

主题：高管视角、课题摘录

交易技术前沿

2025年 第1期 总第61期

——网络安全专刊 (第2期)

ITRDC 证券信息技术研究发展中心(上海)



上海證券交易所
SHANGHAI STOCK EXCHANGE



P02 国泰君安证券威胁情报共享中心体系建设与实践
国泰君安证券 俞枫

P06 AI赋能证券安全建设构建面向未来的智慧安全体系
光大证券 许涛

P10 基金公司信息安全管理建设浅谈
富国基金 李强

内部资料 免费交流
准印证号(K) 0671

交易技术前沿

2025 年 第1期

总第 61 期



总编

邱 勇 蔡建春

副总编

王 泊

本期“安全网络专刊”：

执行总编

道 晟 刘政言

责任编辑

张 涛

运营：

证券信息技术研究发展中心（上海）

网络安全创新实验室

主管、主办：

上海证券交易所



目录

01 高管视角

- P02 国泰君安证券威胁情报共享中心体系建设与实践**
俞枫/国泰君安证券股份有限公司
- P06 Ai赋能证券安全建设构建面向未来的智慧安全体系**
许涛/光大证券股份有限公司
- P10 基金公司信息安全管理建设浅谈**
李强/富国基金管理有限公司

02 安全实践

- P15 基于数据运营的DNS智能安全防护体系在证券行业的应用**
丁安安、夏英杰、杜峥/民生证券股份有限公司
葛锐、张绍峰/互联网域名系统北京市工程研究中心有限公司
- P20 勒索软件防范的探索与实践**
孙一伟、崔毅然、陈其乐、吴鹏、张沁怡/上海证券有限责任公司
- P23 东方证券信创特权账号管理系统的探索与实践**
俞建群、邬晓磊、陈炎津/东方证券股份有限公司
陆凯捷、杨帅/浙江齐治科技股份有限公司
- P30 证券公司核心交易系统安全韧性体系的实践探索**
华仁杰、沈嗣贤、徐俊超、郑征/东吴证券股份有限公司
- P35 业务安全之API越权检测工具的探索实践**
刘正新、樊添、赵子俊、伊鹏/中信建投证券股份有限公司
- P40 “口令+‘三方协同鉴别’”
——一种满足第三/四级等保要求、适用证券业务的, 限定条件的强身份认证方法**
王恩潭、张永启、董延敏、张佳佳、黄强生、马原、张秀敏、李广猛、赵存利/中泰证券股份有限公司

03

新技术应用-大模型

- P48 隐私计算在大模型安全推理中的应用研究**
张迪路、章庆、苗仲辰/上海金融期货信息技术有限公司创新实验室
- P54 金融大模型安全风险与应对**
陈洪炎/上交所技术有限责任公司
- P59 大语言模型在证券业开发安全领域的探索与实践**
谢朝海、齐大伟、谢琪、丁延彪/海云安网络安全技术有限公司

04

思考和观点

- P68 基于全景数据流转论金融行业数字供应链方法论**
侯亮、郑洲豪、翁伟刚、周雪翎/国泰君安证券股份有限公司
- P72 数字安全风险内控与合规教育评价指标体系**
王怀宾/上海市信息安全行业协会
- P75 RSAC 2024聚焦AI安全：证券行业面临大模型安全新挑战**
康乐、盛浩月/奇安信科技集团股份有限公司
- P79 网络攻防新背景下的高质量漏洞运营**
樊兴华/北京微步在线科技有限公司
- P83 证券行业分支机构 IT 降本增效方案**
白昆忠/上海灵畅信息技术有限公司

05 热点解读

- P88 假冒证券基金经营机构网络诈骗活动风险危害及应对流程**
证券期货行业网络安全创新实验室
- P93 量子计算对基础安全带来的挑战和应对措施**
证券期货行业网络安全创新实验室
- P96 证券基金经营机构电子数据取证与分析研究**
证券期货行业网络安全创新实验室

06 2023年度实验室优秀课题摘录

- P102 基于BAS的安全运营自动化闭环技术的研究和实践**
王东、马冰、吴晨炜、秦伟伦/海通证券股份有限公司
- P110 一站式安全可控商用密码服务研究与应用课题**
官俊、徐庆、方优、万强、谢丽君、乔少明、王家阳/国泰君安证券股份有限公司
应志伟、涂海波、陈善/海光信息技术股份有限公司
潘峻翌、黄福飞、朱振中、熊梦彪、何良杰/格尔软件股份有限公司
- P118 证券公司软件供应链安全管理平台研究与实践课题**
王玥、李志龙、吴佳伟、钟蓉、李鹏、曹杰、温志强、韩智鹏/兴业证券股份有限公司
马冰/海通证券股份有限公司
康乐、韩建/奇安信科技集团股份有限公司
- P124 自动化和常态化的网络资产攻击面运营平台的研究与实现**
季常青、宋士明、叶飞、姜玥、汪洋/南京证券股份有限公司
赵武、邓焕/北京华顺信安信息技术有限公司

01 高管视角

P02 国泰君安证券威胁情报共享中心体系建设与实践

俞枫

P06 AI赋能证券安全建设构建面向未来的智慧安全体系

许涛

P10 基金公司信息安全管理建设浅谈

李强

国泰君安证券 威胁情报共享中心体系建设与实践

俞枫 | 国泰君安证券股份有限公司

摘要：在数字化转型的时代背景下，新技术的深度发展与应用正促使金融科技历经巨大变革，金融行业固有安全边界逐渐泛化，导致网络安全风险事件频繁发生。因此，面对数字化转型的新机遇和金融安全的新挑战，金融行业网络安全建设应逐步从传统的被动威胁应对模式转向发展内生网络安全能力，特别是构建基于威胁情报的网络安全主动防御体系势在必行，通过威胁情报共享带动金融行业网络安全防范协同联动，推动行业网络安全工作高质量发展，为织密织牢金融安全网作出积极贡献。

关键字：威胁情报、协同联动、主动防御

一、数字化转型带来的安全风险与挑战

随着全社会逐步进入数字化新时代，数字化的浪潮蓬勃兴起，5G、云计算、大数据、物联网、区块链、人工智能等新数字技术在金融行业领域里得到了越来越广泛和越来越深入地应用。数字化转型带来新技术的深度发展与应用正促使金融科技历经巨大变革，数据资源作为关键生产要素发挥着重要作用，并已逐步成为数字经济时代的核心生产要素。然而，随着海量数据汇聚集中，移动办公、线上服务广泛应用，信息系统复杂度极大提升，企业固有边界逐渐泛化，导致金融行业安全风险事件频繁发生，安全事故损失也急剧扩大。并且全球网络空间局部冲突不断升级，以窃取敏感数据、破坏关键信息基础设施为目标的网络攻击行为大幅上升，表现出有组织、有系统的特征，甚至是国家对抗行为。

由此可见，数字化转型在为金融行业发展注入新动力、带来服务效率提升的同时，也衍生出更多的不确定性和新型风险。在数字化转型的浪潮下，给金融行业带来了新的挑战。

目前，金融行业各机构的安全建设水平和防御能力参差不齐，使用的主流防护产品大多是根据攻击特征匹配攻击行为，并且只有在攻击发生时才会有告警。因此企业的安全防御需要一种可以提前预警的主动式安全防护措施，此时威胁情报就发挥了其价值，利用精准的情报信息提前发现威胁并溯源攻击行为。但当前各机构在威胁情报的建设与应用上都各自为营，呈现竖井式发展，严重限制了整体应对威胁的能力。面对攻击者针对同类目标发起的关联攻击或者更具隐蔽性APT攻击，行业各机构很难借助于孤岛式的情报数据来判断攻击者的攻击手段、攻击路径、攻击目标及攻击范围等上下文关联信息，难以有效的进行攻击者画像，进而导致行业各机构在面对攻击时缺少主动的威胁溯源能

力。

因此，面对新形势下数字化转型的新机遇和金融安全的新挑战，金融行业网络安全建设应逐步从传统的被动威胁应对模式转向发展内生网络安全能力，特别是构建基于威胁情报的网络安全主动防御体系势在必行。金融行业的网络威胁情报应充分发挥网络安全基础数据支撑作用，覆盖多源化情报需求，实现更广范围情报共享，带动金融行业网络安全防范协同联动，并推动行业网络安全工作高质量发展，为织密织牢金融安全网作出积极贡献。

二、威胁情报共享体系建设的必要性和价值

（一）国家有要求，履行网络安全监管职责

国家层面对网络安全工作的重视程度不断提升，强调维护金融安全，是关系我国经济社会发展全局的一件带有战略性、根本性的大事。网络安全法、个人信息保护法、关基保护条例等法律法规规定行业监管等部门应该履行网络安全监管的职责义务。

威胁情报共享体系建设是履行行业网络安全监管职责的重要一环，通过引入威胁情报，才能刻画攻击者的特征、明确攻击手法以及各单位的受攻击情况，从而关联分析出具备行业特色的情报、攻击趋势，共享给相关机构，完成信息通报、监测预警工作，并指导各机构做好安全防范工作。

（二）行业有规划，瞄准行业科技发展十四五规划

2021年证券行业正式发布了《证券期货业科技发展“十四五”规划》（以下简称“《规划》”）。《规划》中提出了“十四五”期间，行业要“与国家网络安全主管机关充分联动，推进行业网络安全的前瞻性预研与部署，提升行业网络安全威

胁感知分析能力”。同时,明确了十四五时期“威胁检测能力建设”任务,“建设行业威胁情报平台,提升行业整体监测预警、溯源分析、联防联控能力。通过人工智能算法和威胁情报机制,提升威胁检测能力,实现全局感知、上下联动、群防群治的效果”。

在《规划》指导下,建立行业威胁情报共享体系,通过威胁情报快速提升机构威胁检测能力,实现行业的安全监测预警和威胁情报共享,达到上下联动、群防群治的效果。

(三) 业内有需求, 情报共享助力联防联控

在网络攻击日趋复杂多样的背景下,证券行业各机构网络安全建设水平和防御能力参差不齐,特别是在威胁情报的建设与应用上各自为营,缺乏有效、充分联动。

证券行业亟需构建威胁情报共享体系,通过行业各家机构自有威胁情报的生产、上报以及实时共享,形成具备区域特性、行业属性的情报信息,对各类风险事件快速感知和预防各类威胁攻击行为,保护业务系统安全性,实现从安全事件的被动响应转变为安全威胁的积极防御。借助于精准的威胁情报信息,通过联合监管机构、公安等部门对非法攻击行为进行打击,真正起到一体化联防联控的作用。

三、构建多源与共享的威胁情报体系助力行业联防联控

构建多源威胁情报共享体系,通过“一套机制、一个中心”打通行业威胁情报共享通道。其中,一套机制:基于威胁情报共享体系进行情报交换共享和管理;一个中心:以情报中心节点为核心,统一运营威胁情报数据,保障情报数据的时效性、准确性和丰富性,提升“一点威胁感知、情报共享联防”能力,为预警通报、事件监测、应急响应、溯源取证、信息共享等安全场景提供动态、持续的风险信息支撑。

(一) 威胁情报的多源建设

为了丰富情报数据、使情报信息发挥最大价值,需要进行多源化的情报信息采集。根据数据采集源的多源性,可将情报分为内部威胁情报和外部威胁情报两大类。

内部威胁情报作为高价值精准情报数据,由机构单位内部产生的情报,或是由监管机构、第三方提供的针对本单位的真实威胁情报。威胁情报采集源主要包括基于设备产生的日志数据,基于已有的安全知识库数据,基于蜜罐蜜网诱捕到的相关威胁攻击数据以及基于本地情报命中的告警日志和本地生产出的情报数据。

外部威胁情报作为溯源分析情报线索,通过引入漏洞库、安全事件库、第三方机构等外部威胁情报,作为线索判断是否在机构内部已经发生过类似攻击或作为预测是否将会发生类似攻击。威胁情报采集源主要包括专业情报厂商多维度威胁情报数据,开源威胁情报数据,相关监管单位推

送的其他行业情报数据以及情报社区产生的广泛情报数据。

(二) 威胁情报的融合分析

要使情报在安全防护中发挥决策性作用,则需要有高价值情报作为依据。因此需要对采集到的海量威胁情报数据做深度融合性分析。

利用ATT&CK、钻石等安全模型,对多源情报数据进行碰撞、去重、去伪、规则匹配,根据影响范围、攻击频率、是否恶意、攻击行为等计算出威胁值,生产出具备高威胁的行业情报,刻画攻击者行为、攻击常用手法、攻击趋势等攻击链,以关联融合、时间序列、流数据等技术从海量的网络信息中提取威胁特征,实现威胁情报的横向和纵向关联分析;以聚类分析、协同推荐、跨界数据融合等技术深度挖掘多维线索之间隐藏的内在联系,进而实现对整体威胁态势进行行为建模与精准描述;并结合大数据分析、深度学习、人工智能等新技术协助构建威胁情报的智能研判与综合预警能力。

(三) 威胁情报的共享建设

通过建立“自下而上”的数据上报、威胁情报生产及“自上而下”的情报共享机制,实现行业与行业、行业机构间、机构内部跨区域的威胁情报数据交换与共享。

共享的情报数据内容:机构单位在发生攻击事件时对攻击者进行溯源取证时需要的相关信息,如攻击设备指纹、攻击者画像、攻击者使用的Domain、IP、URL等。同时,对情报信息的相关字段进行脱敏或去标识化。

情报共享方式:通过定制化开发,支持API调用、KAFKA读取以及离线导入等多种情报共享方式。其中,制定API接口标准,通过威胁情报平台标准化的调用接口实现不同机构和平台间的情报交换与共享;通过统一KAFKA读取标准,进行威胁情报数据交换和共享;通过离线方式将行业情报导入证券机构本地的情报平台节点进行情报的共享和使用。

四、技术创新提升威胁情报共享能力

(一) 基于攻击者画像及标签化构建高质量威胁情报生产和共享能力

基于攻击者画像构建模型,实现多元威胁情报数据的自动采集、融合、关系抽取和质量评估,并进行攻击威胁的深入关联分析,产出高质量情报数据,为攻击溯源提供有价值的线索。

对威胁情报中的被攻击资产IP、URL以及被攻击单位等相关敏感信息进行标签化处理,实现源数据在情报共享前的私密度改写,最大限度降低威胁情报中的信息敏感程度,并对不同情报类型和级别进行标签定义,根据标签控制可

共享的内容、范围和行业机构，从而提升威胁情报在交换与共享过程中的安全性。

（二）规范统一情报数据共享标准，满足共享技术条件

通过统一情报数据在采集、存储、输出、共享等各阶段数据标准，并规范情报交换与共享的安全行为，构建稳定、易维护的情报共享体系，通过行业威胁情报的快速共享提升证券机构威胁溯源能力。

规范统一的共享标准先行试点应用，待成熟后在监管单位的指导下可复制推广到行业间其他单位。

（三）基于威胁情报共享交换机制探索行业安全生态圈建设路径

威胁情报的多源与共享需要建立和遵守共享规则。通过共享规则定义成员单位所能读取的情报级别，实现在不同行业、不同机构间共享威胁情报数据。并在相关监管机构的指导下，通过持续研发情报中心共享和交换功能、输入/输出API接口和情报数据规范，推动与行业机构、第三方单位战略合作，打通情报数据链、丰富情报数据源，实现跨行业、跨机构、跨地域多源情报的采集和共享，探索构建行业安全生态圈，形成网络安全情报数据的快速共享和协同联动机制。

同时，威胁情报的实时共享，可用于快速感知和预防各类威胁攻击，保护业务系统，实现从安全事件的被动响应转变为基于威胁情报的主动防御。

五、威胁情报共享体系建设成果

（一）常态化安全运营赋能主动防御能力

常态化安全运营中赋能主动防护能力建设。威胁情报共享中心系统每日关联分析生产出500-1000条IP情报，累计生产出12万多条高质量威胁情报数据。通过情报查询接口对海量告警日志过滤、筛选和处置优先级排序，提升安全运营平台对恶意IP或域名检测与关联分析能力以及自动化响应处置能力，在每日自动化封禁恶意IP中，有60%以上来源威胁情报。

（二）重保时期助力威胁情报联防联控

重点保障时期助力威胁情报联防联控。在今年国家网络安全演习期间，与中证技术开展联防联控安全防护工作，按照中证技术要求格式，每日共享威胁情报数据17万个，综合贡献值排名前三；演习期间累计面向子公司共享6000多个恶意攻击IP情报，赋能子公司主动防御能力建设。

（三）行业威胁情报共享标准联合研究

行业网络和信息安全三年提升计划中多次提出要加强行业威胁情报共享和联防联控能力建设。目前，我国威胁情

报建设主要参考国际标准STIX和国标《金融网络安全威胁信息共享指南》，但该标准主要适用于通用威胁情报的共享和交换，对证券期货业的业务特性兼顾不够、行业特色情报考虑不足，指导性不强，导致行业各机构对于威胁情报的建设和应用各自为营，机构之间信息交流和合作存在障碍。

国泰君安证券与中证技术联合牵头研究制定一套证券期货业网络安全威胁情报共享标准，基于行业机构需求和情报特点，明确共享范围、方式、内容、机制等，规范共享流程，以促进行业机构间的安全威胁情报共享，持续提升行业网络安全防御能力。

六、总结与展望

在数字化转型背景下，金融行业将面临更加复杂和多样化的网络安全威胁。通过不断优化威胁情报数据收集、归类和关联分析，并以共享机制实现行业内不同机构间的威胁情报信息交换与共享，形成一个动态的、自适应的安全生态体系，并达到安全威胁预警的联防联控效果，将金融行业中面临的网络安全风险问题，以创新的解决方案赋能金融科技发展和数字化转型，推动行业迈向更高水平的安全防护能力，实现全行业的安全共治、共赢。

未来，在威胁情报共享体系建设的过程中，只有更多的行业机构参与进来、破除情报共享壁垒，才能提升整体行业的威胁风险识别能力、预警响应能力以及协同联动能力。但同时，也会引入威胁情报共享的数据安全问题，如目前的相关法规及标准中并未对情报的共享规则、共享协议有明确的规定。因此，为了降低情报共享过程中带来的风险以及更好的发挥情报共享带来的价值，提升威胁情报共享的安全性和有效性，还需持续进行如下工作：

（一）完善情报数据标准

情报数据标准化以及系统接口规范化是情报数据高效共享、合理运用的前提。通过统一情报数据在采集、存储、输出、共享等各阶段的数据标准，规范情报交换与共享的行为，从而保障威胁情报共享平台的安全性、稳定性、易维护性。

（二）确保合法共享情报

与行业各机构以及监管机构共同研讨，逐步优化情报共享策略。通过实施相应的技术措施，从而降低数据安全、隐私合规方面的风险，使其能够在合法合规的前提下，实现情报共享的良性循环。

（三）建立行业攻击态势预警机制

目前，在安全防护体系建设上，各单位缺乏对情报数据的重视程度，未能构筑中高位积极防御能力。为了使行业各

机构能够对特定的网络攻击行为“早知道,早预警”,行业相关监管部门可以管理、监督者的身份牵头组织情报共享体系建设,持续检测所属行业攻击态势,及时对成员单位做出威胁预警。

参考文献

- 1.证券期货业科技发展“十四五”规划。
- 2.证券公司网络和信息安全三年提升计划(2023-2025)。
- 3.GBT 42708-2023金融网络安全威胁信息共享指南。
- 4.GB/Z 42885-2023 信息安全技术 网络安全信息共享指南。
- 5.Structured Threat Information eXchange(STIX) 2.1。
- 6.ATT&CK框架实践指南。

Ai赋能证券安全建设 构建面向未来的智慧安全体系

许涛 | 光大证券股份有限公司

摘要：在数字化转型与网络安全威胁日益加剧的背景下，生成式AI技术在证券行业网络安全中展现出了强大的潜力和独特价值。安全大语言模型(LLM, Large Language Model)凭借卓越的语义理解与威胁情境推理能力，能够高效解析多源异构数据并实现动态威胁检测，显著提升网络安全智能化水平。LLM支持智能日志解析、自动化事件响应和安全知识图谱构建，为证券公司实现高效的安全运营和协同防御提供基础。本文探讨了生成式AI技术赋能证券行业安全建设的路径及其战略意义，推动行业向智慧化安全体系迈进。

关键字：LLM、MOE、威胁情境推理、前瞻性威胁识别、Zero-Shot Learning、智能安全运营中心、多源异构数据分析、安全知识图谱

一、引言

在数字化进程不断加快的背景下，证券行业正面临日益严峻的网络安全形势。复杂的金融产品、海量用户数据和实时交易系统为行业带来了前所未有的安全压力。与此同时生成式AI技术近两年迅猛发展，在网安领域攻防两端都带来巨大的变革。

生成式AI技术使得攻击者可以更容易使用自动化与智能化的攻击。这一变化直接带来了网络攻击“质”与“量”的持续剧增，针对“量”的变化，现有安全体系尚可应对；而针对“质”的变化，现有安全体系正面临巨大挑战。

利用大语言模型(LLM)所具备的卓越的自然语言理解和语义分析能力，赋能证券行业安全建设，以“魔法”对抗“魔法”无疑是必然的发展方向。

Shot Learning)支持，如网络日志、交易数据和访问控制记录，识别关联模式并生成全面的威胁图谱。LLM的动态分析能力打破“数据孤岛”，整合全局数据以提升整体安全态势感知。这种智能体(Agent)驱动的分析不仅支持海量数据的快速迭代和精准识别，为实时异常检测提供了更高效的技术支持，使证券行业向事前预警的方向转型。

(三) 自适应优化与前瞻性威胁识别

LLM具备高度自适应学习能力，在智能体和自我优化(Self-Optimization)的机制下，能够根据历史威胁情境持续更新模型，有效应对新型威胁。LLM在前瞻性威胁检测方面依赖于COT策略和强化学习，自主发现潜在的攻击模式，降低人工维护需求。自我优化与前瞻性能力，使得LLM在安全分析中具备独特优势，为证券行业的安全建设提供深度支持，推动行业向“智慧安全”的未来愿景迈进。

二、LLM网络安全独特价值与技术优势

(一) 语义理解与威胁情境推理

大语言模型具备MOE(混合专家模型, Mixture of Experts)支持下的高效语义解析和情境推理能力，能够深度解析网络安全相关数据，通过COT(思维链, Chain of Thought)识别威胁情境并理解事件的复杂因果关系。大语言模型通过语义关联理解潜在威胁上下文，从而更精确地识别和应对高级持续性威胁(APT)，显著提升了风险识别的准确性，使安全系统具备主动分析威胁的能力，将安全从被动防御推进至预测预防的新阶段。

(二) 数据驱动多源学习与快速识别

LLM通过对多源异构数据的整合和零样本学习(Zero-

三、AI赋能证券行业网络安全应用场景

(一) 智能化日志解析与异常检测

在证券行业中，海量日志数据来自多种来源，包括交易系统、客户行为、访问控制等。传统的日志分析通常需要大量的人力资源投入且效率低下，容易漏报或误报安全事件。大语言模型通过自动化数据解析快速识别出异常模式。通过分析上下文信息，模型自动判定这些事件的优先级并生成告警，使得安全团队能够迅速集中资源处理最紧急的威胁。自动优先级判定机制帮助证券公司更高效地分配安全资源，确保应对高风险事件的快速响应。

(二) 自动化安全事件响应与分析

通过大语言模型的推理和自动分析功能,可以及时识别从最初访问到数据提取的完整攻击路径,帮助安全团队快速定位威胁来源并阻断攻击扩散;并自动生成详细的安全分析报告,分析事件的源头、影响范围和潜在风险,并提供解决建议。大语言模型还支持持续的反馈机制,通过学习历史事件数据,优化其分析与响应的准确性。

(三) 安全知识图谱与威胁情报整合

通过整合多种威胁情报,大语言模型可以帮助证券公司构建专属安全知识图谱,将不同类型的攻击方法、事件特征和情报信息进行系统化管理。这一知识网络能够让安全团队更轻松地获取有关特定威胁的上下文信息,理解威胁的行为模式,并迅速找到应对措施。知识图谱不仅有助于经验积累和知识传承,更可以为整个行业的威胁响应提供共享基础,提升证券行业整体的网络安全水平和协同防御能力。

(四) 数据安全与合规性

1. 敏感数据识别管理

敏感数据识别和分级管理:生成式AI能够自动识别和分类敏感数据,提供数据分级的支持,从而确保证券公司对不同类型的数据进行差异化保护,AI可以使用自然语言处理技术来分析文本、图像等数据,识别出其中的敏感信息,例如客户身份、财务数据和交易信息等。

2. 数据流转监控和动态保护

生成式AI可以在数据流转中实现实时监控,确保数据的使用和传输符合合规要求。例如,当用户尝试访问或转移敏感数据时,AI可以分析访问者的行为、角色权限和访问设备,并判断该操作是否符合预期。一旦检测到异常行为,AI会自动采取措施。

四、生成式AI证券行业落地实践挑战

(一) 数据隐私与合规保障

在处理敏感数据的过程中,生成式AI面临隐私保护的高要求,尤其在证券行业。公司需实施严格的数据治理,以符合《个人信息保护法》和《数据安全法》等合规标准,在模型训练和数据使用的各环节确保隐私防护,降低潜在数据泄露的风险;高标准的治理机制是AI模型应用的关键保障。

(二) 风险防控与模型安全强化

生成式AI模型可能成为攻击目标,需防范数据中毒、模型窃取等威胁。证券公司需建立完善的访问控制和模型保护机制,确保模型仅限授权使用。通过部署异常检测和恶意输入防护工具,增强模型健壮性,确保模型在实际应用中免受恶意攻击。

(三) AI Infra工程技术优化

生成式AI模型的训练和维护需高效计算资源,带来较大成本压力。通过集中和边缘算力结合、模型压缩(如量化和剪枝)等方式优化资源,可在保障模型性能的同时,显著降低算力需求。此外,自动化更新机制和迁移学习技术进一步缩减了训练成本,使模型始终具备高效、安全的性能表现。

(四) 安全专业人员与AI技术的深度融合

1. 复合型安全人才的需求

随着AI技术在证券安全中的应用,单纯的网络安全或AI技术专家已不足以满足实际需求。证券公司亟需具备AI技术和网络安全双重能力的复合型人才,能够理解AI模型的工作原理并快速处理安全事件。公司可以通过内部培养或外部引进的方式,建立一支跨学科的专业团队。

2. 安全团队与AI系统的协同机制

随着AI系统逐步应用于安全工作中,建立有效的协同机制至关重要。安全团队需要对AI生成的警报和分析报告具有充分的理解和信任。团队可采用人机协作机制,利用AI处理大部分基础任务,将复杂问题交由人工决策,形成高效的协同工作流程。这种融合不仅提高了整体的响应速度,还帮助团队不断优化AI系统的实用性和适应性。

五、AI赋能证券行业网络安全未来展望

人、技术、流程是网络安全恒久不变的核心;接下来将从技术路线演进、安全运营未来发展、技术到生态的未来转型三大领域探讨AI赋能证券行业网络安全未来发展可能性。

(一) 从防御到预测:证券安全治理的新战略思维

从防御到预测的转型是证券行业网络安全发展的战略制高点。这种变革不止于技术赋能,而是对行业未来治理逻辑的全面重塑。预测性安全使企业在面对复杂网络威胁时,始终拥有主动权。这一战略思维不仅助力证券在个体竞争中保持领先,更将为证券行业构建集体性的安全生态奠定基础。在这一蓝图下,AI不仅是工具,更是驱动行业长远发展的智慧引擎。

1. 重构证券安全范式:从静态防御到动态预测

传统的安全逻辑以已知威胁为中心,更多地依赖于规则驱动的反应机制,常常滞后于攻击的发生。随着生成式AI的引入,证券行业正进入从静态防御向动态预测的深刻变革阶段。这不仅是技术能力的跃升,更是治理思维的转型——以未来为导向,以预测为核心。生成式AI通过全域数据洞察和行为模式推演,使威胁管理从被动响应进化为前

瞻性防控，奠定了新一代安全治理的逻辑框架。

2. 情境智能：证券安全洞察的战略纵深

威胁治理的核心已从单点事件处理扩展到全局认知优化。生成式AI的情境智能为证券行业提供了多维度的威胁全景分析：它不仅处理分散的数据，更以系统化视角将交易行为、用户特征和系统访问整合成动态威胁图谱。这种全局性认知能力，不是对单一风险的临时应对，而是为企业建立了立体化的风险认知体系，将安全策略从工具层提升到战略层。

（二）证券未来安全智能化决策战略

从局部优化到系统化治理，从人机协作到全面智能化，AI赋能的未来将不仅提升证券行业安全能力，更重塑证券行业对网络安全的定义与实践逻辑。

1. 智能化告警的全局优化

在未来的证券网络安全体系中，告警管理将超越单点工具应用，成为证券行业整体安全架构的战略支柱。AI驱动的智能告警管理不再局限于数据的筛选与分类，而是通过全局视角整合安全事件，以高效的情报转化机制支持企业的风险掌控。告警不再是静态的“提示”，而是动态安全策略生成的核心环节，驱动证券行业从响应驱动转向预测驱动，塑造安全管理的新范式。

2. 人机协同决策的进化路径

未来的智能决策不应被视为AI对人类经验的替代，而是人机协同的进化场域。人辅助AI决策代表了安全治理从“工具”向“伙伴”的转变。在这一模式下，AI将以强大的计算与分析能力为基础，对安全事件进行初步判断与应对；而人类专家的介入则提供了场景化的策略指导与专业经验的补充。这种协同不仅优化了决策的精准性，更创造了一种知识反馈机制，使证券的安全治理体系具备自我学习与成长的能力。

3. 全智能化的闭环安全生态

随着AI技术的持续成熟，证券行业将迈向一个以全智能化为核心的安全生态。AI将不再仅作为风险检测的工具，而是全面驱动企业安全运营的智慧中枢。从威胁检测、动态策略调整到事件分析与报告生成，整个流程将实现完全闭环管理。通过与多源数据和动态情报的融合，AI将打造出具备自适应能力的安全体系，能够快速响应外部环境的变化，保障企业在复杂威胁下的稳健运行。

（三）跨界技术融合：证券行业安全战略的前瞻性变革

跨界技术融合并非孤立的技术创新，而是证券行业整体安全体系的全面升级。通过技术协同构建的安全生态，不

仅增强了企业应对复杂威胁的能力，更定义了未来行业竞争的标准与规则。这一战略愿景代表了从工具防护向智慧化自治安全的历史性跨越，使得证券行业能够在全球数字化浪潮中保持卓越竞争力与长期稳定性。

1. 重构数据信任体系：区块链的战略价值

区块链技术的核心在于其透明性与不可篡改的特性。对于证券行业而言，区块链不仅是数据安全的一种工具，更是重构行业信任体系的基石。在未来的网络安全战略中，区块链将超越技术属性，成为保障数据透明性与可追溯性的框架支柱。通过实时记录和溯源能力，它将推动安全事件处理的规范化和透明化，为证券行业塑造新的治理标准。

2. 量子计算：安全性能的革命性跃迁

量子计算的出现为证券行业开辟了安全技术的新维度。其强大的并行计算能力不仅刷新了AI模型的训练速度，更以量子加密建立了数据保护的终极壁垒。在一个竞争激烈且风险加剧的全球市场中，量子计算的引入意味着证券自身将掌握不可替代的安全优势。这项技术的战略意义超越当下应用，直接关乎行业在未来科技格局中的地位与稳定性。

3. 多维技术协同：构建智能化安全蓝图

生成式AI、区块链和量子计算的协同融合，不仅是技术整合，更是安全治理模式的质变。多层次的智能架构将AI的动态识别能力、区块链的信任机制、量子计算的安全算力融为一体，为证券行业打造出全局性、前瞻性的安全体系。这种体系不再是简单的工具组合，而是一种能够自适应、预测性强的安全生态，全面提升企业的抗风险能力和战略韧性。

六、光大证券智慧化安全防护体系思考

（一）智能化安全运营中心（SOC）

光大证券计划建设基于生成式AI的智能安全运营中心，实现从告警筛选到自动化响应的全闭环管理。SOC将依托AI的自适应学习能力，持续优化事件处理流程，确保高效、精准。

（二）MOE安全专家模型构建

光大证券将构建基于生成式AI的开放性多专家模型架构，使AI能够整合多个垂直领域的模型，以语义理解和多维特征分析替代传统规则，提升安全检测的精准性。通过生成式AI与现有工具的无缝对接，公司内部的安全系统将实现更高的协同性和处理效率。

七、结语

生成式AI将逐步应用于证券行业的日常安全运营，涵盖智能合规检查、威胁检测和事件响应等功能，通过多源数据分析提升检测精度，降低漏报和成本，实现运营自动化并提升效率。从长期战略发展来看，生成式AI将推动前瞻性预测防御、智能安全决策体系的建立，依托跨行业威胁情报共享，实现协同防御。AI不再只是一个工具，更是安全战略的核心支柱，助力证券公司在全球数字化转型中提升网络安全竞争力。

基金公司信息安全管理建设浅谈

李强 | 富国基金管理有限公司

摘要：随着信息技术的迅猛发展，信息安全形势日益严峻，已逐渐成为影响基金公司生存与发展的核心要素之一。鉴于基金公司的业务特性，其必须在确保信息安全的同时，兼顾业务的开放性。然而，基金公司普遍面临着安全投入有限、安全运营能力不足等现实难题。基于以上背景，本文建议信息安全建设思路需要综合评估六个关键措施：建立健全信息安全规章制度、强化全体员工的信息安全意识、实施有效的技术防控措施、构建自动化的安全防护体系、推动高效的安全运营机制及持续优化安全管控策略。

关键字：信息安全管理、安全技术、安全意识、安全运营、自动化、智能化

一、背景与现状

在目前这个全球信息化的时代，互联网的普及和信息技术的飞速发展，伴随的各种新型攻击手段也层出不穷，安全漏洞和信息泄露事件频频发生，信息安全直接关系到公司的生存发展，重要程度不言而喻。这使得我们必须不断建设和完善企业信息安全体系，以保障信息系统的安全稳定运行，保护用户的隐私和财产安全。对于基金公司而言，信息安全的建设也受到监管背景、公司规模、业务模式等多种客观因素制约，呈现出该行业独有的特点与现状，主要情况如下：

业务特点上，基金公司开展业务对互联网具有高依赖性，且实时性、业务连续性要求极高，既要保证信息安全，又要确保高度的业务开放性，同时兼顾安全与业务便利。相较于银行、保险等大集团切断互联网上网、严格控制U盘、邮件等外发途径的集中式管理策略而言，基金公司因为其业务特点，需要具备与外界交互的开放通道，同时为防止敏感数据泄露、钓鱼邮件、木马病毒等安全风险，在避免一刀切式的管理前提下，需要配套更加精细化的柔性安全管控方案，在不影响业务便利的同时，又能做到精准识别并及时拦截风险。

安全投入上，基金公司相较于其他金融公司，如银行、券商而言，整体安全建设投入成本不高，安全专职人员配置较少，然而安全要求、规范标准、监管力度等并没有因此降低。所以如何最大化安全的投入产出比，将有限的成本花在相对有效的安全建设上，是每家基金公司都需要综合考量的问题。同时，由于人员有限，对于日常安全运营中出现的各类告警、事件等，需要更加成熟、高效的自动化运营流程体系，来实现安全的实时监控、及时响应和有效处置。

安全运营上，基金公司普遍存在专职安全人员配备较少，安全系统策略颗粒度不够精细，防护精度低，安全告警自动化处置程度不高，常态化运营机制缺失等痛点。安全运

营的前提是必要的安全设备部署、安全服务支撑和安全人员投入，虽然目前大多数基金公司已经部署了一些基础的安全系统，构建了初步的安全防护体系，并且具备了一些抵御外部风险的能力，但整体管理上仍较为零散，各安全系统几乎都是单兵作战，缺少一定的联动工作机制，缺乏一套标准化、流程化的运营管理体系来支撑其有效运转。目前大多基金公司的现状主要还是停留在各安全系统层面，通过系统内的简单告警，由人工或少量自动化的方式进行分析及处置，一方面消耗的人力、时间成本较高、收益较差，另一方面处置的时效性较差，安全事件处理偏事后，对于没有配套7*24小时安全运营机制的单位而言，空白的安全监控窗口较大，安全风险无法缓解。此外，安全工作呈现出零星的、固定式的被动模式，对待外部威胁，仍是“哪有威胁打哪儿”的打地鼠式补救方法，事中事前预警能力不足，且无法及时感知及捕获未知的安全威胁，以采取有效应对措施。

二、整体建设思路

为了应对上述挑战，基金公司信息安全管理建设宜遵循以下整体建设思路：

一是建立健全信息安全管理规章制度，并不断提升全体员工的信息安全意识，构建扎实坚固的信息安全一道防线，使后续整体的信息安全工作开展有据可依。

其次基金公司需综合考量成本投入、业务便利性与安全管控措施三者间的平衡，合理规划安全投入，确保安全管控既能满足业务需求，又不造成过大成本负担，实现安全与业务的和谐共生。通过不断完善信息安全防护手段，由点到面构建多层次、全方位的安全防护体系，同时以自动化、智能化为目标，减少人工运营成本，提高安全运营的效率 and 准确性。

最后，紧跟安全威胁和技术发展趋势，定期对信息安全

管理体系进行审视评估,调整和完善安全策略,确保信息安全管理体系的先进性和有效性。

三、构建一套科学且有效的规章制度管理体系

以构建一套科学且有效的规章制度管理体系,是基金公司开展信息安全建设的关键基石。管理体系不仅包括技术防护方面的具体要求,还应涵盖管理控制方面的重要内容。只有在完善且严密的规章制度管理体系的支撑下,公司才能有效地应对各种复杂且多变的信息安全威胁,确保业务运营的连续性和整体稳定性得到充分的保障。此外,规章制度的持续更新和优化也极为关键。随着信息技术的快速发展和外部威胁环境的持续变化,公司必须定期审查现有的信息安全政策,识别潜在的漏洞和不足,并据此进行必要的调整和强化。这一系列的审查与调整,构成了信息安全管理体系统持续优化的核心环节,为接下来的关键举措奠定了坚实的基础。具体而言,可参照如下几点来构建基础的安全管理框架:

(一) 信息安全组织架构

自上而下依据监管部门、行业协会等制定的各类办法、规范和标准,构建科学合理的信息安全组织架构。明确各个层级在信息安全管理中的角色和职责,确保信息安全工作有组织、有领导地开展。例如,设立信息安全管理委员会,负责制定公司信息安全战略和重大决策;设置信息安全管理专职岗位,具体执行安全策略的制定、实施和监督等工作;在各个业务部门设立信息安全专员,负责本部门信息安全工作的协调和落实。通过这种分层管理的组织架构,形成全员参与、职责明确的信息安全管理体系。

(二) 建立安全制度规范体系

在建立安全制度规范体系时,要紧密结合自身业务需求,在确保必要安全管控的同时,避免给业务流程带来不必要的阻碍。例如,在制定数据访问制度时,要充分考虑不同业务部门对数据的使用需求,不能因过度限制而影响业务效率。对于交易部门,应确保其在合法合规的前提下能够快速、准确地获取和处理交易数据;对于研究部门,要在保障数据安全的基础上,为其提供充足的数据支持以进行市场分析。同时,制度规范要具有可操作性和适应性,随着业务的发展和形势的变化,及时进行修订和完善。

(三) 完善应急响应机制

建立高效、敏捷的应急响应机制,确保在面临信息安全事件时能够迅速、准确地采取行动。首先,要明确应急响应的流程和责任分工,确保各部门在事件发生时能够迅速协同工作。同时,要制定详细的应急预案,涵盖可能发生的各

类信息安全事件,包括网络攻击、数据泄露、系统瘫痪等,明确每种事件的应急处理步骤和措施。此外,还需定期组织应急演练,检验应急预案的有效性和员工的应急响应能力,及时修正和完善预案。通过建立完善的应急响应机制,基金公司能够在信息安全事件发生时迅速控制事态,降低损失,保障业务的稳定运行。

四、深化员工安全意识培养

(一) 全面深化员工安全意识培养,构筑信息安全软实力防线

员工是企业发展的核心驱动力,亦是信息安全防线的坚实后盾,信息安全与每位员工均息息相关。因此,全面深化员工安全意识的培养,不仅是基金行业信息安全管理核心任务,更是保障企业稳健运营与长远发展的关键环节。

首先,需通过系统且全面的安全培训,来强化员工的安全意识。培训内容应广泛涵盖法律法规、公司政策、安全技术等多个层面,并注重将理论知识与实践操作紧密结合。

以行业通报案例为契机,对案例进行深入剖析,揭示其背后的原因、教训和启示。将案例作为警示教育的素材,组织员工进行学习和讨论,让员工了解安全事件的严重性以及可能带来的后果,增强员工对潜在风险的认知和警惕性。

其次,积极营造浓厚的安全文化氛围,使员工在安全文化的熏陶下自觉提升安全意识。定期举办网络安全宣传活动、安全知识竞赛等,激发员工的主动安全思维,鼓励他们在日常工作中主动发现并解决潜在的安全隐患。在实战化安全演练方面,可以定期组织模拟钓鱼邮件、网络攻击等真实场景的演练活动,使员工在接近实战的环境中体验和学习如何应对信息安全威胁。

(二) 不断提升研发安全意识,以研发提效为驱动实现安全左移

随着公司业务不断发展,业务复杂多态的需求逐步改变了传统的软件工程模式。对于基金公司而言,信息科技人员数相对较少,研发安全概念的普及相对较晚,研发人员的安全意识在一定程度上直接决定了后续应用运行过程中实际遇到的安全风险,是信息科技发展过程中不可忽视的一点。然而相比于普通员工而言,研发人员的安全意识往往更难培养,这不仅需要研发人员对一般的安全理念有所掌握,还需要其对安全攻防的一些基本概念、代码实现等有较深的了解。

同时,在研发过程管理中,对软件工程生命周期设置必要的安全控制点,涵盖从需求、设计、实现、变更到上线运行等环节,并贯穿于项目评审、变更评审等既有生产活动中,将安全深根于整个软件生命周期内,在把控项目安全风险的同时,也能不断提升项目人员的安全意识水平。

五、工具化、碎片化技术防控手段落地

在安全体系构建初期，一般遵循的是自外而内、由边界向核心的纵深安全防护架构建设策略。该策略的核心在于首先确保企业外部边界的安全，随后逐步深入至内部核心区域，进而形成一个多层次且全面的安全防护体系。

在边界防护层面，主要依赖于网络检测类软硬件产品的综合应用，这些产品共同构筑了安全防御架构的基础。依据多种基本网络安全防护技术，例如IPS、WAF、抗DDoS、邮件网关、上网行为管理等协同防御，确保了企业网络边界的稳固。

进一步延伸至内部网络区域防护层面，终端上以防病毒、桌管、EDR、HIDS等客户端安全产品为主，实现全公司终端一体化管理，网络上，主要采用流量分析技术手段，对内网间访问流量中的异常行为或敏感数据泄露情况进行监测。同时，辅以漏洞扫描、代码审计、数据库审计、补丁管理系统等例行化运营系统，及时发现和修复潜在的安全漏洞和隐患，扎实提升内部应用的健壮性和安全性。

在核心区域的安全防护方面，重点在于保护关键资产和敏感数据。按照“知所必需、最小授权”原则，实施严格的访问控制策略，确保只有经过授权的系统或人员才能访问核心系统和数据。通过数据分级分类，针对不同级别的数据，在其产生、存储、传输、使用、销毁等各个生命周期环节中，实施不同程度的安全管控措施。

最后，构建一个多层次且全面的安全防护体系，还需要引入持续的安全评估与改进机制。通过定期的安全评估，识别新的威胁和风险，及时调整和优化安全策略与技术手段。结合威胁情报的分享与协作，提升整体防护能力，构建一个动态适应的安全防御体系，确保企业在面对日益复杂的网络威胁时，始终保持坚实的防护屏障。

六、以自动化、智能化、体系化为目标建设安全技防体系

基金公司在信息安全上的人财物力投入相对有限，无法做到事尽人为，因此亟需建设一套自动化、智能化的安全运营平台，将各类安全手段有效串起来，有序的运转起来，在安全风险监测、挖掘、分析、处置等各个阶段形成闭环管理，通过多系统联动提前发现潜在威胁，快速定位安全事件告警，将安全干预和处置由事后转向事前、事中，由安全监测为辅，人工处置为主的状态，逐步转向实时化、自动化的安全运营体系。

通过实时、统一的告警输出建设，可以有效避免分散式的多系统控制台滚动式的人工监测，减少人力投入的同时，也能更加及时、迅速的输出真实的、具有确切威胁的告警内容，避免漏报、误报。根据数据统计，我司目前已部署约20余个安全系统，每月安全设备告警量约在70万条以上，如果通

过人工逐一分析处置，几乎是不可能完成的事情，且告警威胁程度参差不齐，只有将真正需要关注并及时分析处置的告警筛选出来并及时展现、通知到运维人员，才能够保证以基金公司普遍较少的安全人员投入来覆盖日常安全运营流程。通过对安全日志的聚合分析以及精准筛选，能够大大减少安全人员在日常运维中的人力投入，对安全系统的告警监测效率起到了大幅度提升作用，降低了95%以上的人工分析时间，完美解决了安全人员不足的痛点，弥补了非工作时间无人值守处置的风险缺陷。

通过构建安全运营平台，能够实现对各独立安全系统的整合，达成数据的统一集中管理与深入分析，有效规避“单兵作战”及“打地鼠”式的被动防御模式，从而解决安全系统分散、联动机制缺失的问题。借助多系统的联动分析，可以实现对潜在威胁的预先探测与迅速响应，并且显著减轻了人工操作的负担。这一举措不仅能够显著提升安全管理的效率，还可以确保安全风险能够被提前识别并及时妥善处理，真正达到安全风险闭环管理目标。

七、由点及面的高效安全运营

随着安全系统的广泛部署和安全防护体系的不断完善，如何更有效地利用这些系统来防御日常业务中遇到的安全威胁，及时发现潜在漏洞和弱点，已成为安全运营领域的一大挑战。在安全运营实践中，我们常常遇到许多分散的安全任务，例如补丁管理、漏洞管理、客户端管理等。这些任务虽然看似独立，但实际上相互关联，并且都是安全运营不可或缺的环节。对于基金公司来说，由于资源限制，无法像大型金融机构那样为每个细分的安全任务配备专门的岗位人员进行专项运营。因此，更需要从全局角度统筹安全运营工作，确保每一项细分任务都有标准化的运营流程，并与现有的IT流程系统相结合，以实现运营工作的高效流转。技术上，通过与网络设备或其他平台的联动，实现风险处置的自动化。

总体来说，高效的安全运营依赖于标准化和流程化的管理体系。标准化涉及制定统一的安全政策和操作规范，确保所有安全措施在整个公司范围内得到一致执行。流程化则要求将安全运营任务系统化、步骤化，确保每项任务都有清晰的执行流程和责任分配。只有将这两者结合起来，才能保证安全运营的高效性和一致性，降低因操作失误引起的安全风险。

随着基础安全工作的稳定运行，企业可以逐步将标准化、流程化、自动化的安全运营体系扩展到各个安全领域，包括终端安全、网络安全和数据安全等。“由点及面”的高效安全运营不仅涉及具体的技术和操作层面，还可以提升到企业整体的信息安全战略层面，通过安全运营过程中遇到的实际痛点和经验，可以为公司提供必要数据和案例，来综

合考虑安全治理、合规管理和风险评估等战略性工作。

一个高效的安全运营体系不是构建完以后就一成不变的,还需要在运营过程中通过定期的安全评估和审视,调整和优化安全标准和流程。同时,随着企业业务的发展、监管要求的新增以及外部威胁环境的变化,安全运营体系也必须具备高度的灵活性和适应性,能够做到动态调整以应对新的安全挑战。

八、安全与业务便利相平衡的柔性动态策略调控

数据安全法、个人信息保护法相继出台,数据安全性越来越大。基金公司在日常办公中产生、接触和外发的敏感信息数量繁多,包括客户个人身份信息、投资信息、系统代码、投研持仓类数据等。为防止敏感数据外泄,保证数据使用传输安全合规,大多数单位都采用了终端沙盒、云桌面甚至切断互联网上网等硬性安全控制手段,来限制敏感数据的外泄风险。然而,以上手段存在着易用性差、降低工作效率的弊端,业务用户整体使用满意度较低,在推广过程存在较大抵触,虽然投入较大,但难以发挥真实效果。

因此为寻求一个既能兼顾易用性、又能满足数据安全的合规要求的柔性方案,我司按照“可管控、可审计、可追溯、防泄漏”的安全原则对原有方案进行了改造,将原先以牺牲业务便利性为代价的事前事中控制,在限定使用环境与安全域的前提下,逐步转向事中事后的监控与审计,尽可能不对已有业务流程加塞加码。以下为我司参照该原则制定的具体管控要求:

(一) 可管控原则

- 办公终端必须为安装公司标准安全软件、实施公司标准安全策略的公司电脑;
- 移动端必须使用公司统一的APP进行访问;

(二) 可审计原则

- 电脑须具备审计能力,可对电脑内的用户行为进行审计监控;
- 应用须记录完整的用户访问、操作、下载等日志;

(三) 可追溯原则

- 电脑、手机屏幕访问过程中须覆盖清晰可见的水印;
- 下载敏感数据文件中须添加清晰可见的水印;

(四) 防泄漏原则

- 使用终端须封禁USB移动存储;
- 应用须具备下载数据量超过阈值触发审批机制,以防止大量敏感数据未授权外泄。

九、结语

基金公司信息安全管理体的构建与完善是一项长期而艰巨的任务,它要求我们在制度法规、技术应用、人才培养、安全运营等多个方面做出持续的努力。我们深知信息安全对于企业生存与发展的重要性,因此在实践中不断探索和创新,力求在保障信息安全的同时,兼顾业务的便捷性与高效性。

信息安全工作不是一劳永逸的,而是需要随着技术的发展和业务的变化而不断调整和优化。因此,我们需要继续加强信息安全管理体的建设,不断提升安全技术的应用水平,深化员工安全意识的培养,以构建更加坚固的信息安全防线。

同时,我们也期待与业界同仁共同交流、学习和合作,共同推动基金行业信息安全水平的提升,为投资者创造更加安全、可靠的金融环境。

02 安全实践

P15 基于数据运营的DNS智能安全防护体系在证券行业的应用

丁安安、夏英杰、杜峥
葛锐、张绍峰

P20 勒索软件防范的探索与实践

孙一伟、崔毅然、陈其乐、吴鹏、张沁怡

P23 东方证券信创特权账号管理系统的探索与实践

俞建群、邬晓磊、陈炎津
陆凯捷、杨帅

P30 证券公司核心交易系统安全韧性体系的实践探索

华仁杰、沈嗣贤、徐俊超、郑征

P35 业务安全之API越权检测工具的探索实践

刘正新、樊添、赵子俊、伊鹏

P40 “口令+‘三方协同鉴别’”

——一种满足第三／四级等保要求、适用证券业务的，限定条件的强身份认证方法
王恩潭、张永启、董延敏、张佳佳、黄强生、马原、张秀敏、李广猛、赵存利

基于数据运营的DNS智能安全防护体系在证券行业的应用

丁安安、夏英杰、杜峥 | 民生证券股份有限公司
葛锐、张绍峰 | 互联网域名系统北京市工程研究中心有限公司

摘要：随着互联网的快速发展，网络安全问题日益严重。尤其对于金融服务提供者而言，业务连续性和客户数据安全至关重要。本文以证券行业的安全建设实践为切入点，介绍了一种基于数据运营的DNS智能安全防护体系，以及在提高公司业务和数据安全方面的实践效果。该体系通过实时监测和DNS流量分析，结合威胁情报和数据分析挖掘，实现对恶意域名的识别和拦截，从而保护公司和客户免受网络攻击的影响。

关键字： DNS安全、威胁情报、业务安全、数据安全

一、引言

证券公司作为金融市场的重要组成部分，其业务连续性和客户的数据安全对公司的生存和发展具有重要意义。近年来，针对证券公司的网络攻击事件频发，尤其针对DNS的攻击手段层出不穷，如DNS劫持、DNS隧道、DNS放大攻击等，给公司和客户带来了严重的安全威胁。因此，构建一个高效、智能的DNS安全防护系统显得尤为重要。

二、DNS安全问题错综复杂，形势严峻

DNS安全问题主要有2类：针对DNS服务本身的服务安全问题和针对远控目标的DNS数据安全问题。

（一）DNS服务安全问题

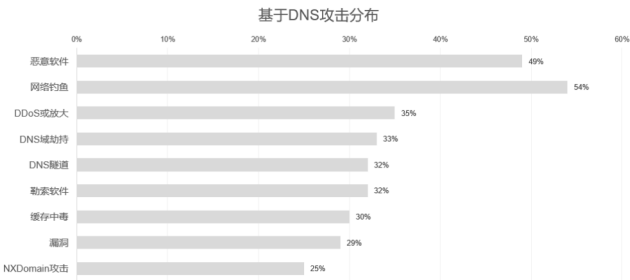
DNS服务安全问题是指DNS服务可用性、服务质量、服务准确性收到影响，无法正常提供DNS解析服务。例如：利用DNS漏洞直接使DNS服务停止导致服务不可用；利用僵尸网络发起泛洪攻击实现DNS网络拥塞，造成解析延伸大的服务质量下降；通过缓存投毒的方式篡改域名解析结果，造成解析结果不准确等。

（二）DNS数据安全问题

DNS数据安全问题是指攻击者利用DNS系统实现恶意攻击者的远程控制和建连，即引导被攻击者访问存在安全问题的域名。例如：挖矿木马、钓鱼网站、垃圾邮件、勒索软件、隧道攻击等有威胁域名和解析数据。

基于IDC《2023全球DNS安全威胁报告》，全球90%的用户曾经遭受过DNS攻击，其中遭受到网络钓鱼和恶意软

件的比例最高，有54%的用户遭受过网络钓鱼攻击，49%的用户遭受过恶意软件攻击。基于DNS攻击分布见下[图一]：



图一：DNS威胁类型

本文对DNS的服务安全和数据安全的攻击手法进行了总结梳理，共梳理出五类十三种攻击方式，具体见下[表一]：

表一 DNS威胁类型

欺骗性攻击	缓存投毒	DNS 缓存投毒会通过诸如未授权地址一类的仿冒数据破坏 DNS 服务器的缓存，为数据盗用和其他威胁开启了方便之门。
	DNS 篡改/劫持	DNS 劫持会覆盖域的注册信息，通常是在域名注册机构进行。修改后的信息指向未经授权 DNS 服务器。
渗透性攻击	恶意域名	网络蠕虫、木马、通过动态域名、CC 域名、DGA 域名、木马域名、心跳域名等方式采用域名关联的方式进行网络信息的窃取。
	钓鱼网站、勒索软件、蠕虫	通过钓鱼域名、开关域名典型案例:Wannacry(2017)，GandCrab(2018)。
	DNS 隧道	DNS 隧道攻击可以为攻击者提供一种永远可用的后方隧道来泄露窃取的资料。
服务资源耗尽	基本 NXDOMAIN 攻击	基本 NXDOMAIN 攻击是一种 DNS 洪水攻击，可以耗尽服务器资源并影响性能。
	随机子域攻击	随机子域攻击可以消耗递归服务器的资源并降低性能。生成由随机字符串作为前缀的查询 xyz123123.zdns.com。
	虚拟域攻击	通过发送异常数据包和查询，致使 DNS 服务器瘫痪。

网络资源耗尽	DNS 反射 /DrDoS 攻击	利用第三方 DNS 服务器(开放的解析器)传播 DOS 或 DDOS 攻击。
	DNS 放大	利用特定查询扩大响应，造成流量拥塞。
	TCP/UDP/ICMP 洪水	通过大量流量拥塞网络或服务，造成第 3 层拒绝服务。
漏洞/异常包	基于 DNS 的漏洞	开源 DNS 软件，如 BIND 目前已知的漏洞已超过 1000 个。
	协议异常	通过发送异常数据包和查询，致使 DNS 服务器瘫痪。

三、DNS智能安全防护体系

在网络安全形势日益严峻的背景下，为了保障证券业务连续性和客户的数据安全，需要构建一套智能化的DNS安全防护体系，立足于DNS协议特点，打造深度DNS协

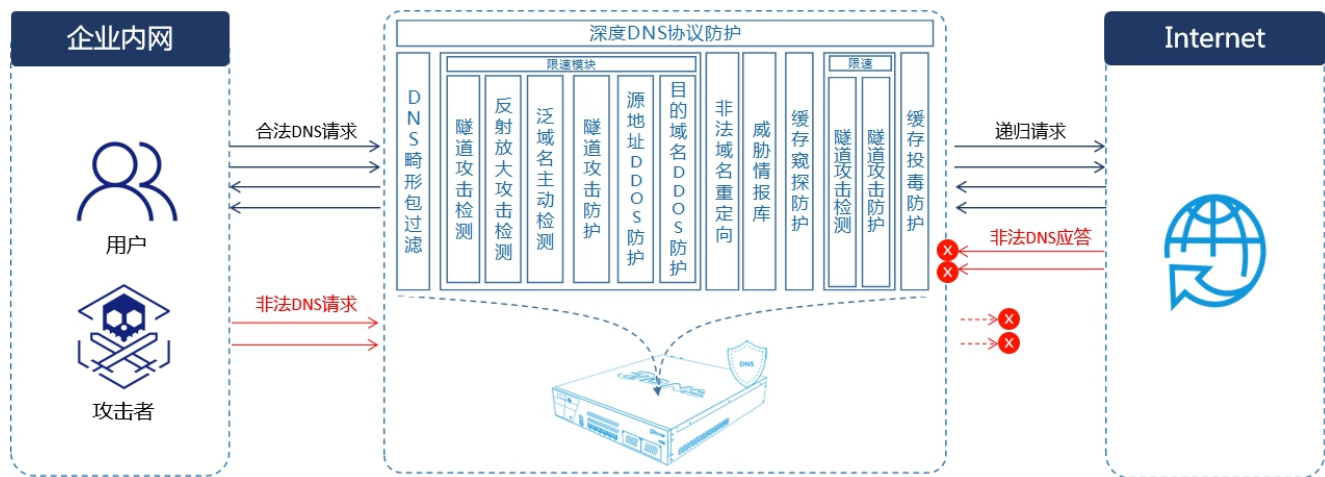
议防护体系，通过多层次的安全防护底座、高性能和强化的安全机制以及基于数据分析的DNS安全运营流程，有效防护各种DNS攻击行为。

（一）基于DNS协议的安全防护底座

由于DNS协议本身的脆弱性，导致攻击者大多基于DNS协议进行攻击。当前，数据窃取、远控连接、重定向流量、DNS拒绝服务是几种主要的DNS攻击方式，基于上述方式衍生出来的攻击手段种类繁多不一而足，但万变不离其宗，所有DNS攻击都需要基于DNS协议来完成，因此，构建DNS安全防护系统需要立足于协议本身来进行安全防护，以加强网络安全纵深防御能力，保证服务稳定可靠，数据不被篡改，隐私不被泄露，风险不被触发。



图二：DNS智能安全防护体系架构



图三 DNS协议级安全防护

本DNS安全防护体系以深度DNS协议防护为安全底座（见图三），具备以下几点能力，能够做到真正的协议级的安全防护：

■**DNS畸形包过滤**：攻击者通过向目标DNS服务器发送有缺陷的请求报文，使得DNS在处理此类数据包时出现崩溃或死机。DNS智能安全防护体系首先会对接收到的请求、应答报文智能检测并判定其合规性，自行阻断和丢弃畸形报文；

■**隧道攻击检测防护**：攻击者利用DNS作为隐蔽通信通道，将敏感数据传输到网络外部，或通过DNS隧道远程控制失陷终端实施其它攻击。DNS智能安全防护体系通过对DNS请求类型、请求数据大小及其规则特点进行深度检测，对异常通信数据及时发现并阻断，保护企业信息安全；

■**反射放大攻击防护**：攻击者利用DNS回复包比请求包大的特点，放大流量，伪造请求包的源IP为受害者IP，将应答包的流量引入受害的服务器，致使服务器性能降级。DNS智能安全防护体系通过对DNS请求类型，响应数据、应答追踪进行判断来识别并阻断非法请求和非法应答流量，既可避免被攻击者利用也可防护反射放大攻击；

■**泛域名主动检测**：攻击者通过对递归服务器发起大量无响应的域名，致使递归服务器持续消耗系统资源，从而影响正常域名解析。DNS智能安全防护体系可通过实时的流量模型分析和行为特征匹配，识别泛域名攻击的恶意子域和恶意IP，并智能启动拦截防护策略，避免影响解析服务质量；

■**源地址DDoS防护**：此类攻击指特定受感染终端发起大量非法请求，持续消耗递归服务器资源，影响正常解析。DNS智能安全防护体系通过对源IP的全局网段、特定网段、特定地址进行精细化控制，结合安全运营的情报和处置经验来扼制源地址DDoS攻击，保证DNS服务质量；

■**目的域名DDoS防护**：攻击者利用受感染的终端或者僵尸程序对受害者的域发起大量随机子域请求，实现对目标域的权威服务器和相关递归服务器的DDoS攻击。DNS智

能安全防护体系通过灵活的目的域安全控制策略来防护此类DDoS攻击；

■**非法域名重定向**：对于攻击特征不明显，但长期存在的非法域名（如每周定期请求），DNS智能安全防护体系嵌入了非法域名重定向功能，通过此功能可对不同域名灵活阻断；

■**缓存窥探防护**：攻击者通过窥探DNS缓存记录，推断DNS用户最近访问过的特定站点，收集用户日常使用信息，为发起攻击做准备。DNS智能安全防护体系加入了校验功能，通过校验查询源、查询方式的合法性，来控制有助于窥探的应答信息，从DNS请求、应答整个过程防护DNS缓存窥探攻击；

■**缓存投毒防护**：DNS缓存投毒指攻击者使用仿冒数据污染DNS缓存，诱使用户访问DNS缓存中的非法地址，实现数据盗用和其他攻击的目的。DNS智能安全防护体系的端口随机、ID随机、域名大小写随机机制，可以增加攻击者仿冒真实数据成本，避免缓存投毒，保证缓存安全，确保DNS解析结果正确。

（二）高性能和强化型安全机制

在安全防护底座的基础上，DNS智能安全防护体系具有高性能防护模式的保障和强化的安全机制，具体为：

■**高性能防护模式**：在遭遇DDoS攻击时，DNS安全防护系统支持启用高性能防护模式，提升系统抗攻击的防护能力，高性能防护模式的处理性能是正常模式性能的数倍。

■**基于TSIG协议的数据更新**：DNS数据更新是否来源于合法渠道，直接关系到DNS解析的正确性。DNS智能安全防护体系通过TSIG协议的加密认证方式验证DNS更新信息的合法性，确保DNS服务器之间数据更新的安全可靠。

■**DNSSEC安全加固机制**：DNSSEC是防护DNS欺骗和缓存污染的一种安全机制，以保障DNS数据来源的合法性以及数据完整性。DNS智能安全防护体系适配了DNSSEC，可基于业务需要灵活配置。

(三) 基于数据分析的DNS安全运营流程

尽管有了协议级别的DNS安全防护、高性能和强化的安全机制,但互联网上仍然存在大量的威胁域名,如果攻击者不利用协议层的脆弱性攻击,仅利用域名的原生属性,让受害者“正常”的回连、访问威胁域名,仍然会给企业造成威胁。因此就需要将威胁情报与DNS智能安全防护体系结合和分析,做到实时阻断失陷终端的非法外联,并按照不同威胁等级进行精细化处置,如预警、预警+阻拦、预警+重定向解析等多种措施进行威胁DNS流量的管控。同时提供DNS威胁预警拦截展示,直观地发现失陷终端、非法域名、威胁事件、威胁情报匹配组织背景等多维度分析统计数据,实现快速溯源,消除隐患。

基于数据分析的DNS智能安全防护系统主要包括以下几个部分:

1. 数据采集处理

实时采集DNS流量数据,包括DNS查询和响应报文,我们需要利用高性能的数据包捕获技术来实现。在这里,我们将采用libpcap库作为数据采集模块的基础,因为它广泛应用于多种操作系统,并具有较低的延迟和高吞吐量特性。同时,为了进一步提高数据采集的性能和灵活性,我们将引入eBPF(扩展Berkeley Packet Filter)技术作为补充。eBPF允许我们在Linux内核中执行用户定义的程序,以处理网络事件等。在高并发的用户场景下,通过编写eBPF程序在内核级别对数据包进行过滤和处理,实现对于DNS流量数据的采集。

为了确保数据采集过程中不对网络性能产生显著影响,我们将采用以下策略:

(1) 结合eBPF与零拷贝技术:虽然libpcap本身已经支持零拷贝技术,通过避免数据包在用户空间和内核空间之间的拷贝,来降低CPU负载和内存消耗,从而提高数据采集效率。但eBPF可以在内核级别进一步减少数据包在用户空间和内核空间之间的拷贝。通过eBPF程序,我们可以在内核中直接处理DNS流量数据,从而进一步提高数据采集效率。

(2) 设置合适的缓冲区大小和超时时间:根据网络流量情况,合理配置缓冲区大小和超时时间,以减少数据包丢失的风险。同时,eBPF程序也可以对内核中的缓冲区进行监控和管理,以确保数据的有效传递和处理。

(3) 并发处理:利用多线程或异步处理技术,并行处理捕获到的数据包,进一步提高数据采集速度。同时,eBPF程序也可以在内核级别并发执行,以提高整个系统的吞吐量和响应速度。

总的来说,eBPF在内核级别的处理能力将进一步提升数据采集的性能,而libpcap的广泛适用性和易用性则为我

们提供了强大的数据捕获和分析能力。两者在不同用户场景下灵活使用,为我们提供一个强大且高效的实时DNS流量数据采集解决方案。

在数据采集阶段,我们还将关注用户隐私保护。为此,我们将对捕获到的DNS流量数据进行加密处理,以防止未经授权的使用。

接下来,我们将对采集到的DNS流量数据进行预处理。预处理操作包括数据清洗、去重、格式化等。为了实现高效的数据清洗和去重,我们将采用以下算法:

(1) 使用哈希表进行数据去重:通过计算数据包的哈希值,将具有相同哈希值的数据包视为重复数据,从而实现快速去重。

(2) 利用正则表达式提取关键信息:使用正则表达式匹配DNS流量数据中的域名、IP地址等信息,以便于后续分析。

在对DNS流量数据进行格式化时,我们将统一采用JSON格式,以便于后续的数据挖掘和分析工作。

2. 威胁情报

收集并整合来自不同来源的威胁情报数据,如恶意域名列表、僵尸网络命令与控制服务器地址等。这些数据将用于辅助分析DNS流量中的恶意行为。

(1) 使用Python编程语言:Python因其易用性和丰富的库支持而被广泛用于网络安全领域。我们将使用Python编写数据收集、清洗、标准化和整合的脚本,以实现自动化处理流程。

(2) 利用API接口:许多威胁情报来源提供API接口,包括各大威胁情报提供商,以使用户获取其发布的最新威胁数据。我们调用这些API接口,实现自动化数据收集。

(3) 数据清洗和标准化:我们将使用pandas库对收集到的威胁情报数据进行清洗和标准化处理。这包括去除重复数据、填充缺失字段、统一数据格式等操作。数据清洗的公式如下:

清洗后的数据集 = 原始数据集 - 重复数据集 - 缺失数据集

(4) 使用Elasticsearch存储数据:Elasticsearch是一个高度可扩展的开源搜索引擎,适用于存储和检索大量数据。我们将使用Elasticsearch作为威胁情报数据的存储后端,以便快速查询和分析。

(5) 数据整合与分析:我们将使用Python的scikit-learn库对整合后的威胁情报数据进行聚类分析,以便发现潜在的关联和模式。聚类分析的公式如下:

聚类结果 = KMeans(n_clusters=k).fit_predict(特征矩阵)

其中,n_clusters表示聚类的数量,k表示预期的聚类数量,特征矩阵表示威胁情报数据的特征向量。

(6) 数据更新和维护：我们将使用Python的schedule库设置定时任务，以定期自动更新威胁情报数据。同时，我们将密切关注威胁情报来源的动态变化，并根据实际情况对数据进行手动修正和调整。

(7) 数据共享和交换：为了促进安全社区的协作防御，我们将积极参与行业共享项目，并通过安全信息交换协议(SIEM)与其他组织共享威胁情报数据。

3.智能分析

结合威胁情报数据，对处理后的DNS流量进行深入分析，识别潜在的恶意域名和攻击行为。该模块采用机器学习和人工智能技术，以提高分析的准确性和效率。

(1) 特征提取：

利用pandas库从处理后的DNS流量中提取关键特征，如域名请求频率、请求时间间隔、域名与IP地址的映射关系等。

使用scikit-learn库中的TF-IDF算法对域名和IP地址进行向量化处理，以捕捉恶意行为的细微迹象。

(2) 模型训练：

收集并标注一定数量的恶意域名和正常域名的DNS流量样本，构建训练数据集。

使用scikit-learn库中的支持向量机(SVM)算法对训练数据集进行训练，得到分类模型。SVM模型的公式如下：

$$f(x) = wx + b$$

其中， w 表示权重向量， x 表示输入特征向量， b 表示偏置项。

使用交叉验证和网格搜索等技术，对模型进行调优，以提高其泛化能力和准确性。

(3) 恶意域名检测：

将处理后的DNS流量输入到训练好的SVM分类模型中，对域名进行恶意性判断。对于被判定为恶意的域名，进一步分析其关联的IP地址和通信行为，以识别潜在的攻击行为。

(4) 攻击行为识别：

利用TensorFlow库构建深度学习模型，如循环神经网络(RNN)或长短期记忆网络(LSTM)，对DNS流量中的时间序列数据进行建模和分析，以识别异常模式和攻击行为。RNN模型的公式如下：

$$h_t = f(Wx_t + Uh_{t-1} + b)$$

其中， h_t 表示当前时刻的隐藏状态， x_t 表示当前时刻的输入， h_{t-1} 表示上一时刻的隐藏状态， W 和 U 表示权重矩阵， b 表示偏置项， f 表示激活函数。

结合威胁情报数据，对识别出的攻击行为进行关联分析和溯源追踪，以揭示攻击者的意图和攻击路径。

(5) 实时分析与预警：

将分析模块部署在网络环境中，实时监控DNS流量，并对潜在的恶意域名和攻击行为进行实时分析。一旦发现可

疑活动或攻击行为，立即触发预警机制，通知相关人员采取应对措施。

4.安全防护运营

通过对各类安全威胁事件聚合、分析，直观反映企业发生安全事件的攻击频率、严重程度等，提高安全运营效率，并通过展示详细威胁背景信息，为安全防护和追溯提供有效的依据。

对识别出的恶意域名和攻击行为，可自定义安全防护策略来进行拦截和阻断，以满足不同场景的安全需求，安全防护策略包括按照不同域名的风险级别设置不拦截+告警、拦截+告警、重定向到自定义页面+告警等。灵活有效的防止公司和客户遭到攻击和损害。

四、结束语

由于互联网发展的历史原因，DNS协议的脆弱性不可避免会带来安全问题，同时，DNS使用场景的多样性使其在遭受攻击时对证券公司所造成的后果越来越严重，因此提升DNS攻击侦测能力、强化DNS安全防护是确保企业数据安全和业务安全的头等大事。本文介绍的DNS安全防护系统结合威胁情报系统形成一套“组合拳”，为企业的安全运营提供更有效的保障。

参考文献

- 1.邢牧怡.DNS安全系统设计与研究[J].电脑编程技巧与维护,2009(6):2.DOI:10.3969/j.issn.1006-4052.2009.06.038.
- 2.钟霖甘.基于SVM方法的DNS服务攻击防范模型[D].复旦大学[2024-0320].DOI:10.7666/d.y1966935.
- 3.段海新.DNSSEC原理,配置与部署(二)[J].中国教育网络,2011(7):2.DOI:10.3969/j.issn.1672-9781.2011.07.027.
- 4.程丽.一种改进的支持向量聚类算法的设计与实现[D].北京邮电大学[2024-03-20].DOI:CNKI:CDMD:2.1012.333271.
- 5.李善玺.基于机器学习的未知恶意代码自优化实时检测技术研究[D].兰州大学[2024-03-20].
- 6.Romain Fouchereau.IDC 2023 Global DNS Threat Report[R].IDC[2023-08].

