CSA 数据安全词汇表

CSA GCR cloud security alliance® GREATER CHINA REGION

CSA cloud security alliance®

数据安全工作组的官方网址是：

https://cloudsecurityalliance.org/research/working-groups/data-security/

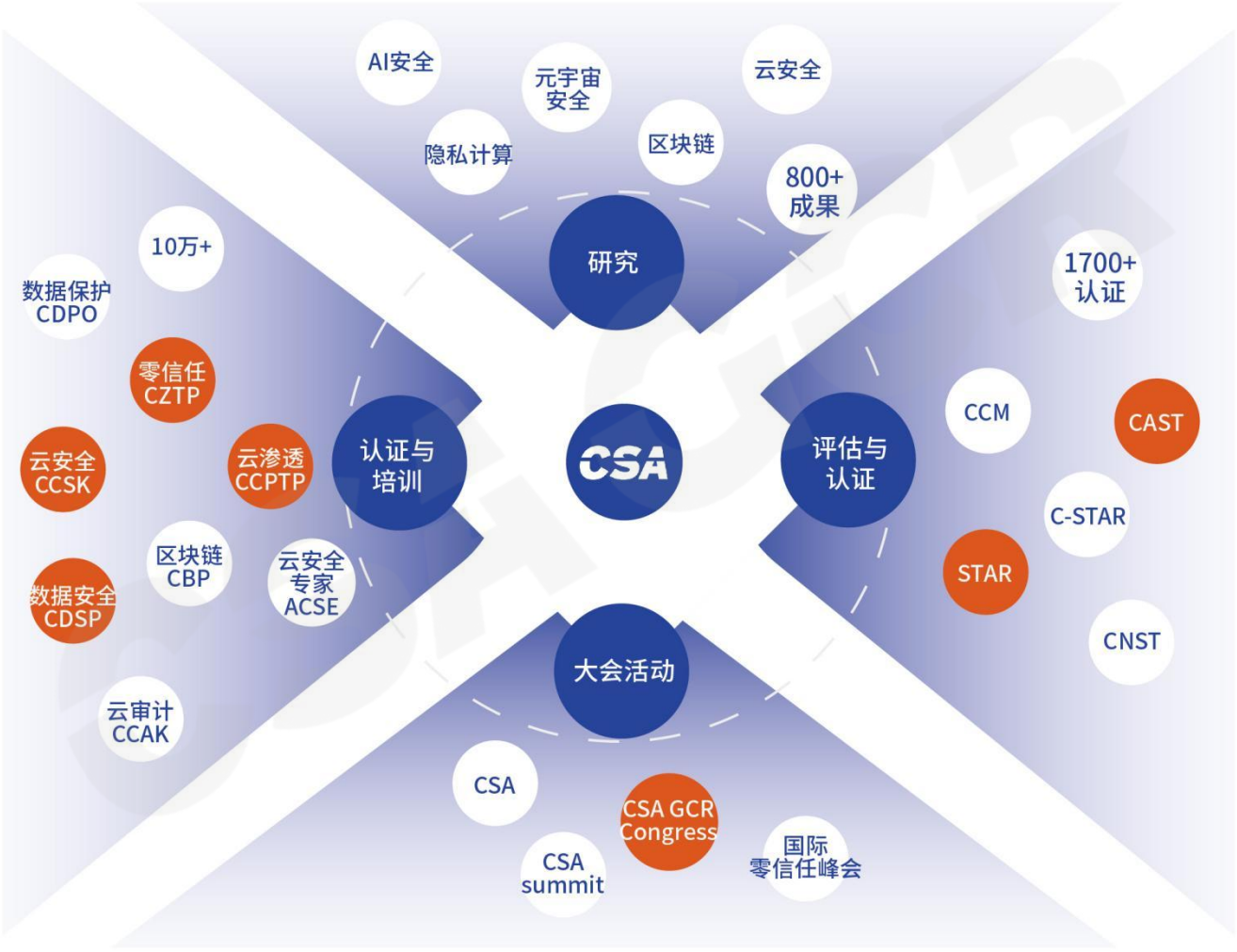
联盟简介

云安全联盟（Cloud Security Alliance,CSA）是中立、权威的全球性非营利产业组织，于2009年正式成立，致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识，推动数字安全产业全面发展。

云安全联盟大中华区（Cloud Security Alliance Greater China Region, CSA GCR）作为CSA全球四大区之一，2016年在香港独立注册，于2021年在中国登记注册，是网络安全领域首家在中国境内注册备案的国际NGO，旨在立足中国，连接全球，推动大中华区数字安全技术标准与产业的发展及国际合作。

我们的工作

联盟会刊下载地址
了解联盟更多信息



加入我们

CSA大中华区官网
(https://c-csa.cn)

点击会员

加入联盟

填写相关申请信息

成为CSA会员

JOIN US

致谢

《CSA 数据安全词汇表（CSA Data Security Glossary）》由 CSA 工作组专家编写，CSA 大中华区秘书处组织数据安全工作组专家进行翻译并在此基础上汇总添加了部分词汇。

中文版翻译专家组 （排名不分先后）：

组　长：王安宇

翻译组：

杨天识　　王曦光　　李春林　　鲁立　　张林成　　王彪

审校组：

王安宇　　姚凯　　郭鹏程　　王彪　　卜宋博

研究协调员：

卜宋博

感谢以下单位的支持与贡献：

OPPO 广东移动通信有限公司　　北京天融信网络安全技术有限公司　　新华三技术有限公司

启明星辰信息技术集团股份有限公司　　广州赛宝认证中心服务有限公司

英文版本编写专家

主要作者：

Alex Kaluza　　Oliver Forbes　　Rocco Alfonzetti　　Onyeka Illoh

贡献者：

Michael Roza　　Pan Maszyna　　Paola Garcia Cardenas　　Parth Jamodkar　　Sanjeewa Fernando

