基于等保 2.0 验证测试与 ATT&CK 攻击矩阵的融合实践*

颜星晨[1,2]，张　鑫[1,2]，周志洪[1,2]，陈恺凡[1,2]
（1. 上海交通大学　计算机学院，上海　200240；2. 上海交通大学　信息安全服务技术研究实验室，上海　201203）

摘　要：围绕网络安全等级保护 2.0 制度框架下的渗透测试方法展开研究，结合 ATT&CK 攻击矩阵构建动态化安全验证体系。通过对等保 2.0 中安全通信网络、安全区域边界、安全计算环境等核心控制点的技术验证要求进行深入分析，将传统渗透测试流程与 ATT&CK 战术技术相融合，提出多维度测试场景设计、攻击链闭环验证和防御能力量化评估三位一体的新型验证框架。选取工控系统典型场景进行实证分析，证明该方法能有效发现等保合规盲区，提升系统主动防御能力和实战对抗水平。研究结果为网络运营者落实等保制度提供了可操作的渗透测试方案，推动网络安全防护从合规导向转向能力导向。

关键词：网络安全等级保护；ATT&CK；渗透测试
中图分类号：TP309　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097-1788.2025.09.003
引用格式：颜星晨，张鑫，周志洪，等. 基于等保 2.0 验证测试与 ATT&CK 攻击矩阵的融合实践［J］. 网络安全与数据治理，2025，44(9)：15-21.

Integrated practice based on Cybersecurity Classified Protection 2.0 validation testing and the ATT&CK matrix

Yan Xingchen[1,2], Zhang Xin[1,2], Zhou Zhihong[1,2], Chen Kaifan[1,2]
(1. School of Computer Science, Shanghai Jiao Tong University, Shanghai 200240, China;
2. Information Security Service Technology Research Laboratory, Shanghai Jiao Tong University, Shanghai 201203, China)

Abstract: This research focuses on penetration testing methodologies within the Cybersecurity Classified Protection 2.0 (CCP 2.0) framework, establishing a dynamic security validation system through integration with ATT&CK attack matrix. By conducting in-depth analysis of the technical verification requirements for core control points in CCP 2.0—including secure communication networks, security boundaries, and secure computing environments—we combine traditional penetration testing processes with ATT&CK tactics and techniques, and propose a novel validation framework characterized by multi-dimensional test scenario design, closed-loop validation of attack chains and quantitative assessment of defensive capabilities. Empirical study on industrial control systems demonstrates that this approach can effectively identify compliance blind spots in CCP implementations while enhance systems' proactive defense capabilities and resilience against real-world attacks. The research provides network operators with actionable penetration testing solutions for implementing CCP standards, thereby advancing cybersecurity from compliance-driven to capability-oriented defense paradigms.

Key words: cybersecurity classified protection; ATT&CK; penetration test

0　引言

随着《中华人民共和国网络安全法》（以下简称《网络安全法》）的深入实施，网络安全等级保护制度[1]（以下简称“等保 2.0”）已成为我国网络空间安全体系的核心制度框架。等保 2.0 不仅对网络运营者提出了法定合规义务，更要求通过技术验证手段证明安全措施的有效性。在这一背景下，渗透测试[2]作为主动安全评估的核心技术手段，在等保测评中扮演着关键角色。然而，当前在等保 2.0 实施过程中，渗透测试仍存在测试场景碎片化、攻击链覆盖不完整、验证标准不统一等问题，难以满足对抗高级持续性威胁（Advanced Persistent Threat，APT）的需求[3]。

*基金项目：国家自然科学基金（62202303，62471301）

除此之外，随着云原生技术的普及，等保 2.0 在云环境扩展要求（如虚拟化隔离、容器安全）面临新的渗透测试挑战（如动态拓扑、短暂生命周期）。同时，ATT&CK 框架[4]的持续演进要求测试方法动态适配新兴攻击技术。

与此同时，MITRE ATT&CK 框架作为描述攻击行为的标准化知识库，为理解攻击者战术、技术和过程（TTPs）提供了系统性参考。将 ATT&CK 矩阵融入等保 2.0 渗透测试实践，可实现从“合规检查”到“能力验证”的转变，这正是本研究要解决的核心问题。

