编号:

大型仪器设备购置可行性论证及审批报告

设 备 名 称 态势感知平台

申 请 单 位 信息中心

经 费 来 源 信息化经费

申请人（签名）

联 系 电 话 15858412040

项目负责人（签名）

填 写 日 期 2026 年 9 月 22 日

信息中心制

编号:

说　明

一、拟购置或自制单价 10 万元（含）以上的大型仪器设备，须先完成本报告中相关内容的填写，由科研管理部审核后，组织专家进行可行性论证。论证完成后，向科研管理部提交相关材料的纸质版和扫描件。

二、专家论证要求

（1）计划购置单价 10 万元（含）至 50 万元的设备时，由申请人所在单位邀请 3 位高级职称的专家组成专家小组，讨论形成论证意见。（论证前，须先向科研管理部报备拟定专家人员信息、论证时间和地点等，经同意后再进行论证）

（2）计划购置单价 50 万元(含)至 200 万元的设备时，由所在单位组织召开论证会，论证会须有 5 位高级职称的专家参加（至少 1 位校外专家，2 位非本院系的专家），形成会议纪要。（论证会前，须先向科研管理部报备拟定专家人员信息、论证会时间和地点等，经同意后再进行论证）

（3）计划购置单价 200 万元（含）以上的设备时，由科研管理部和申请单位共同召开论证会，论证会须由 5 位高级职称的专家（至少 2 位校外专家，2 位非本院系的专家）和 1 位科研管理部工作人员参加，形成会议纪要。（论证会前，由科研管理部确定专家人员信息、论证会时间和地点）

（4）论证专家组成员应为相关领域的专家，但不可以是拟购置仪器设备的负责人、申请人、操作人及校外可能的利益相关者。

三、阐述购置（自制）设备的理由及必要性，包括申请单位或研究项目的情况、拟购置大型仪器的目的（基于什么

需求或实现什么样的作用）和仪器的主要原理、功能及适用范围。

四、通过调研，记录中心是否已有和有已购未入库的同类型设备的情况。如有，须在特殊情况说明处写明在已有和有已购未入库的同类型设备的情况下仍要购置的原因。

五、打印要求：本报告封面单页打印，说明部分双面打印。

六、本报告审核完成后扫描件需上网公示一周无异议方为通过。

七、本报告由科研管理部（要求原件）、条件保障部（原件或复印件均可）、采购申请单位（原件或复印件均可）分别留存一份备查。

编号:

大型仪器设备购置可行性论证及审批报告

设备中文名称	态势感知平台		
设备外文名称	/		
申购数量	1	是否进口设备	否
是否为主件设备	是	是否含有附件	否

附件名称	数量	单价	备注

规格	态势感知平台长 430mm×宽 800mm×高 89mm		
估计单价（万元）	34	估计总价（万元）	34
估计外币（万元）	/	币种	/
主要技术指标	性能参数： 吞吐率：网络层≧5Gbps WEB 检测：HTTP 最大并发数≧9 万/秒 邮件检测：邮件处理数:≧ 180 万封/24 小时 文件检测：≧5 万个/24 小时 硬件参数： 软硬一体化 2U 标准机架式设备 CPU：Intel Core I7-7700/3.6GHz/4 核 8 线程； 内存：≧16G*4； 硬盘：≧2T*1； 电源模块形态：1+1 冗余电源； 额定功率：300W； 管理口：千兆电口*1； HA 口：千兆电口*1； 网卡：≧千兆电口*4、千兆光*4；		
主要功能	态势感知平台可实现全网 7×24 小时主动监测，精准发现挖矿病毒、远控木马等高危行为，闭环落实网安整改工作。		

编号:

应用范围	主动监测终端异常访问、非法外联、病毒隐患等网络安全问题。
共享学科	通用
申购理由和必要性	在试用期平台检出的代理工具、挖矿病毒、远控木马等告警与上级通报的“学生翻墙中毒”事件特征高度吻合，其中上线 1 分钟内 83 条告警覆盖“企图”到“失陷”的完整攻击过程。采购态势感知平台可补齐我校网络安全防护短板，主动防范各类网络风险，保障校园教学、办公等各项工作安全有序开展。

