了解云攻击向量

从 IaaS 和 PaaS 视角

CSA GCR cloud security alliance GREATER CHINA REGION ®

CSA cloud security alliance ®

关于云安全联盟

云安全联盟（CSA）是一个非营利组织，旨在促进和推广云计算的最佳实践，并提供行业内的安全保证。此外，云安全联盟提供云计算使用的教育，以帮助确保其他形式的计算安全。云安全联盟是由一个行业从业者、企业、协会和其他主要利益相关者组成的广泛联盟领导。。欲了解更多信息，请访问 www.cloudsecurityalliance.org，并关注我们的 Twitter 账号@cloudsa。

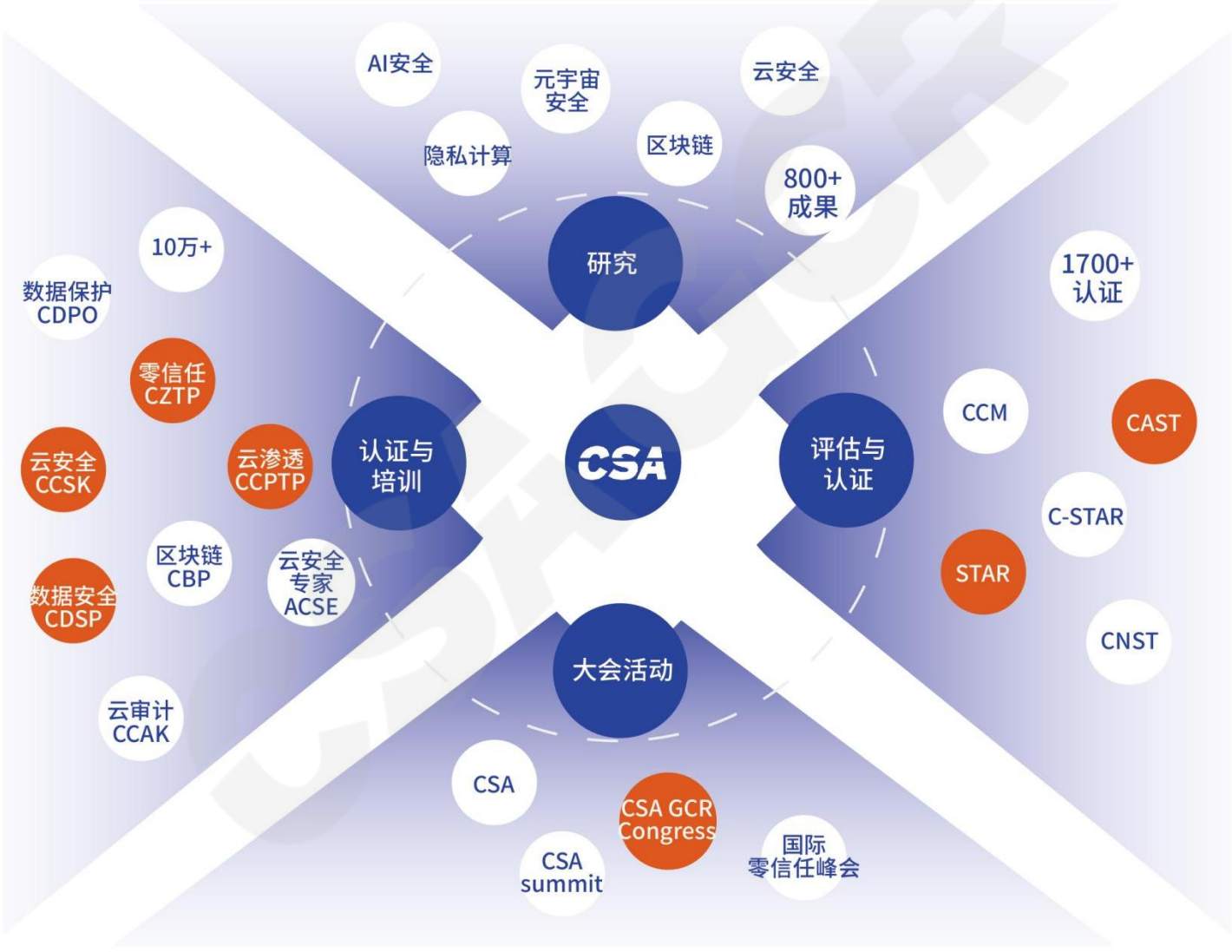
联盟简介

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

报告中文版支持单位

腾讯云鼎实验室成立于 2016 年，是腾讯安全旗下的顶级实验室之一。秉承“一切以用户价值为依归”的理念，云鼎实验室坚持研究创新和实践落地并重的技术路线，专注于云安全技术研究和创新工作，在大规模云安全防护和治理、云原生安全技术、密码学和云数据安全、容器和虚拟化安全、硬固件和基础设施安全等多个领域展开技术研究和产品创新工作。云鼎实验室同时也负责腾讯云平台自身的安全建设、防护和治理工作，通过安全治理体系建设、持续性安全攻防对抗、大数据安全运营平台、和云原生安全托管服务（Cloud-MSS）持续保障腾讯云平台及云上数百万租户的安全。

腾讯是 CSA 全球会员单位，支持该报告内容的翻译，但不影响 CSA 研究内容的开发权和编辑权。

主要贡献专家：

李鑫、高瑞强

报告英文版编写专家

贡献者：

Dina Agafonov　Daniel Begimher　Tony Daskalo　Gidi Farkash　Moshe Ferber

Michael Roza　Yuval Segev　Omri Segev Moyal　Dana Tsymberg　Zur Ulianitzky

审校者：

Oren Elimelech　Eyal Estrin　Patrick Gaw　Chris Kirschke　Mauricio Mendoza Clavero

Venu Reddy　Eitan Satmary　Yuval Sinay　Peter van Eijk　Kobi Zvirsh

CSA 全球员工：

Frank Guanco　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。

序言

随着云计算技术的迅猛发展，越来越多的组织将数据和业务迁移到云平台上，享受着云计算带来的弹性、可扩展和便捷的优势。在云环境中，IaaS（基础设施即服务）和PaaS（平台即服务）作为两种常见的云服务模型，为组织提供了强大的托管应用程序和基础设施的能力。然而，云计算环境也面临着来自不断演化的网络威胁和攻击的挑战。

本白皮书旨在针对 IaaS 和 PaaS 服务模型，详细梳理常见的云攻击向量，并通过与相关的 CSA 研究和其他威胁模型对应，将这些攻击向量一一列举出来。本文包含八个与 IaaS 和 PaaS 相关的攻击向量，涵盖了工作负载、存储等方面的错误配置或漏洞。

我们意识到，尽管风险、威胁和漏洞的数量和重要性不断上升，但使用的攻击向量相对稳定。因此，通过深入了解这些攻击向量，组织可以更好地理解针对云托管应用程序和基础设施的常见攻击方式，并明确在控制和安全工作中需要重点关注的领域。

相信通过阅读本白皮书，组织将能够深入了解这些重要的云攻击向量，并为保护其在云环境中的应用程序和基础设施做出明智的决策。我们希望本白皮书对于提高云安全意识、加强防御措施以及规避潜在威胁带来积极的促进作用。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

目录

简介

我们在不断加深对云上风险和威胁的认识与发展过程中，CSA 顶级威胁等工作组以及其他组织为我们对这一主题的了解和理解作出了巨大贡献。我们尽管已经记录了许多对业务产生广泛影响的风险和威胁，但还是发现其中许多风险和威胁只利用到了少量的攻击向量。这正是本项研究的主题所在。

