四川省生态环境保护信息安全攻防演练项目技术方案

一、项目背景

四川省环境信息中心作为四川省生态环境厅的直属单位,承担了四川省生态环境厅网络安全管理与维护保障工作。根据网络安全法、数据安全法、个人信息保护法、网络安全等级保护基本要求等相关法律法规和标准，结合上级监管部门和行业主管部门要求，在多年不断强化和提升网络安全防护能力的工作过程中，进行了常态化的安全运营，保障了省厅网络和信息安全可靠。

在网络攻击广泛复杂、网络安全威胁形势日益严峻的当下，政务网络和政务信息系统作为国家网络的重要组成部分，成为网络攻击的重点目标，对现有政务网络安全防御体系能力提出了巨大挑战。在新的形势要求下，需从攻防两方面的角度多层级、多手段审视检验当前省厅网络安全防御体系，以实战的方式积极主动应对网络攻击威胁，组织开展实战型攻防演练，对省厅现有安全防护能力、安全运维能力、安全事件的监测、应急响应能力等进行实战检验，查找网络安全建设短板,以短板问题为导向深入分析安全防护管理弱项,持续提升防御体系能力，强化整体防范化解重大网络安全风险水平。

同时，为强化省厅对全省生态环境行业网络安全监督管理职能，推进市（州）网络安全责任落实以及网络安全防护能力建设，了解掌握市（州）安全防护状况，排查网络安全风险，堵塞网络安全漏洞，计划对5个市（州）生态环境局开展网络安全技术检测。

二、服务遵循标准

本次项目服务遵循的法律法规和技术标准规范包括:《中华人民共和国网络安全法》《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》《关键信息基础设施安全保护条例》《信息安全技术 关键信息基础设施安全保护要求》(GB/T 39204-2022)《信息安全技术 网络安全事件应急演练指南》(GB/T 38645-2020)《信息安全技术-网络安全等级保护基本要求》(GB/T 22239-2019)《信息安全技术-信息安全风险评估规范》(GB/T 20984-2022)《 信息安全技术 网络安全事件分类分级指南》(GB/T 20986-2023)《信息安全技术信息系统灾难恢复规范》(GB/T 20988-2007)等。

三、服务目标

组织攻击团队从攻击者视角开展网络安全实战攻防演练服务,将省生态环境厅直属单位、厅管社会组织与21个市（州）生态环境局纳入攻防演练服务范围，通过模拟攻击方视角进行深度实战攻击，检验网络安全现状，并采取威胁通报、督促整改等方式，确保问题风险得到有效解决。同时，以问题为导向深入分析当

前安全防护和管理弱项，提出安全防御能力完善优化建议，作为后续进行安全能力建设的有益输入。

对5个市（州）生态环境局开展网络安全技术检测，了解掌握各被检测单位网络安全管理情况、安全防护现状及能力水平、存在的安全隐患，为省厅开展网络安全工作督导提供有力的依据和抓手。一是评估现状。掌握各被检测单位在网络安全管理制度、技术防护体系、日常安全运营管理等方面的现状。二是发现问题。识别各被检测单位存在的突出问题和薄弱环节，分析面临的安全威胁和风险。三是推动整改。针对发现的问题提出整改建议，并督促各被检单位落实整改措施，形成长效管理机制。四是提升能力。促进各市州生态环境局加强网络安全意识，落实网络安全责任，进一步健全安全管理制度，完善安全技术措施，提升安全防护能力。

四、服务内容

（一）实战攻防演练服务

为切实检验全省生态环境部门网络安全防护水平，提升安全防护意识，计划在2026年12月前组织攻击团队从攻击者视角开展1次全省生态环境系统网络安全实战攻防演练。服务主要内容包括：演练组织、实战演练、复盘研究以及问题整改复查等工作，有效检验全省生态环境系统网络安全防护水平、查找短板。同时，以问题为导向深入分析当前安全防护和管理弱项，提出安全防御能力完善优化建议。