CSA 全球专家：

Claire Lehnert　　Stephen Lumpe

在此感谢以上专家。如译文有不妥当之处，敬请读者联系 CSA GCR 秘书处给予雅正！联系邮箱 research@c-csa.cn；国际云安全联盟 CSA 公众号：

目标

识别、定义和引用相关的数据安全术语，以帮助网络安全专业人员和从业人员更好地理解数据安全。基于《CSA 云安全词汇表》和其他来源，这份相关数据安全术语的汇编将作为数据安全工作组出版物的基础参考。

过程

- 识别并按字母顺序列出与数据安全相关的术语
- 添加来自 CSA 词汇表、NIST 词汇表和其他公共来源的与数据安全相关和适用的术语
- 纳入并审核来自数据安全工作组成员建议的词汇定义
- 纳入并审核来自行业专家评审建议的词汇定义
- 最终确定定义和参考资料

云安全词汇表：https://cloudsecurityalliance.org/cloud-security-glossary/

数据安全术语表

术语	定义
访问控制列表（Access Control Lists，ACLs）	定义授予主体在系统中对对象的访问或更改权限 来源：企业架构参考指南 v2：CSA：技术解决方案服务（TSS）领域 - 信息服务

对抗模拟 **（Adversarial Simulation）**	安全专家模拟专业黑客的网络威胁行为，对组织的信息技术或运营技术环境发动攻击的实践。利用真实攻击者的渗透入侵技术和组织内部安全堆栈的闭环反馈，对抗模拟练习有助于测试和提高对勒索软件和持久性威胁等攻击的网络防护能力。 来源：AON：对抗模拟
匿名化数据 **（Anonymized Data）**	已经删除原始识别特征的个人身份信息（PII）数据 来源：https://www.secoda.co/glossary/anonymized-data
应用程序监控 **(Application Monitoring)**	对应用程序相关事件收集的能力，包括登录、对敏感数据的访问、事务和管理活动。 来源：企业架构参考指南 v2: CSA：业务运营支持服务(BOSS)域
人工智能 **(Artificial Intelligence)**	一种基于机器的系统，能够针对一组人类已定义的目标，做出影响现实或虚拟环境的预测、建议或决策。人工智能系统利用机器和人类的输入（数据）进行： (A) 感知真实和虚拟环境； (B) 通过自动化地分析将这些感知抽象成模型； (C) 利用模型推理来制定信息或行为的决择。 来源： https://www.cisa.gov/sites/default/files/2023-11/2023-2024_CISA-Roadmap-for-AI_508c.pdfources/roadmap-ai

验证 **(Authentication)**	验证用户、进程或设备的身份，通常作为允许访问系统资源的前提条件。 来源：https://csrc.nist.gov/glossary/term/authentication
授权 **(Authorization)**	判定允许或拒绝主体访问系统对象（网络、数据、应用程序、服务等） 来源：https://csrc.nist.gov/glossary/term/authorization
自动化事件响应 **（Automated Incident Response)**	利用人工智能驱动的流程用作自动化识别、遏制和缓解网络安全事件。授权 - 决择是否允许或拒绝主体访问系统对象（网络、数据、应用程序、服务等）。 来源：https://csrc.nist.gov/glossary/term/authorization
大数据 **（Big Data）**	组织收集的各类结构化、半结构化和非结构化数据的集合，可用于信息挖掘，并应用于机器学习项目、预测建模和其他高级分析应用。 来源： https://www.techtarget.com/searchdatamanagement/definition/big-data
业务连续性和灾难恢复 **（Business Continuity and Disaster Recovery (BCDR)）**	在发生任何服务中断的情况下，实施旨在确保业务连续性和恢复能力的措施。 来源：2011 年服务定义分类目录：CSA）

云访问安全代理 **（Cloud Access Security Broker , CASB）**	云访问安全代理（CASB）是部署在企业内部或云平台上的安全策略实施点，放置在云服务消费者和云服务提供商之间，通过整合和嵌入企业安全策略对云资源进行访问控制。CASB 能够整合多种类型的安全策略实施机制。 来源： https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs
网络安全保险 **（Cyber Insurance）**	网络安全保险是指企业可以购买的保险合同，用于降低在线业务所面临的风险。网络安全保险涵盖了组织在网络安全事件导致的大多数数据泄露方面的责任。来源： Trend Micro: What Is Cyber Insurance?
数据 **（Data）**	以数字形态表示的任意事物 来源：企业架构参考指南 v2：CSA：技术解决方案服务（TSS）领域-基础设施服务
数据分析 **（Data Analytics）**	使用数据、技术和工具识别模式和趋势，并生成基于信息的决策行动。数据分析的主要目标是解决与组织相关的特定问题或挑战，以推动更好的业务成果。 来源： https://www.comptia.org/content/guides/what-is-data-analytics
数据架构 **（Data Architecture）**	数据架构描述了数据从收集到转换、分发和使用的管理方式。它为数据及其在数据存储系统中的流动方式提供了蓝图。数据架构是数据处理操作和人工智能（AI）应用的基础。 来源: https://www.ibm.com/topics/data-architecture

数据、资产、 应用和服务 **(Data, Assets,** **Applications,** **Services, DAAS)**	• 数据 – 指那些如果被外泄或误用将带来最大风险的敏感数据。示例包括支付卡信息、受保护的健康信息、个人身份信息和知识产权。在政府环境中，还包括机密信息、国家安全信息和受控未分类信息。 • 应用 – 使用敏感数据或控制关键资产的应用程序。 • 资产 – 包括组织的信息技术（IT）、运营技术（OT）或物联网设备等资产。 • 服务 – 组织最依赖的服务。示例包括域名系统（DNS）、动态主机配置协议（DHCP）、目录服务、网络时间协议（NTP）和定制的应用程序编程接口（API）。 来源: https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management%20%2810-17-22%29.pdf
静态数据 **（Data at Rest）**	在信息技术中，静态数据指的是以数字形式存储的计算机数据，如云存储、文件托管服务、数据库或数据仓库中的数据。静态数据既包括结构化数据，也包括非结构化数据。 来源：https://www.imperva.com/learn/data-security/data-at-rest/
数据泄露 **（Data Breach）**	数据泄露发生在未经授权的个人获取敏感或机密信息时，例如个人信息或财务数据。数据泄露可能由多种原因引起，如网络攻击、员工疏忽或物理盗窃。数据泄露的后果可能非常严重，包括财务损失、声誉损害和法律处罚。例如，医疗机构的数据泄露可能导致病人记录被盗，包括病史和个人信息，这些信息可能被用于身份盗窃或在暗网上出售。