本文从等保 2.0 的技术验证要求出发，结合 ATT&CK 攻击矩阵构建融合式渗透测试框架。研究内容包含：等保 2.0 技术验证要求与渗透测试的映射关系；基于 ATT&CK 的渗透测试场景设计；融合框架在典型行业的应用实践等。研究成果将为网络运营者提供可操作的渗透测试方法论，推动网络安全防护从合规基线向实战能力升级，从而进一步提升网络安全新质战斗力[5]。

1 相关理论与技术背景

1.1 等保 2.0 框架下的验证测试要求

网络安全等级保护 2.0 制度在技术层面构建了分层防护体系，其核心要求覆盖安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心五大领域。在验证测试方面，等保 2.0 强调技术验证与管理核查并重，具体要求包括：

（1）技术验证方法：等保 2.0 明确要求采用漏洞扫描、配置检查、渗透测试等技术手段验证安全措施有效性。其中，三级及以上系统强制要求进行渗透测试，以验证系统的抗攻击能力。测试内容需覆盖网络设备、安全设备、主机系统、应用系统等关键对象，重点验证边界防护、入侵防范、恶意代码防护等控制点。

（2）测评指标体系：等保 2.0 采用分层量化评估模型，将测评指标分为安全控制类（10 类）、控制点（71 项）和安全要求项（211 项）三个层级。2021 年新版测评标准采用缺陷扣分法，对关键指标（权重 3 倍）、重要指标（权重 2 倍）和一般指标（权重 1 倍）设置差异化扣分标准，大幅提高渗透测试发现的漏洞对最终评级的影响。

（3）行业扩展要求：针对工业控制系统等特殊场景，等保 2.0 增设安全扩展要求，如禁止工业控制网络使用通用网络服务（如 Email、Web、Telnet 等）、强制拆除控制设备的 USB（Universal Serial Bus）接口等物理端口等。

基于这些特殊要求需要针对性设计渗透测试方案，基于等保 2.0 要求的验证测试框架如图 1 所示。

1.2 渗透测试在等保测评中的定位

渗透测试在等保测评体系中承担攻击视角验证的关键角色，其定位体现在三个层面：

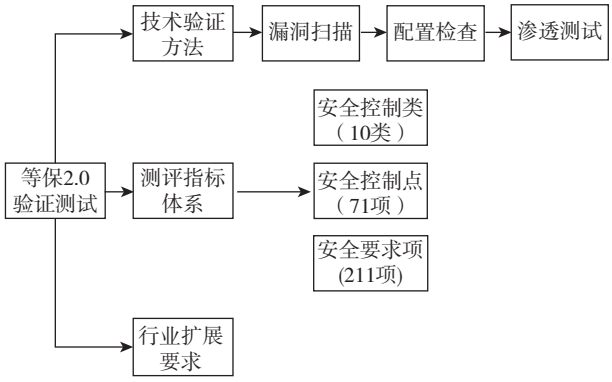

图 1 等保 2.0 验证测试框架图

（1）合规驱动层面：《网络安全法》第二十一条明确要求网络运营者采取“渗透测试、风险评估”等措施保障网络安全。在等保测评过程中，渗透测试通过对系统进行授权模拟攻击，验证其是否满足等保标准中的抗渗透能力要求。

（2）技术实施层面：等保测评中的渗透测试需遵循 PTES（Penetration Testing Execution Standard）标准化流程，包括前期交互、情报收集、威胁建模、漏洞分析、渗透攻击、后渗透攻击和报告七个阶段。测试范围需覆盖网络层（如防火墙策略绕过）、主机层（如权限提升）、应用层（如 SQL 注入）等多维攻击面。

（3）风险管控层面：渗透测试实施需严格遵循授权边界与风险控制原则，禁止未授权测试，避免对生产系统造成影响。测试过程中需采用非破坏性验证手段，如使用流量镜像进行网络嗅探而非直接拦截业务流量。

1.3 ATT&CK 攻击矩阵的核心价值

MITRE ATT&CK 框架通过战术（Tactics）、技术（Techniques）和过程（Procedures）三个层级系统化描述攻击行为，为渗透测试提供结构化知识库。