1.演练组织

目　标	根据四川省生态环境厅需求组织1次实战攻防演练服务，确保演练能有效检验全省生态环境部门现有安全措施的防护水平及应急响应能力。
范　围	省生态环境厅直属单位、厅管社会组织与21个市（州）生态环境局
内　容	配合采购人完成1次实战攻防演练的活动策划、演练方案制定、演练规则制定等工作，并安排专人协调推动演练工作进展。对演练成果进行汇总，按采购人需求进行评分与排名。
★人员要求	裁判服务要求：提供具有网络安全实战演练经验的裁判1名，对演练工作进行总体把控；专家服务要求：提供1名网络安全攻防专家，负责对演练整体方案进行研究把关，在演练过程中对攻击效果进行总体把控，负责演练中的应急响应支撑，保障演练安全可控。**（供应商需提供承诺函加盖供应商公章）**
频次	完成1次服务
交付物	《四川省生态环境厅实战攻防演练实施方案》
技术要求	1.演练活动策划：对演练的组织架构、演练方式、演练时间、演练流程等进行整体策划。 2.演练方案制定：在充分了解掌握省厅当前防御体系现状的前提下，针对省厅实际制定详细的演练实施方案，包括演练筹备阶段、实施阶段、总结阶段的工作内容、时间计划、资源保障计划等。 3.演练规则制定：根据演练目标、对象、方式等制定演练规则以及渗透测试评分规

	则。 4.成果汇总：演练结束后汇总攻击方和防守方成果，统计攻防数据，进行评分与排名。 5.根据采购人需求提供专业网络攻防演练平台对攻击过程进行审计，实现演练组织方与演练参与方之间的成果下发与上报，同时平台需满足以下要求： （1）演练过程审计。网络攻防演练平台能够从网络层捕获对目标主机的访问或入侵的数据信息，能够记录进出目标主机系统的原始网络数据包的数据信息，对捕获到的网络、主机数据信息进行综合分析。可以记录和禁止网络活动，扫描当前网络的活动，监视和记录网络的流量，对违规行为及时进行告警和阻断。 （2）攻防过程可视化。网络攻防演练平台能对抓取的攻击日志进行分析，建立完整的攻击场景，能够直观地反映目标主机受攻击的状况，实时监控攻击过程，并通过可视化系统监控大屏实时展现。真实全面地展示攻击方流量实时状态，展示攻方与被攻击目标的 IP 地址及名称。可展示攻防双方得分、排名、失分情况与攻防实况等，为后续进行总结分析提供数据支撑。 （3）攻防成果提交。攻防双方可通过攻防演练平台后台管理系统提交攻击或防守成果，包括目标系统名称、攻击域名、目标系统 IP、URL、系统描述、攻击队伍、截屏图片、攻击手段等。 3.实施方案内容需包含但不限于演练组织架构、演练时间计划、演练流程设计、演练资源保障计划、演练规则、评分规则等。

2.实战演练

目标	模拟恶意攻击者，从多视角对全省生态环境系统实际网络环境展开渗透攻击，查找全省生态环境部门网络安全薄弱点，全面检验全省生态环境部门已建的安全防护措施是否有效，检验现有安全管理防护流程是否满足应对组织化、规模化网络攻击的实战要求，具体包括： 1.发现单位系统存在的突出问题和深层次漏洞隐患； 2.检验网络安全监测发现能力、安全防护能力； 3.检验各部门之间的快速协同、应急处突能力； 4.积累实战经验，提升监测发现、安全防护和应急处置等能力； 5.全面评估整体安全态势以及网络安全能力。
范围	省生态环境厅直属单位、厅管社会组织与 21 个市（州）生态环境局
人员要求	★1.实战攻防演练需至少安排 4 支（每支 3 人）攻击团队参与渗透测试攻防演练。（供应商提供承诺函加盖供应商公章） 2.每支攻击队需熟悉历年全国实战攻防演练行动中总结的攻击队优秀技战法； 3.参与攻防演练的攻击人员应具备 3 年及以上漏洞挖掘、渗透测试、攻防演练等相关工作经验。 4.参与攻防演练的所有团队人员应为供应商正式工作人员或与供应商签订 1 年以上劳动合同且演练开展前在此供应商工作满 1 年的人员。
风险保障	采取有关措施降低实战演练可能带来的安全风险，包括但不限于参与人员签订保密协议和责任书、演练平台进行攻击队行为审计、攻击队电脑录屏等。
内容	组织攻击队全面模拟外部恶意攻击者可能采取的攻击方式，在适度、安全前提下，按照“一事一报备”原则，对四川省生态环境系统进行渗透攻击。
频次	完成 1 次服务，实战攻击周期为 7 天