为了进行本项研究，我们首先回顾了近期大量 IaaS 与 PaaS 相关的安全事件，并将这些事件的细节细化为实际利用的攻击向量。我们使用 CSA 顶级云安全威胁案例、MITRE 相关分析以及之前对云事件的研究，尽可能多的分析安全事件。

在我们制定了完整的向量列表后，我们邀请了一批在云攻击方面经验丰富的专业人士。我们利用我们的集体经验将不同的个体分组，成为一组八个的主要攻击向量，我们发现它们在各种攻击场景中都非常有效。

本文档的目的

本研究的目标是梳理常见的 IaaS/PaaS 攻击向量并逐一列举，与相关的 CSA 研究和其他威胁模型对应。通过阅读本文档，组织将更好地了解针云托管应用程序和基础设施的攻击中常用攻击向量，并制定在控制和安全工作上应该重点关注的领域。

文件结构和范围

该文档由八个与 IaaS/PaaS 相关的攻击向量组成。每个向量章节包括两部分：

- 主要部分包括以下内容：向量的定义和描述、利用方式、如何避免或减轻该向量的关键要点、利用该向量的示例
- CSA 和非 CSA 框架的攻击向量映射，在本项研究中将会提供更多深入的见解以及相关控制措施。映射包括：
    - 将攻击向量映射到 MITRE 中的相关技术或缓解措施
    - 将攻击向量映射到责任共担模型 - 将相关攻击向量映射到不同责任方：云服务提供商(CSP)、云服务客户(CSC)或共享责任
    - 将攻击向量映射到 CSA 安全指南（第 4 版）中的相关领域，添加有关向量的更多知识

- 将攻击向量映射到 CSA 云控制矩阵(CCM)版本 4.0.X，识别与向量相关的控制措施。X 版本标签标记新的控制措施映射，因此我们的文档与 4.0 版本相关
- 将攻击向量映射到 STRIDE 威胁模型，添加有关向量的更多知识
- 将攻击向量映射到 CSA 顶级威胁研究，帮助识别相关的风险和威胁

目标受众

本文档的目标受众是：

- 对想要了解更多关于实际攻击向量信息感兴趣的，负责云环境安全的 GRC 专业人员和审计人员
- 正在构建 IaaS/PaaS 环境，并寻求安全帮助的安全专业人员、DevOps 和 DevSecOps 专业人员、软件和安全架构师以及 IT 安全人员

IaaS 和 PaaS 云攻击向量

在深入研究攻击向量的详细信息之前，了解 IaaS 和 PaaS 等不同的云服务模型非常重要。

- IaaS（基础设施即服务）：在 IaaS 环境中，客户对基础设施和操作系统具有更多的控制权。这意味着攻击面更大，因为客户需要负责保护自己的虚拟机、存储和网络。在 IaaS 环境中，常见的攻击向量通常针对虚拟机、存储和网络安全设置中的错误配置或漏洞。
- PaaS（平台即服务）：在 PaaS 环境中，客户对软件和应用程序代码拥有更多的控制权，但对基础设施的控制权较少。攻击面与 IaaS 类似，但更加关注应用程序代码和配置中的漏洞。

网络攻击向量是指攻击者用于访问计算机或网络服务器以传递恶意成果的路径或手段。这些向量可以包括多种策略，例如恶意软件、网络钓鱼和社会工程学等，旨在利用目标系统的脆弱点和漏洞。

在云环境中，网络攻击向量可以以多种方式呈现。举例来说，攻击者可能使用网络钓鱼电子邮件诱使用户点击恶意链接或输入其登录凭据。此外，攻击者还可利用云服务

中的漏洞（如错误配置的权限）获取敏感数据的访问权限。

网络攻击向量与脆弱点或漏洞之间的区别在于它们的性质。脆弱点或漏洞是指可以被威胁利用的资产或存在的控制弱点。

另一方面，网络攻击向量是攻击者利用这些脆弱点或漏洞的特定方法或技术。

例如，云服务中的漏洞可能是配置错误的防火墙，允许未经授权的网络访问。在这种情况下，网络攻击向量可能是 SQL 注入攻击，攻击者使用特制的 SQL 查询访问网络上的敏感数据。

软件即服务 (SaaS)、基础设施即服务 (IaaS) 和平台即服务 (PaaS) 的攻击向量区别在于客户对环境的控制级别，而攻击向量存在于所有级别在云堆栈中，服务模型决定由谁负责及缓解。

这项研究的重点是：研究针对 IaaS 和 PaaS 消费者的攻击向量。IaaS 环境中的攻击向量通常是针对虚拟机、存储和网络安全设置中的错误配置或漏洞。

在 PaaS 环境中，客户对软件和应用程序代码有着更多的控制权，但对基础设施的控制权较少。PaaS 环境中的攻击面与 IaaS 类似，但更关注应用程序代码和配置设置中的漏洞。

除了通过用户凭证之外，SaaS 的消费者几乎无法控制云攻击向量。因此，在本研究中，大部分缓解工作将由 SaaS 提供商负责。然而，SaaS 中还存在其他攻击向量，例如利用 Web 应用程序中的漏洞，这是 SaaS 提供商的责任。

需要注意的是，这些攻击向量并不是相互排斥的，攻击者可能会使用多种策略组合，危害目标。因此，客户需要遵循安全最佳实践，并应用多层安全控制措施降低网络攻击带来的风险。

1：可利用的工作负载

定义

根据 CSA 安全指南（第 4 章，7.4 节），CSA 将工作负载定义为“处理单元，可以在虚拟机、容器或者其他的抽象中”。可利用的工作负载是一种攻击向量，详细描述了攻击者利用工作负载的漏洞，在云环境中获取初始访问的能力。这些漏洞可以是已知的漏洞，也可以是零日漏洞。如果不加以缓解，这种对云环境的初始访问可能会增加与攻击向量相关的风险。这种攻击方法的一个常见影响是利用它运行加密货币挖矿或勒索软件攻击。在其他情况下，利用先进的技术，可以使用附加或存储的云凭据在环境中移动，获得数据访问权限，或在云环境中提升权限和横向移动。

描述

可利用的工作负载是指由于云上网络配置错误，从而对内部或外部攻击者提供访问权限的任何虚拟机或容器。如果工作负载具有公网 IP 地址，或者攻击者已经能够访问内部环境，那么可达性就会实现。“可利用的工作负载”表示该资产容易受到配置错误的影响，存在已知的常见漏洞（CVE）和应用程序漏洞等。通过结合访问权限和现有漏洞，攻击者可以成功获取访问权限、控制权或利用云工作负载来进一步实施攻击。**在这种攻击向量中，受损的资产可能会导致攻击者在云环境中实现持久化、获得数据访问权限或进行权限提升。接下来，攻击者可以利用该资产加强其访问和控制能力，执行横向移动操作并寻找其他目标资产。**

要点

为了强化云环境，应该在攻击路径的所有节点上实现安全保护。

- **网络**：尽可能限制网络访问，最好是私有子网并使用安全组和微隔离。使用 IP 限制，专门设定无类别域间路由(CIDR) 范围，并开放对选定端口的访问，而不是过于宽泛的端口访问范围。只要有可能，就使用安全屏障保护对外开放的服务，例如负载均衡器、API 网关和/或 Web 应用程序防火墙 (WAF)。
- **漏洞**：定期扫描所有工作负载以检测已知漏洞，并通过建议的补救措施修复。建议专门针对组织的云环境执行安全评估，确保发现未知风险。请记住，不同的工作负载需要不同的漏洞扫描工具（即容器可能需要与虚拟机不同的工具）。应使用自动

化工具（用于检测开源软件包中的漏洞的软件组合分析工具、用于检测代码中的漏洞的 SAST/ DAST/IAST 工具【取决于应用程序类型】等）执行漏洞扫描，并将其嵌入到持续集成/持续交付(CI/ CD)流程。