中心已有同类设备（_____）_____台，使用情况调研如下（不够可附页）：

所属单位	仪器编号	仪器名称	原值	领用人	年有效使用机时（小时/年）	是否开放
浙大宁波校区						
浙大宁波校区						
资产管理员（签字）						

已论证但尚未入库的同类设备（_____）_____台，调研如下（不够可加行，量大可附页）：

申请单位	仪器名称	数量	预算金额	负责人	审批日期

编号:

特殊情况说明：					
可供货厂商调研情况					
1.厂商名称	安恒信息	型号	明御 APT 攻击预警平台 DAS-APT-2000	售价（万元）	约 28~35（参考）
仪器性能	1. 产品形态：软硬一体化 2U 标准机架式设备，ALL IN ONE 一体化设计（流量采集、沙箱、威胁分析、数据存储、查询与设备管理于一体）； 2. 网络层吞吐率：5Gbps； 3. HTTP 最大并发数：9 万/秒； 4. 邮件处理能力：180 万封/24 小时； 5. 文件检测能力：5 万个/24 小时； 6. 检测机制：静态特征检测＋动态沙箱行为分析＋机器学习＋威胁情报多维关联分析，检测能力完整覆盖 APT 攻击链； 7. 攻击类型覆盖：680 余种，含 Web 攻击、邮件攻击、恶意文件、异常流量、失陷主机、横向扩散、挖矿、隐蔽信道、DGA 域名请求、0day 漏洞利用等； 8. 沙箱技术：融合“虎鲸”沙箱，业界首创“鲸吞”Windows 容器技术，单虚拟机多任务并行分析；具备沙箱快速恢复与防逃逸技术，支持自定义镜像导入； 9. 反病毒引擎：与国际领先反病毒引擎深度合作，病毒库与官方同步更新，采用启发式扫描技术支持变种检测； 10. 协议解析：对 2~7 层全流量审计，支持 HTTP、FTP、SMB、SMTP、POP3、IMAP、NFS、TFTP 等协议文件分离与检测； 11. 自定义检测：支持特征类、周期统计类自定义规则及 YARA 规则导入，支持细颗粒度白名单配置； 12. 部署方式：旁路镜像部署，无服务中断；支持集群部署与 IPv4/IPv6 双协议栈； 13. 联动能力：可与防火墙、WAF、EDR 等阻断类产品联动，在回连环节阻断异常行为； 14. 数据外发：可外发协议审计、风险告警、会话应用流量统计、传输层/应用层统计、文件检测等数据给态势感知/大数据平台； 15. 升级与运维：支持云端自动升级（含集群场景自动升级），具备便捷运维管理模块； 16. 硬件配置：CPU Intel Core i7-7700/3.6GHz/4 核 8 线程；内存 16G×4；硬盘 2T×1（可扩 3 块）；1+1 冗余电源； 17. 接口配置：管理口千兆电口×1、HA 口千兆电口×1；网卡千兆电口×4＋千				

