

技术商务资信评分明细（葛君明）

项目名称：浙江省“智慧医保”安全运维及系统数据安全服务项目（ZJ-2142843）

序号	评分类型	评分项目内容	分值范围	杭州实在智能科技有限公司	杭州美创科技有限公司	浙江鼎顺信息有限公司	网神信息技术（北京）股份有限公司	北京神州绿盟科技有限公司
1	商务资信	①投标人具有ISO27001信息安全管理体认证、ISO20000信息技术服务管理体系认证、每个证书得1分，最高得2分； ②投标人具有国家信息安全测评中心颁发的信息安全服务资质（云计算安全类）的得1分；具有信息安全服务资质（安全开发类）的得1分。 提供以上有效证书扫描件，未提供的不得分。	0-4	2	4	0	4	4
2	商务资信	投标人自2018年1月1日（以合同签订时间为准）至今具有政务平台数据安全类服务业绩，提供合同扫描件作为证明材料，每份合同得0.5分，最多得2分，不提供的不得分。	0-2	0.5	2	1	2	2
3	商务资信	投标人自2018年1月1日（以合同签订时间为准）至今具有政务平台数据安全类产品业绩，提供合同扫描件作为证明材料，每份合同得0.5分，最多得2分，不提供的不得分。	0-2	0.5	2	2	2	2
4	技术	投标人对本项目的理解、对本项目背景、现状、目标、服务内容、部署环境等的理解。	0-3	2	2	2	3	2
5	技术	根据投标人数据安全管理制度咨询服务方案的完整性、方案的针对性和详细程度进行评分。	0-3	2	2	2	3	2
6	技术	根据投标人数据安全技术防护服务方案的完整性、方案的针对性和详细程度进行评分。	0-5	3	3	3	4	4
7	技术	根据投标人数据安全运营服务方案的完整性、方案的针对性和详细程度进行评分。	0-3	2	2	2	3	3
8	技术	采购需求中打★条款的响应情况。每个★条款符合要求的得2分，最高得14分	0-14	0	10	0	14	14
9	技术	采购需求中其余非★条款的响应情况。全部满足的得12分，不满足的每一项扣1分。未体现内的不得分。不满足项超过12项的视作明显不符合采购内容和质量标准，作无效标处理。	0-12	12	10	12	12	12
10	技术	组织实施方案，包括组织机构、实施场所、项目进度安排、项目人员安排、团队管理和沟通机制。根据投标文件体现的内容进行评分。	0-3	2	2	2	3	3
11.1	技术	专家组负责人（1人）具备以下专业证书： ①ISO27001Foundation、②ITIL（国际IT服务管理专业资格认证）、③人社部门颁发的信息系统项目管理师、④CISE注册信息安全工程师或CISP-PTE注册信息安全专业人员渗透测试工程师或CNVD（原创漏洞提交证明）或ITSM IT服务项目经理证书中的一本或多本。每一小项1分，满分4分。提供证书扫描件及参保证明（要求见上述注意事项），不提供的不得分。	0-4	0	3	0	4	4
11.2	技术	专家组成员（不含项目负责人）至少8人，否则本项不得分。人员具备以下专业证书：①CISE（注册信息安全工程师）、②CISP-PTE（注册信息安全专业人员渗透测试工程师）、③ITIL（国际IT服务管理专业资格认证）、④CNVD（原创漏洞提交证明），每本证书得0.5分，同一证书只计算一次，同一人最多计一本证书。本项最高得2分。提供证书扫描件及参保证明（要求见上述注意事项），不提供的不得分。	0-2	0	1	0	2	2

12.1	技术	项目负责人(1人)具备以下证书:①人社部门颁发的网络工程师(中级)、②CISA(信息系统审计师)、③人社部门颁发的信息系统项目管理师,④CISO注册信息安全管理人员证书或ISCCC信息安全体系内审员证书或ITSS-IT服务工程师证书中的一本或多本。每一小项1分,满分4分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-4	0	3	0	4	2
12.2	技术	实施人员(不含项目负责人)至少10人,否则本项不得分。人员具备以下专业证书:①CISO(注册信息安全管理人员)、②人社部门颁发的信息系统项目管理师、③ITSS(IT服务工程师)、④ISCCC(信息安全体系内审员),每本证书得0.5分,同一证书只计算一次,同一人最多计一本证书。本项最高得2分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-2	0	1	0	2	1.5
13.1	技术	驻场负责人(1人)具备以下专业证书:①CISD(注册信息安全开发人员)、②CISSP(信息系统安全专业认证)、③CCSSP(云安全系统认证专家)、④CISE注册信息安全工程师或CISI注册信息安全讲师或CISAW信息安全从业人员认证或CISO注册信息安全管理人员。每一小项1分,满分4分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-4	0	2	0	4	3
13.2	技术	驻场负责人自2018年1月1日以来曾以项目负责人身份从事过政务平台数据安全类服务业绩的0.5分。提供能体现项目负责人姓名的合同或业主证明扫描件。未提供的不得分。此项业绩与序号2的投标人业绩不重复得分。	0-0.5	0	0	0	0.5	0
13.3	技术	驻场成员(不含项目负责人)至少5人,否则本项不得分。人员具备以下专业证书:①CISE(注册信息安全工程师)、②CISAW(信息安全从业人员认证)、③CISO(注册信息安全管理人员)。每本证书得0.5分,同一证书只计算一次,同一人最多计一本证书。本项最高得1.5分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-1.5	0	1.5	0	1.5	1.5
14.1	技术	讲师团队负责人(1人)具备以下专业证书:①CDGA证书(数据治理工程师)、②CCSK(云安全知识认证)、③ISO27001LA、④CISAW(信息安全从业人员认证)或CISI注册信息安全讲师。每一小项0.5分,满分2分。提供证书扫描件,不提供的不得分。	0-2	0	0.5	0	2	1.5
14.2	技术	专业讲师(不含专家讲师)至少6人,否则本项不得分。人员具备以下专业证书:①CISI(注册信息安全讲师)、②CCSK(云安全知识认证)、③CDPSE(数据隐私解决方案工程师认证)、④ISO27001LA(信息安全管理体系主任审核员)。每本证书得0.5分,同一证书只计算一次,同一人最多计一本证书。本项最高得2分。提供证书扫描件,不提供的不得分。	0-2	0	1.5	0	2	1.5
15.1	技术	远程专家团队负责人(1人)具备以下专业证书:①CISA(信息系统审计师)、②CNVD(原创漏洞证明)、③CISSP(信息系统安全专业认证)、④CISO注册信息安全管理人员或CISP-PTE注册信息安全专业人员渗透测试工程师或ISO27001LA信息安全管理体系主任审核员或CISAW信息安全从业人员认证。每一小项1分,满分4分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-4	0	2	0	4	4

15.2	技术	远程专家（不含项目负责人）至少30人，否则本项不得分。人员具备以下专业证书：①CISP-PTS（注册渗透测试专家）10人以上、②CZTP（零信任专家认证）证书10人以上、③CISP-IRE（注册应急响应工程师）5名以上、④EIACE（高级网络信息安全工程师）5名以上。每一小项0.5分，满分2分。提供证书扫描件及参保证明（要求见上述注意事项），不提供的不得分。	0-2	0	0	0	2	1
16	技术	现场演示采用真实或测试系统，其他演示方式不得分。 （演示时长不超过15分钟） 一、数据接口动态防护服务 1、前置机风险感知服务：支持展示当前服务器、进程、账户、软件应用、Web资产、Web服务、Web框架、数据库、端口、网络连接、启动服务、安装包、计划任务、环境变量、内核模块等分类资产数量统计，可对分类资产全局进行快速搜索。（1分） 2、攻击安全防护：提供攻击安全防护服务：对当前API服务端提供安全防护，可对API使用中常见的网络安全攻击进行感知和识别，包括SQL注入，XSS攻击，目录遍历，CC攻击，PHP注入，网站扫描，以及敏感信息访问等（1分） 二、数据安全总体态势感知服务 3、以数据流转的视角出发，按数据的来源和赋能维度实时统计各地市部门的数据采集数量及共享交换数量。（1分） 三、敏感数据安全态势感知服务 4、按敏感数据的安全风险进行统计及可视化展现，并可下钻和跳转展示告警详情；（1分） 四、敏感数据流转监测预警服务 5、提供基于业务应用场景，对其数据流经的节点，包括主机资产、应用服务、数据接口、数据、账号等，根据数据的流向，实现简单拖拽数据流节点的可视化元件，建立数据流程可视化图谱。（1分） 五、高级威胁监测服务 6、提供威胁分析可视化服务：实现从攻击者的视角发现入侵的痕迹从而加固整改“智慧医保”自身安全。基于攻击链的维度将攻击行为科学划分、告警深度调查分析，并以受害主机为线索还原整个攻击过程（侦察-入侵-命令控制-横向渗透-数据外泄-痕迹清理）和可视化展现和推演，来解决威胁分析过程可视化（1分） 7、提供云端联动服务：实现与云端威胁情报联动，可对攻击IP、C&C域名和恶意样本MD5进行一键搜索，查看基本信息、相关样本、关联URL、可视化分析、域名解析、注册信息、关联域名、数字证书等（1分） 8、提供威胁狩猎分析服务：实现对任意线索的自定义拓线及溯源取证分析，以可视化分析画布形式展示拓线过程并支持结果快照导出；对于给定线索的溯源结果展示，包括但不限于攻击溯源、失陷主机分析、暴力破解分析、弱口令分析等。（1分） 六、主动防御服务 9、提供蜜罐模版导入服务，可以配置蜜罐模版名称、服务名称、端口、硬件规格，类型包括高交互蜜罐、中交互蜜罐和低交互蜜罐（1分） 10、提供支持HTTP攻击流量进行诱骗服务，涵盖的Web攻击类型包括：文件读取、目录遍历、命令执行、代码执行、SQL注入、XSS等（1分）	0-10	0	2	3	10	9
17	技术	疫情防控措施。投标人提供项目实施期间疫情防控措施，根据措施的详细程度和可行性评分。	0-1	1	1	1	1	1
合计			0-90.0	27	57.5	30	89	80

