全球数据安全观察

总第 125 期 2023 年第 6 期

(2023.02.13-2023.02.19)

大数据协同安全技术国家工程研究中心

NERCBDS
大数据协同安全技术
国家工程研究中心

目录

政策形势

1、中共中央 国务院关于做好 2023 年全面推进乡村振兴重点工作的意见

2 月 13 日，2023 年中央一号文件发布，其中在持续加强乡村基础设施建设中，明确提出要加快农业农村大数据应用，推进智慧农业发展。落实村庄公共基础设施管护责任。

https://mp.weixin.qq.com/s/jmfpNlqLy2YV2SXp_wbC4g

2、《工业和信息化部行政执法事项清单》公布

2 月 8 日，北京市人民政府印发《2023 年市政府工作报告重点任务清单》，其中，第 247-261 条为新增的数据安全相关内容。

https://wap.miit.gov.cn/jgsj/zfs/gzdt/art/2023/art_5320565039f54cd696c3c07d5077efe0.html

3、广东省《“数字政府 2.0”建设落实“实体经济为本，制造业当家”工作若干措施》出台

2 月 15 日，广东省政务服务数据管理局出台《“数字政府 2.0”建设落实“实体经济为本，制造业当家”工作若干措施》，围绕优化营商环境、赋能实体经济提质增效、促进数据产业

发展、培育数字政府产业生态、推动信创产业高质量发展、推进数字政府网络安全产业发展、营造服务实体经济良好环境等七个方面提出工作措施。

http://zfsg.gd.gov.cn/gkmlpt/content/4/4094/post_4094960.html#4079

4、关于开展2023年广东省电信和互联网行业网络数据安全和应用合规行政检查的通知

2月13日，广东省通信管理局根据《网络安全法》《数据安全法》《个人信息保护法》《反电信网络诈骗法》等法律法规，结合2023年全国工业和信息化工作会议部署要求，发布了即日起对全省电信和互联网行业开展网络安全、数据安全、个人信息保护、移动智能终端及互联网应用合规等方面的行政检查工作的通知。

http://cagd.gov.cn/v/2023/02/2591.html

5、证监会发布《证券公司场外业务资金服务接口》等4项金融行业标准

2月10日，证监会发布金融行业推荐性标准《证券公司场外业务资金服务接口》(JR/T 0273—2023)、《证券期货业机构内部接口 账户管理》(JR/T 0274—2023)、《证券期货业机

构内部接口 资讯数据》(JR/T 0275—2023)、《证券期货业信息系统渗透测试指南》(JR/T 0276—2023),自公布之日起施行。其中,《证券期货业机构内部接口 账户管理》和《证券期货业机构内部接口 资讯数据》2项金融行业标准,分别规范了机构内部账户管理业务系统及资讯数据业务系统的数据接口,通过梳理核心业务模块之间的数据交互场景,对数据接口的数据字段、数据格式、数据交互协议提出了相关要求,对行业机构高效建立内部信息系统、实现跨平台资源共享具有指导意义。

