政府采购项目合同履约抽检评价报告

项目名称	深圳市南山区医疗集团总部安全检测与响应管理平台采购		
项目编号	NSCG2023000417	合同编号	NSQYLJTZB-SZNSMIC-2023-07
采购人	深圳市南山区医疗集团总部		
履约供应商	海之景智能（深圳）有限公司		
抽检机构	深圳市计量质量检测研究院		
委托单位	深圳市南山区财政局		

签发人：

审　核：

主　检：

（盖章）

签发日期：2024 年 10 月 10 日

政府采购项目合同履约抽检评价报告

一、抽检总结

项目名称	深圳市南山区医疗集团总部安全检测与响应管理平台采购		
项目编号	NSCG2023000417	合同编号	NSQYLJTZB-SZNSMIC-2023-07
采购人	深圳市南山区医疗集团总部		
履约供应商	海之景智能（深圳）有限公司		
抽检机构	深圳市计量质量检测研究院		
委托单位	深圳市南山区财政局		
现场抽检地点	蛇口科技大厦 713 室	实验室检测抽样	□是 ☑否
现场抽检日期	2024 年 9 月 27 日	环境条件	（20～30）℃，（60～80）%RH
抽检依据	☑标准 SZDB/Z 319-2018 政府采购项目合同履约抽检及评价规范 ☑深圳市南山区医疗集团总部安全检测与响应管理平台采购项目(项目编号：NSCG2023000417)采购文件		
现场抽检结果汇总	经现场抽检，发现以下不符合项： 1.售后服务：现场未体现抽检方案第 3 项第 1 条要求“★供应商提供的产品安全检测与响应管理平台（XDR）提供原厂三年软件升级、三年规则库升级（包括安全检测特征识别库、文件智能分析模型库、安全知识库、热点事件、白名单库等）”。 2.项目组：现场资料显示项目经理何某煌社保在 2024 年 2 月于海之景智能（深圳）有限公司断缴，其当月离职，与抽检方案第 4 项要求“为保障本项目保质保量、高效实施，供应商为本项目成立项目组，同时为项目组配套专业施工团队，团队情况如下：1）安排项目组项目经理 1 人；2）安排项目组技术经理 1 人；3）安排项目组其他人员 2 人”不符。 3.安全检测与响应管理平台 XDR： (1)现场未体现抽检方案第 5 项第 3 条要求“平台基于 ClickHouse、Flink、pulsar、MongoDB.分布式存储的框架架构，可以提供具备弹性扩展能力和数据高可靠的基础平台”； (2)现场未体现抽检方案第 5 项第 17 条要求“支持通过标签对联动设备进行管理，可以在配置剧本和执行动作时，通过选择标签，快速对具有相同使用场景的设备进行指令下发”； (3)现场未体现抽检方案第 5 项第 19 条要求“支持待我审批功能，可以显示当前用户所有待审批剧本节点”； (4)现场未体现抽检方案第 5 项第 20 条要求“支持从脆弱性页面查看其关联的剧本执行详情”； (5)现场未体现抽检方案第 5 项第 21 条要求“支持一键遏制功能，可以联动对应端侧组件（如 EDR）和网侧组件（如防火墙）端网能力针对 IP、主机等各类实体进行一键处置，同时针对于 IP 可支持展示具体 IP 地址、风险标签与网络类型等，针对主机可展示资产名		