专家（签名）：

技术商务资信评分明细（潘克宇）

项目名称：浙江省“智慧医保”安全运维及系统数据安全服务项目（ZJ-2142843）

序号	评分类型	评分项目内容	分值范围	杭州实在智能科技有限公司	杭州美创科技有限公司	浙江鼎顺信息工程有限公司	网神信息技术（北京）股份有限公司	北京神州绿盟科技有限公司
1	商务资信	①投标人具有ISO27001信息安全管理体认证、ISO20000信息技术服务管理体系认证、每个证书得1分，最高得2分； ②投标人具有国家信息安全测评中心颁发的信息安全服务资质（云计算安全类）的得1分；具有信息安全服务资质（安全开发类）的得1分。 提供以上有效证书扫描件，未提供的不得分。	0-4	2	4	0	4	4
2	商务资信	投标人自2018年1月1日（以合同签订时间为准）至今具有政务平台数据安全类服务业绩，提供合同扫描件作为证明材料，每份合同得0.5分，最多得2分，不提供的不得分。	0-2	0.5	2	1	2	2
3	商务资信	投标人自2018年1月1日（以合同签订时间为准）至今具有政务平台数据安全类产品业绩，提供合同扫描件作为证明材料，每份合同得0.5分，最多得2分，不提供的不得分。	0-2	0.5	2	2	2	2
4	技术	投标人对本项目的理解、对本项目背景、现状、目标、服务内容、部署环境等的理解。	0-3	2	2.5	2	3	3
5	技术	根据投标人数据安全管理制度咨询服务方案的完整性、方案的针对性和详细程度进行评分。	0-3	2	2.5	2	3	3
6	技术	根据投标人数据安全技术防护服务方案的完整性、方案的针对性和详细程度进行评分。	0-5	3	3.5	3	4.5	4.5
7	技术	根据投标人数据安全运营服务方案的完整性、方案的针对性和详细程度进行评分。	0-3	2	2.5	2	3	3
8	技术	采购需求中打★条款的响应情况。每个★条款符合要求的得2分，最高得14分	0-14	0	10	0	14	14
9	技术	采购需求中其余非★条款的响应情况。全部满足的得12分，不满足的每一项扣1分。未体现内的不得分。不满足项超过12项的视作明显不符合采购内容和质量标准，作无效标处理。	0-12	12	10	12	12	12
10	技术	组织实施方案，包括组织机构、实施场所、项目进度安排、项目人员安排、团队管理和沟通机制。根据投标文件体现的内容进行评分。	0-3	2	2.5	2	3	3
11.1	技术	专家组负责人（1人）具备以下专业证书： ①ISO27001Foundation、②ITIL（国际IT服务管理专业资格认证）、③人社部门颁发的信息系统项目管理师、④CISE注册信息安全工程师或CISP-PTE注册信息安全专业人员渗透测试工程师或CNVD（原创漏洞提交证明）或ITSM IT服务项目经理证书中的一本或多本。每一小项1分，满分4分。提供证书扫描件及参保证明（要求见上述注意事项），不提供的不得分。	0-4	0	3	0	4	4
11.2	技术	专家组成员（不含项目负责人）至少8人，否则本项不得分。人员具备以下专业证书：①CISE（注册信息安全工程师）、②CISP-PTE（注册信息安全专业人员渗透测试工程师）、③ITIL（国际IT服务管理专业资格认证）、④CNVD（原创漏洞提交证明），每本证书得0.5分，同一证书只计算一次，同一人最多计一本证书。本项最高得2分。提供证书扫描件及参保证明（要求见上述注意事项），不提供的不得分。	0-2	0	1	0	2	2

12.1	技术	项目负责人(1人)具备以下证书:①人社部门颁发的网络工程师(中级)、②CISA(信息系统审计师)、③人社部门颁发的信息系统项目管理师,④CISO注册信息安全管理人员证书或ISCCC信息安全体系内审员证书或ITSS-IT服务工程师证书中的一本或多本。每一小项1分,满分4分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-4	0	3	0	4	2
12.2	技术	实施人员(不含项目负责人)至少10人,否则本项不得分。人员具备以下专业证书:①CISO(注册信息安全管理人员)、②人社部门颁发的信息系统项目管理师、③ITSS(IT服务工程师)、④ISCCC(信息安全体系内审员),每本证书得0.5分,同一证书只计算一次,同一人最多计一本证书。本项最高得2分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-2	0	1	0	2	1.5
13.1	技术	驻场负责人(1人)具备以下专业证书:①CISD(注册信息安全开发人员)、②CISSP(信息系统安全专业认证)、③CCSSP(云安全系统认证专家)、④CISE注册信息安全工程师或CISI注册信息安全讲师或CISAW信息安全从业人员认证或CISO注册信息安全管理人员。每一小项1分,满分4分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-4	0	2	0	4	3
13.2	技术	驻场负责人自2018年1月1日以来曾以项目负责人身份从事过政务平台数据安全类服务业绩的0.5分。提供能体现项目负责人姓名的合同或业主证明扫描件。未提供的不得分。此项业绩与序号2的投标人业绩不重复得分。	0-0.5	0	0	0	0.5	0
13.3	技术	驻场成员(不含项目负责人)至少5人,否则本项不得分。人员具备以下专业证书:①CISE(注册信息安全工程师)、②CISAW(信息安全从业人员认证)、③CISO(注册信息安全管理人员)。每本证书得0.5分,同一证书只计算一次,同一人最多计一本证书。本项最高得1.5分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-1.5	0	1.5	0	1.5	1.5
14.1	技术	讲师团队负责人(1人)具备以下专业证书:①CDGA证书(数据治理工程师)、②CCSK(云安全知识认证)、③ISO27001LA、④CISAW(信息安全从业人员认证)或CISI注册信息安全讲师。每一小项0.5分,满分2分。提供证书扫描件,不提供的不得分。	0-2	0	0.5	0	2	1.5
14.2	技术	专业讲师(不含专家讲师)至少6人,否则本项不得分。人员具备以下专业证书:①CISI(注册信息安全讲师)、②CCSK(云安全知识认证)、③CDPSE(数据隐私解决方案工程师认证)、④ISO27001LA(信息安全管理体系主任审核员)。每本证书得0.5分,同一证书只计算一次,同一人最多计一本证书。本项最高得2分。提供证书扫描件,不提供的不得分。	0-2	0	1.5	0	2	1.5
15.1	技术	远程专家团队负责人(1人)具备以下专业证书:①CISA(信息系统审计师)、②CNVD(原创漏洞证明)、③CISSP(信息系统安全专业认证)、④CISO注册信息安全管理人员或CISP-PTE注册信息安全专业人员渗透测试工程师或ISO27001LA信息安全管理体系主任审核员或CISAW信息安全从业人员认证。每一小项1分,满分4分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-4	0	2	0	4	4