	兆光口×4（标配千兆多模光模块×2），网卡可扩 3； 18. 额定功率：300W（1+1 冗余），实际运行功耗约 150~200W； 19. 仪器尺寸（长×宽×高）：435mm(宽)*550mm(深)*89mm(高)； 20. 仪器重量：约 20~25KG； 21. 对房间的承载要求：≥300kg/m²（约 3KN/m²），常规机房/机柜即可满足，无需特殊加固； 22. 是否与其它仪器共用：否，独立上架；可与机房内其它安全设备共用 42U 标准机柜； 23. 供水供电及特殊要求：无需供水；AC 100-240V，双路市电或 UPS 供电，10A 以上空气开关与插座，可靠接地，防震防磁，建议机房恒温 22±2℃；				
2. 厂商名称	启明星辰	型号	天阗高级持续性威胁检测与管理系统 APT3000	售价（万元）	约 30~40（参考）
仪器性能	1. 产品形态：标准 2U 服务器式机架设备，配置冗余电源并支持热插拔； 2. 产品成熟度：制造厂商保证产品经过 7 年以上持续研发和市场验证； 3. 网络层吞吐率：≥5G；应用层吞吐率：≥2G； 4. HTTP 最大并发连接数：≥50 万； 5. 每秒新建 HTTP 连接数：≥3 万； 6. 文件处理性能：≥15 万/天（APT800 型号为 ≥12 万/天，实验室环境）； 7. 存储与 RAID：集成 RAID 控制器，必须使用 Raid10，具备高可靠性与高效磁盘结构；硬盘容量 ≥4TB；内存 ≥32GB； 8. 接口配置：1 个 10/100/1000M 自适应管理口、1 个 10/100/1000M 自适应私有云口；业务口不少于 2 个千兆电口，额外配置 6 个接口扩展槽位； 9. 扩展能力：扩展接口理论满配支持 6 个万兆光口或 12 个千兆电口（或光口）； 10. 文件检测能力：具备 100 种以上格式的文件检测能力，涵盖 Windows、Linux、Android 多种操作系统，支持自定义文件类型； 11. 检测机制：具备静态检测、漏洞检测、行为检测不少于 3 种检测机制，每种机制的检测流程可自定义配置； 12. 样本检测工作流：支持不少于 10 种样本检测工作流配置，每种工作流可自定义选取相应样本格式； 13. 检测流程模板：具备“高速”“最优”“全面”三种检测流程配置模板； 14. 沙箱能力：具备二十种以上虚拟沙箱检测环境的能力；支持反沙箱检测不少于 20 种行为； 15. 威胁库：具备恶意样本库、隐蔽信道库、威胁情报库； 16. 已知威胁检测：事件特征库不少于 4500 条，可按协议类型、攻击类型、安全类型、流行程度、事件级别分类编排；策略集至少包括失陷主机、行为分析、攻击路径策略集； 17. 协议分析：具备 35 种以上协议分析能力及拒绝服务扫描类事件检测；弱口令检测口令配置项不少于 7 种； 18. 文件检测协议：具备邮件检测、HTTP 检测、FTP 检测、SMB 检测，支持				