	来源： https://csrc.nist.gov/glossary/term/breach
数据/资产分类 (Data/Asset Classification)	安全策略及其实施的一种方法，包括将信息分为若干类别，每个类别都有关联的安全策略。服务器和端点等其他资产也可进行类似分类。在某些情况下，只能在具有相同分类名称的计算机上处理或存储数据。 来源：《企业架构参考指南 v2：CSA： 安全与风险管理 (SRM) 域
数据目录 （Data Catalog）	数据目录是指组织内所有数据资产的详细清单，旨在帮助数据专业人员快速地找到适合任何分析或商业目的的最合适数据。 来源： https://www.ibm.com/topics/data-catalog
数据语料库 （Data Corpus）	数据语料库是由一系列真实文本或音频组成的数据集。这里的“真实”指的是由该语言或方言的母语者编写的文本或说出的音频。语料库的内容可以多种多样，包括报纸、小说、食谱、广播电台节目、电视节目、电影以及推特等。 来源: Hypersense AI: Corpus
数据发现 （Data Discovery）	指在网络、终端和服务器中扫描和分类存储的数据的过程。 来源：企业架构参考指南 v2: CSA: 安全与风险管理（SRM）领域
数据编织 （Data Fabric）	一种架构，通过使用智能和自动化系统，实现了各种数据管道和云环境之间的端到端集成。 来源:IBM: What is a data fabric?
数据治理 （Data Governance）	指组织在应用程序、服务和企业信息集成活动之间管理数据的过程。在这一过程中，需要有明确定义的治理模型概述数据在整个 IT 基础设施（包括内部和外部服务，如 SaaS、PaaS、IaaS、ASP 等）中的处理、转

	换和存储，并确保其合规性。数据治理包含的流程包括数据所有权、数据分类方式、数据/资产所有者对其应用程序和服务的责任，以及数据在整个生命周期中的必要控制措施。 来源:　业务运营支持服务（BOSS）领域
数据完整性 **（Data Integrity）**	指数据未被未授权的方式更改的属性。数据完整性涵盖了静态数据、使用中的数据以及传输中的数据。 来源: https://csrc.nist.gov/glossary/term/data_integrity
传输中的数据 **（Data in transit）**	传输中的数据是指从一个地方移动到另一个地方的数据。这包括通过电子邮件、协作平台、即时通讯和任何其他通信渠道传输的信息。由于这些数据从一个位置移动到另一个位置时会暴露在互联网或公司的私有网络上，所以通常比静态数据的安全性要低。 来源: 数据传输
使用中的数据 **（Data in use）**	使用中的数据指的是被员工、公司应用程序或客户访问或使用的数据。这种状态下的数据最容易受到攻击——无论是在处理、被读取还是正在修改中。直接授权个人访问这些数据会增加遭受攻击和人为错误的风险，任何这些情况都可能导致严重后果。因此，加密对于保护使用中的数据至关重要。许多公司为了进一步增强安全性，会在加密的基础上增加包括身份验证和严格的数据访问控制在内的安全措施。 来源: https://www.imperva.com/learn/data-security/data-at-rest/
数据互操作性 **（Data Interoperability）**	数据互操作性是指在不损失数据含义的前提下，从多个来源访问和处理数据，并将这些数据集成以进行映射、可视化及其他形式的表示和分析的能力。互操作性使人们能够查找、探索和理解数据集的结构和内容。其本质是能够将不同来源的数据“连接”起来，以构建一

	个具有特定应用场景下的全面局视图，从而简化（有时是自动化）分析过程，提升决策精度并加强问责制。 来　源　:https://www.data4sdgs.org/initiatives/data-interoperability-collaborative
数据湖 **（Data Lake）**	数据湖是一个集中式的存储库，能够摄取并存储大量数据的原始形态。随后，这些数据可以被处理，并作为满足各种分析需求的基础。得益于其开放且可扩展的架构，数据湖可以容纳任何来源的所有类型的数据，无论是结构化（如数据库表、Excel 表格）、半结构化（如 XML 文件、网页），还是非结构化数据（如图像、音频文件、推文），都能够在不损失数据真实性的情况下存储。 来源： https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-data-lake
数据生命周期管理 **（Data Life Cycle** **Management）**	数据生命周期管理包括以下六个阶段：创建、存储、使用、共享、归档和销毁。尽管这一过程被呈现为线性进展，但数据一经创建，在其有效期内，可以不受限制地在各个阶段间流动，并不一定要经过所有阶段。 来源:　安全与风险管理（SRM）领域
数据防泄露 **（Data Loss** **Prevention, DLP）**	数据防泄漏是指实施策略保护关键数据，如知识产权和客户信息，确保这些数据不会无意中泄露给企业外部的第三方。这类解决方案能够识别并分类敏感数据，根据内容和上下文定义并管理策略，监控和控制数据的流动，并对数据泄露事件进行报告、审计和记录。 来源:　安全与风险管理（SRM）领域