15.2	技术	远程专家（不含项目负责人）至少30人，否则本项不得分。人员具备以下专业证书：①CISP-PTS（注册渗透测试专家）10人以上、②CZTP（零信任专家认证）证书10人以上、③CISP-IRE（注册应急响应工程师）5名以上、④EIACE（高级网络信息安全工程师）5名以上。每一小项0.5分，满分2分。提供证书扫描件及参保证明（要求见上述注意事项），不提供的不得分。	0-2	0	0	0	2	1
16	技术	现场演示采用真实或测试系统，其他演示方式不得分。 （演示时长不超过15分钟） 一、数据接口动态防护服务 1、前置机风险感知服务：支持展示当前服务器、进程、账户、软件应用、Web资产、Web服务、Web框架、数据库、端口、网络连接、启动服务、安装包、计划任务、环境变量、内核模块等分类资产数量统计，可对分类资产全局进行快速搜索。（1分） 2、攻击安全防护：提供攻击安全防护服务：对当前API服务端提供安全防护，可对API使用中常见的网络安全攻击进行感知和识别，包括SQL注入，XSS攻击，目录遍历，CC攻击，PHP注入，网站扫描，以及敏感信息访问等（1分） 二、数据安全总体态势感知服务 3、以数据流转的视角出发，按数据的来源和赋能维度实时统计各地市部门的数据采集数量及共享交换数量。（1分） 三、敏感数据安全态势感知服务 4、按敏感数据的安全风险进行统计及可视化展现，并可下钻和跳转展示告警详情；（1分） 四、敏感数据流转监测预警服务 5、提供基于业务应用场景，对其数据流经的节点，包括主机资产、应用服务、数据接口、数据、账号等，根据数据的流向，实现简单拖拽数据流节点的可视化元件，建立数据流程可视化图谱。（1分） 五、高级威胁监测服务 6、提供威胁分析可视化服务：实现从攻击者的视角发现入侵的痕迹从而加固整改“智慧医保”自身安全。基于攻击链的维度将攻击行为科学划分、告警深度调查分析，并以受害主机为线索还原整个攻击过程（侦察-入侵-命令控制-横向渗透-数据外泄-痕迹清理）和可视化展现和推演，来解决威胁分析过程可视化（1分） 7、提供云端联动服务：实现与云端威胁情报联动，可对攻击IP、C&C域名和恶意样本MD5进行一键搜索，查看基本信息、相关样本、关联URL、可视化分析、域名解析、注册信息、关联域名、数字证书等（1分） 8、提供威胁狩猎分析服务：实现对任意线索的自定义拓线及溯源取证分析，以可视化分析画布形式展示拓线过程并支持结果快照导出；对于给定线索的溯源结果展示，包括但不限于攻击溯源、失陷主机分析、暴力破解分析、弱口令分析等。（1分） 六、主动防御服务 9、提供蜜罐模版导入服务，可以配置蜜罐模版名称、服务名称、端口、硬件规格，类型包括高交互蜜罐、中交互蜜罐和低交互蜜罐（1分） 10、提供支持HTTP攻击流量进行诱骗服务，涵盖的Web攻击类型包括：文件读取、目录遍历、命令执行、代码执行、SQL注入、XSS等（1分）	0-10	0	2	3	10	9
17	技术	疫情防控措施。投标人提供项目实施期间疫情防控措施，根据措施的详细程度和可行性评分。	0-1	1	1	1	1	1
合计			0-90.0	27	60	30	89.5	82.5

专家（签名）：

技术商务资信评分明细（徐建锋）

项目名称：浙江省“智慧医保”安全运维及系统数据安全服务项目（ZJ-2142843）

序号	评分类型	评分项目内容	分值范围	杭州实在智能科技有限公司	杭州美创科技有限公司	浙江鼎顺信息工程有限公司	网神信息技术(北京)股份有限公司	北京神州绿盟科技有限公司
1	商务资信	①投标人具有ISO27001信息安全管理体认证、ISO20000信息技术服务管理体系认证、每个证书得1分，最高得2分； ②投标人具有国家信息安全测评中心颁发的信息安全服务资质（云计算安全类）的得1分；具有信息安全服务资质（安全开发类）的得1分。 提供以上有效证书扫描件，未提供的不得分。	0-4	2	4	0	4	4
2	商务资信	投标人自2018年1月1日（以合同签订时间为准）至今具有政务平台数据安全类服务业绩，提供合同扫描件作为证明材料，每份合同得0.5分，最多得2分，不提供的不得分。	0-2	0.5	2	1	2	2
3	商务资信	投标人自2018年1月1日（以合同签订时间为准）至今具有政务平台数据安全类产品业绩，提供合同扫描件作为证明材料，每份合同得0.5分，最多得2分，不提供的不得分。	0-2	0.5	2	2	2	2
4	技术	投标人对本项目的理解、对本项目背景、现状、目标、服务内容、部署环境等的理解。	0-3	2	2	2	2.5	2.5
5	技术	根据投标人数据安全管理制度咨询服务方案的完整性、方案的针对性和详细程度进行评分。	0-3	2	2	2	3	3
6	技术	根据投标人数据安全技术防护服务方案的完整性、方案的针对性和详细程度进行评分。	0-5	4	4	4	4.5	4
7	技术	根据投标人数据安全运营服务方案的完整性、方案的针对性和详细程度进行评分。	0-3	2	2	2	3	3
8	技术	采购需求中打★条款的响应情况。每个★条款符合要求的得2分，最高得14分	0-14	0	10	0	14	14
9	技术	采购需求中其余非★条款的响应情况。全部满足的得12分，不满足的每一项扣1分。未体现内的不得分。不满足项超过12项的视作明显不符合采购内容和质量标准，作无效标处理。	0-12	12	10	12	12	12
10	技术	组织实施方案，包括组织机构、实施场所、项目进度安排、项目人员安排、团队管理和沟通机制。根据投标文件体现的内容进行评分。	0-3	2	3	3	3	3
11.1	技术	专家组负责人（1人）具备以下专业证书： ①ISO27001Foundation、②ITIL（国际IT服务管理专业资格认证）、③人社部门颁发的信息系统项目管理师、④CISE注册信息安全工程师或CISP-PTE注册信息安全专业人员渗透测试工程师或CNVD（原创漏洞提交证明）或ITSM IT服务项目经理证书中的一本或多本。每一小项1分，满分4分。提供证书扫描件及参保证明（要求见上述注意事项），不提供的不得分。	0-4	0	3	0	4	4
11.2	技术	专家组成员（不含项目负责人）至少8人，否则本项不得分。人员具备以下专业证书：①CISE（注册信息安全工程师）、②CISP-PTE（注册信息安全专业人员渗透测试工程师）、③ITIL（国际IT服务管理专业资格认证）、④CNVD（原创漏洞提交证明），每本证书得0.5分，同一证书只计算一次，同一人最多计一本证书。本项最高得2分。提供证书扫描件及参保证明（要求见上述注意事项），不提供的不得分。	0-2	0	1	0	2	2

12.1	技术	项目负责人(1人)具备以下证书:①人社部门颁发的网络工程师(中级)、②CISA(信息系统审计师)、③人社部门颁发的信息系统项目管理师,④CISO注册信息安全管理人员证书或ISCCC信息安全体系内审员证书或ITSS-IT服务工程师证书中的一本或多本。每一小项1分,满分4分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-4	0	3	0	4	2
12.2	技术	实施人员(不含项目负责人)至少10人,否则本项不得分。人员具备以下专业证书:①CISO(注册信息安全管理人员)、②人社部门颁发的信息系统项目管理师、③ITSS(IT服务工程师)、④ISCCC(信息安全体系内审员),每本证书得0.5分,同一证书只计算一次,同一人最多计一本证书。本项最高得2分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-2	0	1	0	2	1.5
13.1	技术	驻场负责人(1人)具备以下专业证书:①CISD(注册信息安全开发人员)、②CISSP(信息系统安全专业认证)、③CCSSP(云安全系统认证专家)、④CISE注册信息安全工程师或CISI注册信息安全讲师或CISAW信息安全从业人员认证或CISO注册信息安全管理人员。每一小项1分,满分4分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-4	0	2	0	4	3
13.2	技术	驻场负责人自2018年1月1日以来曾以项目负责人身份从事过政务平台数据安全类服务业绩的0.5分。提供能体现项目负责人姓名的合同或业主证明扫描件。未提供的不得分。此项业绩与序号2的投标人业绩不重复得分。	0-0.5	0	0	0	0.5	0
13.3	技术	驻场成员(不含项目负责人)至少5人,否则本项不得分。人员具备以下专业证书:①CISE(注册信息安全工程师)、②CISAW(信息安全从业人员认证)、③CISO(注册信息安全管理人员)。每本证书得0.5分,同一证书只计算一次,同一人最多计一本证书。本项最高得1.5分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-1.5	0	1.5	0	1.5	1.5
14.1	技术	讲师团队负责人(1人)具备以下专业证书:①CDGA证书(数据治理工程师)、②CCSK(云安全知识认证)、③ISO27001LA、④CISAW(信息安全从业人员认证)或CISI注册信息安全讲师。每一小项0.5分,满分2分。提供证书扫描件,不提供的不得分。	0-2	0	0.5	0	2	1.5
14.2	技术	专业讲师(不含专家讲师)至少6人,否则本项不得分。人员具备以下专业证书:①CISI(注册信息安全讲师)、②CCSK(云安全知识认证)、③CDPSE(数据隐私解决方案工程师认证)、④ISO27001LA(信息安全管理体系主任审核员)。每本证书得0.5分,同一证书只计算一次,同一人最多计一本证书。本项最高得2分。提供证书扫描件,不提供的不得分。	0-2	0	1.5	0	2	1.5
15.1	技术	远程专家团队负责人(1人)具备以下专业证书:①CISA(信息系统审计师)、②CNVD(原创漏洞证明)、③CISSP(信息系统安全专业认证)、④CISO注册信息安全管理人员或CISP-PTE注册信息安全专业人员渗透测试工程师或ISO27001LA信息安全管理体系主任审核员或CISAW信息安全从业人员认证。每一小项1分,满分4分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-4	0	2	0	4	4