http://www.csrc.gov.cn/csrc/c100028/c7088360/content.shtml

技术、产品与市场

1、贵阳大数据交易所上线全国首个数据产品交易价格计算器

为探索多样化、符合数据要素特性的定价模式和价格形成机制。近日，在国家发改委价格监测中心的指导下，贵阳大数据交易所上线全国首个数据产品交易价格计算器。

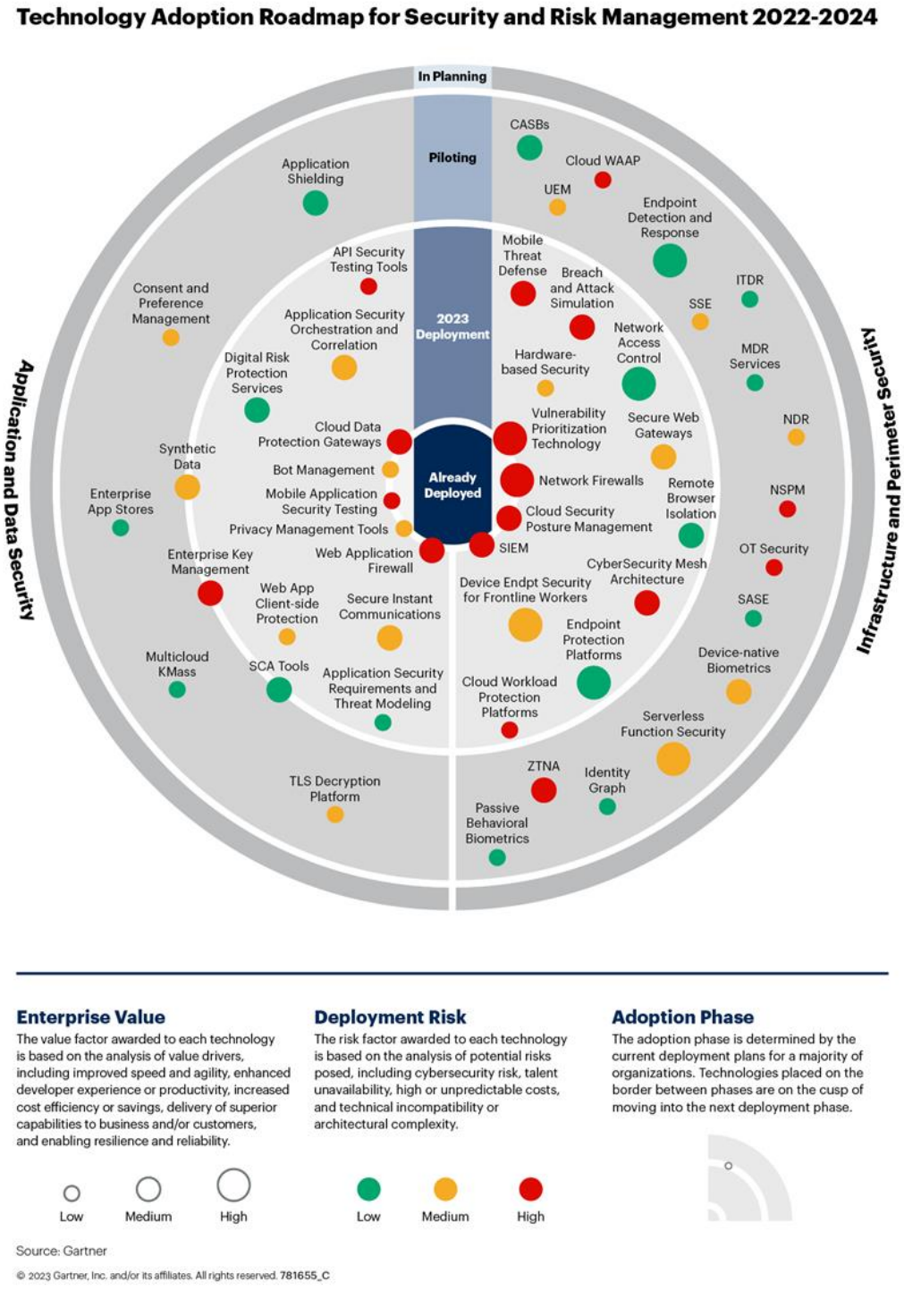
参考成熟要素市场价格机制，基于《数据产品成本评估指引 1.0》等规范，从价格形成原理出发，结合数据要素特性，该产品通过建立估价模型，以数据产品开发成本为基础，综合考量数据成本、数据质量、隐私含量等多重价值修正因子对于数据产品价格的影响，并基于预计的商业模式和市场规模，评估计算数据产品价格，为数据交易买卖双方议价提供参考，补全“报价－估价－议价”价格形成路径中的关键环节，促进数据要素高效配置、公平交易和自由流动。

https://mp.weixin.qq.com/s/stsRkgvFmzVVueznFU3Rvg

2、Gartner 发布 2023 年安全和风险管理技术采用路线图

Gartner 根据采用阶段、部署风险和企业价值，绘制了 2022 年至 2024 年间大型全球企业中 49 项安全相关技术的实施情况。安全和风险管理领导者可以使用此信息图来衡

