以逃避常规的安全检测，并在云环境中长期存在，对用户数据和系统安全构成长期威胁。

攻击向量化：云计算恶意软件可以利用云环境的复杂性和多样性，从不同的角度和层面进行攻击。例如，它们可以利用虚拟机之间的通信、API接口、容器化环境等进行攻击，增加了防御的难度和复杂性。

为了应对这些挑战，云计算平台需采取一系列安全措施，包括加强恶意软件的检测和防御能力、建立完善的安全管理制度、加强数据保护和访问控制、提高用户的安全意识和培训等。同时，云计算平台也需要不断更新和升级安全技术和策略，以应对不断变化的威胁环境和攻击手段。

身份验证和授权

需对云上网站和服务的用户进行身份验证和授权，以确保只有合法用户能够访问敏感信息和进行相关操作。云安全解决方案需要提供强大的身份验证和授权机制，包括多因素身份验证、访问控制和权限管理等。云计算身份验证和授权的挑战主要包括以下几个方面：

多租户环境：云计算平台通常采用多租户模式，即多个用户和组织共享相同的物理和逻

辑资源。在这种环境中，如何确保每个用户只能访问其被授权的资源，避免数据泄露和非法访问，是一个重要的挑战。

动态性：云计算环境具有高度动态性，虚拟机、容器和应用程序可能随时创建、销毁或迁移。这要求身份验证和授权机制能够适应这种动态变化，实时更新访问控制策略，并确保正确的权限管理。

跨域访问：云计算环境中可能存在多个安全域，用户可能需要在不同的安全域之间进行访问。如何确保跨域访问的安全性，实现单点登录和统一的身份管理，是一个具有挑战性的任务。

复杂性和可扩展性：云计算环境可能包含大量的用户、资源和应用程序，因此需要建立一个可扩展的身份验证和授权机制，以支持大量并发请求和高性能需求。同时，这种机制还需要足够灵活，以适应不同组织和用户的需求。

标准化和兼容性：云计算平台可能需要与其他系统和服务进行集成，如第三方应用程序等。这要求身份验证和授权机制具备标准化和兼容性，能够与其他系统无缝对接。

安全性：身份验证和授权机制本身需要足够安全，能够抵御各种攻击，如密码猜测、重放攻击、注入攻击等。此外，还需要保护用户的隐私信息，避免数据泄露和滥用。

针对应用上云带来的安全挑战，需要采取综合的云安全解决方案来确保安全性和可靠性。这包括虚拟化环境安全防护、数据加密、网络攻击防御、DDoS防御、恶意软件检测、身份验证和授权以及安全审计和监控等方面的措施。

攻防变迁带来的新举措

深化威胁情报分析 实时监测网络攻击

由于网络攻击的特殊性、隐蔽性、复杂性，依赖于特征库的安全防护设备，无法有效快速应对零日攻击和APT攻击，为此需做好威胁情报收集工作，将收集到的情报通过智能分析与人工分析，分析完成后调整安全防护设备策略，实现从被动防御到主动防御，保障赛事网络安全。

1）及时发现、识别网络攻击威胁，监测黑客组织、不法份子等的攻击活动、攻击行为、攻击方法手段。

2）通过内置的策略库对拒绝服务恶意脚本、SQL注入攻击、特殊字符URL访问、可疑HTTP请求访问、BashShellShock漏洞、Nginx文件解析漏洞、文件包含漏洞、LDAP漏洞、Struts2远程代码执行漏洞等全量威胁进行识别。

3）对重点保护对象网络、系统、大数据等安全状况，除通过内置的策略库进行定期识别外，还应组织网络安全专家通过人工渗透测试方式，对其安全性进行检验。

4）具备文件沙箱功能，发现网络文件中的恶意行为，通过内部虚拟机实现完全模拟真实桌面环境，发现所有恶意文件的注册表行为、敏感路径操作行为、进程行为、导入表信息等，综合分析这些恶意行为，实现对未知威胁的攻击行为的识别。

5）通过历史流量数据、日志文件和告警数据，对用户进行分析，建模和学习，构建出用户在不同场景中的正常状态并形成动态基线。

总之，威胁情报分析是预防和处理网络攻击的关键。通过实时监测、处理网络攻击、共享情报和提高技术防御措施等手段，可以有效地保护赛事的网络安全，减少潜在的损失和风险。

重视泛在网络安全 强化敏感数据保护

物联网作为一种泛在网络，其设备在赛事中的应用越来越广泛，例如计时记分设备、智能场馆、智能健身器材等。然而，物联网设备的安全问题也随之凸显。以下是一些物联网设备在体育赛事中的安全问题及相应的风险管理措施：

数据泄露和隐私保护：物联网设备采集和处理大量个人数据，包括运动员的生理信息、位置信息、比赛数据等，如果数据未得到妥善的保护，可能会导致个人隐私泄露。风险管理措施：加强数据加密和访问控制，确保只有授权人员可以访问敏感数据。同时，定期进行数据安全审计和检查，及时发现和处理数据安全问题。

设备安全和漏洞利用：物联网设备可能存在安全漏洞，如操作系统漏洞、通信协议漏洞等，攻击者可以利用这些漏洞对设备进行攻击和控制。风险管理措施：对物联网设备进行安全漏洞检测和修复，确保设备的安全性。同时，采用安全的通信协议和加密技术，防止攻击者窃取和篡改数据。

拒绝服务攻击（DDoS攻击）：攻击者可以通过攻击物联网设备，使其无法正常工作或响应请求，从而造成拒绝服务攻击。风险管理措施：在物联网设备上安装防护软件和DDoS防御系统，防止攻击者利用漏洞进行攻击。同时，定期对设备进行安全检查和维护，确保设备的正常运行。

数据篡改和完整性保护：物联网设备采集的数据可能会被篡改或破坏，从而影响数据的完整性和可信度。风险管理措施：采用数据加密和完整性校验技术，确保数据的完整性和可信度。同时，定期对数据进行审计和检查，及时发现和处理数据篡改问题。

总之，物联网设备在体育赛事中具有广泛的应用前景，但同时也存在一定的安全风险。针对不同的安全问题采取相应的风险管理措施，可以有效地保护物联网设备和数据的安全性。

关注视频媒体安全 内容保护与反盗版

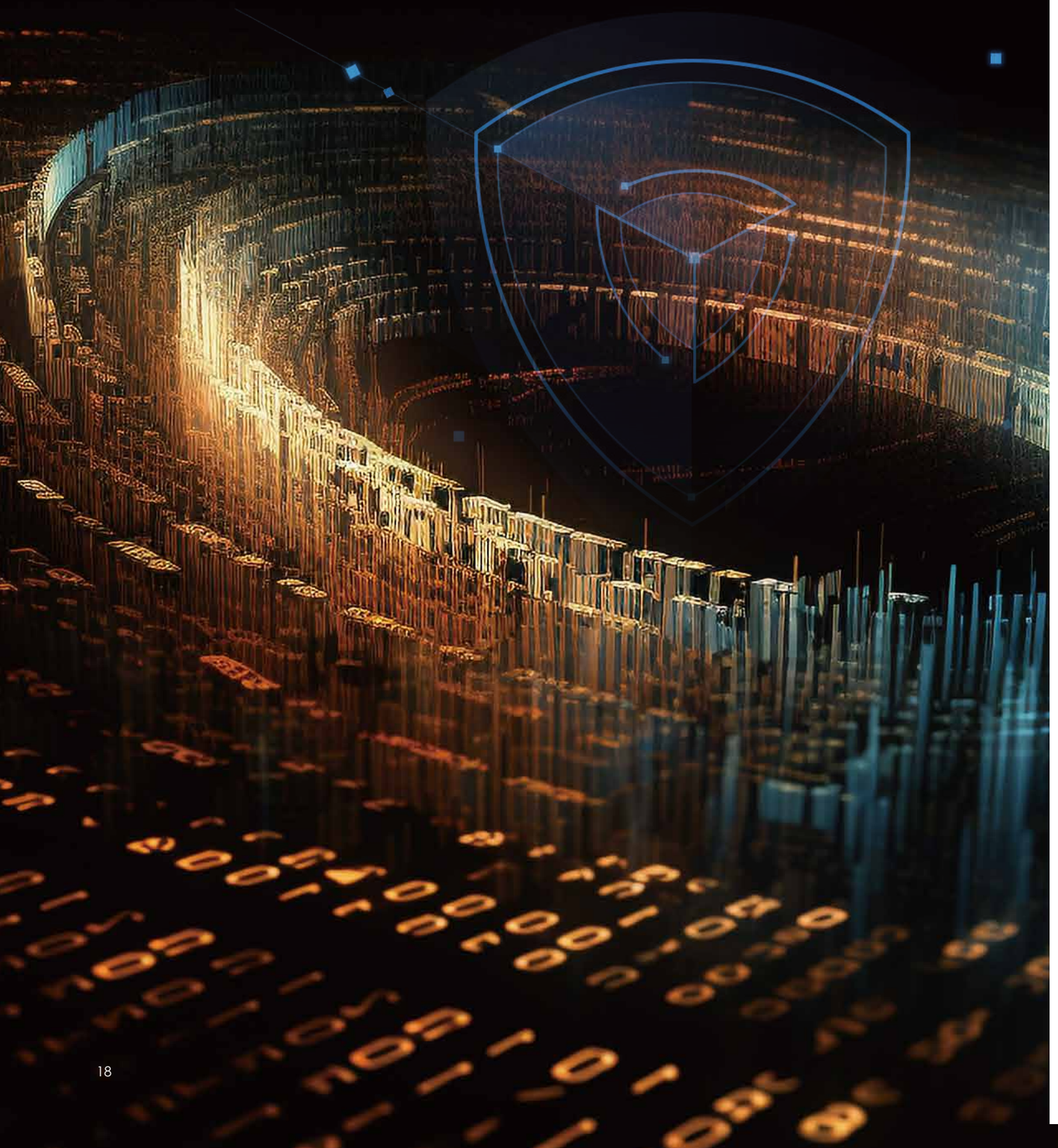
赛事视频媒体的安全问题受到高度关注，主要从视频内容保护和反盗版等两方面进行保护。

视频内容保护

视频加密技术：对赛事视频进行加密处理，确保只有授权用户才能正常观看。使用强密码和密钥管理，防止未经授权的访问。

数字版权管理（DRM）：采用数字版权管理技术，对视频内容进行保护，限制非法复制、分发和共享。通过许可证管理、内容加密和跟踪等技术手段，确保视频内容的合法使用和传播。

访问控制和身份验证：设置严格的访问控制策略和身份验证机制，限制未授权用户对赛事视频的访问。采用多因素身份验证方法，提高账户的安全性。



反盗版措施

水印和追踪技术：在视频中添加独特的水印，以便追踪和识别盗版视频的来源。结合数字指纹技术，为每个正版视频分配独特的标识符，用于快速比对和溯源。

版权声明和宣传：在视频播放前或播放过程中，添加版权保护声明，明确告知观众不得盗版和传播未经授权的视频内容。同时，加强版权知识的宣传和教育，提高公众对版权的认识和尊重。

法律制裁和维权：积极配合国家版权局和其他相关机构，打击网络侵权盗版行为。通过法律途径追究盗版者的责任，维护赛事视频的合法权益。

合作与共赢：与媒体、合作伙伴和观众建立良好的合作关系，共同维护赛事视频的版权。鼓励正面的社交媒体分享和传播，与观众互动并回应用户反馈，共同打造良好的网络版权环境。

实时监测与应对：利用威胁情报分析工具和实时监测技术，对网络上的盗版行为进行监测和识别。一旦发现盗版链接或侵权行为，立即采取措施进行清除和维权。

建立举报机制：设立专门的举报渠道，鼓励观众积极举报盗版行为。对举报属实的观众给予一定的奖励，提高公众参与打击盗版的积极性。

综上所述，赛事视频流的安全需要从多个方面进行保护，包括视频内容的加密、数字版权管理、访问控制和身份验证等。同时，加强反盗版措施，如水印和追踪技术、版权声明和宣传、法律制裁和维权等也是非常重要的。通过综合应用这些措施，可以有效地保护赛事视频的安全和版权，维护相关方的合法权益。

在合规性要求基础上，为应对赛时攻防对抗、实时响应网络安全事件，体育赛事网络安全保障应从运营体系搭建、大数据资产管理、安全验证、场景化预警模型、风险态势管理及研判指挥模式等全周期安全运营的重点方向，建立起全场景、智能化的网络安全防护体系。

体育赛事
网络安全保障实践
蓝皮书 > 2024

第三章
体育赛事全周期安全运营

安全保障理念

传统的体育赛事的网络安全保障以前期的网站安全性测试发现问题为主，即通过渗透测试及时发现网站的漏洞并进行修复，而网络安全保障不仅仅是事前的防护，更应该注重事中时的防护以及事后的分析。因此，针对体育赛事网络安全保障的理念是“自卫模式”、“护卫模式”和“迭代模式”相结合的全方位立体式防护体系。其中，自卫模式是一种以自保为目的的守护防御模式，通过安全策略构建基本安全基线，通过防御系统保护系统安全，并通过灾难恢复守住安全底线。自卫模式通过在事前采取措施，采用漏洞挖掘、基线检查和风险评估等方法发现安全问题，采取加固措施减少攻击面，并借助护网演练以发现新的安全漏洞及脆弱点，力求提前消除隐患。同时通过自行防御，采用如拟态防御、可信计算等“以内生安全技术为主”的方法，保护系统自身不被攻击者发起攻击威胁。事后采用系统冗余、数据备份、应用灾备等方法及时恢复系统和数据，力保减少损失。 护卫模式是以反击为目的的主动防御模式，其以感知检测为基础，通过分析研判发现潜在攻击，最终提前对攻击进行拦截。盾立方是一种典型的护卫模式，其中“四蜜” 通过布陷探察，采用网络拌线、系统拌线等感知检测技术构造网络诱骗环境，用于捕获有助于攻击研判的“蛛丝马迹”。其中“关联研判”基于MDATA认知模型将不同来源的威胁数据进行关联分析，通过数据中台将由各渠道所捕获的“威胁情报”统一汇聚，采用碰撞、关联、聚合等方法，通过MDATA认知模型进行协同分析，及时掌握和发现威胁态势及攻击源头。之后通过渗透清除、访问控制、边界防御和网络治理对攻击来源进行层次式阻击拦截，实现应急响应。迭代模式是一种分析复盘并不断提升防御能力的模式，利用攻击间隙期间进行复盘，发现攻击者蛛丝马迹，标注和更新威胁数据。迭代模式的核心是根据攻防对抗过程中所遗留或泄露的信息来进行防御策略的调整，并迭代增强防御体系。

安全保障框架

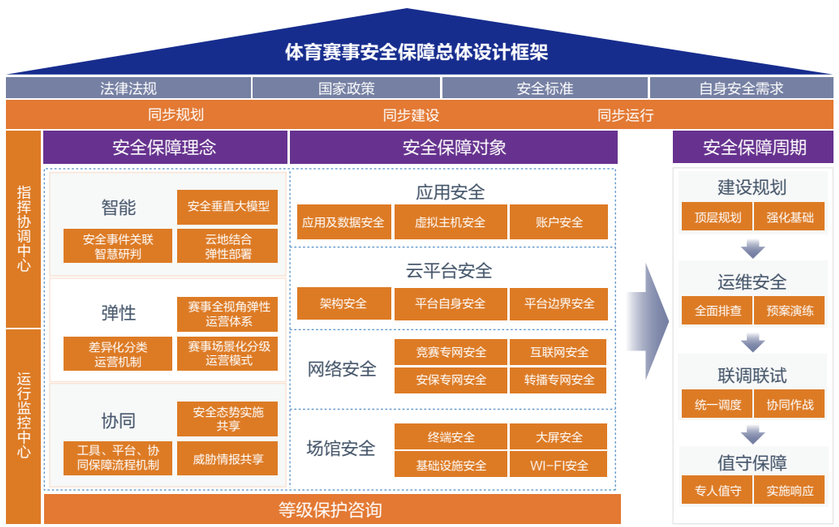


图3-1 安全保障框架

体育赛事安全应遵从法律法规、国家政策、相关安全标准及赛事自身安全需求，坚持同步规划、同步建设、同步运行的原则，以保障赛事相关业务应用如竞赛系统、竞赛服务相关系统、云平台、竞赛网络、场馆安全为目标，安全建设符合等级保护相关要求，强化运行监控、指挥协调、威胁监测、应急处置能力，整体安全事务贯穿赛事建设安全，运维安全、联调联试、值守保障全过程的安全保障总体设计框架。

安全保障关键设计维度

以风险为导向设计安保生命周期

图3-2 安全保障生命周期示意图

体育赛事整体安全保障工作遵从“同步规划、同步建设、同步运行”的原则；整体安全保障工作以赛事生命周期划分为建设规划、安全运维、联调联试、赛事运行保障四个阶段组成。

建设阶段主要以符合赛事业务的网络安全顶层规划设计，强化网络安全基础能力建设，确保体育赛事整体网络安全工作规划设计、安全建设统一规范和要求。

运维阶段主要以建设完成后的运维工作为主，突显赛事网络安全风险排查、建立突发安全事件应急响应处置流程机制与预案演练为主，检验各场馆、赛事服务相关系统安全建设成果和威胁对抗演练的能力。

联调联试主要是模拟体育赛事正式场景，检验赛事运行过程中统一调度、协同作战工作机制的实现情况，同时也是对整体网络安全工作进行查漏补缺，确保正式赛事网络安全保障工作具备全面性风险防控能力。

保障阶段主要是实行专人专岗，对各场馆、竞赛服务系统开展实时的安全监测、风险分析、应急响应及处置，确保赛事保障期间万无一失。

以交付标准化积累安保实施指南

体育赛事网络安全保障工作建设阶段按照整体赛事的系统性支撑资源可分为云平台安全建设、竞赛系统安全建设、竞赛场馆和非竞赛场馆安全建设四个主体部分组成。

建设阶段

图3-3 建设阶段主要实施内容

云平台安全建设

云平台是承载体育赛事运行系统的基础平台，其安全性保障是整体赛事系统网络安全的重要工作之一。由于除了竞赛系统之外还有支撑赛事周边工作的系统会部署在云平台上，因此需要按照系统功能类型和重要程度进行安全区域划分，同时对各系统网络边界进行整合，确保云平台上系统网络边界清晰，所有赛事相关系统都已经被纳管和安全防护。

为确保云平台及系统安全，需要针对云平台及系统被访问方式或路径的安全策略进行设置和部署安全防护能力，并对安全策略和防护能力进行安全评估，确保云平台安全防护策略有效和云平台安全性可控。

云平台的安全关系到整体竞赛信息化安全，整体建设过程需要按照

其重要程度和安全等级保护建设要求进行规划建设，需要通过专业的安全咨询团队进行安全等级建设咨询，并通过备案、测评和等级保护认证，确保其安全能力符合等级保护要求。

需要对云平台整体网络架构进行安全评估，评估网络架构逻辑性安全和防护安全，评估内容包括是否根据系统重要程度和安全级别进行分区分域管理，是否整体网络安全防护能力符合既定的网络安全等级保护级别。