（1）战术维度：涵盖攻击生命周期 14 个阶段，从初始访问（Initial Access）、执行（Execution）、持久化（Persistence）到命令与控制（Command and Control）、数据窃取（Exfiltration）等。这一维度使渗透测试能够模拟完整攻击链，而非孤立漏洞验证。

（2）技术矩阵：提供超过 200 项具体攻击技术描述，如“鱼叉式钓鱼附件（Spearphishing Attachment）”“凭证转储（Credential Dumping）”“域策略修改（Domain Policy Modification）”等。每项技术包含适用环境、检测方法和缓解措施等元数据，为渗透测试技术选型提供决策支持。

（3）防御评估导向：ATT&CK 的核心价值在于将渗透测试从“漏洞发现”提升到“防御突破”层面，通过

映射企业现有防御措施与攻击技术的对抗关系，识别防御盲区和检测失效场景，推动安全体系从“合规达标”向“实战有效”演进。

等保 2.0 技术要求与 ATT&CK 战术领域的映射关系如表 1 所示。

表 1　等保 2.0 技术要求与 ATT&CK 战术领域的映射关系

等保 2.0 控制类	核心要求项	对应 ATT&CK 战术	渗透测试验证点
安全区域边界	边界防护	初始访问（TA0001）	防火墙策略绕过测试
安全计算环境	入侵防范	执行（TA0002）	主机防病毒绕过验证
安全通信网络	通信传输加密	命令与控制（TA0011）	C2 通道加密检测
安全管理中心	安全审计	防御规避（TA0005）	日志清除测试
安全计算环境	身份鉴别	凭证访问（TA0006）	口令破解测试

等保 2.0 技术要求与 ATT&CK 映射模型架构如图 2 所示。

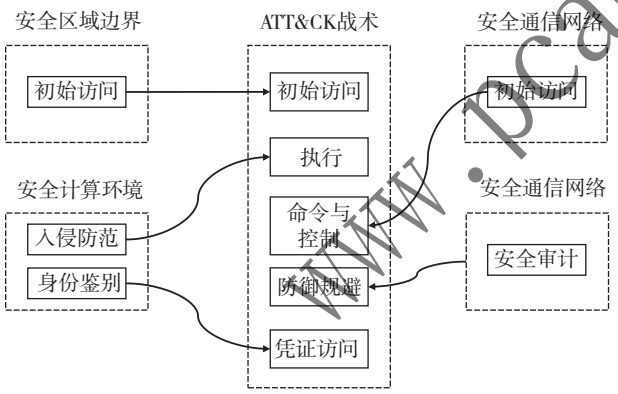

图 2　等保 – ATT&CK 映射模型架构图

2　等保 2.0 下的渗透测试方法设计

2.1　合规要求与技术验证的整合路径

在等保 2.0 框架下开展渗透测试，首先需建立合规要求向技术验证点的转化机制。基于等保 2.0 的三级系统要求，整合路径包括：

（1）控制点分解映射：将等保 2.0 的 211 项安全要求项分解为可测试的技术验证点。例如，针对“安全区域边界 – 入侵防范”要求项，可拆解为网络入侵检测、主机入侵防范、Web 应用防护三个测试维度。每个维度明确测试方法（工具扫描、手动验证）、测试对象（防火墙、IDS、WAF 等）和通过标准（是否有效阻断测试攻击）。

（2）风险场景建模：基于系统定级结果和业务特性，设计威胁场景库。例如，三级金融系统需重点测试支付交易篡改、客户数据窃取等场景；工控系统则聚焦指令注入、控制参数篡改等场景。场景设计需结合历史安全事件分析，如 WannaCry 勒索病毒攻击链、APT 组织攻击手法等。

（3）验证工具链集成：构建覆盖等保 2.0 全控制类的工具矩阵，具体如表 2 所示。

表 2　验证工具链集成详情

网络层	应用层	主机层	密码破解
Nmap	Burp Suite	Nessus	Hashcat
开放端口扫描	Web 渗透	漏洞扫描	GPU 加速破解
Masscan	SQLmap	Metasploit	JohntheRipper
全网资产识别	SQL 注入测试	漏洞利用验证	分布式破解

