在线询价文件

 项目名称：网络欺骗防御系统项目

 采购人：台州科技职业学院

2024年4月

**一、项目概况**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **项目名称** | **单位** | **数量** | **预算金额** | **备注** |
| 1 | 网络欺骗防御系统 | 项 | 1 | 15万元 | 带▲号指标不满足需求或带★号指标超过5项不满足需求，均作为不响应招标处理。 |

1. **技术要求**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 模块 | 技术参数 | 单位 | 数量 |
| 网络欺骗防御系统 | 服务器 | 2U 服务器机箱，服务器主板X11 SSL-F，E3 1230V5 CPU， 16G ECC内存，1T\*2硬盘(支持RAID)，双电冗余电源，2个千兆网口。 | 套 | 1 |
| 威胁溯源反制平台 | 威胁溯源反制平台以多维度方式进行统计展示。★（1）黑客溯源以攻击源的维度进行归类，通过对攻击源进行深度分析整合，将攻击者定性为：真人、扫描工具、未知三大类。针对攻击源可分析其攻击轨迹及身份信息。对真人攻击者支持全方位溯源，包括IP、地理位置、网络ID、操作系统类型等。（2）黑客反制以设备的维度进行归类，获取PC设备的设备精确信息、黑客IP、敏感信息等，并且具备反向控制攻击者主机的能力。★（3）攻击事件以攻击者对沙箱发起的所有攻击行为为维度进行归并展示。通过事件分析可了解攻击者对沙箱发起的一系列攻击行为，运用的攻击手法，以及攻击事件的起止时间和严重程度。（4）行为分析以时间线的方式，展示最近出现的攻击行为，通过查看攻击行为上下文，可深度分析攻击事件之间的关联关系以及攻击者的攻击意图。★（5）钓鱼邮件检测有效的保护企业员工邮箱安全及攻击回溯；获取攻击者IP、对恶意文件进行识别，为企业提供多重防护。 |
| 云蜜网欺骗防御平台 | （1）蜜网管理是核心，包括沙箱管理、中继节点、伪装代理、VPN欺骗、攻击诱捕、诱饵欺骗及智能蜜网。以沙箱为基础，中继节点和伪装代理向外辐射扩大覆盖面，欺骗诱饵散布在各个区域与沙箱信息相关联，形成蜜网拓扑。（2）沙箱模拟服务和业务，包含20余种应用服务、14种系统服务、3种windows服务、10余种工控服务以及自定义模板。沙箱可以关联多个IP，中继节点和伪装代理通过流量转发的方式，将沙箱服务发布到需要覆盖的各个区域。 ★（3）工控安全形势日益严峻，沙箱技术被越来越多的应用在工控领域，也针对modbus、s7、IEC-104、IPMI等工控协议进行模拟；可以模拟真实的工控现场环境，通过部署协议仿真蜜罐伪装工业现场PLC设备，部署组态软件仿真蜜罐伪装上位机系统，二者产生交互模拟真实业务场景，攻击者掉入蜜罐陷阱后，可以迷惑攻击者，达到起到保护真实环境甚至是溯源反制的能力。 |
| 实验内容 | ★以Kill Chain为参考模型，以ATT&CK为技术补充，对应攻击者采取攻击的每一个步骤，通过沙箱业务仿真、漏洞伪装、虚拟系统、脱敏虚假数据、行为记录，学习如何构建入侵攻击链。 |
| ★具备多种捕获入侵者虚拟身份的技术，精准定位，多维度聚合，通过还原攻击过程，溯源追踪攻击者身份，形成黑客画像，学习如何从根源上找到威胁。 |
| ★学习构建沙箱时可以针对现有的模板、自定义等web类、系统服务类沙箱进行随意组合，通过多样化、不同场景下的欺骗思路理论上可以有无限种可能。通过不同的服务、不同的页面、不同场景下的多种服务排列组合可以有效应对攻击者将某沙箱定义为某厂家或是蜜罐的情况 |
| 学习II型虚拟化技术架构，II型虚拟化的Hypervisor(KVM)架构保证资源隔离，虚拟机运行在传统操作系统上，创建的是硬件全仿真实例，被称为“托管（宿主）”型。托管型/主机型Hypervisor运行在基础操作系统上，构建出一整套虚拟硬件平台（CPU/Memory/Storage/Adapter），使用者根据需要安装新的操作系统和应用软件，底层和上层的操作系统可以完全无关化。 |
| ★学习攻击反制，涵盖十余种反向控制手段，如连接MysqlCheat沙箱的攻击者，可反向获取其敏感信息；从mailbox沙箱拖走备份文件的攻击者，可秘密植入反制程序；攻击者从web沙箱下载的伪装控件，捆绑了的反制程序。一旦运行，便可获取攻击者的设备上敏感信息，例如操作系统版本、IP信息、历史登陆的社交账号等，高级反制可反向控制对攻击者的设备 |
| 场景部署 | （1）互联网侧，可部署于DMZ区或互联网出口位置，开启web应用类沙箱或者制作自定义高仿真的沙箱，通过网络设备将沙箱的仿真服务发布至互联网，也可通过负载均衡设备将一些敏感的目录重定向至沙箱，还可以通过与流量设备联动，进行虚拟网站欺骗和公网IP欺骗。（2）内网侧，可部署于安全管理域或测试生产区。开启系统服务类沙箱、windows沙箱以及内网仿真业务沙箱，通过伪装代理覆盖当前网络下已存在的主机，通过中继节点覆盖各个Vlan下空闲的IP，最后辅以主机诱饵覆盖Linux端主机信息混淆，办公网诱饵做windows端的攻击欺骗。（3）在工控场景中，可部署于网络关键节点或者工业企业网络的出口处，合理启用工控沙箱和服务协议，通过中继节点将生产控制大区的空闲IP，利用网络中的空闲IP绑定工控沙箱服务，将攻击流量诱导至部署的工控沙箱中。 |