需要对云平台上所有资产进行核查，梳理资产目录、 明确资产责任人，并形成资产清单，并确定所有资产都已经被安全纳管。

需要对云平台及云上系统开展上线前的安全评估工作，安全评估包括不限于安全扫描、渗透测试、后门检查、代码审计等，并对安全检测及评估发现的问题完成整改，在通过上线前的评估后，云平台和云上系统才允许正式上线。

需对云平台及云上系统开展安全可信众测服务，检测云平台及云上系统整体安全防护能力的有效性和自身应对威胁的健壮性，针对众测发现的问题需完成整改工作。

需对云服务、系统服务、赛事承办方等相关人员开展安全培训工作，培训不限于国际国内网络安全形势、赛事网络安全建设、赛事安全注意事项、日常工作网络安全意识等内容。

竞赛系统安全

竞赛系统是体育赛事信息化工作开展的基础支撑系统平台，其包括不限于赛事成绩、赛事指挥、赛事管理、赛事服务等系统平台。竞赛系统的安全决定整体赛事过程的安全，因此在竞赛系统规划建设过程就应该重点关注，需要针对赛事系统的建设开发过程制定安全编码规范，对赛事系统的业务安全、开发框架、业务逻辑进行安全评估，同时对应用进行安全测试和对赛事系统平台代码进行安全审计，针对测试评估和审计发现的问题需要完成整改工作，以确保赛事相关系统的安全性。

竞赛场馆安全

竞赛场馆是指涉及开展体育赛事项目活动的场馆，针对竞赛场馆需根据其赛事的业务特性制定一馆一册网络安全建设方案。

各竞赛场馆承建方根据一馆一册要求，完成竞赛场馆的基础设施安全、竞赛专网安全建设，按照安全配置规范完成场馆设备、系统的安全策略配置工作，根据竞赛场馆重要程度，开展网络安全等级保护建设咨询、备案、测评和认证工作，需对场馆网络安全建设成果进行安全评估和WIFI接入安全进行测试，针对测试评估发现的问题需完成相关整改工作。

非竞赛场馆安全

非竞赛场馆是指未涉及具体体育赛事项目活动的如“开幕式场馆、闭幕式场馆、媒体中心、运动员村”等场馆，针对非竞赛场馆需根据其开展业务特性和功能用途情况制定一馆一册网络安全建设方案。

各非竞赛场馆承建方根据一馆一册要求，完成非竞赛场馆的基础设施、互联网安全建设，按照安全配置规范完成场馆设备、系统的安全策略配置工作，根据非竞赛场馆重要程度，开展网络安全等级保护建设咨询、备案、测评和认证工作，需对场馆网络安全建设成果进行安全评估和WIFI接入安全进行测试，针对测试评估发现的问题完成相关整改工作。

运维阶段

运维阶段标志着竞赛信息化网络安全建设工作已经基本完成，因此需要对竞赛信息化包括云平台、赛事相关系统、场馆等网络安全建设整体情况进行安全检测评估，并需要针对突发的情况开展应急预案的制定和演练，以检验网络安全工作团队应对突发安全事件的应急响应能力。

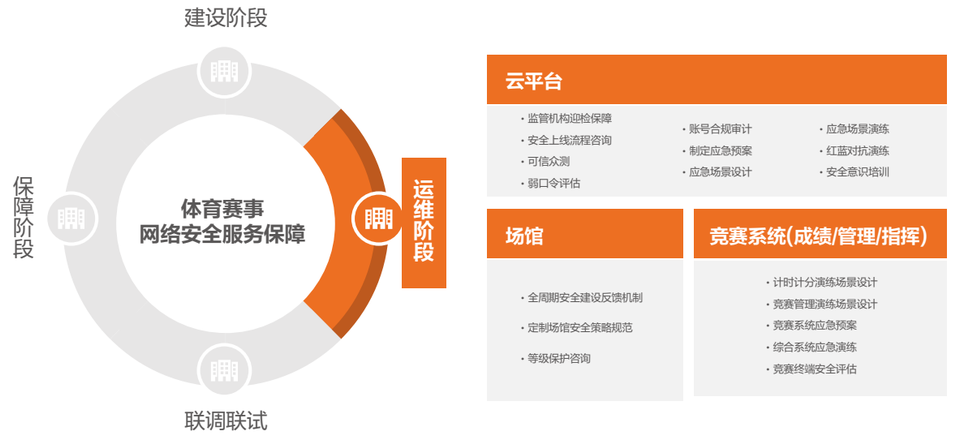


图3-4 运维阶段主要实施内容

云平台

云平台是体育赛事运行的关键信息基础设施平台，云上部署了竞赛信息化系统和官网、志愿者管理系统、抵离系统、智慧医疗等竞赛服务相关应用系统，这些系统的安全、稳定性关系着赛事相关项目的正常开展，为确保云平台及云上赛事相关系统的安全，监管机构如公安、网信等部门会对云平台及云上系统的安全情况开展全面的安全检查评估工作，云平台和竞赛相关系统的承建方及赛事安全服务团队需要积极配合监管机构的安全检查评估工作，并针对监管机构检查评估发现的问题及时完成整改工作。

为确保云平台及云上系统的安全需建立系统上线安全管理流程和机制，确保上线系统都是通过安全评估，明确开放服务端口、所需资源等情况下才允许部署至云平台运行。

上线后的云平台及云上系统需要持续性的开展可信众测服务，通过多轮的安全众测才能将漏洞更全面的发现和降低云平台及云上系统的风险，以确保云平台的整体安全性。

运维阶段需要对各竞赛相关系统的账号、密码进行审计，确保各竞赛相关系统用户账号的合规性和账号密码不存在弱口令情况。

云平台正式上线后需要针对云不同场景应急响应和处置工作制定应急预案，并开展各场景的应急演练工作，演练方式包括不限于模拟环境、桌面推演、真实环境攻击演练和红蓝对抗演练等，针对演练中发现的问题及时调整和修订应急预案，并及时修复发现的漏洞。

运维阶段需针对云上系统相关承建商、运维服务商以及竞赛服务周边系统服务相关机构开展安全意识培训，包括日常运维工作注意事项、安全意识能力提升等培训，以确保各方遵守网络安全合规要求和正确应对突发的安全事件的应急响应处置机制。

场馆

随着进入运维阶段各场馆承建方也将逐渐完成场馆的建设工作，场馆承建方对于场馆的安全建设情况需要实时上报给体育赛事组办机构，以确保场馆安全建设情况符合体育赛事组办机构提出的安全要求。

由于不同场馆的赛事相关项目特殊性存在不一样等情况，需要针对不同场馆开展定制化的安全策略，各场馆按照定制化的安全策略规范开展场馆的安全建设和策略配置工作，以确保场馆安全建设符合既定赛事相关服务项目的安全需求。

场馆承建方需要结合本场馆开展赛事相关服务项目的重要性，组织完成场馆等级保护定级备案、测评、认证相关工作，确保场馆安全符合等级保护相关要求。

竞赛系统

竞赛系统上线进入运维后，需针对竞赛成绩(计时记分)系统、竞赛管理等竞赛相关系统不同突发应急场景设计相应的应急处置预案，并组织开展应急演练工作，针对演练过程发现的问题及时完成整改和预案的调整工作。

竞赛终端主要包括接入竞赛专网的PC终端、移动终端，需要针对竞赛终端的安全进行评估，确保竞赛终端接入安全以及终端自身的系统安全，针对评估过程发现的安全问题，竞赛终端相关方需完成安全问题的整改，并针对同一问题需同步至其他场馆竞赛终端进行检测和问题的整改。

联调联试

图3-5 联调联试阶段主要实施内容

云平台

联调联试在模拟正式赛过程中，场馆会根据赛事服务需要开通必要的安全策略，这会涉及云平台及竞赛相关服务系统策略的开通和调整问题，为保障赛事正常开展和安全运行需要，需要根据赛事服务情况梳理安全策略。

联调联试主要以模拟正式开赛情况，检验云平台、场馆、竞赛系统、工作人员等各项赛事相关的组成部分统一运行有效性情况，安全值守是保障赛事正常运行必不可少的组成部分，安全值守人员需要根据联调联试工作要求对云平台、场馆、竞赛系统运行相关的网络安全情况进行实时的监测，同时开展云平台及云上系统的网络安全攻防应急演练工作，并将联调联试发现的问题进行记录和整合，方便后续完成相关问题的解决和整改，确保赛事过程的安全稳定性。

转播专网

联调联试中转播专网搭建完成后，需要对转播专网的建设情况进行安全评估，对评估发现的安全问题需要及时完成整改，以确保转播专网的安全性；需根据转播专网不同应急场景设计应急处置方案，并组织开展应急演练工作，根据演练发现的问题进行整改，并完成应急预案的修订工作。

竞赛场馆

联调联试过程需要安排专人进行安全值守，以保障模拟赛事过程的网络安全。联调联试需要对竞赛场馆的竞赛专网安全防护能力进行评估，确保场馆竞赛专网的安全，避免非赛事相关的设备接入场馆竞赛专网和非赛事相关内容流转进竞赛专网。

联调联试过程需对大屏幕系统进行安全评估，确保大屏系统的接入安全，需对大屏系统非必要蓝牙、红外等无线接口关闭，封闭USB端口，避免大屏因不可控等因素造成非既定信息的大屏展示。

联调联试需要对成绩系统进行穿行测试，检验成绩系统的计时记分、成绩管理的准确性和有效性情况。

需要对WIFI接入认证进行安全测试，确保WIFI接入认证符合安全要求，并对WIFI接入进行穿行测试，确保WIFI接入符合既定的设计要求。

联调联试过程需开展竞赛场馆侧互联网、竞赛专网等其他专项网络安全攻防应急演练工作，并将联调联试发现的问题进行记录和整合，方便后续完成相关问题的解决和整改，确保赛事过程的安全稳定性。

非竞赛场馆

非竞赛场馆涉及如“开模式、闭幕式、媒体中心、运动员村、指挥中心”等其它场馆，这些场馆在未完成相关项目服务的结束情

况下，是持续开放运行状态，需要安排人员驻守开展日常的安全值守和安全巡检工作，以保障场馆的安全、稳定性。

联调联试需要对非竞赛场馆的互联网安全防护能力进行评估，评估内容包括不限于互联网接入方式，分区分域管理、边界防护能力、互联网访问、发布内容等，以确保场馆互联网的安全。

联调联试过程需对大屏幕系统进行安全评估，确保大屏系统接入安全，必要时大屏系统须关闭蓝牙、红外等无线接口，封闭USB端口，避免大屏因不可控等因素造成非既定信息的输入和展示。

需要对WIFI接入认证进行安全测试，确保WIFI接入认证符合安全要求。

部分非竞赛场馆会涉及到信息发布等互联网系统，需要对互联网系统进行安全评估，系统承建方须针对安全评估发现的问题完成整改工作，以保障非竞赛场馆的互联网系统安全性。

联调联试过程需开展非竞赛场馆侧互联网等其他专项网络安全攻防应急演练工作，并将联调联试发现的问题进行记录和整合，方便后续完成相关问题的解决和整改，确保赛事过程的安全稳定性。

保障阶段

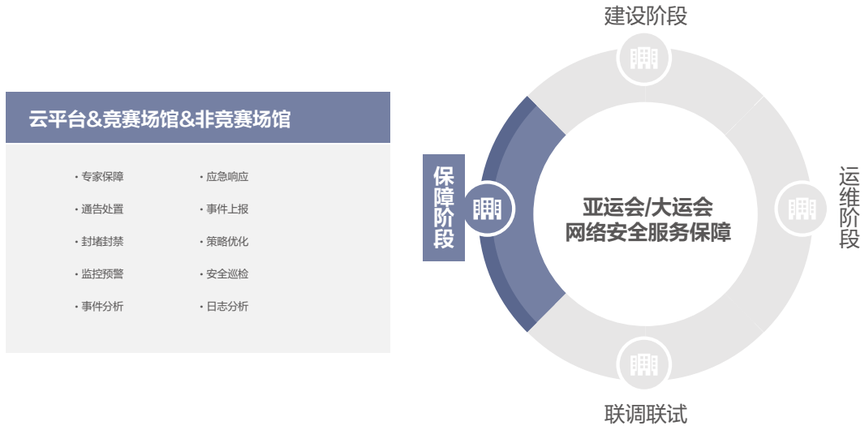


图3-6 赛时阶段主要实施内容

赛事实战保障阶段各场馆均需派驻安全专家进行值守，以至场馆赛事工作完全结束闭馆，安全专家才能撤场。

赛事实战保障阶段需按照建立的监控预警、通告处置、事件上报、应急响应等赛事突发安全事件应急响应流程机制，应对突发的安全威胁并进行应急响应和风险处置工作。

云平台值守专家团队对云平台及云上系统进行7*24小时的安全值守和风险监测工作，一旦发现云平台或云上系统出现威胁情况，通过专家组分析确定是威胁IP或将造成恶意攻击事件等情况，立即通告给相关竞赛服务系统承建商进行处置，或立即采取封禁封堵恶意IP的方式进行处置。

各场馆安全值守专家根据赛事时间安排，需全程实时监控场馆网络安全风险情况，对风险事件进行分析、响应和处置，以确保场馆侧网络安全。

云平台、各场馆需安排专人进行赛事相关系统平台、设备场地的安全巡检工作，定期查看日志分析系统发现的异常情况，根据诊断和处置情况，及时调整并优化安全策略，以保障云平台、云上系统、各场馆网络安全。

以能力即服务发挥快速响应处置

能力包括：大语言模型、MSS能力

结合网络安全行业攻击威胁大数据，构建具备实时自动化机器学习的大语言模型和多元化网络安全威胁场景，借助AI大数据分析网络安全攻击威胁关联性数据链矩阵，检测来自内外部网络安全攻击态势，助力研判真实网络安全攻击行为，为阻断赛事网络安全攻击威胁发挥快速响应处置提供能力支撑，为体育赛事网络安全保障工作提供能力即服务的新网络安全服务模式。

借助完善的MSS安全托管运营服务能力，通过云端安全服务专家团队结合专业技术平台和工具以标准化流程对体育赛事相关网络系统资产的安全风险和安全威胁进行集中研判、快速预警、统一指挥、紧急处置、追查反制，实现事前预警、事中监控、事后响应，快速规范化解决安全问题，力求安全问题闭环管理，持续迭代提升和输出整体安全能力，保障体育赛事业务安全、稳定运行。

拟战演练落实赛事人员技能基线

针对赛事安全保障人员全面开展安全意识培训，对核心运营保障人员进行上岗培训，基于安全操作手册规范运营保障动作。通过多轮安全演练，不断调整优化技术体系、运营管理制度以及人员组织结构。

在赛事安全保障的规划阶段，充分分析在运营过程中人员协作、安全意识等方面的问题，梳理管理与改进清单，制定管理、技术、人员三方面的解决方案。

制度侧，在备战期间开展系列应急演练、针对不同场景的保障工作进行人员响应能力与协作性检验，持续改进并固化制度流程，确保规范性与有效性。

人员侧，对管理、运维、安保等不同团队编写相关培训与操作手册，并开展多样化的场景故事推送，强化安保人员的的安全意识与运营保障能力。

技术侧，深度参与各层次、各级别攻防演练，以实战检验技术能力与人员能力水平，经过各类演练提升人员的实战能力。

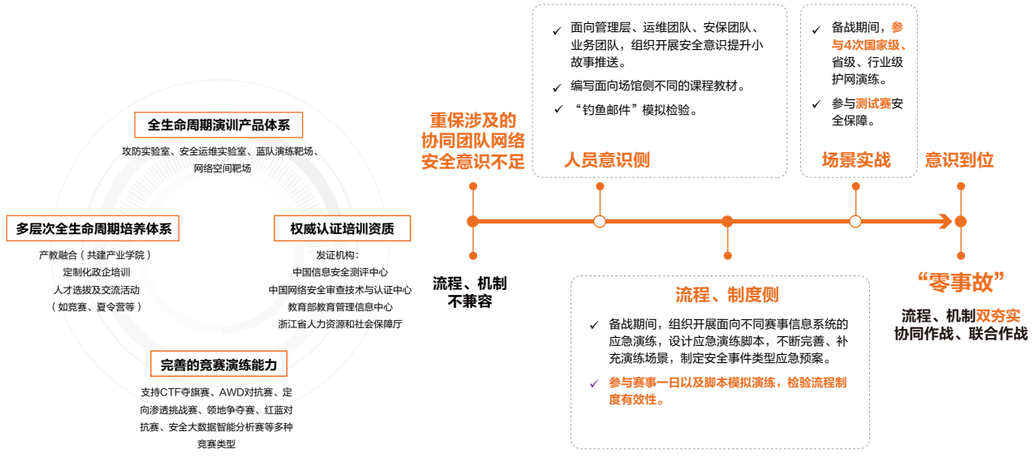


图3-7 多维度安保技术人员培养机制

安全保障核心安全技术

四蜜威胁探测

四蜜威胁探测是体育赛事信息系统威胁感知的核心技术之一。针对现有威胁探测手段在应对未知安全威胁面临“捕不全”、“拦不住”、“看不清”、“抓不到”等问题，使用“四蜜”威胁探测体系，采用护卫模式在信息系统外部建立威胁感知能力。如下图所示，在不影响赛事信息系统前提下，通过蜜点（威胁感知）、蜜庭（前置探测）、蜜阵（协同联动）、蜜洞（溯源威慑）在攻击者潜在攻击路径上进行动态地部署陷阱、诱饵，实现布陷感知、逐层感知的目的，基于网络诱骗实现全面、快速、准确的攻击威胁探测效果。

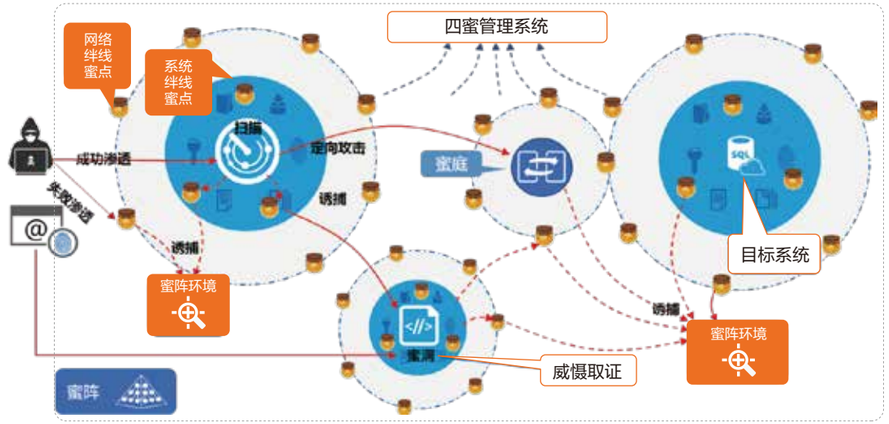


图3-8 四蜜威胁探测架构-原图-广州大学团队

基于网络和系统纵线的蜜点技术

为快速全面探测网络威胁，面向攻击者进入体系赛事信息系统前和进入信息系统后两个阶段，分别采用网络纵线蜜点和系统纵线蜜点，形成纵深威胁感知体系。网络纵线是指大量部署于网络中攻击者可能攻击路径上的“自动触发器”。系统纵线是指精心设计部署在系统中的不会被正常用户使用的“暗功能”，二者一旦被攻击者触碰即可引爆，即可暴露攻击者行为。