- **身份和访问管理(IAM)**：所有对资源的访问都必须经过身份验证和授权。遵循最小权限或已知权限的原则，并向工作负载提供所需的最低权限，使工作负载能够执行指定的任务并将应用程序机密存储在安全位置。
- **应用程序**：确保应用程序的设计符合公认的原则安全开发，包括自动修补。

典型事件和案例

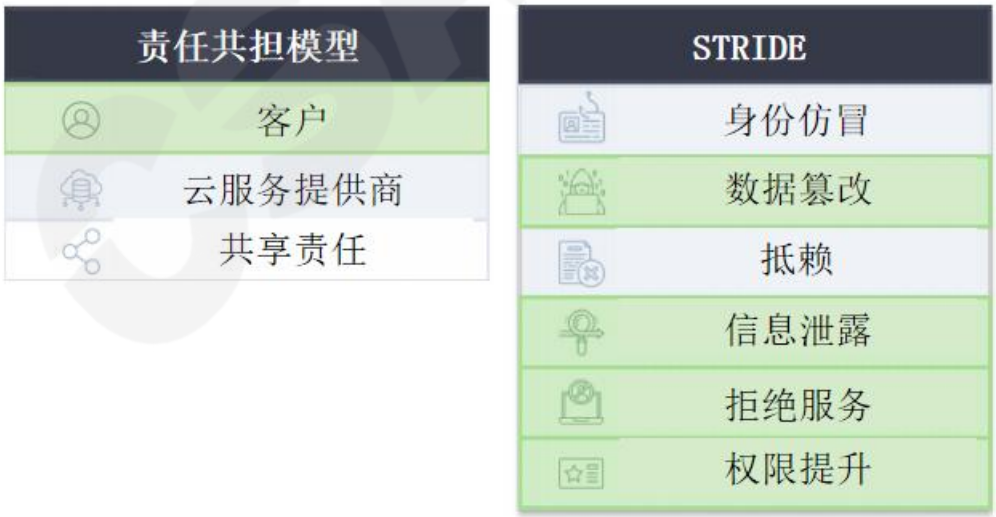
请参阅以下典型事件和案例：

- New TeamTNT Cryptojacking Malware Targeting Kubernetes
- Atlassian Confluence Servers Hacked via Zero-Day Vulnerability

适用于企业 TTP 的 MITRE ATT&CK

请参阅“利用面向公众的应用程序”，MITRE ID： T1190.

责任共担模型和 STRIDE 威胁建模图



CSA CBK 安全指南 4.0 版

领域 4：合规性和审计管理

领域 7：基础设施安全

领域 11：数据安全和加密

CSA CCM Controls 4.0.X 版

AIS - 应用程序和接口安全

AIS- 06：自动化安全应用程序部署

AIS- 07：应用程序漏洞修复

CCC - 变更控制和配置管理

CCC- 06：变更管理基线

CCC- 07：基线偏差检测

IVS - 基础设施和虚拟化安全

ISV- 04：操作系统强化和基本控制

TVM - 威胁和漏洞管理

TVM- 01：威胁和漏洞管理政策和程序

TVM- 03：漏洞修复计划

TVM- 04：检测更新

TVM- 07：漏洞识别

TVM- 08：漏洞优先级排序

CSA Top 威胁映射

此攻击向量与以下内容相关：

安全问题 7：系统漏洞

安全问题 9：Serverless 和容器工作负载的错误配置和利用

2：工作负载权限过高

定义

以下攻击向量描述了云环境中具有过高权限的工作负载。在云环境中，工作负载如虚拟机或容器，通常会分配一个身份或角色，用于执行在云基础设施上的操作。一个典型的例子是为虚拟机分配角色，以便其可以访问云存储。遵循这一向量，如果攻击者能够获取对工作负载的访问权限，就可以利用这些权限获取对整个环境的更高权限。

描述

工作负载是一个处理单元，可以在虚拟机、容器或其他抽象概念（如 Serverless 或 FaaS）中运行。常见的做法是创建工作负载，承载多个作业或任务，这些任务可能具有不同的访问模式和身份验证要求，并需要访问各种服务和资源。为了管理对特定服务和资源的访问，权限通常以策略或角色的形式分配给工作负载。这种复杂性给特定服务和资源的访问管理带来了挑战，从而导致了不良的安全实践，例如过度赋予权限的现象。

这种攻击向量强调了特权提升的可能性。攻击者通常会以低级别权限获得初始访问权限，工作负载过高的权限可能会导致特权提升，攻击者可以通过这种攻击向量获得更好的持久化效果和造成更多危害的能力。

要点

- 始终遵循最小权限原则，为工作负载提供执行分配到的任务，所需的最低权限。
- 优先选择使用临时访问令牌而不是永久权限。
- 与预定义和一般角色相比，应优先定制策略和角色。
- 尝试通过使用权限边界、承担角色等功能更进一步细化您的策略。
- 防止激活具有高权限的本地用户账户，尤其是在使用容器时。
- 验证和审核工作负载的权限，确保没有过多的权限。

典型事件和案例

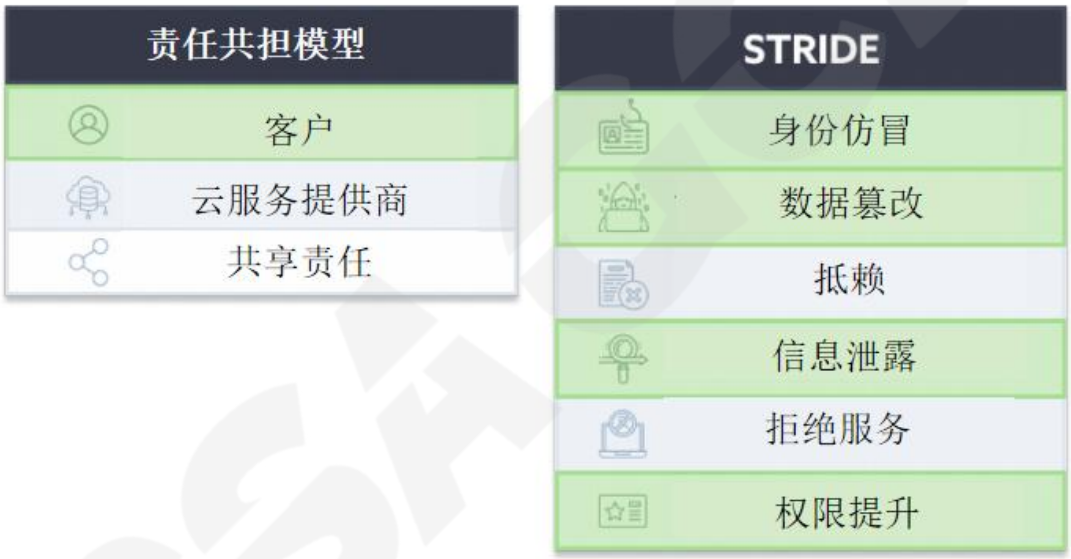
请参阅以下典型事件和案例：

- Lessons learned from the Capital One breach
- The attack on ONUS – A real-life case of the Log4Shell vulnerability

适用于企业 TTP 的 MITRE ATT&CK

请参阅“特权客户管理”，网址为 MITRE ID：M1026.