**三、商务需求**

**1.投标要求**

▲（1）中标人在中标后24小时内提供招标文件内所要求的证明材料电子版本，资料原件备查，如不提供按虚假响应处理，取消预中标资格。

（2）中标人在中标后15个工作日内需进行软件测试，并进行所承诺的所有功能测试，提供测试报告，如经测试发现与标书要求或投标文件不一致，则视为欺诈行为，招标人将不授予合同，投标单位将承担一切后果与责任。

▲（3）投标人在投标时需承诺中标后10日内提供设备原厂商针对本项目的授权函和三年售后（质保）服务承诺函。

（4）产品原厂商需具备国家信息安全测评信息安全服务资质证书（安全工程类一级）。

（5）产品原厂商需中国网络安全审查技术与认证中心信息安全服务资质（信息系统安全集成服务三级）。

（6）产品原厂商需具备国家信息安全测评信息安全服务资质证书（风险评估一级）。

（7）产品原厂商需具备软件能力成熟度模型CMMI 3及以上认证。

注：其中（4）至（7）需至少满足2项，并提供证明材料。

**2.质量保证和售后服务**

（1）提供3年免费升级维护。

（2）提供7\*24小时技术支持热线。

（3）提供安装调试后1天本地操作培训。

（4）本地应急响应时间≤2小时。

（5）产品原厂商项目经理须同时具备以下5个认证中至少2项：①项目管理专业人士资格认证（PMP）、②注册信息安全专业人员认证（CISP）、③信息安全保障人员认证（CISAW(安全集成专业级））、④信息安全保障人员认证（CISAW(安全运维专业级））、⑤信息安全管理体系认证（ISO27001 Foundation）。（提供相关证书复印件及近三个月内浙江省社保证明）。

**3.付款方式**

甲方在合同签订后10个工作日内支付合同金额的40%，安装调试完毕，项目验收合格并收到发票后10个工作日内支付合同金额的60%。

**4.交货时间及地点**

（1）交货时间：合同签订后10天内交货并安装、调试完毕；

（2）交货地点：台州市黄岩区嘉木路288号；

（3）收货联系人：李老师，15057628610。

**四、其他事项**

1.一家供应商只能报价一种品牌，否则作无效标处理；若投标供应商用不满足参数产品恶意投标，影响采购人采购进程的，采购人有进一步追究其责任的权利。

2.招标方根据需要在中标金额范围内提前通知可调整货物配置的，供应商应当配合完成。供应商备货、供货前应当提供细化的供货安装方案，方案须征得招标方同意后方可进场施工，擅自施工造成的后果由供应商承担。

3.投标供应商应当**在询价时附上响应文件。**（请按以下附件格式填写，加盖投标单位公章后扫描制作成PDF格式文件，上传到政采云平台，文件要求：清析、明确；网上自动成交后，需双方根据询价文件确认达成一致结果才为正式成交。

**附件：**

**在线询价响应文件**

**项目名称：**

 **项目编号：**

**投标人名称：（盖章）**

**投标人授权代表：**

**授权代表联系方式：**

**投标人地址：**

  **年 月 日**

**目 录**

1、授权委托书

2、法人或者其他组织的营业执照等证明文件、自然人身份证明

3、技术响应需求表

4、报 价 明 细 表

5、相关检测报告

**附件1：**

**授权委托书**

台州科技职业学院：

（投标人全称） 法定代表人（或营业执照中单位负责人） （法定代表人或营业执照中单位负责人姓名） 授权 （全权代表姓名） 为全权代表，参加贵单位组织的 项目的采购活动，并代表我方全权办理针对上述项目的投标、开标、评标、签约等具体事务和签署相关文件。我方对全权代表的签字事项负全部责任。