15.2	技术	远程专家（不含项目负责人）至少30人，否则本项不得分。人员具备以下专业证书：①CISP-PTS（注册渗透测试专家）10人以上、②CZTP（零信任专家认证）证书10人以上、③CISP-IRE（注册应急响应工程师）5名以上、④EIACE（高级网络信息安全工程师）5名以上。每一小项0.5分，满分2分。提供证书扫描件及参保证明（要求见上述注意事项），不提供的不得分。	0-2	0	0	0	2	1
16	技术	现场演示采用真实或测试系统，其他演示方式不得分。 （演示时长不超过15分钟） 一、数据接口动态防护服务 1、前置机风险感知服务：支持展示当前服务器、进程、账户、软件应用、Web资产、Web服务、Web框架、数据库、端口、网络连接、启动服务、安装包、计划任务、环境变量、内核模块等分类资产数量统计，可对分类资产全局进行快速搜索。（1分） 2、攻击安全防护：提供攻击安全防护服务：对当前API服务端提供安全防护，可对API使用中常见的网络安全攻击进行感知和识别，包括SQL注入，XSS攻击，目录遍历，CC攻击，PHP注入，网站扫描，以及敏感信息访问等（1分） 二、数据安全总体态势感知服务 3、以数据流转的视角出发，按数据的来源和赋能维度实时统计各地市部门的数据采集数量及共享交换数量。（1分） 三、敏感数据安全态势感知服务 4、按敏感数据的安全风险进行统计及可视化展现，并可下钻和跳转展示告警详情；（1分） 四、敏感数据流转监测预警服务 5、提供基于业务应用场景，对其数据流经的节点，包括主机资产、应用服务、数据接口、数据、账号等，根据数据的流向，实现简单拖拽数据流节点的可视化元件，建立数据流程可视化图谱。（1分） 五、高级威胁监测服务 6、提供威胁分析可视化服务：实现从攻击者的视角发现入侵的痕迹从而加固整改“智慧医保”自身安全。基于攻击链的维度将攻击行为科学划分、告警深度调查分析，并以受害主机为线索还原整个攻击过程（侦察-入侵-命令控制-横向渗透-数据外泄-痕迹清理）和可视化展现和推演，来解决威胁分析过程可视化（1分） 7、提供云端联动服务：实现与云端威胁情报联动，可对攻击IP、C&C域名和恶意样本MD5进行一键搜索，查看基本信息、相关样本、关联URL、可视化分析、域名解析、注册信息、关联域名、数字证书等（1分） 8、提供威胁狩猎分析服务：实现对任意线索的自定义拓线及溯源取证分析，以可视化分析画布形式展示拓线过程并支持结果快照导出；对于给定线索的溯源结果展示，包括但不限于攻击溯源、失陷主机分析、暴力破解分析、弱口令分析等。（1分） 六、主动防御服务 9、提供蜜罐模版导入服务，可以配置蜜罐模版名称、服务名称、端口、硬件规格，类型包括高交互蜜罐、中交互蜜罐和低交互蜜罐（1分） 10、提供支持HTTP攻击流量进行诱骗服务，涵盖的Web攻击类型包括：文件读取、目录遍历、命令执行、代码执行、SQL注入、XSS等（1分）	0-10	0	2	3	10	9
17	技术	疫情防控措施。投标人提供项目实施期间疫情防控措施，根据措施的详细程度和可行性评分。	0-1	1	1	1	1	1
合计			0-90.0	28	59.5	32	89	81.5

专家（签名）：

技术商务资信评分明细（张文涛）

项目名称：浙江省“智慧医保”安全运维及系统数据安全服务项目（ZJ-2142843）

序号	评分类型	评分项目内容	分值范围	杭州实在智能科技有限公司	杭州美创科技有限公司	浙江鼎顺信息工程有限公司	网神信息技术(北京)股份有限公司	北京神州绿盟科技有限公司
1	商务资信	①投标人具有ISO27001信息安全管理体认证、ISO20000信息技术服务管理体系认证、每个证书得1分，最高得2分； ②投标人具有国家信息安全测评中心颁发的信息安全服务资质（云计算安全类）的得1分；具有信息安全服务资质（安全开发类）的得1分。 提供以上有效证书扫描件，未提供的不得分。	0-4	2	4	0	4	4
2	商务资信	投标人自2018年1月1日（以合同签订时间为准）至今具有政务平台数据安全类服务业绩，提供合同扫描件作为证明材料，每份合同得0.5分，最多得2分，不提供的不得分。	0-2	0.5	2	1	2	2
3	商务资信	投标人自2018年1月1日（以合同签订时间为准）至今具有政务平台数据安全类产品业绩，提供合同扫描件作为证明材料，每份合同得0.5分，最多得2分，不提供的不得分。	0-2	0.5	2	2	2	2
4	技术	投标人对本项目的理解、对本项目背景、现状、目标、服务内容、部署环境等的理解。	0-3	2	2	2	2.5	2.5
5	技术	根据投标人数据安全管理制度咨询服务方案的完整性、方案的针对性和详细程度进行评分。	0-3	2	2	2	2.5	2.5
6	技术	根据投标人数据安全技术防护服务方案的完整性、方案的针对性和详细程度进行评分。	0-5	3	3.5	4	4	4
7	技术	根据投标人数据安全运营服务方案的完整性、方案的针对性和详细程度进行评分。	0-3	2	2	2	2.5	2.5
8	技术	采购需求中打★条款的响应情况。每个★条款符合要求的得2分，最高得14分	0-14	0	10	0	14	14
9	技术	采购需求中其余非★条款的响应情况。全部满足的得12分，不满足的每一项扣1分。未体现内的不得分。不满足项超过12项的视作明显不符合采购内容和质量标准，作无效标处理。	0-12	12	10	12	12	12
10	技术	组织实施方案，包括组织机构、实施场所、项目进度安排、项目人员安排、团队管理和沟通机制。根据投标文件体现的内容进行评分。	0-3	1.5	2	2	2.5	2.5
11.1	技术	专家组负责人（1人）具备以下专业证书： ①ISO27001Foundation、②ITIL（国际IT服务管理专业资格认证）、③人社部门颁发的信息系统项目管理师、④CISE注册信息安全工程师或CISP-PTE注册信息安全专业人员渗透测试工程师或CNVD（原创漏洞提交证明）或ITSM IT服务项目经理证书中的一本或多本。每一小项1分，满分4分。提供证书扫描件及参保证明（要求见上述注意事项），不提供的不得分。	0-4	0	3	0	4	4
11.2	技术	专家组成员（不含项目负责人）至少8人，否则本项不得分。人员具备以下专业证书：①CISE（注册信息安全工程师）、②CISP-PTE（注册信息安全专业人员渗透测试工程师）、③ITIL（国际IT服务管理专业资格认证）、④CNVD（原创漏洞提交证明），每本证书得0.5分，同一证书只计算一次，同一人最多计一本证书。本项最高得2分。提供证书扫描件及参保证明（要求见上述注意事项），不提供的不得分。	0-2	0	1	0	2	2

12.1	技术	项目负责人(1人)具备以下证书:①人社部门颁发的网络工程师(中级)、②CISA(信息系统审计师)、③人社部门颁发的信息系统项目管理师,④CISO注册信息安全管理人员证书或ISCCC信息安全体系内审员证书或ITSS-IT服务工程师证书中的一本或多本。每一小项1分,满分4分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-4	0	3	0	4	2
12.2	技术	实施人员(不含项目负责人)至少10人,否则本项不得分。人员具备以下专业证书:①CISO(注册信息安全管理人员)、②人社部门颁发的信息系统项目管理师、③ITSS(IT服务工程师)、④ISCCC(信息安全体系内审员),每本证书得0.5分,同一证书只计算一次,同一人最多计一本证书。本项最高得2分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-2	0	1	0	2	1.5
13.1	技术	驻场负责人(1人)具备以下专业证书:①CISD(注册信息安全开发人员)、②CISSP(信息系统安全专业认证)、③CCSSP(云安全系统认证专家)、④CISE注册信息安全工程师或CISI注册信息安全讲师或CISAW信息安全从业人员认证或CISO注册信息安全管理人员。每一小项1分,满分4分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-4	0	2	0	4	3
13.2	技术	驻场负责人自2018年1月1日以来曾以项目负责人身份从事过政务平台数据安全类服务业绩的0.5分。提供能体现项目负责人姓名的合同或业主证明扫描件。未提供的不得分。此项业绩与序号2的投标人业绩不重复得分。	0-0.5	0	0	0	0.5	0
13.3	技术	驻场成员(不含项目负责人)至少5人,否则本项不得分。人员具备以下专业证书:①CISE(注册信息安全工程师)、②CISAW(信息安全从业人员认证)、③CISO(注册信息安全管理人员)。每本证书得0.5分,同一证书只计算一次,同一人最多计一本证书。本项最高得1.5分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-1.5	0	1.5	0	1.5	1.5
14.1	技术	讲师团队负责人(1人)具备以下专业证书:①CDGA证书(数据治理工程师)、②CCSK(云安全知识认证)、③ISO27001LA、④CISAW(信息安全从业人员认证)或CISI注册信息安全讲师。每一小项0.5分,满分2分。提供证书扫描件,不提供的不得分。	0-2	0	0.5	0	2	1.5
14.2	技术	专业讲师(不含专家讲师)至少6人,否则本项不得分。人员具备以下专业证书:①CISI(注册信息安全讲师)、②CCSK(云安全知识认证)、③CDPSE(数据隐私解决方案工程师认证)、④ISO27001LA(信息安全管理体系主任审核员)。每本证书得0.5分,同一证书只计算一次,同一人最多计一本证书。本项最高得2分。提供证书扫描件,不提供的不得分。	0-2	0	1.5	0	2	1.5
15.1	技术	远程专家团队负责人(1人)具备以下专业证书:①CISA(信息系统审计师)、②CNVD(原创漏洞证明)、③CISSP(信息系统安全专业认证)、④CISO注册信息安全管理人员或CISP-PTE注册信息安全专业人员渗透测试工程师或ISO27001LA信息安全管理体系主任审核员或CISAW信息安全从业人员认证。每一小项1分,满分4分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-4	0	2	0	4	4