交付物	《四川省生态环境厅实战演练成果报告》
技术要求	1.实战演练的攻击手段包括但不限于信息刺探、拒绝服务攻击（可选）、社会工程学攻击、供应链攻击、内网横向等。 2.信息刺探是收集四川省生态环境厅暴露于互联网上不需要额外的授权便可获取到的网络资产信息，包括但不限于网站后台、未授权页面，敏感 url、IP、网段、域名、服务端口、微信小程序、APP 等； 3.社会工程学攻击手段包括但不限于钓鱼邮件、水坑攻击、社交诱骗、近源攻击（如 Wi-Fi 破解、U 盘摆渡）等； 4.供应链攻击是收集并利用四川省生态环境厅的网络设备厂商、软件开发商、安全设备厂商等供应链暴露的产品源码、收录编号的漏洞、出厂默认用户名密码等信息，开展渗透攻击； 5.内网横向是突破边界进入内网后进行的渗透，包括但不限于收集当前计算机的网络连接、进程列表、命令执行历史记录、用户信息、管理员登录信息、密码规律，收集网络中明文传输，token 在 cookie 中传送等，以扩大内网攻陷战果，最终拿下目标系统权限； 6.实战演练报告内容需包含但不限于攻击路径、攻陷资产信息、危害描述、问题整改建议等内容。

3.演练复盘研究

目标	通过复盘帮助用户单位进一步了解被成功渗透的原因以及安全防护和管理短板，便于后续有针对性地整改，提高防御能力。
内容	针对实战攻防演练过程中，被成功渗透的重要案例，组织攻防双方进行复盘推演、研究分析问题及成因所在，同时为后续安全整改、建设提出优化指导建议，提升防御能力。
频次	完成 1 次服务（在实战演练后开展）
交付物	《四川省生态环境厅复盘总结报告》
技术要求	1.复盘研究需提供须具备漏洞挖掘、安全事件应急响应分析、对国内外最新攻防技术具有研究分析能力的人员作为复盘研究的专家，针对演练情况进行点评和深度分析。 2.专家点评和深度分析需在充分了解掌握省厅当前防御体系现状和本次演练情况的前提下进行，内容包括但不限于综合剖析演练检验的成果及四川省生态环境厅当前真实的网络安全状况，以及结合实战攻防演练和重大安全保障经验，为四川省生态环境厅提出针对性地实战化防护体系建设优化完善的建议。 3.复盘研究报告内容需包含但不限于对检验过程中所反映的四川省生态环境部门当前防御水平状况和问题、人员安全意识、演练数据和攻陷成果汇总、防守方排名、漏洞风险情况分析、渗透路径概览、安全防护和管理完善建议等。

4.演练问题整改复查

目标	核查修复整改情况，驱动安全问题的解决落到实处，从而达到有效提升安全防护能力的效果。
内容	对实战攻防演练服务中发现的全部问题进行复核验证，检查整改情况，确保过程中发现的风险清零。
频次	完成 1 次服务（在实战演练后开展）

交付物	《四川省生态环境厅问题整改复查报告》
技术要求	1.复核目标覆盖《演练实战报告》当中发现问题的全部网络资产； 2.问题整改复查报告需包含但不限于已修复情况、未修复情况及未修复原因说明等。

（二）安全技术检测服务

从网络安全管理制度方面、网络安全日常管理方面、网络安全技术防护方面以及网络安全风险隐患检测对市（州）生态环境局（含市（州）生态环境监测中心站）开展安全技术检测评估。

1.检测内容

（1）网络安全日常管理方面

从信息资产管理情况、漏洞管理情况、安全运维情况、安全监测情况、应急响应与处置情况、日志留存情况等方面对各被检单位进行检查。

①检查被检单位是否制定网络资产管理制度，是否建立有网络资产清单，是否明确了资产的管理责任人。（注：重点查阅资产管理制度、资产台账等文档。）

②检查被检单位是否建立漏洞管理工作机制，是否定期对本单位主机、网络安全防护设备、信息系统进行漏洞检测，对于发现的安全漏洞是否进行修复处置。（注：重点查阅漏洞扫描记录、漏洞处置报告。）

③检查被检单位是否按照制定的规章制度、运维流程、操作规程等执行网络系统日常维护并有详细记录。（注：随机抽查网络安全设备巡检、安全策略配置变更、系统升级维护等相关运维记录表单。）