针对云环境扩展要求，需集成云原生测试工具如 Kube-hunter（K8s 安全测试）和 ScoutSuite（多云配置审计），以验证虚拟化隔离策略的有效性。

等保 2.0 合规要求与技术验证的整合路径如图 3 所示。

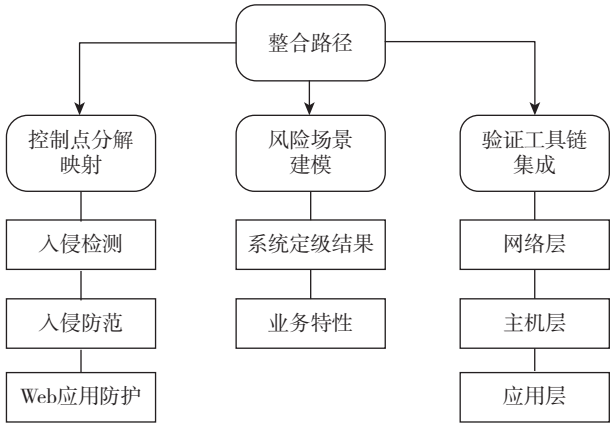

图 3　等保 – ATT&CK 模型的整合路径图

2.2　基于等保要求的渗透测试流程再造

传统渗透测试流程难以满足等保 2.0 的合规验证需求，需进行针对性流程再造，具体如下：

（1）测评准备阶段：在标准 PTES 流程基础上增加合规性预评估环节。

①资产关联映射：识别等保对象涉及的网络设备、安全设备、服务器、数据库等资产，建立与等保要求项的关联关系。

②授权边界确认：书面明确测试范围、测试时间窗

（需避开业务高峰）、禁止测试项（如禁止对生产数据库执行 DROP 操作）。

③风险规避策略：制定系统恢复预案，如虚拟机快照回滚、数据库备份恢复等。

（2）现场测评阶段：采用三层验证法实施测试。

①自动化扫描层：使用 Nessus、OpenVAS 等工具执行基线扫描，覆盖等保 2.0 中 80% 的技术项（如补丁缺失、弱口令、配置缺陷等）。

②手动验证层：对高风险项进行人工验证，如利用 SQL 注入绕过 WAF、通过 Pass-the-Hash 攻击突破网络隔离等。

③攻击链测试层：模拟 APT 攻击链，从外网渗透到内网横向移动，验证等保要求的“纵深防御”有效性。

（3）分析与报告阶段：建立等保符合性矩阵。

①将测试结果映射到等保 2.0 的具体要求项，标注“符合”“部分符合”或“不符合”。

②采用缺陷扣分法计算风险值：高危漏洞（等保关键项）权重 3 倍、中危漏洞（重要项）权重 2 倍、低危漏洞（一般项）权重 1 倍。

③提出合规导向修复建议：优先修复导致等保扣分的关键项，如未配置双因素认证、审计日志留存不足 6 个月等。

2.3 关键控制点的渗透测试实施要点

针对等保 2.0 的三级系统核心控制点，实施渗透测试需重点关注以下技术场景：

（1）安全区域边界验证

①边界防护测试：尝试通过非授权协议（如 ICMP、Telnet）穿越防火墙，检测 ACL（Access Control Lists）策略是否遵循“默认拒绝”原则。

②入侵防范验证：发送包含已知攻击特征（如 SQL 注入语句、缓冲区溢出载荷）的测试流量，验证 IDS/IPS（Intrusion Detection System/Intrusion Prevention System）是否有效告警并阻断。

③恶意代码防护：上传 EICAR 测试文件（无害的防病毒测试样本），检测边界沙箱是否有效识别并隔离。

（2）安全计算环境验证

①身份鉴别测试：使用 Hydra 工具进行口令爆破测试，验证口令复杂度策略和账户锁定机制；尝试绕过双因素认证（如 SMS 验证码重放攻击）。

②安全审计验证：测试审计日志防篡改能力，如攻击者是否可通过删除 Windows 安全事件日志（EventLog）掩盖攻击痕迹。

③数据保密性测试：使用 Wireshark 抓取数据库通信流量，验证是否采用 TLS（Transport Layer Security）加密；检查备份数据是否明文存储。