量他们的计划并根据主要趋势进行衡量。



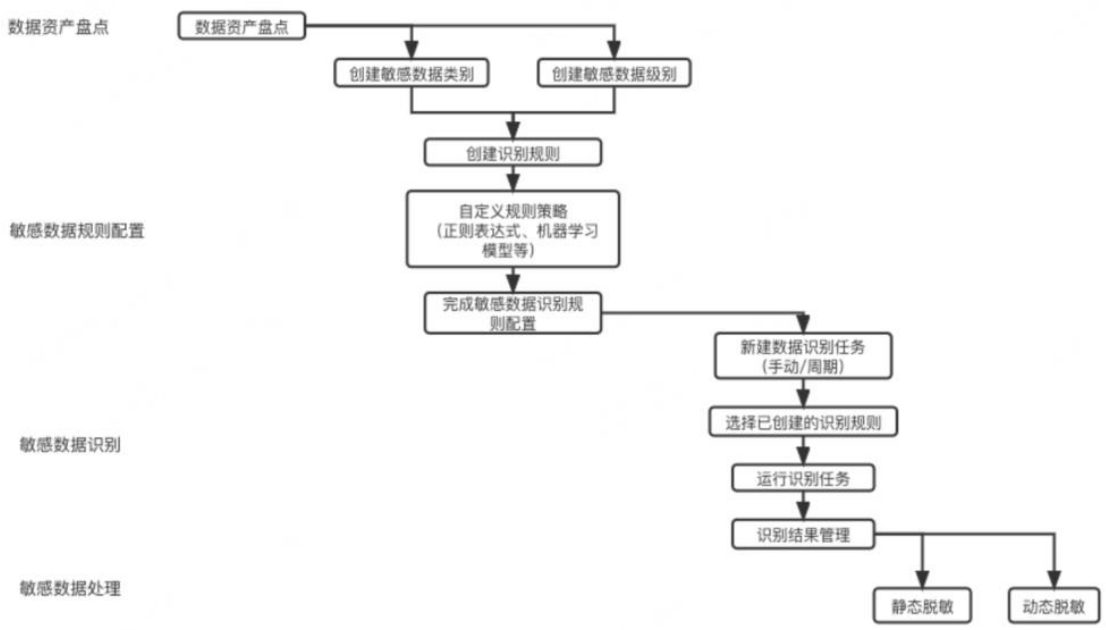
从对技术采用路线图调查数据的分析中得出，**安全和风**

险管理 (SRM) 领导者正在近期部署应用程序和数据安全解决方案，并为基础设施和边界安全制定更长远的规划。在我们调查涵盖的 49 项技术中，51% 处于“部署中”，47% 处于“试验阶段”。与基础设施和边界安全技术相比，更多的应用程序和数据安全技术正在部署中，预计将在 2023 年初更快地被采用。只有一种基础设施和边界安全技术，网络防火墙，已经被大多数人部署 SRM 领导者，由于其成熟度水平。

https://www.secrss.com/articles/51896

3、《智能网联汽车数据分类分级实践指南》正式发布

日前，第二届数据安全治理峰会在北京召开。在峰会上，DSI 汽车工作组组长单位吉利汽车研究院电子电器中心副主任兼架构部部长韩勇发布了《智能网联汽车数据分类分级实践指南》并进行解读，明确智能网联汽车数据分类分级的方法论，及对应不同等级的数据，给出通用的安全措施。



来源：数据安全推进计划

https://mp.weixin.qq.com/s/3KvQpcOzHcemkCozS-HKKA

4、隐私计算在科教卫生领域的应用

过去几年中，教育和卫生行业数字化获得了长足发展，众多学校、医院、科研机构、教育机构和医疗机构积累了大量数据，为隐私计算的落地提供了很好土壤。同时，医疗行业和教育行业所收集的数据具有较强的隐私属性，对隐私保护和数据安全的需求更为强烈。

由绿盟科技联合苏州市卫生计生统计信息中心、深圳大学共同撰写的《隐私计算在科教卫生领域应用白皮书》着重普及科教卫生行业的数据安全现状以及隐私计算在科教卫生领域的一些应用实践。