蜜点工作流程如下：首先，基于被保护目标系统所处的网络、系统、应用等环境，构建高逼真网络纵线蜜点和服务纵线蜜点。其次，基于冷启动技术生成网络纵线蜜点和系统纵线蜜点部署方案，以使得攻击者具有很高概率触碰蜜点。然后，根据所处环境的不同，如云环境和物理网络环境，为蜜点申请和配置所需资源，按照部署方案对蜜点进行部署和启动，同时，实时监测和处置蜜点可能被攻击导致的内容篡改。最后，蜜点运行过程中将采蜜行为全流程记录，并提交关联研判分析处置。

基于服务前置和信任判别的蜜庭技术

针对通过大量外部隐匿IP绕防安全网关难以探测的问题，采用基于服务代理的蜜庭前置服务技术及前置访问观测方法。面向未知访问请求，构建通用和定制化的服务代理，基于服务代理对访问过程行为和数据进行观测跟踪及引流。基于观测数据，采用IP信任判别方法对未知访问进行信任判别和处置，从而有效探测利用大量IP来隐匿攻击意图的攻击行为。

蜜庭支持串接、假名和旁路三种部署方式。蜜庭串接部署是指蜜庭直接部署在被保护系统前，作为前置代理所有访问被防护系统的流量均首先经过蜜庭观测；蜜庭假名部署是指蜜庭采用旁路方式作为被保护系统的前置代理，采用假名（如虚假域名）对外提供真实服务，即用户可通过正常路径访问被保护系统，也可能通过假名来访问被保护系统，通过假名访问系统的用户一般为攻击者。蜜庭旁路部署是指蜜庭通过旁路方式代理蜜点或蜜罐，利用虚假业务从而观测攻击者行为。

蜜庭工作流程如下：首先，确定蜜庭部署方式，基于不同部署配置蜜庭，并进行部署；然后，对于流经蜜庭的流量采用黑白名单、行为观测分析、IP信誉评估等方法进行判断，若判断为黑则直接处置，若判断为白则放行，若判断为灰（可疑者）通过引流方式将可疑访问者引入蜜阵，由蜜阵提供孪生业务，再次过程中不断观测可疑访问者的行为，从而准确判断其行为；最后，蜜庭将访问IP、行为等信息进行记录，并将日志上送给关联研判分析处置。

支持协同联动的蜜阵技术

对体育赛事的产生交大安全威胁的多为隐蔽、未知攻击行为，蜜阵通过对蜜点、蜜庭、蜜洞的协同联动，提升对攻击者对抗能力，探测攻击者隐蔽行为。蜜阵作为四蜜体系内部数据研判分析模块，一方面研究面向蜜点和蜜庭的集中管理方法，进一步研究统一命名和解析方案和配置管理；另一方面，研究协同联动的机理、优化“阵图”部署，形成全网全方位协同探测感知能力。

蜜阵工作流程如下：首先，在四蜜部署段，由蜜阵作为管理中心进行蜜点、蜜庭、蜜洞的配置和部署任务下发；其次，启动蜜点、蜜庭、蜜洞后，将日志上送给蜜阵，由蜜阵进行综合分析，如IP信誉判别、攻击类型分析统计等；再次，根据日志统计情况，展开四蜜节点威胁探测效能分析，基于分析结果进行四蜜节点动态变换。

基于浮动代码的蜜洞技术

传统防御系统主要防范攻击行为而非攻击者，攻击成本和代价较低。针对缺乏有效手段甄别攻击者身份，无法有效震慑攻击者的问题。蜜洞研究浮动代码构造技术、浮动代码精准投递技术及持续粘随威慑技术通过浮动代码投递对攻击者进行多阶信息采集和匹配，并进行非法访问行为阻断，形成持续性攻击监测处置威慑，有效粘随威慑攻击者。

蜜洞工作流程如下：蜜洞可部署部署在被保护系统内部或与蜜点、蜜庭结合部署，当攻击者访问被保护系统关键资源或者踩入蜜点、蜜庭时，则蜜洞对攻击者投递浮动代码，以获取攻击者信息，攻击者可以被检测到。

关联分析研判

关联分析研判是保障体育赛事全周期安全运营的核心安全技术之一。关联研判主要针对各种网络安全防护设备、威胁感知系统等捕获的威胁情报，采用探针为点以聚合、聚点成线以碰撞、联网结面以关联、协感构体以研判的联动模式，基于MDATA认知模型对威胁情报进行表示、获取及分析利用，以递进方式分析研判攻击者。

MDATA认知模型

网络安全事件具有典型的巨规模、演化性、关联性三大特性，全面、准确、实时研判网络安全事件极具挑战。MDATA（Multi-dimensional Data Association and intelligent Analysis，多维数据关联与智能分析）认知模型从人类认知方法的时间、空间及其相互关联维度出发，对人类认知网络安全事件的过程进行建模，实现了网络安全事件的全面、准确、实时研判，支撑网络空间安全事件的三大属性，是网络空间安全领域的首个认知模型。

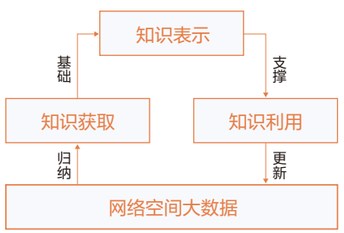


图3-9 MDATA认知模型的系统框架

如上图所示，MDATA认知模型包括三个组成部分：是从语义、时空和关联维度对网络安全知识进行表示和管理，知识获取是基于多维度、多来源、多模态的网络空间大数据获取时空、关联的网络安全知识，知识利用是采用大图计算等方法，对网络安全事件进行全面、准确、实时研判。

MDATA认知模型的工作流程如下：首先基于采集的各类网络空间大数据，利用知识归纳算子对已知的网络安全知识进行抽取；知识表示和管理则对抽取的知识进行高效表示，形成网络安全知识库，并通过多种索引方式提升其检索效率；MDATA知识表示方法具备可理解、可计算的特性，能支撑知识演绎算子推演出未知的网络安全知识，对已有的网络安全知识库进行完善和更新；知识表示和管理支撑各种图计算、雾云计算架构的知识利用。MDATA认知模型是一个活化模型，通过知识表示与管理、知识获取、知识利用以及反馈和迭代，持续更新和完善网络空间安全知识，支撑网络安全事件的研判。

威胁数据表示、采集与管理

为对攻击者进行关联分析研判，需要采集各种类型的网络空间大数据，并对威胁数据进行统一表示、采集与管理。在数据源方面，主要包括部署于系统与网络中的各类型安全防护设备，包括但不限于防火墙、流量探针、EDR（Endpoint Detection and Response）、IDS（Intrusion Detection System）等，同时包括四蜜系统部署的蜜点、蜜庭、蜜阵、蜜洞等探察设备。这些不同的探测来源称为探察点，即探针为点，不同类型探针对被保护范围进行监测，以感知和发现攻击行为或异常行为，并将这些数据进行上传分析。

由于不同类型探察点捕获的数据格式各异，首先需要对威胁数据进行统一表示。基于MDATA认知模型的表示能力，首先确定关联分析相关的核心安全要素，对资产、漏洞、攻击行为以及其对应的时间、空间关联关系进行统一表示。然后对四蜜系统、安全防护设备产生的日志进行高效采集与知识获取，通过抽取其核心安全要素，如IP、告警描述等，基于核心安全要素对各种类型的数据进行归并、融合、去除冗余信息等处理。最后，采用图数据库对各种类型的威胁数据进行存储和管理，并构建时间索引、空间索引、时空联合索引，支撑网络安全数据的高效查询和关联分析。

攻击行为融合与碰撞

攻击者在发起攻击时会经常变换自身所利用的IP以及其攻击手法、攻击工具等，仅依靠单点探针难以检测和发现攻击者的攻击链路，无法有效研判攻击者的意图。为及时检测形态易变的复杂攻击事件，需在同一管辖域内将各种探针中的异常情况进行碰撞和并线研判，即聚点成线，包括不同地址的相似行为、相同地址在不同探针中的行为、不同地址的时序关联行为登，以碰撞出攻击者的攻击行为链路。

基于单点威胁数据进行攻击行为碰撞时，首先根据核心安全要素对MDATA知识库中的单步攻击数据进行关联融合，包括攻击者IP、攻击工具、关联域名等；然后基于攻击链路、IP特征、IP行为模式等对攻击者的同源性分析，即对攻击者IP进行聚合；最后根据网络安全知识库中已知攻击的检测模板，以及融合以后的威胁数据，利用子图匹配等技术进行攻击检测，以内网IP为基础，实现各辖域内攻击链路的准确检测。

网间威胁关联与挖掘

随着网络安全事件出现跨域跨网等特性，实现全网攻击检测需要在不同的管理域间进行网间威胁情报共享，形成关联面，以判断是否存在具有关联性的攻击操作与行为。在跨网复杂攻击IP地址变换频繁、全域复杂攻击隐蔽性强的情况下，需要对不同子网内的威胁行为进行关联和挖掘，即联网结面，基于网间行为关联分析攻击者的同源性，并基于融合的威胁情报检测全网可能存在的复杂攻击。

进行网间威胁挖掘时，首先根据各子网中攻击者IP的历史行为进行关联分析，综合考虑如系统行为、设备型号、端口、网络协议、操作系统等基础信息，结合攻击平均时间间隔、时间间隔方差、载荷平均大小、连接请求个数、攻击类型占比、攻击频率和威胁评级等深层信息，从不同粒度对攻击者IP进行特征聚类，实现攻击者同源IP的聚合；在此基础上，融合不同子网的威胁数据以及开源的威胁情报，结合子网间攻击序列的时序、空间约束关系，基于攻击检测模板的图匹配技术实现跨域跨网的全网复杂攻击检测，对复杂的攻击者、攻击组织的攻击链路进行分析，支撑对攻击者的研判分析。

立体协同交互与决策

实现主动式立体防御体系需要构造“协同感知”的威胁情报中心，通过各点、线、面以MDATA认知模型定义的统一表示形式，向威胁情报中心提交网络威胁情报，来构建全网威胁情报知识库，即协感构体，支撑多层次立体协同的交互式智能决策。

在进行攻击画像和交互式决策时，首先构建威胁情报的MDATA本体模型，从蜜点、蜜庭、蜜阵、蜜洞的“四蜜”体系和“点-线-面”攻击研判威胁数据中抽取出资产、漏洞、攻击等知识；然后利用知识融合与知识更新技术构建面向国家、省市等不同层次的全域MDATA知识库，并对安全知识进行高效存储与管理；最后根据威胁情报知识进行大数据关联计算，提供IP威胁、IP类型等多维度IP画像，并提供威胁情报查询接口供子网实时分析与研判使用，从而结合IP关联查询和IP画像研判结果支持交互式决策。

网络空间测绘

体育赛事信息系统网络安全保障仅依赖被动获取攻击者访问时威胁情报不足以有效支撑研判分析，需要进一步展开主动网络空间测绘，通过对可疑IP展开多维度主动威胁情报采集和分析，从而主动发现可疑IP的异常属性。网络空间测绘以网络空间资源为探测对象，采用

网络探测、网络分析、实体定位、地理测绘和地理信息系统等技术进行分析，获得网络空间实体资源和虚拟资源在网络空间的位置、属性和拓扑结构等情报信息，通过将网络空间测绘结果与正常用户属性对比，从而快速、准确定位攻击者。

网络空间测绘工作方式可分为两类：一类采用实时运行方式，循环扫描全网IP地址以获取对应测绘信息；另一类采用按需测绘方式，当发现有可疑攻击IP地址时，启动网络空间测绘工具，获取对应的威胁情报。

面向主机类型的网络测绘

攻击者和正常用户在访问体育赛事信息系统时，所采用的主机类型往往存在差异。服务器长期稳定运行，计算及网络资源充足，在网络攻击中往往成为攻击跳板的首选，因此，攻击者往往采用受控服务器实施攻击，而正常用户则会采用个人主机访问系统。因此，对于可疑攻击IP，可通过反向测绘该IP是否为服务器，来判断可疑目标是否为攻击者。

面向主机类型的网络测绘以踩蜜或者触发防护系统告警的可疑IP作为测绘目标，采用多维度分析方法，通过主动探测获取目标操作系统版本、开放端口、支持服务、在线时长等信息，结合特定特征或者采用机器学习方法分析可疑IP是否为服务器。一旦判断可以IP为服务器，则可确定可疑IP为攻击者。

面向代理分析的网络测绘

攻击者在实施网络攻击时，为隐藏自己往往采用代理作为自己公开出口，即攻击者通过代发起网络攻击。以上情况使得在赛事网络安全保障活动中，存在大量非法的代理IP地址，给攻击关联研判带来了很大不便。因此，通过网络空间测绘技术展开代理分析非常重要。

面向代理分析的网络测绘技术以踩蜜或者触发防护系统告警的可疑IP作为测绘目标，采用主动、被动和情报库三类方式进行网络测绘。主动测绘通过主动探测获取目标操作系统版本、开放端口、支持服务等信息，结合特定特征采用机器学习方法分析可疑IP是否为代理。被动测绘结合蜜点在仿真页面加入浮动代码，被动等待攻击者踩入蜜点，一旦踩入蜜点则利用浮动代码提取攻击者本地真实IP信息，通过与踩蜜IP对比判断是否为代理。情报库测绘是指网络中存在一些情报库已经保存了IP地址的代理信息，通过查询威胁情报库，也可以获取IP地址代理。

自适应漏洞评估与分级

自适应漏洞优先级（AVPT）技术，结合资产部署环境、资产重要性、漏洞危害程度，重新调整漏洞危害评分，实现漏洞优先级的动态调整和个性化定制，典型扩展技术主要包括：基于基础漏洞信息AVPT评估技术、基于单应用漏洞链AVPT评估技术。

基于基础漏洞信息AVPT评估技术

通过“基于基础漏洞信息AVPT评估技术”，提供定制化的漏洞优先级管理方案，实现漏洞危害的全面评估与实时计算，带来高效、精确的漏洞管理体验，提高系统的整体安全性和稳定性。

定制资产优先级

“基于基础漏洞信息AVPT评估技术”允许我们根据资产部署环境和资产重要性等关键因素，重新调整漏洞的危害评分。我们的平台将根据客户的实际情况，为每个资产定制相应的漏洞优先级。这样，客户能够根据其资产的特点，优先处理最关键、最具影响力的漏洞，最大限度地降低潜在风险。

评估综合漏洞危害

在评估漏洞优先级时，综合考虑漏洞危害程度，结合漏洞攻击复杂度、影响范围、潜在后果对漏洞进行全面评估，确保漏洞优先级的准确性和可靠性，明确漏洞的实际威胁。

实时计算与评估能力

具备实时计算与评估漏洞危害能力，尤其是对于非公开的通用漏洞，即扫描器发现的漏洞，可以实时进行危害评分。实现漏洞评估产品能够处理大量漏洞数据并快速做出优先级排序，快速制定相应的安全策略和漏洞修复计划。

基于单应用漏洞链AVPT评估技术

通过"基于单应用漏洞链AVPT评估技术"，为漏洞管理和安全决策提供更深入洞察、关联分析、风险评估能力，全面透视漏洞链的构成和潜在风险，有效规避潜在的安全威胁，提升漏洞管理和安全决策的精确性和有效性。

快速构建可利用的漏洞链

借助"基于基础漏洞信息AVPT评估技术"的基础，可根据单个应用的已有漏洞信息，快速构建包含含历史漏洞与通用漏洞在内的可利用漏洞链，展现不同漏洞之间的关联性，更好掌握漏洞之间的关系，实现预警攻击者的利用漏洞行为。

综合评估潜在风险

进一步评估新发漏洞与历史漏洞存在组合利用的潜在风险，通过综合考虑不同漏洞链的组合情况，准确地量化潜在风险，有针对性地关注可能导致系统威胁的漏洞组合。

深入洞察系统安全

通过分析和评估漏洞链，掌握系统中潜在的攻击路径和薄弱环节，进而有针对性地加强防御措施，提高系统的整体安全性。

软件成分分析

软件成分分析技术实现智能组件分析及二进制0day风险检测，静态解析源代码、二进制文件及特征文件中的组件，采用机器学习技术，模拟开发过程中包管理的行为，通过算法、策略、模型，高效深层分析被软件引用的组件及漏洞，一站式完成风险分析、缺陷跟踪、风险复测。集成多类版本控制工具、构建工具、CI服务器及缺陷管理系统，在保持现有开发流程的前提下，与版本控制工具（如GIT仓库）无缝对接，分析风险后以缺陷管理平台（如禅道）进行风险跟踪，提供组件/漏洞修复建议，实现开发阶段的风险组件生命周期闭环管理。

结合最前沿的二进制逆向工程技术与源代码特征读取技术，模拟项目构建进行风险分析，融合开源组件分析、依赖解析、特征识别、引用定位等多种技术，实时匹配Maven等中央仓库中开源组件的已知漏洞风险（如部分0day），准确识别应用程序中已使用的易受攻击组件，提高漏洞验证效率，有效减轻开发人员工作量。

二进制0day风险检测

快速逆向和预处理二进制文件风险，基于Ghidra反编译能力，实现基于Ghidra ClangNode的逆向污点追踪算法，包含字符流和文件流，可跨N层函数。

供应链攻击检测

检测软件资产清单，建立企业内部软件源，基于关键特征和技术识别受损的应用或软件包，追踪风险制品包，从而判断制品包是否已被攻击者所控制，定位风险所在项目并预警。

敏感信息检测

高效检出代码中存在的敏感凭证、密钥、URL及IP等，如API keys等信息，确保代码库中没有开发人员遗留的潜在凭证数据或敏感信息，能够有效防止敏感信息意外提交。

镜像风险检测

为容器应用层提供全面的软件供应链安全防护措施，深层分析本地及仓库内镜像，涵盖镜像内组件风险、安全漏洞、合规许可、恶意文件、敏感信息等。通过多维度深度扫描发现不安全镜像，从源头上解决容器镜像安全问题。

组件资产清单管理

结合二进制逆向工程技术与源代码特征读取技术，自动分析软件开源组件，风险检测覆盖Java、C/C++、GO、Javascript、Python、C#、Ruby、PHP等编程语言开发的软件开源组件，二进制文件分析覆盖MIPS 32/64、ARM 32/64、AMD x86/x64、RISCV 32/64共8类系统架构。