针对云环境扩展要求，可额外进行容器逃逸测试，模拟 CAP_SYS_ADMIN 权限滥用场景，验证宿主机隔离机制是否满足等保要求。

（3）安全管理中心验证

①集中管控测试：模拟攻击者控制安全管理服务器，测试是否可通过单点突破获取全网设备控制权。

②安全审计关联：在多个设备生成关联攻击事件（如分布式端口扫描），验证 SIEM 系统能否关联分析并告警。

3 ATT&CK 攻击矩阵的融合应用

3.1 攻击矩阵与等保框架的整合路径

ATT&CK 矩阵为等保 2.0 提供了攻击视角的补充，整合路径包括：

（1）技术映射矩阵：建立 ATT&CK 技术 ID 与等保 2.0 要求项的交叉引用表。例如：

①T1190（利用公开应用漏洞）映射至等保“安全计算环境 - 漏洞修复”要求项；

②T1210（利用远程服务）映射至等保“安全区域边界 - 访问控制”要求项；

③T1059（命令执行）映射至等保“安全计算环境 - 入侵防范”要求项。

该映射使渗透测试既能满足合规要求，又能验证对抗真实攻击的能力。

（2）覆盖度评估模型：通过 ATT&CK 技术覆盖分析，识别等保 2.0 的防御盲区：

①统计企业已部署的安全控制措施（如 EDR、防火墙、WAF）覆盖的 ATT&CK 技术 ID；

②计算防御覆盖率（覆盖率 = 已覆盖技术数/总技术数）；

③针对未覆盖技术设计渗透测试场景（如未覆盖 T1574 - 路径拦截劫持，则测试 DLL 劫持漏洞）。

（3）攻击链闭环设计：基于 ATT&CK 战术序列构建攻击剧本（Playbook），如图 4 所示。该剧本可验证等保 2.0 在多个控制点的协同防御能力。

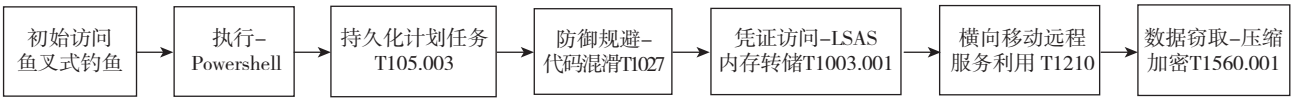

图 4 基于 ATT&CK 战术序列构建攻击剧本图

3.2 基于 ATT&CK 的渗透测试场景设计

将 ATT&CK 技术转化为可执行的渗透测试场景，需遵循可复现、可度量、风险可控三原则[6]。

（1）初始访问阶段测试

①技术模拟：T1078（有效账户利用），测试等保“身份鉴别”要求。

②测试设计：使用 Kerbrute 工具进行域账户爆破，验证账户锁定策略；尝试利用默认凭证（admin/admin）登录管理系统。

③验证指标：成功登录次数、平均检测时间（MTTD）。

（2）执行与持久化阶段测试

①技术模拟：T1053（计划任务）、T1547（启动项注册），测试等保“安全审计”要求。

②测试设计：通过 Metasploit 生成持久化后门，验证主机 EDR（Endpoint Detection and Response）是否检测恶意注册表修改；测试日志是否记录任务创建事件。

③验证指标：后门存活时间、日志记录完整性。

（3）横向移动与数据窃取测试

①技术模拟：T1210（远程服务利用）、T1041（数据压缩窃取），测试等保“安全区域边界”要求。

②测试设计：利用 Pass-the-Hash 攻击突破网络隔离，从数据库服务器窃取模拟数据；检测 DLP（Data Leakage Prevention）系统是否告警。