数据丢失 **（Data Loss）**	通过盗窃数据或泄露数据，暴露专有、敏感或机密信息的行为。 来源: https://csrc.nist.gov/glossary/term/data_loss
数据泄露 **（Data Leakage）**	未经授权地将数据从组织内部传输到外部目的地或接收者的行为。 来源: https://www.forcepoint.com/cyber-edu/data-leakage
数据血缘 **（Data lineage）**	追踪数据随时间流动的过程，可以清晰地了解数据起源、变化方式以及在数据管道内最终目的地。数据血缘工具提供数据在其生命周期内的记录，包括源信息和在任何 ETL（提取、转换和加载）过程中应用的任何数据转换。 来源: https://www.ibm.com/topics/data-lineage
数据本地化 **（Data Localization）**	数据本地化是将数据保留在其来源地区的做法。 来源: https://www.cloudflare.com/learning/privacy/what-is-data-localization/
数据脱敏 **（Data Masking）**	在数据存储中对特定数据元素进行模糊处理（遮蔽）的过程。它确保敏感数据被替换为现实但非真实的数据。目标是敏感数据在授权环境外不可用。 来源: 安全与风险管理（SRM）领域
数据网格 **（Data Mesh）**	是一种解决高级数据安全挑战的架构框架，通过分布式、去中心化的所有权实现。 组织拥有来自不同业务线的多个数据源，这些数据源必须集成以供分析使用。数据网格架构有效地统一不同的数据源，并通过集中管理的数据共享和治理指南将不同数据源的数据链接在一起。业务功能可以控制共

	享数据的访问方式、访问者以及访问的格式。 来源: https://aws.amazon.com/what-is/data-mesh/
数据挖掘 **（Data Mining）**	数据挖掘也称为数据知识发现（KDD），是从大型数据集中发现模式和其他有价值信息的过程。 来源: https://www.ibm.com/topics/data-mining
数据混淆 **（Data Obscuring）**	是通过某种形式的混淆处理（如加密）措施保护数据字段或记录的方法。数据混淆技术可以在源代码中使用，例如，防止应用程序的逆向工程。也有低技术解决方案，如使用墨水印章在硬拷贝上涂抹敏感信息。 来源: 企业架构参考指南 v2: CSA: 安全与风险管理（SRM）领域
数据持久化 **（Data Persistence）**	数据持久化是指在创建它的应用程序关闭后，数据仍然能长期存在。为了实现这一点，数据必须写入非易失性存储器——一种即使应用程序不再运行也能长期保留信息的存储器类型。 来源: https://www.mongodb.com/databases/data-persistence
数据管道 **（Data Pipeline）**	是一种方法，其中从各种数据源摄取原始数据，然后将数据传输到数据存储，如数据湖或数据仓库，以供分析。 来源: https://www.ibm.com/topics/data-pipeline
数据存证 **（Data Preservation）**	数据存证是指在诉讼期间保持实物和电子存储信息（ESI）完好无损以备发现的过程。为保存潜在证据，当事人必须保护信息不被破坏、删除、丢失或以任何方式篡改。 来源：https://zapproved.com/blog/what-is-preservation/

数据溯源 **（Data Provenance）**	在计算机和执法使用的背景下，它是一个相当于监管链的术语。它涉及信息的生成、传输和存储方法，可用于追踪社区资源所处理信息的来源。 来源： https://csrc.nist.gov/glossary/term/data_provenance
数据驻留 **（Data Residency）**	数据驻留指存储和处理数据的物理或地理位置，通常受法律和监管要求的影响。 来源：TechTarget - What is data residency?
数据留存 **（Data Retention）**	根据适用的法律、行政命令、指令、法规、政策、标准、准则和操作要求，管理和保留系统内的信息和从系统中输出的信息。 来源： https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
数据隔离 **（Data Segregation）**	数据隔离是确保数据在多租户环境中隔离的流程和控制措施，因此每个租户都只能访问自己的数据。 来源： 企业架构参考指南 v2: CSA: 技术解决方案服务（TSS）领域
数据主权 **（Data Sovereignty）**	数据受其物理存储所在国家或管辖区法律管辖的概念。 来源： https://www.splunk.com/en_us/blog/learn/data-sovereignty-vs-data-residency.html

数据存储 **（Data Storage）**	使用专门开发的技术来保存信息，并在必要时使其可访问。数据存储是指使用计算机或其他设备使用记录介质来保存数据。 来源：https://www.hpe.com/us/en/what-is/data-storage.html
数据标签 **（Data Tagging）**	数据标签是一个关键字或术语，通常作为元数据的形式分配给一条信息。它有助于描述一个条目，并有助于通过浏览或搜索再次找到它。 来源： 企业架构参考指南 v2: CSA: 安全与风险管理（SRM）领域
数据使用协议 **（Data Use** **Agreement, DUA）**	数据使用协议是管理双方交换特定数据的合同。DUA 确定了谁被允许使用和接收唯一的数据集，以及接收方允许的数据使用和披露。DUA 还为研究人员和接收方分配了使用数据的适当责任。 来源：https://ora.stanford.edu/resources/data-use-agreements
数据整理 **（Data Wrangling）**	也被称为数据清理、数据修复或数据屏蔽——指的是旨在将原始数据转换为更容易使用的格式的各种过程。根据您所利用的数据和您所试图实现的目标，具体的方法因项目的不同而不同。 来源： https://online.hbs.edu/blog/post/data-wrangling
数据去标识 **（De-identification** **of Data）**	删除个人数据标识符和敏感信息以保护给定数据集中的个人隐私的过程。 来源：NISTIR 8053 De-Identification of Personal Information

拒绝服务 **（Denial of Service, DoS）**	使系统、特性或资源对预期用户不可用的行为。在云测试中，拒绝服务通常采取破坏或加密云资源、禁用帐户、凭证或用户的形式。 来源：Cloud Penetration Testing : CSA
数字证书 **（Digital Certificate）**	数字证书是一种验证实体身份的电子文档，用于建立实体双方之间的安全通信。在 IAM 域中，数字证书通常用于身份验证和加密目的。它们由被称为证书颁发机构（CA）的可信第三方颁发。例如，组织可以使用数字证书来验证远程访问网络的员工的身份，或对通过互联网传输的敏感数据进行加密。 来源：https://csrc.nist.gov/glossary/term/digital_certificate
数字取证 **（Digital Forensics）**	将科学应用于数据的识别、收集、检查和分析，同时保持信息的完整性和保持严格的数据监管链。 来源：https://csrc.nist.gov/glossary/term/digital_forensics
灾难恢复即服务 **（Disaster Recovery as a Service, DRaaS）**	一种云计算服务模型，它允许组织在第三方云计算环境中备份其数据和 IT 基础设施，从而在灾难发生后可以重新获得对 IT 基础设施的访问和功能。 来源：Disaster Recovery as a Service : CSA
解密 **(Decryption)**	将加密的数据转换回其原始的、可读的形式的过程。 来源：NIST SP 800-53 Revision 5