15.2	技术	远程专家（不含项目负责人）至少30人，否则本项不得分。人员具备以下专业证书：①CISP-PTS（注册渗透测试专家）10人以上、②CZTP（零信任专家认证）证书10人以上、③CISP-IRE（注册应急响应工程师）5名以上、④EIACE（高级网络信息安全工程师）5名以上。每一小项0.5分，满分2分。提供证书扫描件及参保证明（要求见上述注意事项），不提供的不得分。	0-2	0	0	0	2	1
16	技术	现场演示采用真实或测试系统，其他演示方式不得分。 （演示时长不超过15分钟） 一、数据接口动态防护服务 1、前置机风险感知服务：支持展示当前服务器、进程、账户、软件应用、Web资产、Web服务、Web框架、数据库、端口、网络连接、启动服务、安装包、计划任务、环境变量、内核模块等分类资产数量统计，可对分类资产全局进行快速搜索。（1分） 2、攻击安全防护：提供攻击安全防护服务：对当前API服务端提供安全防护，可对API使用中常见的网络安全攻击进行感知和识别，包括SQL注入，XSS攻击，目录遍历，CC攻击，PHP注入，网站扫描，以及敏感信息访问等（1分） 二、数据安全总体态势感知服务 3、以数据流转的视角出发，按数据的来源和赋能维度实时统计各地市部门的数据采集数量及共享交换数量。（1分） 三、敏感数据安全态势感知服务 4、按敏感数据的安全风险进行统计及可视化展现，并可下钻和跳转展示告警详情；（1分） 四、敏感数据流转监测预警服务 5、提供基于业务应用场景，对其数据流经的节点，包括主机资产、应用服务、数据接口、数据、账号等，根据数据的流向，实现简单拖拽数据流节点的可视化元件，建立数据流程可视化图谱。（1分） 五、高级威胁监测服务 6、提供威胁分析可视化服务：实现从攻击者的视角发现入侵的痕迹从而加固整改“智慧医保”自身安全。基于攻击链的维度将攻击行为科学划分、告警深度调查分析，并以受害主机为线索还原整个攻击过程（侦察-入侵-命令控制-横向渗透-数据外泄-痕迹清理）和可视化展现和推演，来解决威胁分析过程可视化（1分） 7、提供云端联动服务：实现与云端威胁情报联动，可对攻击IP、C&C域名和恶意样本MD5进行一键搜索，查看基本信息、相关样本、关联URL、可视化分析、域名解析、注册信息、关联域名、数字证书等（1分） 8、提供威胁狩猎分析服务：实现对任意线索的自定义拓线及溯源取证分析，以可视化分析画布形式展示拓线过程并支持结果快照导出；对于给定线索的溯源结果展示，包括但不限于攻击溯源、失陷主机分析、暴力破解分析、弱口令分析等。（1分） 六、主动防御服务 9、提供蜜罐模版导入服务，可以配置蜜罐模版名称、服务名称、端口、硬件规格，类型包括高交互蜜罐、中交互蜜罐和低交互蜜罐（1分） 10、提供支持HTTP攻击流量进行诱骗服务，涵盖的Web攻击类型包括：文件读取、目录遍历、命令执行、代码执行、SQL注入、XSS等（1分）	0-10	0	2	3	10	9
17	技术	疫情防控措施。投标人提供项目实施期间疫情防控措施，根据措施的详细程度和可行性评分。	0-1	1	1	1	1	1
合计			0-90.0	26.5	58	31	87	80

专家（签名）：

技术商务资信评分明细（孙叶青）

项目名称：浙江省“智慧医保”安全运维及系统数据安全服务项目（ZJ-2142843）

序号	评分类型	评分项目内容	分值范围	杭州实在智能科技有限公司	杭州美创科技有限公司	浙江鼎顺信息工程有限公司	网神信息技术(北京)股份有限公司	北京神州绿盟科技有限公司
1	商务资信	①投标人具有ISO27001信息安全管理体认证、ISO20000信息技术服务管理体系认证、每个证书得1分，最高得2分； ②投标人具有国家信息安全测评中心颁发的信息安全服务资质（云计算安全类）的得1分；具有信息安全服务资质（安全开发类）的得1分。 提供以上有效证书扫描件，未提供的不得分。	0-4	2	4	0	4	4
2	商务资信	投标人自2018年1月1日（以合同签订时间为准）至今具有政务平台数据安全类服务业绩，提供合同扫描件作为证明材料，每份合同得0.5分，最多得2分，不提供的不得分。	0-2	0.5	2	1	2	2
3	商务资信	投标人自2018年1月1日（以合同签订时间为准）至今具有政务平台数据安全类产品业绩，提供合同扫描件作为证明材料，每份合同得0.5分，最多得2分，不提供的不得分。	0-2	0.5	2	2	2	2
4	技术	投标人对本项目的理解、对本项目背景、现状、目标、服务内容、部署环境等的理解。	0-3	1.5	2	1.5	2.5	2.5
5	技术	根据投标人数据安全管理制度咨询服务方案内容的完整性、方案的针对性和详细程度进行评分。	0-3	1.5	2	1.5	2.5	2.5
6	技术	根据投标人数据安全技术防护服务方案内容的完整性、方案的针对性和详细程度进行评分。	0-5	3	3.5	3	4	4
7	技术	根据投标人数据安全运营服务方案内容的完整性、方案的针对性和详细程度进行评分。	0-3	1.5	2.5	1.5	2.5	2.5
8	技术	采购需求中打★条款的响应情况。每个★条款符合要求的得2分，最高得14分	0-14	0	10	0	14	14
9	技术	采购需求中其余非★条款的响应情况。全部满足的得12分，不满足的每一项扣1分。未体现内的不得分。不满足项超过12项的视作明显不符合采购内容和质量标准，作无效标处理。	0-12	12	10	12	12	12
10	技术	组织实施方案，包括组织机构、实施场所、项目进度安排、项目人员安排、团队管理和沟通机制。根据投标文件体现的内容进行评分。	0-3	2	2.5	2	2.5	2.5
11.1	技术	专家组负责人（1人）具备以下专业证书： ①ISO27001Foundation、②ITIL（国际IT服务管理专业资格认证）、③人社部门颁发的信息系统项目管理师、④CISE注册信息安全工程师或CISP-PTE注册信息安全专业人员渗透测试工程师或CNVD（原创漏洞提交证明）或ITSM IT服务项目经理证书中的一本或多本。每一小项1分，满分4分。提供证书扫描件及参保证明（要求见上述注意事项），不提供的不得分。	0-4	0	3	0	4	4
11.2	技术	专家组成员（不含项目负责人）至少8人，否则本项不得分。人员具备以下专业证书：①CISE（注册信息安全工程师）、②CISP-PTE（注册信息安全专业人员渗透测试工程师）、③ITIL（国际IT服务管理专业资格认证）、④CNVD（原创漏洞提交证明），每本证书得0.5分，同一证书只计算一次，同一人最多计一本证书。本项最高得2分。提供证书扫描件及参保证明（要求见上述注意事项），不提供的不得分。	0-2	0	1	0	2	2