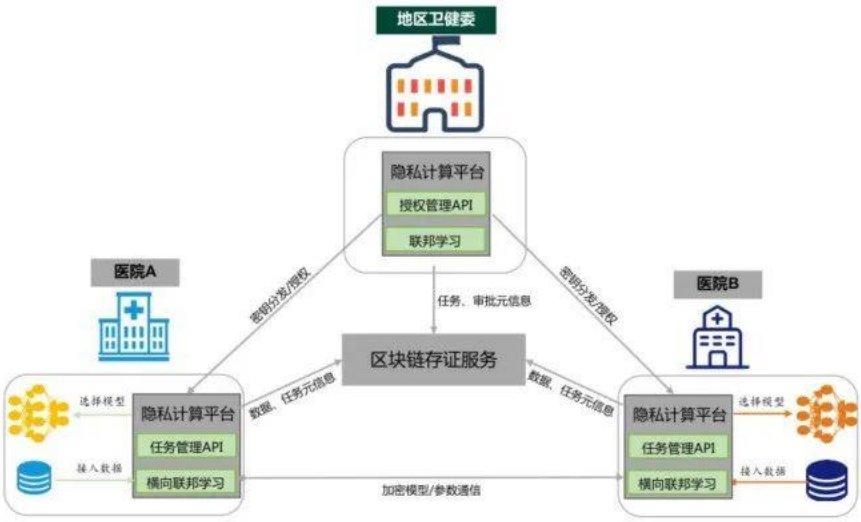


图 17　基于横向联邦学习的脑卒中预测模型总体部署图

https://mp.weixin.qq.com/s/tJyJPdsK447iN3_WlSULzA

5、[调研]：安全工具采用激增

2 月 15 日，身份与访问管理（IAM）供应商 Okta 发布调研报告，详述其广泛用户群中的应用程序使用趋势和安全趋势。报告发现，**零信任安全策略越来越普及**，各种安全工具的采用率急剧上升。

Okta 表示，技术公司是零信任采纳的急先锋，34%的受访技术公司部署了至少一个采用零信任配置的系统，7%部署了两个。金融和银行业也是零信任部署的热门领域，26%采用至少一个零信任配置，5%用两个。

Okta 的调研发现，从移动设备管理（MDM）应用到安全培训应用，各种安全工具越来越畅销。VPN 和防火墙工具无

疑是最火爆的一类，客户同比增长 31%。不过，端点管理和安全应用程序紧随其后，同比增长 25%。报告揭示，去年 Okta 用户中增长最快的一款应用是适用于 iOS 和 Mac 的 MDM 应用 Kandji。该应用过去一年中新增客户 172%。

https://mp.weixin.qq.com/s/Dp92uiF05KZQ6yGjkPBobQ

业界观点

1、李建彬等：2022 年度国内数据安全的现状与发展

华北电力大学李建彬、李智勇、李诗珂对 2022 年度国内数据安全的现状与发展进行梳理和分析，认为现阶段数据安全特点与热点主要包括:

（一）数据安全战略布局初步形成;

（二）数据安全标准化工作加速推进;

（三）数据安全技术发展方兴未艾;

（四）数据安全审查与监管措施逐步完善;

（五）数据安全产业发展迅猛;

（六）数据安全市场需求旺盛;

（七）数据安全问题依然严峻复杂;

（八）数据安全管理及个人信息保护认证体系逐步构建。

为了构建新形势下数据安全治理体系，除了要充分考虑数据要素流通中数据交换、数据集成、数据存储、数据资产管理等方面安全风险，还要重点关注数据安全合规治理、数据供应链安全、数据安全保险、新型数据安全产业生态等四个方面的问题。

（一）数据安全合规治理

数据安全是一项复杂的系统性工程，涉及法律法规和标

准规范众多，数据安全标准解析与落实难度大。为化解新形势下数据安全系统性风险，应从制度、技术和管理三个方面构建立体化数据安全合规治理体系，使得合规行为成为组织运营的有机组成部分。

（二）数据供应链安全

数据要素流通交易带来的最直接的安全风险就是不论数据供应链哪个环节出现问题，都会引发以数据为驱动力的业务和以数据为原材料的产品的安全风险。因此，加强数据供应链安全问题研究，构建数据供应链的安全保障体系，化解数据供应链安全风险，成为新形势下数据安全领域的一项需要优先解决的问题。数据供应链安全应以数据生命周期为基础，从组织建设管理、制度保障管理、技术支撑管理、人员执行管理等维度构建保障框架，对供应方、合作方、集成方、服务支撑方等相关方，从组织建设、制度流程、技术防护、人员能力等四个方面进行要求，尽可能确保数据供应链安全。

（三）数据安全保险

随着数据要素定价确权以及授权制度的逐步完善，数据安全保险作为网络安全保险的一个重要组成部分，基本具备了先行先试的条件。通过完善数据安全保险体制机制，可有效提升全社会数据安全风险管理水平和能力，降低社会总成