勒索软件防范的探索与实践

孙一伟、崔毅然、陈其乐、吴鹏、张沁怡 | 上海证券有限责任公司

摘要：勒索软件因其独有特性，使企业在防范过程中面临“难发现、难应急和难恢复”的挑战。本文简述上海证券勒索软件防范工作的思路和相关实践，缓解勒索软件带来的安全风险。

关键字：勒索软件、情报、能力评估、风险排查、应急处置、数据备份

一、前言

勒索软件与病毒、木马、蠕虫、间谍软件、广告软件等均属于恶意软件，但勒索软件因隐蔽性强、破坏性大和传播速度快以及恢复难度高等特点，使其在恶意软件中“独树一帜”。

2017年，WannaCry勒索软件的爆发标志着勒索软件攻击的全球性觉醒。这场前所未有的网络瘟疫不仅首次将勒索软件的威胁带入了国际视野，更开启了勒索攻击活动的高潮。自此之后，勒索软件的威胁不断升级，其攻击手法变得更加复杂和猖獗，对全球的网络安全构成了持续而严峻的挑战。

据统计，攻击者在投放勒索软件时，远程桌面入侵、漏洞利用以及弱口令成为其主要的投放途径。近年来，勒索软件所带来的数据泄露风险也急剧增加，从行业划分来看，金融行业一直以来是勒索攻击的重要目标。

为保护企业重要数据和投资者个人信息，支撑企业数字化转型并巩固数字化建设成果，同时兼顾“降本增效”大环境下IT投入有限的现状，本文从中小券商视角出发探讨积极利用企业已有资源持续开展勒索软件防范工作，以期为同行提供有益参考。

二、勒索软件防范的探索与实践

（一）面临的挑战

勒索软件因其“独树一帜”的特点，使企业在勒索软件防范过程中面临“难发现、难应急、难恢复”的挑战。

1. 难发现

勒索软件的最初攻击策略主要是通过加密数据勒索赎金，目前则多以威胁泄露数据向受害者施压以获得赎金，主

要表现为在加密数据之前先窃取数据，然后以数据公开或售卖等形式对受害者进行勒索。这类策略的改变，使得勒索软件的攻击行为更为隐蔽，并且对受害者构成了更大的威胁。

2. 难应急

勒索软件因其破坏性大且传播速度快，使得应急响应变得极为困难。一旦感染，勒索软件能在短时间内对大量数据造成加密或锁定，导致系统瘫痪或重要信息无法访问。同时，若企业网络架构设计不合理，区域隔离不完善，勒索软件往往能利用同类漏洞在网络环境中迅速蔓延，感染更多的设备，进一步加剧了应急响应的复杂性。

3. 难恢复

勒索软件通常采用高强度的加密算法，而且其变种多样，每种变种都可能采用不同的加密算法或攻击手段，加之系统环境复杂多样，导致现有解密工具的有效性严重受限。此外，数据备份机制的不足或失效，以及勒索软件在加密数据之前删除或破坏备份文件的行为，进一步加剧了数据恢复的难度。

（二）勒索软件防范的探索与实践

1. “知彼知己”

通过多种途径收集勒索软件相关的情报信息，以实现“知彼”的目的。

收集方式和途径包括积极响应各级监管部门发布的风险预警和风险排查通知、充分利用行业网络和信息安全态势感知平台提供的情报，以及参考各大安全厂商的研究报告和威胁情报分享。通过多元化的信息来源和多维度的信息整合，逐步深化对勒索软件威胁的理解，并构建更为全面的、有针对性的防御体系。勒索软件情报信息汇总表（表1）：

表1 勒索软件情报信息汇总表

勒索软件名称	攻击利用方式	利用信息	情报来源
Wannacry	漏洞利用	CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147 CVE-2017-0148	XX 部门排查通知
Stelobj	弱口令	MSSQL 数据库弱口令	XX 部门排查通知
Lockbit	远程桌面	口令爆破	XX 安全厂商
Lockbit	漏洞利用	CVE-2023-4966	XX 安全厂商
.....			

聚焦两个“有什么”——有什么能力,有什么风险,以达到“知己”的目标。

梳理现有安全资源(安全工具、安全服务等),特别是针对勒索软件及其主要投放途径(远程桌面,漏洞和弱口令),需要明确现有的安全资源是否具备对应的识别和防护能力。在《勒索软件情报信息汇总表》基础上,扩展为安全资源能力评估表(表2):

表2 安全资源能力评估表

勒索软件	利用方式	CVE	WAF	IPS	流量威胁检测设备	恶意软件检测设备	数据库审计设备	操作系统日志审计	域安全监控	主机防病毒	容器安全防护	HIDS	漏洞扫描工具	第三方安全检测服务
Lockbit	远程桌面	--	否	是	是	是	否	是	否	是	否	是	是	是
Lockbit	漏洞	CVE-2023-4966	否	否	是	是	否	否	否	是	是	是	是	是
WannaCry	漏洞	CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147 CVE-2017-0148	否	是	是	是	否	否	是	是	是	是	是	是
Stelobj	数据库弱口令	--	否	否	是	是	是	否	否	是	是	是	否	否
.....														

完成评估后,基于现有安全资源的识别和防护能力,针对可能被勒索软件利用的攻击方式形成专项风险排查报告,以弱口令为例(表3),并持续推进相关的整改工作。

表3 弱口令专项排查表

弱口令专项排查表				
类别	账户名称	系统名称	主机信息	数据库信息
操作系统	域账号			
	本机账号			
应用系统				
服务				
数据库				

综上,通过“知彼知己”感知内外部环境,为企业持续开展勒索软件防范工作奠定基础。

当然,在条件许可的情况下,企业也可以建立安全防护工具的有效性验证机制,定期或不定期的针对勒索软件防范的特定场景,对安全防护工具及其安全策略进行有效性验证。查漏补缺,不断强化安全工具防护体系,持续优化安全检测和告警策略,以确保安全防护工作的有效性和及时性。

2.“未雨绸缪”

依据企业网络安全事件应急管理办法和应急预案,制定并不断完善应急响应操作流程,通过定期演练来缓解勒索软件感染后的应急难题。本文不全面阐述由勒索软件感染导致的网络安全事件的整体应急预案,而是聚焦于应急过程中的技术处置策略与措施。

笔者参照《勒索软件防范应对指南》设计应急技术处置流程(图1),并结合企业现有的安全资源,针对流程中各环节制定对应的处置策略与措施。

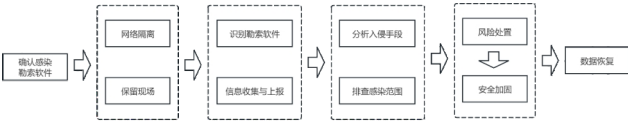


图1 勒索软件应急技术处置流程

以“确认感染勒索软件”环节为例(图2),基于前一小节“知己”章节内容,企业的态势感知平台、SOC或SIEM中应预先设置监测指标,将各类安全工具的事件汇聚分析,关注存在勒索软件特征的异常流量、异常资源占用等。在排查过程中可较为快速的对“感染未加密”情况进行确认,而非感染后在不同的安全工具中逐一排查,导致应急效率降低。

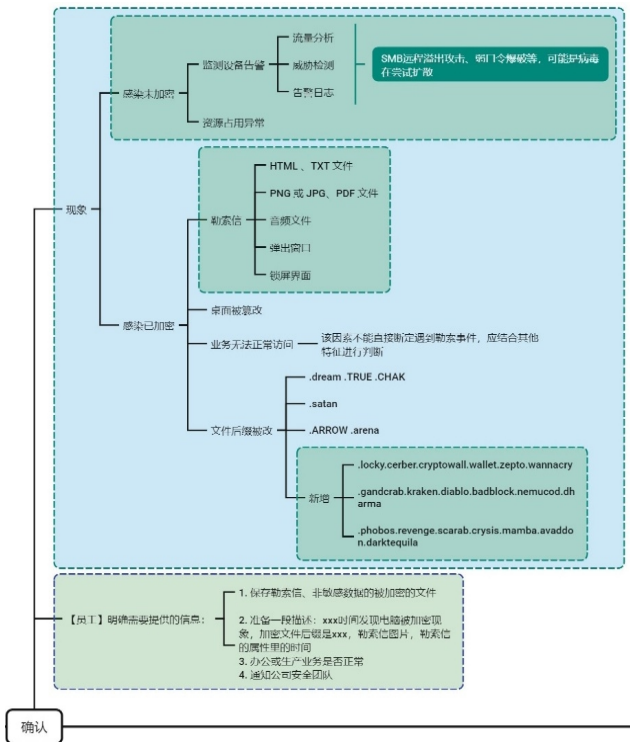


图2 “确认感染勒索软件”环节

再如“网络隔离”环节，除了利用基础设施资源，如拔网线、禁用交换机端口，启用网络防火墙deny策略、虚拟机卡禁用等隔离手段外，还应考虑在基础设施资源无法及时到位的情况下，如何有效利用安全防护工具的主机入侵防御、主机防火墙、微隔离等功能提升应急处置效率。

笔者认为，应急技术处置的每个环节都应尽可能与安全资源进行对应。日常安全运营过程中，应定期梳理现有的安全资源及能力清单，及时更新勒索场景下的应急预案，确保在紧急情况下能够迅速、准确调用所需资源。

3.“有备少患”

针对勒索软件感染后难恢复的问题，通过加强数据备份和验证，强化备份系统的安全管控，以及实施备份区域间网络隔离等策略来缓解风险。

依据《证券基金经营机构信息技术管理办法》《证券期货经营机构信息系统备份能力标准》，企业确定信息系统备份能力等级，实现相匹配的数据备份能力，其中涵盖数据备份的频率、存放的地点以及有效性验证的频率。在有效性验证方面，还需关注通过虚拟机备份实现数据备份场景下的虚拟机有效性验证。

随着勒索软件从单一形式演变为多重勒索，备份系统的安全管理级别需要相应提升，应将其纳入整体的安全管控范围，以防止备份系统被攻破后导致数据备份失效。

此外，根据信息系统备份能力等级，数据备份会进行本地机房存放、同城存放以及异地存放，通常会由“两地三中心”实现。鉴于勒索软件传播速度快的特点，企业通过网络隔离，禁止开通RDP、139、445等高风险端口，避免风险在

两地三中心之间传导。对于必须开通高风险端口且无法进行补丁更新的情况，则利用主机侧安全产品的主机入侵检测、虚拟补丁等功能来降低风险传导的可能性。

三、总结和展望

在勒索软件防范过程中，安全防护工具的重要性不言而喻。然而，这并不意味着单纯通过采购新的工具就可以强化安全防护工具体系。特别是在当前“降本增效”的大环境下，笔者认为更应注重熟悉并掌握现有安全防护工具的能力和功

能，通过合理配置和优化，充分发挥其最大效用。此外，在实践中，我们发现充分利用好现有安全资源，确实可以在较大程度上提升风险的检出率。但考虑到对系统运行的影响，以及人员配合程度、操作复杂度等因素，后续整改工作的实际推进仍然面临较大阻力。为应对这一问题，笔者采用了“控增量，去存量”的策略来推进整改工作。“控增量”是指将勒索软件易于攻击利用的风险点作为系统或主机上线前的强制安全检查项，并将风险点纳入日常的专项安全监测。“去存量”则是遵循“先外围，后核心”的原则，即优先处理外围系统安全风险，逐步向核心系统推进，确保整改工作有序开展的同时，也将对系统运行的影响降到最低。

最后，勒索软件攻击手段不断演变，但网络安全的本质始终不变。坚守本质，针对攻击特性，开展持续的安全运营工作，防微杜渐，才能不断夯实网络安全的基石，有效应对各类新型网络威胁。

参考文献

- 1、《2023年勒索软件流行态势报告》360数字安全 | 360安全大脑
https://cdn.isc.360.com/isc-cxo/2023_Ransomware_Report.pdf
- 2、六年间全球十大勒索攻击事件盘点：没有底线全是算计 腾讯安全
<https://new.qq.com/rain/a/20230512A07TCM00>
- 3、《勒索软件防范应对指南》国家互联网应急中心

东方证券

信创特权账号管理系统的探索与实践

俞建群、邬晓磊、陈炎津 | 东方证券股份有限公司
陆凯捷、杨帅 | 浙江齐治科技股份有限公司

摘要：随着数字化转型的深入，东方证券面临着特权账号管理的网络安全挑战。为此，构建了信创特权账号管理系统（PAM），实现对特权访问的严格控制和可追溯性。该系统采用分层架构，结合堡垒机技术，增强了权限管理和操作记录。通过单中心高可用设计和双中心异地容灾架构，确保业务连续性和数据安全。功能和性能验证显示，系统在高负载下稳定运行，未发现安全漏洞。信创特权账号管理系统的实施显著提升了信息安全管理能力，为金融行业提供了重要参考。

关键字：特权账号管理、堡垒机、风险控制、合规性审计、自动化运维、安全审计、多中心架构

一、概述

在数字化转型的推动下，证券行业的运营方式正在发生深刻变化，信息技术系统的依赖性日益增强。虽然这种转变大幅提升了业务的效率和灵活性，但同时在面对不断升级的网络安全威胁时，也使得安全防范措施落实的难度大大增加，尤其是针对特权账号管理的场景，带来了不小的挑战。

东方证券在数字化转型的浪潮中，积极推动业务与技术的深度融合，这不仅加速了公司的发展，也使得网络和信息安全管理变得日益复杂。面对信息系统建设任务的增加和频繁的上线变更操作，我们的网络和信息安全管理能力正面临更大的挑战。

为了应对这些挑战，东方证券采取了全面而深入的措施，聚焦于解决网络和信息安全领域的基础性和深层次问题。我们依托稳健性、差异性、创新性等原则，构建全面的防护体系，减少潜在的安全风险。在此基础上，东方证券已经部署了特权账号管理系统（PAM），这是我们安全管理体系建设的一个重要组成部分。为了进一步提升网络和信息安全管理能力，我们以建设信创特权账号管理系统为目标，旨在通过这一系统实现对特权访问的严格控制和精细管理，确保关键操作的透明性和可追溯性。通过这些综合性措施，东方证券将不断提升网络和信息安全管理的能力，确保公司在数字化转型的道路上安全、稳定地发展，同时也保障了客户和公司的利益不受侵害。我们致力于打造一个安全、高

效、可靠的网络环境，支持公司的长期发展和创新，为推动行业的网络安全管理做出积极贡献。

目标1：构建一套符合我司现状的特权账号管理体系。

首先，我们需要对公司内部的现状进行全面分析，包括业务需求、信息安全风险、技术架构等方面。然后，根据分析结果确定特权账号管理体系的设计原则和目标，确立适合公司实际情况的技术路线。

目标2：建设全栈信创特权账号管理系统。东方证券积极推进全栈信创特权账号管理系统建设，优先采用国产软硬件设备，设计分层系统架构，确保高内聚低耦合。选择符合国家安全管理标准的管理软件，强化账号权限控制与审计。实施严格安全措施，提升系统稳定性和安全性，保障信息资产自主可控。

目标3：结合堡垒机实现数字资产的访问凭证安全可控。仅通过堡垒机或者特权账号管理系统无法实现账号全生命周期管理，所以在信创特权账号管理系统的实践过程中，需要结合堡垒机，加强对数字资产的访问凭证安全控制。通过免密登录、高危指令控制等技术手段，对特权账号的访问进行严格管控，防止未授权访问和滥用，提升系统安全性。

二、探索与实践

（一）整体架构设计

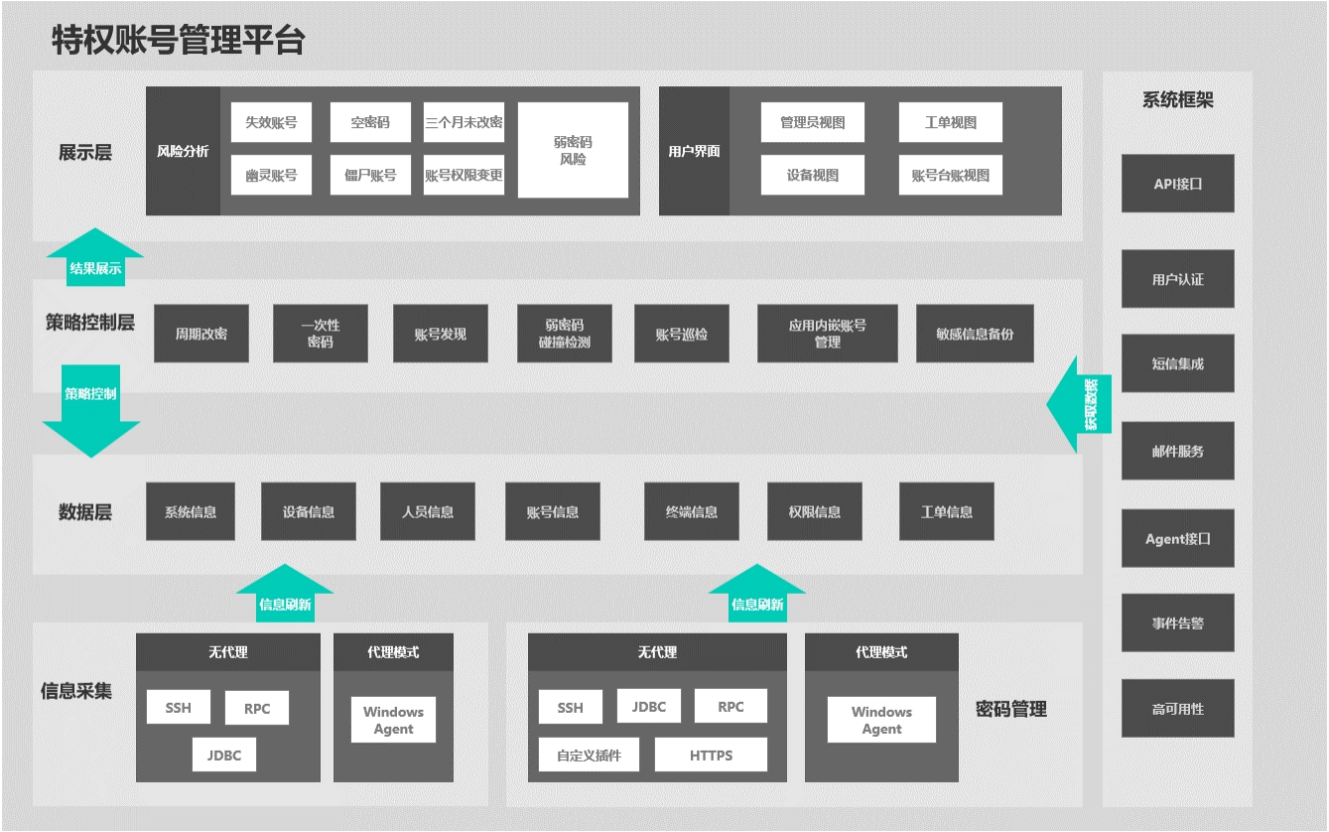


图 1

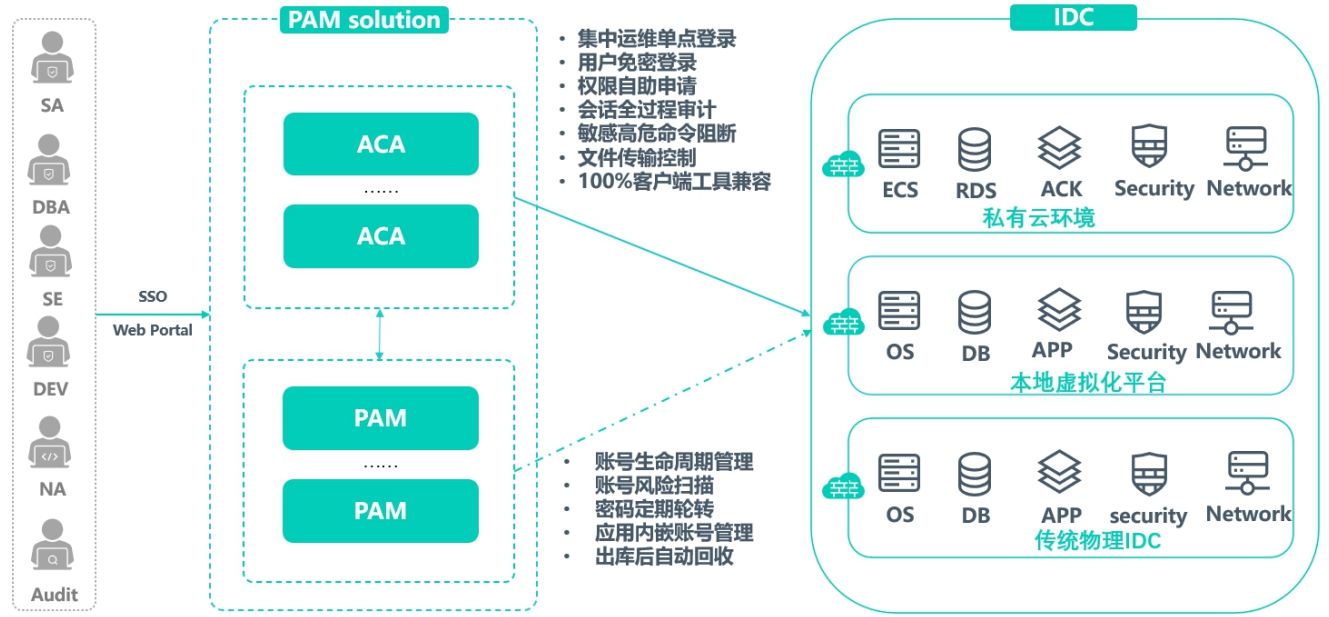


图2

我们的信创特权账号管理系统采用分层架构设计，共分为四个核心层次，以确保系统的高效性和安全性：

信息采集层：在这一层，系统利用远程协议和API等技术手段，自动从服务器、网络设备、数据库和中间件等资源中收集与账号安全相关的数据。

数据层：该层负责对采集到的数据进行分类和整理，根据数据的不同类型和既定规则，确保数据的有序性和可检

索性。

策略控制层：在这一层，系统运用大数据分析和机器学习技术，对数据进行深入的智能关联分析，以识别账号相关的风险和异常行为。

展示层：根据不同的使用场景和需求，将分析结果以分层分类的方式呈现出来，提供了清晰的视角来查看和管理各种异常数据。

此四层架构的设计旨在为安全管理提供清晰的视角和决策支持,确保能够为系统的下一步优化提供准确的整改方向和数据支撑。

在技术方案层面,我们通过整合堡垒机提供的精细化权限控制、全面的操作记录跟踪以及对全运维场景的广泛兼容性,显著提升了数据中心的运维安全管理效能。这一整合策略成就了一套既符合东方证券业务特性又满足其安全需求的运维账号管理规范。

精细化权限管理:利用堡垒机的细粒度权限控制系统,我们能够精确地定义每个运维人员对数据中心资源的访问权限,确保他们仅能执行其职责范围内的操作。

全面的操作留痕:堡垒机的无死角操作记录功能确保了所有运维活动都有详细的日志记录,包括命令执行、文件传输和系统配置更改等,为事后审计和事故追踪提供了坚实的基础。

全运维场景兼容:我们的方案覆盖了从物理服务器到虚拟化环境,再到云平台的全运维场景,确保了运维安全管理的全面性和一致性。

定制化管理规范:结合东方证券的业务特性和安全需求,我们制定了一套定制化的运维账号管理规范,旨在提高安全性的同时,也考虑到了运维效率和业务连续性。

风险控制与合规性:该方案强化了数据中心的风险控制能力,并确保了所有运维活动都符合相关的法律法规和行业标准。

技术与流程的融合:通过技术手段与安全流程的紧密结合,我们不仅提升了系统的安全性,也优化了运维团队的工作流程。

持续改进与适应性:我们的方案设计具有灵活性和可扩展性,能够适应东方证券未来业务发展和技术变革的需要。

账号上线流程:

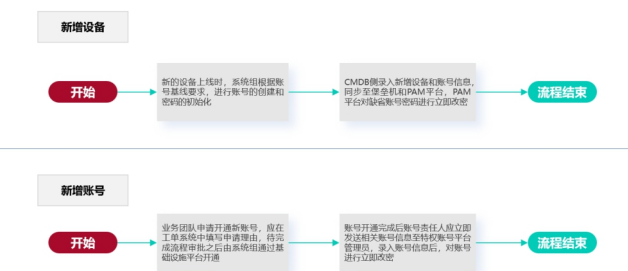


图 3

账号安全检查与维护:

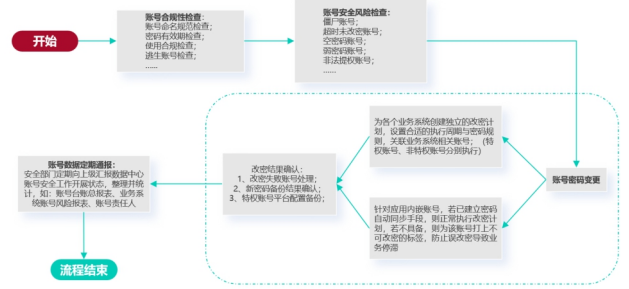


图 4

账号的访问控制与密码安全:

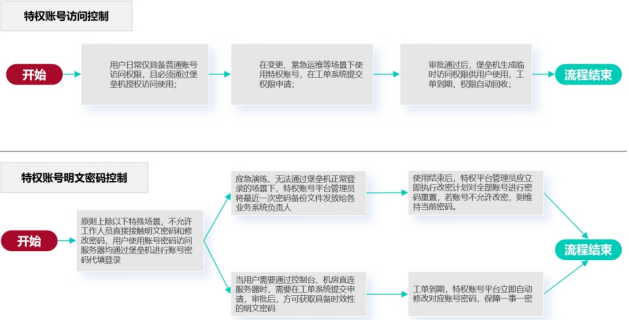


图 5

(二) 业务连续性

1. 单中心HA设计

HA (High Availability), 意指高可用性集群。主要是为了防止单点故障时造成的服务不可用,从而提升系统的可用性。信创特权账号管理系统是集权化的账号管理平台,负责整个生产环境主机、网络设备、数据库、中间件等各类资产上所有账号密码的管理,该系统的业务连续性非常重要。为此我们对于系统的部署架构做了如下设计:单个数据中心部署两台信创特权账号管理系统组成双机热备,使用虚拟IP对外提供服务,两台设备中只有一台对外提供服务,另外一台备节点则会同步主节点的数据,并在主节点发生故障时自动切换备节点。

数据一致性和数据保护

部署完HA后,主备节点的应用用户将会添加双向信任,同时数据加密文件将变为一致。

HA的主节点会将数据不断同步给备节点,以保证两个节点之间的数据一致性,HA同步的数据和同步方式如下:

数据类型	同步方式
配置数据	数据库流复制,实时同步。同步周期为每秒。
ElasticSearch 审计记录	实时同步,由 HA 服务管理
时间	由 Chronyd 服务进行时间同步。在备机的配置文件中会自动将 NTP 服务器配置为主机的地址。

故障检测和恢复

HA部署下信创特权账号管理系统会执行以下周期检测：

- 主、备节点检测ping_ip是否可达；
- 备节点ping主节点，检查主节点是否可达；
- 主节点磁盘空间检测；
- 主节点服务检测。

主备切换机制：当以上检测结果满足以下任一条件时，信创特权账号管理系统会判定主节点故障，并在备机状态正常的情况下，立即将服务切换到备节点，使备节点成为新的主节点。

■在备节点到ping检测地址网络可达的前提下，主节点到ping检测地址网络不可达，默认检测失败次数达到10次，则进行切换；

■主节点服务检测失败，默认检测失败次数达到10次，则进行切换；

■主节点本地剩余磁盘空间小于1GB。检测到空间不足则立即进行切换；

■配置心跳口情况下：备节点ping主节点检测失败，ping检测地址可达，并且距离上一次心跳包接收的时间超过备节点ping主节点检测失败时间上限（检测时间间隔（默认10s）*失败次数（默认10次）=100s），则进行切换。

信创特权账号管理系统在单个数据中心通过HA的部署架构实现应用高可用。

2. 双中心异地容灾架构

信创特权账号管理平台结合东方证券IT架构与管理需求，遵循“两地三中心”的基础设施建设规划思路，一期设计了两地双中心的异地容灾架构。

信创特权账号管理平台在单中心HA设计的基础上，分别部署在上海金桥数据中心、南方数据中心，两个中心的信创特权账号管理平台同时对外提供服务，并且从配置层面实现数据自动同步。

数据一致性和数据保护

多站点部署后，所有站点的服务用户将会添加双向信任，并在各站点上开放到其他站点的防火墙端口

数据类型	同步方式
配置数据	数据库流复制，实时同步。同步周期为每秒。 多活模式下，所有站点对数据库的写操作，均在主站点的数据库中执行，并向其他站点的数据库同步。

故障检测和恢复

多站点中的某个站点出现故障时，支持通过自动切换的方式，将主站点切换到其他站点，从而保证多站点的业务不会中断。

对于2个站点的情况，会将另一个站点提升为主站点。

自动切换的检测机制如下：

站点中的从站点会不断ping检测其他站点的地址是否可达，若不可达，则视作该站点故障；若可达，则会继续通过

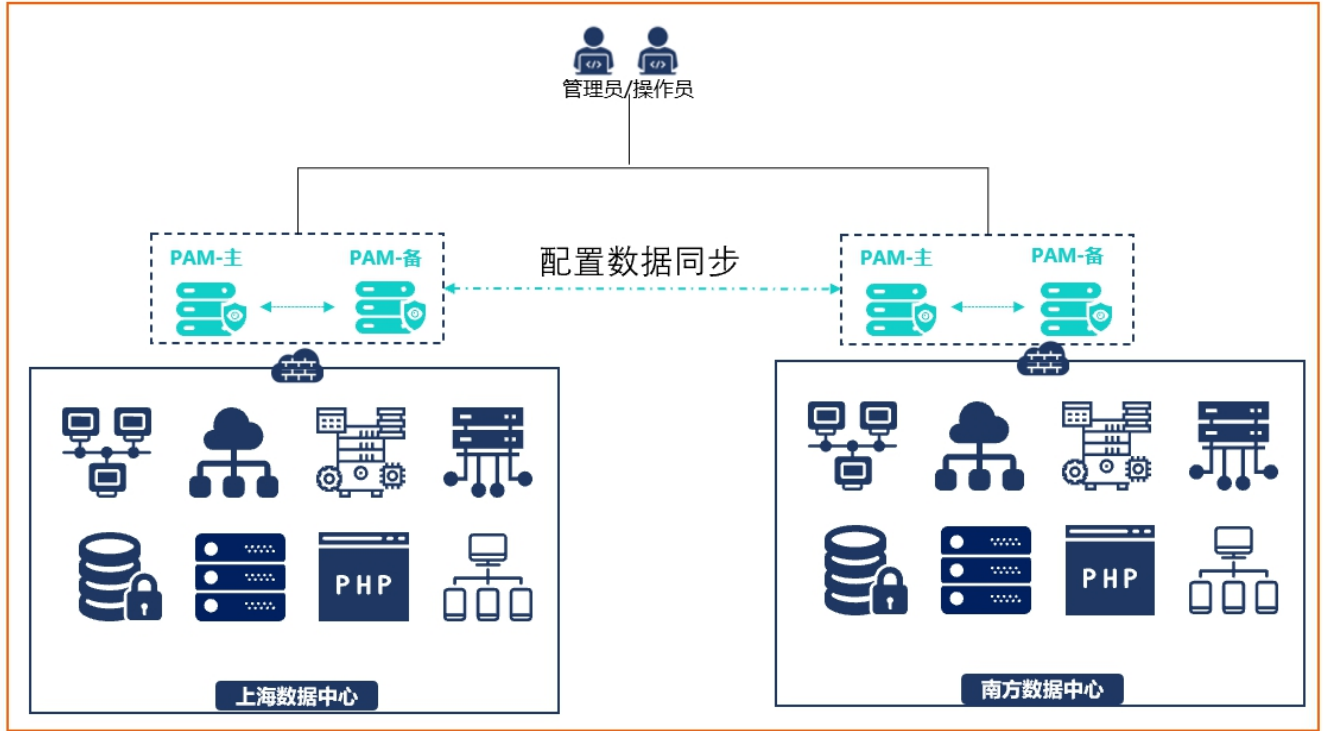


图 6

SSH登录该站点并进行下一步检查。

当第二顺位的从站点发现符合以下所有条件时,发起自动接管,成为新的主站点:

- 检测到主站点故障。
- 该从站点能够正常ping通仲裁节点。

3. 完善的备份恢复机制

鉴于信创特权账号管理系统中存储了东方证券数据中心所有关键账号和密码,因此,一个全面而精细的备份与恢复策略对于保障业务连续性和数据安全性至关重要。该机制旨在确保在面临任何意外故障或数据丢失事件时,能够迅速恢复正常运行,并确保账号信息的机密性。我们采取了以下措施来实现这一目标:

密码缓存机制:为了兼容第三方系统的账号密码使用需求,我们的系统设计了密码代理服务。该代理服务将维护账号密码的副本,确保即便在主系统遇到异常时,也能持续为第三方系统提供所需的账号密码信息。

多元化备份存储策略:除了系统内部对账号密码信息进行加密存储之外,我们还支持多种外部备份方式,以实现数据的多重保障。备份可以通过多种渠道进行,包括但不限于文件服务器、电子邮件、密码打印服务器、密码保险库以及对象存储服务(OOS)。

强化加密与安全性:所有备份的密码文件均采用高级加密措施,支持ZIP压缩加密和PGP加密两种方式。用户在获取明文账号密码信息时,必须使用相应的ZIP密码或PGP私钥进行解密,进一步保障了账号密码信息的安全性。

通过这些设计,我们的信创特权账号管理系统不仅提升了数据备份和恢复的效率,也显著增强了数据的安全性,为东方证券的数据中心提供了一个安全、可靠、高效的账号管理解决方案。

(三) 功能及非功能性验证

1. 功能性验证

信创特权账号管理系统部署完成后,我们根据管理体系要求,对系统开展相关功能验证工作,验证结论如下:

账号自动发现

系统支持通过手动或自动的方式触发账号探测策略,采用预设的特权账号批量连接待测资源。当检测到账号状态变更时,如服务器中新增特权账号或原已有账号缺失等情况,系统将以工单流的方式交由对应资产责任人确认。责任人可通过工单流获悉相应资源中变更的特权账号情况,对其确认后此类账号信息将自动托管至账号管理系统中。

借助周期性的账号自动化探测,实现数据中心特权账号的集中纳管。

异常账号分析

支持特权账号巡检功能,实现对数据中心的各类系统

账号的合规性检测,帮助管理员及时发现潜在的风险账号,规避运维管理风险。通过账号巡检功能,可发现如下异常账号信息:

- ✓ 空密码:未托管密码的账号
- ✓ 弱密码:对密码进行弱密码规则匹配,或者对比弱密码库
- ✓ 僵尸账号:超过三个月未使用过的账号
- ✓ 幽灵账号:新增系统账号类别
- ✓ 网络异常:无法正常连接到该设备
- ✓ 账号异常:该账号密码无法正常登录到系统
- ✓ 三个月未改密:该账号密码超过三个月未更改
- ✓ 权限变更:该账号权限发生变更

密码策略管理

自动改密:系统支持对主机、网络设备、数据库、中间件等各类资源中作为运维管理用途的系统账号密码进行变更操作。可通过改密计划预设密码变更周期、密码复杂度及密码变更范围等信息,采用手动或自动化方式触发改密计划对指定资源账号进行改密操作。

密码验证:支持手动或自动化的方式验证特权账号密码的连通性。

历史密码:针对系统中各类密码变更操作,无论是人为修改还是改密计划自动执行的操作,均支持节点留痕功能,管理员可在任意密码备份节点处进行密码回退操作。

密码工单管理

提供了一种密码动态维护的管理模式,当用户需要获取服务器系统账号密码时,可通过系统 web 页面申请相应账号密码的临时应用权限。工单经管理员审批后,系统将相应服务器账号密码临时分发给相应用户,当密码过期后,系统会自动遵循已有的改密计划对相应账号密码进行改密操作。

通过“一次一密”的自动化管理模式,规避因人工分发密码,未及时回收导致的密码泄露风险,提高特权账号安全等级。

生命周期管理

信创特权账号管理系统支持账号集中化管理功能,可详细记录相应账号从创建至删除的一系列变更操作。同时系统引入自动化管理手段,采用工单流的模式实现对特权账号创建、变更、修改、锁定、删除进行统一维护,统一管控。

2. 非功能性验证

为保障信创特权账号管理系统在面对高负载情况时,依然能够维持高效的响应速度和处理能力,满足复杂的账号密码管理需求,我们执行了一系列的性能验证措施。

压力与负载测试:通过模拟真实业务场景,我们对系统进行了严格的压力测试和负载测试。这些测试旨在模拟系

统在极端工作条件下的表现，确保其稳定性和可靠性。

测试结果分析：测试结果显示，即便在高负载环境下，系统的核心功能，如账号筛选、资产导入、资产删除、账号导入和账号删除等，均能保持在可接受的响应时间内。此外，系统资源的消耗情况也处于合理范围内，CPU性能消耗不到5%，内存性能消耗不超过50%。

性能优化：基于测试结果，我们对系统进行了必要的性能优化，以进一步提升其在高负载情况下的表现。

通过这些综合性能测试和优化措施，我们确信信创特权账号管理系统具备了在高负载环境下稳定运行的能力，能够充分满足东方证券对账号密码管理的高标准要求。最终与非信创版本性能数据对比如下：

测试项	测试要求	响应时间 (全栈信创)	响应时间 (非信创)
资产导入	5000 个资产	1h16m22s	59min56s
资产删除	5000 个资产	59min13s	36min26s
账号导入	5000 个账号	40min26s	25min25s
账号删除	5000 个账号	2min12s	1min48s



图 7



图 8

安全性验证与测试

为了确保信创特权账号管理系统自身的安全防护，从而抵御未授权的访问和潜在的数据泄露风险，我们实施了一系列全面的安全测试措施：

全面安全测试：通过综合运用安全扫描、渗透测试和权限审计等方法，我们对系统进行了细致的安全评估。

第三方安全扫描：为了提高测试的客观性和权威性，我

们引入了第三方专业机构进行安全扫描，确保测试结果的准确性和公正性。

漏洞排查：经过严格的测试流程，最终的扫描结果显示，信创特权账号管理系统的全栈版本未发现任何中等或高危级别的安全漏洞。

持续安全保障：这些测试结果不仅验证了系统的安全性，也为我们提供了持续改进和加强系统安全性能的依据。

通过这些缜密的安全测试，我们确信信创特权账号管理系统已经具备了强大的安全防护能力，能够有效地保护敏感数据，确保系统的长期稳定和安全运行。

(四) 创新及推广性

全面性能与安全保障

信创特权账号管理系统为东方证券提供了一个全面的性能和安全解决方案。系统不仅保障了特权账号的安全管理，还优化了业务流程，提升了系统性能，从而增强了整个信息系统的运行效率和安全防护水平。

集成化的管理平台

该系统的设计超越了单一的账号管理功能，它能够无缝集成多种安全系统和运维管理工具，形成一个全面的一体化管理平台。这种集成化方法实现了安全管理的统一、运维监控的集中化以及问题处理的高效率，显著提升了信息系统的管理效能。

智能化风险控制

利用大数据技术，信创特权账号管理系统实现了智能化的账号风险管理。系统能够自动分析账号数据，比对安全规则，识别潜在风险，并主动采取预防和应对措施，从而提高账号管理的智能化和自动化水平。

自动化运维流程

系统进一步推动了运维流程的自动化，包括自动部署、配置管理、变更管理和故障排查等关键环节。通过自动化，不仅减轻了运维团队的工作负担，还降低了人为错误的风险，增强了系统的稳定性与可靠性。

综合创新与推广潜力

综上所述，信创特权账号管理系统在东方证券的应用中展现了显著的创新性和推广潜力。它不仅提升了信息系统的安全性能，还通过智能化和自动化技术，推动了东方证券信息化建设向更高层次的发展。

三、成效总结

安全性显著提升

东方证券的信创特权账号管理系统通过整合海光国产CPU、银河麒麟V10操作系统、华为OpenGauss数据库以及东方通中间件,实现了全面的信创技术栈适配。这一战略举措极大地增强了系统的安全性能,使系统能够敏锐地识别并迅速响应各种潜在安全威胁,显著降低了安全漏洞和其他风险的发生概率。

可控性与可视化增强

系统的引入,特别是账号可视化管理和运维优化工具的应用,极大提升了管理员对账号安全的监控和管理效率。东方证券因此获得了一个高度可控且数据可视化的信创账号安全管理平台,有效减少了运维成本和人力资源的投入。

合规性与监管遵循

系统设计充分考虑了等级保护和行业监管要求,通过其强大的密码管理、账号权限控制以及审计日志记录等功能,确保了安全合规性。此外,系统还建立了一套完善的合规性审计和监管报告机制,进一步推动了账号密码管理的规范化和行业合规性。

用户安全意识增强

通过开展安全培训和提升安全意识的活动,我们增强了用户对特权账号安全重要性的认识,提高了他们的安全意识和行为规范,从而减少了人为因素对系统安全可能造成的负面影响。

创新技术推广

在信创特权账号管理系统的探索和实践过程中,我们引入了一系列创新技术和理念,不仅推动了系统的创新,也促进了其在行业内的推广应用。

综合成效

总体而言,东方证券信创特权账号管理系统的探索与实践取得了显著成效。它不仅提升了系统的安全性和运维效率,还在业务流程和合规性方面实现了长足发展,为信息安全保障做出了积极贡献。

参考文献

- 1.Garbis J, Chapman J W, Garbis J, et al. Privileged access management[J]. Zero Trust Security: An Enterprise Guide, 2021: 155-161.
- 2.全国信息安全标准化技术委员会. 信息安全技术 网络安全等级保护基本要求:GB/T 22239-2019[S]. 2019.
- 3.国家金融监督管理总局. 银行保险机构数据安全管理办法[S]. 2024-12-27.

证券公司核心交易系统安全韧性体系的实践探索

华仁杰、沈嗣贤、徐俊超、郑征 | 东吴证券股份有限公司

摘要：随着金融市场和数字化转型的推进，证券公司核心交易系统面临复杂的安全和业务风险。以东吴证券为例，介绍了其在核心交易系统安全韧性建设中的经验与成效。该项目通过构建统一的安全管理平台，集成多活服务、异地灾备、预案自动化和实时监控等技术，显著提升了系统韧性与恢复能力。项目不仅符合行业合规要求，还在保障业务连续性、降低运营风险和优化灾备能力方面取得了良好效果，为证券行业的安全建设提供了有益借鉴。

关键字：系统故障、灾备切换、运行安全、韧性体系、业务连续性

一、背景

全球金融市场快速发展，证券核心交易系统作为金融市场的重要基础设施，承载着海量关键数据。面对日益复杂的网络安全威胁和灾难风险，确保系统的安全运行和业务连续性变得尤为重要。

监管机构已就此制定了一系列具体标准：

■《证券期货业网络安全管理办法》要求建立故障备份和灾难备份设施。

■《证券基金经营机构信息技术管理办法》规定每年至少进行一次应急演练。

■《证券期货业网络安全等级保护基本要求》对异地灾备中心和业务实时切换提出了要求。

■《证券营业部信息技术指引》要求每年至少进行两次应急演练。

■《证券期货经营机构信息系统备份能力标准》对恢复时间目标(RTO)和恢复点目标(RPO)作出了明确规定。

■《证券公司网络和信息安全三年提升计划(2023-2025)》强调了预案管理平台的建设及自动化管理的重要性。

这些规范凸显了灾备演练的必要性，常态化管理的迫切性，以及灾难切换的时效性对业务持续性的重要影响。预案体系的自动化、标准化建设将成为证券核心交易系统未来安全建设的重点，也是提升行业运行安全韧性的必由之路。本文将围绕运行安全韧性体系的构建展开实践探索，并分享具体的建设经验。

二、建设挑战

尽管许多证券公司已构建了多活服务和异地灾备中心等基础能力，以应对运行中可能出现的风险，但在实际运营

中依然面临着诸多挑战与困难。首先，运行安全保障机制尚未形成系统化的管理体系，预案体系的自动化和标准化建设缺乏有效支撑。其次，灾备演练的门槛较高，流程复杂冗长，使得常态化运营难以落地。此外，运行风险的快速感知和风险自适应能力仍有待提升，而现有的可视化观测手段单一，难以满足对复杂多变风险环境的全面掌控。这些问题亟需在未来的安全建设过程中得到有效解决。

三、建设目标和任务

证券公司核心交易系统运行安全韧性体系实践，旨在构建统一的运行安全管理平台和一键式应急灾难切换能力，以增强系统的灾难应对能力和稳定性为核心目标，提升系统业务持续稳定运行能力，聚焦专业灾备运营指标，实现运行安全韧性体系建设。项目目标和任务的关系如下图1所示：

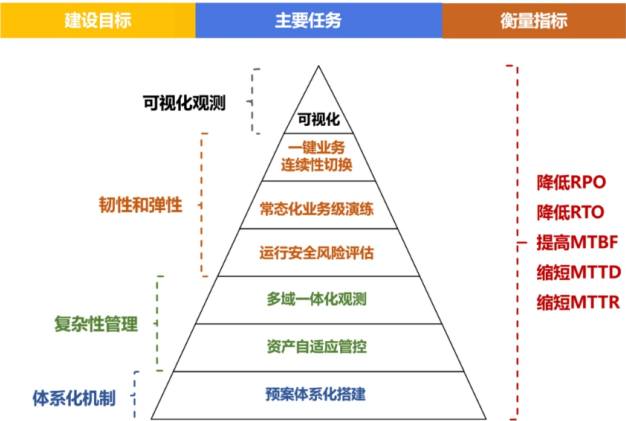


图1 项目建设和任务关系图

项目建设目标聚焦四个方面：

■**韧性与弹性**：实现底线运行能力的原子化管控，构建充足的冗余和自恢复机制。

■**体系化机制**：建立统一的资产管理体系，构建快速感知与风险干预的能力，实现灾备预案的标准化与自动化，确保核心业务具备一键切换的应急保障。

■**复杂性管理**：在有限指导下，全面管控复杂身份、资产及预案的生命周期，通过适度人工干预，管理海量复杂数据和资产的关联协同，控制动态运行风险。借助自动检测关联关系与上下文，有效管理未知变更的影响。

■**可视化观测**：实现多维度、一体化的系统监测，基于可见性驱动，快速干预与决策。

通过优化RPO（恢复点目标）和RTO（恢复时间目标），减少数据丢失及系统恢复时间，提升数据可靠性和业务连续性。提高MTBF（平均故障间隔时间）有助于延长系统稳定运行时间，而缩短MTTD（平均故障检测时间）和MTTR（平均故障修复时间）能够加速故障发现与解决，全面提升系统的韧性及运营能力。

项目主要任务包括：

- 建立体系化预案管理
- 实现资产的自适应管控
- 实施多域一体化监控
- 开展运行安全风险评估
- 推动常态化业务演练
- 实现一键业务连续性切换
- 完善运行安全的可视化观测

通过通过优化RPO（恢复点目标）和RTO（恢复时间目标），减少数据丢失及系统恢复时间，提升数据可靠性和业务连续性。提高MTBF（平均故障间隔时间）有助于延长系统

稳定运行时间，而缩短MTTD（平均故障检测时间）和MTTR（平均故障修复时间）能够加速故障发现与解决，全面提升系统的韧性及运营能力。

项目主要任务包括：

- 建立体系化预案管理
- 实现资产的自适应管控
- 实施多域一体化监控
- 开展运行安全风险评估
- 推动常态化业务演练
- 实现一键业务连续性切换
- 完善运行安全的可视化观测

通过构建完善的运行安全韧性运营机制，围绕这四大建设目标，持续优化核心运营指标。七项任务的有序推进，将确保核心交易系统的合规性与业务连续性，增强系统在面对挑战时的恢复力和适应性。

四、项目建设内容

本项目通过为核心交易系统构建运行安全管理平台，以快速完成运行安全韧性体系实践。运行安全管理平台以保障业务连续性为目标，面对散杂多乱的灾备资产和灾备技术实现集中管控，并提供监控、告警、编排、评估、演练、切换等功能，以降低系统RPO恢复点目标和RTO恢复时间目标、提高MTBF平均无故障间隔时间、缩短MTTD平均故障发现时间和MTTR平均故障修复时间。

（一）平台架构

平台架构如下图2所示：

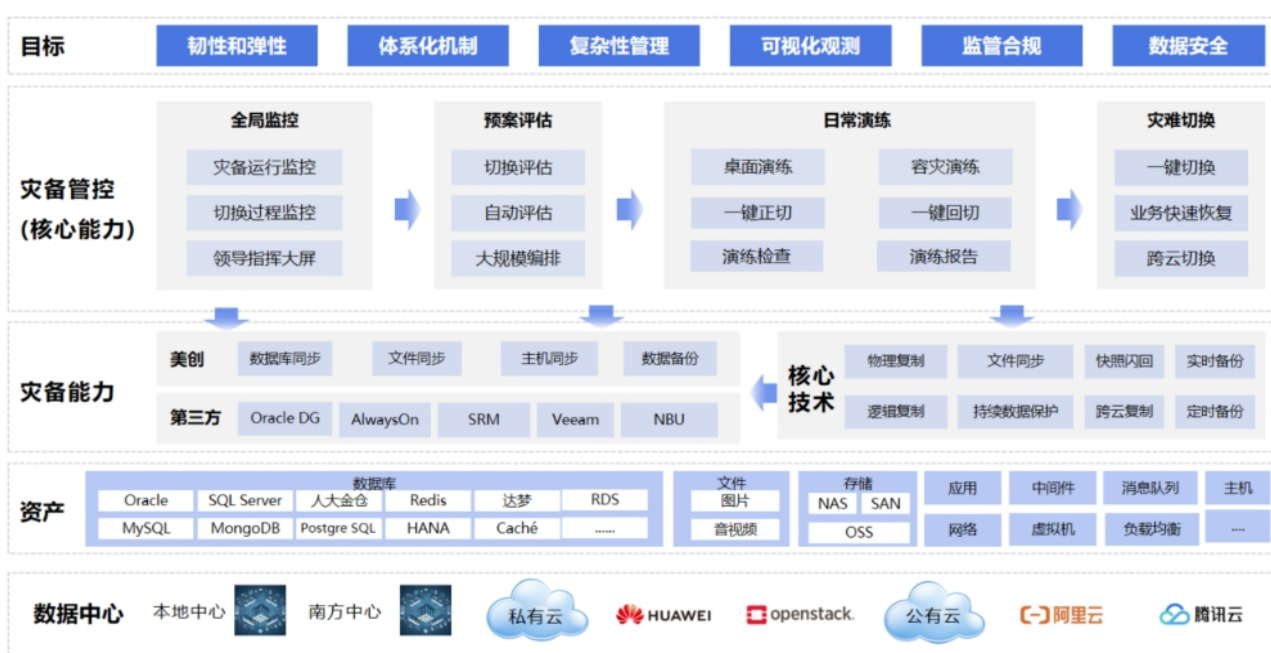


图2 平台架构示意图

运行安全管理平台基于B/S架构，具易于维护、部署、升级和扩展。采用微服务架构，将身份认证、通知中心和CMDB等模块进行模块化拆分，形成独立服务。每个服务可独立运行、部署和扩展，并通过轻量级通信协议互相通信，支持分布式部署和云原生应用部署。

平台中的每个微服务均采用MVC架构，其技术架构如下图3所示：

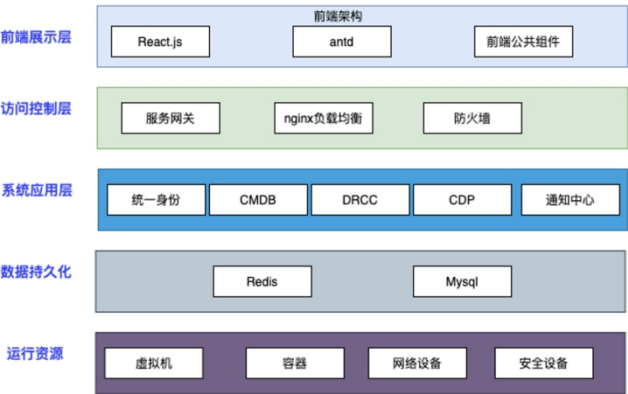


图3 运行安全管理平台技术架构图

(二) 六大核心能力

运行安全管理平台拥有六大核心能力确保运行安全：

1. 核心能力之一：预案体系化搭建

预案是为应对业务中断事件，从事前预警、事中处理到事后归档复盘，建立的完整应急处置方案。平台提供全流程、标准化的数字化预案体系，通过事件库、编排库和预案库三者的有效联动，形成一个高效、灵活和自适应变化的韧性预案体系。韧性预案体系具备提高编制效率、提高预案质量和方便更新维护等优势，同时平台能够根据业务系统的实时状态和风险情况，智能推荐灾备切换预案，有效提高组

织面对各种突发事件的应对能力，保障业务快速从灾难中恢复过来，以实现运行韧性的科学化管理。

2. 核心能力之二：资产自适应管控

核心交易系统资产复杂，涉及数据库、网络、应用、中间件、主机、负载均衡、消息队列、存储等资产，不同资产采用不同容灾技术。运行安全管理平台内置业务级容灾管控能力，平台通过自动检测技术，实现资产自动发现、容灾拓扑自动识别、业务拓扑自动绘制等能力。

3. 核心能力之三：多域一体化监测

运行安全管理平台以业务为视角，提供本地和异地灾资产的一体化监测能力。通过灾备统一监控页面，可快速获取多域容灾资产的运行健康状态和灾备可用性指标信息。

4. 核心能力之四：常态化业务级演练

将业务级演练常态化，检验应急预案的有效性和可操作性，提高组织在面临突发事件时的应急响应能力。通过演练发现预案中存在的问题和不足，及时修订和完善，实现预案自适应性进化。演练包括桌面演练和容灾演练两种场景，常态化高频次的桌面演练，在不影响生产库的前提下，提供了灾备库可用性的验证机制；计划内或满足上级监管部门考核的容灾演练，在保证数据零丢失前提下，验证灾备可用性，通过模拟容灾切换实战的演练过程。桌面演练和容灾演练为灾难场景下的一键容灾切换提供保障。

桌面演练：不做实际切换，对生产系统无影响，无须回切。通过对灾备系统的读写操作，充分验证灾备系统的可用性。桌面演练为高频演练提供基础，填补因缺乏演练而造成灾备系统可用性无法感知的真空。桌面演练流程如下图4所示：



图4 桌面演练流程示意图

容灾演练：做真实切换，确保数据零丢失，可以一键回切。计划内的容灾演练可有效确定灾备的可用性，为系统切换过程的完善和优化提供依据，保障灾难发生时能快速、有效切换。容灾演练在保证数据零丢失的前提下，完成从生产到容灾中心的一键切换；演练完毕自动生成回切链路，并支持一键切回到原生产系统。容灾演练流程如下图5所示：



图5 容灾演练流程示意图

核心交易系统的运行安全韧性实践中，定期演练对于提高组织的应急响应能力、增强团队协作能力、保障人员和财产安全、降低事故损失、缩短系统MTTD平均故障发现时间和MTTR平均故障修复时间具有重要意义和作用价值。

5. 核心能力之五：一键业务连续性切换

灾难场景下往往生产环境处于无法正常运行状态，需要将容灾端快速拉起对外提供服务，以保障业务连续性。运行安全管理平台针对灾难切换场景，提供一键切换能力，它能够在最短时间内恢复业务系统正常运行，避免因系统故障而造成的客户损失和信誉损害。当生产中心发生灾难时（如主库崩塌、系统宕机、网络中断、断电、病毒攻击等）通过一键切换操作，让容灾中心接管生产服务。一键业务连续性切换以快速拉起业务为第一优先级，最大程度缩短业务停机时间，缩短系统MTTR平均故障修复时间，保障业务连续性。灾难切换如图6所示：



图6 灾难切换流程示意图

6. 核心能力之六：运行安全可视化观测

运行安全管理平台以“业务系统”为视线第一切入点，提供灾备资产的运行监控大屏，以快速感知灾备资产信息、运行状态和RPO指标，并实现对异常信息实现主动告警。灾备运行监控如图7所示：



图7 灾备运行监控大屏

切换跟踪大屏通过对网络空间切换的图形化投射，实时动态展示切换进度、切换节点和切换耗时（RTO），保障整个切换过程清晰可感知。切换跟踪大屏如图8所示：



图8 切换跟踪大屏

切换指挥大屏鸟瞰切换全局、实时关注切换进程，通过切换状态可视性和切换过程的可见性驱动风险的快速干预机制，高效助力应急灾难现场的指挥决策。切换指挥大屏如图9所示：



图9 切换指挥大屏

五、项目收益

核心交易系统运行安全韧性体系实践是集成核心业务系统的智能化解决方案，目前本项目的核心载体运行安全管理平台已完成21个系统的对接。平台采用自动化执行技术，实现了单个系统的切换演练或灾备切换在5分钟内完成，有效节约了人力资源，降低了操作风险，提升了业务系统的RPO、RTO水平，平台已连续运行两年，稳定可靠。

平台通过在线管理和协同能力，构建了运行安全管理平台机制，包括事件库、脚本库、预案库、知识库等模块，同

时实现数据中心级资产灾备健康度监控和切换风险感知功能,当发生业务系统或机房宕机等灾难事故时,平台能够立即启动备份系统,大幅缩减故障持续时间,保障业务的高效运行。

(一) 社会效益:

一是贯彻国家安全战略:该项目是贯彻落实总体国家安全观的重要实践。作为数字安全建设的标杆项目,证券企业的业务安全与国家安全息息相关。基于国家安全法、网络安全法和数据安全法的指导,项目不仅响应了国家安全规划,也为行业提供了安全体系建设的参考,助力构建长期稳定的安全格局。

二是完善企业安全体系:运行安全韧性体系是传统安全体系的战略升级,成为保障证券企业核心业务连续性的关键环节。通过引入该体系,企业在面对多种风险和挑战时具备更强的应对能力,确保业务的可持续性和韧性,为业务稳定运行奠定了坚实的基础。

三是提升合规水准:该体系帮助证券企业达到《证券期货业网络安全管理办法》《证券基金经营机构信息技术管理办法》等法规要求,提升合规能力,降低法律风险。同时,通过确保系统在自然灾害、技术故障等事件中的快速恢复,减少业务中断带来的损失。

四是增强用户信任:运行安全管理平台的部署提升了企业应对突发事件的能力,确保核心业务持续稳定运行,履行对用户的承诺。通过保障业务连续性,增强客户对企业的信任,提升企业在市场中的竞争力。

(二) 经济效益:

一是降低人力成本:运行安全管理平台的应用在不影响证券核心业务的情况下,实现无缝对接,大幅减少了运维人员的工作量,显著降低人力运维成本。平台支持一键切换演练和灾备切换,提升了运维效率与工作质量,减轻了运维人员的压力和疲劳。据估算,系统上线后,每年可为公司节省约600万元的人力成本。

二是减少业务中断损失:在部署运行安全管理平台之前,核心业务系统的灾备切换需10分钟以上,且为手动操作。通过该平台,切换时间缩短至5分钟以内,效率提升超60%,RTO(恢复时间目标)和RPO(恢复点目标)减少60%。这有效缩短了业务中断时间,保障业务连续性,为公司减少经济损失。

六、项目的可推广性

证券是推动资源有效配置、促进经济发展的重要工具,同时有助于降低金融系统风险。核心交易系统运行安全管理平台通过完善的安全防护机制、容错与恢复策略、风险监

控、应急预案及培训演练等措施,为证券数字业务带来了显著成果,提升了交易系统的稳定性、安全性和应急响应能力,并为整个行业的稳定发展树立了示范。

此外,该平台还能服务于泛金融行业,实现数字业务的统一管理和实时风险控制,打造标准化的灾备预案,确保数据和资产安全。面对全球数字化浪潮,平台可应用于国防、医疗、金融等关键基础设施,增强其系统可靠性与抵抗力,降低网络攻击和自然灾害带来的风险。

七、总结与展望

在技术创新与合规要求的双重驱动下,通过运行安全韧性体系的建设,东吴证券显著提升了核心业务的安全性与稳定性。运行安全韧性平台的引入不仅大幅降低了运维成本,还通过极速灾备模式有效减少了业务中断带来的损失,增强了业务的连续性和客户信任感。这一体系在保障合规的同时,助力企业应对复杂多变的数字化风险环境,充分体现了安全韧性体系对企业长远发展的推动作用。

展望未来,随着全球金融市场的不断发展和网络安全威胁的日益复杂化,证券行业对安全与业务韧性的要求将更加严苛。我司将继续深化运行安全韧性体系的应用,推动技术升级与创新,提升应急响应速度和系统可靠性。同时,我们也将以此为基础,探索在证券行业中的广泛应用,为行业数字化转型提供更多的安全保障。