12.1	技术	项目负责人(1人)具备以下证书:①人社部门颁发的网络工程师(中级)、②CISA(信息系统审计师)、③人社部门颁发的信息系统项目管理师,④CISO注册信息安全管理人员证书或ISCCC信息安全体系内审员证书或ITSS-IT服务工程师证书中的一本或多本。每一小项1分,满分4分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-4	0	3	0	4	2
12.2	技术	实施人员(不含项目负责人)至少10人,否则本项不得分。人员具备以下专业证书:①CISO(注册信息安全管理人员)、②人社部门颁发的信息系统项目管理师、③ITSS(IT服务工程师)、④ISCCC(信息安全体系内审员),每本证书得0.5分,同一证书只计算一次,同一人最多计一本证书。本项最高得2分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-2	0	1	0	2	1.5
13.1	技术	驻场负责人(1人)具备以下专业证书:①CISD(注册信息安全开发人员)、②CISSP(信息系统安全专业认证)、③CCSSP(云安全系统认证专家)、④CISE注册信息安全工程师或CISI注册信息安全讲师或CISAW信息安全从业人员认证或CISO注册信息安全管理人员。每一小项1分,满分4分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-4	0	2	0	4	3
13.2	技术	驻场负责人自2018年1月1日以来曾以项目负责人身份从事过政务平台数据安全类服务业绩的0.5分。提供能体现项目负责人姓名的合同或业主证明扫描件。未提供的不得分。此项业绩与序号2的投标人业绩不重复得分。	0-0.5	0	0	0	0.5	0
13.3	技术	驻场成员(不含项目负责人)至少5人,否则本项不得分。人员具备以下专业证书:①CISE(注册信息安全工程师)、②CISAW(信息安全从业人员认证)、③CISO(注册信息安全管理人员)。每本证书得0.5分,同一证书只计算一次,同一人最多计一本证书。本项最高得1.5分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-1.5	0	1.5	0	1.5	1.5
14.1	技术	讲师团队负责人(1人)具备以下专业证书:①CDGA证书(数据治理工程师)、②CCSK(云安全知识认证)、③ISO27001LA、④CISAW(信息安全从业人员认证)或CISI注册信息安全讲师。每一小项0.5分,满分2分。提供证书扫描件,不提供的不得分。	0-2	0	0.5	0	2	1.5
14.2	技术	专业讲师(不含专家讲师)至少6人,否则本项不得分。人员具备以下专业证书:①CISI(注册信息安全讲师)、②CCSK(云安全知识认证)、③CDPSE(数据隐私解决方案工程师认证)、④ISO27001LA(信息安全管理体系主任审核员)。每本证书得0.5分,同一证书只计算一次,同一人最多计一本证书。本项最高得2分。提供证书扫描件,不提供的不得分。	0-2	0	1.5	0	2	1.5
15.1	技术	远程专家团队负责人(1人)具备以下专业证书:①CISA(信息系统审计师)、②CNVD(原创漏洞证明)、③CISSP(信息系统安全专业认证)、④CISO注册信息安全管理人员或CISP-PTE注册信息安全专业人员渗透测试工程师或ISO27001LA信息安全管理体系主任审核员或CISAW信息安全从业人员认证。每一小项1分,满分4分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-4	0	2	0	4	4

15.2	技术	远程专家（不含项目负责人）至少30人，否则本项不得分。人员具备以下专业证书：①CISP-PTS（注册渗透测试专家）10人以上、②CZTP（零信任专家认证）证书10人以上、③CISP-IRE（注册应急响应工程师）5名以上、④EIACE（高级网络信息安全工程师）5名以上。每一小项0.5分，满分2分。提供证书扫描件及参保证明（要求见上述注意事项），不提供的不得分。	0-2	0	0	0	2	1
16	技术	现场演示采用真实或测试系统，其他演示方式不得分。 （演示时长不超过15分钟） 一、数据接口动态防护服务 1、前置机风险感知服务：支持展示当前服务器、进程、账户、软件应用、Web资产、Web服务、Web框架、数据库、端口、网络连接、启动服务、安装包、计划任务、环境变量、内核模块等分类资产数量统计，可对分类资产全局进行快速搜索。（1分） 2、攻击安全防护：提供攻击安全防护服务：对当前API服务端提供安全防护，可对API使用中常见的网络安全攻击进行感知和识别，包括SQL注入，XSS攻击，目录遍历，CC攻击，PHP注入，网站扫描，以及敏感信息访问等（1分） 二、数据安全总体态势感知服务 3、以数据流转的视角出发，按数据的来源和赋能维度实时统计各地市部门的数据采集数量及共享交换数量。（1分） 三、敏感数据安全态势感知服务 4、按敏感数据的安全风险进行统计及可视化展现，并可下钻和跳转展示告警详情；（1分） 四、敏感数据流转监测预警服务 5、提供基于业务应用场景，对其数据流经的节点，包括主机资产、应用服务、数据接口、数据、账号等，根据数据的流向，实现简单拖拽数据流节点的可视化元件，建立数据流程可视化图谱。（1分） 五、高级威胁监测服务 6、提供威胁分析可视化服务：实现从攻击者的视角发现入侵的痕迹从而加固整改“智慧医保”自身安全。基于攻击链的维度将攻击行为科学划分、告警深度调查分析，并以受害主机为线索还原整个攻击过程（侦察-入侵-命令控制-横向渗透-数据外泄-痕迹清理）和可视化展现和推演，来解决威胁分析过程可视化（1分） 7、提供云端联动服务：实现与云端威胁情报联动，可对攻击IP、C&C域名和恶意样本MD5进行一键搜索，查看基本信息、相关样本、关联URL、可视化分析、域名解析、注册信息、关联域名、数字证书等（1分） 8、提供威胁狩猎分析服务：实现对任意线索的自定义拓线及溯源取证分析，以可视化分析画布形式展示拓线过程并支持结果快照导出；对于给定线索的溯源结果展示，包括但不限于攻击溯源、失陷主机分析、暴力破解分析、弱口令分析等。（1分） 六、主动防御服务 9、提供蜜罐模版导入服务，可以配置蜜罐模版名称、服务名称、端口、硬件规格，类型包括高交互蜜罐、中交互蜜罐和低交互蜜罐（1分） 10、提供支持HTTP攻击流量进行诱骗服务，涵盖的Web攻击类型包括：文件读取、目录遍历、命令执行、代码执行、SQL注入、XSS等（1分）	0-10	0	2	3	10	9
17	技术	疫情防控措施。投标人提供项目实施期间疫情防控措施，根据措施的详细程度和可行性评分。	0-1	1	1	1	1	1
合计			0-90.0	25.5	59	28.5	87	80

专家（签名）：

技术商务资信评分明细（姜力）

项目名称：浙江省“智慧医保”安全运维及系统数据安全服务项目（ZJ-2142843）

序号	评分类型	评分项目内容	分值范围	杭州实在智能科技有限公司	杭州美创科技有限公司	浙江鼎顺信息工程有限公司	网神信息技术(北京)股份有限公司	北京神州绿盟科技有限公司
1	商务资信	①投标人具有ISO27001信息安全管理体认证、ISO20000信息技术服务管理体系认证、每个证书得1分，最高得2分； ②投标人具有国家信息安全测评中心颁发的信息安全服务资质（云计算安全类）的得1分；具有信息安全服务资质（安全开发类）的得1分。 提供以上有效证书扫描件，未提供的不得分。	0-4	2	4	0	4	4
2	商务资信	投标人自2018年1月1日（以合同签订时间为准）至今具有政务平台数据安全类服务业绩，提供合同扫描件作为证明材料，每份合同得0.5分，最多得2分，不提供的不得分。	0-2	0.5	2	1	2	2
3	商务资信	投标人自2018年1月1日（以合同签订时间为准）至今具有政务平台数据安全类产品业绩，提供合同扫描件作为证明材料，每份合同得0.5分，最多得2分，不提供的不得分。	0-2	0.5	2	2	2	2
4	技术	投标人对本项目的理解、对本项目背景、现状、目标、服务内容、部署环境等的理解。	0-3	2.5	2	2	3	3
5	技术	根据投标人数据安全管理制度咨询服务方案的完整性、方案的针对性和详细程度进行评分。	0-3	2	1.5	2	3	3
6	技术	根据投标人数据安全技术防护服务方案的完整性、方案的针对性和详细程度进行评分。	0-5	2.5	3	3	4.5	4.5
7	技术	根据投标人数据安全运营服务方案的完整性、方案的针对性和详细程度进行评分。	0-3	1.5	2	2	3	3
8	技术	采购需求中打★条款的响应情况。每个★条款符合要求的得2分，最高得14分	0-14	0	10	0	14	14
9	技术	采购需求中其余非★条款的响应情况。全部满足的得12分，不满足的每一项扣1分。未体现内的不得分。不满足项超过12项的视作明显不符合采购内容和质量标准，作无效标处理。	0-12	12	10	12	12	12
10	技术	组织实施方案，包括组织机构、实施场所、项目进度安排、项目人员安排、团队管理和沟通机制。根据投标文件体现的内容进行评分。	0-3	2	1.5	2	3	3
11.1	技术	专家组负责人（1人）具备以下专业证书： ①ISO27001Foundation、②ITIL（国际IT服务管理专业资格认证）、③人社部门颁发的信息系统项目管理师、④CISE注册信息安全工程师或CISP-PTE注册信息安全专业人员渗透测试工程师或CNVD（原创漏洞提交证明）或ITSM IT服务项目经理证书中的一本或多本。每一小项1分，满分4分。提供证书扫描件及参保证明（要求见上述注意事项），不提供的不得分。	0-4	0	3	0	4	4
11.2	技术	专家组成员（不含项目负责人）至少8人，否则本项不得分。人员具备以下专业证书：①CISE（注册信息安全工程师）、②CISP-PTE（注册信息安全专业人员渗透测试工程师）、③ITIL（国际IT服务管理专业资格认证）、④CNVD（原创漏洞提交证明），每本证书得0.5分，同一证书只计算一次，同一人最多计一本证书。本项最高得2分。提供证书扫描件及参保证明（要求见上述注意事项），不提供的不得分。	0-2	0	1	0	2	2