本，落实组织在数据安全方面的社会责任。

（四）新型数据安全产业生态

随着数据要素市场的逐步形成，亟需构建保障要素市场安全稳定运行的新型数据安全基础设施。作为平衡数据流通与安全的重要工具，隐私计算正在成为数字经济的底层基础设施，为各行各业搭建坚实的数据应用基础。随着政策与需求的双重驱动，隐私计算技术和产品的成熟度快速提升，在金融、通信、政务、医疗等行业的应用加速落地。但由于标准滞后，政策不明朗，目前隐私计算在互联互通、性能效率和业务价值体现等方面仍存在较大障碍。为了充分发挥隐私计算等新型数字经济基础设施的作用，保障数字经济健康稳定发展，应围绕隐私计算等以密码技术为基础的数据安全基础设施建设，尽快形成新型数据安全产业生态，加快这一生态体系的政策法规、技术标准、运营体系、市场规制等方面的建设。

https://mp.weixin.qq.com/s/s5efIHDEgU-Ns2MlAGKs9Q

2、郑曦：强化司法领域数据安全保护

为保护司法领域的数据安全，北京外国语大学智慧司法与数字法治研究中心主任、教授郑曦笔者建议从以下几个方面采取相应数据安全保护措施：

第一，建立司法数据分类分级制度。基于国家安全利益对数据保密程度的要求，应当按照保守国家秘密法中密级划分的规定，对司法数据进行绝密数据、机密数据和秘密数据的分类分级，并根据保守国家秘密法和保守国家秘密法实施条例等法律规定，按照不同密级采取相应的保密措施，保障司法数据安全。此外，从保护公民数据权利的角度出发，还可以将司法数据区分为一般数据和敏感数据。

第二，重视作为数据主体的公民在司法数据安全保护中的作用。一方面，作为数据主体的公民既是司法数据的来源者，又是司法数据安全保护的参与者，应当认可数据主体对数据在一定程度上的控制。例如，在案件办理允许的情况下，可以就司法机关收集使用数据的情况向数据主体进行告知，以保障其法定阅卷权。另一方面，作为数据主体的公民也是司法数据安全保护中对公权力进行监督的监督者和制约者，有利于防止权力滥用、保护司法数据安全，也是宪法赋予的公民监督权在司法数据安全保护领域的体现，应当予以尊重。

第三，强化司法机关的数据安全保障职责。首先，司法机关应履行数据处理前的数据安全审查和评估职责。其次，司法机关应承担数据处理过程中的数据安全监测和预警职责。再次，司法机关还应负有数据安全事故发生后的报告和应急处置职责。

第四，设置专门的司法数据安全监管机构。设置独立、专门的数据监管机构，能够有效监管数据处理行为，对于数据安全保护工作的展开具有重要意义。

https://www.spp.gov.cn/spp/llyj/202302/t20230207_600174.shtml

3、李三希等：不断推动数据安全产业高质量发展

近日，工信部等十六部门联合发布了《关于促进数据安全产业发展的指导意见》（以下简称《意见》）。《意见》指出，数据安全产业是为保障数据持续处于有效保护、合法利用、有序流动状态提供技术、产品和服务的新兴业态，既要满足数据处理者履行数据安全保护责任义务的需要，也要满足促进数据资源开发利用、激活数据要素价值的需要，为下一步数据安全产业的高质量发展提供了思路指导。

加强数据安全保护，增强人民群众安全感。“数据二十条”中指出，要“健全数据要素由市场评价贡献、按贡献决定报酬机制”“按照‘谁投入、谁贡献、谁受益’原则，着重保护数据要素各参与方的投入产出收益”。完善权益保障机制，有利于增强消费者对个人数据开发利用的意愿。数据安全企业也应着重优化发展数据识别、数据脱敏等数据加工技术，从而更好满足对海量消费者个人数据的开发利用需求。

加强数据安全保护，不断促进行业规范发展。数据安全服务相关需求迅速上升，数据安全企业可以借此机遇积极拓展产业合作渠道，与数据处理者强化交流合作，推动供需精准对接；同时深度分析工业、电信、交通、金融、卫生健康、知识产权等领域数据处理者的合规与保护需求，发展面向重点行业领域特色需求的精细化、专业型数据安全产品，积极开发适用性产品或解决方案。

