浙江省科学技术奖公示信息表

提名奖项：科学技术进步奖

|  |  |
| --- | --- |
| 成果名称 | 复杂网络环境的安全态势感知与先进防控技术及应用 |
| 提名等级 | 一等奖 |
| **提名书**  **相关内容** | 1、提名书的主要知识产权和标准规范目录   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **知识产权名称** | **类别** | **国家** | **授权号** | **发明人** | | 一种提高三层关联精准度的方法 | 发明专利 | 中国 | ZL201510757700.X | 李绍平、范渊、龙文洁 | | 快速检测SYN Flood攻击的方法及装置 | 发明专利 | 中国 | ZL201710807649.8 | 莫凡、范渊、刘博、龙文洁 | | 基于统计模型的智能地名识别技术 | 发明专利 | 中国 | ZL201410381574.8 | 陈则润、吴鸣旦、范渊 | | 一种基于分词算法的日志解析方法及系统 | 发明专利 | 中国 | ZL201410604098.1 | 谈修竹、范渊 | | 基于文件系统过滤驱动实现沙箱虚拟机多样本运行的方法 | 发明专利 | 中国 | ZL201510455976.2 | 李凯、范渊、吴卓群、寇大强 | | 一种Oracle传输压缩数据还原方法 | 发明专利 | 中国 | ZL201410381264.6 | 李绍平、范渊 |   2、主要代表性论文目录   |  |  |  |  | | --- | --- | --- | --- | | **作 者** | **论文（专著）名称/刊物** | **年卷**  **页码** | **发表**  **时间**  **（年、月）** | | Haifeng Zhou, Liansheng Tan, Qian Zeng and Chunming Wu | Traffic Matrix Estimation: A Neural Network Approach with Extended Input and Expectation Maximization Iteration/ Journal of Network and Computer Applications | 卷: 60  页: 220-232 | 2016年1月 | | Hanguang Luo, Guangjun Wen, Jian Su, Zhong Huang, Inserra Daniele | Multihop Distance-Bounding For Improving Security and Efficiency of Ad-Hoc Networks/ IEEE Internet of Things Journal | 卷: 6  期: 3  页: 5312-5323 | 2019年6月 | | Chunhua Ju; Wanqiong Tao | A novel relationship strength model for online social networks/ Multimedia Tools and Applications | 卷: ‏76 期: ‏16 页: 17577-17594 | 2017年8月 | | 苗春雨,陈丽娜,吴建军，周家庆，冯旭杭 | 无线传感器网络节点位置验证框架/计算机研究与发展 | 卷: 56  期: 6  页：1231-1243 | 2019年6月 | |
| **主要完成人** | |  |  |  |  | | --- | --- | --- | --- | | **姓名** | **排名** | **技术职称** | **工作单位** | | 范渊 | 1 | 教授级高级工程师 | 杭州安恒信息技术股份有限公司 | | 刘博 | 2 | 工程师 | 杭州安恒信息技术股份有限公司 | | 吴春明 | 3 | 教授 | 浙江大学 | | 李顺斌 | 4 | 助理研究员 | 之江实验室 | | 琚春华 | 5 | 教授 | 浙江工商大学 | | 周海峰 | 6 | 工程师 | 浙江大学 | | 苗春雨 | 7 | 高级工程师 | 杭州安恒信息技术股份有限公司 | | 骆汉光 | 8 | 助理研究员 | 之江实验室 | | 吴卓群 | 9 | 高级工程师 | 杭州安恒信息技术股份有限公司 | | 谈修竹 | 10 | 工程师 | 杭州安恒信息技术股份有限公司 | | 聂桂兵 | 11 | 工程师 | 杭州安恒信息技术股份有限公司 | | 潘宇 | 12 | 工程师 | 之江实验室 | | 莫凡 | 13 | 工程师 | 杭州安恒信息技术股份有限公司 | |
| **主要完成单位** | 1、杭州安恒信息技术股份有限公司  2、之江实验室  3、浙江大学  4、浙江工商大学 |
| 提名单位 | 杭州市人民政府 |
| 提名意见 | 该成果在安全事件关联推理及响应技术、认知攻击循环建模技术、IPv4/IPv6混合网络环境资产识别技术、自适应云安全智能防控技术、可扩展的安全分析插件模块化技术等方面进行了深入系统的研究，研究成果是面向互联网、大型特定活动组网、公有云和企业云、工业互联网等复杂网络环境的安全态势感知于与先进防控平台。项目成果具有方案灵活、立体防护、技术领先、高性价比等优势，解决了复杂网络环境中的安全事件智能分析、检测、溯源及自动化编排响应等关键问题，并在安全事件关联推理及响应、高级隐蔽性威胁检测、IPv4/IPv6混合网络环境资产识别、云安全智能防控等方面取得了突破性成果。  成果孵化产品经国家网络与信息系统安全产品质量监督检验中心、公安部计算机信息系统安全产品质量监督检验中心、公安部信息安全产品检测中心检验检测，所检指标符合相关标准要求，产品性能优异。产品已在党政机关、金融、电信、能源等行业和互联网企业规模化应用，获得国家网信办、公安部、财政部、人社部等部门好评，社会和经济效益显著。项目核心关键技术已获发明专利30件，软件著作权21件，发表论文16篇，作为主要起草单位制订国家标准8项、行业标准3项，总体技术处国际先进水平，其中安全事件关联推理及响应和混合网络环境资产识别技术处国际领先水平。  该成果具有良好的推广价值和应用前景，近三年累计销售收入141681.16万元，取得了显著的经济效益和社会效益，极大促进了行业科技进步。同意推荐申报浙江省科技进步奖一等奖。 |