责任共担模型和 STRIDE 威胁建模图



CSA CBK 安全指南 4.0 版

领域 6：管理平面和业务连续性

领域 7：基础设施安全

领域 12：身份、授权和访问管理

CSA CCM CONTROLS 4.0.X 版

CCC - 变更控制和配置管理

CCC- 06：变更管理基线

CCC- 07:基线偏差检测

IAM - 身份和访问管理

IAM- 01：身份和访问管理政策和程序

IAM- 05：最小权限

IAM- 06：用户访问配置

CSA Top 威胁映射

此攻击向量与以下内容相关：

安全问题 1：身份、凭据、访问权限和密钥管理、特权账户不足

安全问题 2：不安全的接口和 API

安全问题 3：配置错误和变更控制不足

3：不安全的密钥、凭证和应用密钥

定义

该攻击向量详细说明了云工作负载、服务或代码存储库中可能存在的明文凭证或未受保护的凭证。这些凭证可能采用不同的形式，并存放在不同的位置。常见的攻击向量包括将 IAM 访问 keys 或 API keys 嵌入配置文件、模板或实际代码中，或者将 SSH keys 嵌入到镜像或工作负载中。这些类型的凭证被称为密钥。

描述

在云服务中，不同的服务之间需要交互，包括与外部服务通信。这种交互涉及到一组权限，因此需要身份验证和授权机制来确保安全性。该机制使用 API 或访问密钥对消费类服务或工作负载进行身份验证并授予相应的权限。

举例来说，一个常见的用例是 EC2 实例为了存储或检索数据，需要访问 S3 存储桶，或者 CI 服务需要 API 密钥验证外部代码存储库的身份。

另一种常见场景是使用 SSH 密钥管理一组虚拟机，从而为管理 SSH 密钥带来挑战。由于访问密钥管理的复杂性，组织对多个计算实例使用相同的密钥。因此，攻击者在攻陷一台服务器后，可以访问使用相同 SSH 密钥对的所有服务器。这是在云环境中移动、收集更多信息并搜索更高权限的简单方法。

许多组织未能建立明确的密钥生命周期管理（生成、存储、检索、轮换和退役）策略，从而导致未经授权的资源访问、执行横向移动的能力以及环境中特权的提升。

要点

存储和使用 API 密钥、密钥、密码、SSH 密钥或证书的推荐最佳实践取决于实际的访问场景。以下是一些示例：

- 云提供商工作负载访问同一提供商的服务：向工作负载授予访问权限的建议方法是为其附加具有所需权限的身份。这将消除对静态访问密钥的需要，并动态分配密钥。此类解决方案的示例包括 AWS STS、GCP OICD 或 Azure SAS。
- 应用程序组件之间交互或与云外部服务交互时，可以将机密存储在指定的安全存储中。示例包括 AWS Secrets Manager、Azure Key Vault 或 GCP Secret Manager。

- 对于 SSH 密钥、具有一次性 SSH 密钥的安全堡垒主机（“jump box”）或基于 IAM 的身份验证解决方案（即 AWS Session Manager、Azure Bastion 或 Google Identity-Aware Proxy）可用于最大限度地提高安全性。一些企业解决方案还支持 MFA 和 SSH 身份验证机制。此外，建议针对不同的环境和分类，使用不同的 SSH 密钥。
- 遵循从生成到撤销的任何密钥生命周期的安全程序。
- 将密钥存储在指定的企业服务中（例如 AWS Secrets Manager、Azure KeyVault 或 GCP Secret Manager）。
- 智能的管理开源解决方案中的公共分发流程，例如容器将流程发布到公共容器注册表或该组织开发并在公共开源存储库中共享的代码库。
- 监控访问日志以检测与访问密钥和凭证相关的任何可疑活动。

要检测不同位置上的明文机密，我们建议定期扫描云工作负载配置、基础架构即代码模板和代码存储库，搜索静态凭据和 key/secrets。

典型事件和案例

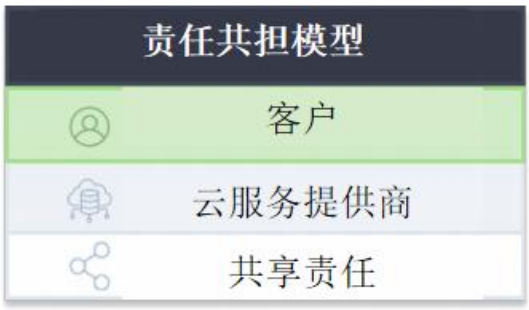
请参阅以下典型事件和案例：

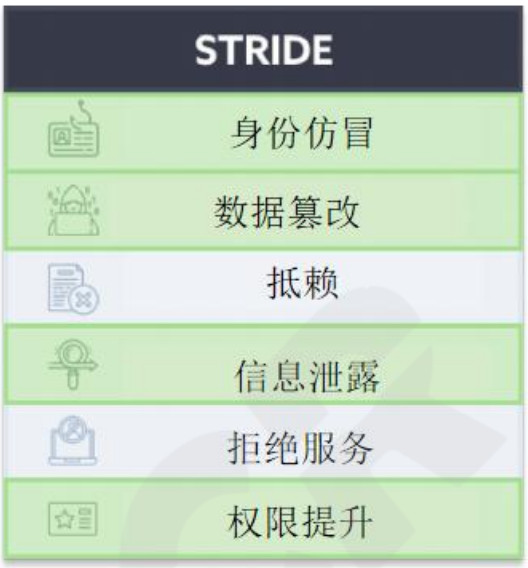
- CircleCI says hackers stole encryption keys and customers’ secrets
- Howebrew Security Incident Disclosure
- Samsung spilled SmartThings app source code and secret keys
- website Animal Jam breached after miscreants spot private AWS key
- GotRoot! AWS root Account Takeover

适用于企业 TTP 的 MITRE ATT&CK

请参阅“不安全的凭证”，网址为 MITRE ID：T1552.

责任共担模型和 STRIDE 威胁建模图





CSA CBK 安全指南 4.0 版

领域 6：管理平面和业务连续性

领域 7：基础设施安全

领域 10：应用程序安全

领域 12：身份、授权和访问管理

CSA CCM CONTROLS 4.0.X 版

AIS - 应用程序和接口安全

AIS- 06：自动化安全应用程序部署

CCC - 变更控制和配置管理

CCC- 03：变更管理技术

CCC- 07：基线偏差检测

CEK - 密码学、加密和密钥管理

CEK- 21：关键库存管理

IAM - 身份和访问管理

IAM- 06：用户访问配置

IAM- 13：唯一可识别用户

IAM- 15：密码管理

IPY - 互操作性和可移植性

IPY- 02：应用程序接口可用性

CSA Top 威胁映射

此攻击向量与以下内容相关：

安全问题 1：身份、凭据、访问权限和密钥管理、特权账户不足

安全问题 2：不安全的接口和 API

安全问题 3：配置错误和变更控制不足

安全问题 11：云存储数据泄露

4：可利用的身份验证或授权

定义

该攻击向量详细描述了对实体（如用户、工作负载、功能、角色、组等）的不当管理和身份验证。每个身份都应该受到安全控制，并得到适当的维护。忽视某些身份，即长期未被使用或根本未被使用但拥有过高权限的身份，可能会导致未被察觉的攻击行为，从而对该身份造成风险。