在撤销授权的书面通知以前，本授权书一直有效。全权代表在授权委托书有效期内签署的所有文件不因授权的撤销而失效。

全权代表无转委托权，特此委托。

法定代表人签字或盖章：

投标人全称（公章）： 日期：

**附：**

|  |
| --- |
| **法定代表身份证复印件粘帖处** |

法定代表人姓名：

传真：

电话：

详细通讯地址：

邮政编码：

|  |
| --- |
| **全权代表身份证复印件粘帖处** |

全权代表姓名：

职务：

传真：

电话：

详细通讯地址：

邮政编码：

**附件2：**

**技术需求响应表**

项目名称：网络欺骗防御系统项目

品牌： 型号：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 名称 | 规格型号 | 技术参数 | 投标参数 | 偏离说明 |
| 1 | 网络欺骗防御系统 | 服务器 | 2U 服务器机箱，服务器主板X11 SSL-F，E3 1230V5 CPU， 16G ECC内存，1T\*2硬盘(支持RAID)，双电冗余电源，2个千兆网口。 |  |  |
| 威胁溯源反制平台 | 威胁溯源反制平台以多维度方式进行统计展示。★（1）黑客溯源以攻击源的维度进行归类，通过对攻击源进行深度分析整合，将攻击者定性为：真人、扫描工具、未知三大类。针对攻击源可分析其攻击轨迹及身份信息。对真人攻击者支持全方位溯源，包括IP、地理位置、网络ID、操作系统类型等。（2）黑客反制以设备的维度进行归类，获取PC设备的设备精确信息、黑客IP、敏感信息等，并且具备反向控制攻击者主机的能力。★（3）攻击事件以攻击者对沙箱发起的所有攻击行为为维度进行归并展示。通过事件分析可了解攻击者对沙箱发起的一系列攻击行为，运用的攻击手法，以及攻击事件的起止时间和严重程度。（4）行为分析以时间线的方式，展示最近出现的攻击行为，通过查看攻击行为上下文，可深度分析攻击事件之间的关联关系以及攻击者的攻击意图。★（5）钓鱼邮件检测有效的保护企业员工邮箱安全及攻击回溯；获取攻击者IP、对恶意文件进行识别，为企业提供多重防护。 |  |  |
| 云蜜网欺骗防御平台 | （1）蜜网管理是核心，包括沙箱管理、中继节点、伪装代理、VPN欺骗、攻击诱捕、诱饵欺骗及智能蜜网。以沙箱为基础，中继节点和伪装代理向外辐射扩大覆盖面，欺骗诱饵散布在各个区域与沙箱信息相关联，形成蜜网拓扑。（2）沙箱模拟服务和业务，包含20余种应用服务、14种系统服务、3种windows服务、10余种工控服务以及自定义模板。沙箱可以关联多个IP，中继节点和伪装代理通过流量转发的方式，将沙箱服务发布到需要覆盖的各个区域。★（3）工控安全形势日益严峻，沙箱技术被越来越多的应用在工控领域，也针对modbus、s7、IEC-104、IPMI等工控协议进行模拟；可以模拟真实的工控现场环境，通过部署协议仿真蜜罐伪装工业现场PLC设备，部署组态软件仿真蜜罐伪装上位机系统，二者产生交互模拟真实业务场景，攻击者掉入蜜罐陷阱后，可以迷惑攻击者，达到起到保护真实环境甚至是溯源反制的能力。 |  |  |
| 实验内容 | ★以Kill Chain为参考模型，以ATT&CK为技术补充，对应攻击者采取攻击的每一个步骤，通过沙箱业务仿真、漏洞伪装、虚拟系统、脱敏虚假数据、行为记录，学习如何构建入侵攻击链。 |  |  |
| ★具备多种捕获入侵者虚拟身份的技术，精准定位，多维度聚合，通过还原攻击过程，溯源追踪攻击者身份，形成黑客画像，学习如何从根源上找到威胁。 |  |  |
| ★学习构建沙箱时可以针对现有的模板、自定义等web类、系统服务类沙箱进行随意组合，通过多样化、不同场景下的欺骗思路理论上可以有无限种可能。通过不同的服务、不同的页面、不同场景下的多种服务排列组合可以有效应对攻击者将某沙箱定义为某厂家或是蜜罐的情况 |  |  |
| 学习II型虚拟化技术架构，II型虚拟化的Hypervisor(KVM)架构保证资源隔离，虚拟机运行在传统操作系统上，创建的是硬件全仿真实例，被称为“托管（宿主）”型。托管型/主机型Hypervisor运行在基础操作系统上，构建出一整套虚拟硬件平台（CPU/Memory/Storage/Adapter），使用者根据需要安装新的操作系统和应用软件，底层和上层的操作系统可以完全无关化。 |  |  |
| ★学习攻击反制，涵盖十余种反向控制手段，如连接MysqlCheat沙箱的攻击者，可反向获取其敏感信息；从mailbox沙箱拖走备份文件的攻击者，可秘密植入反制程序；攻击者从web沙箱下载的伪装控件，捆绑了的反制程序。一旦运行，便可获取攻击者的设备上敏感信息，例如操作系统版本、IP信息、历史登陆的社交账号等，高级反制可反向控制对攻击者的设备 |  |  |
| 场景部署 | （1）互联网侧，可部署于DMZ区或互联网出口位置，开启web应用类沙箱或者制作自定义高仿真的沙箱，通过网络设备将沙箱的仿真服务发布至互联网，也可通过负载均衡设备将一些敏感的目录重定向至沙箱，还可以通过与流量设备联动，进行虚拟网站欺骗和公网IP欺骗。（2）内网侧，可部署于安全管理域或测试生产区。开启系统服务类沙箱、windows沙箱以及内网仿真业务沙箱，通过伪装代理覆盖当前网络下已存在的主机，通过中继节点覆盖各个Vlan下空闲的IP，最后辅以主机诱饵覆盖Linux端主机信息混淆，办公网诱饵做windows端的攻击欺骗。（3）在工控场景中，可部署于网络关键节点或者工业企业网络的出口处，合理启用工控沙箱和服务协议，通过中继节点将生产控制大区的空闲IP，利用网络中的空闲IP绑定工控沙箱服务，将攻击流量诱导至部署的工控沙箱中。 |  |  |