加强数据安全保护，有利于维护国家安全。应当加快建设包含预防、发现、消除泄密隐患为主的数据安全体系，对于信息基础设施运营商等涉及国家关键数据和包含数据跨境流动业务的企业加强监管和安全审查，切实维护国家数据安全与社会公共利益。此外，保障公共数据在开发利用过程中的安全同样重要。要确保以政务数据为代表的公共数据能够在落实数据安全保护责任的前提下，实现安全、高效的开发利用，让数据更好地成为驱动数字经济发展的新动能。

https://www.peopleweekly.cn/html/2023/pinglun_0216/157399.html

4、梅宏院士等：大数据技术的四大挑战与十大趋势

日前，中科院院士梅宏联合中国人民大学、华中科技大学、中科院计算技术研究所、中国科学院大学、北京理工大

学多位专家，发布最新论文《大数据技术前瞻》。该文在计算体系重构的背景下，指出了大数据技术发展的四大技术挑战和十大发展趋势。

一、新型大数据系统技术的四大挑战

挑战一：如何构建数据为中心的计算体系

全球大数据规模增长快速，2020 年全球新增数据规模为 64ZB，是 2016 年的 400%，2035 年新增数据将高达 2140ZB1，大数据呈现指数级增长。如何组织和管理超大规模的数据要素已经成为一项难题：例如，针对大数据管理，面临数据跨域访问带来的各种问题、系统规模持续增大带来的可用性下降、维护大规模数据带来的成本和能耗持续增高等严峻挑战。

挑战二：如何满足大数据高效处理的需求

数据规模呈指数级增长，数据动态倾斜、稀疏关联、应用复杂，传统大数据处理架构数据处理成本高企、时效性差，如何满足规模海量、格式复杂、需求多变的大数据高效处理需求是大数据处理面临的重要挑战。

挑战三：如何实现多源异构大数据的可解释性分析

随着数据量持续地爆炸式增长和各类应用的不断拓展与深化，基于深度学习的主流方法因其仅关注单源单模态数据且模型只知其然不知其所以然的特性已无法满足发展需求。如何打破数据多源异构造成的隔阂，融合多域甚至全域

数据中蕴含的知识，实现分析结果的可解释，从而提升其可用性，是当前大数据分析面临的主要挑战。

挑战四：如何形成系统化大数据治理框架与关键技术

针对大数据应用过程中的对数据汇聚融合、质量保障、开放流通、标准化和生态系统建设的需求，大数据治理技术逐渐成为发展热点，然而当前系统化的大数据治理框架尚未形成，开放共享、质量评估、价值预测等关键技术远未成熟，成为制约大数据发展的主要瓶颈。

二、 大数据技术十大未来发展趋势

趋势一：数据与应用进一步分离，实现数据要素化

趋势二：数联网作为数字化时代的新型信息基础设施

趋势三：从单域到跨域数据管理，促进数据要素的共享与协同

趋势四：大数据管理与处理系统体系结构异构化日趋明显

趋势五：扩展性优先设计到性能优先设计

趋势六：近数处理成为突破大数据处理系统性能瓶颈的重要途径

趋势七：从单域单模态分析到多域多模态融合，实现广谱关联计算

趋势八：从聚焦关联到探究因果，实现分析结果可解释

趋势九：高能效大数据技术是可持续发展的关键

趋势十：大数据标准规范和以开源社区为核心的软硬件生态系统将成为发展的重点

http://www.cbdio.com/BigData/2023-02/16/content_6171907.htm

5、疑似 45 亿条个人信息泄露的背后：危机之下的数据安全建设之痛

数据泄露事件持续上升，泄露成本越来越高，隐性的损失不可估算，应对数据安全威胁涛涛之势，国家及监管部门已高度重视。在解决数据安全问题的过程中，不可能有一劳永逸，也不能存有侥幸心理，要知道，再严苛法律法规也镇不住所有的利益驱动者。

对于每一家企业单位而言，都需要着眼当下、务实建设数据安全体系：

（一）以制度为准则，建立完善数据安全管理体系

管理制度与机制的建立与优化是数据安全工作的基础。企业在开展数据安全建设中，应以安全合规为底线，基于国家、行业数据安全相关法律法规与标准要求，构建涵盖组织、制度、人员在内的完备的数据安全制度和管理体系，对数据收集、存储、处理、应用等关键环节的操作规范、管理部门