政府采购项目合同履约抽检评价报告

	称与责任人”； (6)现场未体现抽检方案第 5 项第 22 条要求“清点可展示相关资产列表，包含关键进程等维度”； (7)现场未体现抽检方案第 5 项第 24 条要求“要求：▲可以智能响应安全事件和安全告警中的关键威胁，针对于高置信度的重复或低危威胁实体可实现全自动化遏制闭环，可自定义对抗规则”； (8)现场未体现抽检方案第 5 项第 31 条要求“▲支持攻击指标检测，对攻击者的攻击手法进行检测，指标覆盖 ATT&CK 所有阶段攻击手法，以检测攻击准确性为目标，通过采集的网端数据进行研判、挖掘。可以发现高级威胁。支持自定义 IOA 规则。支持终端遥测源对 ATT&CK 框架中各种攻击类型的检测技术覆盖面 Windows 系统不低于 320 项，Linux 系统不低于 125 项”； (9)现场未体现抽检方案第 5 项第 32 条要求“提供辅助运营功能，要求至少提供 8 项能力：资产查询与统计”； (10)现场未体现抽检方案第 5 项第 33 条要求“威胁情报解读、恶意文件解读”； (11)现场未体现抽检方案第 5 项第 34 条要求“漏洞预警、排查与闭环”； (12)现场未体现抽检方案第 5 项第 35 条要求“安全告警统计筛选、研判”； (13)现场未体现抽检方案第 5 项第 38 条要求“安全趋势总结”； (14)现场未体现抽检方案第 5 项第 39 条要求“安全百科知识解读”。 4.服务器安全探针： (1)现场未体现抽检方案第 6 项第 2 条要求“管理平台包含高级威胁行为检测、安全日志采集等功能；要求必须能够与本次招标的安全检测与响应管理平台（XDR）无缝兼容”； (2)现场未体现抽检方案第 6 项第 3 条要求“支持全网视角的终端资产统一清点，便于帮助用户快速发现风险面”； (3)现场未体现抽检方案第 6 项第 5 条要求“▲支持一键云鉴定服务，提供云端专家+沙箱+多引擎鉴定能力，结合云端威胁情报对已告警的威胁文件再次进行综合研判并给出 100%黑白结果，用户可自助对管理平台告警的威胁快速判断是否误报和了解威胁详情”； (4)现场未体现抽检方案第 6 项第 6 条要求“支持全网威胁狩猎，可基于威胁情报的行为等各项终端应用层行为数据在全网终端发起搜索”； (5)现场未体现抽检方案第 6 项第 7 条要求“可以与安全检测与响应管理平台（XDR）联动，支持从海量告警中通过引擎和专家提出去真正需要用户关注和处理的事件为 incidents，完整还原整个攻击故事线，通过端点+网络数据历史攻击回溯，有效闭环彻底根治安全威胁”； (6)现场未体现抽检方案第 6 项第 8 条要求“▲可以扩展支持终端安全一体化 AIO(all in one）客户端，实现一次操作完成网络安全准入客户端、终端安全管理软件客户端、远程办公零信任系统客户端的组件安装，并只显示一个托盘图标，对用户安装部署、运维提供便捷性”。 根据现场抽检评价，结合本项目抽检方案，抽检评价总分为 60.6 分，抽检结果评价等级为中。 具体检测结果详见政府采购项目抽检明细。 抽检机构代表签字： 2024 年 9 月 27 日

政府采购项目合同履约抽检评价报告

二、抽检明细

商务条款					
序号	抽检项	代码	商务要求	抽检结果	单项评价
1	交货期	b	★自合同签订或约定之日起30个日历日内完成本项目到货、安装调试完毕、初步验收合格且交付使用（不含试运行时间、项目终验），项目进度满足采购人对项目的总体计划和进度要求	经资料查阅符合要求	符合
2	验收	b	1.供应商提供系统用户手册或产品说明书	经资料查阅符合要求	符合
		b	2.供应商提供系统安装手册，指导如何安装部署系统；负责培训采购人的技术员	经资料查阅符合要求	符合
		b	3.供应商提供系统运行维护手册，列出日常运行维护清单列表	经资料查阅符合要求	符合
3	售后服务	b	1.★供应商提供的产品安全检测与响应管理平台（XDR）提供原厂三年软件升级、三年规则库升级（包括安全检测特征识别库、文件智能分析模型库、安全知识库、热点事件、白名单库等）	现场未体现	不符合
		b	2.★供应商提供的产品服务器安全探针提供原厂三年软件升级	经资料查阅符合要求	符合
4	项目组	b	为保障本项目保质保量、高效实施，供应商为本项目成立项目组，同时为项目组配套专业施工团队，团队情况如下：1）安排项目组项目经理1人；2）安排项目组技术经理1人；3）安排项目组其他人员2人	现场资料显示项目经理何某煌社保在2024年2月于海之景智能（深圳）有限公司断缴，其当月离职	不符合