双重勒索 **(Double Extortion)**	在双重勒索中，网络犯罪分子加密敏感的用户数据，并威胁要将其发布在暗网上，并卖给出价最高的人，如果在最后期限前未付赎金，则永久限制访问。组织通常可以从以前的备份中恢复丢失的信息，但在此类攻击之后，要阻止敏感数据的泄露要困难得多。 来源：ISAGCA: Double Extortion Ransomware: What It Is and How to Respond
出口过滤 **(Egress Filtering)**	过滤出站网络流量的方法，以便只允许明确允许的流量离开网络。 来源： https://www.pcisecuritystandards.org/glossary/egress-filtering/
加密 **(Encryption)**	加密是指使用加密算法将纯文本转换为不可读格式的过程，以保护数据的机密性、完整性和可用性。 来源：Defined Categories of Service 2011 : CSA
终端 **(Endpoints)**	终端是用户在使用 IT 解决方案时所交互的设备。它们被称为终端，因为它们处于技术与人类相遇的解决方案的边缘。 来源：企业架构参考指南 v2: CSA: 技术解决方案服务（TSS）领域
实体 **(Entity)**	实体指的是计算机系统中唯一的、可识别的行为者。在网络安全语境中，实体可以是用户、设备、应用程序或由 IAM 系统标识和验证的系统。实体在系统中可以有不同的角色和权限，它们的操作和对资源的访问通常被记录下来，以用于审计和安全目的。 来源：*（译注：原文无内容）*

ETL 管道 **(ETL Pipeline)**	提取、转换和加载（ETL）是数据仓库中的一个过程，负责将数据从源系统中拉出并将其放到数据仓库中。 来源：https://www.secoda.co/glossary/etl-pipeline
联邦身份管理 **(Federated Identity Management)**	允许在多个实体之间以及跨信任域之间开发和共享身份信息。工具和标准允许将身份属性从一个受信任的标识和身份验证实体转移到另一个实体，用于身份验证、授权和其他目的，从而为已识别的个人、身份提供者和依赖方提供“单点登录”的便利和效率。 来源： https://www.gartner.com/en/information-technology/glossary/federated-identity-management
防火墙 **(Firewal)**	一种限制两个连接网络之间的数据通信流量的网络连接设备。防火墙可以是安装在通用计算机上的应用程序，也可以是用来转发或拒绝/丢弃网络上的数据包的专用平台（设备）。通常，防火墙用于定义区域边界。防火墙通常有限制哪些端口是打开的的规则。 来源：https://csrc.nist.gov/glossary/term/firewall
通用数据保护条例（GDPR）	《通用数据保护条例（GDPR）》是世界上最严格的隐私和安全法。尽管它是由欧盟（EU）起草并通过的，但它却对任何地方的组织都施加了义务，只要它们针对或收集与欧盟人员相关的数据。该法规于 2018 年 5 月 25 日开始生效。GDPR 将对那些违反其隐私和安全标准的人处以严厉罚款，罚款金额最高可达数千万欧元。 来源：https://gdpr.eu/what-is-gdpr/

硬件安全模块 **（HSM）**	一种保护和管理加密密钥并提供密码处理的物理计算设备。HSM 是一个加密模块，或包含一个加密模块。 来源： https://csrc.nist.gov/glossary/term/hardware_security_module_hsm
哈希/散列 **(Hashing)**	一种将数据转换为固定长度的值（称为哈希值）的加密技术。哈希/散列用于验证数据的完整性和检测未经授权的更改。 来源：NIST SP 800-53 Revision 5
同态加密 **（Homomorphic Encryption, HE）**	支持对加密数据进行计算的算法。部分同态加密（PHE）只支持有限的用例，如减法和加法，但对性能的影响很小。完全同态加密（FHE）支持更广泛的可重复和任意的数学操作；然而，它会降低性能。 来源： https://www.gartner.com/en/information-technology/glossary/homomorphic-encryption-he
超文本传输安全协议（Hypertext Transport Protocol Secure, HTTPS）	HTTPS 是一种安全的网络通信方法，在技术上并不是一种协议，它是将超文本传输协议（HTTP）运行在 SSL/TLS 协议之上的结果，从而将 SSL/TLS 的安全功能添加到标准的 HTTP 通信中。 来源：https://iapp.org/resources/article/hypertext-transfer-protocol-secure/

IT 风险管理 **(IT Risk Management)**	信息风险管理是一种将风险敞口和风险管理能力与数据所有者的风险承受能力相结合的行为。它是信息技术资源的决策支持的主要手段，可保护信息资源的机密性、完整性和可用性。确保识别、理解、沟通、接受、纠正、转移或避免所有类型的风险。IT 风险管理部门可以查看合规性管理活动的输出，以帮助组织评估整体的安全态势，并与所定义的风险目标保持一致。 来源：企业架构参考指南 v2: CSA: S 安全与风险管理（SRM）领域
身份 **(Identity)**	在给定的应用场景下唯一地描述一个主体的一种属性或一组属性。 来源：https://csrc.nist.gov/glossary/term/identity
身份识别与访问管理 **(Identity and Access Management，IAM)**	身份识别与访问管理（IAM）是指使组织能够管理和控制用户身份、访问以及对系统和应用程序的权限的策略、技术和流程。IAM 解决方案通常包括用户预置、身份验证、授权和审核功能。IAM 帮助组织确保只有授权用户才能访问敏感数据和应用程序，并且访问权限是基于最小权限原则授予的。IAM 还使组织能够简化用户管理流程，降低内部威胁的风险。 来源: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST. SP.800-203.pdf
事件响应 **(Incident Response, IR)**	管理和处理安全事件的系统化过程，包括检测、响应和减轻事件的影响。