描述

保持健康的安全环境是非常重要的。虽然这并不是一项容易的任务，关注 IAM 的最佳实践至关重要，因为它通常是攻击者首先检查和尝试利用的目标。

不当的管理有多种形式：

- 使用默认密码。一些工具在安装时使用默认密码，管理员无法更改这些默认密码，导致了安全风险的存在。另外，弱密码策略也是一个问题。如果没有定义强密码策略，攻击者可以使用众所周知的技术（如字典攻击、暴力破解等）轻松猜测密码，并获取目标用户的身份以登录其云环境。
- 空组。组通常是为了将用户聚合成一个实体而创建的。在云环境中，可以给组分配权限，并授权其中的用户。这些权限也会被授予组中的所有用户。当添加新用户到组时，这些用户也将被授予该组已有的权限。因此，如果攻击者能够访问 IAM 并且可以重新填充该组，那么未分配给任何用户的组会对环境带来风险。
- 过高的权限。将特定权限授予给资源可能是一项繁琐的任务，这就是为什么我们经常看到用户或组无正当理由地拥有过高的权限。这个安全问题可能导致攻击者访问敏感资源并执行可能损害环境的操作。
- 未开启 MFA。未开启多重身份验证（MFA）时，用户缺乏额外的保护层。在没有启用 MFA 并且仅使用静态凭据（例如用户名和密码）进行身份验证时，攻击者一旦获得这些凭据的访问权限（例如通过网络钓鱼），就有可能轻松的破坏系统环境。首选方法是使用 Google Authenticator 等身份验证器。
- 不活动的身份。可以通过审核日志和上次登录记录来跟踪非活动的身份或用户的活动。这些被认为是被忽视的身份，因为它们通常没有受到监控或维护，可能对环境

构成风险。

- 无日志记录。源端不记录 AAA 操作，导致无法检测恶意利用。
- IAM 信任策略配置错误。如果错误配置身份和访问管理中的外部身份和跨账户访问的信任策略，可能导致对受害者云账户的未经授权的初始访问。

要点

为了主动阻止这种攻击路径，组织应该：

- 启用 MFA。MFA 对所有用户和所有应用程序都应该是强制性的。
- 创建强密码策略。确保用户密码不会轻易被泄露。除了标准密码策略的复杂性（长度、大写字母、小写字母、数字和非字母数字字符）之外，管理员还应该设置密码过期时间并配置设置，以便过期密码需要管理员重置并防止密码重复使用。
- 临时访问。使用临时访问（例如 AWS Assume Role 或 Azure Just- in- Time）而不是静态凭证/权限。
- 重新评估权限。审核和监控政策并确保遵循最小权限原则。
- 空组。如果存在没有用户的组，请删除该组。
- 不活跃的身份。使用审核日志和上次登录记录监控身份活动。如果某个身份在规定的时间内（由组织确定）看起来处于非活动状态，建议将其删除。确保账户在退出流程中被删除。
- 强制记录。对云中的任何 AAA 操作实施日志记录和审核应用级别。

典型事件和案例

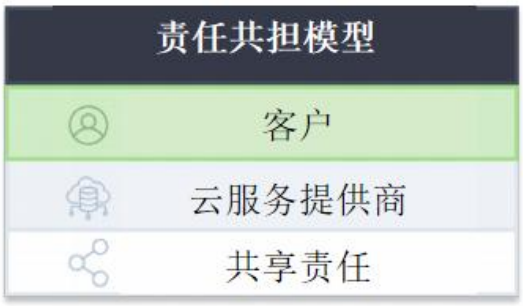
请参阅以下典型事件和案例：

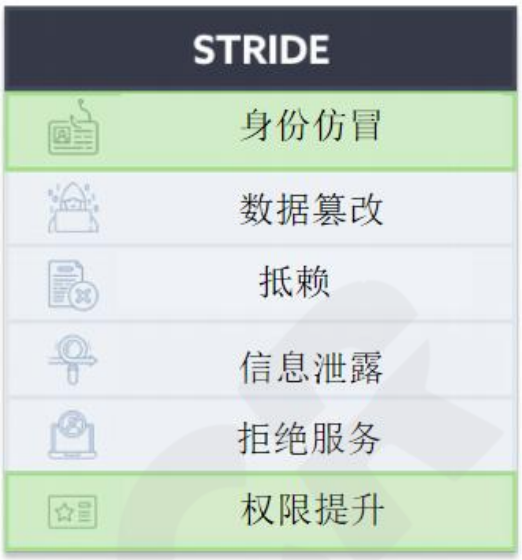
- Hacker Puts Hosting Service Code Spaces Out of Business
- Admin Accounts With No Passwords at the Heart of Recent MongoDB Ransom Attacks
- Equifax used the word ‘admin’ for the login and password of a database

适用于企业 TTP 的 MITRE ATT&CK

请参阅“有效账户：云账户”，网址为 MITRE ID：T1078.

责任共担模型和 STRIDE 威胁建模图





CSA CBK 安全指南 4.0 版

领域 2：治理和企业风险管理

领域 4：合规与审计管理

领域 5：信息治理

领域 6：管理平面和业务连续性

领域 12：身份、授权和访问管理

CSA CCM CONTROLS 4.0.X 版

AIS - 应用程序和接口安全

AIS- 01：应用程序和接口安全政策和程序

AIS- 02：应用程序安全基线要求

AIS- 03：应用程序安全指标

IAM - 身份和访问管理

IAM- 01：身份和访问管理政策和程序

IAM- 02：强密码政策和程序

IAM- 03：身份清单

IAM- 14：强身份验证

LOG - 日志记录和监控

LOG- 01：记录和监控政策和程序

CSA Top 威胁映射

此攻击向量与以下内容相关：

安全问题 1：身份、凭据、访问权限和密钥管理、特权账户不足

安全问题 2：不安全的接口和 API

5：未经授权访问对象存储

定义

对象存储是云中最常见的服务之一。该攻击向量详细描述了云托管存储中存在的公共对象的情况，这些对象无需用户身份验证或授权（通常是由于配置错误导致）。在未经授权的情况下，攻击者可以利用常见工具读取和/或写入数据，从而危害存储数据的可用性、完整性或机密性。

描述

云对象存储在任何部署中的都属于关键因素，大多数应用程序都需要某种形式的存储。假设这些云存储被错误配置为无需额外授权即可公开访问。在这种情况下，攻击者可以使用现成的实用程序破坏数据存储和其中的数据，很可能在不被发现的情况下进行攻击。

对象存储服务构建的主要安全配置有以下几种：

- 公有/私有。在讨论公共云对象存储时，公有和私有之间的区别指的是网络访问（通过端点或主机名）和附加的身份控制措施，例如允许匿名用户从存储中读取和/或写入。在对象存储中创建存储组件时，用户可以选择存储是公有的还是私有的。此配置控制存储的访问设置。当访问是公开的时，存储不需要授权，任何实体都可以访问它，没有特殊限制。
- 加密。根据事件后响应报告显示，许多云存储组件静态存储时是公开且未加密的。使用云原生加密密钥通常需要额外的权限，但这可以防止数据在某些情况下受到损害。
- 身份验证。一些公共云对象存储提供多种配置选项来对资源进行身份验证。大多数情况下，提供无身份验证或基本身份验证（用户名和密码）的选项。其他高级选项包括安全断言标记语言（SAML）或 OpenID connect (OIDC)，或基于云原生 IAM 的身份验证。后一种身份验证方法比前一种方法更能抵御外部攻击。
- 除了这些安全配置之外，还可以实施其他预防措施：
- 安全意识培训。对用户进行对象存储安全意识培训对于维护云中存储的敏感数据的机密性、完整性和可用性至关重要。培训还可以帮助用户识别网络犯罪分子用来诱

骗用户泄露敏感信息或点击恶意链接的网络钓鱼尝试和其他社会工程策略。最终，训练有素的用户群可以作为第一道防线，抵御网络威胁并帮助确保组织数据的安全。

- 安全扫描。对象存储的安全扫描可以成为一种有效的工具识别可能导致数据容易受到攻击的错误配置。通过扫描对象存储中是否存在配置错误的存储桶、可公开访问的数据或设置不当的访问控制，组织可以在安全问题被网络犯罪分子利用之前主动检测和修复安全问题。定期安全扫描可以集成到组织的安全计划中，提供对对象存储安全状况的持续可见性，并帮助确保对数据的持续保护。