政府采购项目合同履约抽检评价报告

技术条款					
序号	抽检项	代码	技术要求	抽检结果	单项评价
5	安全检测与响应管理平台XDR	b	1.品牌型号：深信服 可扩展威胁检测响应平台XDR软件V2.0（XDR平台软件）	经现场检测符合要求	符合
		c	2.纯软件，支持集群部署，可以实现横向扩展弹性扩展，包含3个节点，虚拟机方式部署；虚拟机资源由采购方自备，提供3台虚拟机，每台虚拟机配置：CPU40核，内存128G，系统盘240G，数据盘40T	经现场检测符合要求	符合
		c	3.平台基于ClickHouse、Flink、pulsar、MongoDB.分布式存储的框架架构，可以提供具备弹性扩展能力和数据高可靠的基础平台	现场未体现	不符合
		c	4.配套提供第三方日志分析模块、SOAR自动编排模块、云端威胁情报模块、安全事件深度挖掘模块、移动运营小助手	经现场检测符合要求	符合
		c	**要求：** 5.支持接入第三方品牌的网络安全数据进行呈现、并汇入分析模块进行安全事件的分析和调查	经现场检测符合要求	符合
		c	6.提供可视化拖拽方式灵活自定义编排威胁的响应处置，实现半自动化、自动化联动安全设备进行分析研判、响应处置，内置“半自动化通用攻击事件处置闭环剧本”及众多场景剧本样例，也可自定义编写成客制化剧本，满足不同环境分析、决策、响应动作	经现场检测符合要求	符合
		c	7.提供未知文件/DNS/URL/IP等云端实时查询，实时展示本地IOC在内部网络和全行业社区的出现情况，支持云端专家实时分析互联网热门威胁事件、漏洞等，分析事件对于组织的影响程度和修复建议	经现场检测符合要求	符合
		c	8.支持海量灰度规则+多引擎分析，可基于云端数据湖，对海量线索和数据进行灰度规则和私有引擎二次分析，狩猎师研判后生成报告；可基于狩猎分析师的经验固化成检测模型，对于未知不确信的告警进行深度调查关联，自动化生成安全事件并推送；支持针对XDR平台产生的安全事件，云端专家介入做研判，进一步保障事件检出的准确性	经现场检测符合要求	符合
		c	9.支持安全事件推送，对平台产生的安全事件（非告警）、云端狩猎挖掘的事件、最新发生的新型威胁影响评估报告等事件，可以推送到服务号，随时掌控安全态势；支持移动处	经现场检测符合要求	符合

政府采购项目合同履约抽检评价报告

技术条款					
序号	抽检项	代码	技术要求	抽检结果	单项评价
			置运维，平台移动运维小程序可以实时展示安全事件的详情信息，并且联动网络/端点设备一键处置威胁；提供移动专家直连咨询，遇到不好理解、不易分析、难以处置的安全事件，可以立即联系专家协助处理		
		b	10.▲提供基础的网端、终端侧的检测数据接入和处理，实现对告警日志、遥测数据、审计信息的存储和检索。对跨安全产品的检测和响应机制提供基础的信息汇聚、存储、关联和分析能力，包含管理平台、检测响应分析引擎、数据湖模块、仪表盘、安全事件检索与调查、报表、基础大屏等功能	经现场检测符合要求	符合
		c	11.支持以标准Syslog、Kafka、SNMP Trap、JDBC、FTP、SFTP、Winlogbeat/Filebeat接收安全设备、网络设备、操作系统、应用系统、中间件、服务等各类第三方设备日志并存储，如防火墙、上网行为审计、应用交互、态势感知、扫描器、抗DDoS、DLP、UTM、IPS、IDS、WAF、漏扫等	经现场检测符合要求	符合
		c	12.支持对事件执行剧本和动作	经现场检测符合要求	符合
		c	13.支持展示当前已编排的剧本，同时可在该页面新建剧本	经现场检测符合要求	符合
		c	14.内置节点库：支持自动化执行节点、过滤型节点、人工介入和标记型节点，具备支持动作、过滤、决策、文本、审批、录入等，支持图形拖拽连线形成完整事件处置流程剧本	经现场检测符合要求	符合
		c	15.支持通过类似Visio的拖拽方式灵活自定义编排威胁的响应处置流程，并支持多种执行节点包括：动作调度、剧本应用、决策器、过滤器、人工审批、人工录入等必要的关键节点	经现场检测符合要求	符合
		c	16.支持自定义触发能力（自动和手动），可以基于安全告警、脆弱性的执行条件进行触发；支持配置通知策略，同时可以基于不同的通知场景自定义不同的通知方式及通知模板	经现场检测符合要求	符合
		c	17.支持通过标签对联动设备进行管理，可以在配置剧本和执行动作时，通过选择标签，快速对具有相同使用场景的设备进行指令下发	现场未体现	不符合