职责分工、应急管理与安全检查机制、责任追究等进行全方位规定。

（二）以风险现状为依据，进行安全基础能力建设

开展数据安全资产梳理和风险评估，通过对企业组织实际情况进行现状分析，包括数据资产梳理、使用权限情况、内外部数据安全风险、合规差距梳理等，根据数据安全风险状况进行整体安全规划，进而针对数据不同的安全级别以及不同的应用场景采取不同的防护。

数据安全技术建设可遵“整体施策，分步实施；填平补齐、完善提高；系统可靠，安全优先”的原则，分阶段开展，包括数据内控合规、数据全域管控、风险全局可视。

（三）以持续化运营，实现安全能力持续优化

数据安全需要持续构建、不断改进、提升防护效果，数据安全运营是必不可少的一环，需要从预测、防御、检测、响应四个维度，建立可持续优化的数据安全监控和安全运营体系，对现有的数据安全能力进行审视，发现存在不足进行响应处置，实现数据安全状态持续保障和提升。

http://www.mchz.com.cn/cn/about-us/News/info_45_itemid_6087.html#

数据安全事件

1、全球关键半导体厂商因勒索攻击损失超 17 亿元

2 月 20 日消息，作为全球最大的半导体制造设备和服务供应商，美国应用材料公司（Applied Materials）在上周的财报电话会议中表示，**有一家上游供应商遭到勒索软件攻击，由此产生的关联影响预计将给下季度造成 2.5 亿美元（约合人民币 17.17 亿元）的损失**。

https://mp.weixin.qq.com/s/vsNvVz2l4gvKUmgK8vrOfQ

2、勒索攻击致使国际帆船之都进入紧急状态

因勒索软件攻击导致城市所有 IT 系统离线，奥克兰市宣布进入紧急状态。2 月 14 日的声明中写道，“今天，奥克兰市临时行政官 G. Harold Duffey **宣布当地进入紧急状态，旨在应对 2 月 8 日（星期三）开始的勒索软件攻击所造成的网络中断影响**。”尽管上次的勒索软件攻击只影响到非紧急服务，但当时离线的多个系统目前仍未恢复。目前尚不清楚攻击出自哪个勒索软件团伙。

https://hackernews.cc/archives/43288

3、SAS 航空确认情人节网络攻击期间乘客数据遭到破坏

2 月 17 日报道，斯堪的纳维亚航空公司 (SAS)确认乘客数据在 2 月 14 日的网络攻击中遭到泄露，该攻击导致该航空公司的网站和移动应用程序离线数小时，Anonymous Sudan 声称对此负责。

该航空公司周四在其网站上发表声明，确认“受影响乘客的联系方式、之前和即将搭乘的航班，以及信用卡号码的最后四位数字都是可见的。” 该航司还表示，护照详细信息和 EuroBonus 积分没有受到影响。

https://cybernews.com/news/sas-airlines-passenger-data-leak-valentines-day-attack/

4、GoAnywhere MFT 黑客攻击美国社区卫生系统，引起 100 万患者数据泄露

2 月 15 日，美国社区卫生系统（CHS）披露了一起数据泄露事件，攻击者利用了 Fortra 的 GoAnywhere MFT 平台中的零日漏洞。

社区卫生系统(CHS) 是美国领先的医疗保健提供者之一，经营着 79 家急症医院和 1,000 多个其他护理场所。CHS 最近收到其第三方提供商 Fortra 的通知，称 Fortra 遇到了暴露公司数据的安全事件。CHS 启动了一项调查，以确

定其系统是否受到影响，并发现多达 100 万患者的信息遭到泄露。

https://securityaffairs.com/142242/data-breach/community-health-systems-data-breach.html

5、Atlassian 称泄露的数据通过第三方应用程序被盗

2 月 17 日，据外媒报道，一个名为 SiegedSec 的威胁组织最近发布了据称从开发与协作软件公司 Atlassian 窃取的员工和运营信息缓存。

据报道，Atlassian 解释说由于第三方应用程序遭到破坏，泄露的数据包括员工姓名、电子邮件、部门和位于加利福尼亚州旧金山和澳大利亚悉尼的 Atlassian 办公室部分的平面图。据称，漏洞的发生可能是由于威胁行为者获得了员工凭证的访问权限。

https://www.darkreading.com/endpoint/leaked-atlassian-data-stolen-from-third-party-app-company-says-?&web_view=true

