海油国际终端检测和响应（EDR）平台评审细则

标段编号：24-CNCCC-HW-GK-8058/01

评标方法：经评审的最低投标价法

序号	评审环节	评审因素	评审标准
1	供应商行为分析	硬件信息	对比各投标文件所使用的电脑硬件信息，看是否存在共用电脑的情况
2	供应商行为分析	标书相似度	检查各投标文件之间文本内容的相似度
3	供应商行为分析	标书文件信息检查	对标书文件作者的审查，作为判断围串标的依据之一
4	形式评审标准	★投标人名称	与营业执照一致
5	形式评审标准	★投标函签字盖章	有法定代表人或其委托代理人签字或加盖单位章。由法定代表人签字的，应附法定代表人身份证明，由代理人签字的，应附授权委托书，身份证明或授权委托书应符合第六章“投标文件格式”的规定
6	形式评审标准	★联合体投标人	不接受联合体投标
7	形式评审标准	★备选投标方案	不接受备选方案投标
8	形式评审标准	★分包	不接受分包
9	形式评审标准	★围标串标1	有下列情形之一的，属于投标人相互串通投标，并否决所有涉及的投标： a) 投标人之间协商投标报价等投标文件的实质性内容； b) 投标人之间约定中标人； c) 投标人之间约定部分投标人放弃投标或者中标； d) 属于同一集团、协会、商会等组织成员的投标人按照该组织要求协同投标； e) 投标人之间为谋取中标或者排斥特定投标人而采取的其他联合行动。
10	形式评审标准	★围标串标2	有以下情形之一的，视为投标人相互串通投标，并否决所有涉及的投标： a) 不同投标人的投标文件由同一单位或者个人编制，且投标人不能合理说明的，例如：不同投标人在集团公司数字化供应链平台上记录的文件制作机器码、文件创建标识码和投标电脑的MAC地址内容任何一项一致的；不同投标人的投标文件作者名称（除Admin、经确认为系统自动生成的作者名称）异常一致，且投标人不能合

序号	评审环节	评审因素	评审标准
			理说明的； b) 不同投标人委托同一单位或者个人办理投标事宜：例如：不同投标人在集团公司数字化供应链平台上的电子投标文件记录的投标文件上传IP地址异常一致且不属于中国海油网络IP范围，且投标人不能合理说明的。 c) 不同投标人的投标文件载明的项目管理成员为同一人，且投标人不能合理说明的。 d) 不同投标人的投标文件异常一致或者存在2处以上一致性错误；或者投 标报价呈规律性差异的项数达到报价清单的50%以上，且投标人不能合理说明的。 e) 不同投标人的投标文件相互混装，且投标人不能合理说明的。 f) 不同投标人的投标保证金从同一单位或者个人的账户转出，且投标人不能合理说明的。
11	形式评审标准	★投标保证金	符合第二章“ 投标人须知 ”第 3.4.1 项规定
12	形式评审标准	★投标有效期	投标截止之日起120天内保持有效。
13	形式评审标准	★投标承诺书	投标人应按附件格式提供《投标承诺书》，如未提供，将导致投标被否决。
14	资格评审标准	★投标主体	满足招标公告资格要求中的投标主体要求
15	资格评审标准	★财务要求	满足招标公告资格要求中的财务要求
16	资格评审标准	★业绩要求	满足招标公告资格要求中的业绩要求
17	资格评审标准	★其他要求	满足招标公告资格要求中的其他要求
18	资格评审标准	★不存在禁止投标的情形	不存在第二章“ 投标人须知 ”第 1.4.3 项规定的任何一种情形
19	响应性评审标准	★部署、运行和响应服务要求1	1.系统服务端应采取本地化部署，系统部署实施后应提供36个月系统服务端的产品更新、规则库更新、硬件维护和巡检等维保工作，巡检次数不应少于4次并解决巡检过程中发现的软件、硬件问题。 2.系统服务端应采用硬件化部署，应提供采用国产芯片的信创化设备。 3.系统服务端应采用B/S架构，应兼容Chrome内核、IE内核，适配内核版本为108核的浏览器，管理员只需浏览器访问管理平台即可进行操作。 4.应支持在一个管理平台内同时管理Windows操作系统、信创操作系统办公电脑的客户端。 5.产品管理端支持中英双语自由切换。