③验证指标：横向移动跳数、数据窃取检测率。

后续可结合 AI 辅助技术（如深度强化学习），优化渗透路径选择并识别高风险攻击面。例如使用 GAN 生成对抗样本绕过 AI 安全检测。

3.3 攻击模拟与防御能力量化评估

通过 ATT&CK 渗透测试实现防御能力的可视化度量。

（1）攻击链突破度：记录渗透测试在每个战术阶段的突破成功率，若突破率递减表明纵深防御生效，反之则暴露防御断层。

（2）安全控制有效性：统计各防御层对攻击的检测率与阻断率，具体如表 3 所示。

表 3 基于 ATT&CK 渗透测试的防御能力评估矩阵

防御层	ATT&CK 技术 ID	测试次数	检测率/%	阻断率/%	改进措施
网络边界	T1190	20	85	75	优化 WAF 规则
主机防护	T1059	15	65	50	升级 EDR 策略
身份认证	T1078	25	92	90	维持现状
审计分析	T1070	10	40	30	部署 SIEM 关联规则

（3）风险量化模型：结合等保 2.0 缺陷扣分法和 ATT&CK 技术风险值，计算综合风险指数：

风险指数 =（等保缺陷扣分 × 0.6）+（未覆盖 ATT&CK 技术数 × 风险值 × 0.4）

该模型兼顾合规要求与实战能力，为安全投入提供决策依据。

同时，防御效能评估模型需引入 ATT&CK 技术覆盖率动态权重，并与等保缺陷扣分法融合形成双维度风险指数。

4 融合实践的案例分析

某水厂工控系统在等保测评中暴露关键缺陷，工控扩展要求：禁止通用网络服务、物理端口管控；关联 ATT&CK 技术：T0801（工控协议滥用）、T0889（固件篡改）。

结合 ATT&CK 攻击矩阵以及工控系统特点，确定最优渗透测试路径[7-9]，具体渗透测试过程如下：

（1）信息收集

攻击路径：Shodan 引擎扫描暴露 Modbus 端口，定位 PLC 公网 IP（202. xx. xx. xx）；

工具命令强化：nmap – p 502 – – script modbus – discover – – script – args = ′modbus – discover. aggressive = true′ 202. xx. xx. xx。

（2）初始访问

漏洞利用：通过未授权 Modbus 指令读取水位设定值寄存器；

攻击载荷升级：modbus read – – address 40001 – 40005 – – count 5 – – unit – id 1（扩展寄存器扫描范围）。

（3）执行与持久化

固件攻击链：①分析 PLC 固件更新协议；②利用签名验证缺失；③上传植入后门的恶意固件（SHA-256 样本特征：a1b2c3. . .）。

物理攻击补充：通过未拆除的 USB 接口注入伪装为 "config_ backup. xml" 的持久化恶意代码。

实现攻击步骤可视化，如图 5 所示。

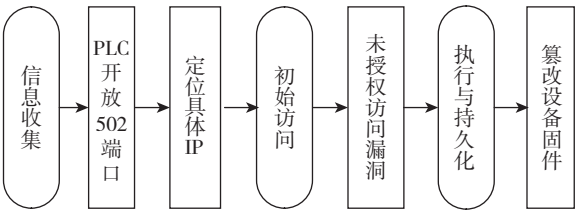

图 5 工控系统攻击步骤图

针对测试结果暴露出的关键缺陷，应用基于等保 2.0 验证测试与 ATT&CK 攻击矩阵的响应流程与融合防护方案，具体如表 4 所示。

表 4　基于等保 2.0 验证测试与 ATT&CK 攻击矩阵的响应流程与融合防护方案

阶段	防护层级	措施项目	具体实施方案
检测阶段	网络层	部署工控防火墙	深度解析 Modbus/S7comm 多协议； 学习水位设定值正常波动范围并设定基线； 实时告警非法 IP 访问 + 自动休眠关联端口
	主机层	物理端口管控强化	硬件级 USB 接口禁用（BIOS 设置）； 主机卫士新增“外设行为监控”模块； 配置文件修改需数字签名验证
	审计层	部署工业安全审计平台	工业安全审计平台部署关联规则：水位设定值修改 & 固件更新事件 → 高危告警； 响应时间优化至 <3 s
响应阶段	动态防御	动态防御联动	攻击告警 → 防火墙阻断 IP → 隔离 PLC 设备 → 自动固件回滚 → 发送告警至 SOC 平台
	固件安全	固件安全增强	建立固件版本库（MD5/SHA－256 双校验），回滚时强制验证版本漏洞状态
溯源阶段	攻击者溯源	威胁来源分析 样本分析	IP 归属地分析 + 威胁情报平台联动（自动比对 Shodan 历史扫描记录） 恶意固件沙箱检测，生成 ATT&CK 技术映射报告（覆盖 T0889 完整攻击链）

