

恒丰银行威胁情报管理平台采购项目 POC 测试供应商征集公告

(招标编号：/)

项目所在地区：山东省

一、招标条件

本恒丰银行威胁情报管理平台采购项目 POC 测试供应商征集已由项目审批/核准/备案机关批准，项目资金来源为其他资金/，招标人为恒丰银行股份有限公司。本项目已具备招标条件，现招标方式为其它方式。

二、项目概况和招标范围

规模：/

范围：本招标项目划分为 1 个标段，本次招标为其中的：

(001)恒丰银行威胁情报管理平台采购项目 POC 测试供应商征集；

三、投标人资格要求

(001 恒丰银行威胁情报管理平台采购项目 POC 测试供应商征集)的投标人资格能力要求：1、供应商须在中国境内注册，具有独立法人资格，持有合法的营业执照。

2、供应商须为所投产品原厂商或代理商。若供应商为代理商，则必须提供所投产品原厂商针对本项目的唯一授权书原件。

3、供应商所投产品须具有公安部计算机信息系统安全专用产品销售许可证。

4、本项目不允许联合体 POC 测试；

本项目不允许联合体投标。

四、招标文件的获取

获取时间：从 2024 年 03 月 21 日 08 时 30 分到 2024 年 03 月 27 日 17 时 00 分

获取方式：网上报名：有意参加本次测试的供应商将报名信息 word 版（项目名称、供应商名称、联系人姓名、联系人手机号、联系人邮箱）及供应商资格要求的资料扫描件发送至 cnshzb@163.com，邮件名称命名为恒丰银行威胁情报管理平台采购项目 POC 测试供应商征集报名-“供应商单位名称”。报名电话：18396818930，15053100509；联系人：张经理，袁经理。测试地点：线上。本次 POC 测试统一要求供应商通过互联网服务形式提供系统测试环境资源、测试账号等，我行内部不再本地化部署供应商软硬件资源。供应商技术支持人员按我行测试人员需要提供必要的远程或现场支持服务。联系人：姚钧译；电话：18829050425



五、投标文件的递交

递交截止时间：2024年03月27日17时00分

递交方式：本项目为征集公告/

六、开标时间及地点

开标时间：2024年03月27日17时00分

开标地点：本项目为征集公告

七、其他

一、采购人：恒丰银行股份有限公司 地址：山东省济南市历下区泺源大街8号

联系方式：0531-59667170；

采购代理机构：盛和招标代理有限公司 地址：山东济南历城区唐冶西路东八区企业公馆B1号楼

联系方式：张经理，18396818930；袁经理，15053100509；

二、采购项目名称：恒丰银行威胁情报管理平台采购项目

采购项目编号： /

标包：1

采购内容：威胁情报管理平台

数量：1宗

供应商资格要求：

- 1、供应商须在中国境内注册，具有独立法人资格，持有合法的营业执照。
- 2、供应商须为所投产品原厂商或代理商。若供应商为代理商，则必须提供所投产品原厂商针对本项目的唯一授权书原件。
- 3、供应商所投产品须具有公安部计算机信息系统安全专用产品销售许可证。
- 4、本项目不允许联合体POC测试。

三、项目背景、测试范围及技术要求

银行保险机构应当建立互联网网络安全漏洞、重大网络安全威胁动态监测机制，加强外部威胁情报共享和服务合作，强化落实金融监管总局建立的网络安全风险通报机制。

本项目拟采购一台/套威胁情报管理平台设备/平台，引入全球领先的威胁情报数据，建立起一套集外部情报共享、内部情报提供、内外联防联控的本地威胁情报管理中心，提高包括安全设备、安全运营人员在内的整体安全运营体系的威胁检测分析、响应处置能力，并挖掘生

代
(2
子
—

产符合我行业务特点的威胁情报。通过实时的威胁情报交付，提升 0Day、未知攻击的发现能力，第一时间阻断攻击，变被动防御为主动对抗，主动进行外部威胁攻击分析、狩猎，沉淀威胁知识库，强化主动防御能力。