政府采购项目合同履约抽检评价报告

技术条款					
序号	抽检项	代码	技术要求	抽检结果	单项评价
		c	18.可以展示当前XDR中已对接的应用，支持网络安全设备的联动，包括防火墙、EDR、即时通讯、威胁情报等进行联动，实现对威胁的快速响应与处置	经现场检测符合要求	符合
		c	19.支持待我审批功能，可以显示当前用户所有待审批剧本节点	现场未体现	不符合
		c	20.支持从安全事件、安全告警、脆弱性页面查看其关联的剧本执行详情	现场未体现“支持从脆弱性页面查看其关联的剧本执行详情”	不符合
		c	21.支持一键遏制功能，可以联动对应端侧组件（如EDR）和网侧组件（如防火墙）端网能力针对IP、主机等各类实体进行一键处置，同时针对于IP可支持展示具体IP地址、风险标签与网络类型等，针对主机可展示资产名称与责任人	现场未体现	不符合
		c	22.支持资产清点，可以通过开放端口、应用软件、数据库、web服务、web框架、web应用、web站点、账号信息、运行进程、运行服务、启动项、计划任务、注册表维度进行资产清点。清点可展示相关资产列表，包含IP地址、资产责任人、数据源、互联网暴露情况、关键进程等维度	现场未体现“清点可展示相关资产列表，包含关键进程等维度”	不符合
		b	23.▲支持智能对抗	经现场检测符合要求	符合
		b	**要求：** 24.▲可以智能响应安全事件和安全告警中的关键威胁，针对于高置信度的重复或低危威胁实体可实现全自动化遏制闭环，可支持页面展示事件自动遏制率，可查看智能对抗记录及自定义对抗规则	现场未体现“要求：▲可以智能响应安全事件和安全告警中的关键威胁，针对于高置信度的重复或低危	不符合

政府采购项目合同履约抽检评价报告

技术条款					
序号	抽检项	代码	技术要求	抽检结果	单项评价
				威胁实体可实现全自动化遏制闭环，可自定义对抗规则”	
		b	25.▲支持业务优先和安全优先的模式切换，可匹配日常运营场景和攻防场景，同时针对于模拟试用场景，支持选择监测模式	经现场检测符合要求	符合
		b	26.▲支持针对网络设备、端侧设备进行联动配置以及针对新接入设备自动添加到智能响应，同时还支持设置IP封堵范围和自定义智能响应生效时段	经现场检测符合要求	符合
		b	27.▲支持基于时间、实体类型、处置状态和实体描述来筛选智能响应记录，并支持针对IP、域名、文件等不同实体类型设置响应黑白名单	经现场检测符合要求	符合
		c	28.支持威胁实体自动提取	经现场检测符合要求	符合
		c	**要求：** 29.安全事件响应处置支持对遏制威胁的实体对象自动提取，包括自动化提取安全事件中需要响应处置的“IP、域名、主机、进程、文件”五类实体，查看实体详情列表	经现场检测符合要求	符合
		c	30.针对IP实体支持导出、复制IP、封禁地址、再次封禁、解除封禁、查看情报等操作，针对主机实体支持隔离主机、导出等操作，针对文件实体支持处置文件、导出、查看请报等操作，针对进程实体支持阻断进程、导出、查看请报等操作，针对域名实体支持处置和复制域名、导出、再次处置、解除处置、查看请报等操作	经现场检测符合要求	符合
		b	31.▲支持攻击指标检测，对攻击者的攻击手法进行检测，指标覆盖ATT&CK所有阶段攻击手法，以检测攻击准确性为目标，通过采集的网端数据进行研判、挖掘。可以发现高级威胁。支持自定义IOA规则。支持终端遥测源对ATT&CK框架中各种攻击类型的检测技术覆盖面Windows系统不低于320项，	现场未体现	不符合

政府采购项目合同履约抽检评价报告

技术条款					
序号	抽检项	代码	技术要求	抽检结果	单项评价
			Linux系统不低于125项		
		c	32.提供辅助运营功能，要求至少提供8项能力：资产查询与统计	现场未体现	不符合
		c	33.HTTP告警数据包解读、威胁情报解读、恶意文件解读	现场未体现“威胁情报解读、恶意文件解读”	不符合
		c	34.漏洞预警、排查与闭环	现场未体现	不符合
		c	35.安全告警统计筛选、研判	现场未体现	不符合
		c	36.安全事件的解读与查询	经现场检测符合要求	符合
		c	37.攻击IP调查	经现场检测符合要求	符合
		c	38.安全趋势总结	现场未体现	不符合
		c	39.安全百科知识解读	现场未体现	不符合
6	服务器安全探针	b	1.品牌型号：深信服 端点安全软件V3.0	经现场检测符合要求	符合
		c	2.包含1个控制中心平台+300个服务器探针授权；管理平台包含终端资产管理清点、终端基线检测、高级威胁行为检测、攻击可视化展示、威胁狩猎、级联管理、行为日志采集、安全日志采集等功能；要求必须能够与本次招标的安全检测与响应管理平台（XDR）无缝兼容，作为安全检测与响应管理平台（XDR）的安全探针，实施网络安全检测、响应、联动	现场未体现“管理平台包含高级威胁行为检测、安全日志采集等功能；要求必须能够与本次招标的安全检测与响应管理平台	不符合