要点

为了主动保护云环境免遭对象存储攻击向量的未经授权的访问，组织可以：

- 保持所有对象存储的私有性。如果不打算公开对象存储或其中包含任何不应公开的数据，则最佳实践是将存储资产的设置更改为私有。
- 使用安全的共享流程。如果需要与外部各方共享数据，可以使用预签名 URL、AWS STS 或 Azure SAS 等解决方案提供临时访问。
- 网络安全控制措施。将所有网络都保留在您的私有对象存储中子网和 CSP 骨干网，而不是使用私有端点等服务穿越公共互联网。
- 使用加密密钥。确保所有对象存储资源在传输过程中和静态时都经过加密。优先使用客户管理的加密密钥并根据预定义的策略轮换密钥（至少每年一次）。使用 CSP 身份和访问管理机制管理对加密密钥的访问。
- 避免使用基本或无身份验证。虽然可能需要额外的资源和服务，但建议使用基于云原生 IAM 的身份验证或其他开放标准，例如 SAML、OIDC 等。
- 确保全面了解责任共担模型- 这涉及了解云服务提供商和使用云服务的组织之间的安全责任划分，并确定哪些安全措施是各方的责任。通过了解此模型并实施适当的安全措施，组织可以帮助确保云中对象存储的安全。

典型事件和案例

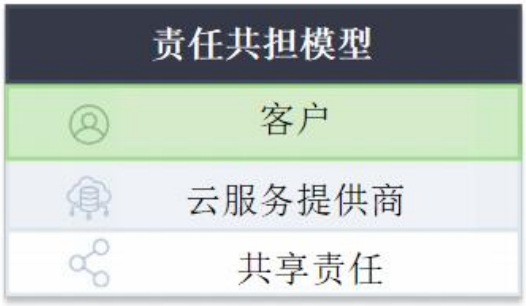
请参阅以下典型事件和案例：

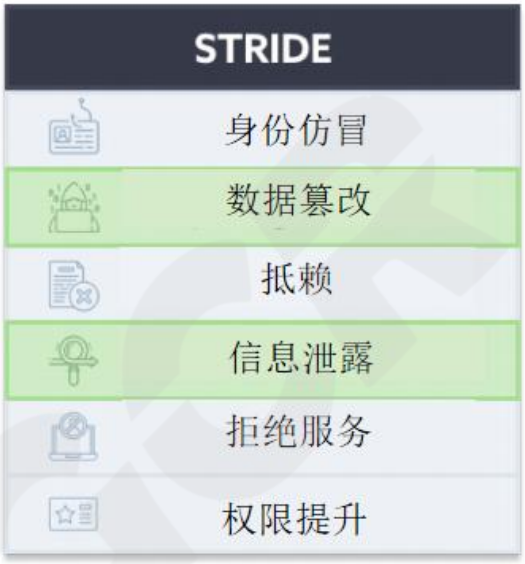
- How a Misconfigured Storage Bucket Exposed Medical Data
- Pfizer suffers huge data breach on unsecured cloud storage
- Millions of Verizon Customer Records Exposed through Open Amazon S3 Bucket

适用于企业 TTP 的 MITRE ATT&CK

请参阅“限制文件和目录权限”，网址为 MITRE ID：M1022.

责任共担模型和 STRIDE 威胁建模图





CSA CBK 安全指南 4.0 版

领域 5 - 信息治理

领域 7 - 基础设施安全

领域 12 - 身份、授权和访问管理

CSA CCM CONTROLS 4.0.X 版

A&A - 审计与鉴证

A&A- 06：修复

AIS - 应用程序和接口安全

AIS- 01：应用程序和接口安全政策和程序

AIS- 02：应用程序安全基线要求

AIS- 04：安全应用程序设计和开发

CCC - 变更控制和配置管理

CCC- 04：未经授权的变更保护

CCC- 06：变更管理基线

CCC- 07：基线偏差检测

DSP - 数据安全和隐私生命周期管理

DSP- 01：安全和隐私政策和程序

DSP- 07：设计和默认的数据保护

DSP- 12：个人数据处理目的的限制

DSP- 13：个人数据子处理

DSP- 17：敏感数据保护

HRS：人力资源

HRS- 03：清洁办公桌政策和程序

HRS- 12：个人和敏感数据意识和培训

IAM：身份和访问管理

IAM- 05：最低权限

IAM- 06：用户访问配置

STA- 03：SSRM 指南

STA- 04：SSRM 控制所有权

STA- 06：SSRM 控制实施

UEM- 通用端点管理

UEM- 11：数据丢失防护

CSA Top 威胁映射

此攻击向量与以下内容相关：

安全问题 8：意外数据泄露

安全问题 11：云存储数据泄露

6：第三方跨环境/账户访问

定义

此攻击向量详细说明了第三方实体或资源访问客户云环境时的信任策略。在此攻击向量中，当授予第三方实体或资源的访问权限过于宽泛，可能导致第三方公司接管账户。在某些情况下，即使权限授予的并不足够强大，但仍有滥用的风险。第三方可获取额外权限或身份，进而导致账户被接管。

描述

组织在支持、监控或保护其环境时，常依赖第三方供应商和托管服务提供商。这种访问可以通过多种方式实现，例如使用 API、IAM 角色、VPC 对等互连、代理软件，或者是由第三方控制的特定 VM 或容器驻留在客户环境中。如果第三方受到攻击或遭受损害，公司可能会面临一定的风险。

要点

- 在执行详细的安全评估后，合理地选择第三方提供商，确保供应商处于所需的安全级别
- 通过提供所需的最低权限实现最小权限原则，并拥有审查和削减权限的流程
- 如果可能（根据法律部门的批准），删除所有不使用的身份和第三方账户
- 确保为外部用户配置 MFA
- 外部支持服务的时间使用 AWS STS、Azure Privileged Identity Management 或 Azure Just- in 等技术
- 审核所有身份执行的所有操作，并确保有适当的日志记录机制检测异常行为
- 确保安全机制到位，防止未经授权的登录活动，例如，用于承担 IAM 角色的外部 ID
- 定期绘制共享资源图，并分析风险及其衍生含义

典型事件和案例

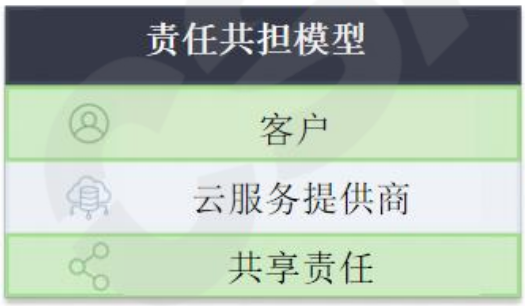
请参阅以下典型事件和案例：

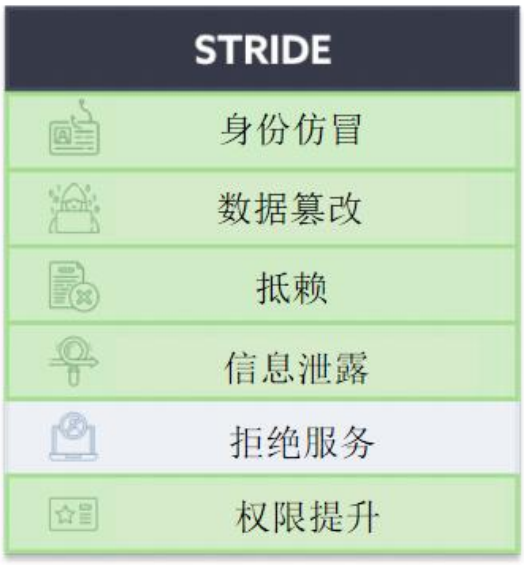
- Customer Guidance on Recent Nation-State Cyber Attacks
- CircleCI warns customers to rotate ‘any and all secrets’ after hack
- criminal actor targeting organizations for data exfiltration and destruction
- LiveAuctioneers Security Breach