**浙江省科学技术奖完成单位公示信息补充材料**

**一、成果名称**

复杂网络环境的安全态势感知与先进防控技术及应用

**二、提名奖励等级**

一等奖

**三、成果简介**

网络空间已成为陆海空天之外的第五大国家主权空间，保卫网络安全就是保卫国家主权。网络安全态势感知与智能防控是构建我国网络空间安全保障体系的核心技术和基础。国外厂商的安全产品较为成熟，但并不能完全符合我国信息安全等级保护建设及检查的相关要求国内安全产品。国内态势感知产品尚不完善，缺少全局的、多维度的检测视角，在多环境应用、异构安全数据关联分析、安全要素统一管理调度、隐蔽威胁检测、资产识别等方面提出挑战。

在应对上述挑战过程中，本成果在以下关键技术中取得了突破：

1、提出安全事件自动化关联推理及响应技术，创新性地提出安全知识图谱，实现复杂网络环境下关联推理、溯源、攻击范围感知以及自动化编排响应，有效构建安全闭环，提高安全运维效率50%以上；

2、提出认知攻击循环建模技术，实现隐蔽性攻击循环路径认知和攻击行为的循环关联建模，有效检测高级隐蔽性威胁，与现有检测方法相比，检出率提高80%；

3、提出IPv4和IPv6混合网络双栈协议识别以及资产智能识别，实现资产重识别和资产地址归一化，解决复杂网络环境内中的审计日志资产识别技术难题，进一步帮助实现安全事件定位和溯源分析等深度分析；

4、提出云环境下自学习检测场景技术，结合不同安全事件的关联性、先后逻辑和对网络系统的依赖关系分析，重点实现特定的云安全分析场景；

5、提出可扩展的安全分析插件模块化技术，实现对于安全事件源推论，安全威胁场景化和模块化功能，提供复杂安全威胁的最小化建模能力，提供5种安全建模能力。

该成果形成国家和行业标准11项，获得国家发明专利授权30项，在IoT、JNCA、TC、GLOBECOM、ICC等期刊会议发表论文16篇，形成论著6本，获得软件著作权21项。应用处于国内领先，国际先进水平。

该成果支持流量数据、日志数据、弱点数据、情报数据等1000+种设备、2000+种协议的数据；日志数据采集延迟低于20秒，流量数据采集延迟低于20秒；数据处理规模达到300K+EPS；支持每天大约30-50亿条数据存储，存储量为4T/日；紧急安全事件能在10秒内进行告警；原始数据检索响应≤8秒，分析结果检索响应≤2秒；性能支持8G /分钟，1千万条／分钟的数据规模。