**要求：**

1.本表参照本招标文件“技术要求”填制，投标人应根据投标设备的性能指标、服务指标，对照招标文件要求在“偏离情况”栏注明“正偏离”、“负偏离”或“无偏离”。

2.对于投标产品的技术偏离情况需严格按照招标文件的技术要求一一比对给出，未达到技术要求中规定的数值应以负偏离标注。若因技术实现方式等其他问题而导致的理解不同未标注负偏离的，需在备注中具体说明；若未按要求标注负偏离又未予以说明的，评审小组将视偏离程度认定为虚假应标。

投标人名称（盖章）：

投标人代表签字或盖章：

联 系 电 话： 职 务：

日 期：

**附件3：**

**报 价 明 细 表**

 项目名称：网络欺骗防御系统项目 [货币单位：人民币元]

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **报价项目** | **品牌、产地** | **型号规格** | **数量** | **单价** | **小计** | **备注** |
| 1 | 网络欺骗防御系统 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **合计人民币：大写 小写** |

**要求：**

1. 本表为报价明细表，如有缺项、漏项，视为投标报价中已包含相关费用，采购人无需另外支付任何费用。

2.投标报价明细表所填内容按询价文件采购设备清单要求为准。如有漏报的，视同已包含在投标总价内或已作优惠处理。有重大缺项的将作无效标处理。

▲4. 本表中的型号规格必须明确，招标文件中明确要求定制的除外。

5. 所有设备（含进口和非进口）均采用人民币报价。

投标人名称（盖章）：

投标人代表签字或盖章：

职 务：

日 期：

**附件4：**

**CNAS认可的检测报告、证书复印件等**

**附件5:**

**售后服务情况表**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **服务项目** | **投标人情况** | **备注** |
| 1 | 提供3年免费升级维护 | 投标人服务情况： |  |
| 2 | 提供7\*24小时技术支持热线 |  |  |
| 3 | 提供安装调试后1天本地操作培训 |  |  |
| 4 | 本地应急响应时间≤2小时 |  |  |
| 5 | 产品原厂商项目经理须同时具备以下5个认证中至少2项：①项目管理专业人士资格认证（PMP）、②注册信息安全专业人员认证（CISP）、③信息安全保障人员认证（CISAW(安全集成专业级））、④信息安全保障人员认证（CISAW(安全运维专业级））、⑤信息安全管理体系认证（ISO27001 Foundation）。（提供相关证书复印件及近三个月内浙江省社保证明） |  |  |

供应商名称（盖章）：

供应商代表签字：

职 务：

日 期：