业务安全之 API越权检测工具的探索实践

刘正新、樊添、赵子俊、伊鹏 | 中信建投证券股份有限公司

摘要：在中国证监会指导下，中国证券业协会起草了《证券公司网络和信息安全三年提升计划（2023-2025）》，推进行业网络和信息安全防护能力持续提升。基于此背景，我们希望实现安全漏洞的早发现、早解决。在诸多安全漏洞中，越权漏洞有着发现率高、危害性大等特点^[1]，且针对越权漏洞的检测依然以人工检测为主，存在着效率低、易漏测等问题。因此，本文设计了一种面向业务API的自动化越权检测工具，并在系统测试过程中实践落地，旨在提升渗透测试效率并减少人为漏测，最终推进系统安全防护能力的持续提升。

关键字：安全防护能力、权限提升、自动化越权检测

一、现状分析

在《证券公司网络和信息安全三年提升计划（2023-2025）》的指导下，证券公司对于网络和信息安全意识明显增强。目前，中信建投证券的网络和信息安全防护体系基本健全，从企业级的网络安全防护策略到各种入侵检测系统的持续探测，从白盒代码扫描、交互式应用安全扫描到厂商专业渗透测试等各个层面均做了全方位的部署，牢牢守住不发生系统性网络和信息安全风险底线。

我们发现尽管公司的系统在各个安全环节都采取了安全措施，包括安全需求评审、开发过程中的白盒代码扫描和交互式动态扫描等多个安全检测，但在交给厂商进行渗透测试之前，仍可能存在一些安全漏洞。我们对近一年的渗透测试报告进行了整理，如图1所示，结果发现53%的漏洞与接口权限相关，包括垂直越权、水平越权和未授权访问等，而且这些漏洞的风险评估结果几乎都是高危。这些漏洞不仅可能导致系统高级别数据信息的泄露，还可能引发恶意越权操作，例如普通用户通过操作管理员接口来增删系统的重要信息。因此，本文的目标是最大程度检测出系统存在越权类漏洞。

在检测越权漏洞方面，我们面临着两大挑战。一是，这类漏洞通常要靠手工渗透测试才能被发现，这涉及到人工修改请求并检查重放结果，整个过程效率不高。二是，由于系统接口数量众多，从几十到几百甚至上千个不等，仅凭人工测试很难全面覆盖，这可能导致只找到部分漏洞，甚至完全遗漏，这样一来系统就有可能暴露在权限威胁之下。

综上，对系统进行越权漏洞的自动化检测具有很高的价值。它不仅能减轻手工检测的负担，节省大量时间，还能最大程度地避免因人为因素导致的漏测。另外，自动化检测工具可以将渗透测试提前到功能测试阶段，由普通测试人

员执行，降低了对人员渗透技能的要求，从而提高了人员的工作效率。

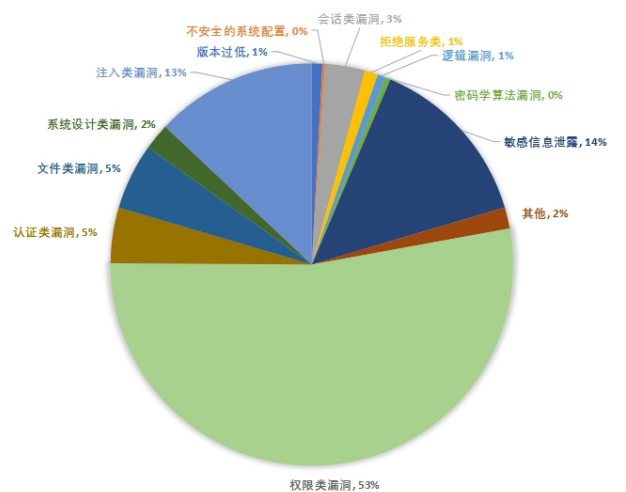


图1 渗透测试漏洞分布

二、自动化越权检测工具的探索实践

（一）自动化越权检测工具的设计

本文的越权检测针对基于角色进行访问控制（Role-Based Access Control, RBAC）的Web应用^[2]。检测场景如图2所示，我们考虑了三种越权情形：（1）垂直越权，也被称为权限提升（Privilege Escalation），指低权限用户向上越权访问高权限接口；（2）水平越权，也被称为不安全的直接对象引用（Insecure Direct Object References），指同级用户间能够通过修改资源ID等标识符来访问到对方的私有数据；（3）未授权访问，指未授权的用户能够直接访问带权限的接口。

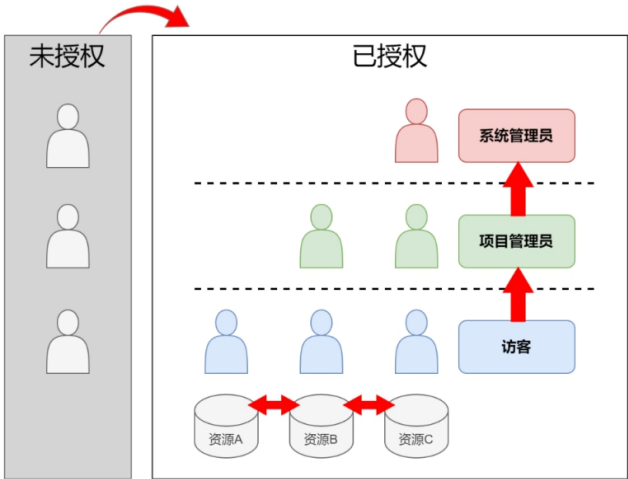


图2 越权场景图

本文设计了面向上述场景的越权检测工具。如图3所示，工具包括四个主要模块：接口收集、接口清洗、越权实施以及越权判定，实现了从原始接口流量记录到越权检测结果的端到端处理。

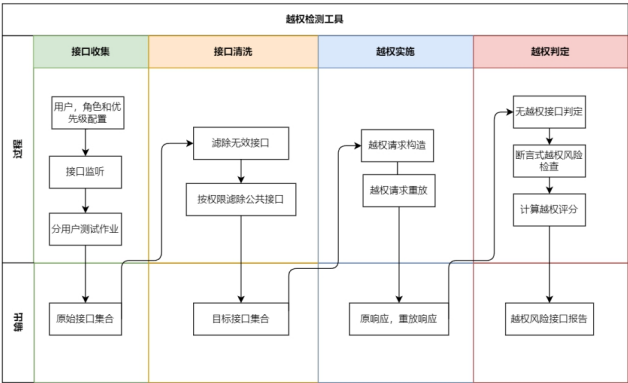


图3 越权工具模块图

1.接口收集

本文讨论的接口专指HTTP接口，将一个接口定义为HTTP请求-响应二元组

$$Pr = \{Q, R\}$$

其中 $Q = \{method, url, header, body\}$, $R = \{code, header', body'\}$, url为统一资源定位符，包含请求的主机、端口、请求路径和参数信息。我们采用代理抓包的收集方式，将接口收集任务与测试工作无缝结合，不会引入额外的时间成本，包括2步：

(1) 测试人员分析系统的RBAC模型，从而建立接口权限索引 $\{U, C, P\}$ ，其中，U为用户名，是收集对象的唯一标识；C代表所属角色，如：系统管理员、项目管理人员、访客等；P是一个正整数，代表角色间的权限优先级，更高的优先级代表拥有更多特权接口，同一优先级下也可以包含不同的角色，他们分工不同但在优先级上并无高低。图4展示了一个典型的项目管理类Web应用的接口收集索引。

(2) 根据接口权限索引抓包得到原始接口集合，针对每个索引 $\{U, C, P\}$ ，测试人员在后台开启代理抓包程序，登录用户账号，开展用户所属角色的测试作业，代理程序会自动抓取所访问接口的请求响应对Pr并记录。对于M个收集目标重复以上过程，该模块的最终输出为 $\{\{U_i, C_i, P_i, X_i\}\}_{i=1}^M$ ，其中， $X_i = \{Pr\}$ 代表原始接口集。

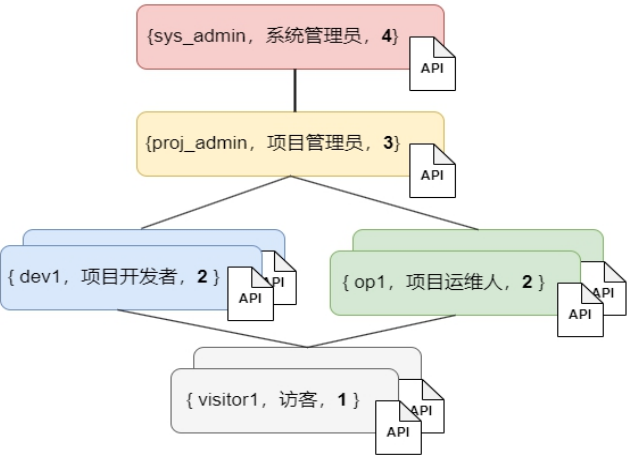


图4 接口收集示意图

2.接口清洗

接口清洗包括两步：无效接口清洗和用户间公共接口清洗。首先，代理捕获的全量原始接口中存在与越权检测无关的接口需要清洗，以使后续检测更加高效准确；随后，不同用户间的公共接口也需要清洗，以避免误报。

(1) 无效接口清洗

对于原始接口集X'，参考表1所述的过滤规则，过滤掉非目标、响应错误、静态样式请求等无效接口，将过滤结果记为X_i'。需要解释两点：1) 在清洗前，测试人员需明确Web系统所采用的授权技术，比如会话、JWT (JSON Web Token)、OAuth2等，将授权字段值（如Cookie、Authorization、sessionId等）和所处位置(url、头部、请求体)写入工具配置，从而滤除权限外接口；2) 在重复接口滤除中，考虑到不同的Web接口实现风格会将资源类型、id等区分不同接口的关键参数置于请求的不同位置，所以采用{method,url,body}为去重键。

表1 单接口过滤规则表

过滤点	过滤方法
非检测目标	根据url的host+port字段，滤除非目标系统接口
权限外接口	按照所配置的系统授权字段，滤除不包含授权字段的接口
请求方法	滤除与用户私有资源无关的 TRACE、HEAD、OPTIONS 和 CONNECT 接口
响应类型	滤除响应为 3XX 的重定向接口 滤除响应为 4XX 的客户端错误接口 滤除响应为 5XX 的服务器错误接口
样式文件	滤除 Web 样式文件，包括 js、css、html、htm 滤除图像和图标文件，包括 jpg、png、gif、ico 滤除字体文件，包括 svg、woff、ttf、eot
重复接口	以{method,url,body}为键，滤除已记录的重复接口

(2) 公共接口清洗

回顾图2所示的RBAC越权场景,越权发生在两个不同的用户 U_i 和 U_j 之间,或未授权用户访问权限内接口。一般情况下, U_i 和 U_j 的接口集存在交集,称这部分接口为二者的公共接口,比如:获取界面中可操作的模块列表、获取系统版本等。这些接口本身不涉及越权所以很难被判定模块正确处理,需要提前清洗掉。

表2具体说明了需要清洗的三种类型,其中,去重键用于计算两个接口集的交集,在垂直场景下,因为角色不同所以公共接口的响应可能也存在差异,所以使用{method,url,body}作为去重键;而在水平场景下,由于同一角色的可访问接口一致,所以将公共接口进一步限制为响应码code和响应体body'也一致。

表2 公共接口过滤规则表

越权类型	去重键	过滤结果集Z	作用
$P_j > P_i$	{method, url,body}	$Z_{i \rightarrow j} = X'_i / (X'_i \cap X'_j)$	低优先级到高优先级的垂直越权,保留高权限用户的特权接口
$P_j = P_i$ 且 $R_j \neq R_i$		$Z_{i \rightarrow j} = X'_i / (X'_i \cap X'_j), Z_{j \rightarrow i} = X'_j / (X'_j \cap X'_i)$	同一优先级间不同角色相互垂直越权,保留各自特权接口
$P_j = P_i$ 且 $R_j = R_i$	{method, url,body, code,body'}	$Z_{i \rightarrow j} = \max_{ Z } (Z_i, Z_j)$, 其中, $Z_i = X'_i / (X'_i \cap X'_j), Z_j = X'_j / (X'_j \cap X'_i)$	水平越权,保留去重后记录最完整的接口

上述过程可以总结为:对于用户 U_i 到 U_j 的越权,通过无效接口清洗可得到 X'_i 和 X'_j ;随后,根据接口权限索引{u,c,p}确定越权类型,从而清洗掉二者间的公共接口,并将最终的清洗结果集记为 $Z_{i \rightarrow j}$ 。

3. 越权实施

越权实施模块模拟了从用户 U_i 到 U_j 的越权过程,也即模拟攻击者掌握用户的登录信息,并希望越权访问用户 U_j 的接口。通过收集和清洗,我们已经确定了实施越权的目标集 $Z_{i \rightarrow j} = \{(Q, R)\}$ 。现在需要将原请求Q中的授权字段进行修改以模拟来自攻击者的越权请求 $\hat{Q}$,采用以下两种修改方式:

■对于垂直(水平)越权,采用低权限(平级A)请求的凭证信息替换高权限(平级B),具体而言,根据授权配置信息,取一批请求中最完整的授权字段作为 U_i 的凭证,用其替换 $Z_{i \rightarrow j}$ 中每个请求的授权字段,从而获得越权请求;

■对于未授权访问,因为没有任何凭证产生,删除 $Z_{i \rightarrow j}$ 中请求的授权字段即可。

随后,重放越权请求 $\hat{Q}$ 并接收响应,作为后续检测依据。本模块输出响应对 $(R, \hat{R})$,其中,R为的 U_j 接口的原响应, $\hat{R}$ 为修改授权字段并重放后得到的响应。

4. 越权判定

越权判定是本工具的核心模块。判定的出发点是尽可

能减少漏报,首先,剔除确定不存在越权的接口;其次,对于剩余接口,工具搜集接口响应中越权相关的证据,并为每个接口估算一个风险评分,根据风险评分做出越权判定结论。

(1) 不存在越权的接口

工具将以下两种接口判定为不存在越权:a.返回权限拒绝响应码的,包括代表缺少凭证的401和无权限的403;b.响应可解析为JSON或XML对象,且消息字段传达了明确的“未授权”语义,工具采用关键词和正则匹配来识别这一语义(见表3)。对于上述两种情况,我们假设服务器在处理这些请求时已经施加了正确的访问控制。

表3 越权关键词以及正则匹配模式表

类型	关键词	正则匹配模式
未授权	无权、未授权、需要登录、非法、unauth、forbidden、login required、illegal	“(无 未 没有).?*权?.*”、“(no un).*(perm right auth verif).*”、“(reject deny denied refuse).*”
成功	成功、完成、生效、success、ok、ready、complete、finish	-

(2) 可能存在越权的接口

对于可能存在越权的情况,设计了基于可扩展的断言式风险检查来辅助测试人员判断。针对响应对 $(R, \hat{R})$,每个检查项 F_i 为对 $(R, \hat{R})$ 的一条断言

$$F_i(R, \hat{R}) \rightarrow \{0, 1\},$$

此外,赋予每个检查项一个有效位 $b_i \in \{0, 1\}$ 和一个0到1间的风险系数 w_i , b_i 表示检查对当前响应是否生效,比如:JSON关键字检查需要返回有效的JSON响应体; w_i 表示断言为真时发生越权的可能性,比如:当越权请求返回正常响应码时,只认为存在较小的越权可能,因为响应码不会包含任何业务信息,故赋予其较小的系数。工具会执行所配置的N条检查项,并计算越权评分为

$$S = 100 \cdot \frac{\sum_i^N w_i \cdot b_i \cdot F_i(R, \hat{R})}{\sum_i^N w_i \cdot b_i},$$

该评分取值范围为[0,100],取值越大,代表发生越权的可能越大。

表4罗列了工具默认配置的一些断言检查项,目前包括4个类别:

■响应码:通过是否返回20X成功响应码判断是否发生越权,但是大部分业务系统即便成功阻拦了越权请求,也不会选择直接返回403,而是正常响应,以便在响应体中附加详细的错误信息,故响应码只能作为一种基本检查。

■文件类型:如果越权请求能够获取有效的音频、视频等资源文件,那么大概率产生了漏洞。

■关键词:若响应为文本类型,检查其是否包含某子字符串或符合某种正则匹配。因为在主流的前后端分离式Web系统中,后端会返回格式化响应(JSON、XML对象),对象中包含系统的自定义响应码、消息、数据等,而消息字段往往用于描述所请求业务的处理情况,能够作为是否越权

成功的佐证。工具内置了常见的表示“成功”语义的关键词（见表3）。此外，测试人员可根据系统的实际情况来补充字典或添加正则匹配模式以提升准确率。

■度量：通过计算响应体的一些数学指标来判断越权。一种重要的度量方式为R和 $\hat{R}$ 间的相似度，显然当二者非常相似时说明攻击者大概率访问到了未授权的内容，相似度计算为

$$Sim = \frac{l_{max} - D_{lvt}(R, \hat{R})}{l_{max}}$$

其中， $L_{max} = \max(|R|, |\hat{R}|)$ ， D_{lvt} 代表编辑距离^[3]，采用该距离的原因是我们只关心字符上的差距而不关心任何语义信息。若Sim大于阈值 Δ ，则断言检查为真，并将风险系数置为Sim，实验中 Δ 取0.75。

表4 越权检查项表

检查类	检查项F	风险系数w
响应码	正常响应码	0.1
文件类型	有效 image 资源	0.8
	有效 audio 资源	
	有效 video 资源	
关键词	Body.text 包含	0.5
	Body.text 正则匹配	
	Body.JSON 包含	0.8
	Body.JSON 正则匹配	
	Body.XML 包含	0.8
	Body.XML 正则匹配	
度量	Body 相似	Sim

对于接口的检测结果，我们引入了判定阈值 $\tilde{\Delta}$ ，并将风险评分 $S > \Delta$ 的接口判定为“存在越权”，将 $0 < S < \tilde{\Delta}$ 接口判定为“疑似越权”。最终，工具对每个可能存在越权的接口输出 $\{(C_i, C_j), (R, \hat{R}), \{F_{true}\}, S, T\}$ ，包括越权角色信息、原响应和重放响应对、断言为真的检查项、越权评分以及判定结果，并按评分降序排列。对于“疑似越权”的接口，测试人员可以参考工具提供的风险检查项，并分析前后响应，从而生成最终的越权漏洞检测报告。结合对当前实验结果的人工分析，工具目前将 $\tilde{\Delta}$ 取为85，在未来，我们会将工具落地实践于更多的实际应用场景，以便收集更全面的样本数据，从而实现更精确的阈值选取。

(二) 越权检测工具的实现效果

上述越权检测工具已经对五个系统尝试做检测，目前，三个系统发现越权漏洞，且均为高危级别。如图5所示，为其中一个系统的越权检测结果。

图5 越权检测结果输出

为了验证工具检测的效果，我们和人工检测进行了简单对比。首先，安排这五个系统按照传统的手工执行来检测越权，测试人员反馈系统平均耗时约为14小时（将近2人天），共检测出24个越权接口；然后，采用越权检测工具进行检测，平均耗时0.2小时（因接口收集在功能测试中完成，故不计入安全检测时间），共计扫描出468个有效接口，检测出72个越权接口（经人工分析，有6个越权接口属于误报），大大提升越权检测效率。人工和自动化检测的对比结果如表5所示。

表5 工具检测和人工检测的效果对比

检测方式	耗时	接口数	检出率	漏报率	假阳率（误检率）
人工	14h	468	5.1%	63.6%	0
自动化	0.2h	468	15.4%	≈ 0%	8%

分析上表，自动化检测的优势总结为三方面：（1）检测耗时显著降低，效率提升了60倍以上；（2）漏测的越权接口几乎不存在，因为工具可以将系统所有接口捕获到，并逐个进行越权检测；（3）降低对人员的渗透技能要求，变相提升人员能效。

同时我们也发现了当前工具的不足，主要是存在少量的假阳接口（误报为越权的接口），需要持续优化越权判定模块的检测逻辑。

三、总结和展望

由于人力和时间等多方面限制,以往的手工越权检测无法覆盖所有接口做逐个越权检测,易存在漏网之鱼。相比之下,本文研究实现的自动化越权检测工具具有省时、省人、命中率高的特点,几乎能够杜绝漏报,将权限类漏洞尽可能消除在测试阶段。

随后,我们会继续研究其它漏洞的自动化检测工具,包括但不限于注入类漏洞、文件类漏洞、认证类漏洞等几大类典型漏洞场景的检测,努力在安全测试中高效且无遗漏地发现漏洞。最终,要在研发测试生命周期中嵌入完整的软件安全开发周期(Security Development Lifecycle,SDL)^[4],形成从安全需求到安全测试的闭环,保证安全需求真正在每个系统中落地实施,将《证券公司网络和信息安全三年提升计划(2023-2025)》中的“信息系统安全”建设落实到位。

参考文献

- [1] Brian Glas et al., OWASP TOP-10 2021[J].OWASP Foundation, 2021.
- [2] 邵森.计算机访问控制技术研究综述[J].中国新技术新产品,2009(02):31.
- [3] 张胜楠.基于编辑距离的字符串相似度算法研究[J].现代计算机,2023,29(14):23-26+32.
- [4] 姜城.商业银行软件安全开发生命周期思考与实践[J].中国金融电脑,2019,(04):68-70.

“口令+‘三方协同鉴别’”

——一种满足第三/四级等保要求、适用证券业务的，限定条件的强身份认证方法

王恩潭、张永启、董延敏、张佳佳、黄强生、马原、张秀敏、李广猛、赵存利 | 中泰证券股份有限公司

摘要：为更好满足国家标准、行业监管要求，更好保障网上证券安全、赋能业务高质量发展，中泰证券探讨提出“三方协同鉴别”技术，并基于此构造了适用证券业务的“口令+‘三方协同鉴别’”强认证方法。这是一种限定条件的投资者身份鉴别方法，通过融合券商、银行、运营商三方资源来实现，需要投资者三方存管绑定Ⅰ类银行账户，同时在券商、银行预留和使用同样的手机号码。该身份认证方法能够全面覆盖手机、PC、Pad等各种SIM卡和非SIM卡终端以及多SIM卡应用情形，普遍适用于三方存管框架下各类网上证券业务场景。本文介绍了“口令+‘三方协同鉴别’”，期待业内外专家关注、评判，共同推进这一电子认证技术早日落地应用，将其打造成为券商数字化转型和网上证券高质量发展的得力工具。

关键字：电子认证、三方协同鉴别、SIM卡、Ⅰ类银行账户、数字铅封、数字证书、网关取号

券商以非现场业务为主，绝大部分种类业务和客户服务均在网开展、线上提供，电子认证是保障网上证券安全稳定运营的关键技术；而实施双因素或多因素强身份认证，则是网络安全等级保护、行业监管和相关技术标准对网上证券用户身份鉴别的一项具体要求。同时，近年券商落实监管要求和《信息安全技术 信息系统密码应用基本要求》，在证券业务中大量使用数字证书，由于缺失适用的强认证技术，致使证书发放严谨性与客户体验之间的矛盾突显。

为更好满足国家标准、行业监管要求，更好保障网上证券安全、赋能业务高质量发展，中泰证券探讨提出“三方协同鉴别”技术，并基于此构造了适用证券业务的“口令+‘三方协同鉴别’”强认证方法。

一、融合券商、银行、运营商资源的“三方协同鉴别”

近年来，运营商推出通讯网关取号技术，已在部分券商中应用、积累了一定使用经验；另一方面，人民银行自2015年开始推行个人银行账户分类管理，并对Ⅰ类账户实施最为严格的金融级实名管理。基于此，结合行业客户资金第三方存管制度，笔者提出一种面向用户的融合券商、银行、运营商三方资源的协同鉴别方法。

（一）可以利用的政策和优质客观条件

1. 证券行业客户交易结算资金第三方存管制度

证券行业客户交易结算资金第三方存管制度，是指客户交易结算资金由券商和投资者以外的第三方——指定的商业银行——负责存管，从而形成“券商管证券、银行管资金”的一种业务模式和行业规制。2001年，“证监会令【第3

号】”发布《客户交易结算资金管理办法》，自2002年1月1日起施行。2007年，“证监信息字〔2007〕10号”发布《证券公司客户交易结算资金商业银行第三方存管技术指引》，其中：第二条规定“本指引所指的第三方存管，是指证券公司将客户交易结算资金存放在指定的商业银行，并以每个客户名义单独立户管理，商业银行负责资金存取，发挥第三方监督作用，以保障客户资金安全为目的的资金存管模式。本指引所指第三方存管系统，是指支撑第三方存管业务运行的网络与信息系统。”第三条规定“本指引适用于第三方存管业务的各参与方，具体包括：参与第三方存管业务的证券公司、商业银行、以及提供数据交换服务的机构。”

2. Ⅰ类银行账户最为严格的金融级实名管理

为进一步落实银行账户实名制并提供安全高效的差异化服务，人民银行自2015年开始推行个人银行账户分类管理，其中Ⅰ类银行账户的实名管理最为严格，此类账户的开立及重要信息变更均要求现场办理。例如《中国人民银行关于改进个人银行账户服务 加强账户管理的通知》规定“通过柜面受理银行账户开户申请的，银行可为开户申请人开立Ⅰ类户……”；“通过远程视频柜员机和智能柜员机等自助机具受理银行账户开户申请，银行工作人员现场核验开户申请人身份信息的，银行可为其开立Ⅰ类户……”。例如《中国工商银行个人银行结算账户管理协议（2022年版）》约定“甲方可以通过柜面、智能设备办理Ⅰ类户或者通过柜面、电子渠道办理Ⅱ、Ⅲ类账户客户信息及账户信息的变更。通过柜面或智能设备可办理Ⅰ类户的姓名、居民身份证号码、手机号码、绑定账户变更业务；……”；“甲方承诺在乙方留存的联系电话号码应与个人身份证件号码一一对应。如甲方无法

证明.....或者.....,甲方同意乙方对相关银行账户中止办理业务。甲方可到乙方营业网点核实身份后对账户恢复功能。”

3. 开放SIM卡验证结果的运营商通讯网关取号技术

SIM卡泛指各类电信运营商“用户身份识别卡”，包括SIM、Micro SIM、Nano SIM、UIM、Micro UIM、Nano UIM、USIM等。SIM卡是手机入网正常使用的连接器与合法凭证，运营商的SIM卡验证基于卡硬件、采用密码技术，SIM卡验证结果可以用于网络生态大环境的诸多场景。近年来，运营商推出的通讯网关取号技术，可用以获取正常入网使用手机的号码，当下包括券商在内的一些行业和领域已有部分应用。此项技术属于运营商专有技术，相当于向合法用户开放了SIM卡验证结果。因为只有SIM卡验证通过、手机正常入网，方能获取手机号码，所以在获取手机号码的同时，也就获得了SIM卡验证通过的信息。运营商通讯网关取号技术流程示意图如下：

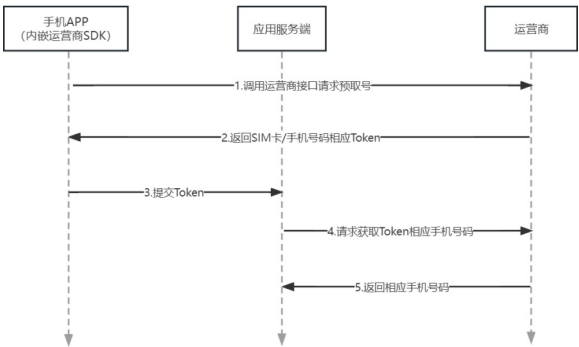


图1 运营商通讯网关取号技术流程示意图

(二)“三方协同鉴别”概述

1. 限定条件的“三方协同鉴别”

笔者充分利用上述监管政策和优质客观条件，通过融合运营商、银行、券商自身三方资源提出一种身份认证方法，称之为“三方协同鉴别”，用以提升券商对网上证券用户的身份鉴别能力，包括鉴别强度和鉴别效率。

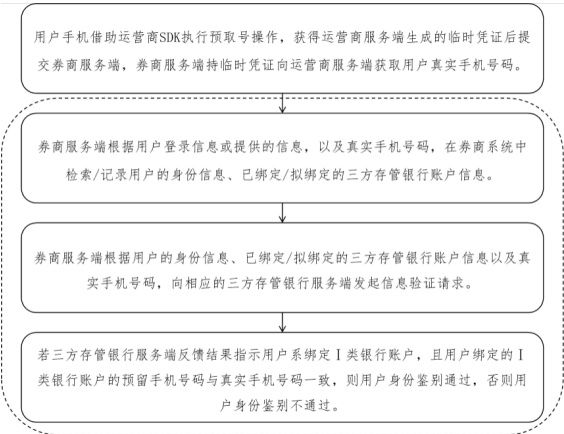


图2 “三方协同鉴别”逻辑框架示意图

由图2可见，“三方协同鉴别”可分为两大步骤：第一步，利用运营商通讯网关取号技术获取网上证券参与人使用的真实手机号码；第二步，利用 I 类银行账户最为严格的金融级实名管理、借助投资者预留手机号码实现认证到网上证券参与人的强鉴别。这是一种限定条件的鉴别方法，需要投资者三方存管绑定 I 类银行账户，同时在券商、银行预留和使用同样的手机号码。

2. “三方协同鉴别”的基本流程

STEP1:用户通过券商手机APP发起业务诉求，如资金账号登录、账户开立等。

STEP2:券商手机APP提取手机网络特征信息、识别运营商；调用相应的运营商SDK，向相应运营商服务端发起预取号请求。

STEP3:运营商服务端响应预取号请求，反馈临时凭证。

STEP4:券商手机APP携带临时凭证向券商服务端请求业务功能。

STEP5:券商服务端收到临时凭证后，携带临时凭证向运营商服务端请求获取真实手机号码。

STEP6:运营商服务端校验临时凭证，若校验成功则返回真实手机号码信息；若校验失败，则向券商服务端推送相应提示信息。

STEP7:券商服务端接收到真实手机号码信息后，根据用户的登录信息，或提供的身份信息、银行卡信息等或其中部分信息，以及真实手机号码，在券商系统中检索、梳理用户信息，记录相关信息。

STEP8:券商服务端携带相关信息以及验证请求向三方存管银行服务端发起验证；相关信息包括用户身份证件号码、银行卡号码等或其中部分信息，以及真实手机号码。

STEP9:三方存管银行服务端比对用户身份证件号码、银行卡号码、预留手机号码，并查验用户相应银行账户是否为 I 类银行账户，并反馈结果。

STEP10:券商服务端获取三方存管银行反馈结果，若用户相应银行账户为 I 类账户且手机号码比对一致，则视为鉴别成功、响应业务功能；否则视为鉴别失败、向用户推送相应提示信息。

3. “三方协同鉴别”解决的问题

■该项技术在借助运营商资源有效鉴别SIM卡（终端设备）的基础上，借助银行资源进一步鉴别到用户本人，提升了鉴别强度。

■使用该项技术可以得到明确的“是”或“否”的鉴别结果，避免了指纹/人脸等生物特征信息识别技术只能以相似度、符合度、匹配概率等百分比形式给出鉴别结果的不足。

■基本鉴别过程透明/无感，将手机短信验证、生物特征信息验证等秒级至分钟级的鉴别耗时，改进至几十毫秒

的网络和系统响应级鉴别耗时。

■参照公安部第三研究所《eID数字身份体系白皮书(2018)》，该项技术借助银行对Ⅰ类账户最为严格的金融级实名管理，通过落实银证双方共同客户的“人证合一认证要求”“到场要求”“颁发记录留存要求”等，将用户数字身份凭证(对应系统中的用户ID)颁发等级从CIL2有效提升至CIL4(顶级)。

■该项技术的广泛应用将有助于落实投资者账户实名制。

(三) 完全解决方案的几方面考量和设计

1. “非SIM卡终端”的跨平台“三方协同鉴别”

首先，“非SIM卡终端”与用户预留号码手机通过软连接(扫描二维码方式连接，或者手机端接收Token后手工输入“非SIM卡终端”等非物理线路连接方式)或硬连接(通过手机多用途充电线USB接口等连接)方式为“三方协同鉴别”跨平台应用建立关联关系；必要时，由券商系统根据业务场景触发或者由用户根据需要主动发起，面向用户执行基于其预留手机号码的“三方协同鉴别”；若“三方协同鉴别”成功，则借助上述建立的关联关系在限定时间内向“非SIM卡终端”开放相应权限。

(1) 二维码(软)连接、Token(软)连接、USB接口(硬)连接的详细步骤。(略)

(2) 其他连接方式

客户端的预留号码手机与“非SIM卡终端”连接方式若满足以下两方面要求，均可作为有效连接方式纳入使用选择范围——

一是预留号码手机与“非SIM卡终端”之间的连接需要有用户的参与并通过其人工操作来实现，以证明用户可以同时近距离控制两个终端(例如NFC近场通信等亦属此类)；

二是预留号码手机与“非SIM卡终端”的连接应该具备抵抗该连接及相关信息被劫持、盗用的特征与防范措施(相反，基于“硬连接”以及基于蓝牙、红外等网络互联互通技术的“文件交互方式”，虽然也可以实现预留号码手机与“非SIM卡终端”之间的信息交互，但是存在交互文件以及非“硬连接”被盗用、劫持的风险，则不属此类)。

2. 多SIM卡应用场景的“三方协同鉴别”

用户使用多张SIM卡的情形，包括使用双卡/多卡手机和使用Pad等其他非手机SIM卡终端的场景。解决方案如下：

(1) 用户使用双卡/多卡手机的场景

STEP1: 用户使用手机APP登录券商系统自动执行“三方协同鉴别”基本流程”。

STEP2: 若“三方协同鉴别”未成功通过，则执行相应日间处理，包括向用户提示有关信息(比如“如果您的手机配

置了两张或两张以上SIM卡，为了提高安全性和享受更多操作便利请选择使用您的预留号码SIM卡”)。

STEP3: 若用户未响应上述提示，则利用现行鉴别技术继续后续业务流程；若用户响应上述提示，则自行切换SIM卡后根据系统提示进行操作或者退出APP重新登录系统。

(2) 用户使用Pad等其他非手机SIM卡终端的场景

若用户使用相应设备的定制版客户端软件，则采取与PC等“非SIM卡终端”一致的应用策略(此类客户端软件无用户登录自动执行“三方协同鉴别”基本流程”设计；跨设备“三方协同鉴别”方法与“非SIM卡终端”的跨平台操作一致)。

若用户使用通用手机APP等客户端软件，则该软件允许用户在初始安装时选择或者安装后配置为“本终端设备不执行本地‘三方协同鉴别’模式”，并在日常业务中采用与“非SIM卡终端”跨平台操作一致的方式实施跨设备“三方协同鉴别”。

3. 技术应用管理方面需要考虑的问题

一方面，对于限定条件的电子认证，满足预期条件是必要前提，而这需要投资者知悉与配合。另一方面，日常业务中若发现问题，系统应自动推送消息至有关当事人，提示及时处理；同时亦应建立与银行的日终和定期核对机制，确保发现异常及时处理。

(1) 公告、与投资者进行约定

主要包括：将投资者的三方存管账户绑定至Ⅰ类银行账户；投资者在券商系统中预留和使用的手机号码应与其在三方存管银行预留的相应Ⅰ类银行账户的手机号码相同；当投资者更换手机号码时，应在三方存管银行和券商系统进行同步更换。

(2) 日间、日终、定期业务处理

有关日间业务流程和日终、期终业务流程如图3、图4所示。

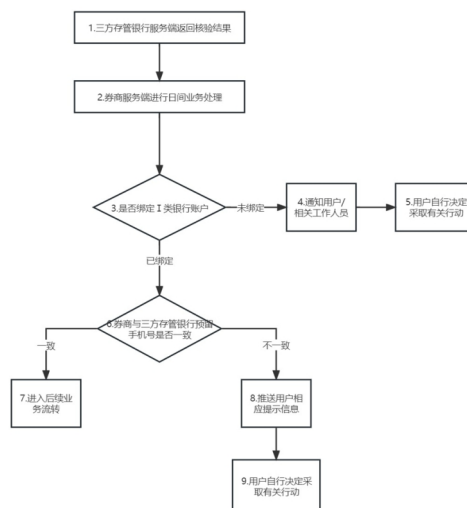


图3 日间业务流程示意图

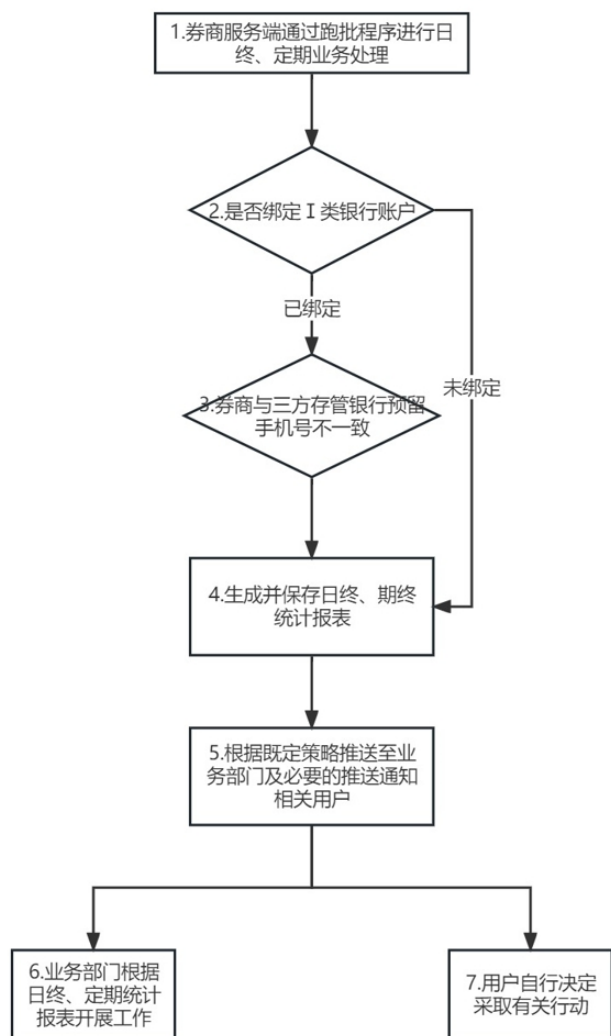


图4 日终、期终业务流程示意图

二、“口令+‘三方协同鉴别’”强身份认证方法

如上所述，“三方协同鉴别”借助银行对Ⅰ类账户最为严格的金融级实名管理和运营商精确到设备的SIM卡验证，利用设备/SIM卡与投资者的紧绑定关系，达成了对网上证券参与者本人的鉴别；接下来，我们结合证券业务中最常使用的“口令”，探讨一种“What you know + What you have”的强身份认证方法。

（一）构造适用证券业务的强认证方法

1. “三方协同鉴别”认证强度尚需进一步提升

正如全国信息安全标准化技术委员会鉴别与授权工作组《电子认证2.0白皮书（2018版）》在3.4“单一鉴别技术面临不断发展的安全威胁”中所述：“事实上，一种鉴别技术从设计理念到具体实施，处处都可能面临着攻击技术进步的威胁和风险。无论何种单一的鉴别技术，都不能确保绝对的安全。”“三方协同鉴别”基于硬件SIM卡/预留手机号码，属于单因素鉴别技术，其认证强度和可靠性仍不够高、尚需进

一步提升。

2. 双因素鉴别认证因子的符合性评估与取舍

一方面，根据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）及《证券期货业网络安全等级保护基本要求》（JR/T 0060-2021）对第三级、第四级系统的要求，“应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现”。运营商SIM卡验证采用安全可靠的密码技术，“三方协同鉴别”通过通讯网关取号技术获取手机号码、利用SIM卡验证结果，符合使用密码技术的要求。另一方面，生物技术较之口令或其他技术，普遍存在生物特征信息保护难、易泄露的问题，信息盗用等风险不容忽视。例如，2023年8、9月间，国家网信办就《人脸识别技术应用安全管理规定（试行）（征求意见稿）》向社会公开征求意见，其中第四条规定：“只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，方可使用人脸识别技术处理人脸信息。实现相同目的或者达到同等业务要求，存在其他非生物特征识别技术方案的，应当优先选择非生物特征识别技术方案。”

3. 适用证券业务的“口令+‘三方协同鉴别’”

鉴于“三方协同鉴别”认证强度需要进一步提升，结合上述对双因素鉴别认证因子的选择分析，以及《证券公司网上证券信息系统技术指引》第二十九条相关规定，即“对于提供证券交易、第三方支付、敏感数据修改等服务功能的网上证券信息系统，除输入账户名、口令、图形验证码外，还应当向客户提供一种或一种以上强度更高的身份认证方式……”，笔者提出一种满足网上证券技术标准要求、符合客户操作习惯的“口令+‘三方协同鉴别’”强身份认证方法。参照公安部第三研究所《eID数字身份体系白皮书（2018）》“8.3. eID数字身份凭证认证等级3（AAL3）”的定义和规定，“口令+三方协同鉴别”具备AAL3（顶级）认证的两大属性特征：一是运营商端的SIM卡验证符合“基于拥有密码协议的密钥”、“基于硬件的、不可复制的”密码认证器的特征，并满足“经过认可的密码技术”的“必需的条件”；二是认证器符合“8.3.1.AAL3允许的认证器类型”（共6种）中的第2种，即“与口令一起使用的单因子密码设备”。

（二）关于“口令”管理的说明

1. 初始“口令”的设置及生效条件

投资者在“网上开户”时设置其账户初始口令，需要验证正身、由开户人亲自设置。若券商在开户过程中已采取有效措施核实投资者身份，则允许口令即时生效；但若开户过程中券商未能采取有效措施核验投资者身份，则不允许口令即时生效、须待进一步核实账户主体身份。例如，在“网上开户”过程中，首先通过“三方协同鉴别”初步识别投资者身

份后开立账户、预置口令；继而在新账户激活环节利用“三方协同鉴别+银证转账”或“三方协同鉴别+其他口令”进一步核实投资者身份后，为投资者开通账户操作权限，此时口令方正式生效。此处，新账户激活亦基于“口令+‘三方协同鉴别’”的思路，其中“口令”借用了开户人Ⅰ类银行账户的口令或其在券商系统设置过的其他可以利用的有效口令。详见笔者相关论文《浅谈网上证券“安可”开户模式——完善技术措施，进一步落实开户人身份核验、无纸化签约2个关键环节》。

2. “口令”的日常管理

投资者账户口令设置成功、生效后，在日常使用过程中主要涉及两方面管理：一是口令更新；二是口令重置。投资者定期/不定期更新口令，可以随时通过“口令+‘三方协同鉴别’”等符合要求的强认证方式证明身份后直接操作实施。而口令重置即投资者因为各种原因忘记口令、需要重新设置的情形，这是一项常规而又特殊的日常业务，其特殊性即需要在缺失口令的情况下证明/验证投资者身份。我们可以采用与初始口令设置同样的逻辑和方法，如上所述，首先通过“三方协同鉴别”初步核验投资者身份，继而借助其Ⅰ类银行账户的口令或其在券商系统中设置过的其他有效口令进一步核实身份，仍然基于同样的“口令+‘三方协同鉴别’”的思路和强认证允许其重置口令。

3. 关于所涉Ⅰ类银行账户的说明

如前所述，在“三方协同鉴别”过程中使用Ⅰ类银行账户时，我们采用了投资者已绑定/拟绑定的三方存管Ⅰ类银行账户，这主要是考虑到在三方存管制度框架下开展协作便于责任落实和保护投资者利益。例如，“三方协同鉴别”过程涉及投资者手机号码的自动获取、信息交互、比对校验等，采用三方存管银行的Ⅰ类账户能更好实现券商和银行对其共同客户的个人信息保护、更好提供及时的贴身服务。而当投资者激活新账户或者遗忘口令后重置需要借用银行端口口令时，为了让客户有更多选择、确保激活和重置功能的有效性，则无需要求相应账户一定是投资者已绑定/拟绑定三方存管的Ⅰ类银行账户，允许投资者自主选择同一主体的任意Ⅰ类银行账户即可。

（三）“口令+‘三方协同鉴别’”应用于证券业务

1. “口令+‘三方协同鉴别’”的一般形式

“口令+‘三方协同鉴别’”是一种可以满足三方存管框架下各类网上证券业务，包括各类重要网上证券业务用户身份鉴别要求的强身份认证方法，如图5所示，具体步骤如下：

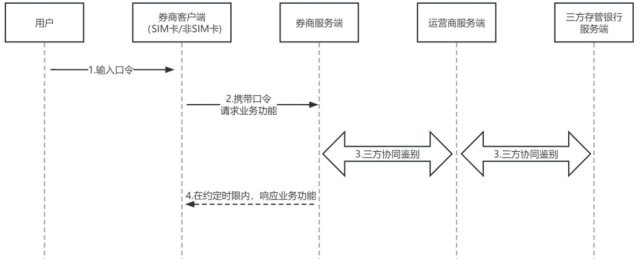


图5 “口令+三方协同鉴别”认证逻辑示意图

STEP1:用户向券商客户端（包括SIM卡终端、非SIM卡终端）输入口令，发起业务诉求。

STEP2:券商客户端携带口令向券商服务端请求业务功能，同时请求执行“三方协同鉴别”。

STEP3:券商服务端将接收到的口令与预设口令进行对比验证；同时，券商服务端发起，面向用户执行基于其预留手机号码的“三方协同鉴别”。

STEP4:若口令和“三方协同鉴别”均能验证通过，则券商服务端根据应用需要、在一定时限内，向用户开放与其业务诉求相应的任何权限。

2. 有助于提高业务规范性、安全性和券商客户服务能力

“口令+‘三方协同鉴别’”应用于现有网上证券业务客户强身份认证，能助其更加安全合规开展；“口令+‘三方协同鉴别’”进一步广泛运用则有助于推动线下业务线上化，为业务开展提供便利、有效改善客户体验。“口令+‘三方协同鉴别’”为券商向客户提供更多精准、及时的贴身服务准备好了技术条件，有助于提升券商服务客户的能力和服务水平。

现以向客户颁发“安可数字证书”为例说明如下：

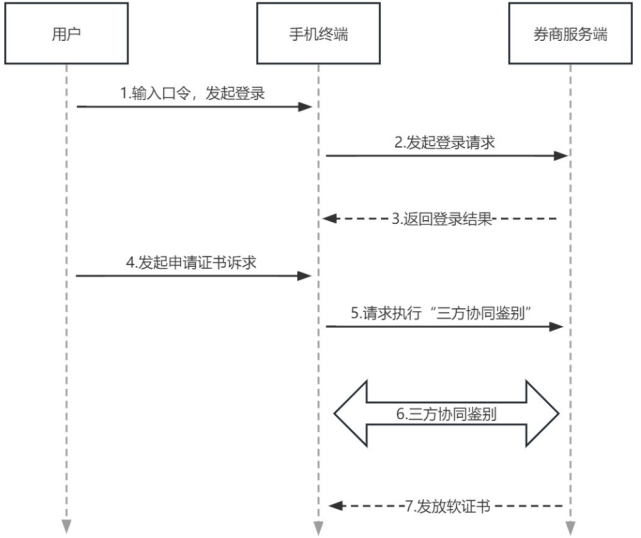


图6 预留号码手机申领软证书逻辑示意图

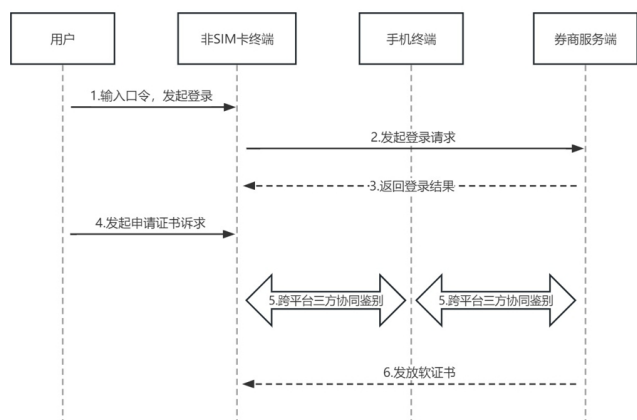


图7 非SIM卡终端申领软证书逻辑示意图

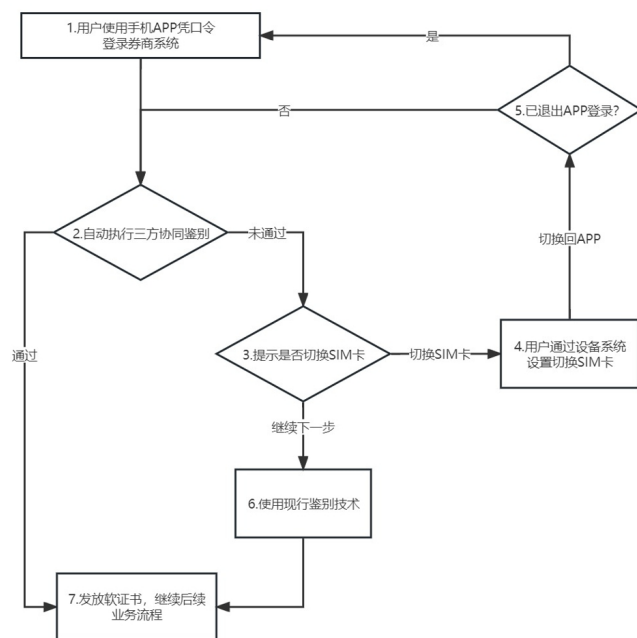


图8 多SIM卡手机申领软证书逻辑示意图

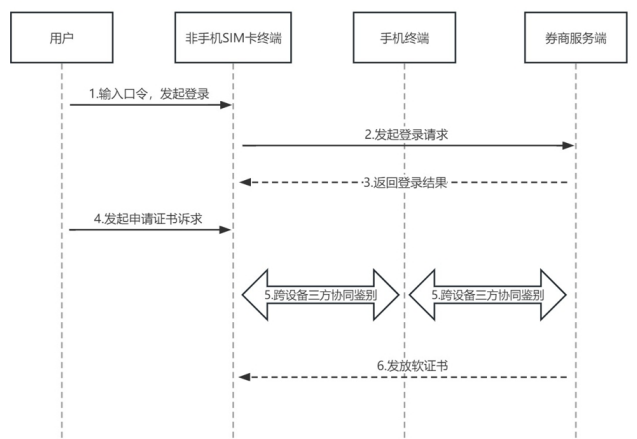


图9 非手机SIM卡终端申领软证书逻辑示意图

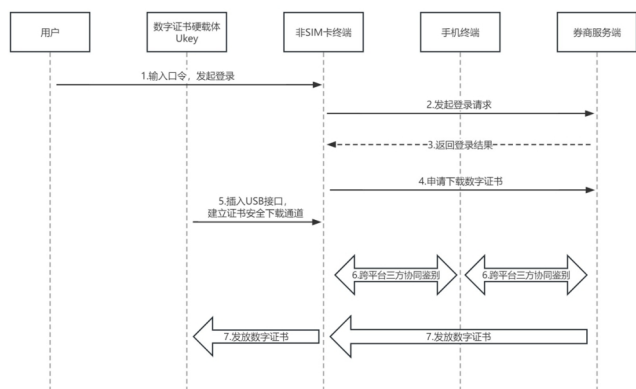


图10 硬证书远程下载辅助加强用户身份验证逻辑示意图

上述利用“口令+‘三方协同鉴别’”验明正身后颁发数字证书的方法(包括预留号码手机、非SIM卡终端、多SIM卡应用场景申领软证书的方法;以及在申领硬证书远程下载时加强用户身份验证的方法),妥善解决了数字证书申领注册环节普遍存在的RA(注册机构)履职不充分问题,达成了向投资者颁发数字证书安全可控,数字证书安全可信,使用证书签名安全可靠的理想目标。同时,在投资者使用预留号码手机申请、券商向其颁发数字证书时,可以做到对投资者透明无感;并借助二维码(软)连接、Token(软)连接、USB接口(硬)连接等方式,较好的实现了向投资者颁发数字证书全面覆盖各类终端设备。

3. 为落实账户实名制提供可靠技术保障

2019年新版《中华人民共和国证券法》通过修改第106条、新增第107条,强化了账户实名制规定和要求,不仅强调账户开立要实名,而且要求账户使用也必须实名。2023年初,证监会第204号令颁布《证券经纪业务管理办法》,在加强客户行为管理方面,进一步督促证券公司严格履行客户管理职责,要求切实做好客户身份识别、客户适当性管理、账户使用实名制等工作……证券行业百余家券商、1.2万分支机构、35.5万从业人员,服务于2.1亿客户。券商以非现场业务为主,绝大部分种类的业务和客户服务均在网开展、线上提供,账户实名制的贯彻落实需要IT保障与科技赋能。参照公安部第三研究所《eID数字身份体系白皮书(2018)》,“口令+‘三方协同鉴别’”强认证技术具备CIL4(顶级)颁证、AAL3(顶级)认证的全部属性特征,可以为行业落实账户实名制提供可靠技术保障。

三、打通最后一公里、打造网上证券高质量发展得力工具

“口令+‘三方协同鉴别’”技术方案的落地实施存在多样性:券商系统与运营商系统交互信息遵循总对总原则,联接线路既可以采用运营商直联,也可以采用相关运营商授权服务机构的技术方案;内嵌券商客户端SDK既可以采用

运营商技术方案,也可以采用相关运营商授权服务机构的技术方案;券商系统与银行系统交互信息遵循总对总原则,联接线路既可以采用银行直联,也可以通过中国银联等中介服务机构进行联接;券商系统与银行系统交互信息,既可以是银行主动推送/券商读取方式,也可以是券商主动请求/银行响应方式,可以采用轮询方式也可以并发执行;用户的银行端操作既可以通过网银、手机银行等银行应用系统进行,也可以通过嵌入券商应用系统的银行或中国银联等的SDK方式进行;“口令+‘三方协同鉴别’”强身份认证的“口令”一般是指用户在券商系统中设置的账户口令,必要时也可以借用同一用户主体在银行系统中设置的有效的账户口令.....

“口令+‘三方协同鉴别’”涉及整合券商、银行、运营商三方,以及相关服务商的多方面资源,方案实施存在一定复杂度。但在关键技术方面,当下运营商通讯网关取号技术在包括证券业务的部分场景已有一定规模的实际应用;券商与银行间的网络互联、业务合作,在三方存管模式下更已稳定开展多年。目前,“口令+‘三方协同鉴别’”电子认证落地需要打通的关键环节,主要集中在券商与银行的系统接口方面,尚需于满足现行监管框架和业务规则的前提下,进一步扩充相应接口功能。

2023年2月,中共中央、国务院印发《质量强国建设纲要》,提出面对新形势新要求,必须把推动发展的立足点转到提高质量和效益上来,培育以技术、标准、品牌、质量、服务等为核心的经济发展新优势.....在此大背景下,中泰证券积极探讨适用证券业务的强身份认证方法,期待业内外专家关注、评判,共同推进这一电子认证技术早日落地应用,将其打造成为券商数字化转型和网上证券高质量发展的得力工具。

参考文献

1. GB/T 39786-2021,信息安全技术 信息系统密码应用基本要求[S].
2. 中国证券监督管理委员会.客户交易结算资金管理办法[Z].2021-06-11.
3. 中国证券监督管理委员会.证券公司客户交易结算资金商业银行第三方存管技术指引[Z].2007-10-08.
4. 中国人民银行.关于改进个人银行账户服务 加强账户管理的通知[Z].2015-12-25.
5. 中国工商银行.关于修订《中国工商银行个人银行结算账户管理协议(2022年版)》的公告.<https://www.icbc.com.cn/page/726650139192172544.html>,2022-07-29.
6. 公安部第三研究所.eID数字身份体系白皮书(2018)[R].北京:2018-04.
7. 全国信息安全标准化技术委员会鉴别与授权工作组.电子认证2.0白皮书(2018版)[R].北京:2018-04.
8. GB/T 22239-2019,信息安全技术 网络安全等级保护基本要求[S].
9. JR/T 0060-2021,证券期货业网络安全等级保护基本要求[S].
10. 国家互联网信息办公室.关于《人脸识别技术应用安全管理规定(试行)(征求意见稿)》公开征求意见的通知.http://www.cac.gov.cn/2023-08/08/c_1693064670537413.htm,2023-08-08.
11. 中国证券业协会.证券公司网上证券信息系统技术指引[Z].2015-03-13.
12. 中华人民共和国证券法[Z].2019-12-28.
13. 中国证券监督管理委员会.证券经纪业务管理办法[Z].2023-01-13.

03 新技术应用-大模型

P48 隐私计算在大模型安全推理中的应用研究

张迪路、章庆、苗仲辰

P54 金融大模型安全风险与应对

陈洪炎

P59 大语言模型在证券业开发安全领域的探索与实践

谢朝海、齐大伟、谢琪、丁延彪

隐私计算在大模型安全推理中的应用研究

张迪路、章庆、苗仲辰 | 上海金融期货信息技术有限公司创新实验室

摘要：大模型的广泛应用被认为是人工智能的一次重大革命，也引发了大模型运营方可能会窥探用户隐私信息的广泛担忧。隐私计算保障了数据在使用过程中的“可用不可见”，与大模型安全推理应用场景中用户隐私保护诉求相契合。但是不同类型的隐私计算方案在通用性、安全性和效率性方面面临多重挑战。本文将介绍广义隐私计算在大模型安全推理中的应用，并提出一种基于可信执行环境的大模型安全推理方案，同时展望隐私计算技术在证券期货行业大模型安全推理中的应用前景。

关键字：大模型、安全推理、隐私计算、可信执行环境

当前，大模型已经在证券期货行业的研报投顾、市场分析等多个场景中扮演重要的角色，但是也可能带来新的隐私安全风险。大模型运营方可能会非法收集用户提问的数据以获取敏感信息、窥探用户个人偏好并结合开放空间高维信息还原用户特征。例如在市场分析场景中，市场经营机构如果把因子指标、分析方法等信息作为提示词输入给大模型，大模型运营方就可以获取关键策略。如果上述机密信息被运营方用作迭代优化，相关信息将存在更大范围泄密的风险。因此如何在保证用户隐私又能使得大模型准确推理得到正确的结果成为重要的研究方向。这样的安全推理技术不仅能够增强使用者对大模型的信任，还有助于大模型运营方开展更加符合监管合规要求的业务。隐私计算是指在保护数据本身不对外泄露的前提下实现数据分析计算的技术，与大模型安全推理应用场景中的用户隐私保护诉求相契合。本文将介绍广义隐私计算在大模型安全推理中的应用，提出一种基于可信执行环境的大模型安全推理流程并展望隐私计算技术在证券期货行业大模型安全推理中的应用前景。

系列技术，包括但不限于：基于数据脱敏的隐私保护技术、基于数据扰动的隐私保护技术、基于密码学协议的隐私保护技术以及基于硬件可信执行环境的隐私保护技术等^[3]。

（二）隐私计算的技术分类

1. 基于数据脱敏的隐私保护技术

数据脱敏指的是在不改变数据信息、保障数据分析结果准确性的前提下，对含有敏感信息的原始数据进行处理，以减低数据隐私风险。此类技术措施多采用屏蔽、替换、删除等脱敏处理手段。常见的数据脱敏技术包括通过生成新的标识符来替代原标识符的假名化技术以及对直接标识符进行屏蔽、间接标识符进行泛化或者随机化的匿名化技术^[4]。

2. 基于数据扰动的隐私保护技术

数据扰动指的是在原始数据中加入随机噪声使数据扰动失真，通过模糊信息以保护个人信息但可以保证部分数据属性、分布特性不变。噪声的大小可以根据具体的安全系数要求作出调整以平衡数据可用性与安全性^[5]。

3. 基于密码学协议的隐私保护技术

基于密码学协议的隐私保护技术主要包括同态加密以及安全多方计算。同态加密是一种可以对密文进行直接计算的隐私保护方式，其运算得到的结果再解密后就可得到明文的计算结果^[6]。安全多方计算的概念由图灵奖获得者姚期智在1982年提出^[7]，是指多个参与者利用自己的私有数据合作计算某个函数，但在计算过程中又能保证私有数据的机密与安全。

4. 基于硬件可信执行环境的隐私保护技术

同态加密和安全多方计算存在性能较低的问题，主要瓶颈在于非线性的比较运算，因此无法适用于任意的计算

一、隐私计算的技术和应用介绍

（一）什么是隐私计算

隐私计算是指在保证数据提供方不泄露原始数据的前提下，对数据进行分析计算的一系列信息技术，保障数据在流通与融合过程中的“可用不可见”^[1]。中共中央、国务院于2022年12月2日发布的《关于构建数据基础制度更好发挥数据要素作用的意见》明确提出探索“原始数据不出域、数据可用不可见”的数据应用模式。广义上看，隐私计算的技术概念可以延伸至通过提高数据可管理性、可分离性和保密性来减轻数据处理所产生的个人隐私风险的任何软件或硬件的解决方案^[2]，是实现隐私保护前提下数据安全共享的一

问题,需要在实际应用场景下设计具体的解决方案。近年来更高性能和通用性的可信执行环境技术^[8]在隐私保护方案中脱颖而出。可信执行环境指的是设备上独立于操作系统的隔离执行环境,它可以确保在安全环境中存储、处理和保护数据。可信执行环境技术的安全性通常由硬件相关机制保证,常见的可信执行环境技术包括Intel SGX^[9]、ARM TrustZone^[10]等。

(三) 隐私计算在大模型安全推理中的应用研究

1. 基于数据脱敏的大模型安全推理技术

2020年微软开源了Presidio项目,提供快速的识别和匿名化模块,用于识别文本中的隐私实体信息,如信用卡号、姓名、地点等^[11]。Presidio利用传统自然语言处理中的命名实体识别模型进行实体识别,再通过正则表达式匹配敏感信息并屏蔽,最后基于规则的逻辑及校验和等多种方式提供脱敏后的文本数据。这种隐私实体匿名化技术为大模型安全推理提供了方案参考,但是因为采用了敏感信息完全替换的方法,导致Presidio对原始提示词中语义表达较弱,可能会对云端大模型理解产生一定影响。为解决上述问题,2023年9月腾讯安全玄武实验室提出Hide and seek方案,基于开源模型Bloom微调了一个可以发现、替换、还原隐私词的模型^[12]。与Presidio直接屏蔽隐私实体信息不同的是,该方案通过近义词替换的掩码方式一定程度上保留了原提示词中的语义信息,还通过对模型输出后处理的方式将替换的近义词进行还原以得到真实结果。基于数据脱敏的安全推理技术虽然效率较高,但是适用范围有限,主要用于润色、理解、分类等简单文本任务。因为数据脱敏是通过只披露部分不敏感信息的方式进行信息截断,并没有对原始数据进行语义改变,因此结合高阶外部信息仍可以还原部分敏感信息,隐私防范效果有限。

2. 基于数据扰动的大模型安全推理技术

2023年10月中国科学技术大学团队提出一种基于数据扰动的大模型安全推理方案PrivInfer^[13]。PrivInfer算法包括扰动模块和提取模块。扰动模块通过添加拉普拉斯噪声构建随机邻接表,将原文本中标记词替换成语义相似的词,在实现差分隐私保护的同时一定程度上保证文本的实用性。提取模块利用了一个便于部署的本地小语言模型,通过原始文档信息以及扰动后云端大语言模型生成结果进行信息解码提炼,最终输出原始提示词推理结果。他们的实验表明根据扰动提示生成的内容与根据原始提示生成的非隐私内容在语义相似性、连贯性上效果相近。2024年2月美国罗格斯大学团队提出PromptCrypt方案,使用表情符号对用户输入进行加密扰动,然后再将其发送给大语言模型,使提示词无法被直接破译,同时保留一定的原始意图,从而使模型的效果不受影响^[14]。此类基于数据扰动的大模型安全推理技术虽然在隐私保护程度和使用效率上有所优势,

但是要实现更加安全的隐私保护,加入原始数据的噪声就会越大,原始数据的可用性就越低,必然也会影响大模型推理得到的结果。

3. 基于密码学协议的大模型安全推理技术

2023年7月,浙江大学团队提出第一个安全两方隐私推理模型CipherGPT^[15]。对于模型中的线性层,CipherGPT通过批量预处理的方式优化了两方交互计算效率。对于非线性层,CipherGPT通过分段查表的方式进行高效近似,从而实现安全两方推理。2023年9月蚂蚁集团的团队提出Puma方案,该方案提出更加准确和快速的非线性函数近似方法^[16]。Puma通过密码学方式改造安全嵌入协议、安全GeLU函数、安全Softmax协议、安全LayerNorm协议以实现模型的推理安全交互。2024年5月该团队又提出了第一个支持量化的安全推理框架Ditto^[17],能够根据数据类型自动执行不同量化精度的密态运算。基于密码学协议的大模型安全推理技术虽然在理想状态下可以实现最为通用的安全计算,但是由于大模型的结构中包含大量的非线性层,安全多方计算一方面会对数据进行近似截断从而导致多层网络模型的准确率严重下降,另一方面还会带来大量的计算和通信开销。以CipherGPT为例,文中实验表明生成1个token需要耗时长达20分钟,带宽占用为15GB。

4. 基于硬件可信执行环境的大模型安全推理技术

2022年9月北京大学团队基于可信执行环境SGX提出了一种面向机器学习推理的安全服务系统S3ML^[18]。S3ML将机器学习模型运行在受保护区域中以保护用户隐私。但由于传统的可信执行环境设计主要集中在CPU上,随着模型参数及规模的不断增大,GPU在处理人工智能大规模计算任务中愈发重要,在GPU上构建安全可信的硬件可信执行环境已成为保护数据隐私的一个重要研究方向。2023年7月英伟达公布了首个的GPU可信执行环境方案^[19],通过高速串行的带宽传输扩展了CPU的可信执行环境功能。2024年7月蚂蚁集团团队发布基于GPU可信执行环境的模型密态推理平台^[20]但尚未公布安全推理流程协议细节。

二、基于可信执行环境的大模型安全推理流程

密码技术的性能瓶颈制约了模型安全推理的实际应用,可信执行环境技术通过在硬件隔离的环境中解密隐私数据并进行计算有效地降低了密码学性能开销。为了实现通用且高效的安全推理流程,本文将基于可信执行环境提出具体的大模型安全推理流程,如图1所示。本节将首先介绍流程中的恶意威胁模型,其次介绍具体的流程细节以及相关分析。



图1 大模型安全推理流程

(一) 威胁模型

我们假设隐私信息窃取者完全了解可信执行环境架构以及本协议方案,预计会利用所有可用信息发动攻击,目的是获取用户向大模型传输的推理信息以窃取用户隐私。隐私信息窃取者可以是应用链路上的任意服务供应商(包括硬件、通信、大模型应用服务等供应商),可以对传入可信执行环境内部的信息进行伪装篡改或重放、可以监听通信信道并获取通信信道中传输的数据,也可以尝试破解信道中传输报文中的信息以窥探用户发送的信息。本文将假设可信执行环境的可靠性,因此针对硬件环境的攻击方式不在本文的考虑范围内。

