附件1

**采购项目需求**

主机安全管理系统

1. 项目概况

网络安全保护工作中主机安全是重要的一个环节，对各类信息系统主机服务器的安全漏洞识别发现、恶意代码防范、攻击入侵防范等有重要意义。我社目前尚未部署此类产品，为弥补此项短板，计划采购主机安全产品。

通过建设主机安全平台，主要满足以下要求：

1. 主机资产识别管理：通过安装软件代理在运行的环境中，识别主机资产，上报中央管控平台，集中统一管理。自动化识别进程、端口、账号、中间件、数据库、系统启动项、Web框架等资产，覆盖通用资产。

2.主机入侵行为实时监控：对疑似黑客行为进行监控，包括系统后门、Webshell、暴力破解、异常登陆、异常端口扫描、本地提权等进行实时的入侵检测，发现远端主机利用端口进行连接的潜在风险。

3. 主机漏洞检测与风险识别：主动扫描，发现系统漏洞和主流中间件漏洞，并对漏洞修复给出依据。识别账户弱密码等安全风险。

4.恶意代码防范：能够适配主流Windows和Linux操作系统，结合病毒检测引擎，对文件进行扫描查杀；同时可实时监控运行进程，发现恶意代码和病毒时上报告警，并进行处置

1. 技术要求与参数

**本次采购的主机安全范围包括我社生产环境和开发测试环境（两环境彼此网络隔离）。 Agent代理授权数量为2000。**

（一）方案架构

主机安全平台系统架构整体由软件代理（也称为探针或Agent）、服务端、控制端三部分构成。

1.Agent主要负责主机信息收集、监控等功能，实时监控进程、网络连接等行为。

2.服务端作为信息处理中枢，能够持续监测并分析agent端收集上来的信息并保存。可从各个维度的信息中发现漏洞、弱密码等安全风险和异常登录等异常行为，从而实现对入侵行为实时预警。

3.Web控制台，主要负责和用户交互，清晰展示各项安全检测和分析的结果，并对重大威胁进行实时告警。提供一个集中管理的安全工具，方便进行系统配置和管理、安全响应等相关操作。

（二）功能要求

以下功能为必须具备功能。

1.资产识别与台账管理：识别主机各类资产并建立台账。

* 主机识别：识别主机基础信息，监控主机状态，并提供自定义主机分组、操作系统、业务进程、安全插件等各种管理维度的主机统计。
* 进程识别：提供进程信息快照，展示进程各维度的信息，对root权限、僵尸进程、IO waiting进程、唯一进程进行分析统计，帮助发现问题进程。
* 端口识别：提供系统端口快照，端口服务分布情况。
* 账号识别：自动识别并分析系统账号与用户组的情况，包含root、sudo、交互账号、启动账号、过期账号、密码锁定账号等多个维度的账号分析。
* 硬件识别：系统硬件配置识别，包括系统内核、CPU、内存、网卡、设备型号、硬盘、磁盘使用分布等各类硬件信息。
* 软件识别：识别系统应用的安装使用情况，覆盖系统架构、Web运维、运维工具、系统应用、安全应用等常见应用。
* Web服务识别：识别服务器中运行的常见Web中间件，包括：Nginx、 Apache、 Jboss、 Tomcat、 Weblogic、 Jetty等。
* 数据库识别：识别主机数据库，覆盖常用集中式和分布式数据库，包括：MySQL、 Redis、 MongoDB、 Oracle、MemCache、Hbase、DB2、Sybase等。
* 其他资产如Web应用、 安装包、Jar包、系统启动项、计划任务、环境变量等的识别等。

2.主机漏洞和风险发现：检测主机操作系统等漏洞，识别弱密码等风险。

* 漏洞检测：使用POC验证等方式检测主机安全漏洞，并对高危漏洞爆发事件提供快速应急响应支持。
* 安全补丁：对安全补丁进行周期性自动检测，并提供详细补丁说明，修复方案及其修复影响。
* 弱密码检查：对主机用户账号进行弱密码检测。对linux 上的常用应用进行弱密码检测，例如mysql、redis、vsftpd等。
* 系统风险：检测由于系统配置不当可能产生的安全风险，如检测路由转发功能是否开启、检测网卡是否处于混杂模式、检测grub密码设置等。
* 应用风险：检测黑客关键攻击路径上常用应用的配置型风险，如SSH、redis、Memcache、MongoDB、Apache等。
* 账号风险：检测linux系统中由于账号配置产生的安全风险，例如，检测无密码可sudo的账号、检测GID/UID重复账号、检测系统中不必要的系统账号等。

3.入侵检测：检测针对主机的入侵行为及可疑活动。

* 暴力破解：实时发现暴力破解行为，如Linux和windows系统暴力破解，以及VSFTPD、WINRM等多种服务，并支持自动封堵。
* 异常登录：对在异常地点、异常时间、异常IP等异常登录行为的识别。
* 反弹shell：实时监控主机上所有利用Shell进行反向连接的行为。
* 本地提权：实时监控用户以低权限进入主机，之后通过某种行为获得高权限的事件。
* 后门检测：结合模式识别和行为检测，识别Rootkit、 Bootkit可疑进程、可疑线程等多种系统后门。
* 可疑操作：记录主机上执行的shell命令，实时监控被审计规则判断为危险的操作。用户可以查看操作并对操作进行审核，也可以对审计规则按自己的需求进行配置。
* Web后门：通过检测主机Web目录下的文件内容，发现是否存在有Web后门，并对发现的后门进行告警通知。