政府采购项目合同履约抽检评价报告

技术条款					
序号	抽检项	代码	技术要求	抽检结果	单项评价
				（XDR）无缝兼容”	
		c	3.支持全网视角的终端资产统一清点，便于帮助用户快速发现风险面。清点信息包括操作系统、应用软件、监听端口和终端账户，其中操作系统和监听端口支持从资产和终端两个视角进行统计和展示	现场未体现“支持全网视角的终端资产统一清点，便于帮助用户快速发现风险面”	不符合
		c	4.支持对系统账号信息进行梳理，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、弱密码账号、可疑root权限账号、长期未使用账号、夜间登录、多IP登录进行账号分类查看，支持统计最近一年未修改密码的账户	经现场检测符合要求	符合
		b	5.▲支持一键云鉴定服务，提供云端专家+沙箱+多引擎鉴定能力，结合云端威胁情报对已告警的威胁文件再次进行综合研判并给出100%黑白结果，用户可自助对管理平台告警的威胁快速判断是否误报和了解威胁详情	现场未体现	不符合
		c	6.支持全网威胁狩猎，可基于威胁情报的病毒文件哈希值、行为、域名、网络连接等各项终端系统层、应用层行为数据在全网终端发起搜索，挖掘潜伏攻击，快速定位出全网终端感染该威胁的情况	现场未体现“支持全网威胁狩猎，可基于威胁情报的行为等各项终端应用层行为数据在全网终端发起搜索”	不符合
		c	7.可以与安全检测与响应管理平台（XDR）联动，支持从海量告警中通过引擎和专家提出去真正需要用户关注和处理的事件为incidents，完整还原整个攻击故事线，通过端点+网络数据历史攻击回溯，有效闭环彻底根治安全威胁	现场未体现	不符合

政府采购项目合同履约抽检评价报告

技术条款					
序号	抽检项	代码	技术要求	抽检结果	单项评价
		b	8.▲可以扩展支持终端安全一体化AIO（all in one）客户端，实现一次操作完成网络安全准入客户端、终端安全管理软件客户端、远程办公零信任系统客户端的组件安装，并只显示一个托盘图标，对用户安装部署、运维提供便捷性	现场未体现	不符合