(二) 身份认证

为了向可信执行环境内部传递加密过的用户提示词,整体流程中需要首先标识每个可信执行环境的身份,在传

统的体系架构中,证书颁发机构负责发放数字证书,标明每个节点的身份。在本威胁模型中模型服务提供方可能会伪造身份以窃取用户信息,因此本协议首先需要一个安全的身份认证方案。

依托可信执行环境的内存保护机制,我们可以设计出一个安全的密钥生成方式。由于外部运营方无法窥探可信执行环境内部信息,我们可以将审计过的公私钥生成程序加载进可信执行环境内部,在可信执行环境内部生成公私钥对并将私钥驻留在可信执行环境内部,将公钥返回不可信区域以表明可信执行环境的身份。为了防范公钥传输过程中可能遭受的中间人攻击,我们可以利用远程认证技术来验证公钥信息的一致性。在远程认证中,应用程序可以通过可信执行环境生成一份报告,并将报告发送给内部认证服务生成证书,证书反映了可信执行环境内部的公钥和整个平台的信息。完整的身份认证协议如图2所示:

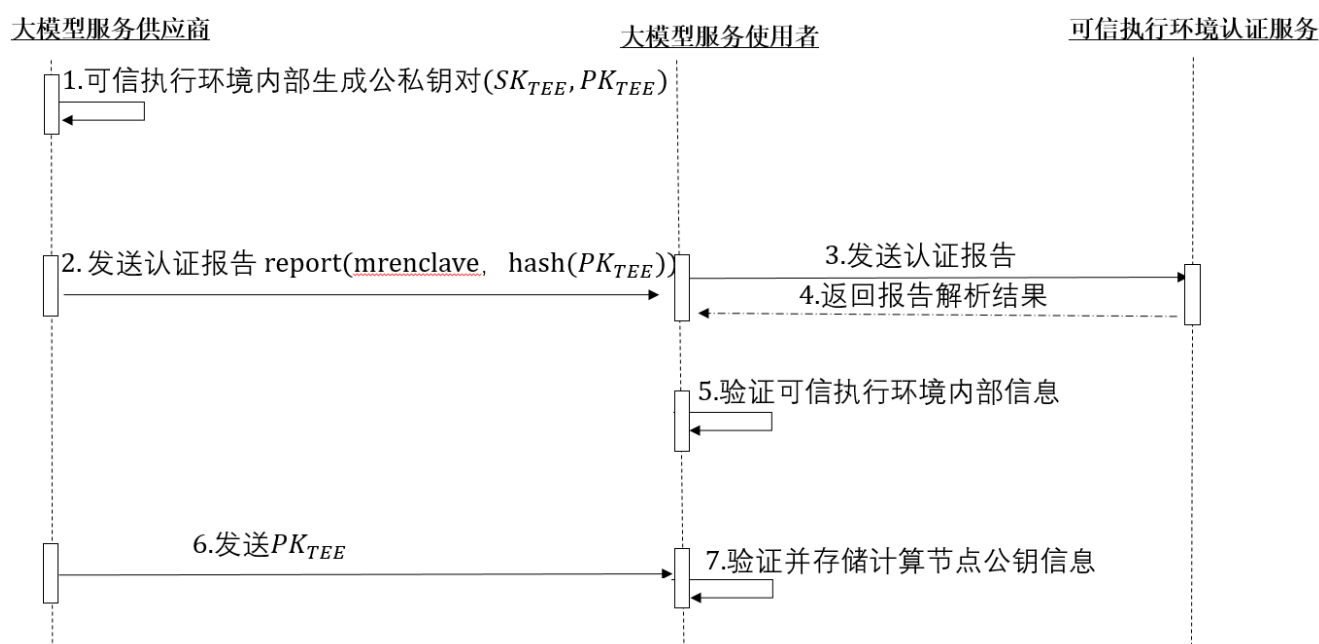


图2 身份认证协议

整体的协议流程如下：

(1)大模型服务供应商首先将审计过的公私钥生成程序加载进可信执行环境内部并运行该程序，得到公私钥对(SK_{TEE}, PK_{TEE})，可信执行环境将私钥通过数据密封持久化存储，以便将来解密使用；

(2)大模型服务供应商向用户发起远程认证，在可信执行环境内部生成认证报告，认证的内容包括大模型服务供应商是否使用了正确的公私钥生成程序(表现为安全区度量值与指定程序相同)及可信执行环境内部相关信息，同时在报告中附带公钥哈希值 $hash(PK_{TEE})$ 以便之后验证公钥的正确性；

(3)用户接收到认证报告后，将报告转发给可信执行环境认证服务以解析报告内容；

(4)用户接收认证服务解析出的报告结果；

(5)用户根据自己指定的规则和报告内容验证大模型服务供应商的可信执行环境的正确性以及完整性，以此决定远程认证是否通过；

(6)若远程认证通过，大模型服务供应商向用户发送自身公钥 PK_{TEE} ；

(7)用户接收到公钥后根据远程认证报告中附带的公钥哈希值验证公钥的正确性，若两者匹配则验证通过，用户保存大模型服务供应商的可信执行环境身份信息以便后续使用。

(三) 加密提示词数据传输

身份认证协议为大模型服务供应商提供了身份标识，每个模型推理节点在初始化身份认证后都拥有了可信的公私钥对。考虑到实际场景下的使用效率问题，对称加密比非对称加密快多个数量级，因此本协议采用数字信封的方式进行隐私提示词的传递。数字信封是将对称加密密钥用非对称加密的方式加密后传递的一种技术。数字信封既发挥了对称加密速度快并且安全性好的优势，又发挥了非对称加密中密钥管理较为方便的优势，有效地结合了对称加密和非对称加密的优点。加密提示词传输协议如图3所示：

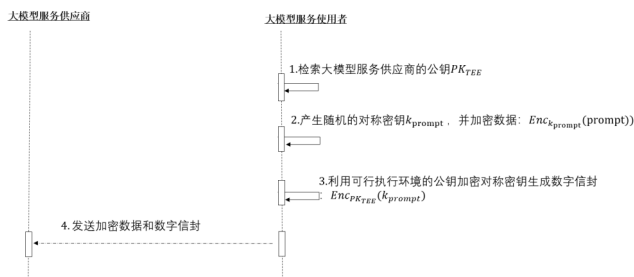


图3加密提示词传输协议

整体的加密提示词传输协议流程如下：

(1)用户检索大模型服务供应商的公钥，并得到 PK_{TEE} ；

(2)用户自身产生随机的对称密钥 K_{prompt} 并使用 K_{prompt} 加

密希望传输给大模型服务供应商的提示词数据 $prompt$ ；

(3)用户使用第一部得到的公钥 PK_{TEE} ，加密 K_{prompt} ，组成数字信封；

(4)用户将第二步和第三步得到的加密提示词数据和数字信封传递给大模型服务供应商的可信执行环境内部。

(四) 安全推理

安全推理协议的目标是保证大模型服务供应商在提供模型服务的过程中只能对密文提示词进行操作，无法知悉明文的相关内容。在推理完成后，得到的推理结果仍然以密文的形式呈现并发送给用户，只有用户可以对密文进行解析并获取最终的推理结果。安全推理协议如图4所示：

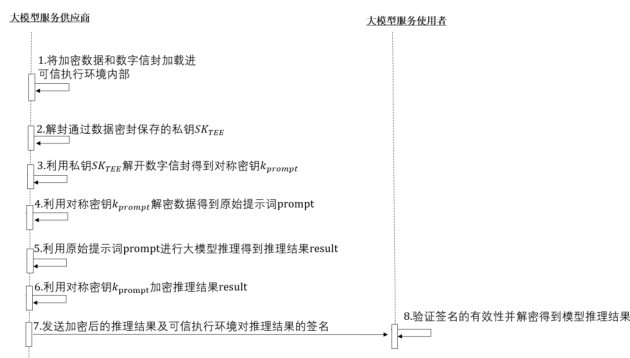


图4安全推理协议

整体的安全推理协议流程如下：

(1)大模型服务供应商将接收到的加密提示词数据和数字信封加载进可信执行环境内部；

(2)大模型服务供应商在同一个可信执行环境中解封之前通过数据密封操作保存的私钥 PK_{TEE} ；

(3)解封成功后，大模型服务供应商在可信执行环境内部通过私钥 PK_{TEE} 解开数字信封，得到对称密钥 K_{prompt} ；

(4)得到对称密钥 K_{prompt} 后，大模型服务供应商解密通过对称加密的提示词数据，并得到原始的提示词 $prompt$ ；

(5)得到原始提示词 $prompt$ 后，大模型服务供应商就可以在可信执行环境内部进行模型推理，并最终得到推理结果 $result$ ；

(6)大模型服务供应商利用对称密钥 K_{prompt} 对第五步生成的推理结果 $result$ 进行对称加密；

(7)得到加密的推理结果后，大模型服务供应商将加密推理结果与可信执行环境对于加密推理结果的正确性签名一起发送给用户；

(8)用户得到加密推理结果和正确性签名后，先验证签名的有效性，若验证通过，用户就利用对称密钥 K_{prompt} 解密并得到推理结果。

通过安全推理协议，大模型服务供应商对密文提示词数据进行了解密推理，并最终返回加密后的推理结果以及正确性签名。在整个安全推理过程中，由于可信执行环境的相关安全特性，服务供应商无法知悉明文提示词的相关内

容,并且在推理完成后结果仍然以密文的形式呈现,服务供应商也不能对推理结果进行解析并获取相关信息。

(五) 安全性分析

根据GPU可信执行环境测试数据显示,安全运算与明文运算相比只会带来10%-20%的性能损耗。因此在满足实际应用场景下的通用性和效率性的前提下,本节将重点从推理节点身份安全性、提示词数据传递机密性与推理过程的安全性角度对基于可信执行环境的安全推理协议进行安全性分析。

1.推理节点身份的安全性

可信执行环境的安全环境保证了大模型服务供应商运行了可信的经过审计的程序,因此该节点在可信执行环境内部通过该程序可以生成一个安全的公私钥对。与硬件信息绑定的数据密封技术保证了密封过的私钥不会被恶意窃取,而远程认证技术保证了密钥传递过程中不会遭受中间人攻击,可信执行环境内部生成的公钥可以被正确而完整地传递给远程接收者。这两个核心安全机制均是基于可信执行环境的安全防护,因此我们认为本协议可以保证节点身份的安全性。

2.提示词数据传递的机密性

由于大模型服务供应商拥有可信的身份信息,其公钥保存在公开可信的数据库中,私钥依靠数据密封的方式存储,仅能由同一个可信执行环境解密,因此其私钥信息无法被攻击者获取。由于数字信封只能由私钥拥有者解开,因此隐私提示词数据的加密密钥仅由用户和可信执行环境知悉。在加密提示词数据的传递过程中,即使攻击者窃听到了加密提示词数据的相关信息,由于缺乏对称加密密钥或可信执行环境内部私钥的相关信息,攻击者仍然无法获悉原始提示词数据的相关信息。因此本协议可以保证提示词数据传递过程的机密性。

3.推理过程的安全性

对于大模型推理过程而言,大模型服务供应商将加密提示词和数字信封加载进可信执行环境内部,最终返回得到加密的推理结果。在整个过程中,大模型服务供应商虽然拥有密封过的私钥文件,但可信执行环境的安全特性保证只有生成私钥的可信执行环境才能恢复出私钥信息,外部不可信区域内的应用程序无法获取文件内部的私钥信息,因此也就无法解开数字信封进而获取原始提示词数据相关信息。而由于可信执行环境的内存加密特性,在大模型的推理过程中,外部不可信应用程序也无法获知内部可信执行环境的相关信息,因此推理过程中不会存在隐私泄露的相关问题。在推理结束后,推理结果被对称密钥加密并附带可信执行环境签名一起返回给不可信区域。由于对称加密密

钥仅由用户和可信执行环境内部知悉,加密过的结果也无法被不可信程序获取并破解,且可信执行环境内部签名无法被伪造与篡改。因此推理结果和签名可以被安全传递回用户,最终由用户使用对称密钥解密得到推理结果。因此,本协议可以保证推理过程中隐私提示词的安全性。

(六) 可行性分析

隐私计算以其数据“可用不可见”的特点,有望成为实现大模型隐私安全的关键一环,有效增强使用者对大模型的信任。但是不能忽略的是,数据脱敏和数据扰动技术在场景通用性、安全防护级别上有所欠缺,密码学协议在应用效率上仍有待提高。因此综合使用场景和应用效率考虑,本节基于硬件可信执行环境提出大模型安全推理协议细节,在保证身份、传输和推理计算过程安全的的前提下不会带来过度的性能损耗,在实际应用方面具有一定优势。虽然可信执行环境也面临包括侧信道攻击、硬件架构自主可控以及异构环境可扩展性和可移植性等多方面挑战,但未来在更为成熟的硬件解决方案以及更为严谨的评估和尝试后,有望成为解决大模型隐私安全问题的重要技术方案。

三、总结与展望

证券期货行业是数据密集型行业,数据的采集、处理和应用至关重要,面临隐私泄露等安全挑战。特别是当前,大模型在证券期货领域的试点正由点及面不断扩大,其应用可能带来的隐私安全风险更加值得重视。部分行业机构通过大模型本地化部署的方式,可以避免数据出域带来的不可控安全风险。但更多中小行业机构需要考虑的是受限于数据资源和部署成本,通过公有云或行业大模型等公共资源开展相关业务,如何确保相关大模型业务隐私安全及合规。本文提出一种基于可信执行环境的大模型安全推理方案,综合平衡了应用系统中身份认证、安全推理性能和便捷性等考量。未来,建议各单位在具体实践中厘清证券期货类业务场景中的安全边界,由制度保障的自律安全向技术保障的可证安全迈进,才有望实现合规可信大模型的普惠应用。

参考文献

- [1].中国信息通信研究院云计算与大数据研究所. 隐私计算白皮书(2021) [R], 2021。
- [2]. The House Committee on Science, Space, and Technology. H.R. 84 7, Promoting Digital Privacy Technologies Act[R], 2022, <https://www.cbo.gov/publication/57941>.
- [3].隐私计算联盟. 可信隐私计算研究报告(2022) [R], 2022。
- [4].王卓,刘国伟,王岩,等.数据脱敏技术发展现状及趋势研究[J]. 信息通信技术与政策, 2020, 46(4): 18。
- [5].张书奎,吴云鹏,杨玉仁,等.基于数据扰动的隐私保护方法,装置及相关组件:CN201910362769.0[P].CN110087237B[2024-09-23].
- [6].Gentry C, Boneh D. A fully homomorphic encryption scheme[M]. Stanford: Stanford university, 2009.
- [7].Yao A C. Protocols for secure computations[C] //23rd annual symposium on foundations of computer science (sfcs 1982). IEEE, 1982: 160-164.
- [8].Sabt M, Achemlal M, Bouabdallah A. Trusted execution environment: what it is, and what it is not[C]//2015 IEEE Trustcom/BigDataSE/ISPA. IEEE, 2015, 1: 57-64.
- [9].McKeen F, Alexandrovich I, Berenzon A, et al. Innovative instructions and software model for isolated execution[J]. Hasp@ isca, 2013, 10(1).
- [10].ARM A. Security technology building a secure system using trustzone technology (white paper)[J]. ARM Limited, 2009.
- [11].<https://microsoft.github.io/presidio/>.
- [12].Chen Y, Li T, Liu H, et al. Hide and seek (has): A lightweight framework for prompt privacy protection[J]. arXiv preprint arXiv:2309.03057, 2023.
- [13].Tong M, Chen K, Qi Y, et al. Privinfer: Privacy-preserving inference for black-box large language model[J]. arXiv preprint arXiv:2310.12214, 2023.
- [14].Lin G, Hua W, Zhang Y. Promptcrypt: Prompt encryption for secure communication with large language models[J]. arXiv preprint arXiv:2402.05868, 2024.
- [15].Hou X, Liu J, Li J, et al. Ciphergpt: Secure two-party gpt inference[J]. Cryptology ePrint Archive, 2023.
- [16]. Dong Y, Lu W, Zheng Y, et al. Puma: Secure inference of llama-7b in five minutes[J]. arXiv preprint arXiv:2307.12533, 2023.
- [17]. Wu H, Fang W, Zheng Y, et al. Ditto: Quantization-aware Secure Inference of Transformers upon MPC[J]. arXiv preprint arXiv:2405.05525, 2024.
- [18]. Ma J, Yu C, Zhou A, et al. S3ML: A secure serving system for machine learning inference[J]. arXiv preprint arXiv:2010.06212, 2020.
- [19].<https://www.nvidia.com/zh-tw/data-center/solutions/confidential-computing/>
- [20]. <https://www.secretflow.org.cn/zh-CN/llm>.

金融大模型安全风险与应对

陈洪炎 | 上交所技术有限责任公司

摘要：随着人工智能技术在金融领域的广泛渗透，金融大模型的技术优越性、行业契合性与实践可行性日益凸显，但金融大模型的复杂性和对数据的依赖性也带来了一系列安全风险。本文探讨了金融大模型的安全挑战，包括模型安全及应用安全，并详细分析了数据收集处理、模型训练、模型部署和模型落地应用各阶段的安全风险，文章提出安全评估框架，包括安全评测数据集的构建、安全评估方法的设计以及安全评测模型环境的部署。

关键字：金融大模型、安全风险、安全评估、安全防护

一、引言

大模型和人类反馈的强化学习的结合进一步重构了AI开发范式，大模型改变了传统的开发活动，极大释放了传统软件中开发投入。大模型作为金融领域的新质生产力的要素之一，金融领域沉淀的大量数据为大模型在金融领域应用及落地提供了良好的数据基础。金融大模型的应用具有高度的技术优越性和实践可行性。但金融大模型在给金融业带来巨大效益的同时也将引发一系列安全风险，主要体现为算法可信风险、隐私泄露风险、数据安全风险和法律监管风险等。随着金融大模型的广泛部署，安全与隐私问题也日益突出。金融机构在采用大模型以提高效率和服务质量的同时，也必须面对数据泄露、系统滥用及不透明的AI决策等风险。金融业务的安全性、隐私性、专业性、合规性和监管等要求对大模型的落地实践也提出了更加严格的风险防控要求。

二、金融大模型的安全分析

金融大模型的数据量、算力规模和模型参数持续增长，推动了大模型相关技术的迅猛发展。当前，金融大模型技术已经在金融业务的领域展现出了巨大的应用价值，极大地推动了金融产业的发展进步。然而，随着金融大模型应用的不断深入，相关的安全问题也日益凸显，新型安全威胁层出不穷，给金融行业带来了严峻的挑战。

不穷，给金融行业带来了严峻的挑战。

在金融业务领域中使用大模型既带来了众多创新，也引入了一系列的安全问题和风险，例如越狱攻击、提示词注入攻击以及数据投毒攻击等，给金融大模型的技术应用带来了严重威胁。这些风险不仅威胁到金融机构的数据安全，也影响个人的安全隐私等风险问题。大模型在金融领域的实践和落地需要考虑多方因素，除了大模型技术框架对现有金融业务的效率提升以外，金融大模型在数据隐私安全、模型推理安全及内容合规等方面存在安全挑战。

金融大模型安全挑战主要分为模型安全及应用安全。模型安全是金融大模型在研发过程中设计的基础设施、数据、算法、训练过程、部署等环节中遇到的安全风险，而应用安全是金融大模型的不合理应用、滥用或恶意使用而引入的决策失控、隐私安全问题、伦理问题和法律风险等。模型安全问题应由大模型研发团队关注，应用安全则需要法律法规和行业管理规范来监管和控制。

金融大模型的研发生命周期可分为数据收集处理、模型训练、模型部署和模型落地应用四个阶段(图1)。其中数据收集处理阶段主要是收集、处理、储存大模型训练需要的预训练数据、安全数据和金融指令等；模型训练阶段对海量数据进行预训练、调参、对齐、构建智能体等；模型部署是将训练好的大模型适配特定的硬件资源，并尽量提高大模型的实时性和推理效率；模型落地应用是用大模型解决各种实际的金融任务。

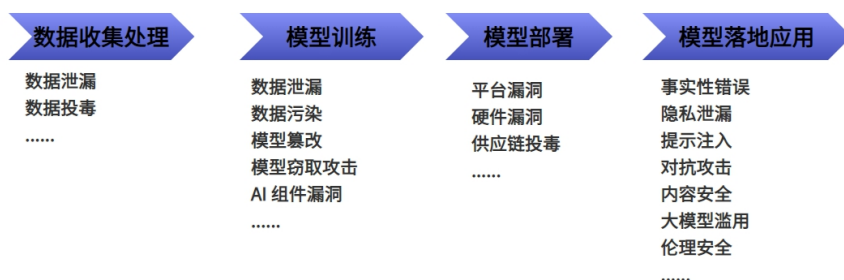


图1 金融大模型的研发生命周期

金融大模型的安全风险在不同的生命周期阶段有所不同,也有部分安全风险贯穿在全研发生命周期中。在数据收集处理阶段,潜在数据泄漏、数据投毒等风险;在模型训练阶段,潜在后门攻击、数据泄漏、数据污染、模型篡改、模型窃取攻击、AI 组件漏洞等风险;在模型部署阶段潜在平台漏洞、硬件漏洞、供应链投毒等风险;在模型落地应用阶段,潜在事实性错误、隐私泄漏、提示注入、对抗攻击、内容安全、大模型滥用、伦理安全等风险。

表1 金融大模型常见安全风险举例

安全风险	说明
隐私安全	训练数据的来源若不透明,可能会带来恶意攻击和数据侵权的隐患。
提示注入攻击	不良用户可能会在常规输入中巧妙地嵌入特定的短语或关键词,以此操纵模型的决策机制,诱导模型突破安全防线。
大模型幻觉	在处理和生成自然语言的过程中,大型模型依赖于训练数据中的模式和结构,有时可能会生成看似合理但实际上并不准确的内容。这导致大型模型在文本生成时,可能会产生与现实不符或完全虚构的信息。
后门攻击	攻击者可能会在大型模型的训练数据中植入特定的输入输出配对,目的是为了在未来某个时刻能够利用这些条件来操纵金融大型模型。
越狱攻击	恶意用户通过巧妙构造的提示词输入,能够绕过大型模型的安全防护,从而诱导模型生成违规信息。
有害信息	由于训练数据的不足和训练过程的不完善,大型模型在生成内容时可能与可验证的现实世界事实存在偏差,这可能导致其输出包含恐怖主义、极端主义、色情、暴力等有害信息。
数据投毒攻击	攻击者可能在模型的训练数据集中植入少量含有恶意内容的有害样本,这些样本会在模型训练或微调过程中对模型造成“污染”,从而损害模型的有效性。
伦理问题	目前,大型模型在全生命周期管理方面的体制尚未完善,这可能导致偏见和歧视、隐私泄露、错误信息传播以及模型决策的不可解释性等问题出现。
侵犯知识产权	由于大型模型在训练数据的采集和使用过程中可能缺乏明确的法律规范,存在被恶意利用的风险,这可能导致数据滥用和侵犯知识产权等问题。
数据泄露	数据泄露是指用户在与大型模型交互时,其敏感信息(如财务资料、交易记录和个人识别信息等)可能在发送请求或接收响应时被非法获取。这类信息泄露一般发生在模型训练、分析推理或与外部系统的数据交换过程中。
数据窃取	数据窃取攻击是一种技术策略,攻击者通过巧妙构造的查询与大型模型互动,目的是从模型的反馈中抽取并拼凑出在模型训练阶段所涉及的敏感信息。通过持续地提供特定的输入,攻击者试图诱使模型无意中透露其训练数据中的保密信息。
RAG 投毒	RAG 数据已成为一个标准配置,知识库数据大部分来源于网络,而且风险经常被忽略,企业为了增强检索,经常外挂知识库,造成安全风险。

三、金融大模型安全评估

为了确保金融大型模型带来的好处并防范潜在风险,必须提前识别、分析和评估可能的风险点。随着新的管理规定和架构的建立,安全性评估已成为开发、部署和监管金融大型模型过程中不可或缺的环节。鉴于金融大型模型的安全风险是固有存在的,因此,实施全面的安全性评估变得尤为关键。安全性评估的核心任务包括:(1)开发安全性评估的数据集,(2)制定安全性评估的策略,以及(3)搭建安全性评估的模型操作环境。

(一) 构建安全评测数据集

创建一个全面的安全评估数据集对于进行有效的安全评测至关重要。这个数据集应该覆盖技术、伦理、社会和法律等多个方面,通过识别金融大型模型在散布错误信息、产生有害内容、引发隐私泄露和侵犯版权等方面的问题,并研究这些安全风险的历史根源。安全评估数据集的构建应该包括以下几个方面:

偏见评估数据集:该数据集旨在从准确性和公正性的角度评估模型是否对性别、种族、年龄等敏感因素存在偏见。

毒性识别数据集:该数据集用于从效果和适宜性的角度识别和过滤网络上的有害言论,目的是保护用户不受负面内容的影响。

隐私泄露评估数据集:该数据集用于从合规性和保护性的角度检测模型是否可能泄露用户隐私,确保用户数据在处理和存储时的安全。

对抗攻击评估数据集:该数据集用于测试模型对各种对抗性攻击的防御能力,通过评估模型在面对攻击时的准确性和在不同攻击强度下的稳定性,来衡量模型的安全性能。

综合评估数据集:该数据集结合了上述多个维度,进行全面的评估,以检测模型在安全性、公正性、隐私保护和对抗攻击能力等方面的整体表现。

(二) 设计安全评估方法

1. 构建多学科融合的评估体系

金融大型模型的开发涉及技术、伦理、社会和法律等众多领域,需要各领域专家的通力合作。为了实现这一目标,必须打破学科间的隔阂,建立一个多学科融合的评估体系。由于不同学科间在语言表述和分析方法上存在差异,团队中需要培养能够理解并桥接不同学科语言体系的“翻译者”。

2. 人工评估手段

人工评估依赖于专家的知识 and 特定规则来对大型模型的输出进行安全性评估。这种方法的优点在于能够深入考虑道德、文化和情感等抽象因素,以及模型在处理复杂、含糊或创新性任务时的表现。然而,人工评估也存在一些缺点,如由于评估者个体差异导致的结果不一致性,以及高成本和低效率,这可能难以跟上大型模型快速发展的步伐。

3. 自动化评估技术

自动化安全评估通常采用基于规则或机器学习的文本分类技术,快速识别模型输出内容是否触及预设的风险类别。通过分析模型中间层的神经元激活和注意力权重等信号,可以发现导致不当行为的关键因素。自动化评估的优势在于成本低、效率高、可重复性强,便于进行不同模型间的

性能比较和建立标准化测试。然而,这种方法在理解复杂语境和隐含意义方面存在局限,数据覆盖率可能不足,且存在过拟合风险,可能无法准确反映模型在现实世界中的表现,也无法评估内容的质量和创造性,以及与人类价值观的一致性。

4. 人机协同评估模式

结合自动化和人工评估方法可以融合两者的优势,实现高效、可量化、准确和客观的评估,以进行全面和精确的安全评估。

5. 安全风险的优先级排序

鉴于金融大型模型面临的安全风险多种多样,建立一个明确的优先级排序机制是必要的,以便集中资源解决最紧迫的安全问题。安全评估应优先关注法律、伦理和隐私等方面。

(三) 部署安全评测模型环境

在线安全评估平台需达到以下四项标准:

1. 即时响应能力

安全评估平台必须具备即时反应功能,以便在第一时间对潜在风险进行处理,防止用户接触到有害内容,同时保护金融大型模型不受攻击。

2. 适应性

鉴于安全需求的不断演变,安全评估平台应能够灵活调整,以实时更新内容安全控制规则,包括增加、删除或修改相关规则。

3. 高可用性

由于安全评估平台可能会频繁被调用,且大型模型运行需要较多的计算资源,平台必须确保高可用性、低延迟、稳定性和鲁棒性。在此条件下,平台应尽可能减少计算资源的使用,以维持高效的安全防护。

4. 可评估性

安全评估平台应提供对安全性能的评价工具,允许用户监控屏蔽率、误报率、准确率、召回率和计算效率等关键指标,并根据这些指标进行优化调整。

四、金融大模型安全应对

金融大型模型面临复杂的安全威胁,包括模型固有的安全隐患,如数据泄露和隐私保护问题,以及来自外部的威胁,如恶意攻击和模型滥用等。为了增强金融大型模型的安全性,需要采取一系列策略,包括但不限于提高数据质量、

加强模型训练、减少错误输出、进行安全评估和加强硬件安全等,以确保数据的安全性、算法的可解释性、模型决策的可靠性、应用的合法性和环境的安全性。至于外部风险,则主要依靠国家法律、法规和行业标准来进行管理和规范。

(一) 金融大模型安全策略

金融大模型的安全策略可以分为五个维度来制定:鲁棒性、可靠性、隐私性、公平性和可解释性。

1. 鲁棒性

金融大型模型的鲁棒性是指模型在遭遇输入数据的波动、干扰或遭到攻击时,仍能维持其效能和可靠性的能力。鲁棒性反映了金融大型模型抵御外界干扰和输入杂讯的能力。在金融行业,鲁棒性尤为关键,因为金融数据往往充满噪音、难以预测,并且可能遭到恶意攻击。金融大型模型必须能够应对数据中的杂音、防御对抗性攻击、处理非典型数据,并保持模型的鲁棒性和普适性。为了增强金融大型模型的稳鲁棒性,可以采取以下策略。

数据预处理与增强:通过清除数据中的杂音和异常值,以及实施数据标准化和增强(例如旋转、缩放、添加杂讯等),提升模型对输入变化的适应性。数据增强对于抵御各种攻击如后门攻击、数据投毒等是一种有效的防御手段,它通过应用多种变换来丰富数据集的多样性,同时减少异常数据的影响。

模型结构与算法的优化:采用更复杂的模型,如深度神经网络,利用集成学习方法整合多个模型的预测,以及通过对抗训练在训练阶段引入对抗样本。

安全合规性与隐私保护:鉴于金融行业对合规性有严格的要求,设计和部署金融大型模型时,必须确保模型遵守相关法律法规,并实施适当的数据保护措施。

提升模型的泛化能力:通过训练使用多样化和具有代表性的数据库,以及应用正则化技术和交叉验证等方法,增强模型对未知数据的适应性。

异常值检测:利用异常样本与正常样本在分布或隐藏特征上的差异,来识别数据中的异常值。

2. 可靠性

金融大型模型的可靠性是指模型在实际应用场景中能够持续稳定地执行任务并准确达成目标的能力,确保模型在处理未知数据时仍能提供准确的预测。这一特性反映了金融大型模型在实际运用中的稳定性、精确度和可信用度。在金融领域,数据的质量与模型的预测准确性直接关系到决策的可靠性,因此,可靠性对于金融大型模型来说极为关键。为了增强金融大型模型的可靠性,可以采取以下措施。

提供高质量的训练数据:确保模型训练使用的数据是精确、全面且具有代表性的,以确保数据的高品质能够正面影响模型的性能。提升数据集质量的方法包括异常数据的

检测与清洗、数据转换、数据增强、以及对数据质量进行持续监控和维护。

强化数据管理:通过数据清洗、整合和验证等机制,确保输入模型的数据质量,从而提高数据的准确性。

推进可解释人工智能技术:通过构建透明模型和提供决策过程的可视化,增强人工智能决策的透明度和可追溯性。

融合大型模型与特定领域小型模型:利用大型模型的认知、理解和沟通能力,同时借助小型模型来精确控制风险并执行严谨的逻辑处理。

结合大型模型与金融知识图谱:将大型模型的参数化知识与结构化、明确的金融知识图谱相结合,以此提升模型的可靠性。

3. 隐私性

金融大型模型的隐私保护能力是指模型在处理敏感数据时,能够确保未授权用户无法访问模型中的隐私信息和输入数据。鉴于金融数据往往包含如账户信息、交易历史和信用评分等敏感个人信息,确保这些信息的安全显得尤为重要。金融大型模型在分析数据时,必须保证个人和机构数据的安全,防止未经授权的第三方获取或滥用这些信息。为了增强金融大型模型的隐私保护能力,可以采取以下技术策略。

数据加密:对数据在存储和传输过程中进行加密处理,即使数据被非法截获,也能确保其内容不被未授权的第三方解读。

访问控制:实施严格的访问控制措施,确保只有获得授权的人员才能访问到敏感数据,并通过角色为基础的访问控制分配不同的权限级别。

隐私保护技术:运用同态加密、安全多方计算等技术,在数据加密状态下进行计算和分析。通过数据加噪技术,限制模型输出对训练数据的敏感度,防止攻击者通过模型输出推断出具体的数据信息。

联邦学习:联邦学习允许数据在加密状态下共享和学习,数据在物理位置上不离开本地,实现数据的间接共享,使得模型能够在不暴露原始数据的情况下进行训练和更新,从而保护数据隐私。

模型水印和指纹技术:为了防止模型被非法复制或滥用,可以通过模型水印和指纹技术来保护模型的知识产权,这些技术有助于追踪模型的来源和使用情况。

4. 公平性

金融大型模型的公平性指的是在处理金融数据和提供服务时,模型能够对所有用户一视同仁,不会因为用户的年龄、性别、种族、地区等与金融无关的因素而产生不公平的对待或偏见。缺乏公平性可能导致模型出现性别歧视、种族

偏见、宗教偏见、文化偏见、地域政治偏差、刻板印象等不利于社会的问题。为了提高金融大型模型的公正性,可以采取以下技术策略。

数据集的均衡性和多样性:应确保用于训练的数据集具有广泛的代表性,包含多样化的样本,以避免模型因数据偏差而学习到不公平的模式。

上下文学习:利用上下文学习的能力,对大型模型进行调整,以减少或消除已知的偏见,确保模型的决策更加公正。

人类反馈强化学习:通过人类反馈来调整和优化模型的输出,使其与人类的伦理道德和价值观保持一致,确保模型的回应既可靠又不会造成伤害。

5. 可解释性

金融大型模型的可解释性指的是用户能够清晰地理解模型的工作原理和决策依据,这是确保人工智能透明度和可追责性的关键特性。鉴于金融决策通常涉及巨额资金和敏感信息,因此对模型的信任度和透明度有着极高的要求。为了确保金融大型模型的决策过程和结果是清晰、易于理解的,用户和监管机构需要能够明白模型是如何做出特定决策的。为了提高金融大型模型的可解释性,可以采取以下技术策略。

采用可解释的算法:选择或设计具有高可解释性的算法,如决策树和线性回归模型,这些模型的决策逻辑通常更直观易懂。

局部和全局解释方法:运用局部可解释性技术(例如LIME、SHAP)来阐释单个预测的结果,以及使用全局可解释性技术(如SHAP、EBM)来分析模型的整体行为模式。

基于梯度的可解释方法:通过分析模型输出与输入特征间的梯度关系,来评估特征的重要性,从而解释模型的决策依据。

可视化技术:利用可视化手段帮助用户理解模型的内部工作机制和决策影响因素。通过展示特征重要性图表、决策流程图等,使用户能够直观地把握模型的运作原理。

(二)金融大模型安全框架

金融大模型安全框架(图2)是从全局视角剖析大模型训练、生产及应用中存在的安全风险问题,为大模型的研发及应用提供安全指导,其安全目标是构建可信、可控、可解释、可溯源的金融大模型,安全框架主要包括大模型安全管理、数据安全、模型安全、环境安全和攻防安全。

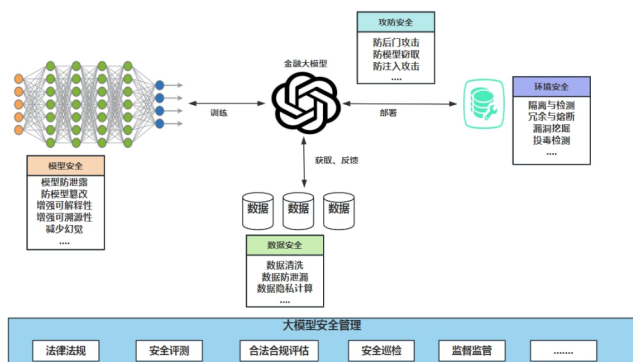


图2 金融大模型安全架构

金融大模型安全管理可以分为大模型安全管理、数据安全、模型安全、环境安全和攻防安全这几部分。

大模型安全管理:整个框架的核心是大模型安全管理,它涵盖了法律法规、安全评测、合法合规评估、安全巡检和监管监督等方面,确保金融大模型在法律和监管框架内安全运行。

数据安全:数据在收集、处理和存储过程中,需进行数据清洗、防泄漏和隐私计算,以保护数据的完整性和隐私。

模型安全:在模型的设计和训练阶段,需实施包括模型防泄漏、防篡改、增强可解释性以及模型可视化等安全措施。

环境安全:模型部署和运行的环境应实施隔离与检测、完整性校验、漏洞挖掘和投毒检测等措施。

攻防安全:在网络环境中,金融大模型需要防范后门攻击、防数据窃取和防注入攻击。

表2 大模型安全管理

法律法规	大型模型的安全治理需要依靠国家层面的法律和规章来制定和执行相关政策。
安全评测	通过安全评测来检测并保证大模型的安全和可靠，如：固定数据集测评和红队模型测评。
合法合规评估	基于法律法规和标准来评估大模型是否合理。
安全巡检	定期开展对大型模型研发和应用过程中涉及的核心资产与关键基础设施的安全检查，以保障模型在整个生命周期内的安全性。
监管监控	实施对大型模型输出结果的持续监督与管理，确保其生成的内容既安全又符合相关法规要求。

表3 数据安全

数据清洗	通过高效地筛选和清洗预训练数据，包括安全数据和金融数据，可以显著减少模型输出可能导致的有害内容和隐私泄露风险。
数据防泄漏	通过识别和分类数据，可以制定相应的策略来预防敏感信息和隐私数据的外泄。
数据隐私计算	可以通过实施差分隐私和同态加密等技术手段来确保数据隐私的安全。

表4 模型安全

模型防泄露	采用模型结构防御、信息混淆防御和查询控制防御等策略，可以最大限度地减少或隐藏模型训练和测试期间交互数据中的敏感信息，从而降低大模型在这些过程中的信息泄露风险。
防模型篡改	利用访问控制和加密技术可以防范模型被篡改和滥用的情况发生。
增强可解释性	提升大型模型的可解释性是其整个生命周期内的一项关键任务，这可以通过确保建模前数据的可解释性、开发具有内在可解释性的模型以及对现有模型进行可解释性分析来实现。
增强可溯源性	确保大型模型生成的内容可以追踪到其数据来源是至关重要的，这种可追溯性对于验证信息的真实性和提高透明度非常关键。通过实施溯源检测和归因分析等技术，可以增强模型输出内容的可追溯性。
减少幻觉	为了降低大型模型产生的错误或不真实的输出，即所谓的“幻觉”，可以采用多种技术手段，如诚实导向的微调、强化学习、对比解码、上下文预训练以及检索增强等方法来实现。

表5 环境安全

隔离与检测	实施不同模块间的权限隔离并严格控制访问权限，能够在一定程度上降低遭受攻击的风险。此外，在系统中部署持续的监控和入侵检测机制，结合对网络安全状况的综合分析，能够及时评估系统的威胁等级，从而有效提高对安全威胁的响应能力。
冗余与熔断	冗余策略涉及同时构建和部署多个模型，这样做可以降低系统在面对单一攻击时彻底崩溃的风险，增强了整个系统的稳定性。而熔断机制则是指在大型模型的输出内容出现高错误率时，立即切换到人工干预和处理流程。
漏洞挖掘	通过识别大型模型中存在的完全漏洞，并对这些漏洞进行详尽的分析来评估它们可能带来的影响，然后实施相应的措施进行修复，可以有效降低潜在的网络安全风险。
投毒检测	对数据、预训练模型、开源组件等进行定期的安全审查，并迅速解决检测过程中发现的安全问题，可以有效降低潜在风险。

表6 攻防安全

后门攻击	鉴于大型模型是构建于神经网络之上，并且主要由参数集组成，这使得在大型模型中隐藏后门的难度比传统系统更高。为了防范后门攻击，可以采用模型剪枝和输入预处理等技术手段。
模型窃取	模型或训练数据的窃取攻击是指攻击者通过发送查询并分析系统的响应以及其它可观察的信息，来推断系统的模型参数和训练数据。为了防止这类窃取行为，可以采用差分隐私技术、为模型添加水印、以及实施隐私保护的聚合学习等措施。
注入攻击	利用安全检测方法，可以识别大型模型在实际应用中是否面临提示注入、对抗性攻击和隐私侵犯等安全威胁。

五、总结与展望

当前金融领域的大型模型尚处于发展初期，存在不少安全漏洞和潜在风险。预计随着深度学习技术的不断进步和研究的深化，未来这些大型模型在攻防对抗中将经历持续的迭代升级。金融大型模型将面临层出不穷且日益复杂的新型安全威胁。因此，迫切需要构建一个全面且统一的安全评估体系，探索有效的防护策略，实现对金融模型的安全监管和可控发展，推动构建一个健康安全、成熟稳固的大模型生态系统。

大语言模型在证券业开发安全领域的探索与实践

谢朝海、齐大伟、谢琪、丁延彪 | 海云安网络安全技术有限公司

摘要：在证券业安全开发领域中，存在着传统代码检测工具漏洞误报率高，研发人员漏洞理解和修复效率低等痛点问题。为了有效解决上述痛点问题，以微调和优化大模型为技术思路，深入研究和探索了大模型在该领域内的应用，为其在开发安全方面的应用积累了宝贵的实践经验。本项目覆盖了AI大模型、智能算法、Agent应用、SAST等相关技术，是大模型的应用的完整案例，可为大模型在金融机构的IT应用提供创新性示范作用。本研究对证券领域内乃至整个金融行业都具有一定的价值，可为开发者赋能，帮助企业实现降本增效，预估一套应用可赋能10名架构师，协助100名开发者大幅提升安全能力，平均提升项目开发编码效率达10%-15%，为千名开发者的金融机构每年节约累计上百万元的开发成本。

关键字：大语言模型、开发安全、安全左移、AI智能修复、AI误报优化

一、引言

近年来随着证券行业的业务和技术快速发展以及DevOps敏捷开发框架等新技术的出现，开发者既要快速交付满足业务发展需求，又要确保代码的安全性和合规性，满足监管要求成为了业务典型的痛点问题。本文对AI大模型在开发安全领域进行技术探索及实践，帮助开发者在开发编码环境直接进行代码和组件安全漏洞与合规风险扫描，并通过借助AI大语言模型，引入AI降低误报、AI生成缺陷成因解释、AI一键修复功能、自动补全代码、交互式快速智能问答等能力，帮助企业整体提升研发效能，助力企业实现安全合规、降本增效的目标。

二、证券行业安全开发领域国内外建设情况

国内近年来随着金融科技投入的持续增长，在大数据、云计算、人工智能等前沿技术的引领和金融数字化转型的驱动下，科技服务已融入金融业务的方方面面，金融科技治理水平全面提升。与此同时，金融机构面临的威胁和挑战也在持续升级，黑客攻击逐渐向专业化、组织化转变，安全攻击事件不断。在众多不同类型的安全风险事件中，企业自主研发或外购的应用软件更容易出现安全漏洞，根据新思科技发布的《2023年软件漏洞快照》报告，2020—2022年，92%的被测应用软件存在风险和漏洞，其中，27%存在高危漏洞，6.2%存在关键高危漏洞。国内金融企业开发安全现状主要表现为4点情况。第一是开发安全建设规划不清晰；该安全是一项系统性、复杂性的长期工作，内容涉及安全组织、安全体系、规范制度、流程平台、安全工具、人员能力等

多个方面。如果没有清晰的规划，寄希望于渗透测试服务、安全产品采购等“突击式项目”解决问题，将无法达到全面、有效的管控目的。第二是未建立融入研发团队的安全组织；开发全生命周期体系更需要所有研发人员共同参与。如果安全团队未能融入研发团队，将面临“孤立无援”、与开发“冲突对立”等困境。第三是金融机构业务复杂，应用系统数量众多，应用安全漏洞层出不穷，缺少“安全左移”机制，将导致安全漏洞发现较晚，漏洞修复成本更高。第四是监管要求严，合规标准多；金融行业属于强监管行业，相关的法律法规、监管规范、行业标准众多，如何有效开展研发安全领域的“外规内化”工作，确保应用系统高标准满足监管合规要求，实现“研发内生合规”目标，一直是金融机构关注的重要问题。

自开发安全的概念提出以来，国际社会对软件开发过程中的安全性给予了高度重视。出于对软件供应链的安全性和脆弱性的担忧，多年前多国便开始规划国家软件开发安全策略，出台了一系列相关政策和重点项目，以便加强软件供应链的安全控制。开源软件作为软件供应链中最重要的部分，世界上许多知名企业都在加大对软件研发的安全风险管理，并利用开源软件的软件构件分析技术，确保第三方开源构件的安全。

三、证券行业安全开发领域现状与痛点分析

随着证券行业的业务需求不断增长和信息技术的快速发展，呈现出网络安全威胁演变快、网络攻击大幅增加、数据泄露事件频发等特点。证券公司成为黑客攻击的频繁目标，其攻击手段不断升级，从分布式拒绝服务(DDoS)攻击到

复杂的持续性威胁(APT),严重威胁着企业及客户的数据安全。

国家及证券行业对数据安全和个人信息保护的重视程度前所未有,陆续发布一系列法律法规及行业监管要求,加大数据安全和隐私合规领域的监管及执法力度,同时针对开发安全也提出了明确的建设要求。《信息安全技术网络安全等级保护基本要求》(GBT22239-2019)中要求企业在软件开发中应制定代码编写安全规范,要求开发人员参照规范编写代码,在软件开发过程中对安全性进行测试,在软件安装前对可能存在的恶意代码进行检测;对外包软件开发应在软件交付前检测其中可能存在的恶意代码。《证券期货业软件测试指南 软件安全测试》(JR/T 0191-2020)中提到通过对软件源代码进行安全扫描和审计,定位漏洞代码所在位置。《证券期货业移动互联网应用程序安全规范》(JR/T 0192-2020)中对移动应用开发安全提出要求:移动互联网应用程序在开发时应考虑编码安全性,减少应用程序安全漏洞。中国证券业协会《证券公司网络和信息三年提升计划(2023-2025)》第四条强化系统研发测试管理能力及健全网络和第六条信息安全防护体系中持续提升代码开发效率及安全,深化漏洞全生命周期管控。

在严格监管的大环境下,软件供应链安全成为业内普遍关注的热点话题,如何保障软件在设计、研发、运营等阶段安全成为了业内的痛点,而开发安全是软件供应链安全及其重要的一环,从此安全不再是一个孤立的审查环节,而是需要将安全风险的治理同开发工具、流程进行有效结合,进而实现真正的安全左移。

现如今行业内多数企业,在进行开发安全建设过程中主要存在3个痛点。第一是绝大多数企业在软件产品研发过程中,缺乏高效的安全检测工具,导致系统带病上线,造成了极大的安全隐患;第二是研发人员(因安全意识及编码技能欠缺),对传统安全检测工具发现的漏洞难理解、难修复的典型现状;第三是传统代码安全检测工具在实际应用中存在误报率高、问题定位不准确、缺陷成因描述不清晰等突出问题,导致漏洞修复成本过高。上述痛点严重阻碍了安全向开发侧“左移”,影响了开发安全工作的顺利进行和研发效能的整体提升。

四、相关大语言模型的技术介绍

(一) AI技术的发展

AI技术的发展历经了四个阶段,分别为通用计算装置、逻辑推理专家系统、深度学习计算系统、大模型计算系统。

智能计算的起点是通用自动计算装置(1946年)。艾伦·图灵(Alan Turing)和冯·诺依曼(John von Neumann)等科学家,一开始都希望能够模拟人脑处理知识的过程,发明像人脑一样思考的机器,虽未能实现,但却解决了计算的自

动化问题。

智能计算发展的第二阶段是逻辑推理专家系统(1990年)。E.A.费根鲍姆(Edward Albert Feigenbaum)等符号智能学派的科学家以逻辑和推理能力自动化为主要目标,提出了能够将知识符号进行逻辑推理的专家系统。人的先验知识以知识符号的形式进入计算机,使计算机能够在特定领域辅助人类进行一定的逻辑判断和决策,但专家系统严重依赖于手工生成的知识库或规则库。

直到2014年左右,智能计算进阶到第三阶段深度学习计算系统。以杰弗里·辛顿(Geoffrey Hinton)等为代表的连接智能学派,以学习能力自动化为目标,发明了深度学习等新AI算法。通过深度神经网络的自动学习,大幅提升了模型统计归纳的能力,在模式识别等应用效果上取得了巨大突破,某些场景的识别精度甚至超越了人类。连接智能的应用更加广泛,包括语音识别、人脸识别、自动驾驶等。在计算载体方面,中国科学院计算技术研究所2013年提出了国际首个深度学习处理器架构,国际知名的硬件厂商英伟达(NVIDIA)持续发布了多款性能领先的通用GPU芯片,都是深度学习计算系统的典型代表。

智能计算发展的第四阶段是大模型计算系统(2020年)。在人工智能大模型技术的推动下,智能计算迈向新的高度。2020年,AI从“小模型+判别式”转向“大模型+生成式”,从传统的人脸识别、目标检测、文本分类,升级到如今的文本生成、3D数字人生成、图像生成、语音生成、视频生成。大语言模型在对话系统领域的一个典型应用是ChatGPT,它采用预训练基座大语言模型GPT-3,引入3000亿单词的训练语料,相当于互联网上所有英语文字的总和。

(二) 大语言模型关键技术概述

大语言模型的关键技术包括Transformer架构、预训练、微调、提示工程。

Transformer架构是目前语言大模型采用的主流架构,其主要思想是通过自注意力机制获取输入序列的全局信息,并将这些信息通过多层网络进行传递。

预训练是一种深度学习模型训练的策略,目标是使用尽可能多的训练数据,使得模型学习到尽可能多的共性特征,从而让模型在其他特定任务上的学习负担变轻、表现更好。

由于在大规模通用领域进行数据预训练的原因导致缺乏对特定任务或领域的知识,因此需要适配微调。微调可以帮助模型更好地适应特定需求,可以提高部署效率、减少对计算资源的需求。大模型具备作为通用任务求解器的潜在能力,但这些能力在执行一些特定任务时可能不会显式地展示出来。在大模型输入中设计合适的语言指令提示有助于激发这些能力,关于提示工程技术的分类见图1。

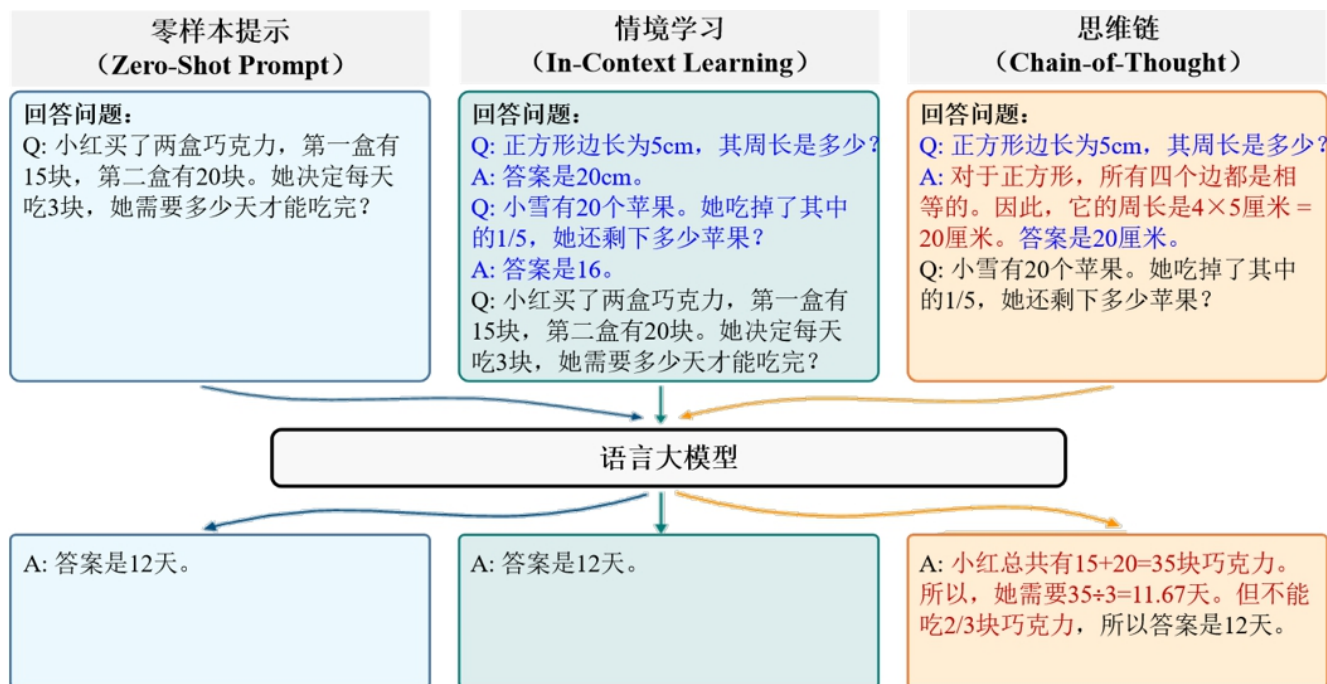


图1 提示工程技术分类

五、AI大模型在证券业开发安全领域的探索

在领域内, 我们通过大模型和SAST工具的有效结合, 对于解决研发难理解和难修复漏洞、白盒漏洞误报率高的问题有相当客观的效果。除此外, 对协助研发人员智能问答、补全代码、生成代码、解释代码、优化代码、为代码生成注释和测试用例方面也取得一定成效。

目前也在积极的探索和模型调优, 期望在误报率优化、AI漏洞智能修复、代码质量问题修复三个方面覆盖更多的语言、缺陷类型和场景。在智能问答功能同当前代码进行关联性探索, 便于用户更加高效的通过AI问答功能咨询源码项目相关问题。

证券公司在开发安全领域的大模型规划, 主要聚焦于IT科技人员, 包括信息安全人员、IT运维人员, 最重要的是研发人员。通过一系列AI相关技术的探索和应用, 深度同白盒检测工具结合起来, 重点打造的AI能力包括AI优化漏洞误报、AI解释漏洞、AI智能修复漏洞、AI生成代码、AI生成注释、AI解释代码、AI代码优化以及智能问答等方面, 主要应用到AI相关技术包括大模型训练、微调、RAG优化大模型、基于长期积累的安全开发知识库和提示工程对通用大模型调优, 智乘AI安全开发大模型总体框架件见图2。

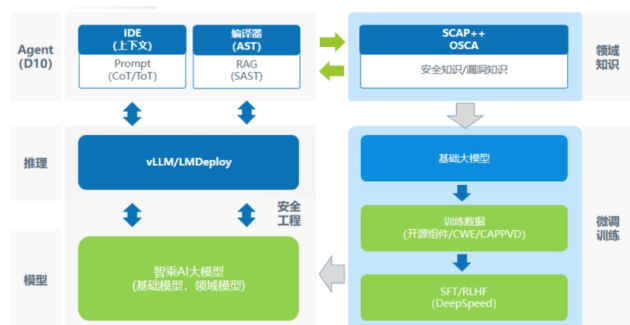


图2 智乘AI安全开发大模型总体框架

(一) AI大模型选择

基于开发安全领域面临的核心痛点, 选择了多种知名的大模型作为自己的底座模型, 充分融合了各模型的优势。选择策略主要包括三个, 第一是参数适量, 最大限度的降低成本、第二是能够支持本地私有化部署、第三是产品的性能要稳定可靠, 适合处理代码数据, 大模型选择策略见图3所示。

大模型底座选择策略



参数适量, 成本低

考虑性价比, 避免不必要的浪费



私有化部署

通用基础大模型可支持本地私有化部署



性能

产品的性能要稳定可靠, 适合处理代码数据

	HumanEval (0)		MBPP (3)	
	k=1	k=100	k=1	k=80
GPT-J ^a	11.6	27.7		
LaMDA ^{bc}	14.0	47.3	14.8	62.4
PaLM ^d	26.2	76.2	36.8	75.0
GPT-NeoX ^d	15.4	41.2		
BLOOM ^e	15.5	55.5		
LLaMA ^e	23.7	79.3	37.7	76.8
GPT-4	67.0 ^f /82 ^g			
LLaMA 2 ^h	29.9	89.0	45.0	81.5
Phi-1.5 ⁱ	41.4		43.5	
Baichuan 2 ^j	17.1		30.2	
Qwen ^k	32.3		40.8	
Codex ^a	28.8	72.3		
PaLM-Coder ^b	36.0	88.4	47.0	80.8
PaLM 2-S ^{kl}	37.6	88.4	50.0	86.8
Code LLaMA ^m	53.7	94.7	56.2	
CodeFuse ⁿ	74.4		61.0	

图3 大模型选择

(二) AI大模型训练

大模型的训练要求精心规划和充足计算资源,如多个GPU。首先需要构建高效的数据管道以快速处理大量数据。其次是设计合适的模型架构,初始化参数,并选择适合大规模训练的优化器。分布式训练成为常态,需合理分配数据和模型参数以平衡负载。在训练过程中,持续监控损失函数和性能指标,适时调整超参数和正则化手段防止过拟合。最后,定期在验证集上评估模型,并根据反馈进行迭代优化,直至达到预期性能。训练完成的模型应经过测试集检验泛化能力后才能部署应用,详细的大模型训练流程见图4。

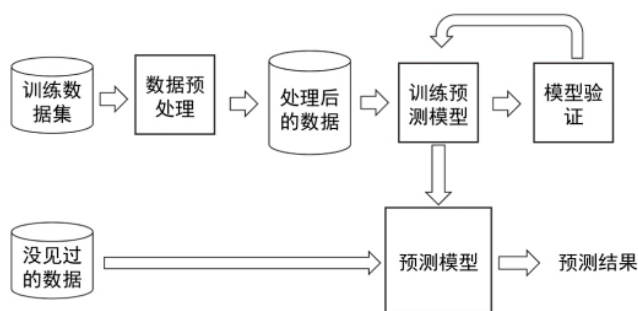


图4 大模型训练流程

大模型主要的训练数据包括开源组件安全数据、CVE/CWE公开漏洞数据、自挖掘漏洞数据以及实际多年来开发安全相关产品积累的场景数据。同时,利用数据蒸馏技术,实现了用大模型训练小参数模型的目的。具体数据蒸馏的步骤是查询样例生成、LLM response检查、中小模型训练,最终实现了高效训练符合业务场景,能够解决关键痛点问题的特定模型。

(三) 大模型微调

为了更好的优化AI智能修复漏洞和降低漏洞误报的效果,我们尝试对大模型基于实际业务场景进行微调。微调的主要优势在于其能够针对特定专业领域调整LLM的行为,从而赋予模型相应的专业能力。例如,我们使用开发安全领域特定数据来进行微调,使模型的行为更加贴近开发安全专家。具体而言,我们利用微调优化了去误报和漏洞修复的效果。

微调包含全参数微调(Full Parameter fine-tuning)和部分参数微调,其中部分参数微调包含诸如Adapter-tuning, Prefix Tuning, Low-Rank Adaptation等方法。微调策略主要包括三部分,第一是可用的标注数据量;第二是可用计算资源,例如时间、内存和处理器;第三是模型性能的具体期望。微调的过程包括配置微调参数、启动微调过程、模型评估和调优。详细大模型微调说明见图5。



图5 大模型微调说明

(四) RAG技术的应用

相较于微调,RAG则通过在大模型生成响应信息之前从知识库中检索相关信息来增强LLM的能力。因此,RAG技术更适用于需要查询数据库、文档或其他结构化/非结构化数据存储库的应用场景。当需要连接外部数据源、数据更新频繁且训练数据准备困难时,RAG技术便成为理想之选。例如,在构建一些知识问答系统时,RAG技术可能更具优势,比如我们在智能问答的功能上,尝试嵌入RAG技术。再比如,当AI生成的代码需要符合客户的编码规范或使用客户内部的公共函数时,通过RAG接入客户的编码规范知识库或者API文档库等。因此,在选择使用微调、RAG或两者结合的方式时,需根据具体场景进行评估。在实际应用中,需要综合考虑训练数据情况、应用场景需求以及模型性能要求等因素,以确定最佳的优化策略。一般建议在深入微调之前尝试使用RAG,这主要是因为RAG在复杂性、成本方面相对较低。

(五) 基于提示工程进行模型调优

我们以长期积累的安全开发知识库数据为训练源,基于提示工程对模型进行调优,首先涉及从知识库中提取关键安全信息并转换为适合模型训练的数据格式,之后再通过数据预处理确保这些信息与模型兼容。同时需要选择合适的大模型架构,并根据安全任务需求对模型进行调整。最重要的是定义明确的训练目标和评估指标后,利用这些专业数据微调模型,并通过迭代训练来优化其性能。最后,根据实际应用中的反馈继续迭代优化,使模型漏洞智能修复和误报优化更加精准和可用。详细大模型调优的流程见图7。

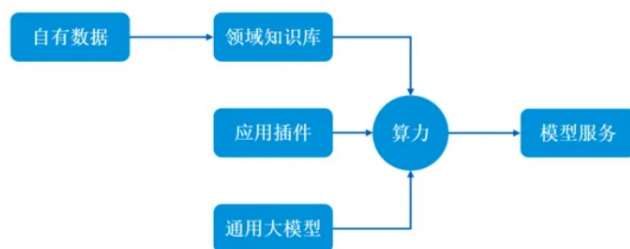


图7 大模型调优流程

六、AI大模型在证券业开发安全领域的应用实践

开发者安全助手(D10)是基于丰富的开发安全专家经验和人工智能AI技术全方位赋能开发者的一套工具,赋能开发者在开发过程中实现代码补全,并实时发现和自动修复代码安全漏洞。D10通过对高敏捷信创白盒检测工具和开源组件应用安全检测系统的无缝对接,并在前端通过IDE插件方式对代码和组件依赖库进行实时漏洞扫描检测代码和组件依赖库安全性,实现即写即测,在AI大模型的加持下,开发者安全助手更加精准的发现潜在的安全漏洞、提供针对性的漏洞解释及自动修复功能。开发者安全助手(D10)整体架构见图8。

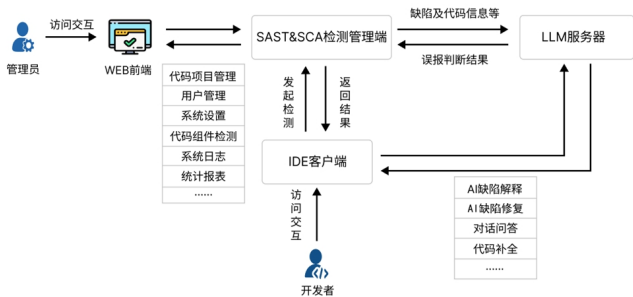


图8 整体架构

(一)AI降低误报

通过利用AI降低误报,开发者安全助手解决了传统工具误报率高的问题,漏洞缺陷准确率可提升到90%以上,帮助快速实现代码缺陷闭环,提高了开发效率,降低了安全成本。AI自动过滤误报的效果见图9。

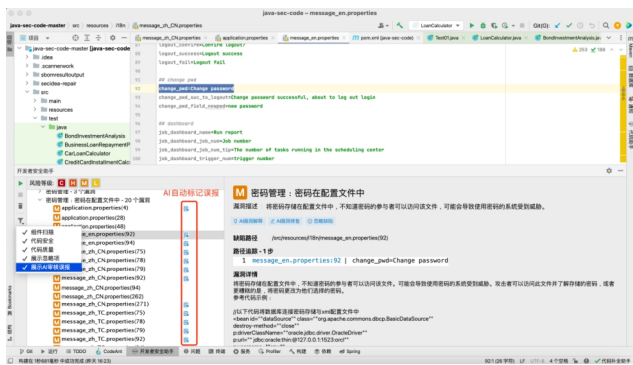


图9 AI自动过滤误报

(二)AI生成缺陷成因解释

针对缺陷成因理解难的问题,开发者安全助手通过AI技术,利用用户代码上下文生成一对一的缺陷成因解释,为开发者直观地分析和理解问题提供更好的帮助。AI生成缺陷成因解释功能如图10所示:



图10 AI生成缺陷成因解释

(三)AI自动生成修复代码

针对开发者不熟悉缺陷修复方法的问题,开发者安全助手利用AI技术自动生成修复代码,实现一键修复漏洞,大大降低修复难度。AI自动生成修复代码功能如图11所示:

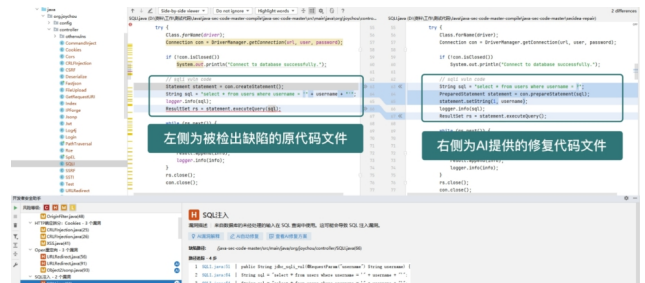


图11 AI自动生成修复代码

(四)AI自动补齐代码

通过对上下文逻辑关系的分析,实时生成补全代码,为研发人员提供参考。支持单行续写和多行续写,在编码过程中短暂停顿,即可实时获取助手推荐的代码。若认为推荐内容合适,可使用tab键采纳代码。此外,还支持注释生成代码,即针对注释内容自动生成相应的方法、函数、判断、循环体等完整代码块。详见效果见图12所示。

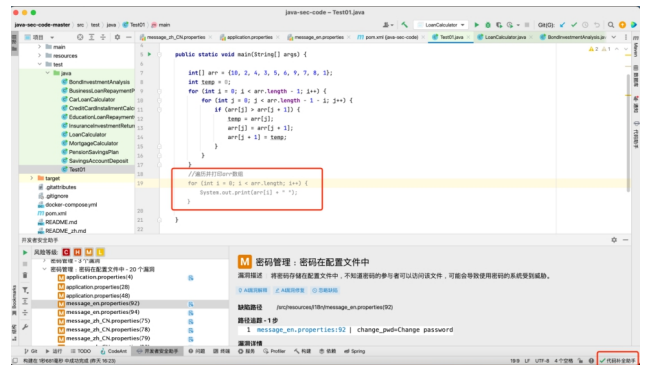


图12 AI自动补齐代码

(五)AI智能交互式问答

基于海量研发文档、产品文档、通用研发知识、SDK/OpenAPI文档等进行问答训练,提供本地化的大语言模型对话功能,为开发者答疑解惑,助力研发人员轻松应对挑战,在提升研发效率的同时保障数据安全。详细效果见图13所示。