基于目标水厂工控系统改进前后的渗透测试结果实证，为量化评估融合渗透测试方法的安全改进效能，现基于 ATT&CK 技术覆盖率、等保合规得分、威胁响应时效三大核心维度，构建如表 5 所示的对比指标体系。

表 5　工控系统渗透测试前后安全能力对比

评估维度	测试前	测试后	提升幅度	关键改进措施
ATT&CK 技术覆盖率	52%	86%	+34%	新增 T0801/T0889 专用检测规则库
等保测评得分	72.5	89.3	+16.8	物理端口拆除率 100% 协议授权全覆盖
攻击检测时间	120 分钟	8 分钟	－93.3%	AI 流量分析引擎部署
漏洞修复周期	60 天	14 天	－76.7%	自动化补丁分发系统

同时，对比测试前后的结果，使用融合防护方案的改进成效如表 6 所示。

表 6　融合防护方案成效量化

安全措施	攻击阻断效果	量化指标	实施验证方式
工控防火墙	拦截 99.6% 非法 Modbus 操作	非法连接数 下降 98%	每月红队攻击 演练数据
主机 USB 管控	阻止 100% 未授权接入	恶意文件 植入归零	硬件审计日志分析
固件签名校验	拦截回滚率 100%	校验成功率 100%	渗透测试 12 次 篡改尝试
安全审计平台	告警响应 <3 s	事件调查效率 提升 90%	实战攻防演习记录

5　挑战与对策

5.1　技术实施挑战

在等保 2.0 与 ATT&CK 融合实践中，面临的主要技术挑战包括：

（1）攻击模拟与业务稳定的平衡：渗透测试可能影响生产系统稳定性，如漏洞扫描引发设备宕机、暴力破解触发账户锁定等。对应对策包括：

①采用镜像流量分析：通过分光镜像复制业务流量，在隔离环境测试；

②实施时间窗口管控：在业务低峰期测试，设置自动回滚机制；

③使用非侵入式验证：如通过元数据判断漏洞存在性（版本比对、配置检查）。

（2）云环境下的测试盲区：等保 2.0 扩展的云计算要求（如虚拟化隔离、容器安全）难以用传统方法验证。解决方案包括：

①利用云服务商 API（Application Programming Interface）获取安全配置（如 AWS Security Hub）；

②部署云原生渗透测试工具：ScoutSuite（多云配置审计）、Kube-hunter（K8s 安全测试）；

②实施混沌工程：模拟节点故障、网络分区等场景验证弹性防护。

5.2　管理协同挑战

组织内部协同障碍同样制约融合实践效果，具体有：

（1）合规与安全的资源冲突：企业安全团队常面临“合规整改优先”与“攻击防御优先”的决策困境[10]，需建立风险驱动的资源分配模型：

资源分配权重 =（等保缺陷风险值 × 0.4）+（ATT&CK 技术风险值 × 0.6）

动态调整投入比例，如高危漏洞修复优先于一般合规项整改。

（2）红蓝队协同机制缺失：渗透测试结果未能有效驱动防御体系优化，应构建紫队模式：

①红队：执行 ATT&CK 渗透测试，输出攻击链突破点报告；

②蓝队：分析检测日志，定位防御失效原因；

③紫队协调：组织攻防复盘会，制定 ATT&CK 技术覆盖提升计划。

6 结论

本文通过融合等保 2.0 技术验证要求与 ATT&CK 攻击矩阵，构建了合规能力一体化的渗透测试框架，取得以下成果：

（1）提出等保 - ATT&CK 映射模型，实现从合规要求到攻击技术场景的转化，解决了传统渗透测试与合规验证脱节的问题。通过建立等保 211 项要求与 ATT&CK 200 多项技术的映射矩阵，为测试设计提供系统化指南。

（2）设计攻击链闭环验证方法，基于 ATT&CK 战术序列构建可度量的渗透测试剧本。在工控场景验证表明：该方法使安全能力可量化（ATT&CK 覆盖率提升 34%）、风险可视化（攻击检测时间缩短 93%）。