注：

1、评价条款分为极重要条款、重要条款、一般条款三类，分别以代码 a、b、c 表示；极重要条款不设分值，重要条款设为 5 分，一般条款设为 3 分。

2、评价分值计算方法：

$$T=\frac{S_1}{S}\times 100=\frac{120}{198}\times 100=60.6$$

式中：

T——评价分；

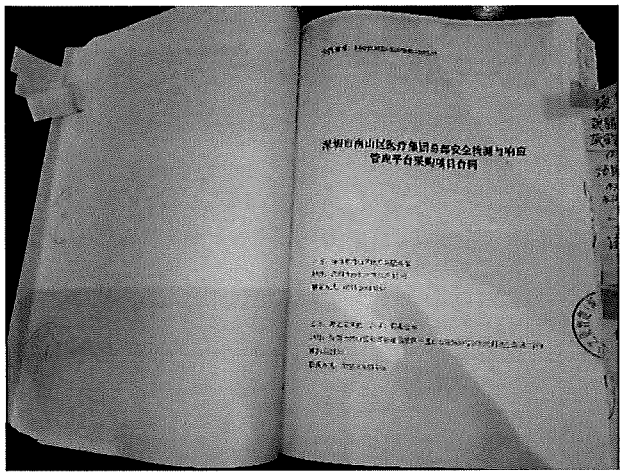
S_1——分项指标实际得分；

S——分项指标总分。

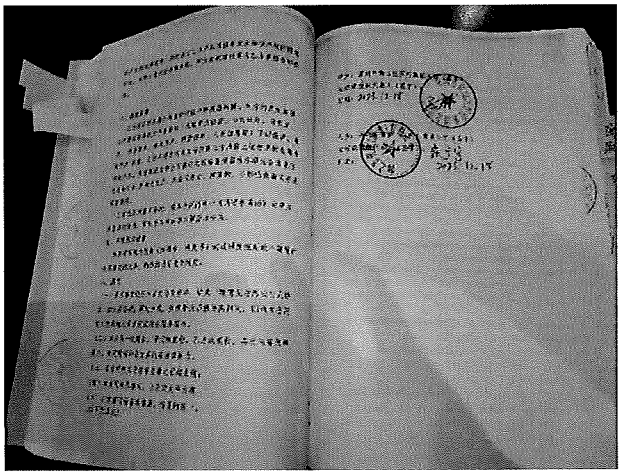
评价等级：　☐ 优　☐ 良　☑ 中　☐ 差

政府采购项目合同履约抽检评价报告

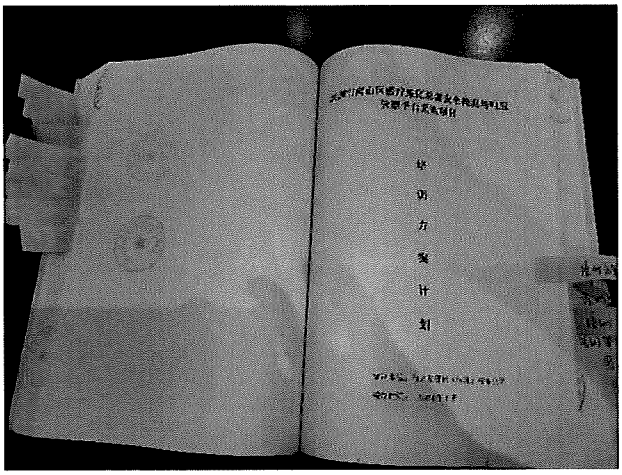
三、抽检照片



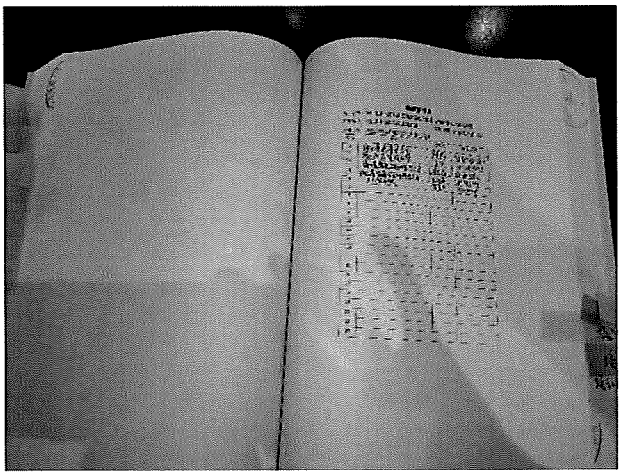