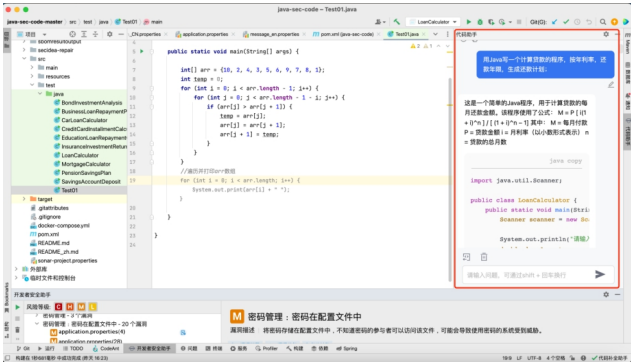


图13 AI智能交互式问答

七、行业应用推广

(一) 实际应用场景

表1

场景分类	场景描述	价值
安全合规	敏捷开发流程，追求检测效率、准确和便捷使用，同时要求降本增效	帮助研发团队在代码上线前快速查改安全漏洞，提高安全性，降低整体开发成本，保障版本如期发布。
	安全左移，开发自治，对安全及合规有较高要求	对于大型自研企业，应用系统数量多，检测频繁，传统代码安全审计已经无法满足。在每次发版进行人工对检测结果进行审核分析和把关，通过开发自治模式赋能和授权开发人员对检测结果进行分析和漏洞缺陷修复闭环。
研发效能	大幅提升研发人员的编码效率和质量规范性	研发人员能够利用 AI 生成、解释、翻译、优化代码，同时能够生成代码注释及测试用例、用户智能问答以满足研发人员日常开发的需求，真正提升研发效能。

(二) 产品使用及配套资源说明

产品支持灵活的使用方式，第一是可以采用订阅式，直接通过分配的账号登录SAAS环境，在IDEA、VSCode等开发工具安装D10客户端插件后，即可使用体验。客户端插件相关说明如下：

表2

支持开发工具	支持版本
Visual Studio Code	2023.10(1.82.2)—2024.1(1.86.0)
Android Studio	4.2.0—Hedgehog 2023.1.1 Beta 1
CLion	2020.2—2023.2
GoLand	2020.2—2023.2
PyCharm	2020.2—2024.1
WebStorm	2020.2—2024.1
IntelliJ IDEA	2020.2—2024.1
PhpStorm	2020.2—2024.1

第二是支持私有化产品部署，当前兼顾到大部分操作系统，GPU、CPU等信创资源。开发者安全助手需要部署在客户方的开发或生产环境，为了防止核心资产以及敏感信息泄露，需把开发者安全助手所在网络环境与外网隔离（部署在内网环境中），相关资源配置要求见表3所示：

表3 私有化部署资源说明

类别	配置	参数	说明	备注
服务器	GPU	RTX4090 * 2	用于 AI 引擎分析计算，如同时使用自动补全代码功能的开发者数量比较多，则需要横向扩展 GPU 的数量。目前已适配英伟达 RTX 40 系列的 4090、A 系列和 H 系列，每套服务器需配置 GPU 数量为：24GB*2。	信创适配： 一、CPU 1. 海光 c86， 7000 系列 (7380) 2. 鲲鹏 ARM， 920 3. 飞腾 ARM， FT2000/64 二、操作系统 1. 银河麒麟(V10) 2. 中标麒麟 3. 统信 UOS(V20) 三、数据库 1. GaussDB for MySQL 2. TDSQL for MySQL 3. 达梦数据库 四、GPU 1、海光 DCU 2、华为昇腾
	CPU	16 核		
	内存	128G		
数据存储	1T			

八、技术示范性创新

(一) 技术应用创新

■ 跨IDE和编译器上下文提示工程信息获取技术。不同IDE/编辑器在编程语言解析能力差别大，影响上下文生成质量，需要靠架构补齐差异。提示工程获取技术流程详见图14所示。

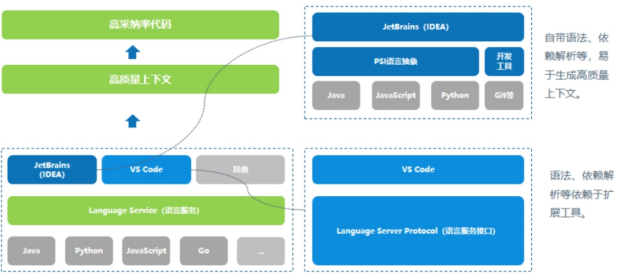


图14 提示工程获取技术流程

■ 研发安全与质量问题自动修复代码生成。自动修改OWASP TOP 10,SANS TOP 25等众多中高危漏洞和代码质量问题。自动修复漏洞效果见图15所示。

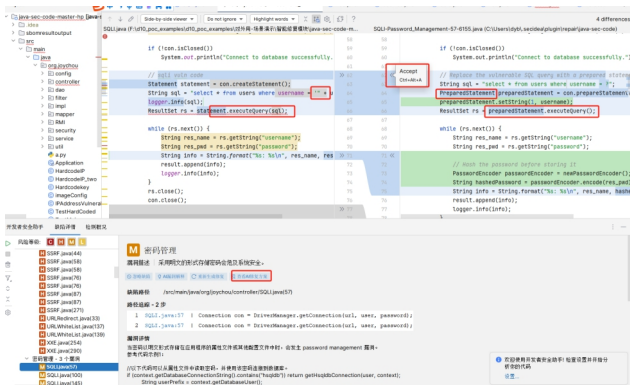


图15 自动修复漏洞效果

■形成开发者Agent,在IDE中全方位赋能开发者。在IDE中形成检测发现问题->上下文分析问题->自动一键修复问题的技术闭环。详细开发者赋能流程见图16所示。

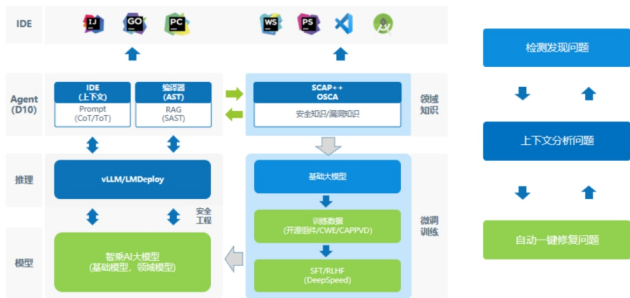


图16 AI全方位赋能开发者流程

(二) 大模型创新

为解决开发安全领域漏洞误报率高、修复效率低等痛点问题,我们对通用大模型的进行了系列探索研究,进行了两点创新。第一是自动生成开发安全专业领域训练语料和评估测试集,并研发了训练数据自动标注生成方法,从千万开源代码无标注数据自动生成高质量标注数据。第二是形成开发安全私有专属领域模型,开发了基于千亿参数大模型来训练开发安全私有专属领域中小参数大模型的方法,实现了大多数用户用得起、用得好的大模型的目的。

九、相关案例效果

AI 在金融领域的应用已经成了行业的热点,从智能营销、智能客服、智能投顾、智慧风控到信贷审批,AI技术正在改变金融行业的传统业务模式,提高服务效率,降低运营成本,同时为消费者带来更加便捷和个性化的金融服务。目前国内金融企业科技部门都在拥抱AI,尝试将AI大语言模型技术应用于金融领域的方方面面。而将AI大语言模型在研发安全领域进行应用,可以真正意义上将开发安全工作左移至编码阶段,帮助团队更早的发现代码安全和质量问题。以下是本研究应用在漏洞检测准确性、代码漏洞下降情况和

整体研发效能提升的效果展示。



图17 提升效果对比

十、社会及经济效益

(一) 经济效益

- 提高效率,节省成本:开发者安全助手可以提高开发效率,通过AI能力可以减少开发者在解决安全问题上的时间成本,从而为金融企业节省大量的人力和时间成本。
- 降低风险,避免损失:通过降低由于安全问题引发的风险,可以避免企业避免潜在的经济损失。
- 经济效益测算:以整体研发效能提升指标进行计算,研发效能提升10%,意味着可以节省10%的人力成本。

(二) 社会价值

- 安全防护与风险管理:及时发现、防范和应对潜在的网络安全威胁,保障金融机构和用户的敏感信息安全。
- 提升金融科技业务效率:在研发编码阶段执行一系列安全合规和质量检测任务,提高研发编码工作效率,减轻人工负担,更专注于核心业务实现。
- 促进金融科技业务创新:支持金融科技发展,开发者安全助手项目作为一项创新技术,推动金融科技的发展,为金融行业注入新的动力和创新活力;
- 促进数字化转型,助力金融机构实现数字化转型,提高业务的数字化程度,使得金融服务更加便捷、高效,推动整个金融体系朝着数字化智能化的方向发展。

十一、总结与展望

证券行业对IT系统的安全合规和业务需求研发效率均提出了严格的要求,通常为满足安全合规和业务需求研发效率的要求,需要投入过多的人力和经济成本。本文基于安全风险治理效率低下这一痛点,对AI大模型相关技术进行了探索和实践,为大模型在证券公司开发安全领域的落地积累了宝贵的经验。未来随着AI技术的进一步发展,融合AI大语言模型能力的开发者安全助手,能够为全行业软件产业的发展带来更大的价值,譬如帮助企业最大限度的保障系统安全和合规、提升研发效能,最终实现降本增效。

参考文献

- 1.桑基韬,于剑.从ChatGPT看AI未来趋势和挑战[J].计算机研究与发展,2023,60(06):1191-1201。
- 2.天翼智库.迎接大模型时代:大模型发展简史及攻略[J].互联网天地,2023(05):8-15。
- 3.中国工程院院士孙凝晖《人工智能与智能计算的发展》

04 思考和观点

P68 基于全景数据流转论金融行业数字供应链方法论

侯亮、郑洲豪、翁伟刚、周雪翎

P72 数字安全风险内控与合规教育评价指标体系

王怀宾

P75 "RSAC 2024聚焦AI安全：证券行业面临大模型安全新挑战"

康乐、盛浩月

P79 网络攻防新背景下的高质量漏洞运营

樊兴华

P83 证券行业分支机构 IT 降本增效方案

白昆忠

基于全景数据流转论 金融行业数字供应链方法论

侯亮、郑洲豪、翁伟刚、周雪翎 | 国泰君安证券股份有限公司

摘要：在数字化时代，数据的价值已经被全面认识，保护数据的流动成为了金融行业竞争力的关键之一。本文探索金融行业供应链安全的战略实践和理论架构，通过多维策略如风险管理、标准制定与技术控制等，构建基于全景数据流转的安全体系，全面提升供应链安全防护能力。

关键字：供应链安全、主动防护、数据安全、安全运营、开源软件安全

一、引言

在金融行业的数字化演进中，数字供应链已迅速从一个支撑功能转变为核心战略要素。源于数据流转不仅是价值交换的媒介，更是维系整个金融行业在数字化背景下的基石，而供应链在数据流转过程中承担着至关重要的角色。但当前金融行业在数字供应链的方法论方面仍显薄弱，尤其缺乏一个全局的、以数据流转为核心的系统性全局方法论。

针对这一缺口，本文提出了一个创新性的解决框架。该框架深刻理解在数字化浪潮下，数字供应链不仅包括保护静态数据的问题，更是确保动态数据流转安全的挑战。从数据生成、传输、使用到最终销毁的每一个环节，都应被纳入全景数据流转的视野内。基于全景数据流转视角审视的（本文简称全景路径）数字供应链方法论的提出，不仅提升了数字供应链的重要层次，更将其定位在保障金融行业稳定运营和可持续发展的核心位置之一，标志着金融行业在数字化时代数字供应链思维的重大进步。

二、数字供应链建设面临的挑战与难点

为应对多维度的挑战并适应未来的发展趋势，相关部门和监管机构近年来陆续出台了数字供应链相关的法律法规和行业规范，包括《关键基础设施保护条例》《网络安全技术 软件供应链安全要求》《关于银行业保险业数字化转型的指导意见》等，对供应链的采购、审查、安全能力建设等都提出了要求。但在实践中，数字供应链建设往往面临以下难点。

内部资产梳理困难：金融机构拥有庞杂的资产采购、服务采购、自研源代码、开源组件、开源应用软件、终端软件等相关数字资产，缺乏系统化的数字供应链资产台账，统一化管控异常困难。

安全评估缺失：供应商的安全资质不统一，软硬件安全评估报告缺失。传统的安全验收方式覆盖的检测场景和能力范围有限，难以持续开展全面的安全风险评估活动。

技术控制效果差：面对多渠道来源的供应链风险，安全工具往往只能针对特定类型的威胁进行防护，难以实现全面覆盖。尤其在面对新型和未知的安全威胁时，安全工具的效果往往大打折扣。

缺少体系化方法：数字供应链建设是一项复杂而庞大的工程，涵盖供应商管理、风险评估、安全控制、应急响应等多个方面。基于传统网络安全防护方案难以以全局视角实现风险闭环。

三、全景路径数字供应链建设方法论

供应链存在于金融行业的每一个环节，数字供应链建设的目标即是保护其数据和信息流高度流转和集成管理中的安全性。全景路径数字供应链的概念诞生于对金融供应链中各个环节数据流动性和透明度要求的不断提升。全景路径涵盖了从核心系统到外部边界，从风险评估工具到管理软件，以及第三方提供的各种服务和工具等。上述所有节点共同构成数据流转的路径，全景路径数字供应链需要做到保障路径上的每一环都是相对安全的。

全景路径视角下，金融行业的数字供应链是一个多维度的问题，涉及从底层物理硬件到顶层应用程序中的各个关键层面，同时这些层面覆盖可信系统、开源组件、第三方云服务商等多个方面。通过分层分析信息技术架构，确保每一关键层面均能实现设定的安全目标，可以有效应对复杂的数字供应链威胁。具体分类见表格。

表1 多维度安全目标分类

访问类型	访问主体	访问通道	访问客体	主要涉及供应链 TOP3 (敏捷安全)	主要安全工具 TOP3 (稳态安全)
外部客户访问	外部客户	互联网	互联网业务	开源组件、行业软件供应商（含外包人员管理）、通用软件供应商（商业应用）	访问控制（防火墙）、应用安全（WAF）、高可用性（抗DDoS）
内部用户访问	内部用户	内网-互联网	互联网业务	可信系统来源（含补丁）、可信应用软件来源（含补丁）、可信通信设备来源	终端安全（杀毒、EDR）、流量监测（DNS 安全）、办公安全（邮件、IM）
	内部用户	内网-内网	内部业务	可信应用软件安装来源、可信办公软件安装来源、可信硬件移动介质	访问控制（防火墙）、流量监测（NDRIDS、SOC）、应用安全（云原生安全、内网 WAF）
运维管理访问	管理人员	内网	内部业务	可信系统来源（含补丁）、开源组件、行业软件供应商（含外包人员管理）	终端安全（杀毒、EDR）、安全审计（堡垒机）、身份和远程访问（零信任）
系统间访问	业务	跨网	业务	开源组件、行业软件供应商（含外包人员管理）、第三方云服务商（GitHub）	流量监测（NDR、IDS、SOC）、应用安全（API 安全）、主机安全（HIDS、微隔离）
	业务	统一网	业务	开源组件、行业软件供应商（含外包人员管理）、第三方云服务商（GitHub）	主机安全（HIDS、微隔离）、流量监测（NDR、IDS、SOC）、攻击面管理

1、数字供应链理论框架的核心原则

构建全景路径数字供应链方法论时，需要遵循以下五大核心原则，即全面性、层次性、动态性、适应性和预防性。全面性原则要求从全局视角考虑数字供应链的各个层面和涉及主体，确保所有可能的威胁点和脆弱性都得到充分的识别和管理，并确保静态和动态数据在整个生命周期内的安全性；层次性原则强调数字供应链建设应分层次、分阶段进行，不同层次的安全措施应相互补充，形成纵深防御体系，避免单点失效导致整体安全的崩溃；动态性原则要求数字供应链框架必须具备高度的灵活性和适应性，能够及时更新和调整安全策略以应对新出现的威胁，同时安全措施能够实时监测和快速响应安全事件；适应性原则要求在设计数字供应链策略时，应充分考虑业务特性及不同地域的法规要求，灵活调整数字供应链策略和措施，确保安全与业务协调发展以及全球化背景下的合规性；预防性原则强调在安全问题发生前就采取措施，包括对潜在威胁的提前识别和评估、建立完善的风险管理机制、实施严格的访问控制和监控措施、定期进行安全审计和评估等，避免或减少安全事件对业务的影响。

2、结构和组成——标准与规范制定

标准与规范制定为方法论提供顶层设计和指导，可以确保供应链各环节安全措施的一致性和可操作性，有助于将复杂的安全要求转化为具体可操作的措施，提高整体安全水平。基于监管单位发布有关数字供应链要求，结合安全领域先进经验与金融行业特性，定义全局性的安全规划、实施计划和自查合规框架。同时，根据内外部环境的变化，及时调整和更新标准规范、技术方法，确保其始终适应新的安全需求。

3、结构和组成——风险评估和管理

风险评估和管理是方法论的基础，其涉及资产识别、风

险评估和预先管控供应链中可能的风险点。风险管理不是一次性的活动，而是一个持续追踪、评估和更新的过程。这个过程需要充分获取信息资产，通过分类归纳软件服务来源和可信等级对全链路信息建立资产台账进行管理，并根据优先级进行主动性风险评估。

商业软件风险评估：建立和完善商业软件准入制度和流程标准，在商业软件入场前进行安全评估审核。

开源软件风险评估：对组件仓库设置安全准入管控；在 DevSecOps 流程加入安全卡口检测应用的依赖组件；成份分析检测扫描实时监测制品仓库动态风险。

内外部持续风险巡检：部署24小时不间断的安全扫描工具，包括但不限于黑盒（DAST）、灰盒（IAST）和白盒（SAST）。这些安全工具协同工作，对内外部数字供应链资产的风险进行持续监测，确保系统上线前后的安全性得到全面保障。

蓝军/渗透测试风险评估：专业蓝军队伍对内外部供应链风险进行主动漏洞发现，通过模拟攻击，全面评估网络、应用、数据、人员等各个层面的安全风险，制定整体的安全防护策略。利用威胁情报收集，有效覆盖安全工具的能力缺陷。

安全有效性验证：建立有效性验证平台提升现有安全工具的威胁检测与响应水平，通过自动化、多样化的攻击用例，优化安全工具防护策略降噪增效。通过常态化应急响应演练模式，优化安全策略和防御体系，建立安全事件与威胁情报的研判和响应、攻击识别和溯源反制的实战防御等能力。

4、结构和组成——安全技术控制

安全技术控制以数据流转为路径，纵深防御为目标，通过聚合安全工具和技术形成敏捷和稳“泰”安全能力核心。

打造以敏捷安全为核心的主动防护平台，负责上线前的供应链安全检测，并对风险进行常态化主动跟踪。通过建立漏洞威胁情报、漏洞挖掘、安全评审、研发流程风险卡点等能力，构建起主动防护体系。包括持续性收集和分析多源漏洞信息；以渗透测试、漏洞挖掘等手段发现潜在的安全风险；引入安全SDK或库对软件和应用进行有效防护；对供应链产品进行威胁建模和研发流程风险卡点确保产品和服务的安全；对制品仓和镜像仓开展持续安全扫描和门禁管理。在开发和测试阶段通过灰盒（IAST）和白盒（SAST）持续地分析和评估代码安全性。在软硬件实际运行之前预防安全问题的发生，确保软件和应用的安全性和可靠性。

打造以稳态安全为核心的安全运营平台，组建主机及终端防护、流量风险监测、应用安全监测、欺骗防御与威胁情报、资产及风险探测、安全审计等六大安全运营能力形成安全矩阵，负责上线后的安全运营检测，构建韧性防御体系。包括对主机和终端进行全面防护，防止恶意软件和攻击者的入侵；对网络流量进行监测，发现异常行为和潜在的攻

击;对应用进行安全监测,防止应用层面的攻击;通过蜜罐和威胁情报收集,对攻击者进行追踪和防御;通过资产和风险探测,实时掌控网络的安全状况;通过安全审计,对整个防御体系进行检查和完善。六项安全运营能力共同组成运营矩阵,确保企业供应链资产运营安全性。

5、结构和组成——响应计划与恢复策略

响应计划与恢复策略聚焦于事后,确保在信息网络遭受恶意攻击后,尽快恢复信息系统的正常运行及在最大限度范围内减少因系统被攻击所带来的损失。响应计划与恢复策略应包括以下关键部分:识别和确认供应链中的安全事件,制定标准化的报告程序,确保事件能够迅速、准确地报告到相关部门和“高级”管理人员。对安全事件进行初步评估,根据事件的严重程度和影响范围,将事件分类,采取不同的响应措施。设立应急响应团队,明确成员的角色和职责。采取必要控制措施,限制事件的蔓延,保护关键资产和数据。通过技术修复、系统恢复和数据恢复等方法,恢复受影响的供应链环节。制定内外部沟通策略,及时向员工、客户、供应商等相关方通报事件进展和应对措施。确定关键业务和系统的恢复优先级,制定恢复时间表,明确各恢复步骤的时间节点和完成期限。必要时需启动灾备切换流程,保障业务运行稳定性、连续性。

6、结构和组成——文化赋能

安全不仅仅是技术和工具的组合,更是全体员工对安全理念的认知和执行。通过构建常态化、体系化的安全文化的融入,可以有效提升整体的安全意识和防护能力,从而保

障供应链的安全性和稳定性,包括但不限于以下方面:将安全文化融入到日常工作流程中;在新员工入职培训中加入安全教育模块;在日常工作流程中引入安全检查和审计环节;设立安全询问和反馈渠道;举办涵盖网络攻击模拟、数据泄露应急响应及内部威胁应对等多个维度的定期化演习。

7、综合治理结构

数字供应链的综合治理结构是确保数字供应链有效管理和实施的关键。一个完善的综合治理结构需要从战略、组织、制度、技术、文化、协同等多方面进行全方位的布局和实施。战略层面的治理结构首先需要制定明确的数字供应链战略,将其纳入整体安全建设发展战略中,明确各阶段的安全任务和指标,确保数字供应链建设有序推进。同时与有关部门和行业安全政策积极对接,确保合规性和规范性;在组织层面,数字供应链治理结构需建立专门的安全管理组织,明确各部门的安全职责,建立跨部门的协作机制;制度层面的治理结构应建立健全的数字供应链管理制度,完善的风险评估和管理制度,定期进行安全风险评估和审计,建立有效的应急响应机制,确保在发生安全事件时能够迅速响应和处置;在技术层面,建立强大的技术防护体系,完善的安全监控和预警系统,强化安全技术的创新和应用;文化层面的治理结构强调企业安全文化的建设,提升全员的安全意识和责任感;协同层面的治理结构强调供应链各环节的协同和联动,确保供应链上下游企业在安全工作中的密切配合。建立供应链合作伙伴的安全管理机制,明确合作伙伴的安全责任和要求。

国泰君安“韧性·数字安全体系” 1.0

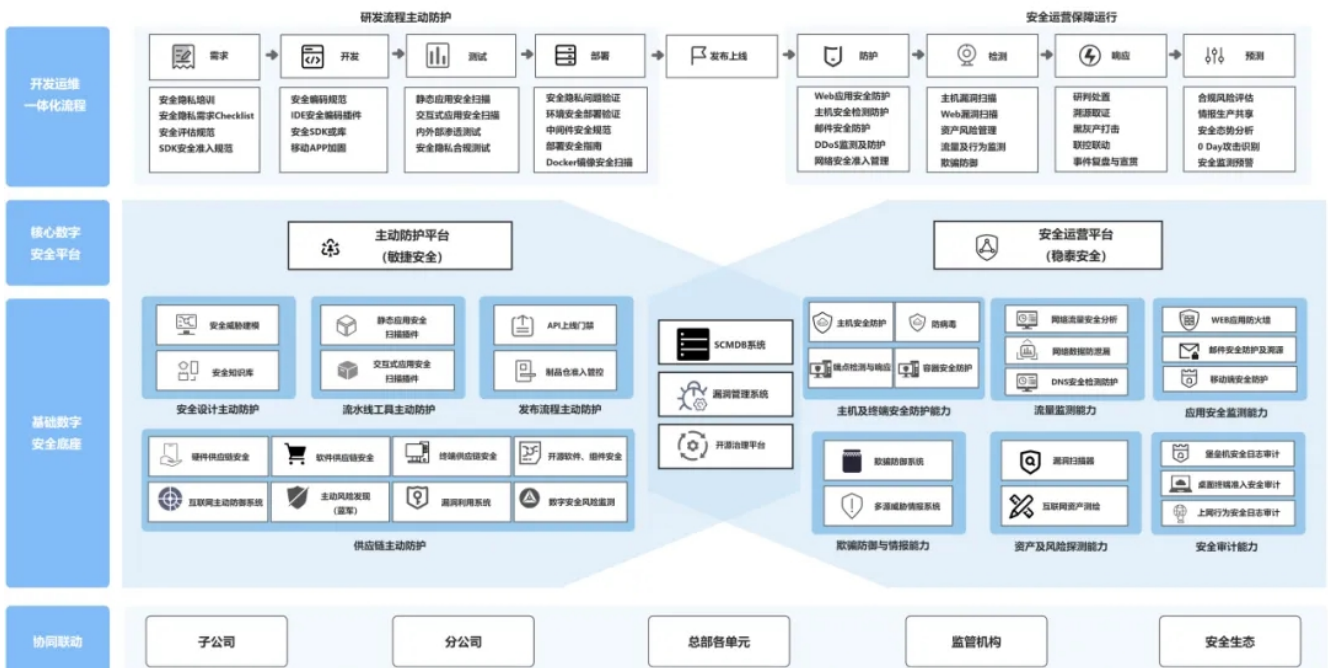


图1 国泰君安“韧性·数字安全体系” 1.0

四、国泰君安韧性数字安全体系实践

国泰君安证券在实践中深知数字安全的重要性和复杂性,面对不断变化的网络威胁和日益严峻的安全挑战,通过以敏捷安全与稳“泰”安全两大核心安全能力作为基础数字安全底座,建立主动防护平台,负责上线前的数字供应链检测,并对风险进行常态化主动跟踪。通过漏洞威胁情报、漏洞主动发现、安全评审和研发流程风险卡点等能力,构建起主动防护体系;建立安全运营平台,组建主机及终端防护、流量风险监测、应用安全监测、欺骗防御与运营威胁情报、资产及风险探测和安全审计等六大安全运营能力,形成安全矩阵。形成基于全景数据流转的数字供应链方法论。通过跨部门、跨条线、跨主体的协同联动,打造韧性数字安全体系,增强整体的安全防护,确保业务连续性和提升应急响应能力。基于敏捷和稳“泰”双核心能力的安全底座,在保障客户信息和业务数据安全的同时,也提升了公司的整体抗风险能力,为公司提供一个强大且具备动态适应性的安全防护网络,应对不断变化的安全威胁,确保业务的稳健发展。

五、总结与展望

数字供应链在金融机构中的战略地位不断上升。在数字化时代,数据的价值已经被全面认识。因此,保护数据的流动——供应链的核心,成为了金融机构竞争力的关键。

展望未来,数字供应链将更多地依赖于智能化和自动化的解决方案。例如,使用机器学习算法来预测和识别安全威胁,自动化的安全运维平台可以提高响应效率;区块链等以其不可篡改和去中心化的特点有望在提高透明度和防篡改方面发挥重要作用;跨行业、跨界的合作将成为常态,通过共享安全情报,共同建设安全标准,共同对抗安全威胁;综合风险管理将从技术层面实施逐渐演变成从整体观、全局观视角上的管理风险,涉及战略、运营、合规和财务等多个方面;此外,数字供应链能力将具备更高的容错能力和快速恢复能力,以应对潜在的中断和威胁。金融机构必须不断创新和调整数字供应链策略,以确保在不断变化的市场中保持竞争力。

数字安全风险内控与合规教育评价指标体系

王怀宾 | 上海市信息安全行业协会

摘要：随着数字化发展，金融证券行业网络安全至关重要。当前数字安全内控与合规教育面临诸多挑战，包括观念薄弱、制度不协调、评价指标体系不完备、技术实现有问题等。美国和欧盟在网络安全教育方面有诸多经验，如立法推动、结合行业应用、强化特定场景教育、加强合作等。为加强风险内控与合规教育，建议夯实制度建设、构建评价指标体系、统一部署及推广教育平台，以提升企业风险应对能力和合规水平，保障网络安全。

关键字：安全意识、内控合规、评价指标、平台化、国际经验

一、概述

11月20日，在2024世界互联网大会乌镇峰会开幕式上，国家主席习近平表示，我们应当把握数字化、网络化、智能化发展大势，把创新作为第一动力、把安全作为底线要求、把普惠作为价值追求，加快推动网络空间创新发展、安全发展、普惠发展，携手迈进更加美好的“数字未来”。

当前，建设数字中国已成为国家发展战略的重要组成部分，如何保障数据安全、促进数字经济发展是事关国家安全、社会稳定和人民福祉的重大问题。其中，金融证券行业的网络和信息安全直接关系到国家金融安全和数字经济稳定，其业务已实现高度数字化。而当今数字安全威胁日益严峻，一直是金融证券行业监管的重点、难点。

从全球网络攻击趋势来看，全球网络犯罪造成经济损失每年高达万亿美元，其中以“人”为突破口发起网络钓鱼、社工攻击、勒索软件攻击等是外部威胁最常用的攻击手法。Verizon发布《2024年数据泄露调查报告》(DBIR)中的数据 displays, 大约68%的网络安全入侵事件与非恶意的人为操作有关，这通常是由受害者受到社会工程学攻击或是操作失误等人为因素导致的。报告强调，虽然控制人为风险因素并不能完全保证网络安全，但如果组织能够有计划地在这人为风险因素控制领域进行投资，就有可能显著减少超过2/3的潜在违规事件。

国家机关与行业的监管部门同样意识到，保障数字安全不仅仅是技术问题，更是人的问题，人员的数字安全意识是数字风险事件的第一道防线。针对金融证券机构，《网络安全法》、《数据安全法》、《金融消费者权益保护实施办法》、《个人金融信息保护技术规范》、《金融数据安全 数据安全评估规范》等法律法规、行业规定均对人员的安全合规与意识教育工作提出了明确要求。

数字安全形势空前严峻，法律法规日趋完善，金融证券

行业组织需要新形势下能够有效落地的以人为本的数字安全治理体系。

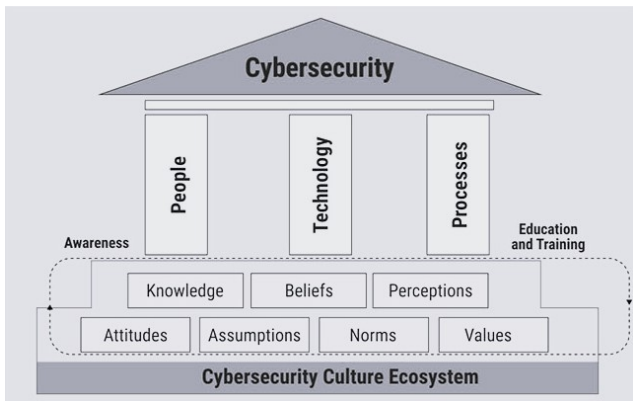


图1 以人为本的数字安全生态示意图

当前组织的安全保护工作有不少短板，重技术，轻管理的问题尤为突出。数字安全生态三件套“人、技术、制度”中，技术是核心要素，管理流程是根本，人员教育是关键，但网络安全隐患“看不到”、安全风险“花样多”、人的思维意识“摸不着”、人的行为模式“抓不住”，亟需建设以人为本的《数字安全风险内控与合规教育评价指标体系》，推动网络安全强国建设。

二、数字安全内控与合规教育面临的挑战

国内安全治理、内控与全员教育尚处于起步阶段，在观念、制度、产业及技术等方面与国际先进相比存在差距。

(一) 观念层面

实践中，各层级积极落实网络安全相关法律法规中的工作要求，但安全意识观念还比较薄弱，主要有这几点：一

是改变个体的安全意识难,人对风险的理解认知存在差异,进而难改变行为,培育自我安全意识需要长期过程;二是业务层的退缩观点,系统相对复杂庞大,安全责任重任务多,而网络安全看不见、摸不着,知识水平跟不上,因此就容易滋生不愿参与或畏难情绪;三是技术层想走回头路,网络安全形势日见复杂,认为网络只要封闭或者保持现状就能确保安全,因此或是拒绝网络开放或者应用新技术;四是管理层的故步自封,认为技防到位、及时宣传培训就够了,较少主动作为提升安全意识、转化为安全行为。

(二)制度层面

落实工作要求关键靠制度,当前制度层面还存在不协调,一是责任主体层面压不实,目前仅上海等地方将网络安全意识教育纳入领导任职考评中,更多地方一方面没有纳入,另一方面也不知道指标分解和考评办法;二是经费缺乏制度保障,目前组织缺乏按照员工数量制定的合规与安全教育经费,或者占用IT的部门预算,不能根据网络安全形势的变化及合规要求进行动态调整;三是总体欠缺常态化机制,“攻防演练”中拔电源或者提前发文通告,使得攻防演练变成“运动式”,失去全员安全意识教育与团队技能训练的本意。

(三)评价层面

目前国内主要在组织层面的安全内控与治理领域主要采用的《等级保护》强制标准,并不适合各类组织的业务特点,在实施等保标准的过程中,可能存在以下问题:一是成本高,开展等保需要对系统进行检测和评估,需要投入大量的人力和物力资源,对于一些小型企业来说可能难以承受。二是技术难度大,等保标准涉及到的技术领域广泛,需要具备一定的技术能力和专业知识才能有效实施。三是人员素质要求高,开展等保工作需要具备较高的网络安全意识和技能水平,否则可能无法准确识别和应对网络安全威胁。当前,组织安全内控与合规评价指标体系不完备,尤其缺少以人为对象的评价标准、框架及度量指标。

(四)技术层面

人员安全风险教育与合规内控在技术实现层面也存在一定的问题,目前来看,突出的是这几点:一是技术手段缺乏融合,理想的内控与教育模式应该是随时随地、平战结合,虽然已经采取各种科技创新手段,如员工风险行为管理、态势感知系统等,但与及时教育、告警等融合度仍然不够;二是教育未形成系统化,员工缺乏全面的、结构化的安全知识框架,容易形成风险敞口。不同岗位员工培训不均衡、较零散或随需而做,“一刀切式”培训内容缺少个性化与针对性。课程时间较长占用工作时间,培训内容过于理论或枯燥,不易于理解、吸收和消化,使培训成了走马观花、被动应付。三是教育效果难体现,培训中习得的知识和技能缺乏

实用性,缺少动手能力,难以迁移到工作中。培训评估与考核往往停留在考试通过率与培训参与度等学习层评估,缺少全面的、客观的度量评估机制,对行为层、结果层缺乏有效跟踪与评估,难以实现安全培训与企业安全文化的良性循环。

三、国内外可参考最佳实践

(一)美国:

美国网络安全教育有四点经验可取:一是立法推动安全教育,除国家安全、保密、网络安全等法规外,早在2010年,美国即启动“国家网络空间安全教育(NICE)计划”,面向学生、社会大众、网络安全从业者等提出教育培训计划;二是与行业应用结合,如美国国会于1996年通过的HIPPA法案,即健康保险携带和责任法案,要求医疗机构、保险公司、医疗设备供应商等所有涉及个人健康信息的实体,必须对其员工进行隐私保护的教育和培训,同时要求这些实体每年对其员工进行一次隐私保护的再教育,以确保员工对隐私保护的理解和遵守始终与最新的法规和实践保持一致。此外,HIPPA还要求这些实体对其员工进行定期的隐私保护检查和评估。以确保他们能够理解和遵守隐私保护的规定,从而保护个人健康信息的安全和隐私。三是针对特定场景强化教育,如美国国防部由其信息系统局(DISA)强制所有与接入系统的用户必须接受“网络意识挑战赛”课程,并不定期采取多种技术手段来强化培训效果;四是积极培育相关市场,GRC软件(治理、风险与合规)成为百亿大产业,在面向风险管理的既有梭子鱼、思科、CyberBit等安全企业,也有SANS等具影响力的认证机构,还培育出KnowBe4、PHISHLABS等数十个专业的教育与培训企业。

(二)欧盟

欧盟通过ENISA加强了跨部门和跨国的合作,通过共享信息和经验,增强了整个欧洲的网络安全防御能力,并取得了一些显著的成绩:一是发布研究报告,ENISA发布了如“Raising awareness of cybersecurity as a key element of NCSS”等报告,这些报告详细分析了欧盟成员国在提高网络安全意识方面的现状、挑战和最佳实践。这些研究为政策制定者和企业提供了一份全面的指南,帮助他们理解和改进网络安全意识提升活动。二是提供教育和培训材料,ENISA开发了一系列教育和培训资源,包括在线课程、指南和手册,旨在提升企业员工的网络安全意识和技能。这些材料覆盖了各种主题,如数据保护、网络威胁识别、安全操作等。三是开发国家能力建设框架,ENISA发布了国家能力建设框架,旨在帮助欧盟成员国评估其在网络安全成熟度方面的自我评估,并提供五个成熟度级别的关键绩效指标(KPI)来提高用户意识。这个框架有助于成员国在战略和运

营层面增强和建设网络安全能力。四是建立合作网络，ENISA与各成员国的公共和私营部门合作，推动网络安全意识的提升和技能教育。这种合作包括共享最佳实践、组织研讨会和培训活动，以及建立信息共享平台。

四、加强风险内控与合规教育的建议

加强建设组织风险内控与合规体系，要利用全社会的力量，通过对产业采用升维布局，夯实制度建设，做好统筹规划，抓好贯彻落实，强化公众教育等来推进网络安全意识教育。

（一）夯实制度建设

政府层面亟须建立健全相关制度，一是加强贯彻网络安全责任制，加强对网络安全问题的监管，压实风险内控与合规教育的党委领导负责制；二是加强安全教育的制度化，细化安全风险与合规意识教育的管理，设定强制性的专项培训经费投入，要求网络安全教育的普及率等；三是由社会第三方开展组织内控成熟度评价，第三方机构的评估结果可以为政府和社会提供参考，帮助政府更好地了解企业的风险治理状况，为政策制定和监管提供依据。同时，也有助于社会公众了解企业的风险状况，为投资决策提供参考。

（二）构建风险内控与合规教育的评价指标体系

完善风险内控与合规教育的评价指标体系有助于提高企业的风险应对能力和合规水平，为企业的发展提供有力保障。首先，要明确评价的目标，通过评价来衡量企业在风险内控和合规教育方面的表现，同时用于改进企业的风险内控和合规教育。制定评价指标：根据评价目标，制定相应的评价指标。对于风险内控，可以包括风险识别、评估、监控和控制等方面的指标；对于合规教育，可以包括合规意识、合规培训、合规行为等方面的指标。同时，要注意指标的客观性和可操作性。针对每个评价指标，设定相应的评价标准。评价标准应该根据企业的实际情况和行业标准来确定，确保评价结果具有可比性和参考价值。引入第三方评价：为了确保评价的公正性和客观性，可以引入第三方机构进行评价。第三方机构可以独立于企业和政府之外，以中立、客观的态度进行评价，提供更加客观、可信的评价结果。定期评价与反馈：建立定期评价机制，对企业的风险内控和合规教育进行评价。同时，根据评价结果进行反馈，帮助企业发现存在的问题和不足，提出改进建议和方向。建立评级机制：根据评价结果，建立相应的分级排名机制。组织评级结果向社会公布，可以激励企业加强风险内控和合规教育，提高企业的风险应对能力和合规水平。

（三）统一部署及推广风险与合规教育平台

培训来源于网络，也应立足于网络，因此应当选择和推

广标准化的培训平台。一是易于贯标，通过统一平台来实施培训，有助于教材教案、师资力量、质量评估、效果检测等多方面实现初步统一；二是多维度评价，允许动态可视化评估各方效果，可以客观评估各地、各单位的实训绩效；三是培训信息共享，实现培训过程全程回溯与培训效果评价。

具有如下特点，一是培训标准明确，应制定安全意识教育相关实施标准、科学可行培训框架，强化培训管理、考虑、评估机制；二是教材教案丰富，针对不同群体及安全场景设计标准化的教材教案，应注重理论与实操相结合，尤其是要有时效性；三是宣贯形式多样化，充分利用现有的宣传渠道、方式，交互式、沉浸式是主流方向；四是教育效果可及时评估，考核方针明确，从知识点及被考核人的薄弱点自主定制考试内容，精准分析考核结果，可信的回溯及复核手段；五是平台化，充分利用AIGC、移动化、在线服务、虚拟化等新兴技术，通过技术嫁接、融合等形成培训教育平台，提供SaaS教育主题订阅与合规评价托管服务。

参考文献

- 1.Verizon, 2024 Data Breach Investigations Report (DBIR)
- 2.104th United States Congress, Health Insurance Portability and Accountability Act of 1996
- 3.NIST, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, NIST Special Publication 800-181
- 4.ENISA, Raising awareness of cybersecurity as a key element of NCSS
- 5.ENISA, National Capacity Building Framework published by ENISA

RSAC 2024聚焦AI安全： 证券行业面临大模型安全新挑战

康乐、盛浩月 | 奇安信科技集团股份有限公司

摘要：人工智能与证券业务正加速融合，安全是AIGC在证券领域应用的核心保障。如果缺乏安全保障，人工智能产业化落地将缺乏稳固的根基，难以持续发展。更重要的是，大模型的安全发展需要与证券行业场景深度融合，才能让大模型真正应用于实际。因此，大模型的安全建设需要实战化、行业化、场景化。只有在实战中不断锤炼大模型的安全能力，才能应对日益复杂的攻防挑战；同时紧密贴合行业需求，才能持续增强模型的专业能力，使大模型真正变得安全可靠。

关键字：人工智能 (Artificial Intelligence)、生成式人工智能AIGC (Artificial Intelligence Generated Content)、大模型 (Large Model)

一、引言

一年一度的全球最大网络安全盛会RSAC 2024于5月6日至9日在旧金山Moscone中心拉开帷幕，本届RSAC的主题定为“The Art of Possible (可能的艺术)”，聚焦网络安全的未来发展及技术创新。在为期四天的会议中，举办了超过600场的主题演讲、研讨会及产品展示。这一吸引全球4万多专业人士的行业会议，透露出安全行业的下一代趋势与变化。人工智能毋庸置疑是今年大会的最热门话题，包括AI重塑网络安全，以及AI相关的隐私与数据安全挑战。美国国务卿首次现身2024 RSAC，凸显出在全球各地陷入了地缘政治冲突之际，网络安全在国家安全中的日益重要作用。

当前，各行各业都在拓展对于AI大模型的应用，证券行业作为金融科技的前沿阵地之一，因其行业数据积累丰富及较高的专业壁垒，与AI大模型的适配度较高，其应用不仅能够提高业务处理的效率，还能够在投研投顾、风险管理、客户服务、市场分析等多个方面为证券公司带来创新的解决方案。

随着技术的不断迭代更新，大模型在带来诸多便利的同时，也伴随着一系列新的安全风险。RSAC 2024大会上，Presidio公司的CISO Dan Lohrmann指出，员工正在利用ChatGPT等公开可用的生成式人工智能工具开展工作，这种现象被称为“自带人工智能”。这给企业带来了许多安全和隐私方面的问题，比如敏感的公司数据被输入到这些模型中，可能会导致信息公开。Secureworks的首席技术官Mike Aiello认为，企业在使用人工智能方面面临的情况已经有点不受控制。他提到了数据中毒和提示注入攻击等威胁，这些问题有可能破坏人们对人工智能技术的信任，造成模糊、偏见和歧视等问题。

证券行业，作为对网络安全要求极高的领域，任何形式的网络攻击或数据泄露都可能给投资者造成重大损失，甚至可能对整个金融市场的稳定性构成严重威胁。在大模型广泛应用的背景下，这些安全风险变得更加复杂且多样化，因此，对大模型进行全面的风险评估并采取有效的安全防护措施显得尤为重要。

二、大模型时代下的证券行业：高效与风险并存

2023年是大模型技术蓬勃发展的一年，从理论研究迈向了实际应用。文心一言、讯飞星火、通义千问等国产通用大模型争相发布并不断迭代，开源大模型生态也在不断完善。头部证券公司从2023年初开启大模型相关研究，并逐步启动大模型在局部场景的落地试点。2023年底至今，已有3家证券公司（东吴证券、海通证券、国泰君安）对外发布了专属的金融垂类大模型，其他证券公司则更多是采购商业大模型进行私有化部署或基于开源大模型进行尝试探索。

当前，多家证券公司启动AI战略，探索大模型在证券领域的广泛应用。截至目前已有至少22家国内证券公司正在投入与探索大模型应用。随着技术的不断演进，尤其是自然语言处理、机器学习和数据挖掘技术的进步，证券公司通过大模型能够显著提升业务效率、优化服务质量、减少人为风险，并在日益复杂的金融市场中保持竞争力。然而，随着大模型应用的深入，数据隐私保护、合规性问题以及模型本身的安全性等挑战也成为行业亟待解决的难题。

目前已经有多起安全事件发生，三星的一名员工将机密源代码粘贴到ChatGPT中以检查错误、另一名员工与ChatGPT和“请求的代码优化”共享代码、第三个人分享了

一份会议记录,并将其转换为演讲笔记,这些信息曾一度公开在 ChatGPT 上使用。

三、自建大模型业务中的网络安全风险分析

大模型应用除了训练数据、输出数据时可能引发隐私数据泄漏外,还可能面临法律合规、内容违规、知识产权、非法使用等风险,攻击者也可能通过伪造大模型应用,非法获得使用者的敏感信息,随着大模型工具与我们工作的深度融合,将会引发很多安全风险,具体有以下几点:

1、向大模型进行不安全的提问

■不合规的提问

在智能客服的问答场景下,若用户提出与黄色、赌博、毒品或政治敏感相关的问题,大模型可能生成不合规的内容。

■指令攻击

攻击者可能通过设计特定的提示或指令,让大模型扮演某个角色(如内部员工、专家等),从而获取敏感信息或进行欺诈。还可能利用反向诱导等策略,引导大模型产生错误或偏向性的回答,误导投资者或决策者。

■敏感话题

涉及伦理道德的问题若处理不当,可能引发广泛的社会争议,进而严重损害金融机构的声誉和形象。同样,大模型在回答涉及种族、性别、宗教等敏感话题时,若未能保持公正和中立,也可能产生歧视性言论,进而造成不良的社会影响。

■数据安全

攻击者可能通过提问的方式,诱导大模型泄露用户的个人信息或敏感数据,从而进行非法活动。

2、大模型的生成内容问题

■内容安全

大模型回复的内容若涉及黄色、赌博、毒品或政治敏感等内容。

■价值观

若大模型生成的回复内容违反社会主义核心价值观,将损害社会公共利益和道德,影响金融机构的形象。

■知识产权

大模型在生成内容时,若未经授权使用了他人的知识产权(如专利、商标、著作权等),将构成侵权行为,可能引发法律纠纷。

3、大模型所处网络中的网络安全问题

■系统漏洞

大模型自身可能包含系统漏洞或缺陷,这些漏洞可能被攻击者利用,进行非法访问、数据窃取或破坏等活动。

■API安全

大模型通常会提供API接口,以便其他应用调用其能力。然而,若API的调用存在滥用、弱密码等安全风险,攻击者可能通过API接口进行非法访问和操作。

■越权访问

若大模型的访问权限设置不合理,某些账号可能能够越权访问敏感数据或执行非法操作。这将严重威胁数据的安全性和完整性。

■DDoS攻击

攻击者仍可能尝试通过发起DDoS攻击来瘫痪大模型的服务,这将导致证券行业的相关业务中断,造成重大损失。同时,由于大模型计算成本高昂,一旦遭受攻击,恢复和重建的成本也将非常巨大。

四、通过内网访问公网大模型应用的网络安全风险分析

1、数据泄露风险

员工在将源代码、交易数据等敏感信息发送给公有大模型进行检查或分析时,可能存在数据泄露风险。一旦这些信息被攻击者获取,将对公司造成重大损失。

2、未知风险

公有大模型作为新兴事物,其AGI能力类似黑盒,具体生成内容的过程和机制尚不完全清楚。因此,在传输内容过程中可能存在巨大未知风险,如被攻击者利用进行恶意攻击、数据窃取等。

另外,OWASP针对大模型提出了10个典型安全问题,涵盖了大模型作为一个业务系统面临的主要攻击风险:

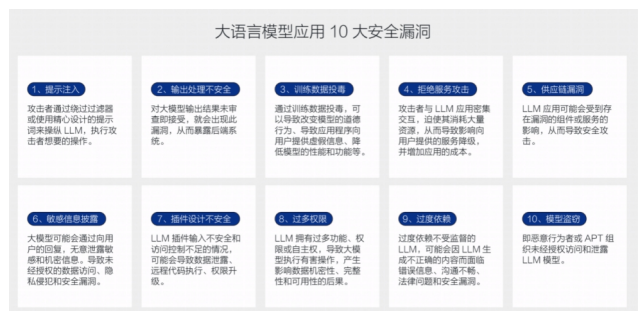


图1 OWASP 发布的大语言模型应用 10 大安全漏洞

五、大模型网络安全风险治理的实践思路

对于证券行业来说,应对大模型网络安全风险需要采取多层次、全方位的防护措施,以下是对此提出的一系列建议:

1、部署大模型安全框架与解决方案

证券企业应及时部署大模型安全检测工具并建立应急响应机制,确保能够及时发现并应对潜在的安全威胁。通过不断更新企业侧大模型应用环境的风险检测能力,以及相应的应对机制,保持与大模型技术迭代的同步,以确保检测的有效性。

■ 选择适合的安全检测工具

大模型风险管理需要持续的运行监控及保护;发现、检测、策略、保护、响应、处置缺一不可,任何环节缺失导致管理失效,安全难以闭环。目前,现有的安全架构应对大模型安全显得捉襟见肘:首先是大模型应用的监测和风险评估难,大模型应用的数量飞速增加、应用更新变化快,缺少风险评估工具,企业使用风险难以评估;其次高危操作、异常使用大模型工具,将会引发敏感信息泄漏或其他风险;最后大模型工具的使用缺乏有效的记录手段,各类信息缺失,使用风险难以追溯。所以在部署大模型安全框架时,首要任务是选择适合的安全检测工具。这些工具应具备以下特点:

威胁检测:能够识别异常访问行为,并对投喂给大模型的文件进行病毒检测。通过实时监控和分析访问行为,可以及时发现并阻止恶意攻击和非法入侵。同时,对投喂文件进行病毒检测可以确保模型在训练过程中不会受到恶意代码的感染,从而保障模型的安全性和稳定性。

内容审计:应具备内容审计功能,能够检测大模型在处理提问和回答过程中的内容,并进行风险报警或拦截。通过实时监控和分析模型输出内容,可以及时发现并处理潜在的违规或敏感信息,从而规避法律风险。

合规管控:安全检测工具应支持对不同身份和职位的员工进行分别授权使用。通过细粒度的权限管理,可以确保每个员工只能访问其职责范围内的功能和数据,从而有效规避风险,实现数据的合规使用。

实时更新:随着大模型技术的不断发展,新的安全威胁和漏洞也在不断涌现。因此,所选的安全检测工具应具备实时更新能力,能够及时获取最新的安全威胁信息和防护措施,并与大模型技术迭代保持同步。这样可以确保工具始终具备最新的检测能力和防护手段,有效应对不断变化的安全威胁。

分析溯源:能够实时关注系统的使用动态,通过直观的图表和数据展示,让监控人员能够迅速捕捉潜在风险。违规行为产生告警后,查看详情可进行追溯,一键追溯到原始日志,并查看完整事件链,通过完整事件链和已解析字段可进一步分析大模型应用使用的合规合法,为快速响应和有效处理提供有力支持。

■ 建立快速响应机制

安全事件响应团队:组建大模型安全快速响应团队,包含安全专家和技术人员等,负责突发安全事件的快速处理。

制定应急预案:针对可能的安全风险,制定详细的应急预案,包括应急处理流程、责任分工、资源调配等。

安全操作手册:编制包括大模型使用、数据保护、员工行为规范在内的标准化操作手册。

跨部门协作机制:技术部门与法务团队联合制定数据保护和大模型使用规范,避免技术与法律之间的脱节。

2、构建大模型时代的数据保护体系

■ 防止敏感数据泄漏

证券企业的数据是其业务运营的核心资源,承载着客户隐私、交易记录、市场策略等高度敏感的信息,因此也成为了攻击者的主要攻击目标。为了保障这些数据的安全,证券企业必须建立严格且有效的数据保护机制,以防止任何形式的数据泄露,特别是因不当的数据投喂行为而导致的敏感信息外泄。

内部技术监管是保障证券企业数据安全的重要手段。其中,数据加密是基础,通过对敏感数据进行加密处理,确保在传输或存储过程中即使被截获,攻击者也难以解读真实内容,显著降低数据泄露风险。同时,建立严格的访问控制机制也至关重要,明确每个员工的访问权限,确保敏感数据仅由授权人员访问和处理,这既能防止数据因员工误操作或恶意行为而泄露,又能提升整体的数据安全效能。

■ 建立身份识别与溯源机制

将身份与数据关联起来,以便在发生数据泄露时能够迅速找到泄露主体,及时采取措施阻止数据进一步泄露,从而有效控制损失范围,保护企业核心数据和客户隐私安全。

3、加强员工安全意识与技能培训

对员工进行定期的大模型安全培训,了解大模型滥用的风险和识别潜在威胁的方法。通过模拟大模型攻击场景进行演习和培训,提高员工的警觉性和应对能力。

4、积极应对外部监管环境的变化

证券行业需要积极应对外部监管环境的变化。随着国家对网络安全和数据保护的重视程度不断提高,相关法规和政策也在不断完善。证券行业需要密切关注这些变化,及时调整自身的网络安全策略和管理措施,以确保符合法规要求并降低潜在的法律风险。

六、结语

人工智能与证券业务正加速融合，安全是AIGC在证券领域应用的核心保障。如果缺乏安全保障，人工智能产业化落地将缺乏稳固的根基，难以持续发展。更重要的是，大模型的安全发展需要与证券行业场景深度融合，才能让大模型真正应用于实际。因此，大模型的安全建设需要实战化、行业化、场景化。只有在实战中不断锤炼大模型的安全能力，才能应对日益复杂的攻防挑战；同时紧密贴合行业需求，才能持续增强模型的专业能力，使大模型真正变得安全可靠。

参考文献

1. RSAC 2024 Review: AI & Data Governance Priorities
2. 2024人工智能安全报告，奇安信科技集团股份有限公司，2024年
3. 2024年AI在网络安全运营领域的现状与前景，《2024年CISO视角：AI现实与炒作》

网络攻防新背景下的高质量漏洞运营

樊兴华 | 北京微步在线科技有限公司

摘要：在当今天高度互联且日益复杂的网络环境中，网络安全威胁呈现出前所未有的多样性和隐蔽性。而随着信息技术的迅猛发展，网络攻击的手段和频率不断增加，漏洞作为网络安全体系中最薄弱的一环，已成为攻击者突破企业安全的主要途径。对于企业而言，高质量的漏洞情报有助于构建企业预防和应对网络安全事件的第一道防线，而打造高效的漏洞运营则更益于企业形成更高效、快速的防护响应，降低被攻击风险，对于企业安全尤为重要。

关键字：漏洞情报、漏洞情报生产、漏洞运营、高质量安全运营

一、概述

漏洞是一个相对古老的话题。自网络出现以来，由于漏洞导致的安全风险隐患就一直存在。随着最近几年网络安全和攻防技术进一步发展，漏洞造成的危害就愈发严重，给企业带来的风险也更大。基于多年行业实操及对行业漏洞运营的思考与洞察，我们从四个方面对企业漏洞运营面临的挑战与问题进行探讨。

二、透过数字，看企业漏洞运营误区

下图展示的，是网络中每年被用于攻击的漏洞数量。从该图呈现的趋势，可以得出几个结论：



图1 每年被用于攻击的漏洞数量

- 第一，每年爆出的新漏洞总量在持续上涨。
 - 第二，未被利用漏洞和已利用漏洞相比，数量更多且增速更快。并且每年新增漏洞量会越来越多，而因此真正被黑客利用进行攻击的漏洞占比会越来越低。
 - 第三，被利用漏洞的比例每年基本都在10%以下。
- 下图展示的，是当前网络“全部漏洞平均被利用所花费天数”的趋势：



图2 全部漏洞平均被利用所花费天数

从图中可以看到，一个漏洞从被披露到首次被观测，到利用的时间已经越来越短，侧面也反映出黑客的攻防研究能力正在快速提升。实际上，从2022年、2023年微步实际观测到的数据来看，一个漏洞从披露到被利用的平均时间确实也已经大大缩短，最多三五天时间就会被利用。危害性大的漏洞，被利用时间甚至更短。

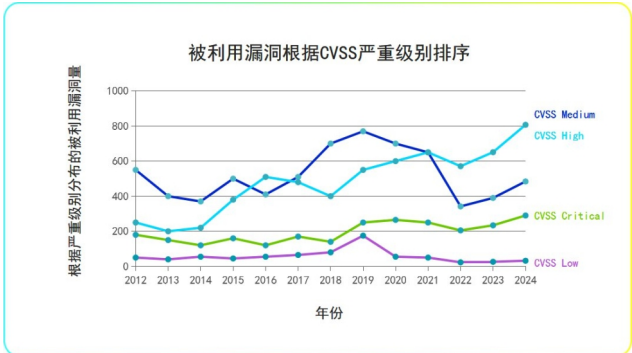


图3 被利用漏洞根据CVSS严重级别排序

上图是按照CVSS (Common Vulnerability Scoring System) 评分来展示的被利用漏洞的数量分布。其中，CVSS评分为中 (CVSS Medium) 的漏洞数量占比最高，然后次之就是评分为高 (CVSS High) 的漏洞，再次之就是严重

(CVSS Critical)的漏洞,最后是评分为低(CVSS Low)的漏洞的分布情况。

该图揭示了企业在漏洞修复上存在的一个很大的误区。从漏洞实际修复维度出发,很多企业都在根据CVSS评分来决策一个漏洞是否要修,这就导致企业往往只关注严重的漏洞,对于绝大部分评分为中或者是低的漏洞,企业可能会直接忽略。但从整体趋势来看,被攻击者利用数量更多的是CVSS评分为中或高的漏洞,而CVSS评分为严重的漏洞被利用的数量相对要少很多。

事实上,黑客是否利用一个漏洞,不会依据漏洞的CVSS评分,而是根据漏洞的易用性、影响范围、利用成功后的权限大小等因素综合评估。但企业实际决策,是根据CVSS评分来的,这就导致攻防双方对于评估漏洞价值的标准不对等,结果就是企业并未完全修复那些会真正带来入侵风险的漏洞。此外,在每年新增漏洞中,尤其是评分严重的漏洞中,真实被利用的漏洞占比也非常低,很多企业急于修复的漏洞,实际危害可能并没有那么大。

三、漏洞运营,企业存在的痛点与挑战

第一,漏洞运营告警多,但效率较低。企业每天会从各种渠道获取新漏洞信息,且有很多告警,但不知道告警的实际危害,以及如何合并重复告警。其次是修复的决策不够科学,评分为严重漏洞的利用条件可能十分苛刻,而同时一些更可能被利用的漏洞却被企业忽略。

第二,漏洞频发,但漏洞详细信息难以及时获取。漏洞本身可以说是网络攻击的“杀手锏”,尤其是0day,企业去缓解攻击和消除漏洞隐患,需要尽可能第一时间获取最新信息,但问题在于最新信息很难稳定获取。同时,企业在做内部修复时还需要PoC等细节,去验证内部资产受影响程度。同时,企业安全团队也需要依靠大量技术细节去说服业务方配合做后续修复及验证,在获取最新漏洞信息和技术细节上仍然存在挑战。

第三,即便第一时间获取到漏洞信息,也确认过漏洞严重性,但不知如何修复。从后台统计数据来看,30%-40%的漏洞爆出来时候没有补丁。同时,漏洞修复需要安全团队和企业业务团队长期拉扯,即便安全团队觉得漏洞很严重,但业务团队可能没有办法第一时间升级,所以需要安全团队给出缓解或加固方案。

四、基于漏洞情报库,化解漏洞运营难题

漏洞运营价值和目的,从漏洞运营视角来说,重心应该在安全风险。因为漏洞运营的本质和目的,是要消除因为漏洞导致的安全风险。请注意,这里的落脚点是安全风险而不是漏洞。这两个落脚点有很大差别。

如果落脚点在安全风险,那么我们修复漏洞的视角,需要考虑的是某个新漏洞是否真的会带来安全风险,然后再决策是修复还是忽略该漏洞。微步认为,正确的落脚点是在安全风险上,但很多时候我们看到企业修复漏洞时,是落在漏洞上,没有反向思考自身业务是否真实存在因为不修复某个漏洞而引入了新的安全风险,这就造成了投入资源但没有意义的情况。

所以,在修复漏洞之前,企业应确认漏洞的真实严重性、漏洞带来的风险究竟有多大,进一步思考整个漏洞运营流程如何优化才能更高效。

很长时间内,漏洞运营依靠的数据是漏洞信息库,但漏洞信息库大部分都是通过公开渠道抓取,存在信息质量低、数据量少、字段杂乱不统一的问题。从现阶段整个网络安全发展趋势和红队攻防趋势来看,单纯依靠这些信息很难解决漏洞导致的安全风险。

相比漏洞信息库,漏洞运营更需要的是一个漏洞情报库。这个漏洞情报库需要具备几个特点,分别解决前面提到的三方面的问题。

第一,及时性。一旦有新漏洞出来,或者在一些小圈子内传播时,企业需要基于漏洞情报库第一时间掌握这些信息。

第二,优先级。由于漏洞量很多,尤其一些大的集团,资产量很大,在做探测和漏扫时会有大量资产告警,如何尽可能降低因为漏洞导致的安全风险?漏洞情报库要有一个比较客观的评估维度,而不仅仅是单纯依靠CVSS的评分进行评估。

第三,可操作性。发现漏洞后,企业需要思考到底如何修复,思考如果没有补丁,如何修复、缓解这个风险;如果有补丁企业怎样升级、怎样修复等等这些评估方面的问题,也包括如何做临时防护、临时缓解措施等解决问题的手段。

这三方面是给漏洞运营提效的三个关键点,微步认为漏洞情报也需要解决这三个问题。

具体而言,微步会从漏洞生命周期、企业漏洞运营和漏洞情报生产三个视角来看漏洞运营:

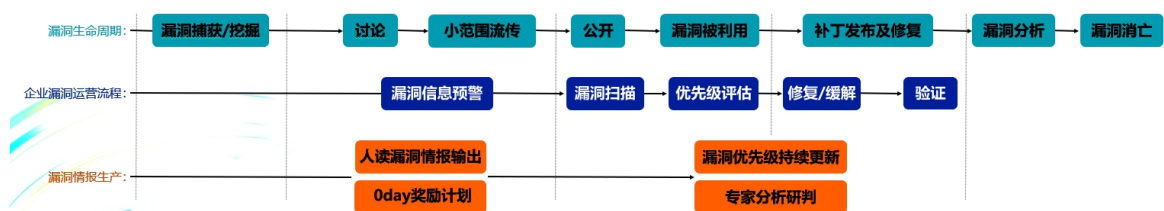


图4 不同视角看漏洞运营

企业需要清楚，在全流程每个阶段该做什么事情。首先，漏洞在被讨论和小范围流传的过程中，企业需要第一时间获取信息从而了解相关漏洞。在漏洞情报上，微步会第一时间通过人工输出社交媒体讨论信息，推送至企业了解关注。同时，微步也会通过“漏洞奖励计划”去收集0day，掌握这些信息之后，企业漏洞运营需要做后续评估、扫描内外网，确定影响面、评估优先级，最后做出对应的修复或者缓解。这个过程中，漏洞情报需要不断跟踪漏洞当前被利用的态势及危害，不断更新漏洞优先级，为漏洞运营的修复提供更多情报信息。

五、漏洞情报库时效性提升策略

为及时获取漏洞信息，企业漏洞运营团队需要关注公开社交媒体、情报社区以及其他安全厂商，同时需持续关注暗网上流传的EXP、信息工具等，通过建立一个强大的监控系统去获取此类信息，并依赖于AI算法进行自动化处理。当前，微步已开始基于微调后的XGPT模型对数据做处理，并且通过全网汇聚、实时感知的态势情报，基于数千事件源信息采集，小时级更新，能够实时了解最新安全事件、最新行业事件。

通过上述过程，运营人员可以迅速获取当前漏洞的相关信息，包括活跃度、涉及到的产品和厂商等信息，以及当前不同行业最新安全事件、攻击技战法、黑客组画像等。微步会持续对社交媒体信息源进行长期评估，从而确定信息源置信度。如果置信度较高，会将相应信息推送至企业参考，最终会让运营人员第一时间感知到最新漏洞情况。

六、漏洞情报库的优先级管理

CVSS评分会基于漏洞的基本信息进行评估，包括但不限于受影响的产品和版本等。在CVSS 2.0到3.1中，评分考虑了漏洞的基础(Base Score)、生命周期(Temporal Score)、环境(Environmental Score)三个维度。其中，生命周期评价指标会关注利用代码成熟度、补丁完善水平和报告可信度。随着CVSS发展至4.0版本，其对漏洞的生命周期评价新增了威胁指标组，包括是否被利用、是否发生基于该漏洞的攻击、是否存在公开可用的PoC等漏洞利用成熟度情况。因此，除了基本的CVSS评分外，企业还应密切关注漏洞是否已被实际利用、其活跃程度以及是否存在公开的PoC(概念验证)代码等因素，以便更全面地评估和管理风险。

而在获取漏洞利用情况这些信息上，威胁情报能够发挥重要作用。由于威胁情报是描述攻击者的数据，包括攻击者的资产、攻击的端口、攻击路径、时间、利用的漏洞

Payload等，这些信息对于企业决策漏洞修复优先级来说，非常有价值。

通过把威胁情报大数据融入漏洞信息，抽象成漏洞VPT (Vulnerability Priority Rating) 引擎，结合漏洞情报数据及威胁情报数据，进行VPT研判，包括漏洞的利用情况、攻击者、活跃度，有无PoC等等，最终与企业内部资产实际情况相结合。这两方面信息结合起来之后，可以决策出企业漏洞修复的最终优先级。从消除安全风险角度来说，利用VPT进行修复决策，科学性更强，实际价值更明显。