快速风险分析

全视角展示受影响组件及应用软件信息，海量组件指纹库与漏洞库，结合多种技术分析引擎，自动化数据分析、清洗、匹配、关联，快速精准匹配风险信息，自动生成开源组件漏洞资产。

开源组件漏洞情报信息兼容通用漏洞披露（CVE）、国家信息安全漏洞库（CNNVD）、国家信息安全漏洞共享平台（CNVD）及多个开源社区漏洞信息等数据源。

知识产权风险评估

有效识别软件开发中所使用的开源软件清单，评估相关知识产权风险，明确对应的开源许可证及权利约束，包含其开源许可证的兼容性及合规性审核等，根据企业制定的许可证策略，评估存储在私服仓库的开源组件许可风险与外部组件的专利侵权风险。

深层依赖分析

精确定位应用开发中使用的开源组件版本，深层分析开源组件间的依赖关系，可视化呈现开源组件依赖分析流，追踪溯源开源组件漏洞的影响范围。

威胁情报

漏洞信息实时关联匹配至相关影响组件及应用，在软件成分列表中搜索漏洞名称即可确认受影响的开源组件及产品版本，提供组件详细信息与修复建议，便于安全人员及开发人员及时进行修复。

软件生命周期管理

集成Jenkins pipeline工作流框架，在pipeline测试流程中融入自动化软件成分安全测试，即在DveOps流程中加入安全测试，形成DevSecOps方案。

集成IDE开发环境，提供IDEA插件于编译环境实效检测代码安全，快速定位风险路径。持续集成发布部署，实现软件自动化构建测试与部署，将安全测试左移，尽早的发现、预防问题，以降低修复问题的成本，提高研发工程质量，让开发更加快捷方便。

在野零日漏洞狩猎

分布式漏洞发现与验证技术

采用分布式部署方式提升稳定性，扫描速度较传统技术提升30%，同时利用动态流量控制方式减少扫描动作对目标系统的影响。通过实时爬取网络漏洞的方式，进行每日自动更新，漏洞发现率和误报率性能改良需要掌握大量渗透测试技术、网络爬虫技术、流量控制技术以及代码语言特性的分析技术，壁垒较高，可替代性低。具备漏洞发现率高、误报率低、对目标系统运行影响低等特点，漏洞库量级与覆盖率实现业内领先，借助该技术已经多次在全球首先发现包括JAVA框架Struts2的S-045、S-046等在内的重大漏洞。

办公软件漏洞挖掘与检测技术

基于文件格式漏洞，可以有效挖掘如Office、WPS、PDF等办公软件漏洞，并对样本所使用的漏洞编号进行标定，应用与多类网关安全防护系统。通过研究已知办公软件漏洞所使用的技术，进行阶段性自动更新。

本地提权在野漏洞捕获与分析技术

通过静态方式精准扫描文件，规避了特定样本运行时检测逃逸的缺陷，极大提升本地提权在野样本的捕获成功率。利用此项技术已多次捕获如CVE-2021-1732、CVE-2022-28252、CVE-2023-37969等Windows本地提权在野零日漏洞，具备在野漏洞捕获效果好、资源开销少等特点。

网络协议漏洞挖掘技术

基于二进制漏洞方向的经验积累，通过动态模糊测试和静态代码审计的方式，提升网络协议类漏洞挖掘的效率，已发现多个影响Windows RDP协议等模块的重大漏洞，具备挖掘网络协议漏洞效果好、适用于不同网络协议漏洞挖掘等特点。

固件漏洞挖掘技术

涵盖嵌入式系统、计算机网络、操作系统、信息安全领域。一是通过静态分析技术反汇编固件代码来提取指令和指针，找出其中的漏洞，并进行深入研究。二是通过.动态分析技术（也称黑盒测试），检查设备的运行行为，动态分析固件运行状态，快速找出存在的漏洞，并提供有关其漏洞的详情。三是利用符号执行技术，基于符号自动创建程序输入，生成各种不同的输入可能性，来帮助挖掘和验证漏洞。四是利用模糊测试技术，生成大量随机的、无序的数据流，在固件漏洞挖掘中发挥重要作用。

安全保障技术特色

智能

安全垂直大模型应用

安全垂域大模型系统，秉承让安全更智能、让智能更安全的使命，依托底层多源异构模型、算法调度引擎及海量安全知识，结合大规模增量预训练与微调，具备恶意代码检测、威胁情报分析、自动化安全编排响应和安全教育等全方位安全能力。可根据体育赛事网络安全保障中各类业务场景需求从容切换多种安全角色，以扎实的安全基本功迎接未来无限可能。

垂域大模型基于通用大模型的训练与再训练，既具备通用大模型的原生能力，又具备安全垂域的专有能力，安全垂域大模型系统作为体育赛事本地化安全运营场景中的“AI Copilot”，可以辅助安全运营团队，构建全面的脆弱性评估能力、提升受赛事信息资产的安全韧性、提升安全事件研判与分析效能，打造体育赛事智能安全运营新场景，全面实现赛事安全运营与保障目标。

安全专家更标准化

通过大模型技术固化安全专家专业知识，以数字身份扮演安全运营角色，基于授权策略，实现全天候值守。将高级专家的专业知识固化到大模型中，可以让模型具备类似于专家的决策能力和运营经验。数字专家可以在安全运营中发挥重要作用，以其深入的行业知识和丰富的经验，在体育赛事安全保障过程中指导决策和行动。

告警清零更高效

基于智能分析与决策，可以有效提升恶意软件检测，攻击流量检测，端点异常行为检测，软件成分分析，钓鱼邮件识别，网页信息分析等速度和精准度。

隐患见底更准确

配合计划任务，关注安全漏洞、介入安全评估、参与渗透测试、审查网络架构、检查应用程序安全性、联动安全监测大规模降低隐患发生的机会和留存的时间。

事件闭环更敏捷

通过对事件全程跟踪，在卡点不断提供专家建议，关注状态和反馈，确保事件处置流程顺利进行和有效推进。

安全意识更深入

大模型系统可以化身成企业员工身边的AI助手，提供网络安全相关的知识科普，提醒常见的网络安全事件应对措施。也可以配合安全主管部门，开发相关的安全培训课件，生成各类相关教材资料。

云地结合的弹性部署模式

采用云端与赛事保障本地数据互通、工具联动、服务联动的方式，安全处置动作与数据信息上升至云端，云端情报与专家服务赋能至赛事安保本地。依据不同时期、不同事件、不同风险等维度设置完备的云地互通流程机制，针对不同保障场景实现弹性保障能力与资源互补。

技术工具层面结合：云端运营中心与本地运营平台、监测工具、处置工具实现联动对接，依据不同事件、脆弱性因素可通过云端运营下发处置策略，远程进行安全处置与防护。

服务体系云地融合：采用云端专家、本地安全服务人员三级服务架构体系，自上而下进行运营服务能力、安全运营工作指导赋能，针对本地服务资源不足或能力缺乏问题，可通过云端进行补充，实现运营服务资源与能力的弹性化。

海量事件自动关联智慧研判

建立态势感知平台、关联研判分析系统，落地体育赛事主动网络安全立体防御体系，应用威胁诱捕和关联研判网络安全数据分析与处置系统，有效支撑体育赛事的网络安全保障。在传统的网络安全保障活动中，攻击方和防御方往往存在攻防不对称的情况，攻击者以点攻面导致防御方处于弱势地位，新型威胁诱捕理念及系统，有效扭转了攻防双方地位，全方位、多层次、多粒度的威胁诱捕手段让攻击者难以成功实施攻击，在赛事保障活动中有效识别恶意IP。

传统的网络安全保障活动需要安全专家根据大量的网络安全数据进行综合研判，由于网络安全监测数据体量大、威胁数据来源多、

攻击行为隐匿强且变换快等特点，安全专家往往需要投入大量时间和精力进行综合分析。利用创新的关联分析理念及系统，将不同来源的威胁数据采用MDATA认知模型进行统一表示与管理，包括威胁诱捕系统日志、防火墙日志、入侵检测系统告警、上网行为管理系统日志等，聚点成线，利用MDATA模型的分析能力，将攻击者的行为和路径进行碰撞，有效识别针对体育赛事信息系统的高危复杂攻击行为，并结合历史网络安全保障活动的威胁情报，结网成面，对攻击者的目的、方法、路径等进行综合研判，大幅度提升了网络安全保障活动的分析和处置效率。体育赛事主动网络安全立体防御体系实现了针对攻击者的主动检测与关联分析，将“被动监测到响应”的安全流程提升到“预警到主动反制模式”，通过攻击画像和攻击者图谱，将攻防对抗左移至业运安全边界外部，真正实现了体育赛事安全保障快速处置流程。

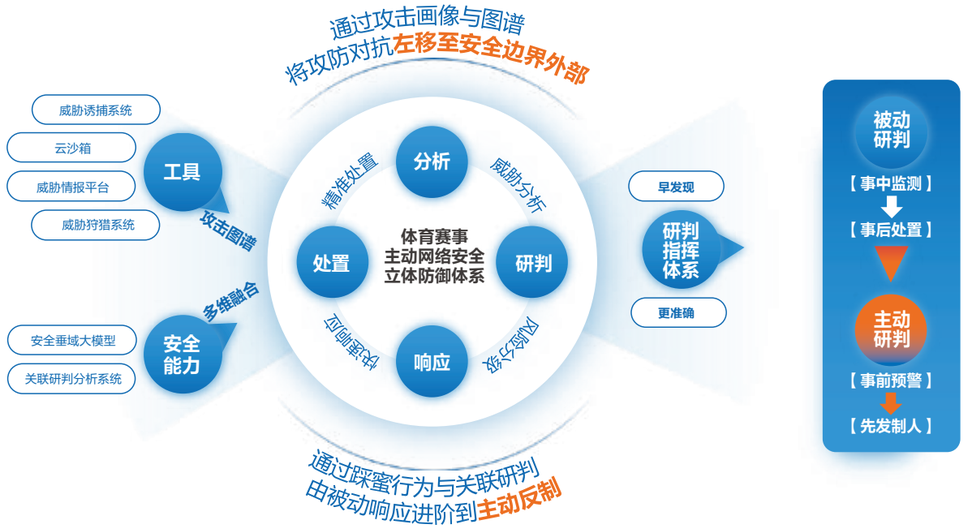


图3-10 研判指挥体系

弹性

构建赛事全视角弹性运营体系

共生安全理念，回归安全本质，结合体育赛事安全保障目标与风险状态，提供贴合业务形态、IT架构等方面，最原生、最根本、最可靠安全能力。通过与安全运营体系进行共生融合，构建基于场馆侧、赛事侧、供应链侧三类场景的个性化、规模化、轻量化全视角弹性运营体系。

规模化运营：即以赛事信息系统、官网等为保护核心，确保体育赛事业务安全稳定，并对各类场馆进行安全监管与赋能。组织上定位指导，赛事侧安全运营在保障强度、人员规模、安全要求方面最高且更加完善。

个性化运营：即以各类场景作为安全运营保障核心，针对场景级别、信息系统数量、功能定位等确立不同运营级别与工具、人员、流程等内容，确保运营保护需求与场馆定位相一致。

轻量化运营：即以体育赛事供应链作为安全运营保障核心，其中包括软件维度供应链、重要供应商维度供应链。针对软件供应实现上线前的整体运营管控，对重点供应商进行远程安全监测与处置，规模供应链带来的赛事网络安全风险。

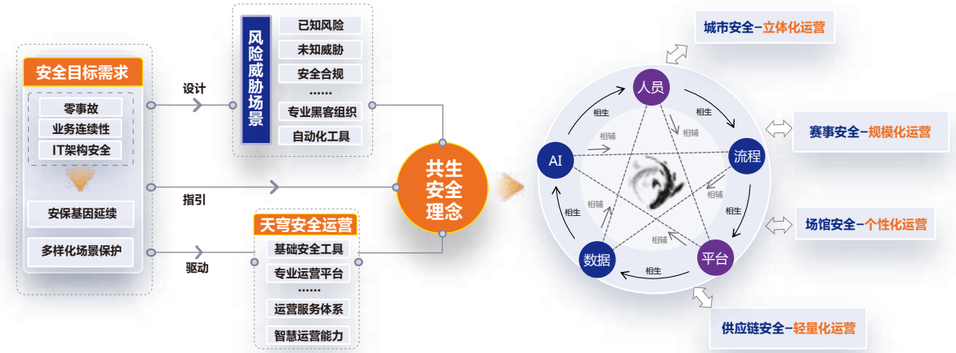


图3-11 弹性运营体系

定制赛事场景化分级运营模式

依据个性化、规模化、轻量化安全运营模式，服务侧构建三层服务体系，垂直向下赋能补充，并在不同运营模式配备不同运营工具平台，通过三层服务体系实现多级产品能力提升，面向赛事保障场景提供多元化、持续性安全运营保障服务。

服务体系分级方面，L3以MSS为能力主体并借助云端大数据与情报能力为L2、L1赋能，L2作为运营专家服务为L1提供运营高阶赋能，提升安全服务能力与运营效能。

运营工具平台方面，依据不同运营场景定义，工具平台丰富度、覆盖范围、安全场景能力逐级提升，对应的运营服务种类也随之增多，适配不同运营模式所需要的安全能力与运营工作指责。

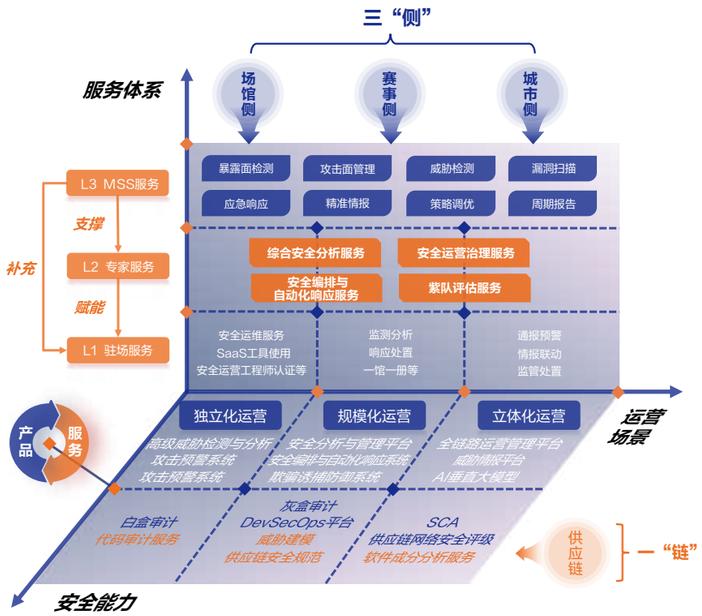


图3-12 事场景化分级运营模式

保障对象差异化分类运营机制

赛事侧规模化运营

赛事侧规模化运营以赛事安全指挥层为中心，面向各安全监管单位进行上报与安全合规执行，同时对所有比赛场馆、数据中心安全保障团队进行保障任务调度与责任落实。建立赛事侧安全运营管理中心，将赛事专网、互联网安全防护能力进行集中，为安全运营指挥管理提供技术支撑，同时承载上报、赋能、联防联控各项运营流程。

赛事侧运营管理机制一方面要面向监管层进行整体安全运营态势、安全事件等方面的常态化上报，针对下发的安全监管要求执行后续的合规响应动作，另一方面也要面向场馆、数据中心等实际保护对象进行监管与赋能，确保赛事整体安全性。

赛事侧运营场景根据赛事数字化、互联化等新变化，包括云安全、工控安全数据安全等多场景，既要考虑不同场景的安全风险特性与业务特性，又要符合安全运营统一化的特点，引入AI安全实现智能化运营保障。

图3-13 规模化运营模式

场馆侧个性化运营

充分考虑赛事场馆级别不同、应用属性不同、保护对象场景多样、安全需求不统一、安全风险威胁类别不同的特点，设计个性化、弹性规模的运营能力建设。基于个性化运营要素设计不同的技术运营方案，配备不同规模、不同值守强度的运营组织队伍，依据场馆承载业务属性的不同细化管理制度，规范运营动作。

在场馆个性化运营模式下，可参照属性、重要程度、用途等维度将赛事场馆、运动员村等初步进行分类分级。在运营维度分析不同场馆面临的风险威胁，配备不同运营工具与服务类型，实现运营资源投入与安全防护要求适配性。

同时，充分考虑场馆侧人员能力参差不齐、工作分类差异较大的现状，须建立与场馆安全强相关的运营管理制度与操作手册，规定各岗位各角色运营责任与操作基线，保障个性化运营的稳定持续。

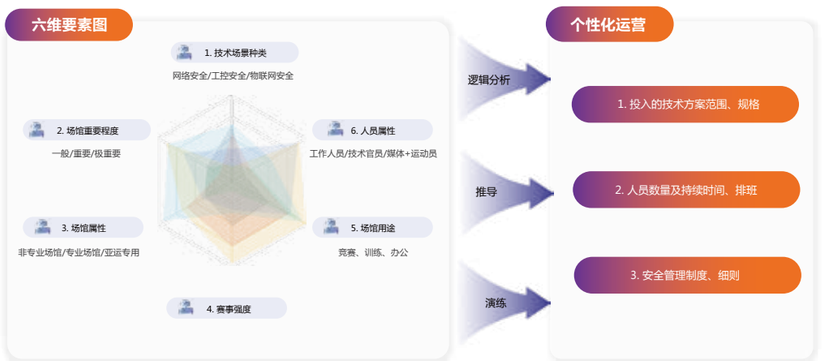


图3-14 个性化运营模式

供应链轻量化运营

体育赛事供应链安全保障包括各类软件应用系统、赛事相关供应商两方面。软件供应链以本地保障为核心，针对待上线入网的全量软件应用进行安全脆弱性检测，依据安全标准进行处置决策。供应商安全保障以云端保障为核心，实时监测网络攻击态势并开展相关分析处置工作，规避对赛事安全带来的安全威胁。

在软件供应链安全审查层面，建立软件系统开发、交付全过程的安全标准，配备软件安全质量检测平台，针对代码、框架、组件、版本等进行严格审查，建立安全风险检测与修复流程机制，在保障赛事信息系统上线的前提下进行安全风险的全量管控。

在供应商安全保护层面，基于安全托管服务平台，建立针对资产状态、安全防护、安全态势等方面的实时监测与检测能力，并对各类告警进行及时有效处置，确保供应商自身网络安全质量。