项目合同资料 1



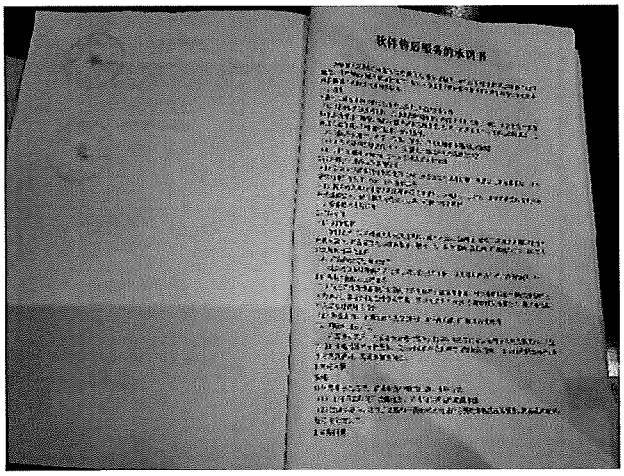
项目合同资料 2



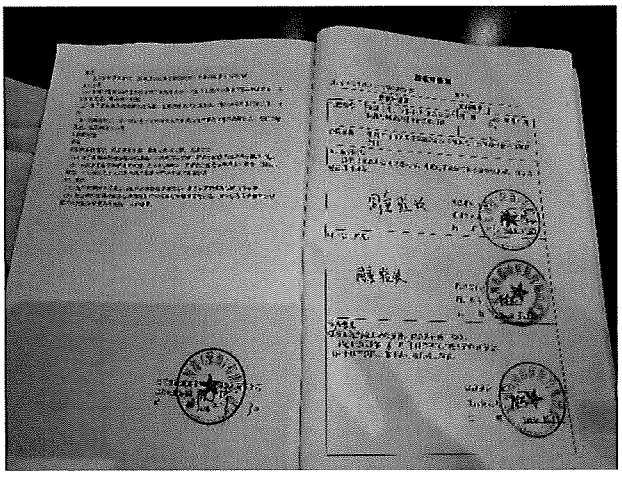
项目培训方案计划



项目培训签到表

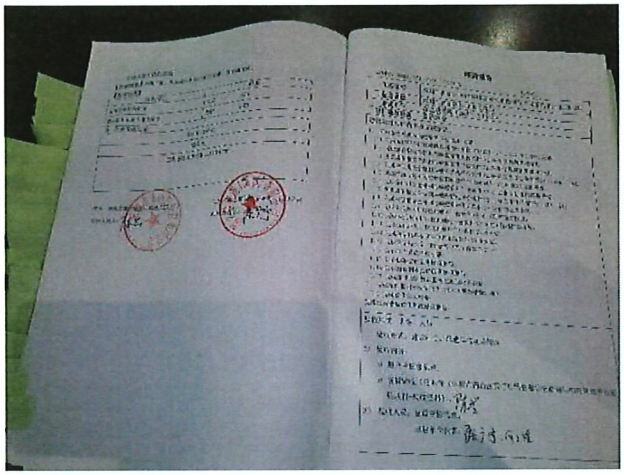


软件售后服务承诺书



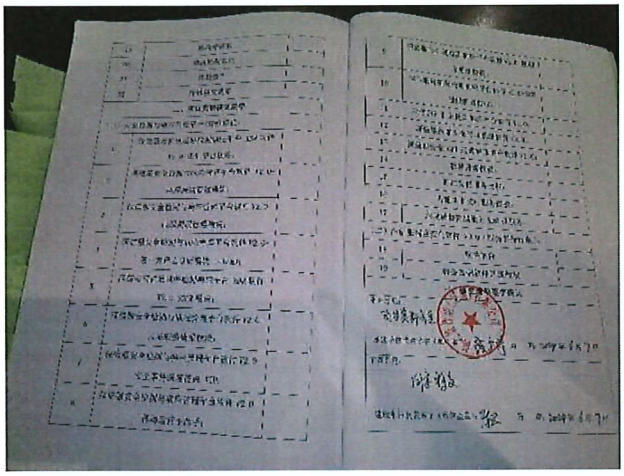
项目验收申请表

政府采购项目合同履约抽检评价报告

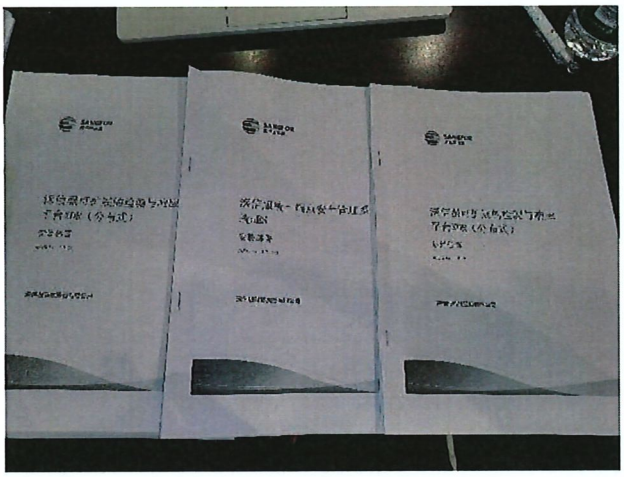


项目终验报告

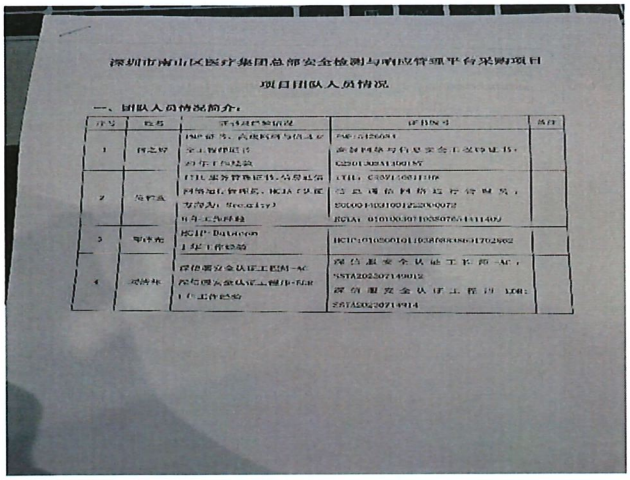
项目移交清单 1



项目移交清单 2



项目安装部署及运维管理文件