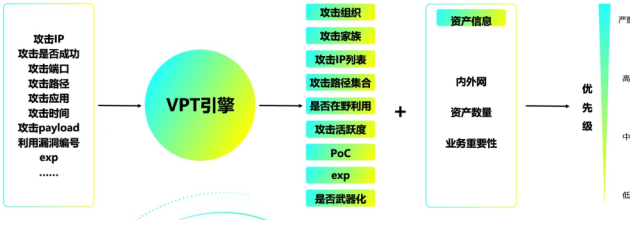


图5 利用VPT引擎进行漏洞修复科学决策

七、漏洞情报库的可操作性

这一点依赖于企业是否具备专业的漏洞专家团队，根据漏洞VPT的评估结果对严重漏洞进行专项分析，输出不会产生实际危害的无损PoC，甚至一些检测规则和自查工具，以及针对尚无补丁的漏洞输出临时缓解方案。如果对技术分析比较关注，企业安全团队还需要输出原理层、相对详细的分析报告，包括漏洞复现信息等等。

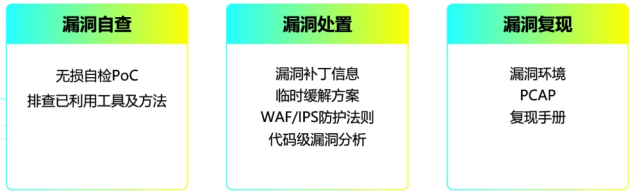


图6 漏洞情报库可操作性

八、高质量漏洞情报的生成机制

很多因素会决定漏洞情报的质量，我们总结了以下几点：

第一，漏洞信息库的全面性。这取决于企业能否把各种公开信息源第一时间抓到。这一点很重要，但没有壁垒。

第二，是专家分析。专家分析依靠人才，如果企业有一个比较大的漏洞团队，有相对专业的人员，这个门槛也不是特别高。

但真正决定一家企业或者安全厂商漏洞情报能做好的，是下面两点：

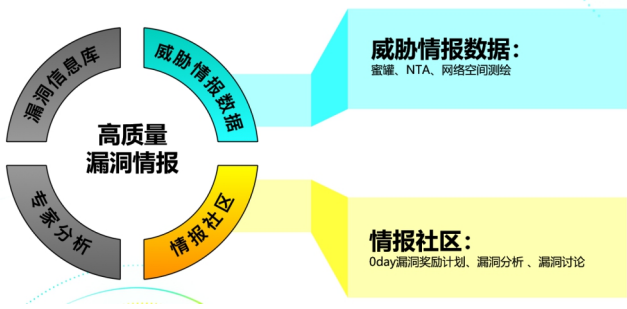


图7 高质量漏洞情报生产的关键

第一是威胁情报数据。企业或者漏洞情报供应商是否有极强的威胁情报能力，能否从威胁视角提供关于具体漏洞的全网真实利用数据，这一点决定了厂商或者企业能否提供相对客观、完整、及时的评估建议。而强大的威胁情报能力，至少需要包括一流的情报生产能力和高覆盖度的威胁情报数据，以及蜜罐、全网测绘能力等等。

第二是情报社区。情报社区可以把白帽子力量聚合起来，同时通过奖励计划，从包括红队等小圈子去收集一些高价值漏洞。所以，是否拥有一个一流的情报社区，对于解决这个问题也非常关键。

九、总结与展望

漏洞情报不仅提供了关于潜在安全威胁的早期预警，也为高效漏洞运营奠定了坚实的基础。通过系统化、结构化的漏洞情报收集、分析与共享，以及科学有效的管理方法，企业可迅速识别并评估新发现的漏洞，进而制定有针对性的修复策略。这其中，高质量的漏洞情报对于安全团队，优先处理对业务影响最大、被利用风险最高的漏洞，确保资源的有效分配，增强安全防护能力，更是至关重要。

未来，随着人工智能(AI)和机器学习(ML)技术的不断进步，漏洞情报的生产也将变得更加智能和精准，其在现代网络安全防御体系的作用必将越来越重要。为有效应对当前复杂网络攻击形式，企业需持续提升漏洞情报生产，尤其是高质量漏洞情报生产的能力，才能逐渐构建一个坚固、高效的网络安全防护体系。

证券行业分支机构 IT 降本增效方案

白昆忠 | 上海灵畅信息技术有限公司

摘要：证券行业分支机构面临 IT 降本增效需求，轻型 / 微型营业部兴起。本文分析其 IT 现状、信息安全与合规需求，提出采用 SASE 终端管理方案，该方案融合多种功能，可私有化部署，满足信创要求，支持多系统。经预算对比，五年总费用相比传统架构大幅度降低，并能解决运维人力不足等问题，增强信息安全防护能力，适应行业发展需求。

关键字：SASE (Secure Access Service Edge/安全访问服务边缘)；据防泄漏 (Data Loss Prevention, DLP)；EDR (Endpoint Detection and Response/终端检测与响应)；SD-WAN (Software-Defined Wide Area Network/软件定义广域网)；零信任网络访问 (Zero Trust Network Access, ZTNA)；上网行为管理 (Secure Web Gateway, SWG)；MFA (Multi-Factor Authentication/多因素认证)。

一、环境与背景说明

轻型/微型营业部的背景：

随着证券行业发展模式趋于成熟，分支机构增速放缓，券商从规模扩张转向高质量发展。新设营业部面临经营成本压力，收入难覆盖成本。同时，互联网发展使线上服务模式成熟，客户倚重线上服务，现场交易需求减少，年轻客户群体对线上服务依赖度高。外资券商涌入改变经营环境，轻型营业部可作获客窗口和营销渠道，适应市场竞争。这些因素推动证券行业在经营模式和服务方式上不断变革。

IT 管理主要面临的挑战：

证券行业需降本增效。交易系统关键依赖集中于证券公司总部，A 类证券营业部占比极小且维护成本高、效益不佳。随着信息技术发展，信息安全重要性凸显，分支机构在攻防演练中常为薄弱环节，提升其信息安全防护能力迫在眉睫。

如当前证券行业，A 类营业部减少，C 类成主力，营业部向轻型或微型转型。A 类机房设备过保断保增多，C 类营业部缺专业人员，工作压力大。营业部信息安全设备基础，缺乏准入机制等。分公司 IT 运维费用批复可能致续费中断，营业部 IT 费用或被削减。故障时靠分公司人员或外包修复。券商合并趋势下，营业部降本增效，降租金、缩设备、调架构、转人员。未来 A 类网点可能转型，需调整营业部架构和 IT 投入，发挥 IT 效益，保障安全合规，适应行业发展，支持券商业务稳健发展。

二、证券营业部 IT 现状

在证券公司营业部与总部联网架构中，部分采用“三层架构”或“二层架构”。三层架构下，营业部有客户网和业务网，主路由器多网络接入，分公司与 A 类营业部有专线或备援线路。营业部与分公司、分公司与总部通过不同方式对接，分支机构外网和业务网隔离。头部券商营业部多双线路高可用，部分单臂网络有风险。二层架构下，营业部与总部专线或 VPN 对接，业务网加密直连总部。大部分营业部配备防火墙或上网行为管理设备，部分网点“裸奔”，还有部分上网行为管理设备兼具防火墙功能但防护弱，存在信息安全风险。

三、证券营业部信息安全与合规需求

一、人员与运维

(一) 人员配置与分工

当前，许多证券营业部受人员编制限制，缺少 IT 专岗老师，IT 相关事务不得不由分公司或总部老师兼管。这使得 IT 相关责任人任务繁重，运维压力极大。为提高分支营业部的 IT 运维效率和专业性，有必要合理规划人员编制，根据信息化系统集中管理原则建议在总部设立专门的 IT 岗位，并明确其职责分工。

(二) 运维能力提升

在遇到网络问题时，由于现场协助排查的人员往往非 IT 专业出身，排查能力明显不足。因此，应加强对非 IT 专业人员的基础 IT 知识和信息安全知识培训，提升他们的网络问题排查能力与信息安全自查能力。同时，建立更高效的远程技术支持机制、应急响应机制，以便在遭遇复杂问题时能及时获取专业的 IT 支持。

二、网络架构与管理

(一) 网络拓扑清晰化

分支机构网络拓扑架构模糊不清, 这给 IP 冲突或信息安全问题的快速定位与排查带来了困难。需重新梳理和绘制网络拓扑, 建立详尽的网络文档, 涵盖网络设备连接关系、IP 分配情况等, 并利用网络管理工具对网络拓扑进行实时监控和可视化展示。

(二) 网络安全接入管理

部分营业部缺乏网络准入控制, 无法有效通过技术手段管理外来设备接入业务网。应部署网络准入控制系统, 设定严格的准入规则, 如设备认证、用户身份验证等, 防止未经授权的设备接入, 保障业务网安全。此外, 在设备接入业务网前, 应进行有效的安全基线核查, 确保入网设备满足安全、合规条件, 如安装防病毒软件并更新病毒库、修补安全漏洞使本机不存在中到高危等级风险。

三、安全策略与设备

(一) 统一安全策略

分支机构网络与信息安全策略难以统一管理, 因设备部署架构不统一、品牌多样、数据分散, 导致总部无法收集日志与下发安全策略。需对设备进行标准化选型, 建立集中的安全管理平台, 实现安全策略的统一制定、部署和管理, 同时集中收集和分析日志数据, 并进一步进行数据分类分级, 提高数据可用性。

(二) 终端安全管控

终端设备无法进行桌面管控, 存在随意安装软件(包括非法软件、绿色软件)的现象, 且缺少必要的防病毒软件、EDR 软件等关键软件, 无法监控漏洞与关键修复补丁, 无法统一禁用高风险端口(如 445、135、145、21 等), 也无法控制共享网盘、文件的传递。

(三) 数据防泄漏

大部分营业部无法实现数据防泄漏(Data Loss Prevention, 以下简称DLP)(超过 98%的券商尚未解决网点DLP 问题), 原因是实施 DLP 成本较高, 且需要制定准确的分类规则与配备审计人员。

(四) 安全上网

根据网络安全法与证券行业相关要求, 需要对钓鱼邮件的 URL、高危 IP 地址的访问进行阻断, 对挖矿软件的使用进行阻断, 对涉及黄赌毒的网站、境外非法博彩等的外联 IP 进行阻断。

四、合规与监管要求

(一) 内部交易审查与上网留痕设备

依据证监会要求, 需对内部交易审查并将上网留痕, 但

部分营业部因预算问题缺少此类设备。

(二) 内部网络管理规定

根据证券公司内部管理规定, 需禁用除本公司以外的交易软件使用。

四、降本增效解决方案

为应对证券营业部在人员配置、运维能力、网络架构、安全策略以及合规要求等多个方面的问题, 需进行全面优化与改进, 从而提升整体运营效率与安全性, 以适应证券行业日益严格的监管要求和快速发展的业务需求。鉴于此, 提出全新解决方案, 以解决上述问题, 并实现降本增效的目标。

证券公司通常具有数据中心与网点两种不同的网络架构及生态环境。数据中心拥有丰富的服务器资源、大量运维人员以及信息安全组织和专业人员, 因而适合构建强大的防护体系, 采用纵深防御策略, 层层保护核心业务系统, 配备防火墙、WAF、IPS、威胁情报、态势感知、堡垒机、各类安全探针、API 安全防护、流量监控、性能监控等设备。然而, 证券公司营业部无法像总部数据中心那样构建众多安全防护设备并配置充足的信息安全人员。于是, 一个值得深思的问题浮现: 网点网络设备是否一定需要防火墙呢? 倘若所有上网设备在终端就得到管控, 需接入业务网的终端设备具备强大安全防护能力, 而其他设备仅允许上互联网, 那么是否连硬件防火墙都不再需要, 就如同茶馆或俱乐部一般, 仅需一个高速上网的路由器即可解决问题。

终端拥有强大安全防护能力, 包括防火墙、防病毒、桌面管理、零信任网络、SDWAN、上网行为管理、DLP 等, 等同于 SASE。通过 SASE 机制接入总部数据中心, 加密回传终端用户的信息、日志及各种事件分析, 总部可进行统一策略下发与用户行为分析, 终端入网前可进行安全合规基线检查, 一旦发现安全隐患事件, 总部能够远程断网、禁用该终端入网, 实现细致的信息安全管理。

一、何谓 SASE?

SASE 是“安全访问服务边缘”(Secure Access Service Edge) 的缩写。SASE 是一种将网络和安全功能融合的云服务模式。它的出现是为了应对现代企业数字化转型过程中, 日益复杂的网络安全威胁和分散的用户、设备接入场景。传统的网络安全架构通常是基于边界防护, 例如防火墙、VPN 等设备部署在企业网络的边界。

SASE 将软件定义广域网(SD-WAN)功能与网络安全功能(如零信任网络访问、云访问安全代理、防火墙即服务等)整合到一个统一的云服务平台中, 为企业提供一站式的安全网络访问解决方案。

终端管理	资产管理	设备管理	版权检测	软件仓库	软件分发	软件禁用
终端安全	漏洞修复	基线检查	EDR	DNS安全	安全指纹	安全日志
数据安全	EDLP			NDLP		UEBA
	终端数据分类分级	外设传输通道管控	图像识别&图像OCR	应用访问控制和审计	应用敏感数据识别	自动化用户风险画像
网络安全	屏幕水印	文件水印	违规截屏取证	网络外发通道管控和审计	HTTPS应用数据防泄露	数据地图&数据溯源
	零信任网络访问(ZTNA)			上网行为管理(SWG)		
网络服务	应用隐身	多因素认证	应用自动发现权限智能梳理	域名&应用访问控制	威胁情报检测	文件上传下载管控
	应用/API访问控制	动态访问控制	无端访问	PAC引流	上网合规检测	上网行为审计
	全球分布	就近接入	自动选路	跨运营商优化	多云容灾	无需改动企业现有网络

图1

二、SASE有哪些功能组件？

以下是对各个模块的说明：

终端管理相关模块：

- 资产管理：对终端资产进行有效管理。
- 设备管理：实现对设备的管控。
- 版权检测：检测终端内容的版权情况。
- 软件仓库：提供软件存储及管理功能。
- 软件分发：负责将软件分发到终端。
- 软件禁用：可禁止特定软件在终端上运行。

终端安全相关模块：

- 漏洞修复：修复终端存在的漏洞。
- 基线检查：检查终端是否符合安全基线要求。
- EDR：终端病毒与威胁响应（拥有病毒查杀与自动更新能力）。
- DNS安全：保障域名系统的安全。
- 安全指纹：通过指纹技术确保终端安全。
- 安全日志：记录终端安全相关操作日志。

数据安全相关模块：

- 终端数据分类分级：对终端数据（非结构化数据）进行分类和分级管理。
- 外设传输通道管控：管理外设传输通道如USB、蓝牙、U盘等。
- 图像识别&图像OCR：实现图像识别和光学字符识别功能的数据防泄露。
- 应用访问控制和审计：对应用的访问进行控制并审计，对及时通讯传输文件进行管控。
- 应用敏感数据识别：识别应用中的敏感数据。
- 自动化用户风险画像：自动为用户构建风险画像。
- 屏幕水印：在屏幕上添加明水印，具有威慑作用。

- 文件水印：为文件添加暗水印，有利于文件外泄路径追踪与甄别。
- 违规截屏取证：对违规截屏行为进行取证。
- 网络外发通道管控和审计：管理和审计网络外发通道。
- HTTPS应用数据防泄露：防止HTTPS应用数据泄露。
- 数据地图&数据溯源：提供数据地图和数据溯源功能。

网络安全相关模块：

- 零信任网络访问（ZTNA）：以零信任理念实现网络访问控制、满足多因素（MFA）认证能力。
 - 上网行为管理（SWG）：管理上网行为。
 - 应用隐身：使应用在网络中隐身。
 - 多因素认证：采用多种因素进行身份认证。
 - 应用自动发现权限智能梳理：自动发现应用权限并进行智能梳理。
 - 域名&应用访问控制：控制域名和应用的访问。
 - 威胁情报检测：检测威胁情报。
 - 文件上传下载管控：管控文件的上传和下载。
 - 应用/API访问控制：控制应用和API的访问。
 - 动态访问控制：实现动态的访问控制。
 - 无端访问PAC引流：对无端访问进行PAC引流处理。
- 【当出现无端访问（即没有明确目的或未经授权的访问）时，通过PAC（Proxy Auto-Configuration，代理自动配置）技术将这些访问引流到特定的方向进行处理。】
- 上网合规检测：检测上网行为是否合规。
 - 上网行为审计：审计上网行为，可以取代网点的“上网行为网关”功能。

网络服务相关模块：

- 全球分布:使用云端服务,POP 点服务全球分布,使用数据中心部署可以建设多 POP 网络接入点。【POP(Point of Presence)网络接入点是指互联网服务提供商(ISP)在特定地理位置设置的接入设施。它的主要作用是为用户提供网络连接服务,使得用户能够通过该接入点接入到更广泛的网络中。】

- 就近接入:实现 SASE 终端就近 POP 点接入服务。
- 自动选路:自动选择网络路径。
- 跨运营商优化:对跨运营商网络进行优化。
- 多云容灾:提供多云环境下的容灾能力(云端部署版本)。
- 无需改动企业现有网络:使用该服务无需改动企业现有网络,使用终端连接,由后台网络管理中心进行软件定义网络。

三、SASE能否私有化部署？

SASE 能够进行私有化部署,置于证券公司的数据中心。它采用 AES-256 加密隧道技术,将网络连接封装于安全隧道之内。如此一来,可隐藏真实的网络地址与通信内容,令外部攻击者难以追踪和定位网络连接的来源及目的地,对常态化攻防演练中的安全水平提升大有帮助。

四、SASE是否满足信创要求？

目前国内较领先的 SASE 厂商已经提供信创版本,支持信创系统(UOS、麒麟)部署;支持鲲鹏、飞腾、海光、兆芯等信创芯片,满足信创环境。

五、SASE支持哪些操作系统？

Windows、macOS、Linux、UOS、KylinOS,并支持手机端 iOS、安卓系统使用 APP 进行 SDWAN 接入网络。

六、SASE必须要一次性部署全模块吗？

根据国内领先的厂家实际情况,可以拆分购买,随时添加功能,按需部署终端安全能力。

五、分支预算分析对比

传统架构方案中,每个证券营业部至少需要 2 台防火墙以及 1 台上网行为管理设备,且每年还会产生维保费用。具体情况可参照《证券营业部 IT 传统架构与 SASE 终端管理方案的成本对比表》。

SASE 方案具有诸多优势,初次建设费用低且支持弹性订阅,功能十分齐全,能够解决网点在实施桌管、网络准入、漏洞检查、合规检查、数据分类分级、DLP、SDWAN 等功能时面临的难题。经对比,五年的总费用大约仅为传统架构方案总费用的 40%。

对于证券公司而言,总部通过 SASE 可回收数据并进行

集中管理,这是其带来的最大效益。同时,SASE 降低了网点运维人力需求,在提升信息安全能力的同时实现了降本增效。

类别	项次	内容	传统架构方案	费用(元/年)	SASE 终端管理方案	
传统架构方案	1	营业部专线租用	A、B 类租用, C 类不租用 (带宽 4~10M)	带宽 3W (不含税)	参考 SD-WAN	SASE 已涵盖
	2	营业部 VPN(IPSec)	IPSec VPN 设备连接到分公司、分公司连接到总部	X	使用 SD-WAN 组网与分区	SASE 已涵盖
	3	防火墙设备	采用小型防火墙, HA 架构 (A/B, 冗余)	4.4W (A/B, 8500/395)	云原生防火墙, 全面云原生管理, 软件使用 SASE	SASE 已涵盖
	4	上网行为管理	采用小型上网行为管理设备, 以策略控制上网行为	8500/395	使用 SASE 替代上网行为管理功能	SASE 已涵盖
	5	网络准入管理系统	802.1X 为基础, 部分采用 ARP 技术	80 /人	使用 SASE 替代网络准入功能, 防范钓鱼攻击	SASE 已涵盖
	6	桌面管理系统	部分通过准入与桌面, 部分通过代理, IPG 也有部分市场	100 /人	使用 SASE 替代桌面管理系统功能	SASE 已涵盖
	7	终端安全软件 (EDR)	国产化产品逐步推广, 从单机杀毒转向 EDR、MDR	150/人	使用 SASE 实现终端安全, 杀毒软件	SASE 已涵盖
	8	漏洞扫描系统 (DLP)	终端漏洞扫描系统, 以 IPG、绿盟为主	500/人	使用 SASE 实现终端安全, DLP 功能	SASE 已涵盖
	9	漏洞扫描与补丁验证	绿盟、安恒、Nessus	X	使用 SASE 实现终端安全, 漏洞扫描与补丁验证	SASE 已涵盖
	10	漏洞扫描	绿盟、安恒、Nessus	X	使用 SASE 实现终端安全, 漏洞扫描与补丁验证	SASE 已涵盖
	11	安全合规检查	以策略形式进行	X	使用 SASE 实现安全合规检查与联动	SASE 已涵盖
传统架构方案五年总费用 (不含人力运维费用)			575,450.00		初次建设费用 (不含人力运维费用) (1200)	¥8,250.00
SASE 终端管理方案	1	总部 SASE 终端管理	A、B 类租用, C 类不租用	X		
	2	营业部 VPN(SD-WAN)	IPSec 设备连接到分公司、分公司连接到总部	X		
	3	防火墙设备	采用小型防火墙, HA 架构	4.4W		
	4	上网行为管理	采用小型上网行为管理设备, 以策略控制上网行为	1800~3700		
	5	网络准入管理系统	802.1X 为基础, 部分采用 ARP 技术	20 /人		
	6	桌面管理系统	部分通过准入与桌面, 部分通过代理, IPG 也有部分市场	40 /人		
	7	终端安全软件 (EDR)	国产化产品逐步推广, 从单机杀毒转向 EDR、MDR	60/人		
	8	漏洞扫描系统 (DLP)	终端漏洞扫描系统, 以 IPG、绿盟为主	100/人		
	9	漏洞扫描与补丁验证	绿盟、安恒、Nessus	X		
	10	漏洞扫描	绿盟、安恒、Nessus	X		
	11	安全合规检查	以策略形式进行	X		
SASE 终端管理方案五年总费用 (含 SASE 终端管理费用)			¥1,700.00		首次建设费用 (含 SASE 终端管理费用)	¥8,250.00
SASE 终端管理方案五年总费用 (含 SASE 终端管理费用+4 年维保)			¥104,250.00		首次建设费用 (含 SASE 终端管理费用)	¥41,250.00

图2《证券营业部 IT 传统架构与 SASE 终端管理方案的成本对比表》

六、效益说明与总结

SASE 如今已是一项成熟的终端管理方案。在国外,领先的证券行业与金融行业已采用此架构,且被证实为有效的 IT 管理方案。在我国,SASE 提供本地化部署,不依赖公有云,满足自主可控要求,同时实现数据留存于自有数据中心,这种做法更加可靠。推荐证券营业部采用 SASE 终端管理方案,它能有效解决网点 IT 运维人力不足的问题,同时增强终端信息安全防护能力。将全员终端设备部署终端防病毒、网络准入、SDWAN、多因素认证、桌面管理、上网行为管理、漏洞管理、数据分类分级、数据防泄露 DLP 等多种功能,满足网络链路加密、加速功能以及数据集中、策略下发等监管要求,大大节省了传统架构的初次部署与运维费用。对于证券公司合并、营业部转型而言,SASE 是最有利的降本增效方案,节省运维人力,而这或许才是最大的成本节省之处。

参考文献

- 1.Secure Access Service Edge (SASE): A New Architecture for the Digital Enterprise.
- 2.SASE in the Context of Cloud Computing and Network Security.
- 3.2024-2026 年中国证券业 ICT 应用市场深度分析及投资战略咨询报告。

05 热点解读

P88 假冒证券基金经营机构网络诈骗活动风险危害及应对流程
证券期货行业网络安全创新实验室

P93 量子计算对基础安全带来的挑战和应对措施
证券期货行业网络安全创新实验室

P96 证券基金经营机构电子数据取证与分析研究
证券期货行业网络安全创新实验室

假冒证券基金经营机构 网络诈骗活动风险危害及应对流程

证券期货行业网络安全创新实验室

摘要： 本文从实践的角度，详细介绍了证券基金经营机构反网络钓鱼面临的挑战,常见钓鱼手法,总结了主要的监测与处置应对措施,可以帮助证券基金经营机构实现对网络钓鱼的事前监测、事中处置、事后补救的全流程管控。

关键字： 假冒钓鱼、网络诈骗、全流程措施、主动监测、拦截关停

一、背景

近期全国各省市证监局陆续发布《开展集中整治假冒证券基金经营机构等诈骗活动专项行动》通知,要求各证券基金经营机构加强行业监测预警分析,积极借助第三方力量,主动对假冒证券基金经营机构等网络诈骗活动进行持续监测,常态化巡查、监测互联网上是否出现新的假冒公司网站、APP 下载站点、客服电话、社交账号等,如发现相关情况及时举报,并通过官网及时发布提示性公告、联系相关服务商等方式尽快阻止假冒行为。

二、面临挑战

据国家互联网应急中心(CNCERT)发布的《网络安全信息与动态周报-2024年第10期》数据显示,进入2024年,境内仿冒网页数量快速增长,3月4日-3月10日环比增长高达77.7%,如下图所示:

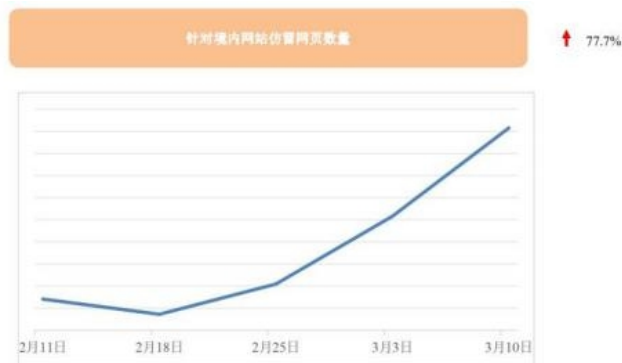


图1 针对境内网站仿冒网页数量

据北京亿盾互联科技有限公司发布的《钓鱼网站侦测报告》数据显示,2023年共监测证券业钓鱼网站 16346 例,涉及数十家券商,如下图所示:

2023年证券业钓鱼网站统计

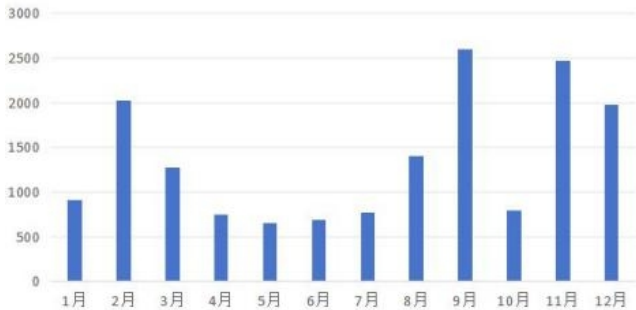


图2 2023年证券业钓鱼网站统计

据公安部 2024 年 1 月 9 日举行新闻发布会得知,2023 年,全国公安机关共 破获电信网络诈骗案件 43.7 万起,缉捕 263 名电信网络诈骗犯罪集团重大头目和骨干,拦截诈骗电话 27.5 亿次,短信 22.8 亿条,处置涉诈域名网址 836.4万个,紧急拦截涉案资金 3288 亿元。

面对日益增加的网络钓鱼攻击,证券基金经营机构客户面临网络诈骗威胁。主要体现在:

1. 钓鱼网站

钓鱼网站是指欺骗用户的假冒网站。“钓鱼网站”的页面与真实网站界面相似,欺骗消费者或者窃取访问者提交的账号和密码信息。钓鱼网站是互联网中最常碰到的一种诈骗方式,通常伪装成银行及电子商务、窃取用户提交的银行账号、密码等私密信息的网站。典型钓鱼网站案例如下图所示:

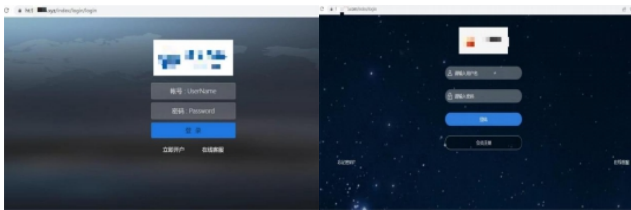


图3 钓鱼网站示例

2. 假冒 APP

假冒 APP 指具有与被假冒的官方 APP 相似的应用图标或应用名称的一类APP,存在假冒官方名义、非法收集客户信息、实施投资理财诈骗、传播违规内容、植入恶意代码等一系列风险,同时给官方声誉造成严重的社会不良影响

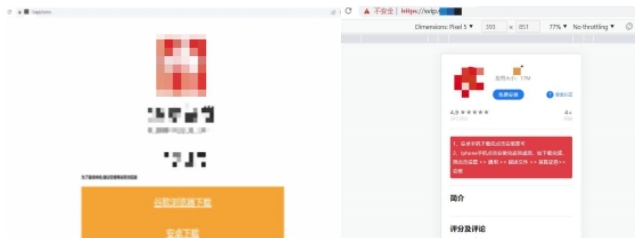


图4 假冒 APP 示例

3. 钓鱼公众号

钓鱼公众号是指欺骗用户的虚假公众号平台,涉及平台包括微信的公众号、小程序、视频号,以及支付宝生活号。不法分子通过钓鱼公众号来开展虚假活动宣传、骗取客户资金、套取敏感信息、传播木马工具等行为,致使网民遭受重大财产生命损失,造成个人隐私泄露。而且,由于这类公众号基于微信、支付宝的熟人社交平台,且很多用户绑定了银行卡,对于诈骗团伙来说更容易完成网络诈骗闭环。典型钓鱼公众号案例如下图所示:



图5 钓鱼公众号示例

4. 钓鱼社交媒体

钓鱼社交媒体是指欺骗用户的虚假社交媒体,涉及的社交媒体包括抖音、快手、微博、小红书等。不法分子通过钓鱼社交媒体,欺骗用户参与虚假活动,达到非法目的;这可能包括诱骗资金转移、获取敏感信息或散布恶意软件。这些行为侵犯用户权益,对社会秩序构成严重威胁。典型钓鱼社交媒体如下图所示:

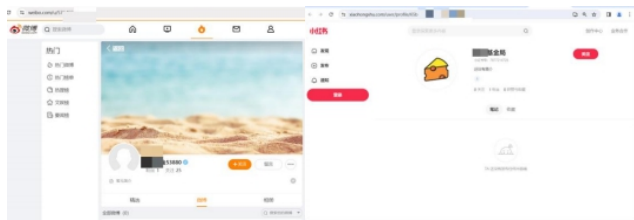


图6 钓鱼社交媒体示例

5. 假冒客服电话

近几年不法分子频繁通过招标、招聘、微博、贴吧等信息发布平台,发布假冒客服电话来开展虚假活动宣传、骗取客户资金、套取敏感信息、传播木马工具等诈骗行为,致使网民遭受重大财产生命损失,造成个人隐私泄露。典型假冒客服电话案例如下图所示:



图7 假冒客服电话示例

6. 假冒客服短信

假冒短信是一种常见的欺诈形式,因为不法分子利用人们对于证券基金经营机构的信任来发送诈骗短信。近几年由于数据泄露事件频发,不法分子手里可能掌握着“较为准确”的客户信息,导致假冒短信的伪装性、欺骗性越强,配合着如假冒网站、假冒APP等其他手段,侵犯人们的个人财产权、个人隐私权。典型假冒客服短信案例如下图所示:

冒充证券公司发送荐股短信 男子观察一个月后仍陷骗局

2018-11-04 22:24

人民网北京11月4日电“我知道不少骗子打着荐股的旗号诈骗,所以刚开始我并没理睬,可是荐股发了一个多月,感觉荐股的很准,我就忍不住上当了,没想到被骗了这么多钱。”11月4日,居民王先生带着与骗子短信联系及转账记录到北京市公安局下辖区分局报案,称被骗。

据了解,王先生是一个股民,平时比较关注股票的涨跌信息。一个月前,王先生手机上收到一个“1066347xxx”号码发送的短信,短信自称来自知名“某证券”,内容是近期的推荐股票和涨停股信息。此后一个多月,王先生每天收到该号码的短信,刚开始王先生认为这是诈骗信息,没有予以回复。时间长了,王先生每天关注股市,认为短信所提供的信息比较准确,因此对该号码不再怀疑。

10月26日,王先生加了短信所留的微信号,该微信号除继续发送荐股和涨停股信息外,还多次建议王先生加入会员,以获得更大的利益。王先生为了获利,先是缴纳了3980元会费,成为某网站的注册会员。为了显示其正规性,该微信号还以“某证券有限公司”的名义给王先生发了一张“投资咨询服务”发票,指定了“导师”,合同内称注册会员需向对方办理认证资金1万元,用于集合竞价拉升股票互惠互利,王先生此时已经深信不疑,在缴纳1万元后,“导师”又说1万元太少,不够操作,诱导王先生再次投入5万元。当钱转到对方账号后,王先生发现对方并没有给自己买股票,于是要求对方退款,此时该微信号已将王先生拉黑。拨打“导师”所留的电话,对方也不接听,王先生这才知道自己被骗了。



图8 假冒客服短信示例

三、应对措施

证券基金经营机构要想有效应对各类网络诈骗问题,需要体系化、全局化角度来综合考虑应对措施,以便闭环、完整解决问题。从证券基金经营机构角度出发,核心目标可分为三项:

- 1.主动作为，尽量避免客户被网络诈骗；
- 2.监测感知，及时发现风险、处置风险；
- 3.借助行业、国家生态力量，黑灰产对抗；

为达成以上三个目标，建议可以从加强内部管理、加强监测发现能力、加强真假研判能力、事中处置、复盘改善这五个过程做起，主动作为，避免对国家、社会、人民、机构声誉造成不必要的损失，具体过程详见下图：

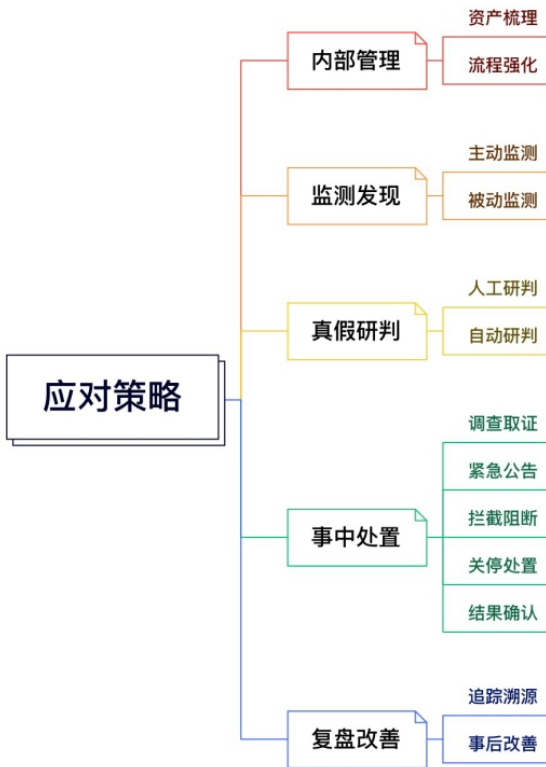


图9 应对措施内容

1.内部管理

证券基金经营机构在日常开展工作的过程，无法避免需借助第三方渠道、平台、供应商等进行对外宣传、业务获客等工作。在这过程中，证券基金经营机构需强化内部流程管理、人员管理、供应商管理工作，一方面避免因疏忽导致发生网络诈骗事件，另一方面也是为后续的监测提供辅助价值。

(1) 资产梳理

证券基金经营机构需要梳理清自己有多少对外的“窗口”，形成一张“窗口”“资产台账”，一方面，该台账内资产是机构重点监测和保护的对象列表，另一方面也便于后续真假研判工作的顺利开展。（从技术侧看，监测与研判需要依赖“白样本”的输入，将监测到的数据与“白样本”数据进行比对得出是否构成仿冒诈骗，此处的“白样本”即指《资产台账》）

针对网站，台账内建议包含“域名”“IP”“网站名称”“备案信息”“图标信息”“域名指纹特征（如dom_hash、html_

hash等）”。

针对APP/小程序，台账内建议包含“APP备案信息”“APP发布站点”“App包名称”“Apk指纹特征（如MD5）”“证书指纹特征（如MD5）”。

针对宣传渠道，如小红书、微博、公众号、知乎等社交媒体，台账内建议包含“渠道名称”“账号名称”“账号注册信息”。

针对客服、短信渠道，台账内建议包含“渠道名称”“号码”“短信关键内容”。

(2) 流程强化

证券基金经营机构也需要加强内部人员、流程、供应商的流程管理能力。避免因内部人员无意泄露机构官方媒体账号导致账号被用于网络诈骗，避免因无内容审核机制，内部人员可以任意编辑对外发送的内容导致用户被诱导甚至诈骗的情形，对机构声誉造成严重影响，甚至带来法律风险。

2.监测发现

(1) 被动监测方式

网络钓鱼监测方法分为主动监测和被动监测，证券基金经营机构传统上采用被动监测的方式，包括：人工举报发现、情报共享发现、渠道收集发现和监管通报发现。

由于网络钓鱼攻击的隐蔽性和即时性，被动监测方法往往只能在攻击发生后才能发挥作用，而无法在攻击发生前、发生中，及时预警或阻止；所以，被动监测方法存在时效性差、信息准确性不足、覆盖范围有限等诸多不适应网络钓鱼攻防特点和业务保障要求的问题。

被动监测关键点：

■建立举报/信息收集的机制，并对外公示该机制（如投诉举报联系方式），以便尽快能获悉事件，降低事件潜在影响性。

(2) 主动监测方式

在采取被动监测的同时，更需要主动监测的技术手段，以便更及时、有效地应对网络钓鱼威胁。

网络钓鱼主动监测方法，需要对整个全球互联网，进行7*24小时监测，覆盖境内外网站、APP、公众号、社交媒体等网络钓鱼渠道。

考虑到网络钓鱼攻击的手段越来越隐蔽、发现难度大，以及攻击时效性强、往往在短时间内迅速传播和变化，建议使用IP发现、反查发现、搜索发现、域名发现、衍生发现、爬虫发现等主动监测技术手段。

主动监测关键点：

■可监测渠道的覆盖率；

■监测节点的在线率；

■空间搜索引擎的准确性；

3.真假研判

(1) 人工方式

人工方式对网络钓鱼进行真假甄别,通过比对官方或合作伙伴数据,凭借个人经验来判断,经常出现误报情况。

(2) 自动方式

■黑白名单过滤:

对积累的海量官方数据和网络钓鱼数据,进行清洗和结构化,形成网络钓鱼黑白名单,在进行智能识别前进行过滤,提高识别效率,降低误报风险。

■深度机器学习:

对历史积累的海量网络钓鱼数据,采用深度机器学习算法进行模型训练,形成风险评估模型,智能识别具有高度模仿和相同攻击手法的新增未知网络钓鱼,有效地提升了检测速度和准确性。

4.事中处置

在发现并确认了网络钓鱼数据后,要快速进行事中处置,典型的处置过程包括如下环节:

(1) 网络钓鱼的调查取证

证券基金经营机构在调查取证过程中,对关键内容一定要让受害用户保存好截图、录音和视频,然后再完善其他信息,形成完整证据链。

(2) 发布紧急公告

证券基金经营机构在调查取证过程后,一旦确认该事件真实准确,需及时通过公众号发布信息公告、APP推送、短信推送等方式进行提示性预警,避免出现更多受害者导致事态进一步恶化。

(3) 网络钓鱼的拦截阻断

证券基金经营机构在处置网络钓鱼事件前,建议优先做拦截阻断,以提升处置效率,降低网络钓鱼欺诈风险。网络钓鱼拦截方法主要包括:

■终端拦截:通过向国家反诈中心、12321、12377、360、腾讯、微软、谷歌等渠道投诉,在用户终端对网络钓鱼进行拦截、警告,阻断,防止用户访问上当受骗;

■网关拦截:通过向国家反诈中心、电信、移动等运营商投诉,在网络出口对网络钓鱼进行拦截、警告,阻断,阻止用户继续访问,防止用户访问上当受骗。

(4) 网络钓鱼的关停处置

证券基金经营机构在网络钓鱼处置过程中,要掌握正确的方法,第一要定位准确,第二要材料齐全,第三找到有效的投诉方式。

网络钓鱼处置方法,域名冻结、停止解析、删除托管、应用下架、账号冻结、内容替换等。为了保障处置效率,建议多路并行进行投诉。网络钓鱼处置的投诉流程如下图所示:

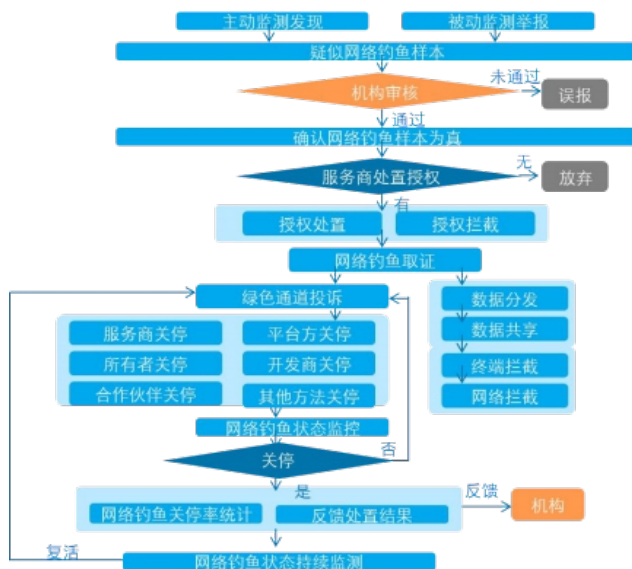


图10 网络钓鱼处置流程

(5) 网络钓鱼的结果确认

最后,需要对网络钓鱼处置结果进行确认,确认的内容包括:网络钓鱼内容拦截情况、关停情况和复活情况。为了保障网络钓鱼处置结果确认的有效性,建议采用多种确认方法,如:不同电脑、不同手机、不同用户、不同地区、不同通信链路打开确认。

5.事后改善

在对网络钓鱼进行了事中处置后,还需要进行事后的改善、优化工作,主要包括:

(1) 网络钓鱼的补救措施

证券基金经营机构在在网络钓鱼处置后,需要综合分析并采取措施对存在的薄弱环节进行安全加固,防止网络钓鱼攻击再次发生,常见的补救措施包括:

■提醒疏导:对已经被窃取密码和盗取钱款的受害用户,进行电话、短信提醒,心理疏导;

■加固升级:对已经被窃取密码的受害用户,进行账号查封,待密码重置后恢复使用;提高交易安全策略,增加安全认证强度;

■干扰对抗:对网络钓鱼进行反向干扰,消耗对方资源;编写自动化脚本,输入干扰数据;

■交易反诈:启动核心系统交易反欺诈机制,对异常登录、异常交易、黑产账户等进行拦截;

■修补漏洞:修补业务系统漏洞,防止被诈骗团伙利用实施网络钓鱼攻击。

■学习演练:制定反网络钓鱼应急预案、制度和流程,并定期进行学习和演练。

■购买服务:购买第三方专业的反网络钓鱼安全服务,提供网络钓鱼监测发现和关停处置能力;

■其他:向当地公安机关报案,抓捕犯罪嫌疑人。

(2) 网络钓鱼的追踪溯源

有技术实力的证券基金经营机构，在事中处置了网络钓鱼事件后，还建议对钓鱼网站、假冒 APP、钓鱼公众号、钓鱼社交媒体、假冒客服电话，进行溯源分析，追踪受害用户、嫌疑人的具体情况，为后续打击抓捕和加固补救提供数据支撑。

四、事中处置措施经验分享

(1) 事中处置-拦截经验分享



图11 事中处置-拦截类效果示例图

表1 常见拦截渠道清单

处置类型	分类	具体渠道	
拦截	社交软件类	QQ	微信
		微博	小红书
		知乎	贴吧
	浏览器类	360 浏览器	safari 浏览器
		IE 浏览器	UC 浏览器
		华为浏览器	Firefox 浏览器
		QQ 浏览器	Oppo 手机浏览器
		Vivo 手机浏览器	搜狗浏览器
	安全软件类	腾讯管家	金山
		360 安全卫士	安天

(2) 事中处置-关停经验分享



图12 事中处置-关停类效果示例图

表2 常见关停渠道清单

处置类型	分类	具体渠道	
关停	监管关停	CNCERT	12321 工信部
		通管局	国家反诈中心
	DNS 停止解析	阿里云	帝恩思
		聚名网	dnspod (腾讯)
		新网 xinnet	百度智能云
		青云 QINGCloud	西部数码
		中科三方	
	停止主机服务	腾讯	阿里
		华为	移动云
		天翼云	联通云
		金山云	世纪互联
		优刻得 UCLLOUD	Microsoft Azure
		AWS 亚马逊	Cloudflare
		godaddy	

注:关停通常需要给对应的渠道提供相关材料,常见的如营业执照、授权书、商标权属证明等

五、总结

本文从实践的角度,详细介绍了证券基金经营机构反网络钓鱼监测与处置的应对措施,可以帮助证券基金经营机构实现对网络钓鱼的事前监测、事中处置、事后补救的全流程管控,以便满足《开展集中整治假冒证券基金经营机构等诈骗活动专项行动》通知要求。

量子计算对基础安全带来的挑战 and 应对措施

证券期货行业网络安全创新实验室

摘要：量子计算技术的快速发展将对现有的公钥加密体系产生颠覆性的影响，现阶段部署的一些经典密码算法（特别是公钥密码算法）将受到巨大的安全性挑战。量子计算机的到来，将对当前密码技术带来颠覆性影响，严重影响信息系统安全与稳定运行，甚至影响国家安全。围绕抗量子计算的新一代密码技术——后量子密码成为全球竞争的焦点和战略抓手。根据NIST的最新公布的研究报告可知，美国将在2024年底发布正式的后量子密码算法标准，并于2030年完成后量子密码的迁移应工作，这对现有的基于传统公钥密码体系实现数据隐私和信息安全的行业具有重要现实意义。本文简要分析了量子计算技术对现有的基础安全带来的威胁和挑战、后量子密码技术的实现原理、技术路径、应用前景和迁移规则，并对存量加密系统的后量子密码平滑迁移方案给出了相关建议。

关键字：量子计算、密码技术应用、抗量子密码(PQC)、后量子密码

一、背景与挑战

量子计算是一种利用量子力学原理来进行信息处理的技术。与传统的经典计算不同，量子计算使用量子比特(qubit)作为信息的基本单位，量子比特可以同时表示0和1的状态，使得量子计算机在处理大量数据时具有极高的并行性，算力将会实现爆发式的增长。由于量子计算机在密码破译、物质模拟等领域有望带来革命性的进展，普遍受到了各国政府、全球科研机构 and 巨头企业的重视。美国在2018年签署“量子科技发展战略”，欧盟在2020年发布“欧洲量子计算战略”，日本在2017年制定“量子科学技术战略”。在生态方面，产业侧2017年IBM成立量子计算产业联盟，2022年其量子处理器Osprey已经达到了433量子比特，预计未来3年将突破1000量子比特，到2030年实现100万量子比特。国内的量子计算生态也在逐渐构建，诞生一批如阿里巴巴达摩院量子实验室、本源量子、国盾量子、启科量子、格尔软件等企业，专门从事量子计算研究和开发工作，开展各种基础研究和应用实践。2020年，美国白宫网站发布的《美国量子网络战略构想》提出，开发一种由量子计算机和其他量子设备组成的量子互联网的设想，并指出下一步的工作是使量子信息科学全民化。2021年，中国提出了新的“十四五”规划，指出这5年是中国量子技术实现“弯道超车”的关键时期，其目标之一就是研制通用量子计算原型机和实用化量子模拟机。

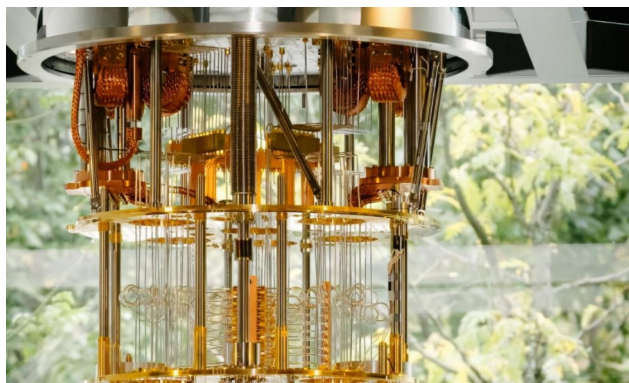


图1 50比特量子计算机

量子计算机发展将带来算力的爆发式增长，可以解决大量复杂的数学问题，加上Peter Shor提出的Shor算法，给当前已经发展成熟并且应用广泛的现代密码体制带来了巨大的威胁与严峻的挑战。

对于非对称加密算法，如RSA、SM2、ECC，其安全性依赖于大数分解和离散对数问题的难度。Shor算法能够在多项式时间内解决这些问题，这意味着一旦有足够强大的量子计算机，就能够破解这些非对称加密算法。例如，RSA算法的安全性基于将两个大素数相乘的难度，而量子计算机可以快速分解这样的乘积分解，从而破解密钥。对称加密算法，如AES，其安全性依赖于密钥的保密性。Grover算法表明，量子计算机可以在平方根时间内搜索密钥空间，从而破解对称加密算法。这意味着，如果密钥长度为n比特，量子计算机只需要大约 $n/2$ 比特的量子比特就能破解该密钥。总体来说，在量子计算时代，RSA、SM2、ECC算法已经不再安全，需要升级换代为抗量子密码算法，对称算法和杂凑算法可以通过增加密钥长度来提高安全等级，影响相对小一些。

表1 算法安全挑战

密码体制	密码算法	图灵模型 安全强度	量子模型 安全强度	主要量子 模型算法
公钥体制	RSA-2048	112bits	不安全	Shor Regev RV
	RSA-4096	144bits		
	ECC-256	128bits		
	ECC-384	192bits		
	SM2	128bits		
对称密码	AES-128	128bits	64bits	Grover
	AES-192	192bits	96bits	
	AES-256	256bits	128bits	
	SM4	128bits	64bits	
密码杂凑	SHA-256/SHA3-256	128bits	80bits	Grover
	SHA-384/SHA3-384	192bits	128bits	
	SHA-512/SHA3-512	256bits	160bits	
	SM3	128bits	80bits	

二、典型风险场景

在实际的应用层面，后量子密码算法的应用场景涵盖几乎所有领域，特别是对于安全性和数据敏感性要求高的金融行业挑战很大。例如金融领域的身份验证和访问控制、现有采用经典公钥加密体系的区块链、可信计算、医疗领域敏感数据的隐私保护、工业控制领域的复杂传感器系统的安全通信、电力系统的分布式能源网络的最后一公里安全等。

证券交易过程中，密码技术发挥的作用为：(1) 通过动态令牌或数字证书客户端工具实现用户和券商的身份认证，保证身份真实性、合法性。(2) 客户端与交易系统之间建立基于密码算法的加密传输通道，保证数据在网络传输过程的保密性。(3) 通过数字签名技术和散列函数保证交易信息不被篡改，保证了交易信息的完整性。(4) 通过数字证书和数字签名技术保证了用户和券商的交易行为的不可否认性。

证券行业密码技术应用场景受到量子计算安全威胁主要包括：

- (1) 传统安全的密码算法强度不再安全；
- (2) 传统安全的密码算法协议不再安全；
- (3) 系统的安全性同时依赖于上述两者。

其次，对于需要长久保护的高敏感数据，存在前向安全风险，即未来的量子计算机可能会破译这些机密数据。一些恶意组织将当前无法破译的信息保存起来，等到量子计算机商业化之后再破译和攻击，以获取商业机密。所以，即便量子计算机 10 年或 20 年之后才具有实质威胁，如果当前传输的数据具有较长期限的机密性或敏感性要求，那么这些数据仍然具有前向安全风险。因此在关系国防安全、国计民生、商业机密的战略领域应该尽早开始部署后量子密码技术。目前如常用的 TLS 协议，TLS1.2 中 DHE、ECDHE

支持前向安全，TLS 1.3 全都支持，但在量子计算带来的威胁下，TLS 工作组扩展了 TLS 1.3，使用外部预共享密钥来抗量子攻击。IPSECME 工作组 2020 年发布了 RFC 8784，在 IKEv2 中支持混合预共享密钥以抗量子攻击。2022 年发布了 RFC 9242，为 IKEv2 协议的后量子演进提供支持。2022 年扩展了 RFC 7296 使 IKEv2 支持多重密钥交换，包含后量子密钥交换。

后量子密码技术作为一种全新的加密体系，从长远来看是现有公钥加密体系的有机补充和替代。随着后量子标准化评选工作进入尾声，传统的加密基础设施向后量子密码方案迁移已成为重要的发展趋势。如何在现阶段设计有效的后量子密码平滑迁移方案，同时在实例化部署过程中实现后量子密码与现有存量加密设备的低成本工程化适配，是一个需要重点研究和解决的问题。

三、应对措施

抗量子密码 (Post-quantum Cryptography, PQC)，也称之为后量子密码，是能够抵抗量子计算机对现有密码算法攻击的新一代密码算法。在量子计算时代来临之际，我们需要对现有的密码体制进行升级换代，使得我们的交易系统具备抗量子计算攻击的能力。

当前，学术界也在大力推动抗量子密码相关技术的研究，抗量子密码技术主要分为基于格的、基于哈希的、基于多变量的、基于编码的、基于多源的等多种技术路线。从安全性、资源开销、适用场景三个方面对入选方案进行综合评估。多变量密码方案一般公钥尺寸较长，所依赖的底层数学问题是求解多变量平方等式，缺乏严格的基于复杂性规约的可证明安全。基于哈希的方案和基于编码的方案所对应的底层数学问题分别是抗第二原像攻击和随机线性码解码，也存在同样的安全性问题。另外基于哈希的方案仅适用于数字签名，不能用于公钥加密和密钥协商，而编码基方案的私钥和公钥矩阵维度过高，计算较为复杂。基于同源的方案还处在理论研究阶段，存在大量尚未解决的实际问题，均不适合广泛应用。格密码方案能够更好地平衡安全性、公私钥尺寸、计算速度三个方面的因素，被认为是最有希望标准化的技术路线之一。

在目前的格基密码中，有两条路线：LWE 和 NTRU，前者技术成熟、安全性、性能、容错等各方面能力都很好，但是存在较为复杂的专利制约因素。NTRU 是历史最悠久的实用抗量子格基密码体制，且没有专利限制。中国学者基于 E8 编码格技术提出的 CTRU 密钥封装机制改进了传统基于 NTRU 的不足之处，与美国 NIST 目前唯一标准化的基于 LWE 技术路线的 Kyber 密钥封装算法，CTRU 在安全性、计算效率、带宽、以及错误率方面性能全面超越 Kyber。在实际应用层面，CTRU 方案同时具备较好成熟度和稳定性，并且不存在任何

专利问题,具备更好的工程化基础和实用化前景。

从宏观层面出发,随着后量子标准化评选工作进入尾声,传统的加密基础设施向后量子密码方案迁移已成为重要的发展趋势,据NIST的最新研究报告可知,美国将于2030年完成后量子密码的迁移工作,这对于整个密码学领域的学术研究和产业应用来说都是一次重大的机遇和挑战。要做好后量子密码的应对,具体的设计方案应重点考量三个方面的因素:(1)在抗量子安全迁移方案中,针对敌手“先截获、后破译”的前向安全风险,对保密通信链路进行抗量子前向安全增强具有更高的优先级和迫切性。(2)通信链路的抗量子前向安全增强要综合考量技术因素和成本因素。具体地,需要在过渡阶段首先解决与现有的大量存量密码设备进行低成本平滑兼容的关键问题。(3)在我国后量子密码标准正式颁布之前,核心的通讯协议需要为密码算法的优化和改进提供兼容空间,这对于抗量子安全迁移方案的商业应用具有重要的现实意义。

四、抗量子密码迁移建议

量子计算机预计将在2030年得到规模化应用,所以抗量子密码的推广及迁移到了刻不容缓的地步。美国政府非常重视抗量子密码技术的应用,抗量子密码技术被美国作为保持“先发优势”、遏制中国“后发优势”的关键手段,被美国列为制衡中国崛起的7个优先事项之一。在标准方面,2022年9月美国发布了抗量子迁移时间表:2030年基本完成抗量子迁移,2033年全部完成抗量子迁移,并积极引导科技企业进行PQC迁移。当前,谷歌等科技巨头已经开始在其浏览器等产品中采用抗量子密码技术,苹果公司也在其iMessage产品中使用了抗量子密码技术,亚马逊已经将混合后量子 TLS 与 Amazon KMS 结合使用。除了美国以外,欧盟也在积极响应美国的迁移要求,加速商业化进程。

我国也非常重视抗量子密码技术的研究和应用,2018年后量子密码被中国科协列为60个我国亟待解决的重大科技难题之一,并在军事、外交等关键基础领域具有重要的应用需求。2019年我国开展了抗量子密码算法设计竞赛,共14套算法获奖,其中12套算法为格基密码;2020年中国人民银行发布了金融系统应用后量子密码技术指南;2023年复旦大学的CTRU算法在国家密标委立项,正式启动商密领域标准转化工作。

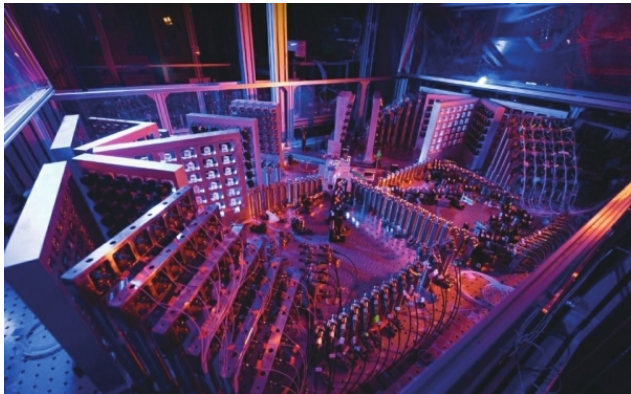


图2 九章二号量子计算机

推进抗量子密码迁移是一项复杂的系统工程,需要政策引导、技术研发、标准化建设、人才培养、资金支持等多方面的协同努力。一是提早布局,确保平稳过渡到量子安全的密码体系中。后量子密码迁移是一项极为复杂的长期系统性工程,需要耗费相当长的时间,必须提前规划。密码迁移通常要全面考虑算法安全性、算法性能、实施的便利性、合规性等方面。以往密码安全体系的迁移工作历时往往达到10年以上,如ECC早在20世纪80年代就被提出,花了20多年才获得广泛的采用,目前我国的SM系列国密标准的推广时间也约为10年。相比之下,后量子密码的过渡更为复杂,周期可能更长。考虑到未来不断增长的密码安全需求,每一类别的后量子密码都只适用于部分应用场景,因此需结合应用场景的实际需求具体选择,客观上增加了后量子迁移的复杂程度。二是尽量不改变上层PKI以及下层对称密码,对现有系统安全架构影响最小。主要为随着现有PKI底层硬件及系统逐步升级迭代以对标准的后量子时代密码算法扩展支持。三是结合国家相关标准和监管要求,制定符合行业特点和场景的标准制定,加快量子计算等前沿技术的研发和应用推广。

参考文献

- 1.《后量子密码应用研究报告》
- 2.《Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process》
- 3.<https://blog.cloudflare.com/tag/post-quantum>
- 4.吕仲涛:量子计算对银行密码算法的威胁及对策
- 5.金磐石:量子信息技术在金融领域的探索实践
- 6.唐明环、许一骏、徐秀:加强商用密码在金融行业应用

证券投资基金经营机构电子数据取证与分析研究

证券期货行业网络安全创新实验室

摘要：本文从实践的角度，结合证券投资基金经营机构常见的典型安全事件场景，简要介绍了在发生相关安全事件时证券投资基金经营机构如何获取必要的证据，通过常用的取证手段和流程妥善保障证据的真实性和完整性，如何准备相关报告，以更好履行配合监管调查的义务。

关键字：电子数据、取证分析、典型场景、取证分析流程

一、背景

随着计算机犯罪及网络失泄密案件的频繁发生，电子数据证据作为一种新的证据形式势必越来越多的出现在司法活动中。1984年，美国FBI成立专门的计算机核查小组，成为电子数据取证的开始。2001年，我国正式引入计算机取证概念，2012年至2014年，民事、刑事、行政三大诉讼法正式将电子证据作为独立的诉讼证据之一。近些年来，大国纷争不断，以网络为媒介的攻击手段层出不穷，电子数据取证技术在网络攻击窃密、反欺诈调查、内部审计、失泄密痕迹发现、恶意网站查处等场景可以发挥举足轻重的作用。

证券投资基金经营机构涉及全国上亿证券基金业务参与人群的敏感信息，其中又涉及大量高净值人群，数据价值大、数据转化率高，一直是境内外黑客、敌对势力、黑灰产团伙、商业间谍的重点攻击目标，因此面临的安全压力极大。证券基金行业也是强监管行业，需要满足监管合规要求，并在发生安全事件后，履行配合监管调查的义务，这就离不开电子取证与分析技术。当发生安全事件后，证券投资基金经营机构需要获取必要的证据，并妥善保管，保障证据的真实性和完整性，以支撑后续的分析 and 监管报送任务。

二、关键名词解释

电子数据(Electronic Data)：是指基于计算机应用、通信和现代管理技术等电子化技术手段形成包括文字、图形符号、字母、数字等的客观资料。

电子数据源：是指存储电子数据的存储介质，常见例如硬盘、磁盘、数据库、存储服务器等。

电子数据取证：是指对电子数据源里的电子数据证据进行发现、固定、提取、分析、检验、鉴定、出示、存档的全过程。

三、行业电子数据取证与分析典型场景

场景1.网络安全入侵取证场景

经营机构安全从业者对于网络安全入侵场景下的取证分析一定再熟悉不过了。以网络安全经典模型——PDRR为例，PDRR将网络安全保障划分成防护、检测、响应、恢复这四个重要环节，其中“取证分析”即对应应在“响应”环节。网络安全事件处置过程中，需要进一步调查原因，首要目的是查漏补缺，发现网络安全管理中存在的问题和漏洞，进行响应恢复工作。如果是人为网络攻击或破坏行为，分析取证的重要目的之一就是追责。惩治责任人或犯罪份子。

在实际的实践中，分析取证工作贯穿整个网络安全应急处置全过程，安全事件的原因调查分析也有助于更好地理解黑客攻击行为和作案特征，一方面调查真相用以追责，另一方面形成黑客画像、威胁情报、特征检测规则等，反哺安全运营工作。

常见技术类型：

■ **内存取证技术：**网络攻击内存化和网络犯罪隐遁化，使部分关键数字证据只存在于物理内存或暂存在页面交换文件中，这使得传统的基于文件系统的计算机取证不能有效应对。通过全面获取内存数据，详尽分析内存数据，并在此基础上提取于网络攻击或网络犯罪相关的数字证据。常见例如明文密码、密钥等信息(如BitLocker、TrueCrypt等密钥)，文档打开记录、即时通信信息(如聊天软件内容)、用户密码Hash、驱动程序信息、服务信息、加载动态链接库等信息。

■ **数据包分析与取证技术：**数据包分析也称为流量分析或协议分析，指的是捕获网络上在线传输的数据用以分析是否包含恶意流量、恶意行为。常见是通过Web应用防护系统(Waf)、入侵防护(IDS)全流量探针等对流量数据进行检测，具体分析数据包常用工具如Wireshark、Tcpdump等。

■ **数据库取证技术：**大量的攻击最终的目的是瞄着经营机构的“宝藏”——数据库，数据库已成为犯罪分子的首

要目标,大量数据库被“拖库”用于网络盗窃和网络诈骗等活动。数据库具备完善的日志,因此数据库日志模块也记录了大量证据,可以根据这些证据回溯犯罪过程、固定证据并确定入侵者。常见工具包括数据库自带日志功能(存在被入侵者删除的风险)、日志审计工具、数据库审计工具等。

■Linux系统取证技术:Linux系统多用于服务器,相较于PC终端的Windows系统,面临的风险更大。本质上, Linux和Windows取证程序并无较大差异,主要内容都是现场勘验和电子证据检验鉴定两种方式。现场勘验的目的是为了分析提取证据数据,如网络连接信息、系统进程信息、日志信息、文件信息等。电子证据鉴定是指在确保电子证据合法有效、不被恶意篡改的情况下,使用相关取证设备进行分析。现在多用一些自动化脚本进行现场勘验,如基线比对脚本。

■恶意程序分析技术:恶意程序分析技术即恶意代码分析技术,主要可分为静态分析和动态分析两大类。静态分析方法是在没有运行恶意代码时对其进行分析,而动态分析方法则需要运行恶意代码,对相关行为进行检测,多在沙箱、虚拟机环境中执行。

■动态仿真取证分析技术:这是最新的一类技术,是一种基于仿真技术的取证方法,可以将物理磁盘或磁盘镜像中的操作系统进行模拟运行,以所见即所得的方式运行。该方法不局限于网络、操作系统、恶意代码等单点取证分析,而是模拟原始操作系统环境和应用服务并将之视为整体,可以无限次还原安全事件发生时的状态,给予恶意程序充分发挥的“土壤”,以进行取证分析。目前常用的工具包括LiveView(开源)、GetData、ATT-3100等。

场景2.钓鱼仿冒诈骗取证场景

证券基金经营机构一直面临着钓鱼网站、仿冒APP等风险,不法分子针对经营机构制作对应的仿冒官网、APP、社交媒体公众号,用以诱骗经营机构的用户进行下载以进行诈骗。这对于经营机构会造成商誉的损失,甚至会招致监管处罚和客户的流失,对机构带来较深的负面影响。为此,全国各省也发布《开展集中整治假冒证券基金经营机构等诈骗活动专项行动》通知,要求机构尽快阻止假冒行为。

从取证分析角度看钓鱼仿冒这个场景,当机构发现钓鱼仿冒网站、APP时,应当及时收集数据并固定证据,向相关监管部门提交证据,及时进行下架处理,并对仿冒运营主体进行维权诉讼。

常见类型:

■仿冒APP取证分析:在仿冒APP或APP侵权纠纷中,确定仿冒APP运营主体是案件得以推进的前提。通常仿冒APP的名义运营者都是经营机构,但实际运营者通常都是犯罪团伙,需要尽量锁定背后实际运营者。常见的可通过抓包技术进行,抓取、分析APP向服务端发送的请求,获得相