12.1	技术	项目负责人(1人)具备以下证书:①人社部门颁发的网络工程师(中级)、②CISA(信息系统审计师)、③人社部门颁发的信息系统项目管理师,④CISO注册信息安全管理人员证书或ISCCC信息安全体系内审员证书或ITSS-IT服务工程师证书中的一本或多本。每一小项1分,满分4分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-4	0	3	0	4	2
12.2	技术	实施人员(不含项目负责人)至少10人,否则本项不得分。人员具备以下专业证书:①CISO(注册信息安全管理人员)、②人社部门颁发的信息系统项目管理师、③ITSS(IT服务工程师)、④ISCCC(信息安全体系内审员),每本证书得0.5分,同一证书只计算一次,同一人最多计一本证书。本项最高得2分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-2	0	1	0	2	1.5
13.1	技术	驻场负责人(1人)具备以下专业证书:①CISD(注册信息安全开发人员)、②CISSP(信息系统安全专业认证)、③CCSSP(云安全系统认证专家)、④CISE注册信息安全工程师或CISI注册信息安全讲师或CISAW信息安全从业人员认证或CISO注册信息安全管理人员。每一小项1分,满分4分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-4	0	2	0	4	3
13.2	技术	驻场负责人自2018年1月1日以来曾以项目负责人身份从事过政务平台数据安全类服务业绩的0.5分。提供能体现项目负责人姓名的合同或业主证明扫描件。未提供的不得分。此项业绩与序号2的投标人业绩不重复得分。	0-0.5	0	0	0	0.5	0
13.3	技术	驻场成员(不含项目负责人)至少5人,否则本项不得分。人员具备以下专业证书:①CISE(注册信息安全工程师)、②CISAW(信息安全从业人员认证)、③CISO(注册信息安全管理人员)。每本证书得0.5分,同一证书只计算一次,同一人最多计一本证书。本项最高得1.5分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-1.5	0	1.5	0	1.5	1.5
14.1	技术	讲师团队负责人(1人)具备以下专业证书:①CDGA证书(数据治理工程师)、②CCSK(云安全知识认证)、③ISO27001LA、④CISAW(信息安全从业人员认证)或CISI注册信息安全讲师。每一小项0.5分,满分2分。提供证书扫描件,不提供的不得分。	0-2	0	0.5	0	2	1.5
14.2	技术	专业讲师(不含专家讲师)至少6人,否则本项不得分。人员具备以下专业证书:①CISI(注册信息安全讲师)、②CCSK(云安全知识认证)、③CDPSE(数据隐私解决方案工程师认证)、④ISO27001LA(信息安全管理体系主任审核员)。每本证书得0.5分,同一证书只计算一次,同一人最多计一本证书。本项最高得2分。提供证书扫描件,不提供的不得分。	0-2	0	1.5	0	2	1.5
15.1	技术	远程专家团队负责人(1人)具备以下专业证书:①CISA(信息系统审计师)、②CNVD(原创漏洞证明)、③CISSP(信息系统安全专业认证)、④CISO注册信息安全管理人员或CISP-PTE注册信息安全专业人员渗透测试工程师或ISO27001LA信息安全管理体系主任审核员或CISAW信息安全从业人员认证。每一小项1分,满分4分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-4	0	2	0	4	4

15.2	技术	远程专家（不含项目负责人）至少30人，否则本项不得分。人员具备以下专业证书：①CISP-PTS（注册渗透测试专家）10人以上、②CZTP（零信任专家认证）证书10人以上、③CISP-IRE（注册应急响应工程师）5名以上、④EIACE（高级网络信息安全工程师）5名以上。每一小项0.5分，满分2分。提供证书扫描件及参保证明（要求见上述注意事项），不提供的不得分。	0-2	0	0	0	2	1
16	技术	现场演示采用真实或测试系统，其他演示方式不得分。 （演示时长不超过15分钟） 一、数据接口动态防护服务 1、前置机风险感知服务：支持展示当前服务器、进程、账户、软件应用、Web资产、Web服务、Web框架、数据库、端口、网络连接、启动服务、安装包、计划任务、环境变量、内核模块等分类资产数量统计，可对分类资产全局进行快速搜索。（1分） 2、攻击安全防护：提供攻击安全防护服务：对当前API服务端提供安全防护，可对API使用中常见的网络安全攻击进行感知和识别，包括SQL注入，XSS攻击，目录遍历，CC攻击，PHP注入，网站扫描，以及敏感信息访问等（1分） 二、数据安全总体态势感知服务 3、以数据流转的视角出发，按数据的来源和赋能维度实时统计各地市部门的数据采集数量及共享交换数量。（1分） 三、敏感数据安全态势感知服务 4、按敏感数据的安全风险进行统计及可视化展现，并可下钻和跳转展示告警详情；（1分） 四、敏感数据流转监测预警服务 5、提供基于业务应用场景，对其数据流经的节点，包括主机资产、应用服务、数据接口、数据、账号等，根据数据的流向，实现简单拖拽数据流节点的可视化元件，建立数据流程可视化图谱。（1分） 五、高级威胁监测服务 6、提供威胁分析可视化服务：实现从攻击者的视角发现入侵的痕迹从而加固整改“智慧医保”自身安全。基于攻击链的维度将攻击行为科学划分、告警深度调查分析，并以受害主机为线索还原整个攻击过程（侦察-入侵-命令控制-横向渗透-数据外泄-痕迹清理）和可视化展现和推演，来解决威胁分析过程可视化（1分） 7、提供云端联动服务：实现与云端威胁情报联动，可对攻击IP、C&C域名和恶意样本MD5进行一键搜索，查看基本信息、相关样本、关联URL、可视化分析、域名解析、注册信息、关联域名、数字证书等（1分） 8、提供威胁狩猎分析服务：实现对任意线索的自定义拓线及溯源取证分析，以可视化分析画布形式展示拓线过程并支持结果快照导出；对于给定线索的溯源结果展示，包括但不限于攻击溯源、失陷主机分析、暴力破解分析、弱口令分析等。（1分） 六、主动防御服务 9、提供蜜罐模版导入服务，可以配置蜜罐模版名称、服务名称、端口、硬件规格，类型包括高交互蜜罐、中交互蜜罐和低交互蜜罐（1分） 10、提供支持HTTP攻击流量进行诱骗服务，涵盖的Web攻击类型包括：文件读取、目录遍历、命令执行、代码执行、SQL注入、XSS等（1分）	0-10	0	2	3	10	9
17	技术	疫情防控措施。投标人提供项目实施期间疫情防控措施，根据措施的详细程度和可行性评分。	0-1	1	1	1	1	1
合计			0-90.0	26.5	56.5	30	89.5	82.5