该成果已在国家政府机关、测评机构、公安、金融、运营商、教育、能源等行业规模化应用，圆满完成G20峰会、进出口博览会等多项重大活动的网络安全保障工作，获得国家网信办、公安部、财政部、人社部等部门好评。截至2019年12月底，产生销售收入141681.16万元；

该成果形成良好的网络安全产业生态系统，促进区域经济社会健康发展。

**四、第三方评价**

1、查新报告

评价单位：浙江省科技信息研究院

报告编号：202033B2109520

结论：该项目研究技术其他文献中未见具体述及。

2、科学技术成果鉴定评价

组织鉴定单位：浙江火炬科技评估中心

编号：浙火鉴字[2020]第19号

结论：项目研发了网络安全态势感知通报预警平台、AiLPHA大数据智能安全平台、天池云安全管理平台、APT攻击（网络战）预警平台、工业防火墙等产品，解决了包括互联网、大型特定活动组网、公有云和企业云、工业互联网等复杂网络环境下的安全事件智能分析、检测、溯源及自动化编排响应等关键技术，在安全事件关联推理及响应、高级隐蔽性威胁检测、IPv4/IPv6混合网络环境资产识别、云安全智能防控等方面取得了突破性成果。核心关键技术已获发明专利30件，软件著作权21件，发表论文16篇，作为主要起草单位制订国家标准8项、行业标准3项，总体技术处国际先进水平，其中安全事件关联推理及响应和混合网络环境资产识别技术处国际领先水平。

**五、推广应用情况、经济效益和社会效益**

**1、推广应用情况**

该成果具有方案灵活、立体防护、技术领先、高性价比等优势，解决了复杂网络环境中的安全事件智能分析、检测、溯源及自动化编排响应等关键问题，并在安全事件关联推理及响应、高级隐蔽性威胁检测、IPv4/IPv6混合网络环境资产识别、云安全智能防控等方面取得了突破性成果。

该成果已在国家政府机关、测评机构、公安、金融、运营商、教育、能源等行业规模化应用，圆满完成G20峰会、进出口博览会等多项重大活动的网络安全保障工作，获得国家网信办、公安部、财政部、人社部等部门好评。

**2、经济效益**

通过实施，杭州安恒信息技术股份有限公司2017-2019年与该成果相关产品等业务销售收入为141681.16万元。

**3、社会效益**

该成果已实现大规模应用，产生了明显的社会效益。

1、助力国家网络安全态势感知建设，将大数据、人工智能等技术应用于安全行业，研发具有自主知识产权产品，并完成国产化硬件适配，综合提升了我国网安全行业的自主可控力度；

2、应用于国家重要部门及重大行业，为国家政府机关、国家测评机构、国家公安等单位，金融、运营商、能源、电力、教育等行业提供持续的安全监测、运营及态势感知能力，得到客户认可；

3、保障国家重大活动网络安全，为G20峰会、世界互联网大会、金砖国家峰会、中国国际进口博览会等大型会议活动提供网络安全保障支撑，保障期间，平均监测和拦截数十万次网络攻击，保障重大活动顺利举行，获得国家网信办、公安部、财政部、人社部等部门一致好评；

4、保障国家重大活动网络安全，为G20峰会、世界互联网大会、金砖国家峰会、中国国际进口博览会等大型会议活动提供网络安全保障支撑，保障期间，平均监测和拦截数十万次网络攻击，保障重大活动顺利举行，获得国家网信办、公安部、财政部、人社部等部门一致好评；

5、形成国家标准8项，行业标准3项，与中国信息通信研究院联合发布UEBA、SOAR方向技术白皮书2本，为网安行业前沿技术研究提供指导；

6、为社会培养大批网络安全人才，与国家信息中心、之江实验室、浙江大学、浙江工商大学形成产学研结合的运行机制，培养网络安全技术人才，利用项目技术成果，为CISP-CSE、CISP-ICSSE、CISP-BDSA等提供培训方案和材料。