关APP的请求对象、服务器地址等信息,借助此类信息进一步锁定背后犯罪团伙。

■钓鱼网站取证分析:针对钓鱼网站,更多的是获取并分析钓鱼网站的注册信息,可通过域名注册网站(如万网)获取网站的备案信息、域名指纹特征信息进行取证分析。备案信息多用于确认域名服务商、注册人员等信息。

■钓鱼邮件取证分析:钓鱼邮件主要指冒充官方部门、知名企业、公司领导或上级主管部门等诱骗用户信任,从而实施诈骗行为。针对于钓鱼邮件的取证分析,首先需要获取并记录发件人邮箱、发件人IP、发件人计算机名称等关键信息。若钓鱼邮件中是附带钓鱼网站地址,则通过链接指向的域名进行取证分析;若钓鱼邮件中附带恶意样本,则通过恶意程序分析技术,尽可能获取恶意代码中指向的C&C服务器地址,通过服务器地址进行进一步的分析。

场景3.舞弊取证场景

注册舞弊审查协会(ACFE)将职业舞弊定义为:“利用某人的职权,通过有意误用、滥用雇佣企业的资源或资产来谋取个人利益”。员工舞弊不仅为经营机构带来经济上的损失,还会损害经营机构品牌形象和文化,造成声誉损失。随着科技和数字化的广泛运用,舞弊行为愈加呈现智能化、隐蔽化的趋势。舞弊人员可轻松将涉案证据损毁、消灭,这时就需要引入电子取证手段了。

在该场景中,需特别注意对于员工的隐私权保护问题。需要保证取证行为的合法性,这依赖于经营机构前期对反舞弊电子取证的制度构建,如机构应明确对存储介质的所有权,保障反舞弊调查有权收缴存储介质;明确重点内控人员的电子数据检查机制;推行数据备份机制,避免证据被随意删除;推行规范化的电子办公制度;内部推行隐私协议,提前将可能会收集的数据类型列出并要求签署隐私协议,保障“告知-同意”原则等,为之后的反舞弊调查夯实基础。

常见手段:

■存储介质取证分析:从实践看,大多数舞弊人员出于掩盖犯罪的需要,往往会将暴露犯罪行为的电子数据特意存储在私密的存储介质中,例如个人电脑、手机、U盘、记忆棒、存储卡、存储芯片中。在取证分析时,应当针对具备数据存储功能的介质展开,包括采用密码破解、数据恢复等手段获取必要的证据数据。需要注意的是,如果是公司采购提供的存储介质,公司在必要时可主动获取其数据,若是员工私有存储介质,需考虑员工的隐私保护问题。

■通信介质取证分析:舞弊人员在通信信息中也可能无意暴露数据,这类数据往往以手机短信、电子邮件、即时通信记录为主要方式。由于该类电子数据并非舞弊人员刻意存储,而是日常犯罪活动所积累形成的,因此易被舞弊人员疏忽。在针对此类介质取证分析时,也需考虑员工的隐私

保护问题。

四、电子取证分析基本流程

步骤1.取证准备

当发生事件或疑似发生事件时，明确需要取证分析团队介入时，取证分析团队需要针对不同类型的事件进行准备工作，具体包括：

- 了解事件：了解事件类型、事件背景、事件影响等基础信息
- 明确勘验对象：勘验的对象大体分为两个方面，第一类是需要了解事件相关人员，另一方面了解勘验的物理对象，如服务器、存储设备、办公终端、安全设备等
- 制定策略：针对不同事件的情况和勘验的对象，明确制定策略，包含团队人员分工、工作流程等
- 合法性授权：部分类型事件可能面临侵犯隐私权的情况，取证团队需获得必要的授权，如法律授权或公司内部授权
- 准备工具：针对不同的事件和勘验具体对象，提前准

备好相关取证工具，如取证存储介质、必要的技术工具，如网络入侵取证需要准备wireshark、日志分析设备；Linux取证需要准备必备的脚本工具

步骤2.现场保护

当取证团队开始具体工作前，需对取证工作的现场环境进行保障，避免因人为因素破坏证据，阻塞取证工作的进行，具体包括：

- 勘察人员电子证据保护原则：开机不关、关机不开，对电子证据所在区域首先进行保护，并保证电子证据所在区域电源正常使用，不可随意断电
- 保障人身安全：防止取证过程中被调查人员不配合产生冲突，或其他可能对人身造成伤害的情况
- 保障设备安全：防止取证过程中对证物或存储有证物的取证设备产生的破坏
- 调查对象隔离：涉及到人员问询调查情况下，应及时对被问询人员进行隔离，避免潜在的破坏行为，防止其接触电子证据设备及任何电源



图1 电子取证分析基本流程



图2 现场保护示意图

五、总结

电子数据取证与分析技术是一个庞大的体系,本文受限于篇幅限制,不涉及过多深入性技术内容,仅浅尝辄止的介绍证券基金经营机构常见涉及电子证据取证分析的场景和电子取证的标准流程。取证作为一个细分专业领域,从取证的合法性、证据链的完整性、涉及到的技术难度要求都很高,通常需要寻求专业并具备相关资质的公司做支撑,但对于大部分企业和个人,需要掌握基本的保护现场的能力,熟悉相关的处置流程,并掌握初步的技术分析和定位能力。

六、附录

以下为一些不同平台下常见的取证分析工具和学习参考资源,便于相关感兴趣人员自行下载研究:

工具类资源

1.FTK Imager 镜像取证工具:该工具可在不进行任何更改的情况下创建数据副本,并尝试保留证据,通过计算MD5哈希值确认数据完整性。

链接:<http://www.exterro.com/digital-forensics-software/ftk-imager>

2.X-Ways Forensics取证工具:该工具可以访问磁盘和RAID,支持NTFS和备用数据流ADS文件格式、支持书签或批注、分析远程计算机。

链接:<https://www.x-ways.net/winhex/forensics.html>

3.SIFT Workstation取证工具:该工具是以虚拟机为形式的一套免费开源的取证分析工具,旨在各种环境下执行数字取证检查,可以灵活匹配当前的事件响应和取证工具套件,以实现高级事件响应与数字取证需求

链接:<https://www.sans.org/tools/sift-workstation/>

4.Winhex数据恢复编辑器:该工具是一款16进制编辑器,提供检查和修复文件、恢复删除文件、检查硬盘损坏造成的数据丢失情况、检测隐藏程序、文件和数据等功能

链接:<http://www.winhex.com/winhex/index-m.html>

5.Sleuth Kit(+Autopsy)分析工具:该工具主要简化对分析工作,提供图形化UI检查用户的硬盘驱动器和移动手机,提供电子邮件分析、短信、通话记录、联系人等方式的数据提取与分析

链接:<http://www.sleuthkit.org/autopsy/>

6.Forensic Investigator分析工具:该工具是一个分析工具集,包含了许多其他工具,如Ping、横幅抓取器、端口扫描器、SNB共享、NetBIOS查看器、URL解码器等能力

链接:<https://forensictools.dev/>

7.Autopsy取证工具:该工具基于GUI的开源数字取证程序之一,能通过移动手机和硬盘驱动器进行有效分析

链接:<https://www.autopsy.com/>

8.Dumpzilla浏览器分析工具:该工具支持提取浏览器插件、cookie、书签、历史记录、密码、下载、表单填充数据等浏览器常见信息,用于取证分析工作

链接:<https://github.com/Busindre/dumpzilla>

9.Browser History浏览器分析工具:该工具可以读取不同浏览器内数据并在同一浏览器内显示,便于提高分析效率

链接:<https://www.foxtonforensics.com/browser-history-capturer/>

10.Wireshark网络分析工具:该工具用于捕获和分析网络流量中的数据包,包括网络封包捕获、数据包分析、数据包过滤、数据重组等核心能力,用于对网络流量进行分析,以分析潜在的安全威胁

链接:<https://www.wireshark.org/>

11.Toolsley调查工具:该工具主要用于收集文件标识符信息、文件签名验证器、二进制检查器信息、哈希验证信息、文本编码、数据URI生成信息和密码生成信息,便于开展分析工作。

链接:<https://geekflare.com/forensic-investigation-tools/>

06 2023年度实验室优秀课题摘录

P102 基于BAS的安全运营自动化闭环技术的研究和实践

王东、马冰、吴晨炜、秦伟伦

P110 一站式安全可控商用密码服务研究与应用课题摘录

官俊、徐庆、方优、万强、谢丽君、乔少明、王家阳

应志伟、涂海波、陈善

潘峻翌、黄福飞、朱振中、熊梦彪、何良杰

P118 证券公司软件供应链安全管理平台研究与实践课题摘录

王玥、李志龙、吴佳伟、钟蓉、李鹏、曹杰、温志强、韩智鹏

马冰

康乐、韩建

P124 自动化和常态化的网络资产攻击面运营平台的研究与实现

季常青、宋士明、叶飞、姜玥、汪洋

赵武、邓焕

基于BAS的安全运营 自动化闭环技术的研究和实践

王东、马冰、吴晨炜、秦伟伦 | 海通证券股份有限公司

摘要：传统网络安全运营，主要是通过周而复始的发现和消除资产弱点来降低安全风险，而疏于关注网络安全防护效果。究其根本，在于缺乏高效的手段来检验防护效果与预期之间的差距。2017年Gartner首次提出了入侵和攻击模拟技术（BAS），该技术的提出，推动了安全产业将攻击行为工程化为用例，但安全验证是一套闭环体系，其中安全防护自动化识别、防护失效修复补丁以及全过程自动化闭环等技术，仍然影响着大规模验证时的准确性和效率。本研究正是针对性的研究相关痛点，并将研究技术加以实践，力求在证券期货业具有普遍的适用性。

关键字：安全验证、防护自动化识别、自动化闭环

一、研究背景

（一）研究的目的和意义

随着信息技术的快速发展，网络威胁不断演变和升级，给个人、企业乃至国家的信息安全带来了前所未有的挑战。尽管企业部署了各类安全防护措施，但运营中如果没有进行正确的变更、升级或使用，已构建的安全防护措施就会出现防护效果不好，甚至有防护无效现象，难以有效发现和防范入侵攻击行为。2023年10月，证监会发布《证券期货业信息安全运营管理指南》，提出对“安全运行状态、安全检测与防御能力”进行有效性验证；同期，国家金融监督管理总局发布《关于加强网络和数据安全管理防范勒索病毒攻击的通知》，要求持续验证防护措施有效性，建立验证其健康性、安全效果的机制，形成持续化保障能力。

当前证券期货行业金融机构不同程度的建设了安全防护设施，初步形成了安全防护体系，但对于技防体系的效果验证，仍然处在伊始阶段。

本文将着重从安全验证领域发展中已有取得的研究成果上，深入分析当前安全运营自动化闭环存在的问题，结合行业特点对相关技术进一步研究，力求揭示出同类问题的共性特征，并结合海通证券实际的案例进行比较分析，对证券期货行业安全运营自动化闭环技术的应用提出建议。

（二）国内外技术发展趋势

■起源

2017年全球著名的信息技术研究和咨询公司Gartner在发布的《面向威胁技术的成熟度曲线》（Hype Cycle for Threat-Facing Technologies）中首次出现入侵与攻击模拟（Breach and Attack Simulation）概念，并将之归到了新兴技术行列。如Gartner描述的，该框架“可供

安全团队以一致的方式持续测试安全控制措施，贯穿从预防到检测（乃至响应）的整个过程”。

■发展

从技术发展来看，2020年4月在MANDIANT发布的《SECURITY EFFECTIVENESS REPORT 2020》报告中提出，衡量安全控制措施的有效性并证明其合理性已成为一项关键绩效指标，正在成为安全运营建设的一种趋势性需求。基于入侵与攻击模拟的安全验证可以量化安全措施的实际有效性，建议实施持续安全验证。

2021年，Gartner在发布的《2021安全运营技术成熟度曲线》中，将BAS的技术优先级评为“高”，表明其在企业安全运营中的重要性日益凸显。

2022年8月权威机构Forrester《规划指南2023：安全与风险》中明确提出在运营技术（OT）威胁情报、安全分析平台等8个领域将成为全球企业重点建设投入的方向。安全运营，是未来发展重心。

2022年，Gartner在《2022中国安全成熟度曲线》报告中再次提及BAS，将其认定为具有潜力的高价值技术。

2023年，Gartner最新的《2023年9大网络安全趋势》中，网络安全验证（Cybersecurity Validation）作为九大趋势之一被提出，真正明确了BAS在网络安全验证方面的应用，并预测到2026年，超过40%的组织将应用网络安全验证。

从技术引领的角度来看，上述机构（尤其是Gartner）连续多年将BAS技术列为网络安全领域的重要趋势，直接推动了该技术在全球的发展和应用。

■应用

从技术应用的角度来看，从国外网络安全验证市场相

对成熟，以AttackIQ、Cymulate、SafeBreach为代表的国际知名公司在技术创新方面持续投入，不断推出安全验证产品和服务，在金融服务、医疗保健、政府机构等行业进行了广泛的应用。

国内对于安全验证从行业到应用都存在巨大的研究和发展空间。已经有不少比较先进的组织，已经开始实践网络安全验证。

金融业落地实践多，效果显著。目前金融行业对“安全验证”应用实践步伐最快，与金融行业高度相关。同业的大行、大型券商已经在考虑安全验证的问题，部分开始建设安全验证平台和工具，如部分股份制商业银行、部分大型券商行动较快，已经或正在建设安全防护有效性验证平台，或正在建设安全策略验证平台等，正在调研或立项的金融同业也有不少，从同业应用趋势的角度来看，网络安全验证将受到更高的重视。

央企、智能制造密集跟进。已经有电网、能源等涉及基础设施的企业已经在部署和实践安全验证；众多头部大型制造业企业都在进行调研和选型，部分已经落地，如中兴、OPPO、华大智造、顺丰速运等。

互联网创新巨头积极落地实践。类似小米、百度、贝壳、度小满等互联网创新公司本身技术团队较强，甚至自研HIDS、WAF等安全产品，深刻认识安全验证的重要性，鉴于较高的人力成本纷纷落地实践安全验证。

二、研究对象及方法

（一）研究对象

本文以基于BAS的海通证券安全运营自动化闭环技术的研究和实践为基础，对证券期货行业的安全验证中的关键技术、重难点和共性问题进行研究探讨。该技术的研究，拟解决组织对网络安全运营实施效果和安全防护水平缺少验证方法、手段的问题，并通过海通证券的实践，验证相关技术的合理性和可操作性、探索相关网络安全工作经验。

（二）研究的方法与手段

一是技术研究。就安全防护措施识别技术、自动化闭环技术、安全防护失效修复补丁技术进行研究并取得突破；

二是业务建立。基于现有的安全运营工作流程，增加安全验证环节，通过执行该动作并观察其实际效果，验证关键技术业务流程中的适用性和合理性。

三是效果评价。在海通证券生产环境部署安全验证系统，使用技术手段模拟真实的各类攻击，对已部署的各类安全产品和规则策略开展常态化效果验证。通过执行该动作并观察其实际效果。

三、研究与实践成果

（一）研究成果概述

网络安全验证技术旨在评估组织在网络空间安全领域的防御和应对能力。本课题以入侵和攻击模拟技术为基础，创新性的研究和运用了安全防护自动化识别技术、自动化闭环技术和安全防护失效修复补丁技术，构成了更高效的网络安全验证技术体系，基于该验证体系，能够高效识别安全防护效力，快速发现和改善防护体系短板。

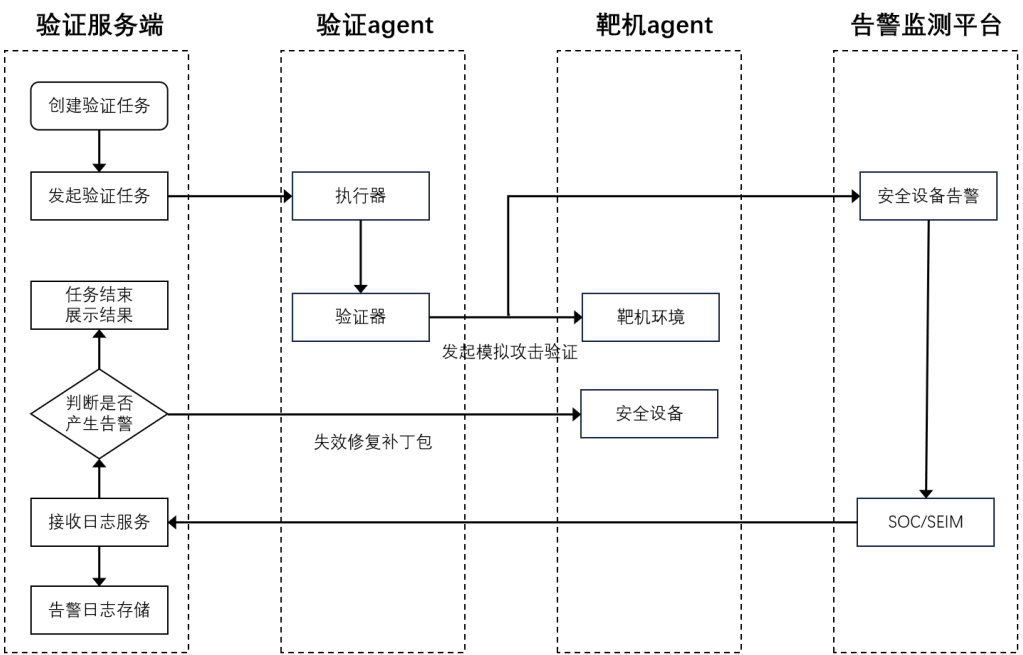
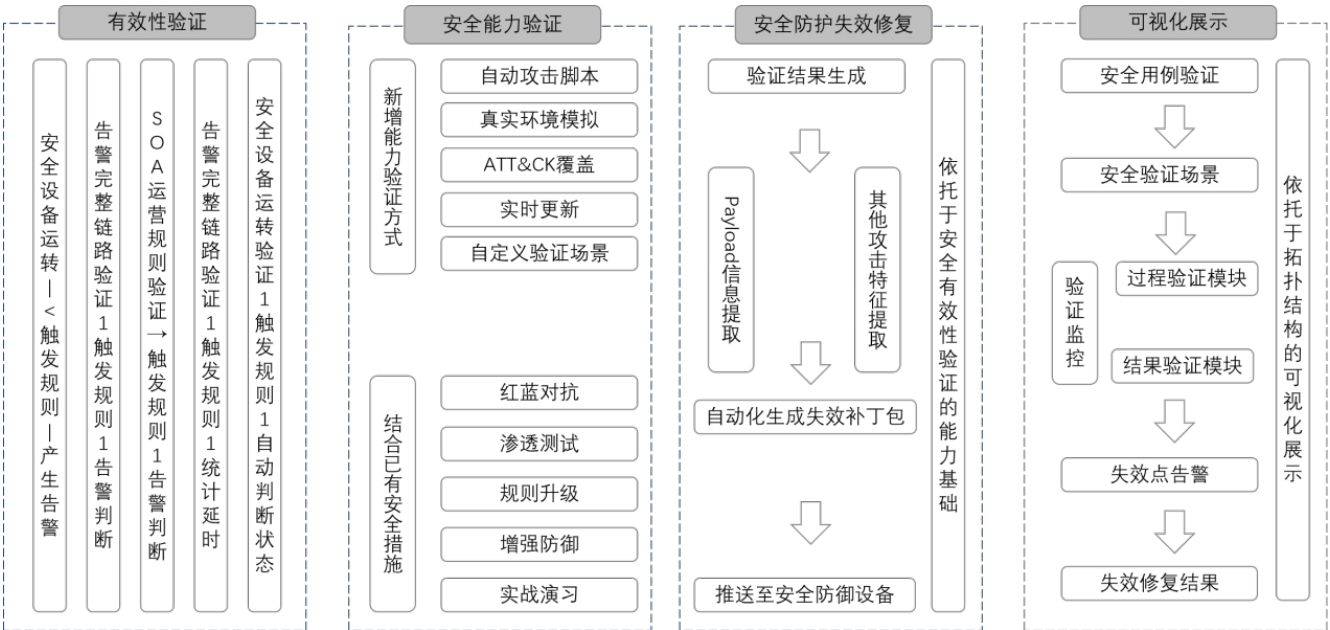
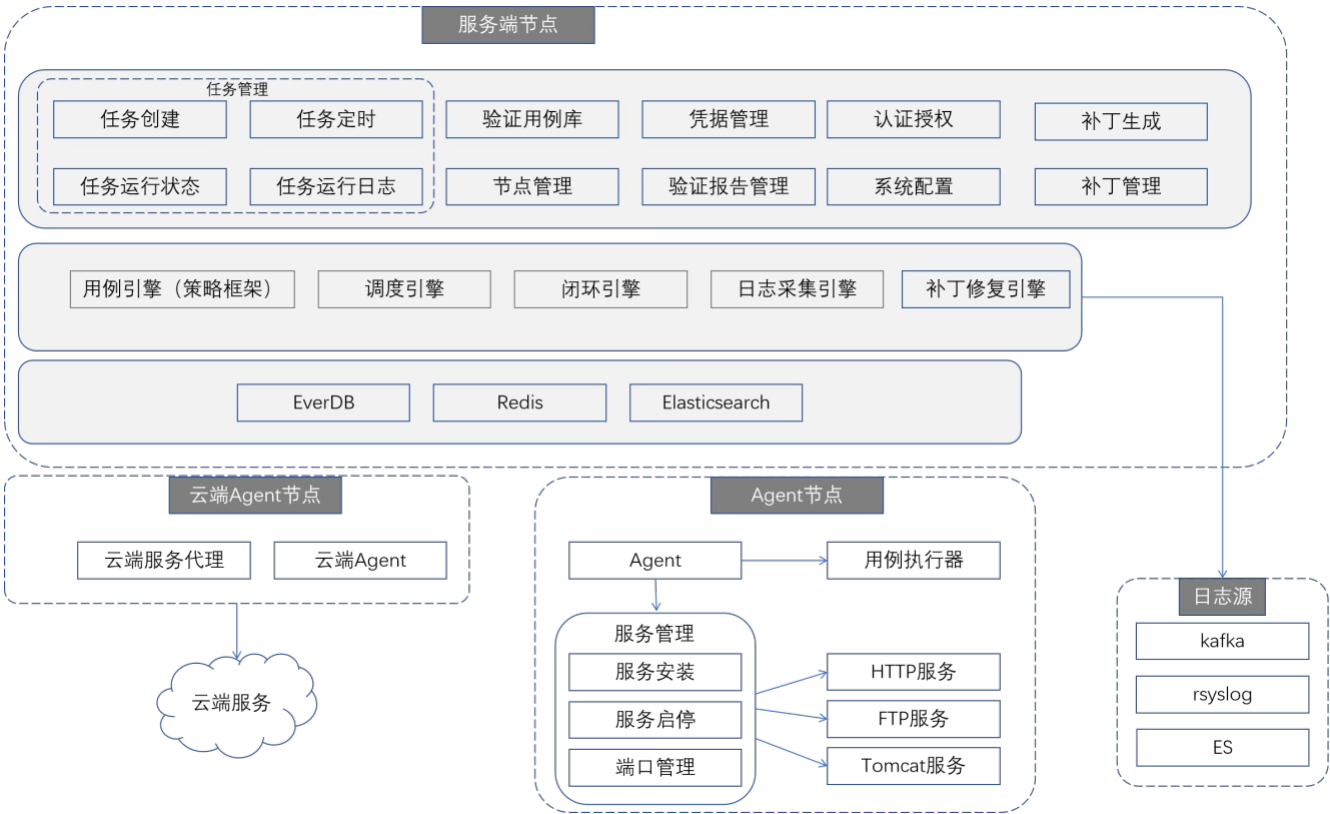


图1 逻辑架构



服务端：负责验证任务创建、任务调度、任务下发、失效补丁包生成和推送、验证结果展示、靶机和验证机管理、验证场景创建和升级管理等；

验证机agent：负责模拟攻击者对目标靶机发起攻击验证；

靶机agent：作为被攻击主机，用来充分验证安全防护

监测能力、安全策略运行的有效性等；靶机上无任何真实生产业务，但部署有和真实环境一致的安全防护软件/设备。

告警监测平台与服务端联动：系统支持通过与安全运营中心SOC平台联动，同步安全设备资产信息、同步告警日志，接收系统验证结果，判断安全设备的防护有效性，实现自动化验证结果闭环。

应用层:任务管理负责任务的创建、和任务运行状态反馈等;用户可通过灵活的选用验证用例和场景进行验证、可快速输出验证统计报告等。

引擎层:负责验证用例可调参数执行、验证任务调度、验证闭环和日志采集和解析。

数据存储层:利用mysql数据库存储结构化数据、ES和redis存储非结构化数据。

Agent节点:部署在内网和互联网,可适用于互联网边界及内网全场景验证。

安全有效性验证模块:用于执行攻击模拟验证,确定安全设备及规则检测链路是否正常工作,对重要安全防护措施进行验证。同时与海通证券安全运营中心进行对接,获取日志和告警,以白盒的方式进行有效性验证。

安全能力验证模块:用于自动化模拟攻击验证,在各个攻击平面覆盖更全量的攻击手段,结合现有的红蓝对抗等验证安全防护是否真实生效。

安全防护失效修复补丁模块:基于 Suricata、yara及部分自研安全设备的安全规则,通过自动化的方式基于验证结果生成失效补丁包,从而实现失效点的自动化闭环。

可视化展示平台模块:用于实时动态展示安全有效性验证结果,第一时间掌握安全有效性。

(二) 自动化闭环技术

自动化闭环技术是一种基于反馈机制的控制策略,通过将防护设备输出与模拟攻击输入进行比较,并根据比较结果调整系统输入,实现系统输出的精确控制。主要通过以下几个自动化步骤实现验证过程的全自动化闭环:

自动化攻击用例执行:利用预设的攻击用例模拟真实的网络攻击行为,测试安全防护体系的效能。

自动化告警拦截信息捕获:通过与SOC进行对接,实时捕获并传输来自各类安全防护设备的告警拦截信息。

自动化数据清洗与适配:对捕获的海量、不同格式的数据进行清洗和适配,统一转换为便于分析处理的格式。

自动化关联分析:利用多种闭环逻辑的灵活组合(如返回判断、页面相似度分析、告警闭环、拦截查杀闭环、进程分析、连接状态分析等),对清洗后的数据进行精确匹配,揭示防护失效的内在逻辑,暴露潜在威胁。

自动化反馈:基于关联分析的结果,自动触发预设的反馈策略,给相应的负责人提供输入,结合安全防护失效修复补丁技术,第一时间发现和处置安全失效。

技术优势:

高效性:自动化处理流程显著提高了安全响应的速度和效率,降低了人工干预的成本和错误率。

精准性:智能关联分析引擎能够实现对海量告警信息的精确识别和定位,提高了安全响应的准确性。

全面性:覆盖了从攻击识别到响应、再到修复与优化的全链条流程,实现了安全防护的闭环管理。

可扩展性:支持多种通信协议和闭环逻辑,能够灵活适应不同规模、不同场景的网络安全需求。

(三) 实践效果总结

海通证券是实践工作的组织方,负责协调内外部资源,制定实践方案,组织实施实践全流程工作,并对实践情况进行总结归纳。实践工作取得了以下效果:

1、增设安全工作流程,完善安全运营逻辑

基于海通证券现有的安全运营工作流程,增加安全验证环节,并根据防护目标设置了安全验证指标,通过将该指标转化为具体的验证动作,实现按需安全验证,通过该工作的执行,发现了不少日常网络安全运营工作中难以察觉的问题,对提升安全水平有较大的促进作用。

从结果来看,该工作流程的建立和执行,对现有的网络安全运营从逻辑上做了补全和完善,在现有的建设、使用基础上,增加了“监督”环节,构成了“同步建设、同步使用、同步验证”的网络安全运营机制。该工作流程的应用,对完善当前网络安全运营逻辑,提升安全运维水平,具备较强的现实意义。

2、常态化验证,安全防护效果持续改进

在海通证券的生产环境进行安全验证,并通过模拟真实的各类攻击,对海通证券已部署的各类安全产品和规则策略开展常态化效果验证,验证频率从小时到天不等,通过验证发现不少安全失效。从安全运营的短周期(以事件为维度)来看,通过在网络安全运营实施过程中增加常态化安全验证,能够及时发现和改善网络安全运营效果,提升网络安全运营的管理和实施水平,真正做到了防护效果可视、可度量,符合“有度量才有改进”的安全逻辑,更符合网络安全运营过程中“短循环周期内持续改进”的安全理念。

3、度量价值,为安全规划、建设和决策提供输入

从安全运营的长周期来看,安全工作需要根据一个长周期内(如1年)的表现进行规划和改进,通过对当前网络安全运营的真实效果进行周期性度量和评价,观察安全防护在长周期内的变化趋势,寻找安全预期和现状之间的差距,为后续安全规划、建设和决策提供输入。

(四) 共性失效点分析与总结

通过对实践期间发现的安全失效进行结果分析,总结并归纳主要失效点40项,为后续本单位安全运营、证券期货同业的安全防护失效识别和处置提供输入。

根据已发现的失效点,进行同业交流和共性问题归纳,通过安全防护体系和失效原因两个维度进行分析。

安全防护体系包括边界防线、流量防线、主机防线、终端防线、邮件防线、运营中心防线、网页防篡改防线、最后还

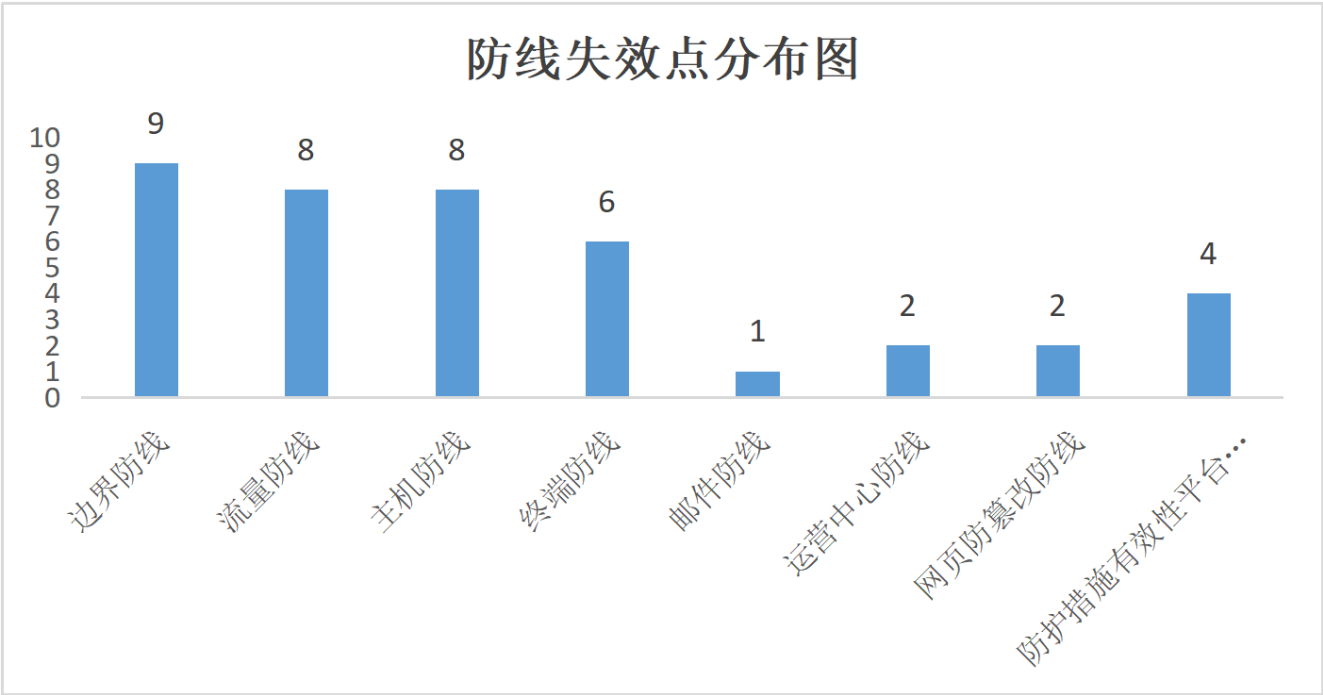


图5 安全防护失效点分布图

有防护措施有效性平台自身优化。

按照安全防护体系中设备失效的结果进行分析失效案例最多的是边界防线,其次是流量防线和主机防线并列8个,最少的是邮件防线1个和次少的是运营中心防线和网页防篡改防线都是2个。根据验证经验,边界、流量、主机和终端是最常见的基础防护阵线,但同时也是最容易失效的部分。

失效原因包括防护资产缺漏、设备规则优化、设备配置优化和设备bug优化。

按照失效原因的结果进行分类发现失效最多的是设备配置优化17个,其次是设备规则优化,另外防护资产缺漏4个和设备bug优化类3占比较少。由此可知,安全设备上线后由于配置设置错误或漏配置是导致安全运营效果下降很重要的原因。其次设备自身的功能性不足也值得关注。安全设备需要及时规则库更新,保障企业安全运营体系快速响应外部攻击。

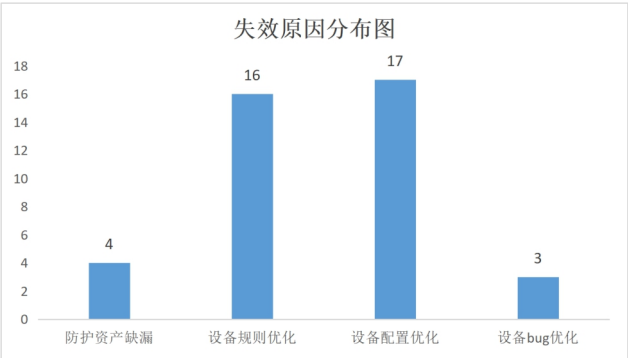


图6 失效原因分布图

将高频失效点进行整理,可归纳如下:

互联网站点未被防护覆盖:部分对外发布的互联网站点,因为互联网资产统计不全、加密证书未卸载、镜像流量未分发等原因,导致互联网边界的防护及流量检测失效,从而无法完成有效性验证闭环。

部分绕过攻击无法覆盖:针对各类攻击存在绕过的形式,包括编码、异常字符、字母变体、大包绕过等形式,需要针对拦截检测设备进行规则优化,提高检测能力。

终端防病毒未识别常见的恶意文件:由于误报等因素,在服务端开启了特定目录的例外策略,同时特定目录没有进行运营维护,导致部分目录不进行查杀;

流量分析平台性能不足:在部分横纵向流量较大的区域,业务波峰会出现部分攻击无检测的现象,发现分析平台性能存在瓶颈,需保持关注流量峰值情况,确保分析平台足够容量

设备更新升级:完成设备更新升级后,由于授权未更新、配置未同步等原因,导致防护失效。

安全运营中心日志异常:安全运营中心由于日志收集异常导致无法闭环,需要加强安全运营中心日志健康度的监控,确保安全设备的日志能正常接入。

四、结论

本文在现有网络安全验证理论的基础上,系统性的阐述了海通证券基于BAS的安全运营自动化闭环的研究,并根

据研究结果的实际运用,对暴露出的共性失效点进行了分析归纳,通过本课题的研究和实践,对海通证券当前网络安全防护水平有较大的促进作用,具体为:

业务安全性的显著提升

通过BAS技术的常态化应用,海通证券的安全防护体系得到了全面而深入的测试与优化,显著提升了业务的安全性与可靠性。

安全运营效率的提高

安全防护自动化识别与修复补丁技术的应用,使安全事件的发现与处置变得更加高效、快捷,大幅提高了安全运营的整体效率。

持续改进机制的建立

自动化闭环技术的实现,为海通证券建立了一套持续改进的网络安全运营机制。通过不断迭代与优化,海通证券的安全防护体系将能够持续适应不断演变的威胁环境,保持领先的安全防护能力。

总的来看,本课题的研究成果在海通证券的实际应用中取得了显著成效,为构建智能化、高效化的网络安全运营体系提供了有力支持,本课题的研究成果有望进一步推动证券期货业网络安全验证领域的创新发展。

五、建议

基于BAS的网络安全验证技术正在全球范围内快速发展,该技术能够有效帮助组织识别和修复防护弱点,该理念先进,必将发展为网络安全防御的重要手段,亦将逐步成为证券期货组织网络安全的核心组成部分。

考虑到证券期货行业普遍的安全需求,本课题基于BAS,创新性的融入了安全防护自动化识别、安全防护失效修复补丁和自动化闭环技术,而在大模型、AI快速发展的今天,安全技术尤其是网络安全验证,在本研究的基础上,可以考虑融入人工智能、机器学习算法等技术,提升安全验证、安全运营的智能化水平。

参考文献

[1]GB/T 22339-2019《信息安全技术 网络安全等级保护基本要求》
[2]GB/T 20984-2022《信息安全技术 信息安全风险评估方法》
[3]GB/T 39204-2022《信息安全技术 关键信息基础设施安全保护要求》
[4]MANDIANT, SECURITY EFFECTIVENESS REPORT, 2020
[5]SANS. Measuring Cybersecurity Controls Effectiveness with Security Validation.2020

[6]Gartner. Hype Cycle for Threat-Facing Technologies, 2017
[7]Gartner. Hype Cycle for Security Operations, 2021
[8]Gartner. Hype Cycle for Security Operations, 2022
[9]Gartner. Hype Cycle for Security in China, 2023
[10]Gartner Identifies the Top CybersecurityTrends for 2023

六、常见安全验证失效点案例情况

名词解释

失效修复等级:根据失效点的修复难度进行排级,星级越高难度越大。

★★★暂时无法修复,需考虑其他补充检测或拦截手段

★★ 能修复,需进行系统版本或规则库升级

★ 容易修复

序号	失效描述	失效类型	失效发现及依据	失效修复等级	修复措施
1	针对主机入侵检测设备检测发现失效,未形成闭环	运营中心设备配置优化	针对主机入侵检测设备检测发现失效,经排查为SOC告警时间与主机入侵检测的告警时间相差20分钟以上,因此未形成闭环。SOC与主机入侵检测之间的TCP syslog有中断情况。需针对TCP通信增加keepalive报文。	★★	优化SOC日志收集keepalive机制
2	流量检测针对同一个公网IP的请求全部失效	运营中心设备配置优化	针对互联网资产进行有效性验证,发现流量设备缺失全部告警,经分析排查为SOC设备正在进行升级,升级完成后消息队列中的topic名字发生变化	★	调整消息队列的topic名称
3	网页防篡改有效性检测失败	网页防篡改设备bug优化	经排查为sysmon_edr.ko驱动问题导致服务失效,更换了sysmon_edr.ko驱动文件后问题解决。	★★	更新驱动
4	网页防篡改有效性检测失败	网页防篡改设备bug优化	网页防篡改服务端windows rpcservice失效	★★	重启windows rpcservice
5	应用防火墙主机池配置失效	边界防线防护资产遗漏	历史上针对某业务80/443有效性验证一直有效,经变更后添加8080端口导致有效性验证失败,经排查与流量编排有关,8080端口需进行其他设备配置。	★★	需在网络编排设备上将8080端口流量分发至应用防火墙
6	应用防火墙防护失效	边界防线防护资产遗漏	站点8888端口未覆盖在应用防火墙防护中。	★	将8888端口纳入应用防火墙防护。

序号	失效描述	失效类型	失效发现及依据	失效修复等级	修复措施
7	应用防火墙防护覆盖度不全	边界防线 防护资产缺漏	针对互联网资产 IP、域名进行全量有效性验证,发现部分应用防火墙未能有效防护,整体覆盖率约为 90%。	★	补充缺失站点
8	针对某类攻击无法检测	边界防线 设备规则优化	有效性验证专项测试发现 winhex 编码注入手段可绕过应用防火墙拦截。	★★★	实现 winhex 解码
9	针对大包攻击无法检测	边界防线 设备规则优化	有效性验证专项测试发现利用 5M 10M 等大包能绕过应用防火墙拦截。	★★★	实现对大包的检测
10	针对某类 SQL 注入未拦截	边界防线 设备规则优化	在对该站点进行渗透测试过程中发现应用防火墙的 SQL 拦截策略可被“%”绕过。判断为产品检测缺陷,反馈至设备厂家进行优化。	★★	针对相关内容进行规则优化
11	应用防火墙防护策略失效	边界防线 设备配置优化	应用防火墙无法有效防护 WEB 攻击,验证发现应用防火墙配置为监控模式,未开启拦截模式	★	通过人工巡检及有效性验证,确保各数据中心边界应用防火墙开启拦截模式
12	针对某类攻击无法检测	边界防线 设备配置优化	在对该站点进行渗透测试过程中发现应用防火墙针对 URL 多次编码后的 Payload 及 XML payload 无法拦截,经分析后为 URL 递归解码配置及 XML 检测配置未开启。	★	打开递归 URL 解码功能及 XML 检测配置功能,并关注对应用防火墙的性能影响
13	应用防火墙配置不同步	边界防线 设备配置优化	在一台机器上没开 API 的防护,经排查为应用防火墙策略不同步。同区域其他几台应用防火墙策略配置是相同的。	★	同步应用防火墙配置
14	检测到异地数据中心部分告警未闭环	流量防线 防护资产缺漏	通过查看设备日志发现流量设备未覆盖相关流量	★	覆盖流量
15	检测到冰蝎 4.0 失效	流量防线 设备规则优化	查下来流量日志有但是没形成告警	★	通过更新规则实现
16	发现流量检测设备告警漏报问题	流量防线 设备配置优化	针对互联网 20 个区域进行互联网流量覆盖度验证,发现流量检测告警存在延迟和漏报的情况,告警漏报原因为流量检测分析平台性能瓶颈,导致存在丢包的情况	★★	增加流量检测设备探针数量,解决性能问题
17	发现流量检测告警日志转发至 SOC 时延大	流量防线 设备配置优化	在测试过程中发现流量检测设备告警转发到 SOC 时延较大,在 2-30 分钟区间徘徊,很不稳定。经排查分析为流量检测探针性能问题。	★★	增加流量检测设备探针数量,解决性能问题
18	从流量检出到形成告警超时	流量防线 设备配置优化	有效性验证发现告警检测失效,原因是虽然所有数据都在 ES 中,但是部分告警形成时间超过 10 分钟,因此被判定失效。需要加强分析平台性能,从而加快日志形成告警时间。	★★	增加分析平台性能
19	流量检测针对同一个公网 IP 的请求有缺失	流量防线 设备配置优化	针对互联网资产进行有效性验证,发现流量设备缺失部分流量,经分析排查为设备字分析节点与主分析平台之间密码错误导致业务积压。	★	修改与主分析平台的连接密码。

序号	失效描述	失效类型	失效发现及依据	失效修复等级	修复措施
20	有效性验证告警无法闭环	流量防线 设备配置优化	针对部分 webshell 场景进行有效性验证,发现均为验证失败,但在流量设备上能形成告警。经排查为流量设备把相关告警定级为低危,但是低危类告警没有将日志打到 SOC。	★	调整流量设备 syslog 配置。
21	发现流量检测设备有效性验证失效项增多	流量防线 设备 bug 优化	针对流量设备进行常态化有效性验证,发现失效日志增加,经排查为流量设备检测引擎工作异常。	★★	重启设备,并联系厂商进行排查,分析为信创版本引擎工作异常,需进行重启。
22	主机命令执行检测失效	主机防线 设备规则优化	针对主机命令进行有效性验证,通过执行 WEB 命令执行如 id、Whoami 等进行信息收集,相关命令由于和运维人员操作较接近,通过自定义检测规则后会导致告警量增加	★★★	通过自定义规则进行检测,但会导致告警量增加,难以收敛,需通过 AI、机器学习等技术进行优化
23	主机入侵检测没检出 frp 工具	主机防线 设备规则优化	针对有效性验证 frp 工具,检测失效。主机入侵检测设备未能识别重命名过的 frp 工具。需优化检测逻辑。	★★	优化识别机制
24	主机入侵检测部分 webshell 失效	主机防线 设备规则优化	通过有效性验证检测,发现部分 webshell 检测失效,经排查为未识别到网站目录,通过自定义添加目录后能正常检测。优化目录检测机制,做到自动化检测	★★	自定义网站目录,增强自动化检测目录机制
25	主机入侵检测针对 2M 文件无法自动检测。	主机防线 设备规则优化	主机入侵检测针对 2M 的 webshell 进行检测,检测失败。需针对主机入侵检测设备的检测配置进行优化,支持 2M 的文件检测。	★★	更新文件检测阈值,目前能支持 5M
26	主机入侵检测无法识别站点目录	主机防线 设备规则优化	主机入侵检测发现 webshell 检测失效,经排查应用服务器进程改为了 java-8088.exe 不是标准的 java.exe,所以导致主机入侵检测没有发现应用目录,无法检测 webshell	★★	优化目录检测机制
27	发现主机入侵检测用例检测失败	主机防线 设备规则优化	针对主机入侵检测用例失败:包括 Ruby 反弹 shell 攻击未告警、Win 系统的注册表后门、希希传递攻击、部分 JSP/PHP/ASP 类型的 Webshell、部分端口转发等未能检测	★	优化相关规则
28	主机入侵内存码无法检测	主机防线 设备配置优化	主机入侵内存码检测失败,经分析日志,内存码状态运行异常,注入进程失败导致,原因为主机 agent 未升级导致。	★	升级主机 agent
29	主机入侵检测内存码模块过期	主机防线 设备配置优化	经过有效性验证测试,发现主机入侵检测设备针对内存码检测失效,经确认为内存码模块已经过期。	★	重新部署内存码授权
30	勒索行为模拟检测无法识别	终端防线 设备规则优化	勒索行为模拟检测发现 EDR 无法识别,经排查原因是检测逻辑(全盘扫描触发靶标文件告警)与测试逻辑(频繁修改文件、加密文件)冲突故无法触发检测。	★★★	需优化有效性验证的逻辑
31	防病毒 apt 组织恶意文件落盘防病毒端无法检测	终端防线 设备规则优化	有效性日常任务发现 3 例 apt 组织恶意文件落盘防病毒端无法检测,	★★	更新 agent 端规则

序号	失效描述	失效类型	失效发现及依据	失效修复等级	修复措施
32	防病毒检测失效。	终端防线设备配置优化	经常为该终端部署的防病毒客户端版本错误，服务端无法完成识别。需针对相关终端进行重装。	★	重新安装防病毒 agent
33	有效性验证无法闭环	终端防线设备配置优化	有效性验证发现防病毒告警无法在 SOC 闭环，经排查为防病毒服务端升级后 syslog 外发服务器配置错误。	★	更新 syslog 服务器
34	防病毒有效性失效	终端防线设备配置优化	防病毒有效性验证发现部分终端监测失败，经排查为此类终端查杀病毒例外目录过大，导致无法查杀	★	减少例外目录
35	部分勒索样本无法被落盘识别	终端防线设备配置优化	勒索样本落盘模拟检测发现部分勒索样本无法被落盘识别，经确认 EDR 只开启了行为检测模块，对于恶意文件仅支持 hash 碰撞匹配，需开启防病毒功能	★	开启防病毒功能
36	邮件网关对压缩包加密方式的恶意附件无拦截	邮件阵线设备配置优化	对于 rar 压缩加密的附件没有自动识别正文或者标题中的密码进行解密和检测，默认策略不包含此项，未开启相关策略	★	开启加密文件识别功能
37	弱口令检测批量失败	有效性验证平台	针对弱口令的有效性检测大量失败，经检查为有效性验证平台未把不通站点进行删除	★★	在弱口令检测前需对连通性进行检测
38	验证文件上传失败，但是最后执行显示验证成功	有效性验证平台	针对流量设备执行 webshell 用例，显示有效性验证成功，但是实际文件被病毒查杀，需优化测试文件上传机制	★★	优化病毒测试文件上传机制
39	发现流量检测设备检测失效蝎	有效性验证平台	检测到流量检测设备针对短时间大量有效性验证均检测失败，经排查为流量设备有归并机制，同类型攻击会归并为一类告警。需优化防护措施有效性验证机制，设置 sleep 属性，确保攻击包的间隔时间。	★★	针对设备告警归并问题进行优化，设计 sleep 机制
40	有效性告警闭环失败	有效性验证平台	有效性验证平台从 SOC 平台拿去设备告警日志时，会对地址进行过滤，导致部分日志缺失	★	过滤条件进行优化

一站式安全可控商用密码服务 研究与应用课题摘录

课题负责人：官俊

课题组单位：国泰君安证券股份有限公司
海光信息技术股份有限公司
格尔软件股份有限公司

课题组成员：徐庆、方优、万强、谢丽君、乔少明、王家阳、应志伟、涂海波、陈善、潘峻翌、黄福飞、
朱振中、熊梦彪、何良杰

摘要：商用密码的推广和信息技术应用创新是各行业应对网络安全严峻形势的重要手段。目前，证券期货业主要采用硬件加密卡来完成网上交易系统的商密改造，存在对接难度大、扩容不方便、改造成本高等问题。

国产CPU技术的发展，为商用密码算法的应用带来了新的机遇。本课题基于CPU内部芯片，将密码技术与密码服务相结合建设统一密码服务平台，在不改变业务流程前提下，为网上交易系统密码应用提出了一个新的商密改造方案，也为其他系统的密码应用提供一站式密码服务。

同时，本课题在网上交易系统商密改造项目中，完成了富易客户端与该平台的对接，进一步证实了方案的可行性。与传统的方案相比，本课题将信创和商密联系起来，具有性能更好，更稳定安全，可快速扩容，成本低，密码服务使用方便的优势，在行业具有较强的推广价值。

关键字： CPU、可信密码模块、快速扩容、商用密码算法、密码平台

一、背景

（一）商密应用现状

结合证券期货业密码应用和推广情况，商用密码算法的应用现状呈现出广泛且深入的态势。

首先，商用密码算法已经在多个领域得到了广泛应用。例如，SM2和SM4算法已经被国际标准化组织采纳为国际标准，并在国内外的加密应用中得到了广泛应用。这些算法不仅用于数据加密、网络通信和云计算等领域，还广泛应用于数字签名、身份认证和密钥交换等领域。

其次，随着密码技术的不断发展，密码算法的种类也日益丰富。除了商用密码算法外，还有LBlock算法、LDHC算法等多种国产密码算法。这些算法在安全性、效率和适应性等方面得到了显著提升，为我国的信息安全提供了更加坚实的保障。

特别在信创领域，商用密码算法的应用也呈现出加速发展的态势。随着信创产业的不断发展壮大，商用密码算法作为其中重要的组成部分，也得到了更加广泛的应用和更加深入的应用。例如，在信创云的建设中，商用密码算法已

经得到了广泛的应用，为云计算提供了更加安全、可靠的信息安全保障；在信创CPU芯片的设计中，商用密码算法得到了更加深入的应用，为底层的密钥存储和密码运算提供更高性能，更加安全的算力支持。

（二）商密在行业推广难点

尽管商用密码算法已经取得了显著的进展和成果，但在行业应用过程中仍面临一些挑战和问题：

1、标准指引规范仍需补充；金融机构在密码改造建设中，对密评密改的标准理解不一致。密评涉及多项国家和金融行业标准，标准之间存在交叉，部分内容解释较为模糊，给金融机构的改造带来不确定因素影响。

2、密码产品性能不足；金融机构普遍反映服务器设备、操作系统、数据库、网络通信、云计算等IT基础设施设施距离金融行业商用密码要求有较大差距，在运用密码技术进行身份鉴别、关键信息机密性、完整性保护、商用密码算法使用上仍需做大量工作，缺乏满足要求且适合金融行业IT基础环境的成熟产品，导致机构在计算和设备等基础领域无法全面开展改造和替代。

3、密码服务兼容复用率低；改造过程中，多数厂商从自身产品角度出发，围绕产品形成密改方案，在未结合金融机构存量密码产品设备情况且缺乏改造示范引导的情况下，导致金融机构大多通过采购新设备来完成密改工作，对现有设备的复用率较低。

4、密码应用方案存在优化空间；目前，行业内各证券公司网上交易系统商用密码改造方案是使用支持商密算法的协同签名网关（包括安全认证网关服务端和协同签名服务），数字证书系统以及硬件加密卡配合完成通讯链路的安全加固，硬件加密卡的引入在一定程度上不利于商密推广。

理论上，密码作为底层技术，广泛分布并被集成于各类IT软硬件中，用对用好商用密码需要联合密码、操作系统、数据库、服务器硬件、网络通信、云计算等行业，共同推动供给侧为金融等行业应用提供成熟的商用密码产品、技术和服务。鉴于上述密码应用的难点和密码应用的目标，我司联合格尔软件，海光信息打造了基于海光CPU（以下简称“CPU”）的一站式密码服务平台，为集中交易系统等其他系统的密码应用提供高效、便捷的一站式密码服务。

二、基于CPU的密码服务平台研究

（一）可信密码模块

商用密码算法在CPU内部的实现，主要依赖于CPU内

部可信密码模块。可信密码模块的边界定义为CPU芯片加固件，包括执行密码算法的硬件模块和软件模块，其中硬件模块核心部件是集成了密码算法专用加速硬件密码协处理器模块CCP (Cryptographic Coprocessor)，通过密码协处理器提供芯片级的密码技术应用方案，为安全处理器上密码运算提供加速，实现高效商密运算。软件模块主要为CCP提供的不同逻辑接口的驱动程序以及用户态库，用于访问处理器内部集成的硬件商密算法，用于实现高效的商密加解密和数字签名等功能。

（二）可信密码模块实现

基于CPU的密码技术，是实现可信密码模块的核心。基于CPU的密码技术是调用密码加速能力的密码技术的统称，它基于CPU芯片密码协处理器以及密码指令集特性，自主设计研发的一套密码算法加速软件开发套件。其中，主要有两方面能力组成：密码运算加速和密钥管理。密码运算加速包括指令集和密码协处理器，特点是性能高，全面支持SM2/3/4商密标准，支持同步异步多种模式，且向上提供标准化的OpenSSL/Tongsuo等接口，方便用户适配使用；密钥管理主要是内置的密钥管理模块TKM，提供全面的密钥生命周期管理，达到密钥“可用不可见”的效果，同样也是全面支持SM2/3/4商密标准，向上提供标准化的接口如0018 SDF接口。

基于CPU的密码技术软件栈如下图。

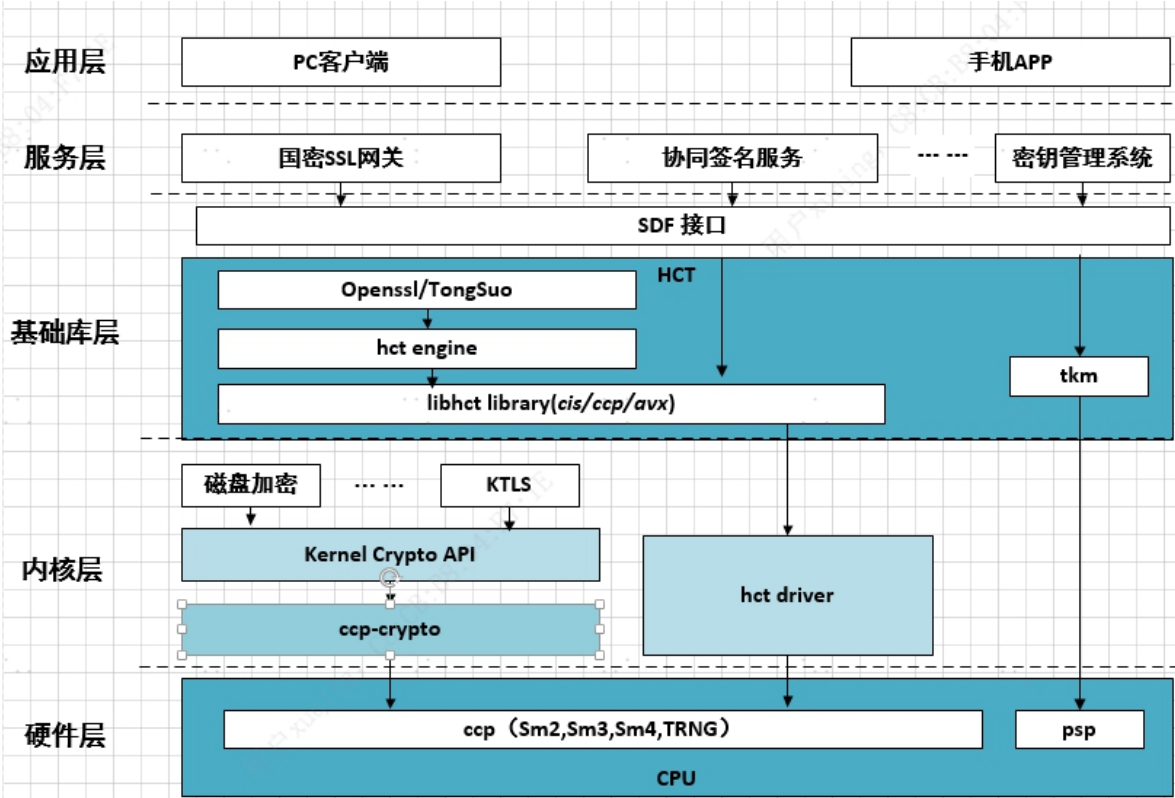


图1 基于CPU的密码技术软件栈

在OS内核层,开发相关驱动并且适配了内核Crypto API接口,可以支持内核磁盘加密、KTLS等应用,CCP-Crypto模块包含了密码协处理器在内核层的驱动;

在基础库层,HCT模块包含了密码协处理器在用户态的驱动,提供了密码基础库支持,基础库提供标准的OpenSSL接口和SDF接口等,可以向上支撑VPP、Ipsec、密码机等各种应用,满足不同应用场景的密码需求。

(三) 密码服务平台设计

本方案基于"应用层+服务层+基础层"的分层架构,构建起一套全栈化、全场景的证券期货行业云密码服务平台。通过对密码基础设施的池化管理和服务化改造,平台可以将密码能力以API或者密码服务的形式输出,灵活赋能各类行业应用,助力证券期货行业数字化转型和创新发展。

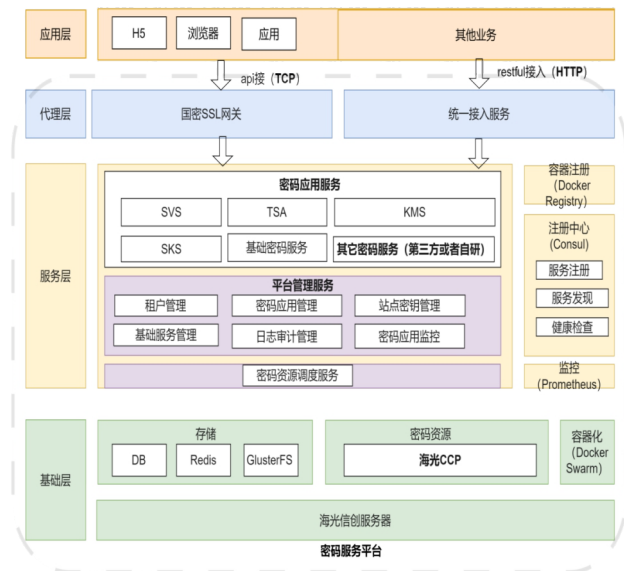


图2 密码服务平台分层设计图

1.应用层设计

应用层提供了多样化的前端接入方式,包括通过互联网访问,面向客户端用户的H5网页、Android App、iOS App和桌面应用程序等,以及通过局域网访问,面向业务端其他系统等。同时使用反向代理,还提供了商密SSL网关、和统一接入服务,用于应用的访问路由、协议转换、安全防护等。通过采用Nginx、Spring Cloud Gateway等成熟的开源框架,可以快速构建高可用、高性能的统一接入服务。中间代理层主要使用商密SSL网关和统一接入服务作为接入反向代理。应用层与服务层之间通过REST API和API实现松耦合对接。

2.服务层设计

服务层采用微服务化的设计理念,将密码服务能力下

沉,封装为一系列细粒度的API服务,包括:

1、密钥管理服务(KMS):提供密钥全生命周期管理,包括密钥生成、导入导出、轮换、销毁等,确保密钥永不明文出现在系统之外。

2、签名验签服务(SVS):提供数字签名、验证、时间戳等服务,支持多种数字证书格式。可用于认证授权、不可抵赖等安全场景。

3、协同签名服务(SKS):提供密钥分片管理、多方计算等服务,支持多方参与的密钥使用流程,满足监管合规要求。

4、时间戳服务(TSA):提供精确的时间戳,可用于对关键业务数据进行时间点认证。

5、基础密码服务:提供SM2/SM3/SM4等主流密码算法的运算API。

6、密码资源调度服务:支持云上密码资源池的统一调度和管理。

3.基础层设计

基础层主要包括存储模块和物理资源模块。存储模块为服务层提供数据持久化和缓存加速等能力。重要的数据存储服务包括:

1、关系型数据库:采用蚂蚁集团自主研发的数据库OceanBase,用于存储结构化数据,主要存放服务端的密钥分量以及平台用户的一些配置信息,支持SQL操作,保证数据强一致性。

2、缓存数据库:采用Redis等内存数据库,用于存储高频访问的热点数据(如Session会话、Token令牌等),提升服务响应速度。例如,缓存协同签名服务端密钥分量。提高系统处理效率。

物理资源模块为服务层提供了高可靠、高安全的计算、网络、存储等IT基础设施,是平台安全稳定运行的底座。其中密码基础设施采用自主可控的商用化软硬件产品,包括:

1、操作系统:采用银河麒麟等商用操作系统,保障系统安全可控。

2、服务器:使用信创CPU服务器,CPU内置密码协处理器(CCP)和安全处理器(PSP)。支持商用密码算法,通过硬件隔离保护关键密钥,提供密钥全生命周期管理,满足合规要求。

(四) 密码服务平台实现

本方案的密码服务平台主要由密码硬件(CPU)、API网关(密码接口)、服务层(密码服务)、容器部署等组件构成,如下图所示:

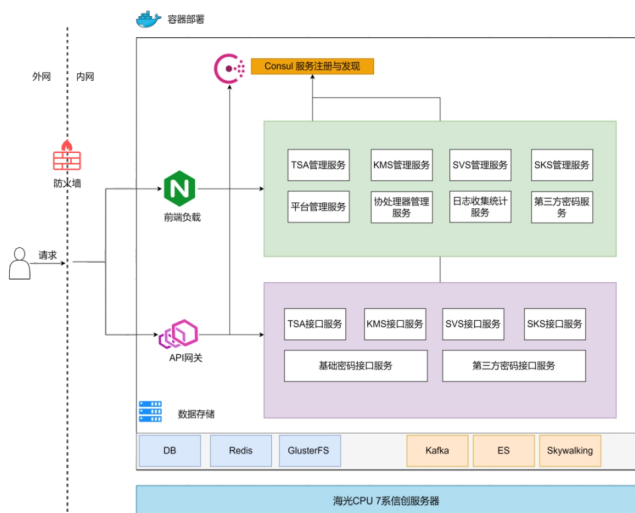


图3 密码服务平台实现图

1.密码计算资源池实现

密码计算资源池采用信创CPU构建了强大的计算平台,CPU内置密码协处理器(CSP)和安全处理器(PSP)为上层密码运算服务提供高速、安全、稳定的密码运算能力。信创CPU提供强大的通用计算能力,支持各种复杂的密码算法和大规模并行处理。

2.密码服务接口实现

密码接口采用Spring Boot框架构建微服务架构的API层,同时使用Spring Security进行身份认证和授权管理。Restful API使用HTTP调用时,需要先进行接口认证。接口认证主要包含两部分,WEB调用的HMAC(也称为AKSK)认证和服务访问权限认证。具体如下图:

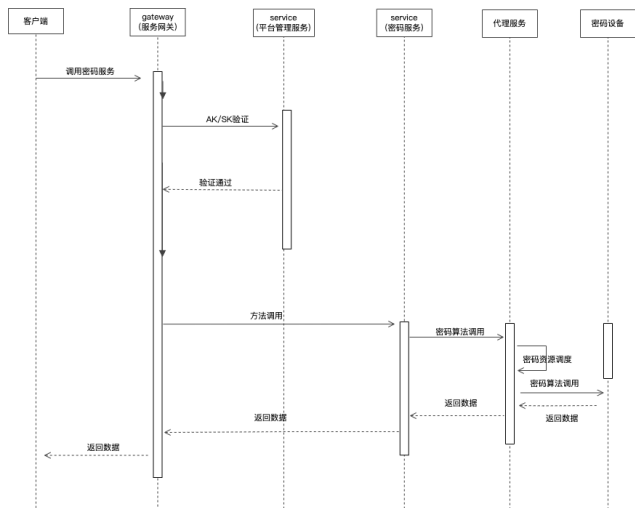


图4 Restful接口调用验证流程图

采用多语言代码生成工具自动生成多语言SDK基础代码。支持C++,java和python等多种语言调用,SDK调用时,客户端使用TCP长连接访问后台接口,客户端只需要按照接

口文档方式,设置对应的参数则可以获得平台提供的加解密,签名验签的原子能力,相对比较简单。

3.密码服务实例实现

服务型密码组件基于信创服务器部署,并以1对1的形式为用户提供服务。为确保安全互通,用户和密码服务之间采用了云原生的SDN (Software-Defined Networking) 技术。密码服务侧的终端节点服务绑定了内网4层负载均衡CLB(云负载均衡),对后端RS(Real Server)进行健康检查及故障自动剔除,从而确保密码服务的高可用性。

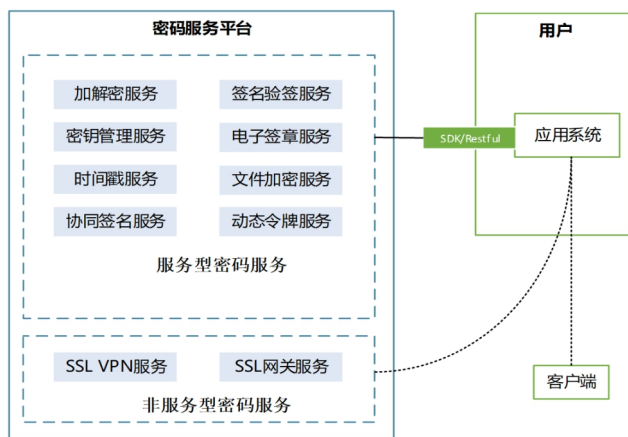


图5 密码服务实例功能图

4.密码服务全链路监控实现

通过对密码服务平台各项数据的收集、分析,动态、整体的洞悉密码服务中台运行风险,从密码服务平台全局视角提升对异常状态的发现识别、理解分析、响应处置,实现对密码服务平台整体运维的态势感知。