<table>
<tr><td></td><td colspan="5">可疑样本手动上传检测；支持手动导入 pcap 包检测；
19. 自定义规则：支持自定义 YARA 规则进行检测；支持加密压缩文件解密及子文件单独检测；
20. 联动能力：可与防火墙、终端防病毒、网闸、网络审计、入侵检测、入侵防御、WAF 等 7 种以上专业安全设备协同联动；
21. 部署模式：支持旁路部署、集群部署；全面支持 IPv6（IPv6 管理、IPv6 流量检测）；支持私有云扩展能力；
22. 响应与导出：具备 Syslog、SNMP trap 响应能力，支持邮件报警、Kafka 接口外发检测日志、FTP 加密方式外发样本；
23. 报表能力：提供分析报表、基础统计报表、高级统计报表、详细事件报表，支持 HTML、PDF、EXCEL、WORD 格式输出；
24. 自身安全：核心构件通信采用 SSL 加密传输，支持访问控制列表；中文管理界面，可配置管理员、用户管理员、审计管理员；
25. 额定功率：2U 冗余电源（参考 550W×2），实际运行功耗约 250~350W；
26. 仪器尺寸（长×宽×高）：约 700mm×448mm×88.9mm（2U 标准机架，参考值）；
27. 仪器重量：约 25~30KG（满配含 4 块硬盘，参考值）；
28. 对房间的承载要求：≥300kg/m²（约 3KN/m²），2U 设备上标准 42U 机柜，无需加固；
29. 是否与其它仪器共用：否，独立上架；可与机房内其它安全设备共用 42U 标准机柜；
30. 供水供电及特殊要求：无需供水；AC 100-240V，双路市电或 UPS 供电，16A 以上插座（冗余电源需双路），可靠接地，防震防磁，建议机房恒温 22±2℃；</td></tr>
<tr><td>3. 厂商名称</td><td>亚信安全</td><td>型号</td><td>信桅深度威胁监测系统 TDA
TDA EE 3800</td><td>售价（万元）</td><td>约 35~45（参考）</td></tr>
<tr><td>仪器性能</td><td colspan="5">1. 产品形态：软硬一体化 2U 标准机架式设备；
2. 吞吐量：6Gbps；
3. 接口配置：标配 2×千兆电口＋2×万兆多模光口；闲置插槽 3 个全高＋1 个半高；
4. 硬件配置：CPU 12 核×1；内存 32G；硬盘 1T×4；电源 750W×2 冗余；
5. 协议支持：支持超过 100 种网络协议，如 HTTP、HTTPS、FTP、TFTP、SMTP、POP3、IMAP、SNMP、IRC、DNS、DHCP、P2P、SMB、RDP、VNC、TELNET、SSL/TLS 等；
6. 数据库协议：MSSQL、MySQL、Oracle、PGSQL；
7. 挖矿检测：提供多样性挖矿检测手段，可检测挖矿木马投递、挖矿木马横向移动行为、挖矿软件、矿池域名解析、矿池连接、矿池协议等；矿池协议告警提供虚拟币种类别，并设独立挖矿专项告警页面；
8. 恶意文件侦测：能够侦测勒索病毒、木马、僵尸、后门等文件型病毒，支持 Ransomware、WORM_DOWNAD.E、WORM_RONTKBR、TROJ_FAKEAV、PE_VIRUX 等多种高危病毒；</td></tr>
</table>

	9. 恶意行为分析：威胁流量与协议异常检测，含勒索病毒、零日攻击、网络蠕虫、木马、后门、间谍软件、网页威胁、暴力攻击、数据库注入攻击等； 10. 沙箱分析：内置沙箱系统并允许导入自定义镜像；支持服务器级 Windows 2003/2008/2012 与用户端级 Windows XP/7/8/10；可定制客户环境特性的操作系统平台与应用；支持未知威胁证据留存、样本分析报告与灵活投递策略； 11. 常见漏洞检测：Tomcat 写文件、ImageMagick 命令执行、ElasticSearch 命令执行、Samba 远程命令执行、ThinkPHP SQL 注入、Adobe ColdFusion 任意代码执行、GhostScript 沙箱绕过、Weblogic 反序列化、Fastjson 反序列化等； 12. WebShell 检测：支持冰蝎、哥斯拉、菜刀、蚁剑、weevely、开山斧等主流工具检测； 13. 黑客工具检测：支持 SQLmap、Cknife、AWVS、Havij、Nmap、EarthWorm、Masscan、FRP、Neo-reGeorg、Chisel、fscan 等 50 余种工具攻击检测； 14. 威胁分类告警：支持按网络攻击、挖矿、扫描、暴力破解、恶意文件、威胁情报等告警分类； 15. 自定义能力：网络威胁自定义（兼容业界最常用 snort 规则写法）＋威胁情报自定义（IP、URL、DOMAIN、文件 HASH 四种类型）； 16. 威胁溯源：恶意文件流转溯源（以文件为中心图形化展示）、威胁流量自动存储及 PCAP 下载、网络流量威胁验伤、抓包与 pcap 回放（回放告警与生产流量分页面展示）； 17. 资产管理：流量自动发现资产、自定义资产导入、按 IP/类型/标签查询、资产分组；自动发现弱密码资产及明文密码传输资产，密码脱敏存储展示； 18. 日志管理：支持 Syslog（CEF 格式，可集成第三方 SIEM/SOC）、Kafka；可同时接入 10 个日志服务器；支持原始日志与聚合日志两种类型； 19. 部署方式：支持旁路安装、TAP 分流安装、非对称路由；支持思科与华为远程端口镜像协议； 20. 部署架构：支持监测探针独立部署或平台＋监测探针分布式部署；平台支持多级组织分级分权管理，平级数据隔离、上级可见下级； 21. 报表能力：预设日报、周报、月报并支持自定义报表时间，内置通用报表模板与挖矿专项报表模板，支持即时报表； 22. 升级方式：支持实时在线升级、自动在线升级、手工升级多种方式； 23. 额定功率：750W×2（1+1 冗余），实际运行功耗约 350~450W； 24. 仪器尺寸（长×宽×高）：约 700mm×448mm×88.9mm（2U 标准机架，参考值）； 25. 仪器重量：约 22~28KG（满配，参考值）； 26. 对房间的承载要求：≥300kg/m²（约 3KN/m²），2U 设备上标准 42U 机柜，无需加固； 27. 是否与其它仪器共用：否，独立上架；可与机房内其它安全设备共用 42U 标准机柜； 28. 供水供电及特殊要求：无需供水；AC 100-240V，双路市电或 UPS 供电（750W×2 建议双路），16A 以上插座，可靠接地，防震防磁，建议机房恒温 22±2℃；
预计效益及风险	