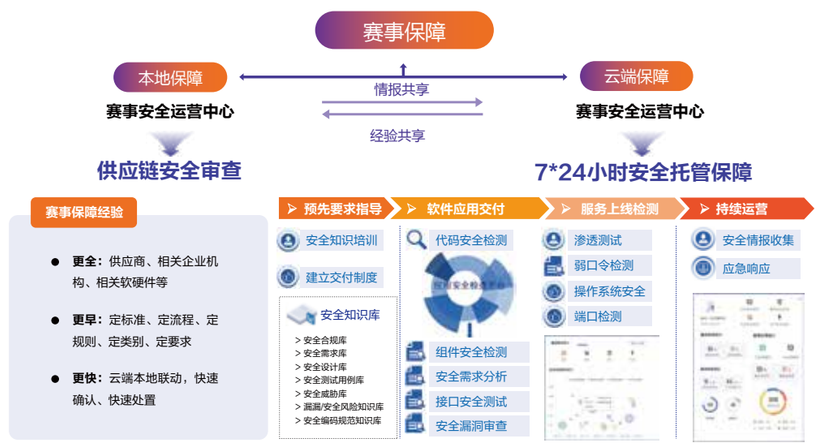


图3-15 轻量化运营模式

协同

基于赛事侧、场馆侧、供应链侧安全保障场景内容构建的不同运营模式，划分网络安全保障责任，在安全运营数据、流程、情报等方面进行高效协同，实现运营动作协调、安全威胁联防联控、安全态势实时共享，构建体育赛事网络安全保障体系化防护能力、动态化运营机制、主动性保障效果。

安全工具平台协同是赛事安全运营保障的技术基础，包括涉及软件安全、边界与终端、网络边界与流量、安全审计等方面的工具，也包括安全大数据分析管理平台等，共同构成运营技术能力。

安全解决方案与服务是赛事安全保障能力重构与增强的必要途径。将工具、服务、流程进行有效结合，形成安全运营整体合力。

整体安全运营依托AI大模型进行智能分析与调度，能够将池化的运营能力进行高效协调，实现安全运营能力自身的协同性。

图3-16 多维安全能力协作

体育赛事
网络安全保障实践
蓝皮书 > 2024

第四章
亚运安全保障先锋实践

亚运天穹弹性安全运营体系建设

当前国际体育赛事的举办高度依赖信息化基础设施、数字化技术手段以及互联网化服务模式，构建具备主动防御能力的赛事安全运营体系，是有效应对各类潜在的网络攻击风险与威胁，保障赛事顺利、安全举办的基础。

以亚运天穹打造赛事保障安全运营体系

亚运天穹运营体系集成自动化安全运营工具、一体化智能分析运营平台、外部情报信息赋能等能力，依托遍布全球的130多个安全运营节点，为赛事安全保障提供海量的专家资源支持，获取最高等级安全保障能力成本降低35%。

网络安全态势感知和监控体系做为主动防御运营体系的重要能力，通过项目运作和企业合作等方式，已开展中国、美国、哈萨克斯坦、委内瑞拉、马来西亚等多个国家1000多家政企用户服务，帮助全球800余名客户构建主动防御运营体系。自G20峰会网络安全保障建立全国首个重大安全运营体系后，主动防御运营体系在2019年世界军人运动会、第31届世界大学生运动会、历届世界互联网大会、进博会等实战场景中不断提升。

图4-1 亚运天穹安全运营“飞轮”理念

天穹安全运营智能平台-亚运网络安保的“安全引擎”

亚运天穹运营智能平台基于亚运总体网络安全运营要求，贴近亚运网络安全工作者实际业务需要，采用工具分层解耦、服务嵌套聚合的理念，多手段、多维度、多层次共同进行亚运网络安全保障。

全源化采集确保系统数据来源的全面性，实现亚运网络安全领域基础安全数据要素归集管理。实战化应用，通过智能网络安全态势分析打通运营、运维、安服、决策各维度能力，涵盖监测、态势、通报、处置、情报、网络安保调度等环节，形成网络安全态势监测业务闭环；基于系统获取的各类监测数据及日常业务流转产生的业务数据，建立亚运安全指标、规则、情报等模型，实现智能网络安全态势分析。

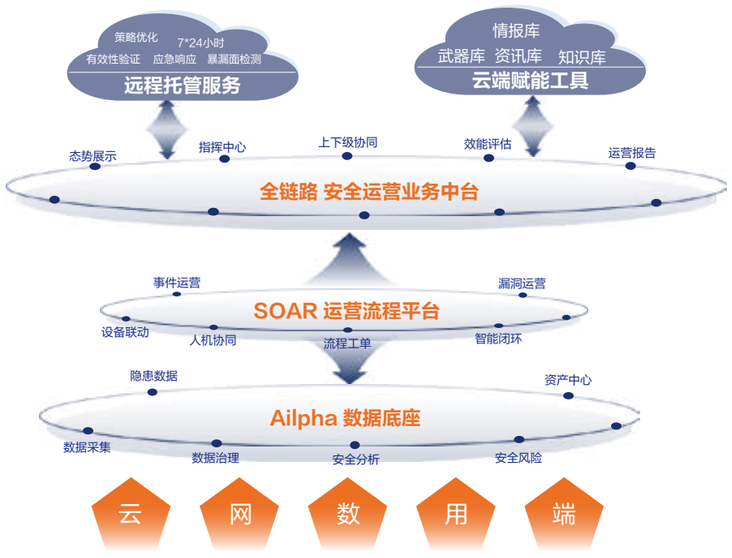


图4-2 基于亚运保障不同角色的安全运营智能平台

以天穹安全运营中心探索国际体育赛事保障新思路

国际体育赛事因其巨大的国际影响力，在网络安全保障方面具有极高的强度要求，结合其自身网络、应用、数据等各方面的复杂性与脆弱性特点，网络安全保障工作面临诸多不确定性与较大难度。

天穹安全运营中心在各国际体育赛事安全保障工作中的成功应用，是因为符合当前以工具替代服务、以技术赋能人员、以攻击验证防守、以情报赋能安全的安全运营发展趋势，实现平台解耦、工具提效、专家介入。相比传统堆人、堆设备且保障力度弱的保障思路，实现了在赛事保障目标的完成与安全资源投入之间的良性平衡，探索出一条赛事保障的新思路，也可在重大国际会议网络安全保障、高价值业务目标网络安全防护方面提供可实践与可复制的经验。

图4-3 亚运天穹-新一代主动防御运营中心

安恒恒脑辅助智能亚运

网络安全威胁日益加剧。随着互联网应用普及化，所对应的网络威胁数目随之上升，而且其复杂性也相对增加，对网络安全带来了巨大挑战。特别是在杭州亚运会这样利用人工智能、大数据、云计算等先进技术，从办赛、参赛到观赛，都智能感十足，科技感满满，高规格体育赛事中，通过恒脑在网络安全方面的作用是辅助杭州亚运会降低入侵风险，并改善其整体安全状况。恒脑通过从过去的数据中学习来识别模式和趋势，然后这些信息被用来预测未来的袭击。恒脑驱动的系统还可以配置为自动响应威胁，并在更快的时间内对抗网络威胁。

威胁情报聚合

恒脑从各种来源收集海量安全邻域的通用知识和深度知识、威胁情报数据。包括但不限于：安全常识和术语、安全运营知识、政策规范、论文期刊、实战攻防技巧、安全日志、网络流量、威胁情报库等。在数据预处理阶段，需对其进行标签化，标注数据的来源和所属领域。图片数据则进行OCR提取文字内容，并将文字与图片进行关联。原始数据经过数据预处理后，形成高质量的安全知识。具备处理网络安全相关通用知识问题的理解和解释能力。

威胁/恶意IP分类分级提供处置动作

恒脑能对IP、域名、文件hash开展分析，识别是否存在威胁，包括威胁信息分类、通讯样本、域名注册信息、IP地理位置、关联信息、防范措施等。可支持批量查询，IP情报查询结果的威胁类型包括但不限于：僵尸网络、垃圾信息、代理、扫描、暴力破解、漏洞利用、DDoS攻击、白名单等。IP情报查询结果的威胁等级包括：严重、高、中、低、可疑、安全、未知。IP情报查询结果的可信度包括：高、中、低、未知。

通过引入AI大模型技术，提升原有安全系统平台告警降噪的效率与精准度。此外，对于降噪后的告警结果，可以由恒脑系统实时研判分析，并给出有效、准确的告警分析结论。最后由恒脑智能系统给出相关合理的处置建议，供亚运保障工程师员进行最终决策。

安全告警收敛降噪

面对日常安全运营中产生的数以亿计的告警日志，通过传统系统与安全运维工程师的研判，很难快速发现风险事件，也无法完成告警日志清零目标。因此急需要借助新的智能化技术和系统去实现关键风险事件的发现，达到告警清零与精准研判的目标。

通过引入恒脑，提升原有安全系统平台告警降噪的效率与精准度。此外，对于降噪后的告警结果，可以由恒脑系统实时研判分析，并给出有效、准确的告警分析结论。最后由恒脑智能系统给出相关合理的处置建议，供现场安全运维人员进行最终决策。

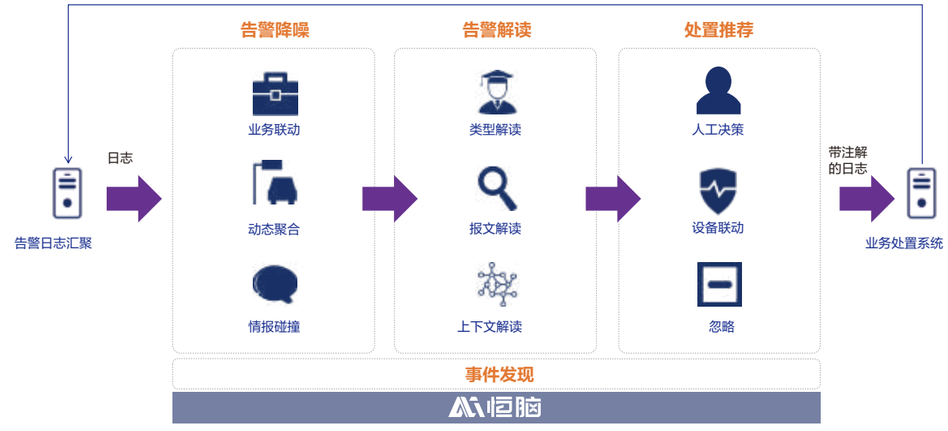


图4-4 降噪研判流程

告警日志获取：通过在亚运会各场馆部署日志探针，通过syslog及Aigent插件方式采集场馆AGIS专网内的安全设备、网络设备、终端和服务器产生的相关日志数据，LAS对告警日志进行标准化处理，同时传至本地化安全运营平台将日志进行汇聚，恒脑系统可通过接口主动获取告警日志，可进行全量、增量的周期性获取。

告警降噪：首先对告警日志按条件进行聚合，形成告警聚合组。按照攻击者、受害者、告警类型、告警名称这4个字段完全一致进行告警聚合。其次，在降噪过程中，场馆安全运营工程师会对告警进行人工研判和验证，确认比如实际发生的真实攻击和僵木蠕毒事件、现场业务系统需允许的白名单、正常测试和扫描的授权行为等。最后，在降噪过程中进一步使用威胁情报进行碰撞，对威胁情报命中的告警进行打标。攻击者IP碰撞为白名单：打标“加白”，攻击者IP碰撞为恶意IP，打标“风险”，攻击者IP未匹配：打标“未知”。

告警解读：将单个告警聚合组的攻击者IP、受害者IP、告警类型、告警名称、告警时间等字段作为输入，通过模板的方式对上下文进行解读。同时调用IP地址的威胁问答能力获取攻击者IP对应的威胁研判结果。对于“授权”、“加白”等标签的告警聚合组按照默认模板进行上下文说明。对于“风险”、“未知”等标签的告警聚合组按照对应的模板进行上下文说明。部分HTTP协议告警中有对应的HTTP报文，需要结合恒脑对HTTP报文进行分析，包括攻击方式、攻击意图、攻击载荷等信息。

攻击者视角研判指挥模式实践

亚运会网络安全保障实践率先采用盾立方立体防御体系，从攻击者视角构建研判指挥体系，部署和应用四蜜威胁诱捕系统和关联研判处置系统，其中四蜜系统采集潜在攻击者的攻击行为数据，和已有安全防护设备采集的告警数据互补，关联研判处置系统通过对多来源、多维度、多视角的威胁数据进行关联分析，发现和研判攻击行为，并提供处置建议。亚运会在赛前、赛中、赛后分别采取自卫、护卫、迭代的模式，全流程保障赛事系统平稳运行。本次亚运会安保研判期间，发现可疑IP　1300个左右，实现了针对攻击者的主动检测与关联分析，保障了亚运会在整个赛事周期内的平稳顺利进行。

攻击者视角的研判指挥体系构建

重大赛事活动中，网络攻击者位于暗处，是攻防对抗的优势方，攻击方和防御方存在攻防信息不对称的情况。为了有针对性地实现对攻击者的精准防御，需揭示攻击者行为的规律与特征，从攻击者的思路出发来进行防范。本次亚运会安保从攻击者视角出发，重新审视网络安全对抗操作域的三个核心要素：研究“攻击者用什么”，以揭示“攻击隐藏”要素；研究“攻击者干什么”，以揭示“攻击着点”要素；研究“攻击者的目的是什么”，以揭示“攻击意图”要素。

图4-5 攻击者视角分析

针对攻击者的攻击三要素，盾立方立体防御体系通过布陷的方式探察，通过关联的方式研判，通过协同的方式阻截攻击者。在亚运会全生命周期内的不同阶段采取不同的安全防护模式：在事前阶段采用“自卫模式”，实施内生安全自保，依靠系统自身来抵抗攻击；在事中阶段采用“护卫模式”，进行外部防御对抗，依靠外部来阻断攻击；在事后阶段采用“迭代模式”，依靠复盘来强化防御体系。亚运会部署的盾立方立体防御体系主要包括四蜜威胁诱捕系统和关联研判处置系统，构建的攻击者视角研判指挥体系成功实现了对未知攻击者的主动探测与分析，保障了赛事平稳顺利进行。

四蜜威胁诱捕系统部署与迭代优化

盾立方的四蜜威胁诱捕系统部署在赛事外网和内网，其中外网的四蜜系统部署在互联网VPC（Virtual Private Cloud）上，内网的四蜜系统部署在专网VPC上。外网的四蜜系统共部署蜜点18个、蜜庭2个、蜜阵2个、蜜洞2个，位于DMZ（Demilitarized Zone）区，通过路由分配IP，供互联网用户访问，对攻击者的访问行为进行探测；蜜阵管理系统、关联研判处置系统等部署于内网区，通过隔离确保安全分析核心系统的安全。

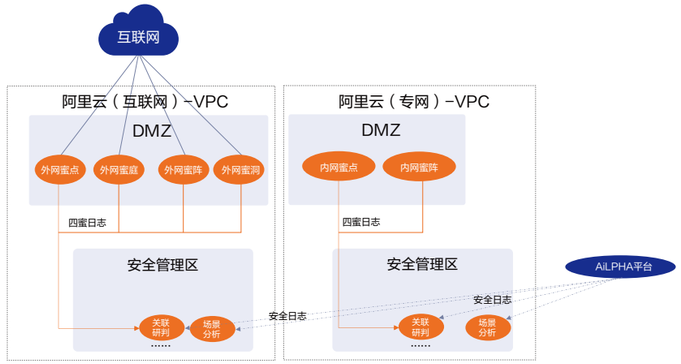


图4-6 亚运会“四蜜”系统部署概况

在亚运会周期内，四蜜系统根据实时研判状况对蜜点的部署进行调整和优化。例如，基于边际效益确定蜜点部署个数，在部署资源消耗相对小的条件下，获取最大化的威胁探测收益；根据蜜点甜度确定蜜点效果，对于甜度较低的蜜点域名及时替换，借由蜜点更换和新增蜜点的威胁探测结果进一步观察攻击者行为，发掘其动机；对蜜点、蜜庭进行内网统一命名与管理配置，根据亚运赛事系统场景优化“阵图”部署方法，实现赛事系统周围的全方位协同探查感知。

关联分析与研判系统

亚运会的网络安全研判以四蜜威胁数据为主要分析对象，并结合网络安全防护设备产生的多维度威胁数据，从宏观和微观两个角度对潜在的攻击者进行分析研判。在宏观态势上，对每日新增潜在攻击者IP个数进行统计分析，并研判新增攻击者IP与历史赛事活动的重叠情况，统计新增IP的C段及B段同源情况、地理位置分布情况等；在微观态势上，研判每个IP的威胁情况，包括其威胁性质、代理信息、payload信息等，通过汇总多个威胁情报数据源对IP性质进行综合研判。

踩蜜IP宏观分析

图4-7 亚运会研判期间踩蜜IP趋势

在亚运会开幕前夕及举办期间，对四蜜系统采集的潜在攻击者IP（即踩蜜IP）的数量进行统计分析。在研判周期内，每日踩蜜IP个数整体趋势呈现先上升后下降趋势，而后波动中下降，趋于稳定。每日踩蜜IP个数在研判系统上线后的第四天达到峰值，在亚运会结束前一天回落到较低值。研判期间踩蜜IP数超过千余个，日均踩蜜IP数70余个，潜在攻击者踩蜜数量整体在可控范围内。

除统计每日踩蜜IP个数外，关联研判系统对潜在攻击者IP的数据进行多维度分析，包括：威胁日志数、新增与非新增IP数、每个蜜点的被踩次数、踩蜜IP在历史重大活动中出现的情况等，通过结合赛事已部署的大量网络安全防护设备进行综合分析，包括分析踩蜜IP与访问业务系统的关联情况、踩蜜IP与告警日志的关联情况等对踩蜜IP的性质进行研判，同时结合多个威胁情报数据源，对踩蜜IP的性质、IP类型、历史行为、关联域名等信息进行自动化分析，从而实现微观分析，为处置提供数据支撑。

踩蜜IP历史行为分析

盾立方体系已应用于奥运会、大运会、广交会等多个赛事中，针对亚运会期间出现的踩蜜IP，同时关联分析其在历史活动中的出现情况，以大运会（第31届世界大学生运动会）、广交会（第134届中国进出口商品交易会）为例，将亚运会期间的踩蜜IP进行碰撞分析，可以发现有138个IP也出现在大运会活动中，有49个IP出现在广交会处理列表中，有20个IP在三项赛事活动中均被发现，以此进一步对上述IP的攻击组织、攻击目的进行研判。

图4-8 历史赛事活动中的踩蜜IP重叠情况

踩蜜IP地理分布

图4-9 踩蜜IP地理位置分布

为直观了解潜在攻击者地理分布，关联研判系统对踩蜜IP进行地理位置分布的可视化，并对亚运会期间出现的踩蜜IP按照同C类地址进行分段，共识别出70个左右C类地址段，其中，境内30个左右，境外约40个。

踩蜜IP威胁性质研判

对于每个踩蜜IP，关联研判系统结合4个威胁情报源对其威胁性质进行判定，即恶意或非恶意，并通过多种方式判断该IP是否为代理，为处置提供数据支撑。同时，以踩蜜IP为核心的其他微观态势信息包括：该IP踩蜜类型及个数、踩蜜行为类型、是否访问正常业务系统、是否关联安全设备告警登。根据踩蜜IP的具体分析情况，系统自动化生成其攻击链路，并对链路中的每个节点进行处置分析。