事件响应计划 **(Incident Response Plan)**	一套清晰的文档，可帮助组织准备、检测、分析和从事故中恢复。 来源: Cloud Penetration Testing : CSA
失陷指标 **(Indicators of Compromise, IoC)**	用于主机系统或网络上潜在入侵的取证证据。这些攻陷检测指标使信息安全专业人员和系统管理员能够检测入侵企图或其他恶意活动。安全研究人员使用 IoC 更好地分析特定恶意软件的技术和行为。IoC 还提供可操作的威胁情报，可在社区内共享，以进一步改进组织的事件响应和补救策略。 来源: TrendMicro: Indicators of compromise
入侵检测系统 **(Intrusion Detection System)**	网络安全工具，用于监视网络流量和设备是否存在已知的恶意活动、可疑活动或违反安全策略的行为。 来源: IBM: What is an intrusion detection system (IDS)?
恶意软件 **(Malware)**	旨在执行未经授权的进程的软件或固件，这将对信息系统的机密性、完整性或可用性产生不利影响。恶意软件包含感染主机的病毒、蠕虫、特洛伊木马或其他基于代码的实体。间谍软件和某些形式的广告软件也是恶意代码的示例。 来源: https://csrc.nist.gov/glossary/term/malware
主数据管理 **(Master Data Management, MDM)**	是一门技术驱动的学科，确保业务和 IT 技术部门共同合作，以确保企业官方共享的主数据资产的一致性、准确性、管理性、语义一致性和可追责性。 来源： https://www.gartner.com/en/information-technology/glossary/

	master-data-management-mdm
元数据 **(Meta data)**	描述和解释数据的信息，提供了包括数据源、类型、所有者和与其他数据集的关系等上下文细节。因此，元数据可以帮助你理解特定数据集的相关性并指导您如何使用它。简而言之：元数据是现代企业数据栈的基石。
多因素验证 **(Multi Factor Authentication, MFA)**	这是一种身份验证方式，它依赖于两个或更多的“因素”，其中一个因素是“你拥有的东西”，如智能卡，另外一个因素是“你知道的东西”，如密码或 PIN 码，以及“你是什么”，如物理指纹或表征行为的按键节奏。 来源：企业架构参考指南 v2: CSA: 安全与风险管理（SRM）领域
网络分段 **(Network Segmentation)**	这是一种网络安全技术，它将网络划分为更小、独立的子网络，使网络团队能够将子网络分隔开，并为每个子网络提供独特的安全控制和服务。 来源: VMware: What is network segmentation?
非人类身份 **(Non-Human Identity)**	非人类身份指的是与一个非人类用户（即非人类实体）相关联的身份。这可能包括与自动化进程或服务相关联的身份，例如脚本或应用程序。非人类身份经常被用于执行那些不由人类用户完成的任务，如运行计划任务或访问网络服务。它们也可以被用在如物联网设备或其他能够使用特定权限与系统交互的机器上。 来源： https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800- 63a.pdf
口令 **(Password)**	用于验证身份或验证访问权限的字符串（字母、数字和其他符号）。 来源：

	https://csrc.nist.gov/glossary/term/ password#:~:text=memorized%20
口令管理 **(Password Management)**	指定多个密码策略、定义密码组合约束、维护口令历史记录、限制口令、配置口令有效期、创建口令规则等的过程。 来源: 企业架构参考指南 v2: CSA: 安全与风险管理（SRM）领域
渗透测试 **(Penetration Testing)**	一种测试方法，测试人员以单个二进制组件或整个应用程序为目标，目的是确定组件内或组件间的漏洞是否会用于危害应用程序、其数据或其环境资源。 来源: https://csrc.nist.gov/glossary/term/penetration_testing
个人可识别信息 **(Personally identifiable information, PII)**	可以用来识别或追踪个人身份的信息，例如姓名、社会保障号、生物识别数据记录等，无论是单独使用还是与其他个人或可识别信息结合使用，这些信息与特定个体有关联或可关联（例如出生日期和地点、母亲的婚前姓氏等）。 来源: https://csrc.nist.gov/glossary/term/personally_identifiable_information
网络钓鱼 **(Phishing)**	一种试图通过电子邮件或网站上的欺诈性招揽获取敏感数据（如银行账号）的技术，犯罪者伪装成合法企业或信誉良好的人。 来源: https://csrc.nist.gov/glossary/term/phishing
网络钓鱼模拟 **(Phishing Simulation)**	一种网络安全演练，用于测试组织识别和响应网络钓鱼攻击的能力。 来源: IBM: What is a phishing simulation?

策略管理 **(Policy Management)**	策略管理是一个用于集中创建、存储和管理策略的流程或平台。策略管理的目标是维护一个组织结构和流程，这个结构和流程支持策略的创建、实施、异常处理，并提供代表业务需求的框架。 来源: 企业架构参考指南 v2: CSA: 安全与风险管理（SRM）领域
主数据管理 **(Principal Data Management)**	管理访问控制决策主体的所有属性的能力。这些主体可以是用户、机器或服务。授权决策可能需要考虑关于这些主体的许多属性，包括角色、位置、与帐户的关系、与其他主体的关系等。 来源: 企业架构参考指南 v2: CSA: 安全与风险管理（SRM）领域
服务质量 **(Quality of Service, QoS)**	为不同的应用程序、用户或数据流提供不同优先级的能力，或保证数据流具有一定级别的性能的能力。 来源： https://www.iso.org/obp/ui#iso:std:iso:20205:ed-1:v1:en:term:1.6.3
勒索软件 **(Ransomware)**	**勒索软件**是一种恶意软件，它能够侵入组织的系统和数据，然后加密这些系统和数据，使其在没有解密密钥的情况下无法访问。攻击者只有在受害者支付一笔费用（赎金）后才会提供解密密钥。**勒索软件**可以通过多种途径侵入系统，例如用户与钓鱼邮件或受感染的网站进行交互。 来源: Disaster Recovery as a Service : CSA
勒索软件即服务 **(Ransomware-as-a-Service, RaaS)**	一种涉及向买家（称为附属机构）出售或出租勒索软件的商业模式被称为“勒索软件即服务”（RaaS）。RaaS 可以说是勒索软件攻击迅速蔓延的主要原因之一，因为它使各种威胁行为者，甚至那些技术知识较少的行为者，更容易对目标部署勒索软件。 来源: TrendMicro: Ransomware as a Service