序号	评审环节	评审因素	评审标准
			6.支持实现双因素认证登录方式（原则上应支持与基于竹云产品的统一身份认证平台进行集成）。
20	响应性评审标准	★部署、运行和响应服务要求2	1.系统部署实施后应提供36个月1000个系统客户端授权续约、客户端产品更新、规则库更新、日常巡检等其他产品维保服务，每年巡检次数不应少于4次并解决巡检过程中发现的软件问题。完成部署实施后应提供告警监测、事件分析、反查溯源、现场应急响应及处置支持、安全策略调优等安全运营服务。 2.系统客户端应支持部署在麒麟V10（含 SP1 22H2及其他版本）和Windows操作系统的办公电脑上，客户端除了支持本地安装部署的方式外应支持通过终端安全管理软件或其他方式进行后台推送安装。 3.客户端应支持中英双语自由切换。
21	响应性评审标准	部署方式	系统客户端支持静默安装包、开启静默运行模式。
22	响应性评审标准	功能1	支持根据分组、IP地址、MAC地址、通信IP地址、接入点、客户端类型、操作系统等条件的组合筛选出符合条件的终端进行管理，自由对终端进行转移分组、删除终端、释放授权。
23	响应性评审标准	功能2	提供灵活的开放接口，支持将系统数据接入第三方平台进行统一监测、分析，支持与其他威胁监测类设备进行联动处置。
24	响应性评审标准	情报共享	具备获取专业的IOC（Indicator of Compromise）威胁情报能力，支持在中国海油内网环境下将最新病毒库、补丁库、威胁情报（文件哈希值、行为、域名、网络连接等特征）更新至系统服务端，识别定位风险，并提供详细威胁分析结果。
25	响应性评审标准	数据采集1	支持采集终端全量行为记录和日志数据，发现异常实时告警，支持对采集的行为记录和日志数据进行筛选、检索和导出。
26	响应性评审标准	数据采集2	支持搜索定位特定行为、日志条件的终端。
27	响应性评审标准	数据采集3	支持数据采集例外设置，实现在终端对进程路径、进程名、数字签名、IP、域名添加过滤。
28	响应性评审标准	数据采集4	采集的终端全量行为和日志数据包括但不限于：IP访问、DNS访问、进程注入、注册表变更、文件操作、账户变更、下载文件检测、U盘文件传输、IM文件传输、PowerShell命令执行、命名管道事件、进程权限信息、WMI事件、驱动文件加载、映像文件加载、无文件脚本执行、内网横向渗透、内存执行事件、账户登录登出等多种行为。上述19种功能须通过功能截图证明可实现相关功能。
29	响应性评审标准	威胁检测1	应实现基于ATT&CK框架分析检测威胁事件的全过程，评估攻击所处阶段和影响，支持对采集的行为和日志按照ATT&CK进行告警统计、分析、筛选、检索、导出。
30	响应性评审标准	威胁检测2	支持基于威胁情报提供的特征在全网终端发起搜索，快速定位出全网终端感染情况，支持常态化检测。

序号	评审环节	评审因素	评审标准
31	响应性评审标准	威胁检测3	支持自定义IOC（Indicator of Compromise）、IOA（Indicator of Attack）规则库，匹配规则进行自动化告警。
32	响应性评审标准	威胁检测4	支持图形化展示威胁事件中文件、进程的调用过程，可直观看出攻击入口、相关操作行为、高危实体文件等信息，提供研判、溯源支持。
33	响应性评审标准	威胁响应1	系统客户端支持对恶意域名、恶意进程、恶意软件进行自动阻断。包括但不限于：用户点击钓鱼恶意链接、访问恶意外链、运行恶意附件、安装了含恶意软件的盗版软件时，对访问、进程、软件进行自动阻断。
34	响应性评审标准	威胁响应2	支持通过服务端对终端进行断网操作，只允许与服务端进行通讯。
35	响应性评审标准	威胁响应3	支持对办公终端的高危端口按照自定义规则进行封禁。
36	响应性评审标准	威胁响应4	应支持按照告警名称、严重级别、攻击手法、攻击阶段、攻击主体等配置自动化响应策略，可在这些攻击和告警发生时自动出发响应动作。
37	响应性评审标准	威胁响应5	支持对确认为误报的告警进行加白，自定义加白规则，加白后不会再产生告警。
38	响应性评审标准	项目实施、运营人员要求1	项目应设置1名专职项目经理，应同时具备以下条件： 1、须提供由投标人出具的社保纳税证明（投标文件递交截止时间前连续6个月由投标人缴纳的社保记录）、个人简历及人力资源和社会保障部颁发的高级信息系统项目管理师证书或PMP证书扫描件。 2、该项目经理近5年来须至少完成1个以上（含1个）终端EDR（含EDR或终端安全）类项目，需提供人员简历，未提供将不予认可。
39	响应性评审标准	项目实施、运营人员要求2	项目实施工程师，应同时具备以下条件： 1、须提供由投标人出具的社保纳税证明（投标文件递交截止时间前连续6个月由投标人缴纳的社保记录）、个人简历及CISP证书扫描件。 2、该实施工程师近5年来须至少完成1个以上（含1个）终端EDR（含EDR或终端安全）类项目，需提供个人简历，未提供将不予认可。
40	响应性评审标准	项目实施、运营人员要求3	安全运营工程师，应同时具备以下条件： 1、须提供由投标人出具的社保纳税证明（投标文件递交截止时间前连续6个月由投标人缴纳的社保记录）、个人简历及CISP证书扫描件。 2、该安全运营工程师近5年来须至少完成1个以上（含1个）终端EDR（含EDR或终端安全）类项目中的安全运营工作，需提供个人简历，未提供将不予认可。
41	响应性评审标准	★响应性评审偏离要求	对响应性评审一般指标的非实质性偏离条款数量不超过3项。

序号	评审环节	评审因素	评审标准
42	响应性评审标准	★商务合同偏离要求	对招标文件商务及合同的非实质性偏离条款数量不超过4项。注：标准合同格式按二级条款记为一项偏离，如：第一条、第十三条。投标人须将偏离项逐条填写在偏离表中，如未明确应答偏离条数的，视为完全接受招标文件及合同条款，未在偏离表中体现的偏离在合同签订阶段不予考虑。
43	响应性评审标准	★其他	不存在国家法规和招标文件明确否决投标的其它条款和要求
44	投标报价评审	是否需要评分：不需要 是否多轮报价：否 评标价计算规则：评标价=算数修正投标报价+偏离调整	
45	投标报价评审	是否需要评分：不需要 是否多轮报价：否 评标价计算规则：评标价=算数修正投标报价	