（3）形成动态防御优化机制，通过渗透测试结果驱动安全策略迭代。案例显示，采用紫队协同模式后，漏洞修复周期从 60 天缩短至 14 天，防御有效性显著提升。

随着等保制度的深化和攻击技术的演进，后续研究可从以下三方面拓展：

（1）云原生环境适配：研究容器（如 Kubernetes）、无服务器（Serverless）等云环境下的渗透测试方法，解决动态拓扑、短暂生命周期带来的测试挑战。重点突破方向包括：容器逃逸漏洞自动化检测、云服务配置合规扫描等。

（2）AI 辅助测试技术[11]：探索机器学习在渗透测试中的应用：

①攻击侧：基于 GAN 生成对抗性攻击样本，绕过 AI 安全检测；

②防御侧：利用深度强化学习优化渗透路径，识别最优攻击面；

③决策侧：构建风险预测模型，评估漏洞修复优先级。

（3）合规自动化工具链：开发集成等保测评与 ATT&CK 测试的自动化平台，实现：

①等保要求项自动分解为测试用例；

②ATT&CK 剧本一键执行；

③合规风险与攻击风险双维度报告生成。

本研究的融合框架为网络运营者落实等保制度提供了有效工具，并结合安全可信网络生态[12]，推动网络安全建设从“合规通过”向“能力提升”转型。随着国家网络安全等级保护制度的深入实施，该框架有望成为支撑关键信息基础设施安全防护的标准化实践指南。

参考文献

[1] 中国信息安全标准化技术委员会. 信息安全技术 网络安全等级保护基本要求（GB/T 22239 - 2019）[S]. 北京：中国标准出版社，2019.

[2] 全国信息安全标准化技术委员会. 信息安全技术 网络安全等级保护测试评估技术指南（GB/T 36627—2018）[S]. 北京：中国标准出版社，2018.

[3] 孙永清，陆臻，沈亮. 等级保护移动应用软件渗透测试技术研究 [C]//2020 中国网络安全等级保护和关键信息基础设施保护大会论文集，2020：43 - 47，68.

[4] BLAIR R. Aligning security operations with the MITRE ATT&CK framework：level up your security operations center for better security [M]. Packt Publishing Limited，2023.

[5] 郭启全. 论网络安全新质战斗力的构建与提升 [J]. 中国信息安全，2024（11）：67 - 72.

[6] 李元诚，罗昊，王庆乐，等. 一种基于 ATT&CK 的新型电力系统 APT 攻击建模 [J]. 信息网络安全，2023，23（2）：26 - 34.

[7] 张玮炜，邹春明，胡亚兰. 深度学习在工控网络入侵检测中的应用 [J]. 工业信息安全，2023（6）：89 - 95.

[8] 张静，张光洲，金学奇，等. 电力监控系统基于 ATT&CK 框架的威胁路径构建方法研究 [J]. 电力信息与通信技术，2024，22（12）：55 - 61.

[9] 曹旗升，徐裴行，周纯杰. 基于强化学习的工控系统渗透测试最优路径生成方法 [J]. 信息安全研究，2023，9（12）：1159 - 1165.

[10] 陈长松，张仪方，孟彩霞. 面向攻防对抗的网络安全防护体系研究 [C]//2019 中国网络安全等级保护和关键信息基础设施保护大会论文集，2019：166 - 169.

[11] 陈可，鲁辉，方滨兴，等. 自动化渗透测试技术研究综述 [J]. 软件学报，2024，35（5）：2268 - 2288.

[12] 黄坚会，张江江，沈昌祥，等. 基于 TPCM 可信根的双体系可信终端计算架构 [J]. 通信学报，2025，46（4）：1 - 14.

（收稿日期：2025 - 06 - 26）

作者简介：

颜星晨（1995 - ），男，本科，工程师，主要研究方向：漏洞挖掘、等级保护、网络安全。

张鑫（1985 - ），男，本科，工程师，主要研究方向：等级保护、网络安全、信息技术。

周志洪（1979 - ），男，博士，高级测评师，主要研究方向：网络安全检测与风险评估、密码应用安全、车联网安全。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部