实时过滤 **(Real Time Filtering)**	一种控制机制，用于根据策略实时跟踪使用模式和信息，如访问和阻止哪些网站。 来源: 企业架构参考指南 v2: CSA: 安全与风险管理（SRM）领域
恢复计划 **(Recovery Plans)**	恢复计划描述了中断或灾难后恢复服务交付所需的流程和程序。这些计划通常包括在达到每个阶段性目标时逐步恢复服务的步骤，同时监控每个目标的性能和系统健康状况 来源: 企业架构参考指南 v2: CSA: 技术解决方案服务（TSS）领域
报告服务 **(Reporting Services)**	报告服务提供了以多种方式呈现数据的能力，从顶层的聚合仪表板到原始数据。报告服务还提供了挖掘和分析数据并为决策者提供商业智能的能力。 来源: 企业架构参考指南 v2: CSA: 技术解决方案服务（TSS）领域
资源数据管理 **(Resource Data Management)**	授权在数据管理中发挥着关键作用，它同时为应用程序信息资源提供访问和保护。 来源: 企业架构参考指南 v2: CSA: 安全与风险管理（SRM）领域
风险 **(Risk)**	“业务风险”的一个子集，因此应该用业务术语来讨论。与高管沟通时，网络安全专业人员不应该用技术术语来定义风险，而是应该采用几乎每位业务经理和董事会都使用的风险定义：潜在货币损失。在这种情况下，“风险”指的是事件可能导致盈利能力下降的可能性。因此，网络事件对组织品牌或声誉造成的损害可以进行量化。 来源: Information Technology Governance, Risk and Compliance in Healthcare : CSA

风险评估 **(Risk Assessments)**	风险评估从参考框架角度（如 COBIT、ISO27001）和监管角度（如 SOX、PCI）衡量组织控制措施的成熟度。 来源: 企业架构参考指南 v2: CSA: 技术解决方案服务（TSS）领域
Rootkit	攻击者在获得对主机的 root 级别访问权限后使用的一组工具，用于隐藏攻击者在主机上的活动，并通过隐蔽手段允许攻击者维持对主机的 root 级别访问权限。 来源: https://csrc.nist.gov/glossary/term/rootkit
数据保留规则 **(Rules for Data Retention)**	这种能力负责管理与企业和监管要求相关的数据（交易信息、电子邮件、文档图像、刷卡信息、在线浏览历史记录）的保留政策和程序，或相关要求，然后进行安全处置。 来源: 企业架构参考指南 v2: CSA: 业务运营支持服务(BOSS)域
安全数据飞地 **（Secure Data Enclave）**	一个安全的、集中式服务，为处理敏感研究数据的教职员工和研究人员提供支持。安全数据飞地符合高水平的安全政策，以确保根据当地、联邦和国际法律保护受限信息。 来源：https://securedata.uchicago.edu/
数据的安全销毁 **（Secure Disposal of Data）**	确保数据被适当销毁，以防止其被恢复（例如，通过数字取证技术）。应当有相应的销毁记录，并应纳入信息生命周期管理流程中。 来源：企业架构参考指南 v2：CSA：业务运营支持服务（BOSS）领域
安全套接字层 **（Secure Sockets Layer, SSL）**	一种安全协议，为两个通信应用程序之间提供隐私和数据完整性保护。该协议由两个层组成：TLS 记录协议和 TLS 握手协议。 来源：https://csrc.nist.gov/glossary/term/secure_sockets_layer

安全审计 **（Security Audit）**	对系统记录和活动进行独立审查和检查，以确定系统控制的适当性，确保符合既定的安全政策和程序，检测安全服务中的违规行为，并推荐针对防范措施所需的任何变更。 来源：https://csrc.nist.gov/glossary/term/security_audit
安全事件 **（Security Incident）**	一种实际或潜在地危及信息系统的保密性、完整性或可用性，或者危及系统处理、存储或传输的信息，或构成违反安全政策、安全程序或可接受使用政策的侵犯或即将发生的安全威胁的事件。 来源：https://csrc.nist.gov/glossary/term/security_incident
安全补丁 **（Security Patch）**	通常来自安全开发人员的更新会传递给任何需要该更新的设备。延迟的补丁更新通常是因为在软件最初发布或大更新推出之前，并未发现某个漏洞或问题。 来源：CyberDB: What is a Patch in Cybersecurity?
安全令牌 **(Security Token)**	安全令牌是用户访问系统所必须的物理设备。身份验证数据必须在用户和系统之间交互，从而验证身份和访问权限。安全令牌是上述数据的传输通道。 来源: Okta: What Is a Security Token?
安全令牌服务 **（Security Token Service, STS）**	为*（身份）*联邦内请求访问的受信任系统、用户和资源，发放、验证、更新和注销安全令牌的组件。 来源: Radiant Logic: Secure Token Service