4.恶意代码检测

* 能够适配主流Windows和Linux操作系统；
* 结合恶意代码检测引擎，对文件进行扫描，同时可实时监控运行进程，发现恶意代码时上报告警。
* 具备自动或手动恶意代码处置或隔离能力。

5.安全响应：对检测出的安全风险具备一定处置能力

* 针对主机暴力破解行为，具备封停非内网IP的能力。
* 主机上发生异常登录行为时，可封停非内网IP，阻止登录。
* 检测出的后门文件可隔离，阻止黑客渗透。
* 检测出的web后门可隔离，避免黑客渗透带来的业务风险。
* 本地提权的进程可阻断，阻止黑客利用高权限执行更多恶意操作。
* 当反向连接发生时，阻断主机内维持连接的进程，阻止黑客利用连接远程控制主机。

以下功能为可支持功能。

A.合规基线

* 支持对各版本的linux系统、Windows系统按照等保、CIS的基线要求检测，覆盖主流操作系统的检测，例如：Centos、Ubuntu、RedHat、SUSE、Windows Server 2019、中标麒麟等。
* 支持对常用应用的等保、CIS基线的检测，例如：Apache、Nginx、Tomcat、Jboss、Resin、WebSphere、Weblogic等。
* 支持对主流数据库的等保、CIS基线的检测，例如：Mysql、MongoDB、Oracle、DB2等。

B.微隔离

* 访问关系可视化：Agent探针自动采集主机的出入站流量，获取IP、端口、协议、进程等网络信息。以拓扑图、列表等形式展示主机之间、分组之间的网络访问关系。
* 精细化访问控制：可在关系拓扑图上交互式设置微隔离策略，根据访问信息一键生成访问控制规则，实现以主机为颗粒度的精细化访问控制。通过微隔离策略，可对业务之间的访问关系进行管控，避免威胁横向扩散和业务违规访问。
* 支持出站访问限制，可控制主机的出站访问行为，对于特定主机严格管控对外访问，只有策略允许的访问行为可放行，策略外的访问行为一律拦截。
* 失陷主机一键隔离：可通过Agent一键隔离失陷主机，避免威胁持续扩散。

C.微蜜罐

* 微蜜罐包含网络蜜罐和文件蜜罐。
* 网络蜜罐是在蜜罐主机中，设置多个蜜罐端口，监控对这些端口的攻击行为，以记录各类黑客行为的线索，同时为系统提供一定的安全防护能力。
* 文件蜜罐是在蜜罐主机中，部署多个蜜罐文件，监控黑客对这件文件的操作行为，以记录黑客行为的线索，使潜在风险暴露。

D.文件完整性监测

* 对目录及文件进行定时扫描检测，同时也支持对特定的文件进行实时监控。支持用户在各个主机配置其特定的文件监控策略，适应多样化的文件监管需求。

E.安全大屏

* 安全大屏基于对主机持续的安全监控和分析，向客户可视化地呈现主机的总体安全情况，结合用户真实的使用场景，提供覆盖“资产”“风险”“入侵”“合规”等全方位的安全监控能力，以可视化图表的形式呈现，辅助用户进行安全监管和分析，并支持对模块内容定制化配置。

（三）系统安全控制措施

1.系统安全性要求

1. 主机安全控制台登录应支持双因素认证。
2. 主机安全控制台访问应采用HTTPS协议。

**2.**Agent要**求**

1. Agent采用绿色进程方式，不修改内核，不绑定驱动。
2. Agent安装或者启动功能，应无须重启应用或者操作系统。
3. Agent运行占用CPU一般不超过3%。
4. Agent正常运行的心跳数据和监控自身状态的数据传输不能造成网络拥堵。

（四）产品兼容性要求

1.服务端兼容性

 支持部署在RedHat、CentOS操作系统。

信创环境支持：支持银河麒麟、中标麒麟、统信UOS等国产化操作系统，支持X86和Arm架构。

2.Agent兼容性

支持RedHat、CentOS、Ubuntu、Debian、Windows Server等操作系统。

信创环境支持：支持银河麒麟、统信UOS等信创环境，支持X86和Arm架构。

1. 实施、验收和维保

（一）实施部署与培训

本阶段交付结果,包括不限于：

《项目部署实施方案》

《系统安装手册》

《用户操作手册》

《系统应急处置方案》

《项目上线总结报告》

根据项目实施需要，对我社人员提供培训完成知识转移。

（二）验收

部署完成并运行一个月后，由投标方提请验收。投标方应将项目相关的全部有关技术文件、资料、及招标文件和合同要求的其他材料交付招标人。

（三）维保服务

投标方须提供**3**年的维保期，维保期从项目验收合格之日起开始计算。维保服务包括但不限于系统的稳定运行维护和应急保障、系统软件更新、漏洞库更新、恶意代码库更新等。