高危IP的攻击行为分析

对于系统研判的高风险等级的IP，同时通过其payload进一步分析其具体攻击行为，包括使用弱口令登录蜜点系统，访问蜜点系统绊线的敏感目录和文件，漏洞利用，向特定恶意IP请求下载和执行恶意脚本文件，构造恶意post请求，非法以管理员权限登入系统等，通过payload分析实现对高危IP的攻击技战术、攻击目的的深入研判。

在亚运会期间，系统对约30个高危IP进行分析，通过威胁情报标签与踩蜜日志payload交叉验证等方式，结合其踩蜜行为、攻击画像等信息，推断出其疑似所属APT组织，包括：Gamaredon Group、FIN6、Muddywater等国外APT组织，以及TEMPER PANDA等国内APT组织。研判中对于疑似TEMPER PANDA的踩蜜IP进行重点研判，对涉及的场馆相关主机进行现场溯源，及时抑制了潜在的风险。

复杂多步攻击行为时序关联分析

对于存在的复杂多步攻击的攻击者，系统综合关联其踩蜜日志、系统访问日志、安全设备告警日志等，基于MDATA知识库对存在相似攻击行为、相似攻击目的、相似攻击手法的IP进行同源性判定，然后结合踩蜜、访问行为日志等的时序约束关系，对攻击步骤进行关联，利用MDATA模型子图匹配等技术，还原攻击者尝试的攻击链路，研判攻击者的攻击目的及下一步攻击方向，基于上述分析，对于可能涉及的场馆内部主机进行了及时处置和策略部署，支撑了对潜在攻击者的研判和处置。

研判处置策略与建议

基于关联分析与研判系统提供的数据，本次活动对IP的威胁程度进行量化，即通过“威胁值”反映攻击者IP的威胁程度。研判系统综合IP的踩蜜点数、基础攻击次数、攻击危险等级、复杂攻击影响节点数、业务系统访问次数、安全设备告警次数等多个维度，综合计算IP的威胁值。研判处置系统提供不同条件的处置策略，生成处置建议。包括：

根据踩蜜类型处置：如某IP在指定时间段内检测到指定次数的某特殊蜜点的踩蜜行为，则永久添加黑名单；

根据基础攻击类型处置：如某IP存在暴力破解、webshell远程控制、或异常登录等特定基础攻击行为，则将其加入黑名单指定时限或永久；

根据复杂攻击方式处置：如对某IP检测到DDoS攻击，则临时添加黑名单指定天数；检测到某IP存在复杂攻击，且其攻击链路的节点数超过指定个数，则将该IP添加黑名单达指定时间，后续每新链一个节点，则对源IP重新加黑等；

根据威胁值处置：如某IP的威胁值大于指定阈值时，则对其临时加黑指定时长或永久加黑。

本次亚运会的关联研判处置系统主要采用以下三种处置方案：

> 对于扫描类IP、代理类IP、访问过正常业务系统的IP、有恶意情报标签的IP，建议长封（永久封禁）；
> 对于其他踩蜜IP，如爬虫类、非代理IP，建议临封（临时封禁）；
> 此外，对于高威胁IP，若其地理位置在国内，则报告相关部门进行外部和内部溯源。

面向重保活动的威胁情报能力建设与积累

威胁情报能力建设与威胁情报库的积累是提升重大赛事活动安全保障能力的关键。在亚运会等赛事活动中通过迭代模式不断积累威胁情报数据和能力，包括：

各赛事活动中出现的踩蜜IP：将历次活动中出现的踩蜜IP进行持续积累，在后续的潜在攻击研判中支持对踩蜜IP在历史赛事活动中的踩蜜记录碰撞，有助于挖掘踩蜜IP的行为特点，获取更多的信息推断攻击者动机；

踩蜜IP的威胁性质及标签：将亚运会等赛事活动中研判出的IP威胁性质及情报标签建库进行持续积累，逐步建成覆盖全网的自产情报库，有助于提升研判速度和效率；

开源威胁情报：从技术博客、社区论坛、社交媒体、公开报告中不断采集和积累开源情报，进行抽取和标准化表示，构建开源威胁情报库，有助于丰富研判依据，提升威胁研判的准确性；

攻击画像情报：目前研判所采用的信誉情报，在刻画复杂的攻击手法时存在局限性，需要逐步将“IP信誉情报”升级为“IP攻击画像情报”，从历史攻击手法、攻击目标、传播木马情况等指标定性攻击者归属家族，通过历史攻击活跃程度、攻击包详情等细节佐证分析结论，以层级方式刻画攻击画像；

情报验证能力：亚运会等赛事活动的安全研判对于研判结果的准确性要求较高，对于情报信息和研判结果，需要有交叉验证机制。验证能力的积累可通过不同来源的威胁情报厂商、实际攻击场景和攻击行为等实现。

本次亚运会的安全保障研判分析历时近一个月，重点分析蜜点和蜜庭采集的威胁数据，通过蜜阵进行蜜点及蜜庭的部署和调度。研判期间共分析千余个踩蜜IP，对其中重点IP上报溯源，推断出其疑似所属APT组织。从宏观态势和微观态势完成对踩蜜IP的综合分析研判。研判期间持续同步相关部门确认研判结果、支撑即时溯源。在分析研判的同时，系统在迭代模式下持续积累和提升威胁情报信息和能力，在完成安保任务的前提下力求进一步提升研判效率、准确性和交互性。

盾立方立体防御体系在亚运会保障先锋实践中迅速识别和研判恶意IP行为，对于高危IP及时进行封禁，确保亚运会赛事系统的平稳运行，在识别和研判潜在攻击者方面发挥了重要作用，成功实现了从攻击者视角的研判指挥与处置。

亚运云计算环境数据风险态势管理实践

杭州亚运会作为近年来赛事规模最大、竞赛项目最多、参与人员规模最大的综合性体育赛事。6大赛区，88个场馆，49个核心业务系统、赛事成绩、赛事管理、赛事支持三大类核心系统群全面上云、1万多终端设备接入访问，系统众多、敏感数据量大、人员繁杂、接入方式多样、数据安全挑战严峻。

亚运数据安全风险

赛事核心系统采用云计算作为亚运会算力基础设施，从底层支持赛事系统群，向上支撑云上转播、亚运钉等智能应用，实现核心系统和应用服务的云上打通，为亚运各类智能应用提供云底座支持，由此带来更多数据安全风险。

亚运数据安全防护中面临5大防护难点，重点关注敏感数据资产、运维权限管控、系统间数据共享、数据使用监控与溯源、终端数据泄露等，具体包括：

> 敏感数据广泛分布在各个涉亚信息系统中，底数不清，分布不明。
> 运维人员多，身份复杂，数据访问权限控制难。
> 系统间数据共享频繁，数据系统间业务数据交互量大，泄露风险大。
> 数据使用监控难度大，数据泄露事件感知、监控、溯源难度大。
> 终端访问、办公场景接入终端多，人员杂，敏感文件数据泄露风险大。

云上数据安全架构设计

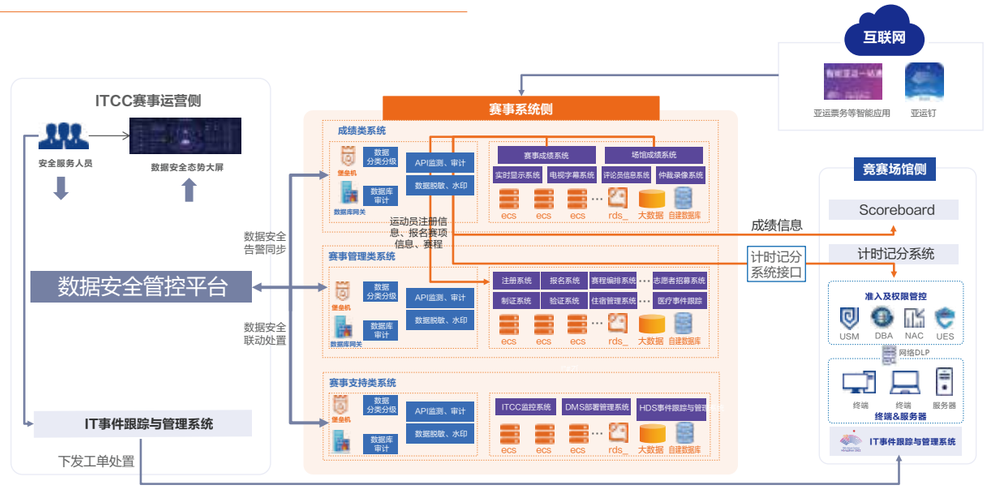


图4-10 杭州亚运会数据安全总览

通过云上技术体系构建云上数据安全整体架构，保障整体支撑核心业务应用，并通过持续风险评估不断优化防护方案和数据安全运营体系。

云上数据安全技术体系，通过资产梳理、数据库审计监控、接口监测、数据水印、数据脱敏、权限管控、防泄漏、态势感知等基础能力的云化部署，强化云上安全资源自动编排能力，对多租户场景实现安全能力服务总线功能，按需支撑业务系统的数据安全防护需求，并持续监控业务数据资产的安全态势。针对云上数据赛事侧、场馆侧安全场景，持续优化完善数据安全风险监测模型和新业务场景的风险评估，形成数据安全运营体系闭环管理。

基于杭州亚运的数据安全防护整体设计，安恒信息在云上数据安全提供了敏感数据发现、数据脱敏、数据调用接口监测、数据访问权限精细管控、敏感数据防泄漏、整体大数据态势感知等能力。

在竞赛场馆侧

通过堡垒机、数据库安全网关、数据库审计、一体化终端安全管控系统、网络防泄漏措施，有效管理运维层面的数据访问权限控制，防范多角色用户接入层面的数据泄露风险。

赛事信息系统侧

应用云上数据安全资源池，防护数据访问使用中的篡改、泄露、异常请求事件。

在赛事运营侧

通过统一数据安全管控平台，实现数据安全态势一屏通览，持续监测涉亚系统的数据安全态势。

数据安全防护主要场景

在云上数据安全防护能力上提供了敏感数据发现、数据脱敏、数据调用接口监测、数据访问权限精细管控、敏感数据防泄漏、整体态势感知能力，针对亚运防护难点，覆盖对应五类主要业务场景。

敏感数据发现与梳理

涉亚核心业务系统包含大量异构数据源，多种数据库中的结构化和非结构化数据，其中票务、注册中心等业务系统中含有大量运动员、注册人员、观众、工作人员等个人信息敏感信息。

整体设计规划

安恒信息结合《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等要求，结合2008年北京奥运会、G20杭州峰会、成都世界大学生夏季运动会等过往重保成功经验，制定契合杭州亚运会现状的《重大赛事数据安全分类分级标准》，作为系统化梳理全量数据的标准规范。

技术保障

将云与数据安全深度耦合，与阿里云打通账号体系，全面对接ODPS、RDS、OSS等云上服务模块，做到自同步资产。同时引入AI大模型进行敏感数据建模，通过学习大量数据，做到敏感数据精确识别率超过95%。

后续应用

精确识别敏感数据并进行分类分级，基于分级实施敏感数据打标，奠定数据安全防护与监测基础，在跨系统调用、人员读取时，根据分类分级结果对数据执行差异化管控策略。同时打通分类分级与其他数据安全防护系统，实现直接把分类分级的结果同步给数据脱敏、网关等其他数据安全能力系统，作为下一步处置的基础条件。

数据资产运维安全

杭州亚运会合作商众多，涉及不同维度、多层面的系统维护保障工作，数据范围十分广泛，因此需要负责开发运维的人员也繁多。如何精准管控运维动作、实时发现高风险操作并能够及时处置将会变得十分关键。

针对数据资产运维安全，安恒信息构建起“身份权限管控+数据处理管控”的双重保障机制。一方面，运维人员全部要通过浙政钉扫码登陆，进行身份认证，获取唯一的权限账号，保证专人、专账号、专权限，一旦发生问题，能够快速精准回溯定位人员。另一方面，通过数据安全网关细颗粒度管控“通过SQL语句执行数据库操作”行为，结合分类分级结果，针对高敏感数据的运维操作进行风险告警或向上审批的不同防护机制。同时实现操作过程录像、操作命令记录、传输文件备存等功能，实现全面审计溯源。

数据共享交换安全

当前产业数字化发展如火如荼，数据的传递也从1.0阶段的表格复制共享，到2.0阶段的前置机文件共享交换，慢慢到3.0阶段通过API接口进行调用。因此如何加强API监控，成为数据安全管控的关键。

为做好数据的交换管控，首先须精确识别API接口资产，通过检测对报文头，有效区分URL静态地址与Restful API接口资产，杜绝无效告警，做出正确的运维判断；其次双向识别API接口调用的流量，打通分类分级能力，精确定位问包流量中的敏感数据；同时，安恒信息与阿里云深度合作，通过对接阿里云ODPS，实现无Agent模式的流量解析与分析，解决云上租户业务引流难题。

办公网数据防泄漏

办公网场景是最容易发生数据泄露的场景之一。办公网涉及人员众多，场馆办公场所条件不一，导致办公网管控措施难以有效落地。针对此场景，我们首先盘点泄露路径，主要分两大类，一类是通过网络流量侧的泄露（如：IM软件、邮件等），另一类是终端侧的泄露（如：移动介子，摄屏等）。基于泄露路径实施定制管控策略，网络侧采取封禁即时通讯软件发送动作、审计邮件发送流量，终端侧通过一体化终端办公组件，采取接入用户认证、杀毒、监测外接终端等，同时采取暗水印技术回溯审计屏摄动作，有效震慑此类泄露行为。

除了管控泄露路径，办公网数据防泄漏场景方案还进行了防护左移，终端用户接入赛事竞赛专网之前，除了通过浙政钉的身份认证，还须安装Agent感知终端环境安全，评估运行环境符合要求之后，基于权限开放后端应用的访问。

数据安全监测与审计

数据分类分级、运维、共享交换、办公网构成杭州亚运网络安全保障过程中最重要的细分场景，此外，利用整体监测审计能力，呈现亚运整体数据安全态势，通过数据安全管控平台对接各数据安全探针，一体化展示场馆侧、赛事侧、供应链服务商侧的数据安全状态，真正做到一屏通览数据安全风险态势。

通过汇集数据，梳理数据流转链条，包括前端用户通过应用调用数据的动作、应用中间件访问API接口行为、访问数据库落盘数据的SQL语句，真正做到数据全生命周期的数据流转血缘分析，理清风险脉络。同时数据安全管控平台通过对接探针，可基于风险类别一键下发处置策略，高效完成数据安全风险的操作闭环。

基于亚运业务的场景化预警模型实践

多源异构数据的融合性分析思路

安全运营平台可实现的威胁挖掘总体分为三大类，分别为网络威胁分析、系统安全分析以及用户行为分析。具体的类型如下：

网络威胁分析：主要包括网络层面的入侵和攻击分析。如应用密码猜测攻击（暴力破解）、CC攻击、注入攻击、Web Shell攻击、跨站攻击、0day漏洞利用攻击、恶意扫描、木马回链、SMB行为、文件威胁、DGA、恶意DNS通讯、蔽信道通信、DOS/DDOS攻击以及异常流量攻击等；

系统安全分析：主要包括服务器系统运行层面和脆弱性层面的安全威胁挖掘分析，包括应用服务器、数据库服务器、邮件服务器等。如数据库拖库行为检测、服务器口令爆破、恶意文件活动、系统日志被恶意删除/修改、系统账户提权、沉睡账户激活、新增系统账户、恶意进程、设备性能异常等系统运行层面的安全威胁分析；系统脆弱性层面主要包括系统漏洞被利用、弱口令分析；

用户行为分析：用户行为分析主要包括构建个体用户画像和群体用户画像，在用户画像的基础上，结合安全事件，关联分析出用户行为相关的异常事件。主要包括用户账户异常时间/地点登录、账户权限变更、用户高频操作行为检测。

模型管理

基于以上多源异构数据的融合性分析思路，安全运营平台提供规则模型、关联模型、统计模型、情报模型、AI模型五种模型自定义能力，帮助亚运安全运维团队根据亚运实际业务场景，进行安全告警策略模型的自定义。

规则模型

通过规则模型，允许亚运安全运维团队针对设备告警进行进一步处理与转发、对各类安全设备告警日志和流量日志进行二次匹配，形成嵌套式的安全策略。 亚运过程中，安全运维团队遇到了如hostAliveScan、主机存活扫描、statistics等威胁类型，检测到针对IP网段内服务器存活性的探测行为。通过平台进行规则模型的建立，使用ping或者tcp等连接尝试等方式，确认目标IP是否在线并对探测包做出回应。

关联模型

亚运重保过程中，可能存在部分业务存在关联性，部分威胁存在关联性，通过关联模型，允许亚运安全运维团队形成具有关联性和序列性的安全策略。 如可基于时序关联顺序进行关联模型的建立，如将疑似扫描爆破行为与后续的木马植入行为、远控行为进行一定时间范围内的时序关联，进行安全事件间关系定义或进行事件间属性关联，有效掌握攻击链信息，快速挖掘出潜藏攻击者。

统计模型

亚运重保过程中，会出现大量统计阈值相关的安全告警限制条件，不同的亚运场馆即使针对同一统计指标，设定的阈值可能也不同，通过统计模型，允许亚运安全运维团队形成针对各类亚运场馆的个性化统计指标或个性化阈值的安全策略。 依据不同常规大小不同，场馆侧会接入包含运动员、技术官员、媒体等各类、各国人员的相关互联网数据，还有各类赛事系统、保障系统、流程系统等，如爆破行为、扫描行为的阈值设定和内网业务系统数据和互联网数据接入基线密切相关。

情报模型

亚运重保过程中，会出现大量的实时情报数据（如疑似攻击IP等），这些情报数据需要尽快纳入平台的检测策略中，通过情报模型，允许亚运安全运维团队形成基于安全情报的实时安全策略。 与恶意域名、远控服务器做交互通信的场景，例如远控木马、挖矿木马、已知APT组织等，对接安恒数据大脑情报库（威胁情报中心），碰撞相关协议字段。 内置的情报类型包括：扫描主机、C&C、黑产IP、僵木蠕通信域名、恶意软件、APT组织、扫描主机、放马地址等。

AI模型

通过AI模型针对不同类型的数据采集与处理（全部日志SOC接收解析后统一放入原始日志中），配置对应的监控模型策略及告警策略（处理结果统一放入异常记录中，当模型中标记为原始告警时，放入异常记录中同时放入原始告警中）。 在元数据统一管理下，亚运运维人员根据不同的关注领域灵活操作，包括对数据处理逻辑的新增、删除、修改、查询、启动、停止等。针对AI建模和其他算法建模的场景，将每类场景使用多种算法进行学习和监测，如使用贝叶斯算法，机器自动选择概率最高的模型进行基于基线偏离情况的违规行为或非法行为探查工作。

模型编排

安全运营平台可实现对模型的智能编排，支持对亚运用户不是常用的数据挖掘和集群学习基础算法，模型智能编排逻辑如下。

- 模型编排画布中，元素左侧代表输入，右侧代表输出；
- 使用有向连接线标书模型数据的流程，支持多个元素的链接；
- 支持已建立的模型复用（可直接调用已有模型作为下一个模型的输入）；
- 模型编排修改模型时，在完成界面显示模型指标的增删改情况。