恒丰银行威胁情报管理平台采购项目。我行主要针对以下功能指标进行测试评估：

（1）情报来源及质量

情报库中的威胁情报数据来源（如公安部、国有银行、金融机构、运营商等机构）及质量（误报率）。

（2）情报种类

威胁情报数据种类（是否包括如远控、恶意软件、钓鱼邮件、傀儡机、扫描、IDS 服务器、动态 IP、代理、CDN、网关等）。

（3）情报数量规模

商用机读情报（包括商用 IP 信誉、失陷指标（IOC））数量级别，情报库中各类型情报（如 IDC 主机、傀儡机、网关 IP 等）数量级别；是否支持批量 IP 信誉检测。

（4）溯源分析能力

对常见威胁（如挖矿、勒索、蠕虫、钓鱼链接类等）的追踪溯源分析能力，包括：

IP 情报有效字段（如威胁类型、相关攻击团伙信息、安全与否判定、可信度级别、严重级别、情报来源、端口、RDNS 记录、ASN 信息、SSL 指纹、地理位置、经纬度、运营商信息、当前和历史 pDNS 等）。

域名情报有效字段（如威胁类型、相关攻击团伙信息、安全与否判定、可信度级别、严重级别、情报来源、SSL 指纹、域名 Alexa 排名、Umbrella 排名、当前和历史指向 IP 数据、当前和历史 whois 数据、子域名等）。

（5）失陷检测

失陷检测能力（如能否提供佐证域名失陷的上下文文本、佐证失陷的取证样本名称、取证样本文件类型、恶意家族、恶意类型、检测标签、威胁等级、相关域名、处置建议等），是否支持批量失陷检测。

（6）联动能力

与 IPS、WAF、SOC 等其他网络安全设备的联动处置能力。

四、议程安排：

1. 报名参与时间：自 2024 年 3 月 21 日起至 2024 年 3 月 27 日止，上午 8:30—11:30，下午 14:00—17:00（北京时间，法定公休日、法定节假日除外）

一
有
用

2. 报名方式：网上报名：有意参加本次测试的供应商将报名信息 word 版（项目名称、供应商名称、联系人姓名、联系人手机号、联系人邮箱）及供应商资格要求的资料扫描件发送至 cnszhb@163.com，邮件名称命名为恒丰银行威胁情报管理平台采购项目 POC 测试供应商征集报名-“供应商单位名称”。

3. 报名电话：18396818930，15053100509；联系人：张经理，袁经理。

4. 测试地点及联系人：

测试地点：线上。本次 POC 测试统一要求供应商通过互联网服务形式提供系统测试环境资源、测试账号等，我行内部不再本地化部署供应商软硬件资源。供应商技术支持人员按我行测试人员需要提供必要的远程或现场支持服务。

联系人：姚钧译；电话：18829050425

五、有关说明：

1. 采购人不统一组织供应商对现场进行勘察。无论供应商对现场考察与否，都将被视为熟悉履行合同有关的一切情况，并承担一切与磋商有关的风险、责任和义务，勘察现场所发生的一切费用由供应商自行承担。

发 布 人：盛和招标代理有限公司

发布时间：2024 年 3 月 20 日

八、监督部门

本招标项目的监督部门为恒丰银行股份有限公司。

九、联系方式

招 标 人：恒丰银行股份有限公司

地 址：/

联 系 人：丛经理

电 话：0531-59667170

电子邮件：/

招标代理机构：盛和招标代理有限公司

地 址：山东省济南市历城区唐冶西路东八区企业公馆 B1 楼

联 系 人：张明昊、袁家莹

电 话：18396818930

一
展
章

电子邮件: cnszb@163.com

招标人或其招标代理机构主要负责人(项目负责人): 袁家宝 (签名)

招标人或其招标代理机构:



7/11