适用于企业 TTP 的 MITRE ATT&CK

- Valid Accounts
- Valid Accounts: Cloud Accounts
- Steal Application Access Token
- Account Manipulation
- Exploitation for Privilege Escalation
- Trusted Relationship

责任共担模型和 STRIDE 威胁建模图





CSA CBK 安全指南 4.0 版

领域 2：治理和企业风险管理

领域 4：合规与审计管理

领域 6：管理平面和业务连续性

领域 7：基础设施安全

领域 12：身份、授权和访问管理

CSA CCM CONTROLS 4.0.X 版

IAM- 01：身份和访问管理政策和程序

IAM- 02：强密码政策和程序

IAM- 03：身份清单

IAM- 04：职责分离

IAM- 05：最低权限

IAM- 06：用户访问配置

IAM- 07：用户访问权限更改和撤销

IAM- 08：用户访问审核

IAM- 09：特权访问角色的隔离

IAM- 10：特权访问角色管理

IAM- 11：CSC 批准约定的特权访问角色

IAM- 12：保护日志完整性

IAM- 13：唯一可识别用户

IAM- 14：强认证

IAM- 15：密码管理

IAM- 16：授权机制

CCC- 04：未经授权的变更保护

DSP- 07：设计和默认数据保护

HRS- 10：保密协议

LOG- 0：记录和监控政策和程序

LOG- 02：审计日志保护

LOG- 03：安全监控和警报

LOG- 04：审核日志访问和责任

LOG- 05：审核日志监控和响应

LOG- 06：时钟同步

LOG- 07：日志范围

LOG- 08：日志记录

LOG- 09：日志保护

LOG- 11：事务/活动记录

LOG- 12：访问控制日志

LOG- 13：故障和异常报告

CSA Top 威胁映射

此攻击向量与以下内容相关：

安全问题 1：身份、凭据、访问权限和密钥管理、特权账户不足

安全问题 3：配置错误和变更控制不足

安全问题 4：缺乏云安全架构和策略

安全问题 6：不安全的第三方资源

安全问题 11：云存储数据泄露

7：不安全/未加密的快照及备份

定义

该攻击向量涉及云平台或服务中存在的不安全或未加密的快照或备份。这些快照/备份可能包含敏感信息，例如密码、个人数据或机密商业信息。如果没有采取加密或其他安全措施进行适当保护，未经授权的人员可能会访问这些快照/备份。因此，正确的保护方式是着以原始数据相同的安全级别保护它们。

这些快照/备份可以存储在不同的位置，通常用于数据丢失或其他中断情况下恢复数据。因此，确保对这些快照/备份的适当访问以及保持完整性级别非常重要。

本文档将使用短语“不安全备份”指代不安全或未加密的快照或备份。

描述

一些潜在的攻击向量正在使用不安全的云备份，包括：

1. 权限提升：攻击者可能使用不安全的备份进行横向移动或获得过多的权限（使用备份来定位密钥和密码）。

2. 勒索软件危害增强：攻击者可能会删除不安全的备份，阻止组织从勒索软件攻击中恢复。

3. 权限配置错误：如果备份没有正确配置适当的权限，未经授权的各方可能会访问备份，进而访问和操纵敏感数据。

4. 恶意代码注入：攻击者可能会使用不安全的备份作为向系统或网络注入恶意代码的手段，从而可能导致数据丢失、系统中断和其他负面影响。

要点

以下是防止不安全备份带来的潜在攻击向量的一些建议和最佳实践，如下所示：

- 在云备份上也使用数据最小化策略（通过数据保留策略），消除不必要的信息，从而降低风险。
- 对所有云备份账户使用强度高而独特的密码，并定期更新以防止未经授权的访问。
- 为云备份人员账户启用 MFA，并限制服务账户的访问已知的流量来源，以添加额外的安全层。

- 对所有云备份和快照使用加密，防止敏感数据被泄露被未经授权的各方访问。
- 使用客户管理的加密密钥，并将其存储在安全的保管库中（例如 AWS KMS、Azure Key Vault 或 Google Cloud KMS）。
- 每季度审查和更新所有云备份和快照的权限，确保只有授权身份才能访问。
- 实施备份和恢复计划，确保数据得到正确且轻松地备份，在数据丢失或其他中断期间恢复。
- 定期审查和更新安全措施，确保有效防范对备份和快照的潜在威胁。
- 将备份和快照保存在存档层或其他云提供商中，并进行适当的访问管理，以不可变的形式存储，并监控任何对备份和快照的访问。

典型事件和案例

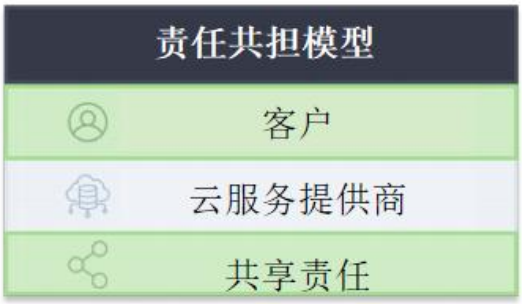
请参阅以下典型事件和案例：

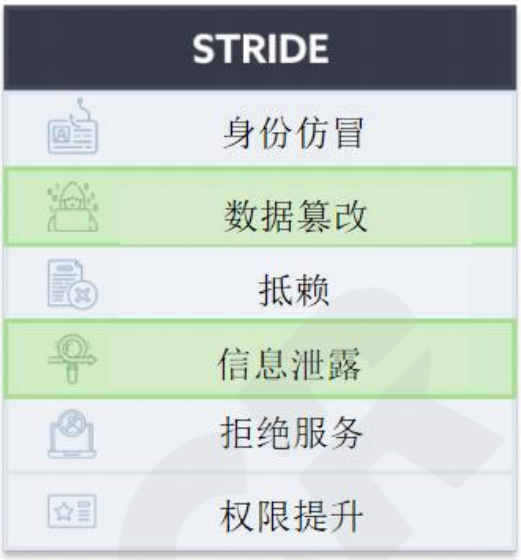
- Bonobos clothing store suffers a data breach
- Finding Secrets In Publicly Exposed Ebs Volumes
- Loot Public EBS Snapshots

适用于企业 TTP 的 MITRE ATT&CK

请参阅“数据备份”，MITRE ID： M1053.

责任共担模型和 STRIDE 威胁建模图





CSA CBK 安全指南 4.0 版

领域 5：信息治理

领域 7：基础设施安全

领域 11：数据安全和加密

领域 12：身份、授权和访问管理

CSA CCM CONTROLS 4.0.X 版

BCR- 08：备份

DSP - 数据安全和隐私生命周期管理

DSP- 01：安全和隐私政策和程序

DSP- 07：设计和默认的数据保护

DSP- 12：个人数据处理目的的限制

DSP- 13：个人数据子处理

DSP- 17：敏感数据保护

HRS- 12：个人和敏感数据意识和培训

IAM 身份和访问管理

IAM- 01：身份和访问管理政策和程序

IAM- 02：强密码政策和程序

IAM- 03：身份清单

IAM- 05：最低权限

IAM- 14：强身份验证

LOG - 日志记录和监控

LOG- 01：记录和监控政策和程序

UEM- 11：数据丢失防护

CSA Top 威胁映射

此攻击向量与以下内容相关：

安全问题 8：云数据意外泄露

安全问题 11：云存储数据泄露

8：受损镜像

定义

镜像是用于为工作负载提供初始安装文件的文件（或文件集合）。该攻击向量描述了攻击者为了漏洞利用而恶意修改的镜像，从而使用这些镜像访问云资源。通常是通过在镜像中创建后门或混淆恶意软件的方式实现。