编号:

预期年有效使用机时:8760小时/年

其中教学:0小时/年，科研:0小时/年，共享服务:8760小时/年

风险预测：仪器设备运行过程中不会对环境产生的影响，不涉及危险气体、有害废液、危险化学品、高温、低温、高压、放射性、激光、紫外线、粉尘、强磁、高压电、噪音、震动等各类危险源情况

管理人员安排及仪器安装条件

1. 人员安排

人员性质	姓名	职称	电话	是否专职
仪器负责人				
操作人员				
操作人员				
操作人员				

2. 安装条件

（1）仪器安置地址：浙江大学软件学院4号楼101机房；

（2）存放房间面积：248平方米；存放房间层高：4.7米；

（3）仪器尺寸：长430 mm×宽800 mm×高89mm；仪器重量：25KG；用电功率：0.3Kw；

（4）仪器设备对房间的承载要求：大于5KN/m^2；

（5）是否与其它仪器共用：否；

（6）供水供电及仪器特殊要求（防震、防磁、超净、恒温、接地等）落实情况：需单独拉线，接地，配置25A以上空气开关和插座，已落实。

编号:

专家论证意见

会议时间	2026 年 9 月 23 日　　14:00 - 16:00
会议地点	浙江大学软件学院 6 号楼 306 会议室

非专家参会人员（签名）：

专家论证意见：

专家组听取了申请人对拟购设备的汇报，查阅了相关资料，经质询与讨论，形成论证意见如下：

针对本次态势感知平台采购事项，我校组织专家开展专项技术论证。专家组按照网信部门安全要求，研判校园网络风险现状，认为项目建设目标明确，技术方案具备可行性，有效补齐现有安全短板，专家组一致同意通过论证。

进口产品专家论证意见：

☐1. 国内尚无同类产品，必须进口

☐2. 国内有同类产品，但技术参数满足不了需求，必须进口

☐3. 其他：_____

专家姓名		工作单位	职称	联系电话	签名
组长	王磊	宁波市数据服务中心	高工	13567845204	王磊
成员	樊明锐	宁波市大数据发展管理中心	高工	15168596411	樊明锐
	金学光	宁波市职教中心	高级	13071975678	金学光

编号:

审批意见

申请单位意见	签名（公章）： 2026 年 9 月 24 日
科研合作部门意见	项目管理员： 签名： 年 月 日
条件保障部门意见	签名： 2026 年 9 月 24 日
财务部门意见	签名： 2026 年 9 月 24 日
分管领导审批意见	签名（公章）： 2026 年 9 月 28 日
补充说明	