④了解被检单位是否建立网络安全监测工作机制，是否安排专人对网络安全系统产生的网络入侵、病毒木马等告警事件进行监测、分析、研判和处置。（注：查阅网络安全事件分析、处置报告或工作记录。）

⑤检查被检单位是否针对网络安全事件制定应急预案，是否定期（每年至少一次）组织开展网络安全应急演练，是否根据演练情况对预案进行修订完善。（注：重点查阅应急预案、演练方案、演练实施记录文档。）

⑥检查被检单位是否按照规定采集并留存网络安全设备、主机应用系统日志，日志留存时间是否符合不少于6个月的时间要求。（注：随机抽取2—3台网络安全设备和服务器，上机查看日志配置情况，登录日志审计系统，查看日志留存时间。）

（2）网络安全技术防护方面

从网络整体架构安全情况、边界安全防护情况、核心应用系统安全防护情况、终端计算机安全防护情况等方面对各被检单位进行检查。

①检查网络拓扑图，评估网络的整体设计，包括网络分区、关键系统的隔离措施，以及不同网络区域之间的通信是否采取了合适的安全措施。

②检查是否在网络边界部署了访问控制（如防火墙、入侵防御、安全审计以及非法外联检测、病毒防护）等必要的安全防护设备。（注：查阅网络拓扑，机房实物勘查。）

③检查重要应用系统（如门户网站、环境监测系统）是否部署应用安全防护系统，是否定期对主机和应用进行漏洞扫描和安全加固。（注：抽取1至2个三级等保系统，上机勘查是否部署防护系统，查阅具有相应的漏洞扫描、渗透测试、整改加固等报告。）

④检查终端计算机是否安装了防病毒软件，并评估其是否保持更新以应对最新的病毒威胁，是否建立了补丁管理制度和流程，并定期进行漏洞检测和补丁更新。（注：随机抽取4—5台办公终端，查验杀毒部署情况、病毒库更新情况、系统补丁修补情况。）

（3）网络风险隐患检测方面

主要对重要网络安全防护设备、重点业务应用系统的安全基线配置进行检查，对安全漏洞隐患进行探测，对安全防御设备的有效性进行评估，对异常受控外联情况进行检测。

①通过人工上机排查方式，针对关键网络安全设备和重要应用服务器，对其安全策略、密码策略、账户权限管理、日志审计、访问控制策略等配置进行核查，识别不安全的配置项。（注：网络安全设备（如边界防火墙、入侵防御系统、WAF等）抽选2—3台；重要应用系统（三级等保）抽选2—3台服务器。）

②利用网络风险资产监测分析技术对被检单位的核心应用服务器网段进行风险探测，识别系统存在的高危漏洞、高危端口、弱口令等风险隐患。（注：扫描对象为被检单位本地机房服务器网段。）

③利用网络安全防御策略有效性检测评估技术检验被检单位的相关安全防护设备在面对各类互联网边界突破攻击时，是否能够对攻击行为进行有效识别和拦截阻断，验证安全防御措施的有效性。（注：检测对象为被检单位互联网网络区域的安全防护设备。）

④基于国家权威威胁情报资源，利用威胁情报联防阻断对被检单位网内主机产生的异常外联行为（如APT隐秘通道、后门木马、勒索病毒、挖矿病毒）进行侦测，发现内网失陷主机风险隐患。（注：检测对象为被检单位本地机房的服务器区域和办公终端区域，检测设备旁路部署至被检单位核心网络交换机。）

（4）网络安全管理制度方面

协助采购人从网络安全管理制度建设情况、安全管理机构设置情况、服务外包管理情况、安全教育培训情况、网络安全经费保障情况等方面对各被检单位进行核查。

2.检测形式

通过人员访谈、文档查阅、配置核查和技术测试相结合的方式对被检单位开展网络安全现场安全技术检测。

（1）人员访谈。通过与被检单位的网络安全负责人、系统操作员等进行访谈、交流，了解被检单位网络系统的运行状况、安全策略的制定与执行情况，以及对网络安全政策的理解和遵守程度。