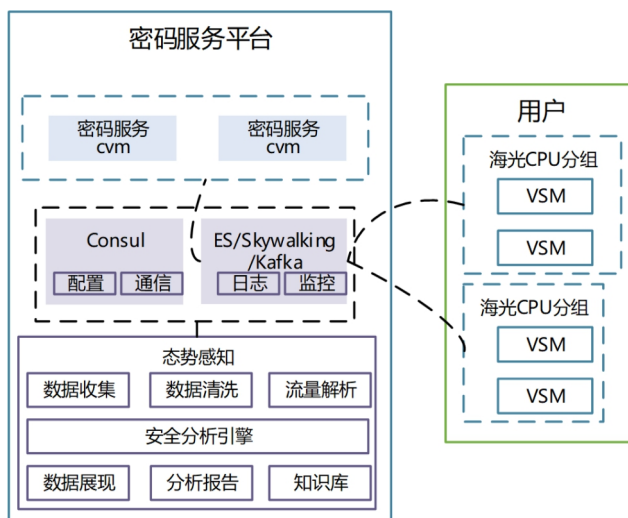


图6 密码服务平台监控实现示意图

密码服务平台通过Kafka,ES收集保存密码服务、密码资源的监控数据、业务日志数据和运行日志数据,由密码服

务平台内置的安全引擎收集ES中所有类型数据并对数据进行清洗,对流量数据进行解析,深入分析密码服务与密码资源业务情况,向用户输出辅助运营决策内容。

同时,密码服务平台通过Skywalking实现数据在平台内部交互的全链路监控,及时监控系统的运行情况,第一时间发现生产问题。

(五)密码服务平台核心功能

基于CPU强大的算力和内置的商密协处理器CCP,密码服务平台构建了全面、完备的密码服务功能体系,可为证券行业各类应用场景提供灵活、高效的密码服务,提供的核心功能主要如下:

1.有效地管理密码资源池

平台基于CPU的硬件虚拟化能力,实现了异构密码资源的池化管理。通过将分散的物理CPU进行逻辑划分和抽象,平台形成了一个统一的虚拟密码资源池。资源池中不同类型、不同性能的密码资源可灵活调度,实现按需分配。

通过抽象资源池,平台实现了密码基础设施与上层应用的解耦,让资源供给能够灵活适配业务变化。租户无需关心背后复杂的物理资源管理,只需按需申请所需的虚拟密码资源即可。这种弹性、敏捷的资源供给机制是传统密码机无法比拟的。

2.提供标准的密码服务能力

平台提供了通用密码服务、典型密码应用服务、密码基础服务等多个层次的密码服务,可满足证券行业的多样化密码应用需求。

通用密码服务主要面向签名验签、加解密、摘要计算等常见密码应用,提供SM2、SM3、SM4等商密算法的基础运算能力。服务基于CPU的CCP硬件实现,性能远超加密卡性能。在通用服务的基础上,平台还针对证券行业的常见应用场景,设计了一系列典型密码应用服务,包括时间戳服务、数字信封服务、电子印章服务等。

3.构建全生命周期的密钥管理机制

平台采用分层密钥体系,将密钥分为根密钥、密钥加密密钥(KEK)、数据加密密钥(DEK)三个层级。关键的根密钥使用CPU内部的物理不可克隆功能(PUF)进行保护,由硬件直接生成,存储在芯片内部,无法被读取。PUF造就了一个无法复制、不可篡改的硬件根。KEK和DEK则在根密钥保护下存储在CCP的安全存储区中,并通过严格的权限控制和访问控制避免被非授权方获取。多级密钥配合使用,避免了根密钥的频繁访问,降低了暴露风险。

平台提供了完整的密钥全生命周期管理,包括密钥产生、分发、更新、备份、销毁等。密钥产生使用CCP的随机数发生器,保证了随机源的安全性。密钥分发和存储则充分利

用CPU的内存加密、可信执行环境、安全指令等特性,保证了密钥不落地、不出芯片边界的物理隔离。例如,分发密钥时,采用SM2椭圆曲线临时密钥协商,协商得到的会话密钥全程由CCP硬件保护,不会暴露在内存中。

4.提供统一的密码服务接口

为了便于各类应用系统的集成使用,平台提供了多种灵活的服务集成方式,既有标准统一的API接口,也有简单易用的SDK,还有现成的密码组件。

平台的密码服务提供RESTFUL风格的API,涵盖了密钥管理、加解密、签名验签、摘要、随机数等主要密码功能。API将CPU的商密算法能力进行抽象封装,采用通用的JSON格式进行参数传递和结果返回。应用只需调用相应API并传入明文数据,即可获得密文结果,并不需要理解底层密码学细节。

5.支持云原生友好的部署模式

平台采用分布式微服务架构,天然适配云原生部署环境。平台的服务组件以容器镜像的形式封装,可一键部署到Kubernetes等容器编排平台上。容器化部署带来的好处是服务实例可快速启停和动态伸缩,资源利用率大幅提升。

三、网上交易系统商用密码应用实践

(一)网上交易系统目前密码应用方案

目前,行业内各证券公司网上交易系统商用密码改造方案是使用支持商密算法的协同签名网关(包括安全认证网关服务端和协同签名服务),数字证书系统以及硬件加密卡配合完成通讯链路的安全加固(以下称原方案),架构如下图所示:

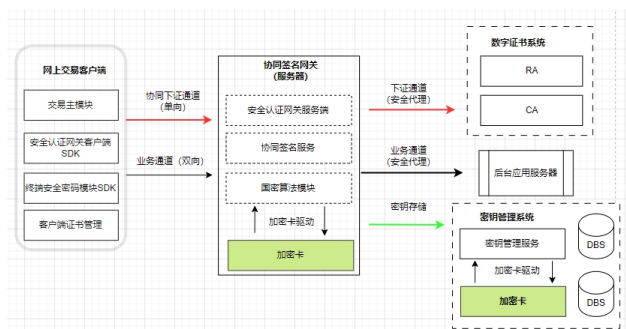


图7 目前商密应用方案

协同签名网关主要有安全认证网关服务端和协同签名服务构成,安全认证网关服务端主要负责客户端的安全接入以及通讯数据加密;协同签名服务和数字证书技术主要负责保证客户端身份安全;硬件加密卡主要为上层的协同签名应用和SSL网关提供安全、高效的算力支持。

当前方案虽然完成了通讯链路的安全加固,但存在以下不足,主要表现在:

- 1、兼容性成本高。服务器操作系统的升级或者修复补丁,需要密码卡硬件厂商在新的环境下重新编译硬件驱动,整个流程十分繁琐耗时长,工作量大。
- 2、密码服务不能很好响应快速扩容。扩容增加服务器都需要进入机房安装加密卡现场调试确认,不能响应快速扩容需求。
- 3、密码服务不能复用,密码硬件采购成本高。由于行业合规风控要求,不同系统之间的交易通道需要做物理隔离,新的系统如果要使用密码服务,需要重新搭建一套密码服务和采购加密卡,提高了公司采购成本。

(二)基于密码服务平台的商用密码应用方案

基于密码服务平台的密码应用方案(以下称新方案)是使用可信密码模块替换硬件加密卡,来完成上层密码应用所需要的密码计算与密钥存储功能。同时,结合密码服务平台应用层提供的能力,完成网上交易系统安全加固。架构如下图所示:

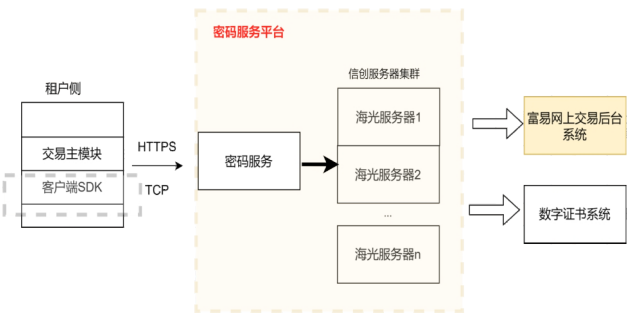


图8 基于密码服务平台的商用密码应用方案

不同模块的功能如下表所示:

表1 新方案不同模块功能

系统	模块	功能
网上交易客户端	交易主模块	交易模块,实现交易业务功能
	客户端 SDK	使用该 SDK 提供相关的接口对接云密码服务平台
密码服务平台	SSL 网关	安全认证网关服务端,实现符合 0024 标准的 SSL 服务端协议
	协同签名服务	协同签名服务端,实现协同签名的服务端密钥分量生成,配合客户端生成协同签名
	密码管理系统	负责安全存储协同签名服务端的密钥分量
	可信密码模块	内置于服务器 CPU,提供密钥生命周期管理和签名验签,加密和解密等能力
数字证书系统		提供基于 SM2 的证书签发服务
富易网上交易后台系统		国泰君安网上交易后台系统

(三)方案的等效性分析

原方案与新方案在实现功能上,两个方案是等效的,均能满足业务需求。但在安全性、稳定性及性能上新方案会更优、扩展性和易用性更强。

1.安全性

原方案使用硬件加密卡,在安全上,一方面,加密卡需要CPU通过PCI-E总线接口访问加密卡外设,这种完全通过外部总线与CPU相连的方式,由于增加了物理暴露面,容易受总线类物理攻击,如侧信道攻击等。另一方面,传统加密卡采用集中式提供密码运算服务(类似加密机),密码运算和密钥管理通常需要借助网络进行传输,增加了数据泄露和篡改的风险。新方案使用CPU内置可信密码模块,可以将密钥管理和密码运算放到本地进行,避免网络数据传输中数据泄露和篡改的风险。

2.稳定性

稳定性上,原方案使用传统加密卡,容易出现接口松动、物理总线接口损坏以及加密卡本身损坏等问题,而新方案使用CPU内置密码模块,集成于CPU内部,与处理器形成一个整体,可以避免接口松动、物理接口损坏、接触不良等问题,模块本身损坏率大大低于加密卡本身。

密码模块内置于CPU内部,其本身稳定性等同于CPU自身稳定性。“海光3号”CPU芯片采用了高可靠性设计技术和严格的产品检测技术,设计寿命10年。

3.性能

性能上,新方案使用可信密码模块直接在CPU内部提供密码运算,无需经过网络和主板上的总线通信,整个过程在CPU内部完成,是一种简单高效的处理方式。这种方式降低了数据通信的延迟,实测数据表明,海光3号可信密码模块验签功能的性能(吞吐量)是当前市场高端加密卡的3倍以上。

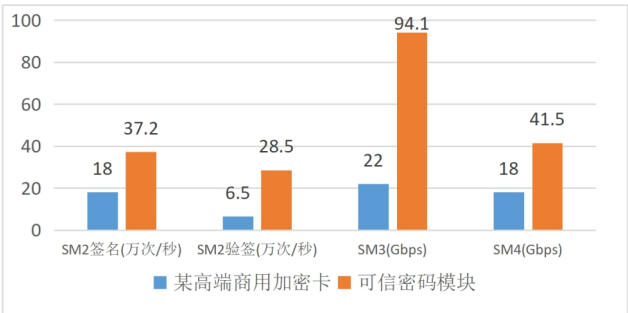


图9 平台底层可信密码模块性能

4.快速扩容

在快速扩容方面,新方案采用可信密码模块支持虚拟化方式调用,可以在云环境实现快速扩容及密钥的同步。相比原方案,在扩容方面更加灵活高效。同时,可信密码模块在密码模块数量、虚拟机数量、密钥槽数的支持上都大大优于传统PCI-E加密卡,单独的物理机可以支持更多的虚拟密码资源。

表2 可信密码模块与加密卡可支持虚拟密码资源对照表

对比项	可信密码模块	某 PCIE 加密卡
密码模块	64	32
虚拟机	无限制	32
密钥空间独占	支持	支持
密钥空间共享	支持	否
密钥槽数	20000	1024

可信密码模块在CPU内部，扩容时，用户无需插拔密码卡，无需适配加密卡设备驱动，能响应快速扩容的需求，同时借助密码服务平台能力，方便对上层的密码服务一键扩容，使用起来十分方便。

5.对接难易程度

在对外提供接口上，新方案采用可信密码模块实现了国标定义的通用SDF接口，可以无缝和原方案采用加密卡设备进行替换，其内部包含多个密码处理器资源来提供高性能的密码运算。

但是，新方案借助平台一键部署的优势，用户无需关心密码服务的实现和部署细节，无需关心运维，拿来即用，对接的难易程度比原方案要容易得多。

6.密钥管理方式

借助平台提供的密码资源统一管理的能力，平台能实现服务端密钥的统一管理与分发，用户无需一台一台机器上去同步密钥，更不用担心服务端证书和密钥更新难，同步慢的问题。密钥管理简单且效率高。

四、方案的优势

(一)信创与商密同步推进

在基于CPU的商用密码应用方案中，商密和信创统筹规划，同步推进。信创适配工作是证券行业重点工作，是否满足信创已经成为行业内新系统能否上线的重要衡量指标。新方案采购的密码服务均运行在商用信创银河麒麟V10操作系统上，采购的是基于信创CPU的服务器，采用的加密模块是国产自研具有二级密码资质的可信密码模块，在满足商密要求的同时，完全适配信创。

(二)更高的性能指标

可信密码模块直接内置在CPU芯片内部，相较于插在主板上的PCI-E加密卡，天然地更加接近CPU运算单元，拥有更低的通信延迟和更高的吞吐量。

通过使用性能测试工具实测结果显示，CPU内置密码模块性能在商密运算上的性能指标优于传统商用加密卡。经测试，可信密码模块签名验签功能的性能是传统加密卡的3倍左右。

(三)更安全稳定的加密方式

可信密码模块，内置于处理器内部，降低额外增加硬件、维护的成本，并且减少系统攻击面。同时，可信密码模块直接内置于CPU内部，其安全性和稳定性可由CPU本身安全性进行保障。

(四)兼容性好，支持快速扩容

可信密码模块支持主机、容器、虚拟机等业务场景，兼容K8S、OpenStack等云平台管理工具，满足当前密码服务平台业务需求。扩容时，无需添加额外硬件设备，支持虚拟化部署和动态扩容。

(五)降低采购成本

基于CPU的商用密码应用方案盘活了当前采购信创CPU已有的商密计算资源，减少了采购成本。相对于原硬件加密卡方案，一台服务器上需要采购1张加密卡，新方案充分利用信创服务器计算资源，可以省去加密卡的采购成本。

(六)更便捷的密码使用方式

一方面，基于CPU的密码服务平台可以支持通过SDK调用和HTTP接口的方式为其他系统提供低耦合、轻量化、原子化的操作接口，提供统一的密码服务。另一方面，密码服务使用非常便捷，用户无需过多关注服务端适配和部署，更无需关注密钥同步等问题，拿来即用，使用便捷。

五、课题不足及未来展望

(一) 课题不足

为了营造更方便的商密推广应用环境,追求密码技术从能用到好用的目标,基于CPU内置的可信密码模块,我们打造统一的密码服务平台,该平台屏蔽底层密码设备的差异,为上层应用提供标准的密码服务和统一的接口,减少公司的开发和运维成本;同时,平台支持远程调用底层的CPU内置可信密码模块,进一步盘活底层的密码计算资源,减少公司采购成本。方案在满足信创要求的同时,天然支持商密算法,有很强的应用价值。

但是,由于项目时间紧,任务重,密码服务平台虽然满足了密码应用的业务需求,但仍然存在以下的不足:

1、平台底层的密码设备目前只对接了X86架构的海光可信密码模块,尚未完成和ARM架构的主流鲲鹏密码计算设备进行对接,存在一定的风险。

2、使用密码服务平台的系统不多,目前,只有网上交易系统与密码服务平台完成了对接,通过平台提供的密码能力完成了网上交易系统互联网侧的安全加固,其他系统尚未完成对接。

(二) 未来展望

鉴于上述的不足,未来,一方面我们要督促供给侧,提供ARM架构可用的可信密码模块,并完成平台与它的对接;另一方面,提供详尽的使用说明和接口文档,加大密码服务平台的推广力度,将公司其他的签名验签,电子签章以及数据加解密的功能迁移到平台上来,实现平台的使用价值。

同时,随着商密技术在行业推广,我们会将此平台应用到其他系统商密应用改造项目中,让平台赋能于其他系统,真正实现密码技术从能用到好用的目标。

证券公司软件供应链安全管理平台 研究与实践课题摘录

课题负责人：吴佳伟

课题组单位：兴业证券股份有限公司
海通证券股份有限公司
奇安信科技集团股份有限公司

课题组成员：王玥、李志龙、吴佳伟、钟蓉、李鹏、曹杰、温志强、韩智鹏、马冰、康乐、韩建

摘要：随着证券行业数字化转型的加速，软件供应链安全成为行业发展的关键挑战。为应对高复杂度软件、广泛开源组件使用以及众多外部供应商带来的安全隐患，国家与行业相继发布了相关法规和规范要求。证券公司软件供应链安全管理平台研究与实践课题从软件供应商管理、开发安全管理及开源安全治理三个维度出发，通过自研和外购两种渠道软件引入的全流程平台化安全管控方案，快速建立起软件供应链安全管理流程，实现对供应链的攻击发现和风险预警，通过软件供应链安全一体化管理提升软件供应链安全管理水平。

关键字：软件供应商安全管理、开发安全管理、开源软件安全治理、软件供应链安全一体化管控平台

一、课题研究背景和价值

随着针对软件供应链的攻击强度和激烈程度不断加深，以及证券行业信息化建设及应用的不断深化，重点领域软件系统更新、新建速度加快，加之网络空间战略地位的日益提升，作为行业性的重要软件系统极易成为网络攻击目标^[1]。以破坏设施为目的的分布式拒绝服务（DDoS攻击）、勒索为目的的勒索病毒、窃取信息为目的的高级持续威胁（APT攻击）等类型的网络攻击活动日益频繁和活跃，同时演变出更多、更复杂、更隐蔽的攻击工具和方法。传统的网络安全解决方案已经对组织网络建立起较为全面的防护，攻击者从传统渠道的攻击成本大幅提升，此种背景促使攻击者寻找组织新的突破口。由于不安全的服务软件和技术，许多机构都曾遭受过系统故障、信息被盗、客户流失、被罚款等各种问题，软件供应链已经成为攻击组织进行重要软件系统网络攻击的重点切入点^[2]。

基于公安、网信、证监会等各监管机构多年来持续推进针对重要软件系统的等保建设、攻防演练工作，重要软件系统的安全保障能力有了根本性的提升。但近年来各种真实安全事件和攻防演练暴露出了更多的软件供应链安全风险，突出风险有两类：一类是供应商自身存在的安全风险，

例如供应商网络安全缺陷导致运维权限被盗用、源代码泄露、敏感信息泄露等；另一类是软件产品本身的安全风险，例如开源组件漏洞、代码缺陷等。

由于证券行业重要软件系统具有行业专属性，以及业务向云端互联网等服务界面的延伸，软件系统功能及性能受到业务需求、合规需求等多方驱动不断提高，软件的复杂度也随之不断上升^[3]。近年来，证券行业数字化转型，容器、中间件、微服务、DevOps等新技术得到广泛应用，软件复杂度高、开源组件使用广泛、外部供应商多等特征凸显，由此导致证券行业软件供应链的安全隐患愈发突出。近年国家、行业发布《网络安全审查办法》、《关键信息基础设施保护条例》、《证券期货业网络和信息安全管理办法》、《证券公司网络和信息三年提升计划（2023-2025）》等法规和规范，对证券行业软件供应链安全提出更高要求，软件供应链安全已成为行业网络安全工作中不可或缺的一部分。

当前证券行业软件呈现商业采购占比大、外部供应商相似度高的特点，有着共性的上下游供应链生态，一旦发生软件供应链安全风险，可能产生行业级影响，我国在软件供应链安全方面的基础比较薄弱，国家、各行业尚未建立成熟的软件供应链安全管理平台^[4]。当发生供应链安全事件时，无法在短期内进行上报和整体统筹，重要软件系统相关安

全问题难以集中分析处理,无法准确发现全局性、整体性的安全威胁,以及有针对性的发出信息通报预警并进行联动处置。基于上述问题,从软件供应链的安全管理、安全技术、安全运营三个维度出发进行体系化建设,建立软件供应链安全管理平台,基于一个平台对软件供应链中供应商安全、开发安全、开源软件安全进行一体化管理,强化软件供应链安全保障,赋能行业业务稳健发展。

二、课题研究内容和目标

软件供应链安全管理平台的研究是基于一个平台对软件供应链中供应商安全、开发安全、开源软件安全进行一体化管理,形成软件供应链安全管理支撑平台,有效提升软件供应链安全管理能力。本课题主要研究内容分为以下三个方面:

- 1、软件供应商安全管理:行业外部采购占比大,供应商安全管理是行业软件供应链安全重要组成部分,对软件供应商安全资质、商业风险、历史信息系统漏洞、开发安全能力、应急响应能力等方面进行画像,为供应商准入、持续评估提供管理依据,合理有效管理软件供应商的安全能力,从源头提升软件供应链安全水平。
- 2、开发安全管理:将安全技术措施嵌入软件研发各阶段,对软件研发过程中开展的安全需求分析、源代码安全检

测、软件成分分析等开发安全工作进行平台化集中管理,结合安全编排流程,将威胁建模工具、SCA、SAST、DAST、IAST、漏洞管理等能力由平台实现统一自动化调度,保障软件开发中快速交付的安全性。

3、开源软件安全治理:实现开源软件准入、持续安全评估和退出的全生命周期安全管理。开展开源软件风险评估,识别软件资产中使用的开源软件并定位已知漏洞,发生新漏洞公开或许可证协议变更等情况做到及时预警。

围绕软件供应商管理、开发安全管理及开源安全治理三个维度开展软件供应链安全体系化建设,建立软件供应链安全管理平台,实现软件供应链安全平台化管理,降低软件供应链安全风险,提升商业采购软件、自主研发软件、开源软件的安全性。

三、平台架构设计

为了实现三大目标,即软件供应商安全管理、开发安全管理、开源软件治理,平台的架构主要分为数据采集和处理层、平台支撑层和业务应用层。数据采集和处理层主要是解决自动化数据的来源,平台支撑层主要是平台的配置管理和流程实现,业务应用层是三个模块的体现和总体的软件供应链风险态势呈现。证券公司软件供应链安全管理平台的系统架构如图所示:

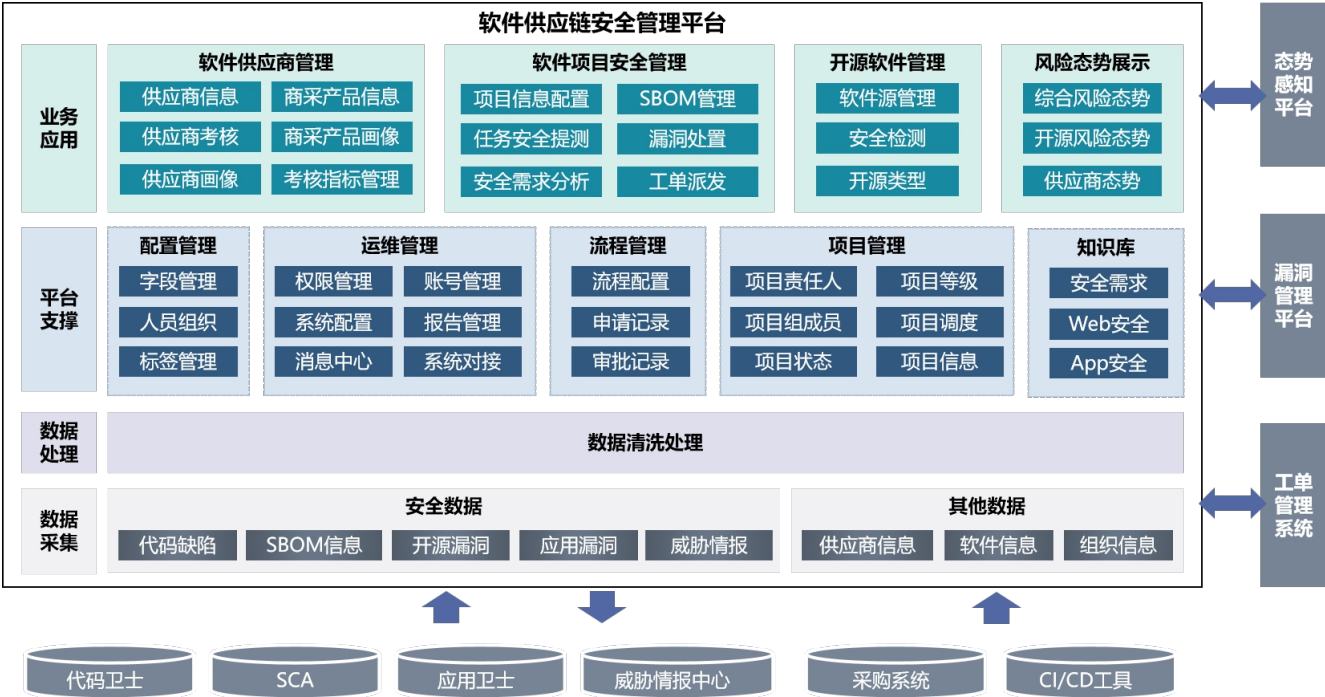


图1 系统架构图



图2 软件供应商安全管理

1.软件供应商安全管理

软件供应商安全管理模块通过对接各类项目流程、配置平台、外部情报信息库等实现对证券行业软件供应商信息自动化管理,为软件供应商准入、持续评估及退出提供管理依据。合理有效管理软件供应商的安全能力,从源头提升软件供应链安全水平。

系统通过软件供应商基本信息绘制软件供应商安全画像,供应商画像主要由四个层面组成:软件的安全漏洞情况、软件实施过程评价情况、软件的安全事件情况、供应商的自身风险。软件的安全漏洞情况数据来源于供应商交付软件过程中的上线测试漏洞数据及历史漏洞预警情况,不同级别的漏洞对应不同分数。软件实施过程评价主要来自供应商在开发测试和部署软件中的实施风险评价。实施风险评价由一系列问卷组成,问卷围绕软件供应商在实施过程获取的权限、完成的风险操作及人员误操作等问题构成,不同回答对应不同分数。软件的安全事件情况数据来自安全运营过程中发现的安全事件归因数据,不同级别的事件对应不同分数。供应商自身风险基础评估数据来自供应商安全资质、供应商的行业软件占比等数据。对于不同维度的参数,平台通过加权赋值的方式构建了打分体系。

通过对供应商各项指标进行数据统计汇聚分析,构建行业软件供应商风险指标。



图3 软件供应商画像

2.开发安全管理

微软在2004年正式提出了安全开发生命周期模型(SDL),并在其软件开发过程中广泛应用。SDL模型旨在通过整合安全能力到软件开发的各个阶段,从而提高软件系统的整体安全性,减少安全漏洞的产生。随着时间的推移,SDL已成为一种广泛应用的企业应用安全建设模型,已经被越来越多的组织和企业使用,并被证明是一种有效提升系统安全性的方法。SDL的核心理念就是从需求、设计到发布产品的每一个阶段都增加相应必要的安全活动,以减少软件中漏洞的数量并将安全缺陷降低到最小程度。在该种理念下,该平台的开发安全管理模块对软件研发过程中开展的安全需求分析、威胁建模、源代码安全检测、软件成分分析、安全测试等开发安全工作进行平台化集中管理。



图4 开发安全管理工具调度

在软件建设的立项环节,开发建设方需要在平台上完成软件相关设计的基础调研,平台会基于各类软件风险建模方法如STRIDE、证券行业内外规如《证券期货业网络安全等级保护基本要求》、《兴业证券股份有限公司信息系统开发安全规范》及《兴业证券股份有限公司个人信息保护管

理办法》等规范及兴业证券各类系统的基线标准输出安全需求报告、安全设计报告、安全测试报告，指导建设方按照符合行业规范及兴业证券内部标准的要求构建软件。



图5 安全需求分析

在软件开发测试环境，平台统一自动化调度编排SCA、SAST、DAST、IAST、等工具对软件进行安全检测。开发建设方通过配置系统测试地址、软件代码仓库地址及制品仓库地址等，实现对软件应用的应用、代码及引入的第三方开源组件进行快速扫描。安全管理方负责日常安全工具运营，明确安全工具检出漏洞的修复标准，提升平台汇聚漏洞的准确率。同时平台也提供了人工测试的角色，将人工渗透的漏洞结果于平台统一进行汇聚。



图6 安全检测任务

3. 开源软件安全管理

证券行业的软件供应链中自研和外购系统均引入的大量开源组件和软件，目前兴业证券内部已形成了开源组件使用的相关规范--《兴业证券股份有限公司开源公共基础软件管理规程》及开源组件引入的相关标准--《兴业证券股份有限公司开源公共基础软件准入标准》。

在此基础之上，本平台将工具、内规和流程结合。在工具维度，平台通过调度SCA工具的检测能力，通过多层次的开源软件依赖分析、高效的软件指纹分析、源代码片段分析等分析技术，对软件中所使用的开源软件进行精确识别，识别哪些软件使用了哪些开源软件，并提供开源软件的引入路径和引入方式。提取证券公司端对软件中使用的开源软件标识、维护组织、版本等特征信息，提取开源软件特征文件、软件源代码包、远程代码仓库、容器镜像包等并发起开源软件分析任务。



图7 开源组件分析能力

在流程维度，平台实现了开源软件安全的准入评估、引入后的持续跟踪及退出评估流程。通过定期开展开源软件风险评估，识别软件资产中使用的开源软件并定位已知漏洞，发生新漏洞公开或许可证协议变更等情况做到及时预警并联动软件成分分析的网关实现主动拦截。

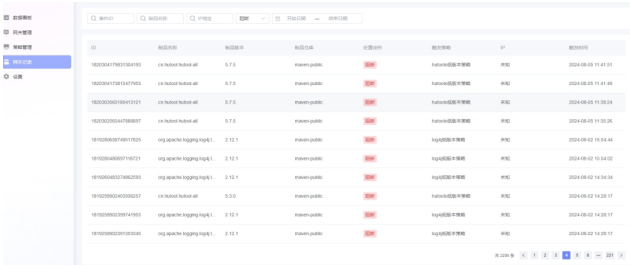


图8 开源组件出入库管理

4. 软件应用的安全图谱

软件供应链安全管理平台设计了可视化的软件供应链安全图谱。软件供应链安全图谱能够帮助用户更好地理解和管理所运营软件的供应链安全相关的风险和数

据，梳理软件引入各环节各层级的风险，并以更直观的形式呈现软件各层级的风险指标。

基于供应商管理、开发安全管理、开源软件安全治理等功能模块收集的基础数据，进行整合分析，平台梳理软件供应商→软件系统→代软件漏洞及安全事件+实施风险等各层次的风险，并以层级图关系展示，以便安全管理方发现软件供应链管理最薄弱环节。



图9 软件供应链安全图谱

在供应商层级,安全图谱显示地展示了各个供应商自身的风险及在兴业证券落地的各个系统所存在的风险。在商业软件供应链漏洞爆发时,该图谱能有效助力内部安全管理人员快速定位商软内部使用团队。

在软件层级,通过证券公司软件供应链安全管理平台形成证券行业软件供应链清单,如OA办公平台、电子邮件系统、业务终端软件、行业专用软件等,能够与供应链商信息关联。



图10 软件管理

平台还建设了软件供应链安全态势分析大屏,安全管理者能通过大屏实时观测公司内部的软件供应链风险。供应链态势大屏主要有两方面的数据来源,其一是系统建设过程中引入的各项风险数据,其中又分为供应商风险和软件风险,其二是来自互联网的软件供应链威胁情报监测。多方数据将在看板汇聚,形成宏观的统计数据,揭示目前证券公司内部重大风险排名情况。

大屏主要包含供应商等级排名、软件风险等级排名、供应商风险等级分布、软件类型分布、各风险评分项对应的供应商数量分布。实现了供应商及软件资产的安全风险综合评估,反映实际安全状态,以量化的方式体现安全风险及安全工作成果。



图11 应用安全态势分析

四、课题技术创新

1.信创底座

经过国产化改造,该系统已全面适配麒麟操作系统,实现了与国产数据库OceanBase和中间件宝兰德等的深度集成。这一改造不仅提升了系统的自主可控能力,还确保了数据安全和信息安全。系统利用Java的跨平台优势,保证了在

国产环境下的高效运行和稳定服务,满足了国内用户对信息技术产品国产化的需求。

2.多形态软件供应链产品的检测能力

证券行业的软件供应链主要依赖外部采购,其交付形式呈现多样性。具体来看,从物理形态角度,可以区分为以下几种类型:集成了硬件与软件的一体化设备、纯粹的软件系统、以及基于云计算的服务等。进一步地,从软件形态的角度进行分类,可以发现包括镜像文件交付、制品交付、以及源代码交付等多种形态。此外,从软件架构的角度分析,主要可以分为证券公司端/服务器(C/S)架构和浏览器/服务器(B/S)架构。

由于分类方法的不同,相应所需的检测工具也各不相同,这就要求平台必须能够支持多种扫描器的集成和调度。该平台汲取了应用程序安全编排与关联(ASOC)的核心理念,能够从各种扫描工具(例如静态应用程序安全测试SAST、动态应用程序安全测试DAST、交互式应用程序安全测试IAST)中收集数据,并将其融合进入统一的数据库中。随后,平台会对收集到的数据结果进行综合关联分析,并对关键的修复任务进行优先级排序。这一流程的实施,旨在以一种更加明智和高效的方式,简化并优化安全检测活动。

3.证券公司软件供应链的全流程管理

平台通过与公司内部的立项、采购、项目建设平台以及各类软件开发基础设施实现对接,确保了在软件引入的各个关键环节中有效地融入安全措施。

在项目立项阶段,进行的安全评审主要关注以下几个方面:平台规划中所涉及的账户密码认证体系、内部功能设计、平台架构、数据在平台内部的流转方式,以及开源组件的使用情况等。通过软件建设方填写的基础信息安全问卷以及与安全评审人员的评审会议,对系统在当前规划阶段需要满足的内外部规定要求以及安全架构设计要求进行梳理,并最终形成文档手册。

在软件建设过程中,自研软件和外购软件的流程的区别主要为是否涉及采购环节。针对自主研发的系统,平台通过与内部的DevOps平台进行对接,实现对开源组件引入的限制以及在代码迭代过程中设置及时的扫描检查点。对于外购的系统,采购前供应商评分被纳入采购评分参考,签订合同中相关安全需求作为软件需求,采购完成后供应商的分数作为事后供应商评价的参考。

在软件即将上线前,项目建设方可以通过相关流程触发平台的对应扫描任务。平台随后通过调度扫描器,自动化地完成安全检测。在进行大规模版本发布时,人工安全测试将被纳入流程之中。不论是工具自动生成的输出结果还是人工检测结果,都会在平台上进行展示。

软件上线后,平台利用安全图谱功能,通过关联互联网上的软件供应链情报,实时反映软件的安全态势。这样的措

施有助于持续监控并维护软件的安全性,确保及时发现并响应潜在的安全威胁。

五、课题完成情况和应用成果

本课题围绕软件供应商管理、开发安全管理及开源安全治理三个维度开展软件供应链安全体系化建设,建立软件供应链安全管理平台,实现了软件供应链安全平台化管理,降低软件供应链安全风险,提升商业采购软件、自主研发软件、开源软件的安全性。

课题建设主要分为三个阶段,一是调研和平台设计阶段,二是开发测试阶段,三是上线推广阶段。在课题调研和平台设计阶段,通过多个外部金融单位和内部的风险评估,课题组总结了目前证券公司所面临的软件供应链风险集中在软件供应商、软件开发和引入的开源软件三个维度。为了提升软件供应商安全,首先需要构建一套评价体系去量化现有数百家软件供应商的安全水平。该阶段项目的难点主要在于软件供应商的安全模型构建。课题组协同内外部专家评审出四个维度,并构建了不同的打分体系,并借鉴过往数据修正加权。开发测试阶段,平台需要完成数据层的接入和处理,以及平台支撑层各模块功能的处理。最后是上线推广阶段,目前平台已接入新建系统流程,纳管了多套新建系统,积累了多套软件全流程建设的基础安全数据。对于存量系统,仍需时间和数据积累。

六、课题总结

通过建设证券公司软件供应链安全管理平台,实现软件供应链安全入网、软件供应链安全检查、软件供应链安全监测的安全能力建设,形成常态化的软件供应链安全管理机制,为行业关键基础设施、重要证券公司提供检查能力,保障证券行业常见交易软件、行情软件等软件应用,提升安全性,实现对软件供应链攻击的有效防护。

参考文献

[1]王勇,赵雨雨.软件供应链安全保护措施[J].信息与电脑(理论版),2024,36(01):189-192.

[2]上官晓丽,孙彦,李彦峰.信息通信技术供应链安全政策法规与标准研究[J].中国信息安2021,(10):43-46.

[3]何熙翼,张玉清,刘奇旭.软件供应链安全综述[J].信息安全学报,2020,5(01):57-73.DOI:10.19363/J.cnki.cn10-1380/tn.2020.01.06.

[4]纪守领,王琴应,陈安莹,等.开源软件供应链安全研究综述[J].软件学2023,34(03):1330-1364.DOI:10.13328/j.cnki.jos.006717.

[5]苏仟,赵娆.开源软件供应链安全风险分析与发展建议[J].信息安全研究,2022,8(08):831-835.

[6]董国伟.软件供应链安全现状分析与对策建议[J].中国信息安全,2021,(10):34-37.

自动化和常态化的网络资产攻击面运营平台的研究与实现

课题负责人：季常青

课题组单位：南京证券股份有限公司
北京华顺信安信息技术有限公司

课题组成员：宋士明、叶飞、姜玥、汪洋、赵武、邓焕

摘要：本课题聚焦证券行业网络资产安全，创新并构建自动化和常态化的网络资产攻击面运营平台。平台通过集成多源数据，并归一化整合、自动化检测和修正，实现网络资产全面发现与暴露面收敛，优化管理流程，构建漏洞风险评估与应急响应机制，提升风险评估精度及加快应急响应速度。本课题深度融合大语言模型、网络资产发现与集成、资产与业务画像构建等技术，在降低工时支出、每日自动采集资产状态数、资产安全差距分析、漏洞优先级排序及处置等方面有较大的提高。这些创新技术的协同应用显著提升了南京证券网络资产的管理效率和安全水平，有效降低了网络安全风险。本课题的相关研究与实践，聚焦证券行业资产攻击面管理面临的共性问题，对证券行业具有较高的参考价值，可以有效助力证券行业的数字化转型进程加速推进，为证券市场的安全稳健运行提供了坚实保障。

关键字：网络资产、攻击面管理(ASM)、风险暴露面管理(CTEM)、漏洞扫描、漏洞修复、风险评估、应急响应、自动化、智能化

一、课题研究背景及意义

(一) 研究背景

随着“互联网+”政策的推动与贯彻，多种信息技术的发展与数字化建设的加快，“后疫情”时代网络威胁复杂多变，各行业网络资产攻击面激增，有组织、有目的的网络攻击频发，全球重大网络安全事件不断，勒索软件、数据泄露等危害升级，为网络安全防护工作带来更多挑战。网络攻击者的攻击成本在不断降低，手段更加先进，关键信息基础设施的网络安全形势日趋严峻，威胁了国家安全。根据国家计算机网络应急技术处理协调中心发布的《中国互联网网络安全报告》，我国网络安全威胁有以下特征：1) APT借社会热点、供应链等攻击重要行业，远程办公致攻击面扩大；2) 历史重大漏洞利用风险依然严峻，修复工作紧迫；3) 供应链中网络安全产品自身漏洞风险攀升。

(二) 证券行业网络资产安全现状

近年来，随着网络安全相关的“三法一条例”的颁布施行，国家及行业监管机构更加重视网络资产及其漏洞的管理。《证券期货业网络和信息安全管理办法》《证券基金经营机构信息技术管理办法》等行业规章明确了证券经营机构

的相关要求，网信部门多次发文强调“加强互联网基础资产管理”，《证券行业等保2.0标准》也提出“编制并保存与保护对象相关的资产清单”、“对漏洞风险持续跟踪”等监管合规要求。

随着证券公司数字化转型和金融科技的发展，网络资产规模快速增长，形成了复杂的网络架构，攻击面不断扩大，迫切需要掌握完整的网络资产及网络架构，识别各种类型攻击，并采取适当的措施来减少攻击面。同时，业务迭代使网络资产持续变化，使用传统手工评估方式已难以应对资产更新快和攻击升级的现状。此外，金融科技外包的场景也越来越多，证券公司的供应链安全管理难度越来越大。因此，证券公司在重点时期保障和日常安全运营工作中，都需自动盘点网络资产，建立动态台账，实时关注其风险与漏洞情况。

为了更加深入了解证券行业的资产风险现状，2024年1月到2月，课题组面向53家行业机构（含证券公司、期货公司、基金公司、核心机构等），针对网络资产攻击面管理情况做了一个问卷调查。调研数据凸显，网络资产数据在多个安全平台虽广泛应用，但其完整性和准确性亟待改进。具体而言，高达80%以上的平台（如安全运营、SOC、漏洞管理平台）强烈需求高质量数据支持，而数据质量问题成为瓶颈。

此外,风险处置高度依赖人工经验(60.38%),限制了复杂威胁下的响应速度。同时,风险评估方法传统且缺乏攻击者视角(仅占49.06%),精准定位责任人需求未获充分满足(58.49%),亟需转型与创新以应对日益严峻的安全挑战。

(三)国内外研究情况

本课题聚焦证券行业“摸清家底、认清风险、收敛攻击面”的网络资产与漏洞管理实际需求,梳理内外部攻击面。其中攻击面运营为近年来的新兴领域,受到国内外研究机构重视。

自2021年起,Gartner在多个报告中强调了外部攻击面管理(EASM, External Attack Surface Management)、网络资产攻击面管理(CAASM, Cyber Asset Attack Surface Management)和攻击面管理(ASM, Attack Surface Management)的重要性,并详细描述了这些技术的定义和应用场景。国外如Axonius、Balbix、Tenable等厂商,在多能力融合、可视化技术的应用方面取得了显著成果,实现了资产、漏洞和风险的关联分析,通过整合漏洞管理、Web应用安全、云安全、身份安全及外部攻击面管理等功能,实现对网络安全风险的全面监控和有效应对。

国内安全厂商则侧重网络资产测绘、漏洞检测、应用安全防护、溯源管理及网络空间地图等领域,通过主、被动测绘技术实现对组织内部IT资产、API资产、开源组件、僵尸资产以及合规资产外连的识别,实现组织内部资产的快速盘点与收敛。国内厂商在网络资产攻击面运营方面各具特色,但普遍存在未能完全贴合业务场景的问题。例如,如何快速定位资产责任人、及时有效识别供应链组件、自动化地风险告知等业务需求尚未得到完全满足。技术创新面临挑战且与国际先进技术的接轨和融合方面也有待加强。

虽然国内外在相关研究方面已取得一定成果,但在具体实践和应用中仍存在较大差距。国外企业在技术创新和实际应用方面更为领先,而国内企业则更多关注于技术的引进和本土化改造。国内外企业在行业应用侧重不同,国外在金融、电信等行业的应用更为广泛和深入,而国内更多聚焦于政府、能源等领域。这在一定程度上影响了技术选型和应用场景的匹配。国内外企业需加强合作与交流,共同推动技术的创新和应用,以更好地应对网络安全挑战。

结合国内外市场研究报告,目前网络资产攻击面运营在国内外均为热门方向,已经具备一定基础,但仍处于相对起步阶段,均在探索如何能够结合实际场景建设自动化和常态化的攻击面运营方案。

(四)研究意义

证券公司已普遍建设了资产运维管理、Web扫描、HIDS、漏洞扫描、漏洞管理和态势感知等系统或服务对攻击面进行梳理,但在安全运营管理中普遍存在不足:1)缺乏专业、成熟的技术,全面、准确和完整地发现网络空间中与组

织相关的网络资产;2)缺少安全运营视角下的资产之间的相关性展示;3)无法及时应对组织的流程、人员和系统频繁变更而导致的网络资产变更;4)缺乏将碎片化和遗漏的资产属性数据进行统一集成的能力;5)传统的资产管理、漏洞管理等平台缺乏资产组件信息,难以快速有效应对供应链攻击;6)缺乏1day/Nday历史漏洞利用爆发时快速评估攻击面和影响面的能力;7)资产管理系统与安全相关系统缺乏联动,降低安全运营效能;8)缺少安全度量方法和工具。

综上,目前证券行业亟需建立一套自动化和常态化的网络资产攻击面运营平台,帮助证券公司提高攻击面管理水平,缩小信息差,及时有效地采取防御和反制,有效降低人工成本和规避操作风险。其研究意义如下:

1.有助于引领证券行业在网络资产攻击面安全管理的实践,对网络资产和漏洞实现闭环运营,助力推动行业数字化进程。

2.有助于通过多源数据融合发现并补全资产数据的空白点,构建资产知识图谱,提升资产数据价值,并能更便捷地实现资产安全的差距分析及安全能力覆盖度分析,得出资产的防护清单,为资产的安全配置提供赋能支持。

3.有效地建立员工资产台账,用于员工身份管理、资产关联管理,解决身份识别、资产追踪等痛点。形成从资产发现风险,精准定位并一键告知负责人,实现风险及时处置,完成资产风险的闭环运营管理。

4.有力的连接业务系统资产库,将资产信息与业务系统储存资产关联,提高风险评估的效率,以便对重点资产安全威胁,进行快速的应急处置。

5.自动化的实现漏洞处置,结合资产价值评估漏洞优先级,自动化的处置流程大幅提高漏洞管理效率。

6.有效的推动流程再造,网络安全制度、流程和运营操作的优化,依托资产安全中台与相关信息系统集成,提高网络资产攻击面管理效能。

二、研究目标

一是构建全面数据视野。本课题致力于研究和实现多源数据的汇聚分析,通过收集不同渠道(如用户行为、系统日志、外部威胁情报等)的数据,进行集中处理和综合分析,提供更全面、丰富的视角,为安全管理和业务决策提供支持。

二是统一数据平台,自动化数据收集和融合。研究将聚焦于如何高效、准确地收集和整合多源数据。包括设计有效的数据收集机制,确保数据的完整性、准确性和及时性;采用数据融合技术,将异构数据统一,为分析奠定基础。

三是数据驱动业务优化。进一步探索如何将数据分析的结果与证券行业的业务场景紧密结合。通过深度挖掘数据间的关联性和规律性,将网络安全管理赋能给业务,提升

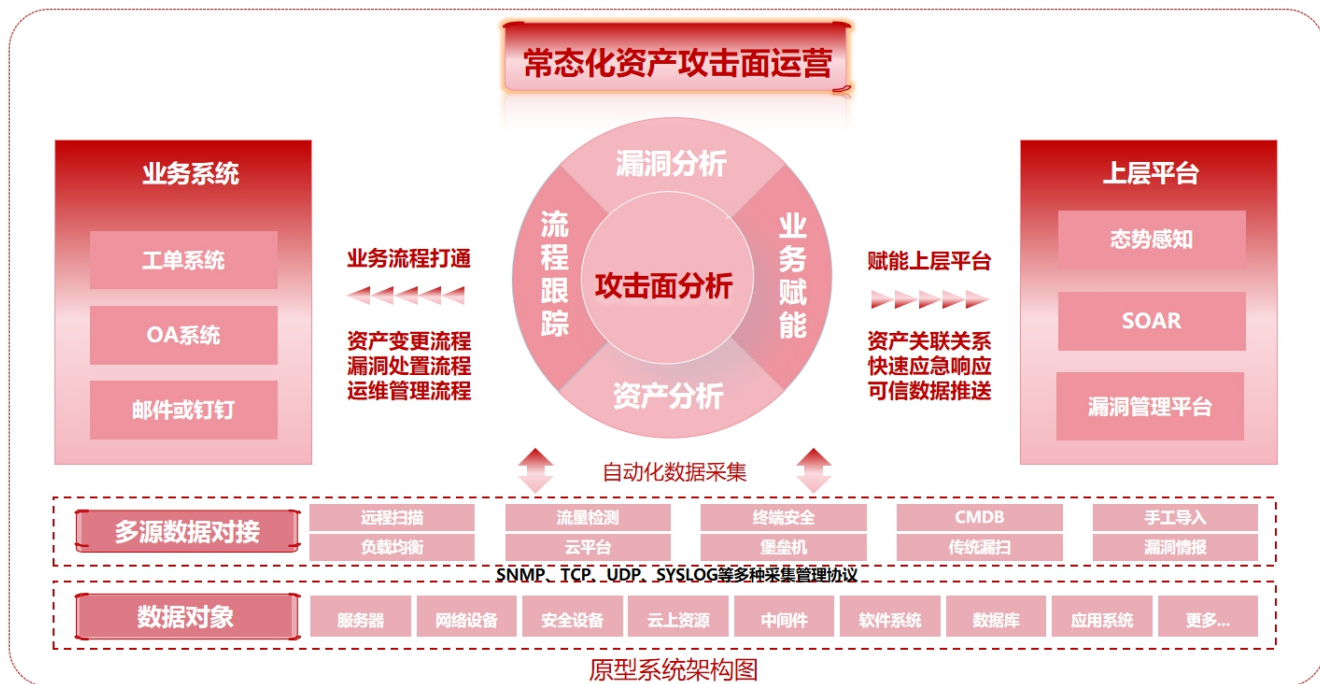


图1 系统原型架构图

企业对市场动态的敏感度和响应速度。

四是业务场景精准洞察。在研究中，将特别关注多源数据在特定业务场景中的应用。通过构建分析模型，实现对业务安全场景的全面洞察和精准预测。

五是资产驱动安全。基于“资产驱动安全”理念，实现网络资产的精细化管理和实时安全监控，提升安全防御的主动性和精准度，保障业务连续性。

六是构建自动化安全体系。研究和实践，创新性地构建、优化一个实现自动化、常态化运营的资产攻击面安全体系。为证券行业的数字化转型奠定坚实的安全基础，提升整个行业的安全水平和竞争力。该体系如图1所示。

三、研究主要方法

(一)研究内容

本研究聚焦于从实战攻防的角度出发，旨在探索并实践自动化与常态化的网络资产攻击面运营平台在实战攻防演练与日常安全管理中的应用。具体研究内容与实践方向包括：

(1) 攻击面识别与暴露面收敛

以攻击者的视角，通过多渠道搜集目标的网络资产信息以寻找突破点为背景，自动化且持续地发现并管理组织在互联网上暴露的网络资产。对未知资产、影子资产、供应链资产进行收敛，以有效缩小暴露面。

(2) 持续威胁暴露面管理(CTEM)体系构建

研究将从传统的攻击面管理(ASM)升级为持续威胁暴露面管理(CTEM)，全面强化网络资产暴露面的管控。研究内

容将涵盖暴露面的发现、风险评估与修复、对抗能力验证以及威胁的持续监测，提升组织整体的安全防护能力。

(3) 纵深防御与核心保护策略实施

研究将借鉴战争中的纵深防御与核心防护理念，通过多层次、重点突出的防御策略，延缓攻击者的渗透速度，增加入侵成本，从而将潜在损失最小化。首先获取全量资产清单与重点资产详情，并建立资产关联关系图谱；其次，将漏洞关联资产图谱，形成闭环的漏洞运营机制；同时，进行安全防护差距分析，为后续安全运营建设提供精确指导；结合模拟攻击技术，度量安全覆盖的有效性。

(二)技术方法

1.网络资产发现与集成技术

网络资产发现与集成技术致力于研究并应用异步无状态扫描、爬虫技术、有效URL验证、资产指纹验证以及网络服务扫描等先进技术，实时采集来自各类异构的资产数据，旨在建立一个全面的资产台账，结合变更机制，确保所有变更都被准确记录并留存变更日志。

2.资产与业务画像构建技术

课题致力于建立资产和业务画像。可全面反映资产的设备属性信息、网络属性、用户信息、指纹信息以及归属信息等关键要素。而业务画像则深入揭示了技术的属性、管理的属性以及资产间的差距等核心特征。

3.多数据源融合技术

为了实现异构数据的集成管理与关联分析，课题着重解决了来源各异的资产数据在格式和语义上的不一致问

题。通过这一努力，课题实现了实时的数据集成、关联、去重以及质量提升，极大地增强了数据处理的有效性和准确性。

4.网络资产差距分析技术

课题定义了明确的资产配置基线和合规策略，并深入研究了实时资产状态与差异检测算法。在此基础上，课题提出了支持资产差距分析的建模技术，为更精准地把握资产状况提供了有力支持。

5.漏洞风险评估技术

通过漏洞风险评估模型，可对资产的价值、漏洞的风险进行优化评级，实现自定义策略下的资产漏洞优先级修复排序。这一模型的应用，可紧密结合证券公司实际业务情况，建立起价值驱动的漏洞优先级和应急响应机制。

(三) 关键技术与创新点

课题的创新点在于融合了综合性、系统性、自动化、智能化、动态适应性与持续性等特点，构建了一个全方位的安

1.大语言模型分析技术在资产梳理中的应用

依赖传统的资产梳理方法不足以应对资产日益增长所带来的资产管理挑战。利用大语言模型语义分析技术，可以对异构数据源之间的实时资产数据进行更为深度的整合和分析，提取资产数据的显性信息，洞察潜在的资产关系与隐含结构，从而确保资产数据的连续性、完整性以及实时性。利用先进的网络空间测绘技术，结合大语言模型分析，对证券行业的资产进行全面、精准的识别与梳理，进一步增强了资产管理的效率和准确性。

表1 引入大语言模型前后工作量对比

工作环节	引入大语言模型前 (每周/月)	引入大语言模型后 (每周/月)	节省工作量 (每周/月)
数据整合	40 个人工时	自动化处理，无需人工	40 个人工时/160 个人工时
信息提取与分析	18 个人工时	自动化处理，少量人工复核	18 个人工时/72 个人工时
异常检测与修正	0 个人工时 (每月集中处理)	实时自动检测与修正	0 个人工时/20 个人工时
报告编制	20 个人工时	自动化生成，少量人工调整	20 个人工时/80 个人工时
总计	78 个人工时/312 个人工时	自动化为主，少量人工辅助	78 个人工时/332 个人工时

2.网络资产关联关系知识图谱可视化展示技术

证券行业网络环境复杂，资产间关系难以直观展现。通过深度分析资产实体间的多维关联类型与语义，使用语义分析技术进行资产关联关系的模型研究，分析资产实体之间的关联类型，设计支持关联推理的知识图谱构建方法。不

仅增强了在复杂网络环境中的资产视图，还为安全运营团队提供了更为清晰且易于管理的网络资产框架。为证券行业提供了更为直观和全面的资产视图。

通过对核心节点、安全问题、内部通信、负载均衡、外部访问、CNAME记录等网络资产复杂性和关联性进行图谱可视化，解决了证券行业网络环境复杂，资产间关系难以直观展现的问题。为安全运营团队提供了清晰、易于管理的网络资产框架，提升了安全运营的效率。

3.网络资产差距分析与合规技术

证券行业对合规性要求极高。基于大数据分析定义资产配置基线和合规策略。研究实时资产状态与差异检测算法，提出支持资产差距分析的建模技术，实时资产状态与差异检测算法为持续的网络资产攻击面管理和网络安全运营提供有力支撑。差距指标具体包括：(1) 性能指标：CPU使用率、内存占用率、网络带宽利用率等；(2) 安全指标：漏洞数量、入侵检测事件、安全合规性等；(3) 异常状态指标：同类资产服务差异。平台定期（每小时、每天）将实时资产状态数据与配置基线进行对比，计算差异值。引入统计测试来评估差异是否显著。当检测到显著差异时，通过邮件、短信、即时消息等方式向相关人员发送报警通知。报警信息应包含差异详情、可能的原因、建议的解决措施等。

4.结合大语言模型分析技术与VPT管理

证券行业对业务连续性和安全性要求极高，传统漏洞处置方式难以满足漏洞应急响应的需要。结合大语言模型分析技术与VPT管理，综合考虑资产价值和漏洞可利用性，制定更为合理的漏洞优先级排序方案。同时，提供自动化的应急响应机制，确保在发现漏洞后能够迅速、有效地进行处置。

5.网络空间测绘技术

证券行业网络资产类型多样，数量庞大，传统方法难以全面梳理。以网络空间测绘技术为基础，利用安全大数据分析技术全面、精准地识别网络资产，构建详尽的网络空间资产库，为网络安全防护提供坚实的基础。

6.信创资产识别与发现技术

目前平台还可对信创资产进行识别发现，可深度识别1800+的信创指纹，同时针对现有的业务环境，整合了信创非信创资产的统一管理，避免了多套平台分属管辖的弊端。在信创替换背景下，通过测绘技术，和多源数据的接入，对接入资产分析后还可以做到对目前信创率的统计，为信创替换提供数据支撑。

(四) 应用成果

本课题针对证券行业高效运营、风险管理的实际需求，



图2 资产总览

形成了科学完善的资产管理体系。同时，基于系统的研究思路，深入研究并构建了一个涵盖数据分析与风险预警的综合性管理平台。

1.平台整体架构

本平台整体架构如图2所示，旨在构建一个全面、高效的攻击面运营资产安全中台，通过系统化的模块划分与协同，实现资产安全的全方位管理和监控。

2.核心功能模块

(1)资产管理

资产管理是平台的重要功能模块，平台支持主动测绘、流量采集、对接主机安全和CMDB等多种方式全面采集资产数据，通过资产的标准化、归一化和标签化能力实现资产管理的全面性和准确性。平台关注资产及资产间关联关系，发现薄弱资产，建立全局资产视角。

在资产梳理与多维度呈现方面，平台结合实际的业务需求，以设备视角、业务系统视角、IP视角、组织人员视角、网站等维度进行资产的多视角管理，同时可进行灵活快速查询，以应对安全运营中对资产属性信息可视化的需要。

(2)漏洞管理

针对平台上已添加的支持接收扫描任务的扫描器，可以配置扫描策略、下发扫描任务、查看扫描进度及扫描结果。通过扫描策略中的定时配置，可以完成自动化的批量扫描，达到动态监测的目的。

①漏洞总览

通过对扫描出的漏洞数据统计分析，综合展示漏洞风险态势。包括：全部漏洞数量统计、待处理漏洞数量、待派发漏洞数量、互联网IP漏洞数量、内网IP漏洞数量；漏洞发现趋势、漏洞修复状态占比、漏洞分类统计、漏洞风险等级。

②漏洞管理

展示通过扫描节点上报到平台的资产漏洞数据，平台对漏洞的检测、处置、验证做全生命周期管理，跟踪漏洞从发现到修复全过程。页面展示漏洞数据来源、漏洞IP、漏洞名称、CVE编号、漏洞等级、CVSS、风险值、漏洞类型、漏洞地址、业务系统、责任人、漏洞状态-责任人、发现时间、上次扫描时间等字段。

③漏洞情报

漏洞情报库内涵18w+漏洞数据，每天从各大漏洞情报平台获取最新漏洞数据并做归一化处理，每天更新1次。默认展示最新的10条漏洞数据（漏洞名称、CVE编号、影响软件、影响软件版本等），用于漏洞应急。

④优先级排序配置

系统根据优先级排序配置计算漏洞风险值，在漏洞管理中默认按照漏洞风险值排序，从而反映真实的漏洞修复优先级。

3.安全运营场景支撑

(1)资产发现与管理场景

平台能够自动化地发现企业网络中的各类资产，包括

硬件、软件、云资源等，覆盖了98.11%的硬件信息、IP、端口、服务、协议资产、云服务厂商，86.79%的域名、证书、URL资产，以及75.47%的泛资产（如公众号、小程序、APP）等，形成全面的资产清单。通过对资产的持续监控，能够实时反映资产的变化情况，为安全运营团队提供100%准确的资产信息支撑。通过对资产的持续监控，平台能够实时反映资产的变化情况，为安全运营团队提供准确的资产信息支撑。在资产管理方面，平台支持对资产进行分类、标记和属性配置，帮助安全运营团队快速定位关键资产和高风险资产，为后续的漏洞扫描、风险评估等工作奠定基础。

(2)漏洞扫描与修复场景

平台集成了先进的漏洞扫描工具和技术，能够定期或按需对网络资产进行漏洞扫描，及时发现潜在的安全漏洞。扫描结果将自动整合到平台中，形成漏洞报告，为安全运营团队提供修复建议。在漏洞修复过程中，平台支持全程跟踪漏洞修复进度，验证修复效果，确保95%以上的漏洞得到及时、有效的处理。同时，平台能够基于漏洞的严重程度和潜在影响，对已知漏洞进行智能优先级排序，帮助安全运营团队合理分配资源，优先处理70%以上的高风险漏洞。

(3)威胁情报与预警场景

平台通过整合超过数十个外部威胁情报源和内部安全日志数据，实现对网络威胁的实时监测和预警。当发现潜在的攻击行为或恶意活动时，平台能够准确识别90%以上的已知威胁和60%以上的新型威胁，同时能够迅速触发预警机制，通知安全运营团队采取相应的应对措施。威胁情报的整合与分析有助于安全运营团队全面了解当前的网络安全态势，提前制定应对策略，降低安全风险。

(4)应急响应与处置场景

在发生安全事件时，平台能够迅速启动应急响应流程，为安全运营团队提供事件分析、影响评估、处置建议等支持。通过自动化的应急响应机制，平台能够缩短响应时间，降低事件对企业业务的影响。在处置过程中，平台支持记录处置过程和结果，为后续的安全审计和改进工作提供依据。

(5)合规性管理与审计场景

随着网络安全法规的不断完善，企业面临着越来越严格的合规性要求。该平台能够支持对网络安全合规性的全面管理，包括合规性策略的制定、执行和审计等方面。通过自动化的合规性检查和报告生成功能，平台能够帮助企业确保网络安全措施符合相关法规和标准的要求，降低合规性风险。

(6)暴露面监控与收敛场景

通过暴露面管理，全面识别和评估网络系统中的潜在暴露点，包括未授权的设备、服务、应用程序等。这有助于及时发现并修复安全漏洞，防止攻击者利用这些暴露点进行恶意攻击。因此，暴露面管理的实施能够显著提升网络安全防护能力，降低安全事件的发生概率。

(五)知识产权成果

目前本课题涉及1个软件著作权及1个发明专利正在申请中，如表2所示。

表2 课题知识产权成果

序号	类型	名称
1	软件著作权	《南京证券自动化和常态化的网络资产攻击面运营系统》
2	发明专利	《一种基于未知网络资产空间探测的方法》

四、总结与展望

本课题集成与汇聚多源数据，引入大语言模型，对其进行归一化整合以及自动化检测和修正，辅以知识图谱可视化等技术，实现了对网络资产与漏洞的全面发现与展示，有效收敛潜在网络暴露面；通过优化网络资产管理流程，有效结合大语言模型与VPT管理，完善漏洞风险评估与应急响应机制，提升风险评估精度，加快应急响应速度。在实战攻防演习场景中，本课题研究成果能够有效发现和定位风险资产与漏洞，快速定位责任人并提供有效的应急处置措施，显著降低了南京证券面临的网络安全风险。

本课题的相关研究与实践，聚焦证券行业资产攻击面管理面临的共性问题，对证券行业具有较高的参考价值，可以有效助力证券期货行业的数字化转型进程加速推进，为资本市场的安全稳健运行提供了坚实保障。本课题后续拟在以下方面开展进一步的研究：

(一)深度集成与智能化提升

平台将进一步深化与南京证券现有网络安全技术平台的集成，实现更全面的资产管理和更精准的威胁检测。同时，借助更先进的AI和机器学习技术，平台将能够更智能地分析网络行为、识别异常模式，并自动采取相应的防护措施，进一步提升响应速度和处置效率。

(二)动态适应与灵活扩展

面对不断变化的网络威胁和新兴的攻击手段，平台将具备更强的动态适应能力和灵活扩展性。这意味着平台能够快速集成最新安全工具和技术，同时保持对现有安全策略的持续优化和更新，以应对新出现的威胁。

(三)合规性与隐私保护的强化

平台将在设计和实现过程中更加注重证券行业对合规性和隐私保护的要求，通过自动化的合规性检查和隐私保护机制，平台将确保南京证券的网络资产始终符合相关法规和监管要求，同时保护客户数据的隐私和安全。

(四)用户体验与业务融合的深化

平台将更加注重用户体验和业务需求的融合。通过用

户调研和反馈机制,平台将不断优化其功能和界面设计,以提供更符合南京证券业务需求和使用习惯的网络资产攻击面运营体验。同时,平台将更好地支持南京证券的业务发展和创新,为其网络安全提供有力保障。

(五)加强行业合作与共享安全情报

展望未来,南京证券将积极寻求与其他证券行业机构以及安全厂商的合作,共同构建跨行业的网络安全防护体系。通过共享安全情报和最佳实践,平台将能够更快速地识别和有效应对跨行业的网络安全威胁,提升整体安全防护水平。

(六)信创资产安全运营能力建设

平台将继续聚焦信创资产安全管理,进一步优化信创资产识别与分类能力,针对证券行业信创化改造过程中暴露出的新型威胁,持续完善风险评估模型,确保覆盖信创场景的多样化需求,为信创资产安全运营提供坚实保障,全面提升证券公司国产化环境下的网络安全能力。

参考文献

- [1]周余阳,程光,郭春生.基于贝叶斯攻击图的网络攻击面风险评估方法[J].网络与信息安全学报,2018,4(6):11-22.
- [2]刘胜娃,高翔,王敏.基于贝叶斯网络的攻击图方法在网络安全评估中的应用[J].现代电子技术,2013,36(9):84-87.
- [3]张璇,廖鸿志,李彤,徐晶,张倩茹,钱晔.基于信息熵和攻击面的软件安全度量,计算机应用,2013,33(1):19-22,48.
- [4]高春东,郭启全,江东,等.网络空间地理学的理论基础与技术路径.地理学报,2019,74(9):1710-1722.
- [5]蒋秉川,万刚,徐锐.网络空间剖分机理与可视化方法研究.系统仿真学报,2017,29(S1):1-8.
- [6]沙明、张旭、李佶、樊芳、张天意、房慧丽、侯春晓.上海证券交易所技战法报告-互联网暴露面收敛.网络安全防护专刊,2020,42:42-51.

投稿邮箱：
wsil@sse.com.cn.

ITRDC

ITRDC证券信息技术研究发展中心(上海)



中国上海市杨高南路388号

邮编:200127

公众咨询服务热线:4008888400

网址:<https://www.sse.com.cn/>



内部资料 免费交流

本资料仅为内部交流使用,本期印200册,编印单位为上海证券交易所,面向证券期货行业发送,印刷时间为2025年2月,印刷单位为上海町麦广告有限公司。

部分图片或文字来源于互联网等公开渠道,其版权归属原作者所有,如有版权相关事宜,请发送邮件至wsil@sse.com.cn.