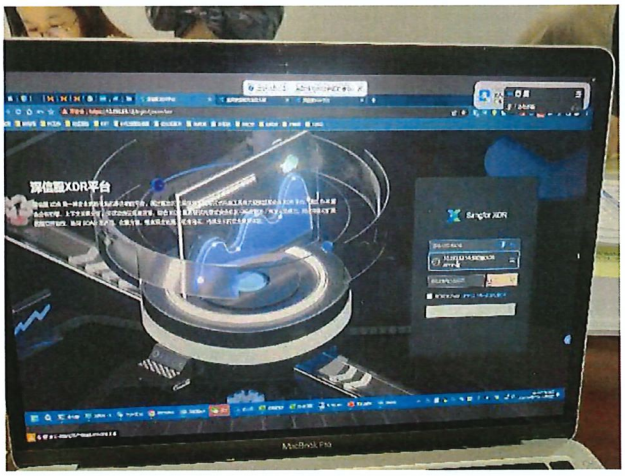


深圳市南山区医疗集团总部安全检测与响应管理平台采购项目

项目团队人员情况

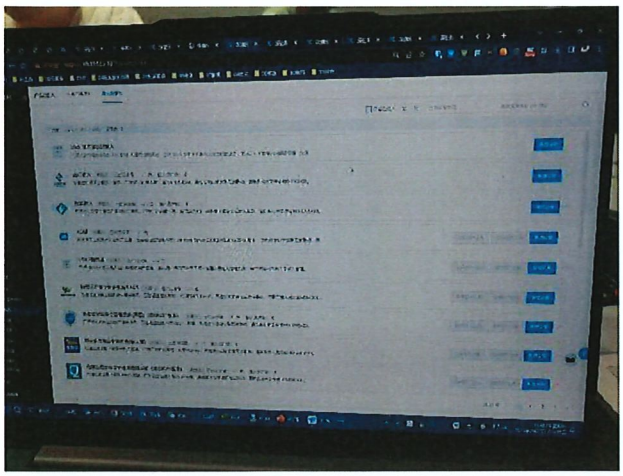
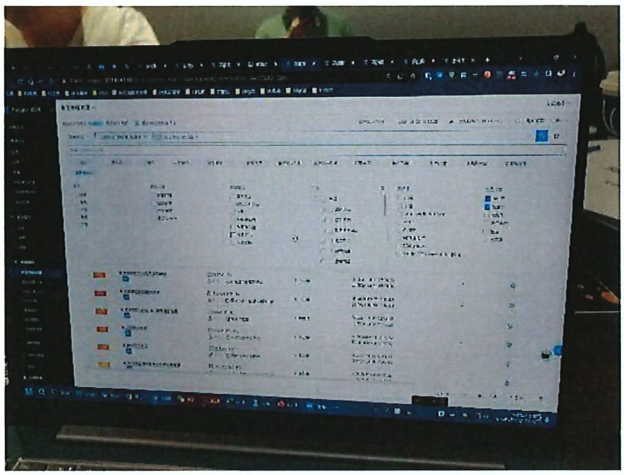
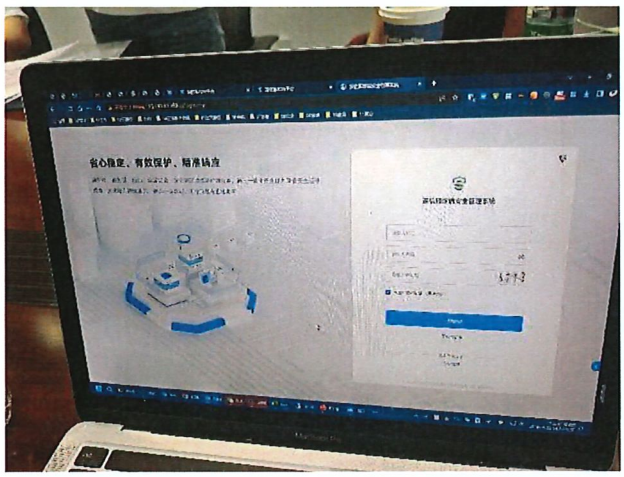
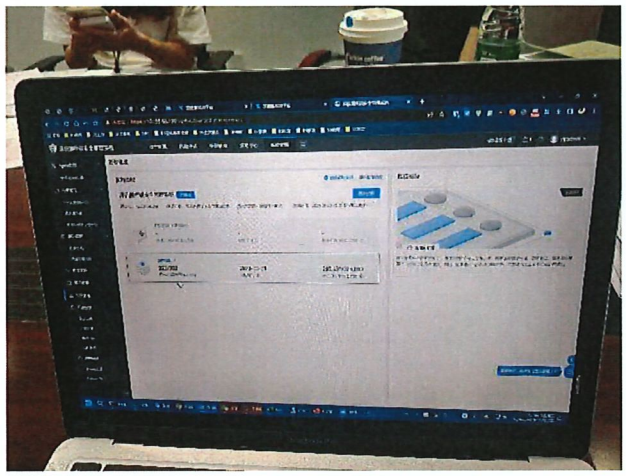
一、团队人员情况简介：

项目团队人员情况



安全检测与响应管理平台 XDR 界面 1

政府采购项目合同履约抽检评价报告

	
安全检测与响应管理平台 XDR 界面 2	安全检测与响应管理平台 XDR 界面 3
	
深信服终端安全管理系统界面 1	深信服终端安全管理系统界面 2

以 下 空 白