（2）文档查阅。通过查阅被检单位的相关网络安全管理文档、操作日志、事件处理记录等，评估网络安全管理的规范性和有效性。

（3）配置核查。使用配置管理工具或手工检测方式，对照安全配置基线，检查关键系统和设备的配置，识别安全配置风险隐患。

（4）技术测试。利用有关技术工具，对被检单位网络安全防护措施有效性进行验证，对信息系统安全风险隐患进行检测评估。

3.检测流程

（1）开展现场检测。编制检测方案，依据检测方案，通过人员访谈、文档审查、配置核查和安全测试等方式，对被检单位的网络安全管理、技术防护体系的现状、风险、漏洞隐患等进行识别、分析。对检测过程中发现的网络安全漏洞、隐患、问题和风险，进行逐条整理登记。

（2）检测结果分析。根据访谈交流、资料审查、现场检测和技术测试的结果，对被检单位的网络安全防护情况进行综合评价，指出存在的问题和不足，并提出针对性的整改建议，形成正式检测评估报告。

（3）检测结果复测。根据整改报告，针对检测过程中发现的问题，进行复测，确认整改完毕。

五、★服务要求

1.供应商应具有与本项目匹配的服务能力。

2.本次服务所涉及的专业平台与工具由供应商自行筹备。

3.在项目实施或服务过程中，需明确1名项目经理负总责，项目经理应具有丰富的网络安全服务项目管理、咨询、沟通协调能力，具有预见和应对项目风险能力，明确有网络安全技术检测及网络安全实战演习经验的安全专家1名、对项目实施质量总体把控。除此之外，攻防演练服务还须提供裁判1名，4支（每支3人）攻击团队，安全技术检测服务中需至少保证2名网络安全专业技术人员开展实施。供应商应保证提供服务的团队人员的稳定性，未经采购人同意不得随意更换团队成员。

4.在服务过程中应采取安全可靠的技术控制措施，在开展技术服务过程中不得影响系统和网络的正常运行(包括系统功能显著下降、网络拥塞、服务中断等)，

不得使用境外 ip 地址，确因技术检测需要的，须提前报备，在得到采购人确认后方能开展相关技术服务工作，同时严禁批量获取、存储、分析、篡改、删除系统或设备的数据。服务结束后，供应商应及时全量清理服务过程中植入系统的攻击武器或工具，恢复还原系统原有配置，彻底删除服务过程中产生的日志和获取到的系统信息等各类数据。

5.供应商在服务期内应提供 7*24 小时技术支持服务，服务方式包含但不限于现场、语音电话。服务请求应在 10 分钟内响应，如现场人员解决不了，高级技术人员应于 1 个小时内到达现场，应于 2 小时内处理相关故障，并形成书面处理记录。在服务过程中，根据采购人要求，供应商有义务对采购人相关人员进行相关安全技术培训。

6.供应商对过程数据和结果数据严格保密，未经采购人授权不得公开发布、泄露给任何单位和个人，不得利用此数据进行任何侵害采购人的行为，否则采购人有权追究供应商的责任。供应商提供的技术服务，不得侵犯任何第三方的合法权益，由此而引起的纠纷或者给第三方以及采购人造成的损失，应由供应商承担全部责任。

7.供应商在提供攻防演练服务过程中，不得对靶标以外的网络和系统、靶标使用的信息技术产品上下游供应商实施网络攻击，确需开展的，需提前报采购人同意。演练期间的攻击流量、操作日志等数据在演练服务结束后应及时移交采购人。

8.供应商服务过程中发现危害或可能危害国家安全、公共利益的网络安全风险事件，应及时报告。涉及安全漏洞的，不得擅自出售、透露、转让、公布漏洞的技术细节、利用方法、工具等。供应商不得向服务范围内涉及的单位额外或变相收取费用，或者要求其购买指定产品或服务。

9.供应商应协助、配合采购人、监理单位等的工作，按照经采购人同意的技术要求和实施要求进行项目实施，完成与项目有关的采购人提出的其他任务。供应商项目实施、人员等管理按照采购人项目管理制度执行。同时根据采购人需求，提供网络安全体系化防御咨询建议， 梳理网络安全上级监管机构、监管要求、网络安全建设遵循及要求等。

10.供应商在项目交付过程中应遵循国际、国内主流安全技术交付标准，提供要素齐全规格统一的成果报告资料，并对其负责。交付物包含但不限于服务要求的所有报告。

11.为采购人 3 名指定人员提供 CISP 证书到期续期指导与代办服务。