描述

云用户应当了解与虚拟机/容器镜像相关的潜在风险，并采取预防措施来防范来自受损虚拟机/容器镜像的云攻击。泄露的镜像可用于发起基于云的攻击，如云恶意软件注入、挖矿加密货币、数据泄露或账户接管。

受损镜像的来源可能是来自内部的，即由云客户从不受信任的来源创建的镜像，随后被恶意威胁行为者访问；或者来自镜像存储、公共镜像存储库，甚至来自官方市场的外部恶意镜像，这些镜像由于缺乏管理而导致恶意内容得以传播。

要点

针对受损虚拟机/容器镜像的防范措施包括仅使用来自受信任来源的镜像、监控对镜像存储的访问并验证镜像完整性、针对更改或修改发出警报、确保虚拟机/容器镜像具有最新的安全补丁，并定期扫描虚拟机/容器镜像。此外，云管理员应实施有关开源软件和镜像的使用策略，设计访问控制策略并使用与云无关的云管理工具管理云部署。通过采取这些额外的预防措施，云管理员可以保护部署免受镜像受损等攻击向量的影响。此外，云安全管理员应考虑实施云原生容器安全解决方案，加强针对受损镜像和其他云攻击向量的防护。Kubernetes 网络安全策略、云原生安全解决方案、云应用防火墙可以进一步强化云安全。利用云安全工具，管理员可以通过检测与受损镜像相关的恶意活动快速响应云上任何风险或威胁。

典型事件和案例

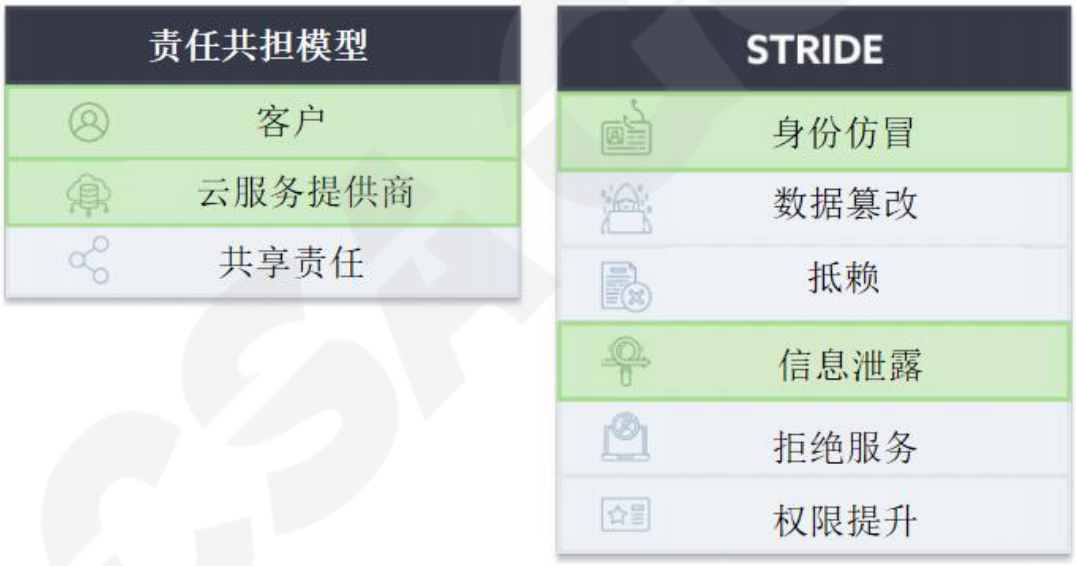
请参阅以下典型事件和案例：

- CodeCov Kills Off Bash Uploader Blamed for Supply Chain Hack
- Docker Hub repositories hide over 1,650 malicious containers
- An AWS Virtual Machine Is Infected With Mining Malware. There Could Be Others
- Analysis on Docker Hub malicious images: Attacks through public container images – Sysdig

适用于企业 TTP 的 MITRE ATT&CK

请参阅“在主机上构建镜像”， Mitre ID:T1612.

责任共担模型和 STRIDE 威胁建模图



CSA CBK 安全指南 4.0 版

领域 7 - 基础设施安全

领域 8 - 虚拟化和容器

CSA CCM CONTROLS 4.0.X 版

基础设施和虚拟化安全 IVS

ISV- 01：基础设施和虚拟化安全政策和程序

ISV- 04：根据各自的最佳实践，强化主机和来宾操作系统、虚拟机管理程序或基础设施控制平面，并得到技术控制的支持，作为安全基线的一部分

供应链管理、透明度和问责制 - STA

STA01：SSRM 政策和程序

STA07：制定并维护所有供应链关系的清单

CSA Top 威胁映射

此攻击向量与以下内容相关：

安全问题 4：缺乏云安全架构和策略

安全问题 6：第三方资源的安全

安全问题 9：Serverless 和容器工作负载的错误配置和利用

结语

总的来说，随着云计算的普及，网络威胁和攻击呈显著增加趋势。虽然风险、威胁和漏洞的数量和重要性有所提升，但使用的攻击向量相对稳定。本文旨在聚焦在这些攻击向量上。

在我们的研究过程中，发现的另一个有趣的观察结果是攻击技术的多样性。一些攻击向量是旧的、众所周知的、并且不特定于云环境（例如易受攻击的虚拟机）的。然而，我们也看到一些人员正在利用云提供的新功能（例如跨账户攻击）进行攻击。

在阅读本文档时，请注意相同的攻击向量可能会产生不同的风险或业务影响。举例来说，对于对象存储权限的破坏可能导致丧失文件可用性（如勒索软件加密）。此外，还可能带来机密性风险（如数据泄露）或完整性风险（如更改文件内容）。每种风险都需要采取不同的缓解措施，尽管这些风险与同一攻击向量直接相关。

总体而言，随着云计算的不断发展，组织必须将云安全置于首要考虑，并保持对潜在威胁和攻击的警惕。通过深入了解风险与所使用的攻击向量之间的关系，云安全专业人员可以更好地确定工作重点应落哪些方面。

延伸阅读

- NIST SP 800-161 - Supply Chain Risk Management Practices for Federal Information Systemsand Organizations

  https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final

- NSIT SP 800-218 - Secure Software Development Framework (SSDF) Version 1.1 Recommendations for Mitigating the Risk of Software Vulnerabilities
  https://csrc.nist.gov/publications/detail/sp/800-218/final

- Strengthening the Connection: VERIS and MITRE ATT&CK®

  https://medium.com/mitre-engenuity/strengthening-the-connection-veris-and-mitre-attck-c3aac3fa9cd

- CSA Cloud Controls Matrix
  https://cloudsecurityalliance.org/research/cloud-controls-matrix/

- Microsoft STRIDE threat modeling

  https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats

- Ramimac - AWS-customer-security-incidents at Github
  https://github.com/ramimac/aws-customer-security-incidents

- AWS Security Incident Response Guide
  https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/aws-security-incident-response-guide.html

- Microsoft cloud security benchmark documentation
  https://learn.microsoft.com/en-us/security/benchmark/azure/

- AWS Well-Architected Framework - Security Pillar
  https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html

- Microsoft Azure Well-Architected Framework - Security documentation
  https://learn.microsoft.com/en-us/azure/architecture/framework/security

- Google Cloud Architecture Framework: Security, privacy, and compliance
  https://cloud.google.com/architecture/framework/security

- CSA Security Guidance for Critical Areas of Focus in Cloud Computing
  https://cloudsecurityalliance.org/artifacts/security-guidance-v4/

- CSA Top Threats to Cloud Computing Pandemic Eleven
  https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-pandemic-eleven/

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