6、AI 图像编辑工具 Cutout 泄露用户图像和数据

2 月 16 日消息，Cutout.pro 是一款流行的 AI 图像编辑工具，被发现泄露了 9GB 的用户数据，其中包括用户名、电子邮件地址和通过特定查询请求的图像。

这一泄露事件是由 Cybernews 发现的，其发现了一个开放的 ElasticSearch 实例，其中包含 2200 万条引用用户名的日志条目，包括个人用户和企业帐户。但是，由于日志条目包含重复项，受影响的用户总数尚不清楚。

https://www.hackread.com/ai-image-editing-tool-cutout-data-leak/?web_view=true

7、加利福尼亚医疗机构遭遇数据泄露，330 万患者受到影响

2 月 19 报道，Bleeping Computer 网站披露，加利福尼亚州 Heritage Provider Network（全美最大的综合医疗服务网络之一）中多个医疗机构遭遇勒索软件攻击，大量患者敏感信息泄露。

2 月初，受影响医疗机构集体发布一份安全通知，透露此次攻击事件约 330 万名患者敏感数据暴露，并表示已经与加利福尼亚州总检察长办公室报告了攻击事件。

从安全通知披露的信息来看，2022 年 12 月 1 日，勒索软件攻击开始行动，根据日志审查，可以确定以下数据已被泄露：患者全名、社会保障号码（SSN）、出生日期、住址、医疗诊断和治疗记录、实验室测试结果、处方数据等等。勒索软件攻击者窃取上述敏感数据，并以此向医疗机构勒索赎金。

https://www.secrss.com/articles/52027

8、百事可乐遭遇恶意软件攻击发生数据泄露

2 月 14 日，据 Bleeping Computer 报道，百事可乐装瓶风险投资有限责任公司遭受网络攻击导致数据泄露，攻击者在百事可乐瓶装风险投资公司的网络中安装信息窃取恶意软件并从其 IT 系统中提取数据，目前尚不清楚有多少人受到数据泄露的影响。

根据百事可乐最新的内部调查结果，受影响用户的以下个人信息遭到泄露：全名、家庭住址、财务帐户信息（包括密码、PIN 和访问号码）、驾驶执照号码、社会安全号码（SSN）、护照信息等等。

据悉，百事可乐瓶装风险投资公司已实施额外的网络安全措施，重置所有公司密码，并通知执法部门。百事可乐还通过 Kroll 向受数据泄露影响的用户提供为期一年的免费身份监控服务，以帮助他们防止因数据被盗而可能发生的身份盗用。

https://www.secrss.com/articles/51860

9、BlackCat 泄露了属于爱尔兰大学的数据

2 月 13 日，据外媒报道，BlackCat 勒索软件即服务组织泄露了从爱尔兰明斯特科技大学窃取的价值超过 6 GB 的信息。

据爱尔兰公共广播公司 RTÉ 报道，在爱尔兰高等法院发布临时禁令禁止勒索软件攻击者泄露数据几天后，就发生了该事件，BlackCat 窃取的信息包括员工医疗诊断和学生银行账户信息等敏感数据。据报道，法院命令还要求黑客将他们拥有的任何机密数据移交给大学。

https://www.bankinfosecurity.com/blackcat-leaks-data-belonging-to-irish-university-a-21192?&web_view=true

10、B&G Foods 遭到 Daixin 的攻击约 1000 台主机被加密

媒体 2 月 12 日称，Daixin 近期的一次网络攻击导致 B&G Foods 约 1000 台主机被加密。Daixin 的发言人表示，B&G 于 2 月 4 日被加密，但他们不确定是否已对所有备份进行加密，并表示该公司可能已经恢复。此外，他们在本地上留下了赎金记录并发送了几次通讯，但 B&G 一直没有回应。研究人员称，泄露数据中确实包括公司内部文件，然而，整个转储似乎没有更严重或机密的公司文件、人事文件或承包商文件。

https://www.databreaches.net/b-files-leaked/

《全球数据安全观察》周报

政策形势： 政策法规/地方动态/标准动态

技术、产品与市场： 技术研究/行业洞察/市场趋势

业界观点： 大咖观点/业界报告

数据安全事件： 合规事件/数据泄露/数据勒索

编委会： 钟力、唐会芳、王雨薇、陈璐

如有反馈 邮件请至 nelab@360.cn

http://www.nelab-bdst.org.cn/