基于事前预防理念的安全验证技术亚运实践

亚运事前准备阶段安全验证

在亚运整体安全建设中,安全设备的安全策略有效性一直是黑盒状态，面对亚运举办过程中可能会遭受的手段丰富多样的不法分子的攻击，需要做到防患于未然。因此，需要通过安全验证平台的攻击用例，有效结合自动化工具及服务流程，帮助安全运维人员在亚运事前准备阶段全面梳理安全防御体系化建设。对现网安全设备的检测能力及阻断能力进行验证，充分验证安全设备策略有效性，全面提升安全亚运重保中重要安全设备的检测准确性和防护有效性。

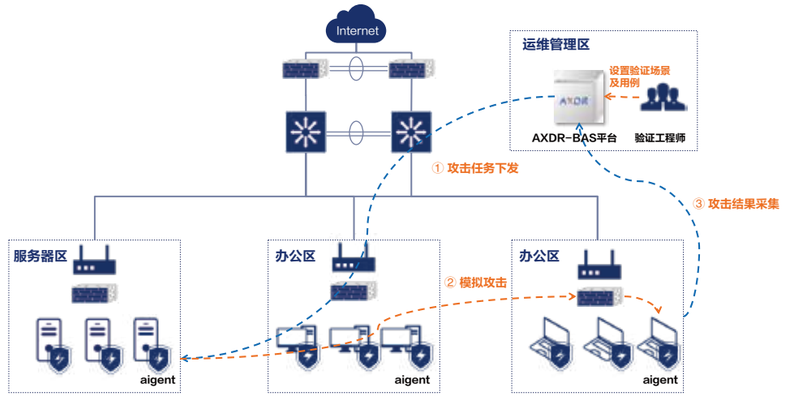


图4-11 安全验证部署示意图

自动化攻击模拟

选定服务器区或者亚运场馆对应PC或服务器作为攻击机及靶机，安装进行攻击模拟的agent，通过BAS对攻击机下发攻击指令，通过攻击剧本模拟发起攻击，并通过靶机安装的agent采集反馈攻击结果，在平台上统一进行展示，从而验证攻击过程经过的安全设备的防御能力，安全设备是否具有检测最新漏洞的能力，安全设备流量覆盖情况，安全设备日志是否丢失，规则是否生效等现网安全防护及安全策略问题，更好服务于亚运前的安全加固工作。

特定攻击场景模拟

同时，在亚运前的临战及备战阶段，XDR-BAS还能模拟特定的攻击者或攻击场景，对现网已经加固安全设备的安全策略进行预检验，有效为亚运中可能存在安全防护策略的薄弱之处，尤其是针对较新的漏洞利用、数据泄露等攻击提供先验依据。

ATT&CK模型匹配模拟

BAS导入ATT&CK模型，基于该攻击模型，从攻击的各阶段持续评估防护能力，涵盖信息收集、邮件网关、防火墙、WEB网关、执行与C2、流量设备、数据渗出等阶段。全面覆盖网络层面、应用层面、主机层面、数据层面等的84类攻击向量并依据安全验证结果，覆盖70%以上ATT&CK模型。通过自适应匹配ATT&CK模型，统计攻击结果，直观展现对应该模型的安全防护及检测能力，并为安全运维人员进行进一步分析研判提供系统性依据。

亚运防御强化阶段应用场景

通过攻击模拟实现亚运防御强化阶段快速查漏补缺

安全策略防护，尤其怕百密一疏。通过BAS针对常见安全威胁场景进行快速高效的自动化验证，例如检验各类安全设备对IP端口扫描、DNS隧道、ICMP隧道等常见安全问题的防护和检测成效，能够与安全运维团队的人工核验形成有机互补，在亚运临战强化工作中实现快捷查漏补缺。

通过用例剧本实现亚运常见BAS攻击手段重点防护

在亚运前的防御强化阶段，需要对安全设备进行针对性安全加固，尤其是对于大型赛事中APT组织常用的攻击手段，如各类SQL注入漏洞利用、远程代码执行漏洞利用、各类横向移动、各类提权手段等。BAS通过内置攻击用例及剧本，对将在亚运中出现的红队常见攻击手段进行多维度验证，并利用安全验证成果指导后续安全加固工作，实现对常见红队攻击手段的重点针对性防护和加固工作。

亚运后复盘及后续经验沉淀

在亚运前及亚运期间的安全防护能力，本质上是在短时间之内对现网安全能力进行突击加固和强化的结果，无法完全真实体现真实的安全防护能力。因此，在亚运之后复盘亚运过程，总结亚运经验，应用在日常安全运维体系建设中。

提升运营团队攻防实战

创新结合亚运攻防对抗实践、ATT&CK战术，全面提升亚运安全运营团队攻防实战能力。通过安全验证对安全攻击的模拟，安全策略的调优加固及在后续亚运实战中对应安全攻击的相应处置等流程产生的各类安全验证报告及攻击剧本，有效沉淀安全经验，提升安全运营团队攻防实战能力。

通过纵深防御逐层验证形成攻击链路

通过agent的多级部署，通过纵深防御模拟技术实现对现有安全设备进行逐层验证，形成对应攻击链路。并对照常见BAS攻击流程，根据验证结果，对每个环节所需的安全设备防护或检测能力进行评分，并通过趋势折现图呈现安全验证得分趋势。

全链数据进行大屏展示

通过安全验证大屏直观展示安全总分及趋势、模拟攻击趋势、高危攻击用例TOP5、区域风险TOP5、攻击阶段统计、攻击阶段设备得分、ATT&CK防守得分等，便于安全运维人员通过大屏实时监测现网安全验证成果及趋势。

基于大数据的资产管理能力亚运实践

资产管理的目的是支撑网络安全管理与运营，需要围绕着系统建立良好的管理制度与运营机制，将资产管理规范起来。针对本次亚运，安全运营平台的主机资产管理功能通过人工录入、资产导入、资产同步、流量自动发现、主动扫描发现多种方式接入资产数据，结合批量编辑功能、资产属性导入导出功能，逐步完善系统中各资产属性。

安全运营平台的主机资产支持多样标识，支持添加私网IP、公网IP、MAC地址、域名、主机名作为资产标识。支持多种资产的管理，风险识别及控制。通过与安全漏洞、安全告警的关联，支持对每个资产评级评分，以资产作为出发点对风险进行控制，发生安全事件后，第一时间确定受影响资产，提升分析研判速率，能够做到及时应急处置响应。具有如下两项亮点实践。

资产识别

亚运各场馆及赛事管理机构内存在大量的日志资源收集设备，并且存储较多的网络隔离，通常需要采用分布式日志采集的方式进行复杂异构数据采集。采用日志源资产重识别技术，通过资产识别技术实现对日志信息中包含的资产信息进行识别和处理。主要解决在不同的网络环境中，存在原资产直接发送日志或者间接通过日志平台中转日志等多种途径和方法，并且不同的传输方式通常采用不同的协议，甚至可能同一类型的资产位于不同的网络环境中。通过提出双栈协议识别技术实现不同网络环境的发送协议识别，实现对不同资产的识别和归类，有效的解决了复杂网络环境中的审计日志资产识别的技术难题。

资产分析

实现以业务资产视角，辅助亚运安全运维团队以资产为核心的工作层面之上构建一个面向业务部门和管理层的业务资产模型。业务建模功能主要管理用户的业务支撑系统，实现业务资产拓扑和资产安全等级评价等功能，为用户提供业务的实时监控能力，保障亚运业务的可持续平稳运行。为亚运提供如下功能：

针对亚运资产的自动发现和从客户现有的资产平台同步功能，实现了资产的修改、删除等管理功能，并根据客户资产的用途和网站结构进行划分，分为内部资产、互联网资产和重点安全资产；

> 提供安全资产拓扑视图，支持根据网络架构自定义资产拓扑，支持拓扑的模板导入和编辑好的资产拓扑文件导出；

> 提供根据近期重点关注基于业务安全威胁和业务脆弱性的业务健康度评价和资产评分；

> 用户可以根据具体的业务流程构建相应的业务模型，支持业务模型的管理功能。

> 同时支持选中某两天风险资产进行对比，通过对比，快速了解，修复了哪些资产、新增了哪些风险资产，风险上升有哪些资产，风险下降有哪些资产，可针对性对新增风险资产进行处置。

基于亚运场馆网络安全防护实践

赛事场馆包括竞赛场馆、非竞赛场馆和训练馆。这些场馆在体育赛事中发挥了不同的作用。竞赛场馆主要是比赛专用的场地，非竞赛场馆不直接用于比赛，主要是工作人员、运动员、媒体人员等活动的场地，训练馆主要是运动员在赛前比赛训练的场地。因此着重围绕竞赛场馆和非竞赛场馆提供网络安全保障，训练场馆可根据业务需求选择。

场馆分类

体育赛事场馆网络安全保障首要工作是根据场馆的规模、业务属性特点对场馆进行分类，以便更有针对性地实施相应的安全策略和措施。以亚运为例，将场馆分为一类场馆、二类场馆、三类场馆。

一类场馆包括杭州亚运会开闭幕式场馆、足球田径等大型比赛场馆、亚运村、MOC、ITCC、IBC、MPC等重要非竞赛场馆。

二类场馆包括杭州亚运会普通竞赛场馆（含临建场馆）、亚运分村、注册中心等非竞赛场馆。

三类场馆（所）包括总部酒店、高铁站、机场等迎宾场所和PC工厂等一般性非竞赛场馆。

场馆网络安全防护

赛事场馆主要涉及竞赛专网、互联网、设备网。其中竞赛专网和互联网为赛事组织机构负责建设的网络，也是赛事的核心网络。是场馆网络安全保障防护的重点。设备网一般是场馆自建的网络，虽然责任主体不在赛事组织机构，但其安全也将间接影响赛事的进行，也要兼顾考虑网络安全防护。

根据场馆的分类及场馆的业务特性针对性设计场馆网络安全防护，即场馆一馆一册，设计场馆网络安全防护内容。

竞赛专网是用于场馆比赛的专用网络，重要性高，其网络安全保护定级通常为三级，因此需要遵循网络安全法、等级保护2.0的三级标准要求进行网络安全防护设计。须部署下一代防火墙、堡垒机、日志审计、终端准入、流量分析、终端杀毒等防护和检测安全设备，同时一类场馆由于场馆资产数量众多，可以独立部署态势感知平台，感知场馆的整体网络安全态势。

互联网是用于场馆工作人员的使用的网络，其网络安全保护定级为二级/三级，因此需要遵循网络安全法、等级保护2.0的二级/三级标准要求进行网络安全防护设计，部署相关网络安全设备，但场馆工作人员众多，还须部署上网行为审计设备，实时分析上网行为，保障场馆互联网安全。

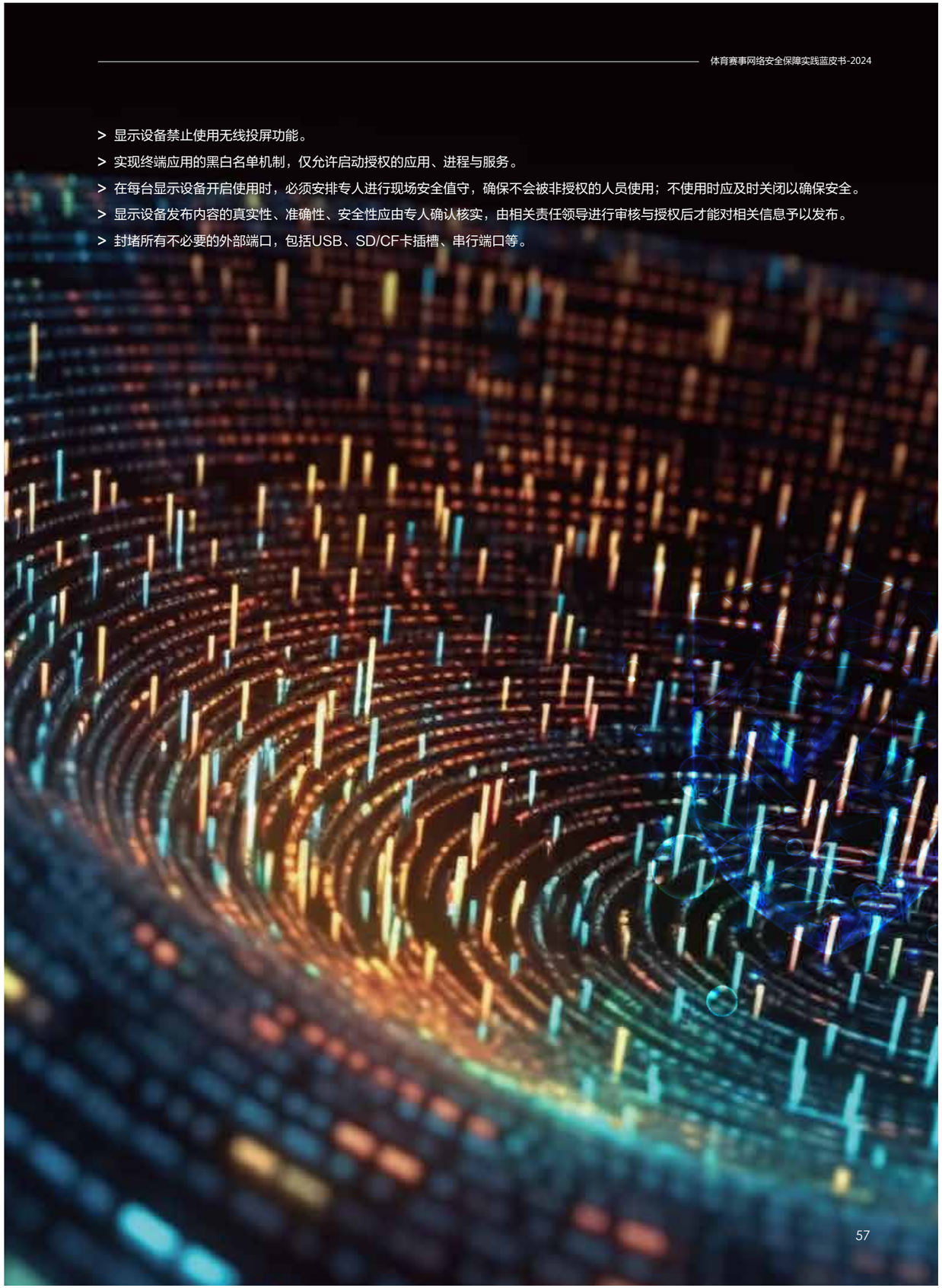
设备网属于自建网络，其网络安全防护需要根据调研情况后进行网络安全防护设计，主要通过网络安全检测服务和值守保障两项服务来增强设备为的网络安全防护能力。网络安全检测内容包括但不限于：设备网网络、大屏控制器、设备网信息系统（如：升旗系统、门禁系统、音响控制系统等）、物联网设备等。

显示设备安全防护

显示设备，包括电视机、LED显示屏、灯光带等以及一切进行图像、文字输出的专用设备，遭受攻击将直接影响显示设备内容，引起舆论效应，因为显示的网络安全防护主要围绕显示内容控制端、内容审核管理机制、网络、接口等展开。

> 显示设备必须是一个相对封闭的网络，不允许与互联网进行任何通信，只允许同时接入一个固定的专用网络，如AGIS竞赛专网、视频专网等，不允许同时和多个网络进行通信。而针对显示设备需要发布的信息内容，必须采用专用U盘等人工方式进行内容上传/修改，不允许采用互联网平台进行内容管理。

> 显示设备禁止使用无线投屏功能。
> 实现终端应用的黑白名单机制，仅允许启动授权的应用、进程与服务。
> 在每台显示设备开启使用时，必须安排专人进行现场安全值守，确保不会被非授权的人员使用；不使用时应及时关闭以确保安全。
> 显示设备发布内容的真实性、准确性、安全性应由专人确认核实，由相关责任领导进行审核与授权后才能对相关信息予以发布。
> 封堵所有不必要的外部端口，包括USB、SD/CF卡插槽、串行端口等。



体育赛事
网络安全保障实践
蓝皮书 > 2024

第五章

赛事网络安全保障对城市级安全防御带来的应用与思考

赛事网络安全保障实践在企业级安全运营场景的应用

以安全运营视角的网络安全保障思路，在面对资产与流程多样、创新技术应用较多、安全保障场景复杂等综合维度时，在杭州亚运全期保障过程中，我们也积极地思考将赛事网络安全运营与保障能力，通过标准化的方式，赋能和转移到城市级安全防御的各类场景中，其中重点关注如何从亚运安保整体建设理念与思路出发，更加全面地实施重点行业场景相关业务系统应急响应、处置和保障，重保中的创新能力与技术手段如何赋能、以亚运视角分析如何在行业安全场景用好运营人员的能力与培养思路、从亚运中的网络安全突发事件处置过程获取丰富经验。

赛事侧规模化运营在集团化场景实践

赛事侧规模化安全运营与大型央国企、私有企业集团对安全运营的需求高度一致，一方面均要构建强有力的运营体系保障自身安全，面向监管侧进行安全合规层面的执行动作。另一方面要对下属分支机构（场馆）进行安全监督与赋能，确保整个组织（赛事）的安全有效。风险点位多、管理难度大、技术要求高，所以规模化运营赛事保障安全实践的经验，能够为集团化运营场景需求提供必要的赋能与思路创新。

在规模化运营实践中，基于安全态势感知、运营自动化处置平台构建运营技术支撑体系，通过传统网络安全服务与安全保障专家服务共同赋能，建立起覆盖内部风险与外部威胁的运营制度流程体系，确保安全保障的全面性与运营能力全面性，使集团化企业机构能够标准化执行安全保障管理动作。

图5-1 集团化场景实践

场馆侧个性化运营在中小规模机构场景实践

场馆侧个性化运营模式与众多中小规模机构组织运营需求高度适配。各类企业机构业务形态各异、安全基础水平不同、保护侧重不同，需要基于自身业务实际需要与安全资源确立自身安全运营实践路线，基于安全与业务平衡性的原则构建自身运营体系。

个性化安全运营模式，以网络端、主机端轻量化运营工具作为运营保障技术平台，配套云端各项安全治理与处置服务，配合本地基础安全服务与面向产品能力提升的专家服务，使中小规模企业机构在安全资源有限情况下实现自身安全运营保障闭环机制。