敏感数据扫描 **(Sensitive Data Scanning)**	是识别以各种格式存储的敏感数据的过程，例如文档、数据库和其他数字文件。敏感数据扫描的主要目的是识别组织内所有与个人身份信息（PII）相关的数据，确定此类数据的数量和位置，并评估数据的安全性。数据扫描可能有类似的名称，如敏感数据发现工具、PII 扫描工具和机密数据扫描。数据扫描使用的工具有不同的功能，如在存储或传输敏感数据时对其进行检测。其他一些工具还可以评估每项数据的脆弱性及其对数据安全标准的重要性。 来源： https://www.splunk.com/en_us/blog/learn/data-scanning.html
单点登录 **（Single Sign-On, SSO）**	提供单次身份验证的能力，并在访问各种目标系统时自动进行后续的验证。它消除了需要单独对个别应用程序和系统进行验证和登录的需求，本质上充当了客户工作站和目标系统之间的用户代理。 来源: https://www.gartner.com/en/information-technology/glossary/sso-single-sign-on
威胁 **(Threat)**	任何可能通过信息系统未经授权的访问、破坏、披露、修改或拒绝服务，对组织运营（包括使命、职能、形象或声誉）、组织资产、个人、其他组织或国家造成不利影响的情况或事件。 来源: https://www.niap-ccevs.org/Ref/CNSSI_4009.pdf (March 2, 2022,Page 200)

第三方供应商 **(Third Party Providers)**	支持组织运营制造系统的外部服务提供商、集成商、供应商、电信以及基础设施。 来源: Third-party Providers - Glossary | CSRC (nist.gov)
威胁情报 **(Threat Intelligence)**	指经过聚合、转换、分析、解释或丰富的威胁信息，为决策过程提供必要的背景信息。 来源: https://csrc.nist.gov/glossary/term/threat_intelligence
威胁与漏洞管理 **(Threat & Vulnerability Management)**	这个领域涉及安全核心问题，如漏洞管理、威胁管理、合规性测试和渗透测试。漏洞管理是一项复杂的工作，企业通过跟踪其资产，监控、扫描已知/新出现的漏洞，并采取修补软件、更改配置或部署其他的控制措施，以收敛资源层的攻击面。威胁建模和安全测试也是有效识别漏洞的一部分。这个领域旨在通过主动检查云基础设施，使用漏洞扫描、虚拟补丁以及安全测试和响应的其他手段来应对新的安全威胁。 来源: 企业架构参考指南 v2: CSA: 安全与风险管理（SRM）领域
令牌化 **(Tokenization)**	是一种保护高度敏感信息的技术，通过将其从数据库中移除并采用一个等效的、非敏感的元素替代。这个非敏感的元素被称为令牌。敏感数据被保存在一个高度安全、加密的保险库中。 来源: https://www.ibm.com/cloud/architecture/architectures/security-data-tokenization-solution/

传输层安全协议 **（Transport Layer Security, TLS）**	一种加密协议，是 SSL 的升级版本，用于在计算机或 IP 网络上的通信中提供安全性。 来源: https://csrc.nist.gov/glossary/term/transport_layer_security
战术、技术和程序 **(Tactics, Techniques, and Procedures, TTPs)**	攻击者的行为描述。**战术**是对这种行为的最高级别描述，而**技术**则是在战术背景下对行为的更详细描述，**程序**则是在技术背景下对行为的更低级、更详细的描述。 来源: https://csrc.nist.gov/glossary/term/tactics_techniques_and_procedures
虚拟专用网络 **(Virtual Private Network, VPN)**	现有物理网络基础上构建的虚拟网络，可以为在网络之间或同一网络上的不同节点之间传输的数据和 IP 信息提供安全的通信机制。 来源: https://csrc.nist.gov/glossary/term/virtual_private_network
脆弱性 **(Vulnerability)**	脆弱性是信息系统、系统安全程序、内部控制措施或实施中存在的可被威胁利用的弱点。 来源: Special Publication 800-30 Revision 1 Guide for Conducting Risk Assessments, National Institute of Standards and Technology
Web 应用防火墙 **(Web Application Firewall, WAF)**	应用防火墙，通过检查 HTTP 流量来监视、警报和阻止攻击。 来源: The Six Pillars of DevSecOps: Automation : CSA

白名单 **(Whitelisting)**	一种仅允许预先批准的实体访问特定服务或环境，而默认自动拒绝所有其他实体访问的方法。 来源: What is Whitelist and How Does It Work
零日漏洞攻击 **(Zero-day exploit)**	零日漏洞攻击是一种利用计算机软件、硬件或固件中未知或未解决的安全漏洞实施网络攻击的手段或技术。 “零日”指的是软件或设备供应商未及时修复漏洞前，恶意人员已利用它获取易受攻击系统的访问权。 来源： IBM: What is a zero-day exploit
零日漏洞 **(Zero-Day Vulnerability)**	系统或设备中已经被披露但尚未修补的漏洞。由于这些漏洞在安全研究人员和软件开发人员意识到它们之前就被发现，并且尚未发布修复补丁，当网络罪犯竞相利用这些漏洞来牟利时，零日漏洞将对用户构成更高的风险。在供应商发布补丁之前，易受攻击的系统会一直暴露在风险之中。 来源: Trend Micro: What is a zero-day vulnerability?
零知识证明 **（Zero Knowledge Proof, ZKP）**	在密码学中，**零知识证明**或**零知识协议**是一种方法，通过该方法，一方（证明者）可以向另一方（验证者）证明给定的陈述是正确的，同时避免向验证者传达任何超出该陈述的信息。 仅仅是陈述的真实性。 来源：https://en.wikipedia.org/wiki/Zero-knowledge_proof

零信任 **（Zero Trust，ZT）**	零信任是一种网络安全策略，其基本理念是默认不信任任何用户或资产。它假设入侵已经发生或即将发生，因此，不应该通过企业边界单一的验证来授予用户敏感信息的访问权。相反，每个用户、设备、应用程序和交易都必须不断地进行验证。 来源： https://cloudsecurityalliance.org/blog/2023/06/20/cisa-s-zero-trust-maturity-model-an-important-step-forward-in-implementing-zero-trust-security-principles

CSA GCR cloud security alliance GREATER CHINA REGION ®

Cloud Security Alliance Greater China Region

扫码获取更多报告

云安全联盟大中华区
官网：https://c-csa.cn 电话：0755-86548359
地址：上海市浦东新区东育路255弄5号3FB30（前滩国际经济组织集聚区）/
广东省深圳市南山区粤海街道北京航空航天大厦1号楼905