专家（签名）：

技术商务资信评分明细（吴洪森）

项目名称：浙江省“智慧医保”安全运维及系统数据安全服务项目（ZJ-2142843）

序号	评分类型	评分项目内容	分值范围	杭州实在智能科技有限公司	杭州美创科技有限公司	浙江鼎顺信息工程有限公司	网神信息技术(北京)股份有限公司	北京神州绿盟科技有限公司
1	商务资信	①投标人具有ISO27001信息安全管理体认证、ISO20000信息技术服务管理体系认证、每个证书得1分，最高得2分； ②投标人具有国家信息安全测评中心颁发的信息安全服务资质（云计算安全类）的得1分；具有信息安全服务资质（安全开发类）的得1分。 提供以上有效证书扫描件，未提供的不得分。	0-4	2	4	0	4	4
2	商务资信	投标人自2018年1月1日（以合同签订时间为准）至今具有政务平台数据安全类服务业绩，提供合同扫描件作为证明材料，每份合同得0.5分，最多得2分，不提供的不得分。	0-2	0.5	2	1	2	2
3	商务资信	投标人自2018年1月1日（以合同签订时间为准）至今具有政务平台数据安全类产品业绩，提供合同扫描件作为证明材料，每份合同得0.5分，最多得2分，不提供的不得分。	0-2	0.5	2	2	2	2
4	技术	投标人对本项目的理解、对本项目背景、现状、目标、服务内容、部署环境等的理解。	0-3	1	2	1	2.5	2
5	技术	根据投标人数据安全管理制度咨询服务方案内容的完整性、方案的针对性和详细程度进行评分。	0-3	1	2	1	2	2
6	技术	根据投标人数据安全技术防护服务方案内容的完整性、方案的针对性和详细程度进行评分。	0-5	1	2	1	4	3
7	技术	根据投标人数据安全运营服务方案内容的完整性、方案的针对性和详细程度进行评分。	0-3	1	2	1	2	2
8	技术	采购需求中打★条款的响应情况。每个★条款符合要求的得2分，最高得14分	0-14	0	10	0	14	14
9	技术	采购需求中其余非★条款的响应情况。全部满足的得12分，不满足的每一项扣1分。未体现内的不得分。不满足项超过12项的视作明显不符合采购内容和质量标准，作无效标处理。	0-12	12	10	12	12	12
10	技术	组织实施方案，包括组织机构、实施场所、项目进度安排、项目人员安排、团队管理和沟通机制。根据投标文件体现的内容进行评分。	0-3	1	2	1	2.5	2
11.1	技术	专家组负责人（1人）具备以下专业证书： ①ISO27001Foundation、②ITIL（国际IT服务管理专业资格认证）、③人社部门颁发的信息系统项目管理师、④CISE注册信息安全工程师或CISP-PTE注册信息安全专业人员渗透测试工程师或CNVD（原创漏洞提交证明）或ITSM IT服务项目经理证书中的一本或多本。每一小项1分，满分4分。提供证书扫描件及参保证明（要求见上述注意事项），不提供的不得分。	0-4	0	3	0	4	4
11.2	技术	专家组成员（不含项目负责人）至少8人，否则本项不得分。人员具备以下专业证书：①CISE（注册信息安全工程师）、②CISP-PTE（注册信息安全专业人员渗透测试工程师）、③ITIL（国际IT服务管理专业资格认证）、④CNVD（原创漏洞提交证明），每本证书得0.5分，同一证书只计算一次，同一人最多计一本证书。本项最高得2分。提供证书扫描件及参保证明（要求见上述注意事项），不提供的不得分。	0-2	0	1	0	2	2

12.1	技术	项目负责人(1人)具备以下证书:①人社部门颁发的网络工程师(中级)、②CISA(信息系统审计师)、③人社部门颁发的信息系统项目管理师,④CISO注册信息安全管理证书或ISCCC信息安全体系内审员证书或ITSS-IT服务工程师证书中的一本或多本。每一小项1分,满分4分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-4	0	3	0	4	2
12.2	技术	实施人员(不含项目负责人)至少10人,否则本项不得分。人员具备以下专业证书:①CISO(注册信息安全管理证书)、②人社部门颁发的信息系统项目管理师、③ITSS(IT服务工程师)、④ISCCC(信息安全体系内审员),每本证书得0.5分,同一证书只计算一次,同一人最多计一本证书。本项最高得2分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-2	0	1	0	2	1.5
13.1	技术	驻场负责人(1人)具备以下专业证书:①CISD(注册信息安全开发人员)、②CISSP(信息系统安全专业认证)、③CCSSP(云安全系统认证专家)、④CISE注册信息安全工程师或CISI注册信息安全讲师或CISAW信息安全从业人员认证或CISO注册信息安全管理证书。每一小项1分,满分4分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-4	0	2	0	4	3
13.2	技术	驻场负责人自2018年1月1日以来曾以项目负责人身份从事过政务平台数据安全类服务业绩的0.5分。提供能体现项目负责人姓名的合同或业主证明扫描件。未提供的不得分。此项业绩与序号2的投标人业绩不重复得分。	0-0.5	0	0	0	0.5	0
13.3	技术	驻场成员(不含项目负责人)至少5人,否则本项不得分。人员具备以下专业证书:①CISE(注册信息安全工程师)、②CISAW(信息安全从业人员认证)、③CISO(注册信息安全管理证书)。每本证书得0.5分,同一证书只计算一次,同一人最多计一本证书。本项最高得1.5分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-1.5	0	1.5	0	1.5	1.5
14.1	技术	讲师团队负责人(1人)具备以下专业证书:①CDGA证书(数据治理工程师)、②CCSK(云安全知识认证)、③ISO27001LA、④CISAW(信息安全从业人员认证)或CISI注册信息安全讲师。每一小项0.5分,满分2分。提供证书扫描件,不提供的不得分。	0-2	0	0.5	0	2	1.5
14.2	技术	专业讲师(不含专家讲师)至少6人,否则本项不得分。人员具备以下专业证书:①CISI(注册信息安全讲师)、②CCSK(云安全知识认证)、③CDPSE(数据隐私解决方案工程师认证)、④ISO27001LA(信息安全管理主任审核员)。每本证书得0.5分,同一证书只计算一次,同一人最多计一本证书。本项最高得2分。提供证书扫描件,不提供的不得分。	0-2	0	1.5	0	2	1.5
15.1	技术	远程专家团队负责人(1人)具备以下专业证书:①CISA(信息系统审计师)、②CNVD(原创漏洞证明)、③CISSP(信息系统安全专业认证)、④CISO注册信息安全管理证书或CISP-PTE注册信息安全专业人员渗透测试工程师或ISO27001LA信息安全管理主任审核员或CISAW信息安全从业人员认证。每一小项1分,满分4分。提供证书扫描件及参保证明(要求见上述注意事项),不提供的不得分。	0-4	0	2	0	4	4

15.2	技术	远程专家（不含项目负责人）至少30人，否则本项不得分。人员具备以下专业证书：①CISP-PTS（注册渗透测试专家）10人以上、②CZTP（零信任专家认证）证书10人以上、③CISP-IRE（注册应急响应工程师）5名以上、④EIACE（高级网络信息安全工程师）5名以上。每一小项0.5分，满分2分。提供证书扫描件及参保证明（要求见上述注意事项），不提供的不得分。	0-2	0	0	0	2	1
16	技术	现场演示采用真实或测试系统，其他演示方式不得分。 （演示时长不超过15分钟） 一、数据接口动态防护服务 1、前置机风险感知服务：支持展示当前服务器、进程、账户、软件应用、Web资产、Web服务、Web框架、数据库、端口、网络连接、启动服务、安装包、计划任务、环境变量、内核模块等分类资产数量统计，可对分类资产全局进行快速搜索。（1分） 2、攻击安全防护：提供攻击安全防护服务：对当前API服务端提供安全防护，可对API使用中常见的网络安全攻击进行感知和识别，包括SQL注入，XSS攻击，目录遍历，CC攻击，PHP注入，网站扫描，以及敏感信息访问等（1分） 二、数据安全总体态势感知服务 3、以数据流转的视角出发，按数据的来源和赋能维度实时统计各地市部门的数据采集数量及共享交换数量。（1分） 三、敏感数据安全态势感知服务 4、按敏感数据的安全风险进行统计及可视化展现，并可下钻和跳转展示告警详情；（1分） 四、敏感数据流转监测预警服务 5、提供基于业务应用场景，对其数据流经的节点，包括主机资产、应用服务、数据接口、数据、账号等，根据数据的流向，实现简单拖拽数据流节点的可视化元件，建立数据流程可视化图谱。（1分） 五、高级威胁监测服务 6、提供威胁分析可视化服务：实现从攻击者的视角发现入侵的痕迹从而加固整改“智慧医保”自身安全。基于攻击链的维度将攻击行为科学划分、告警深度调查分析，并以受害主机为线索还原整个攻击过程（侦察-入侵-命令控制-横向渗透-数据外泄-痕迹清理）和可视化展现和推演，来解决威胁分析过程可视化（1分） 7、提供云端联动服务：实现与云端威胁情报联动，可对攻击IP、C&C域名和恶意样本MD5进行一键搜索，查看基本信息、相关样本、关联URL、可视化分析、域名解析、注册信息、关联域名、数字证书等（1分） 8、提供威胁狩猎分析服务：实现对任意线索的自定义拓线及溯源取证分析，以可视化分析画布形式展示拓线过程并支持结果快照导出；对于给定线索的溯源结果展示，包括但不限于攻击溯源、失陷主机分析、暴力破解分析、弱口令分析等。（1分） 六、主动防御服务 9、提供蜜罐模版导入服务，可以配置蜜罐模版名称、服务名称、端口、硬件规格，类型包括高交互蜜罐、中交互蜜罐和低交互蜜罐（1分） 10、提供支持HTTP攻击流量进行诱骗服务，涵盖的Web攻击类型包括：文件读取、目录遍历、命令执行、代码执行、SQL注入、XSS等（1分）	0-10	0	2	3	10	9
17	技术	疫情防控措施。投标人提供项目实施期间疫情防控措施，根据措施的详细程度和可行性评分。	0-1	1	1	1	1	1
合计			0-90.0	21	56.5	24	86	77

专家（签名）：