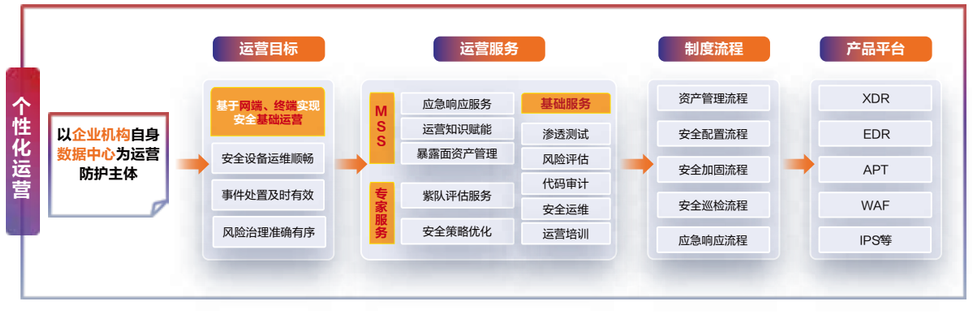


图5-2 中小规模机构场景实践

供应链轻量化运营在供应链场景实践

供应链轻量化安全运营与各企业机构软件供应链安全保障场景高度匹配。软件供应链日益成为企业机构安全事件的突破口，对软件供应链安全进行深度管控与运营显得尤为重要。参照赛事软件供应链保障经验，一方面可制定相关标准要求，设置软件交付的安全质量标准。另一方面针对上线前软件应用系统进行平台化安全检测，规避软件的带病上线。从而实现软件供应链安全的轻量化运营。

软件供应链安全轻量化运营，在面向各类企业机构软件供应链过程中，在设计、开发、测试、上线各环节潜入风险管控设备，配套相关安全服务内容，制定软件应用交付与上线安全标准，确保软件的健壮性与安全上线，在应用层面规避漏洞等风险威胁。

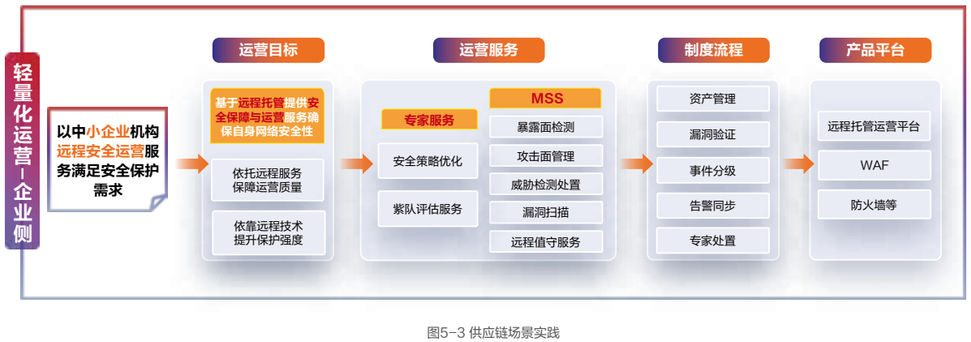


图5-3 供应链场景实践

护卫、自卫、迭代模式相结合的网络安全保障体系建设及应用

亚运会等大型赛事活动系统复杂、影响广泛、参与人数众多，往往成为攻击者的首选目标。针对赛事系统的攻击可能导致数据泄露甚至服务中断，而现有的攻击检测与防御手段在面对大型赛事活动时，暴露出实时性及准确性等问题，同时难以研判潜在的攻击者及攻击组织。盾立方网络安全立体防御体系针对重保活动不同阶段的特点，提出基于护卫、自卫、迭代模式相结合的网络安全保障体系，并在亚运会等赛事活动中进行了应用。该体系将大型赛事活动的安全保障划分为三个阶段：赛事前、赛事中和赛事后，并针对每个阶段的特点采用不同的防御模式。

赛事前：自卫模式

在活动开始之前，主要依赖自身的防御措施来确保安全，即“自卫模式”。在该阶段提前发现并修复可能存在的安全问题，强化系统和应用的安全性。为实现这一目标，可采用如下手段：

> **漏洞挖掘：**通过专业的安全团队对系统和应用进行全面的漏洞扫描和风险评估，提前发现并修复潜在的安全隐患；
> **拟态防御：**通过模拟攻击者的行为来检测和防御潜在的攻击，增强系统的防御能力；
> **可信计算：**通过确保系统和应用的完整性和可信度，防止恶意软件的植入和未经授权的访问；
> **主动免疫：**通过实施一系列的安全策略和防护措施，提高系统和应用对攻击的抵抗能力；
> **护网演练：**通过模拟真实的攻击场景进行演练，检验和提升团队的应急响应能力。

赛事中：护卫模式

在活动期间，主要依靠外部防御措施来对抗攻击，即“护卫模式”。该阶段实时监测和精准防御外部的攻击行为。为实现对赛事系统的安全护卫，采用盾立方威胁探测、关联研判与阻截体系，具体包括：

- **威胁探测：**通过部署四蜜系统来诱捕和监测潜在攻击者的行为，为后续的防御提供情报支持；
- **关联研判：**通过分析不同来源的安全情报和日志信息，分析和研判潜在的安全威胁和攻击行为；
- **设障阻截：**通过协同不同层面的安全防护设备和防御措施，如终端安全、网络边界安全等，实现立体化的防御阻断。

赛事后：迭代模式

在活动结束后转入系统重建和迭代阶段，即“迭代模式”。该阶段通过复盘和分析攻击行为来强化防御措施。利用每次赛事活动之间的窗口期来分析攻击IP的历史活动痕迹和攻击特点，为未来赛事活动提供更有针对性的防御策略。同时，通过对攻击IP进行统一的攻击画像，可以更深入地了解攻击者的行为模式和意图，为未来的防御工作提供有力的支持。

城市级信息系统是城市运行的重要支撑，保障其安全对于城市的稳定运行至关重要。护卫、自卫、迭代模式相结合的网络安全保障体系可以为城市级信息系统提供全方位的安全保障，有效防御各种未知的网络攻击和威胁。在城市级安全防御中，在不同阶段采用不同的防御模式，可以更好地应对各种潜在的安全威胁和攻击行为。此外，随着技术的不断发展和网络威胁的不断演变，城市级安全防御需要不断更新和适应新的技术。护卫、自卫、迭代模式相结合的网络安全保障体系通过持续的技术研究和创新，可以不断提升城市级安全防御的水平和技术适应性，有效应对不断变化的网络安全威胁。

城市级网络威胁情报库建设与应用

城市级网络威胁情报库建设与应用是支撑城市重大赛事活动、保障关键基础设施安全、提升城市网络安全防护能力的关键环节。建立一个全面且实时更新的城市级威胁情报库，可以应用于风险评估、策略制定、事件响应等多个场景，为城市的网络安全决策提供支持。

建设城市级网络威胁情报库，建议从以下几个方面进行考虑。

需要网络安全管理机构强力统筹、协同建设

网络安全管理机构拥有对城市网络安全整体状况的综合视角，能够更全面地了解城市网络威胁态势。通过整合各相关利益方的资源和专业知识，实现城市级网络威胁情报库的科学建设和可持续发展。网络安全管理机构应促使各方共享威胁情报，形成更为完整和准确的威胁图景，提高城市整体的网络安全水平，有效防范和应对横向攻击。此外，网络安全管理机构还要整合城市范围内的网络安全资源，包括技术专家、设备、工具等，提高资源利用效率，避免冗余投入，从而提升城市的整体网络安全水平。在法规合规方面，网络安全管理机构能更好地理解和落实相关法规政策，以确保相关数据的合法获取、存储和共享，同时保护个人隐私。

需要构建威胁情报信息（Cyber Threat Intelligence, CTI）汇总通道

威胁情报信息汇总通道的建立旨在实现全面、实时、可操作的威胁情报数据采集、整合和分发，以增强城市网络安全的监测和响应能力。通过收集开源情报、私有情报、政府情报等多源信息，使得城市级网络威胁情报库能够获取更广泛、更多样化的威胁数据，提高对各类潜在威胁的辨识和理解。构建CTI汇总通道不仅有助于城市网络防护团队及时获取最新威胁信息，实现实时响应和采取防御措施，同时也支持城市级网络威胁情报库深入了解当前威胁形势，分析攻击趋势，提升网络安全感知度。

需要制定CTI统一描述框架

在构建城市级网络威胁情报库的过程中，来自不同来源的威胁情报数据可能存在多样的格式和结构。为确保威胁情报的高效融合、互操作性、可读性和易于管理，必须制定一个完善的威胁情报统一描述框架，以确保各类威胁信息能够准确、一致地被描述、存储和分享。一些已存在的行业标准，如STIX（Structured Threat Information eXpression），提供了一套结构化威胁信息表达方式，通过特征化威胁源、攻击动机、攻击手段和防御措施等，成为目前广泛采用的威胁情报数据格式之一。TAXII（Trusted Automated eXchange of Indicator Information）规定了数据传输共享的规范，支持在组织、产品和服务之间跨界共享网络威胁情报。威胁情报内容多、格式复杂、差异性大，在构建城市级网络威胁情报库的时候，可根据城市的特点和特色，制定符合其特点的CTI统一描述框架，更好地实现各类威胁情报的融合，为网络安全管理提供更为全面、深入的信息支持。

需要建设城市级的统一的威胁情报共享分析中心（Cyber Threat Intelligence Center, CTIC）

CTIC旨在协调、整合和分析各类网络威胁信息，提供更全面、深入的洞察力，以加强城市网络安全的防护和应对能力。CTIC的建设需要与整体的网络安全战略规划相协调，确保其目标与城市级网络威胁情报库的构建一致。该中心应在整个网络安全生态系统中发挥协调作用，确保各相关方能有序共享和获取关键的威胁情报信息。同时，CTIC应成为不同部门和机构间协同合作的平台。通过促进政府机构、行业组织、企业和学术机构之间的协同，确保各方能够共享实时的威胁情报，有力应对复杂多变的网络威胁环境。

需要建立威胁情报跨部门分享与激励机制，鼓励并促进威胁情报分享

在构建城市级网络威胁情报库的过程中，缺乏有效的激励机制可能导致共享成员之间的互不信任和共享动力的不足，进而影响共享的安全性。为促进各部门之间的积极合作和信息共享，建议建立威胁情报跨部门分享与激励机制，通过设计激励机制，如奖励制度、荣誉奖项等多方面的激励手段，以激发部门间威胁情报分享的积极性，确保分享者能够得到应有的认可和回报。通过建立完善的威胁情报跨部门分享与激励机制，城市级网络威胁情报库能够更充分地利用各方的专业知识和资源，形成一个联防联控的网络安全防线，以提高城市网络的整体抵御能力，确保网络安全得到更有效的保障。

需要有强力机构组织协调并执行相关策略

网络威胁通常呈现出复杂而动态的特性，涉及多个层面和多个参与方。为了建设城市级网络威胁情报库，必须整合各种信息来源，分析大量数据，制定和执行相关策略。因此，建议通过一个强力机构来协调和管理，从而确保系统的高效运作。强力机构的强制性可以更迅速地协调行动，追踪攻击者，并采取紧急措施。这种迅速而有力的反应能力是城市网络安全的重要保障。通过建立这样一个强力机构，城市网络威胁情报库能够更好地组织、协调各方力量，强制执行相关政策和策略，从而提升城市网络安全的整体水平。

各端边网疆对来自CTIC的策略要具有参考执行的能力

在建设城市级网络威胁情报库的过程中，应确保端点、边界、网关、疆界的拦截阻断系统对来自CTIC（威胁情报共享分析中心）的策略具有参考执行的能力。为此，需要在各个网络节点和边缘设备上实现高效、实时的威胁情报传递和执行策略的机制。鉴于网络威胁的不断变化，各端边网疆对来自CTIC的策略参考执行可根据最新的情报和威胁模式调整防御策略，使其更具适应性。将威胁情报集中管理在城市级数据库中有助于更有效地进行分发和同步，确保各端边网疆从同一来源获取并执行最新的策略，保障整个城市网络的一致性和协调性。

基于城市级网络威胁情报库进行网络安全防御能够及时分析已发生的入侵，并对未来威胁态势进行推测预判，并据此评估潜在的安全风险以指导制定有效的安全决策，系统化增强城市网络空间防御能力。城市级网络威胁情报库为城市的重大赛事活动的开展提供了不可或缺的支持，通过实时更新和分析网络威胁信息，能确保在重大赛事活动期间有效监测和防范潜在的网络攻击，保障赛事相关业务系统的稳定性。城市级网络威胁情报库可进一步提升城市关键基础设施的安全保障能力，通过关联能源、金融、教育、通信等多个行业领域的威胁情报，为城市级安全保障提供强有力的助力。此外，城市级威胁情报库通过全面、实时的威胁信息融合与分析，可为城市制定更加精准、有效的网络安全策略提供支持，通过最小化潜在网络攻击的影响，确保城市网络的可用性和完整性。因此，构建城市级网络威胁情报库，建立跨部门的信息共享与协同机制，形成联防联控的网络安全防线，有助于提升整体网络安全水平与能力。

网络安全保障人才培养标准化实践

体育赛事网络安全保障活动中网络安全保障人才培养是确保保障活动顺利进行的基础。因此，网络安全保障人才培养应从技能、课程、实验平台、认证以及管理等方面展开，确保能系统化培养数量足够的符合标准的网络安全保障人才。

网络安全保障技能体系

对于不同类型的安全保障人员，建立网络安全保障所需的基础技能体系树。总体可从攻防两端建立技能：

攻击方面，为全员建立基础的攻击知识体系，确保知攻才能善守；针对攻击测试人员，建立完备的渗透测试技能体系，从而在赛事开始前通过大量渗透测试发现赛事系统安全问题。

防护方面，为全员建立基础的防护知识体系，攻击测试人员通过了解防护可更好地展示渗透测试；针对专门防护人员，围绕网络安全保障运用的防护工具/系统，建立功能、操作、运维和告警处置的技能体系，确保人员能熟练运用系统解决安全问题。

网络安全保障课程体系

课程体系是人才培养的重要基础，网络安全保障课程体系建设可从两方面展开：

一方面，与高校合作，推动高校课程理论结合实践，结合高校课程体系建设，将人才培养所需的技术方法融入高校现有的课程体系建设中，作为高校课程实践的重要部分进行设计、推动。

另一方，建立独立的快速培训机制和对应的课程体系，通过1-2周的短期强化培训，针对当前赛事活动培养一批速成网络安全保障人员。

网络安全保障实验平台

针对专业实践教学在人才培养过程中的作用和有效性落实不足、虚拟仿真教学资源缺乏特色这两方面的问题，探索实践教学开展新模式，通过采用“虚、实”结合的解决路径，打造学习平台，基于网络靶场，构建网络安全保障教学实践平台，解决历届体育赛事实际情况，构建赛事演练场景并应用于实践教学。充分利用靶场优势，将攻击和防护一些实操训练和人才选拔在靶场上进行，培养和挖掘更多符合安全保障需求的网络安全人才。

网络安全保障人才认证体系

针对体育赛事网络安全保障不同人员类型，建立对应的人才认证体系。明确人才培养目标、人才应具备的技能水平、人才认证方式和方法、人才认证的机构设置等一系列机制，建立可操作的人才认证方法和举措。通过人才认证体系选拔出一批符合网络安全保障的人才队伍，作为安全保障的预备军。

网络安全保障人才管理

考虑依托网络安全人才教育联盟，成立网络安全保障人才管理相关部门，打通网络安全保障人才培养、召集链路，形成规范化流程。充分利用网络安全企业和高校的人员优势，联合培养网络安全保障人才，建立网络安全保障人才蓄水池，做到一旦遇到体育赛事网络安全保障活动，可有充足的可用人员。

推动网络安全保障专家的培养和挖掘，维护一支相对稳定的网络安全保障专家团队，作为整个网络安全保障的“智囊团”，为保障工作提供保障思路和建议。

建立网络安全保障人才责任机制和激励制度，一方面，明确人员职责，做到工作任务明确、责任归属清晰，确保人员工作有据可依；另一方面，建立有效地激励帝都，从荣誉、经济两方面激励人才发挥主观能动性。

附件、场馆十大风险

场馆是体育赛事的主要载体，控制和监控体育赛事场馆网络安全风险，制定恰当的场馆风险控制技术、管理手段是体育赛事进行风险控制的有效手段。结合体育赛事场馆大量网络安全风险、案例，现将场馆十大风险列举如下：

1 大屏（视频）

风险描述：场馆电子显示设备被恶意插播或页面被篡改。

风险应对：赛时期间安排人员定期巡检，关闭电子显示屏多余端口，关闭WIFI连接，制定电子显示设备内容播放审核流程制度。

2 广播（音频）

风险描述：场馆广播设备被恶意插播。

风险应对：赛时期间安排人员定期巡检，制定广播设备使用审核流程制度。

3 网络（竞赛专网&互联网）

风险描述：一机两用，接入互联网的电脑未经任何病毒查杀就接入竞赛专网，使此台电脑成为攻击者入侵专网的跳板。

风险应对：部署APT进行攻击检测，出口边界部署防火墙、准入控制等做访问控制，终端PC安装EDR做为终端管控，安装上网行为设备对日常上网行为做审计记录，定期进行安全审计、审查，并做好安全意识培训。

4 门禁

风险描述：赛事场馆筹备与赛时，不法分子可能蓄意以各种方式窃取、破坏场馆信息资产，可能导致资产机密性缺失、不可用或者不完整；近而干扰或破坏赛事的正常召开。

风险应对：（1）主要设备放置在机房内，将设备或主要部件进行固定，对机房等重要场所划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域；重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。

（2）加强安保巡逻，增加巡检频度。

5 通讯

风险描述：通过在赛事场馆内或周围对无线wifi、有线网络电磁泄露进行嗅探、偷听、搭线窃听等途径非法获取信息。

风险应对：接入场馆wifi应采用身份验证，禁止私搭wifi，各类设备应做好接地。

6 防火墙

风险描述：场馆业务系统与外部单位业务系统进行数据对接时，未进行权限管控和逻辑隔离，存在安全风险；

风险应对：通过边界防火墙与外部业务系统进行访问控制；策略多进行沟通，并做好流量监测。

7 信息系统

风险描述：境内外非法组织、不法分子、黑客等没有权限的用户试图越权访问到场馆业务信息，或者较低权限的用户试图访问更高权限的场馆信息，近而控制系统或窃取赛事相关敏感信息；

风险应对：部署APT做攻击检测、出口边界部署防火墙、准入控制等做访问控制，终端PC安装EDR做为终端管控，配置上网行为设备对日常上网行为做审计记录，并定期进行安全审计、审查。

8 数据信息泄露

风险描述：在场馆业务系统开发过程中滥用真实、敏感数据、资源或服务，场馆业务系统因攻击或内部人员操作出现数据泄露风险；

风险应对：（1）涉及的承建单位应做好相应系统数据管理工作；

（2）场馆业务系统事前配置数据库审计、入侵检测等产品。

9 人员管理

风险描述：境内外非法组织、不法分子、黑客等非授权人员冒用赛事执委会或赞助商、承建商等授权人员身份；

风险应对：（1）采用账号密码类身份认证措施，设备采用双因素认证机制。

（2）对执委会和场馆所有人员加强安全意识培训。

10 网络攻击舆情

风险描述：境内外非法组织、不法分子、黑客等以技术手段对赛事系统进行DDoS攻击，造成系统不可用，出现舆论影响；

风险应对：全力防御；消除舆论影响。