2017 可信云大会
可信云标准新一代
客户满意是未来
Cloud Computing Summit 2017.7.25-26

CSA云安全标准与最佳实践集

钱晓斌 CSA北京分会秘书长

目录

公有云安全风险，最大的安全问题包括

1. 通过员工凭证滥用进行未经授权的访问(63%)
2. 不正确的访问控制以及账号劫持(61%)
3. 恶意的内部人士(43%)

云计算安全趋势分析

无服务器框架的出现

云计算中最具挑战性的创新可能是无服务器架构的兴起。它们包括像亚马逊Web服务（AWS）和PaaS代码（基于代码的平台即一种服务），IT部门将不再需要管理操作系统或虚拟机。

这是云安全战略的一个很大的变化，因为这**意味着API正成为一个额外的攻击区域的漏洞**。这也正是IT团队通常不习惯配置和抵御这些类型的威胁的区域。

基于主机和网络的安全措施移动到控制平台

区别与传统数据中心环境，云安全的另一个特点是，安全功能从主机与网络端移动到控制平台上。

这种变化有利有弊，集中管控给带来额外的安全风险，但同样给云安全带来独特优势，可以集成多种安全能力，可以实时通过API升级网络上主机和服务器的安全能力，并作出快速响应。

云计算安全趋势分析

更多老牌厂商交付云安全解决方案

云基础设施变得更加重要，各种规模的组织的云计算安全解决方案都将迅速发展。这一演变将会影响各种规模的云安全供应商，包括一些在IT安全行业的大厂商。例如，多个供应商的市场解决方案为Windows以及在AWS上运行的Linux工作负载。其他的厂商会看到谁需要他们支持混合部署模式，包括传统的数据中心和AWS的客户面临着更多的压力。

无论是通过收购规模较小的IT供应商还是通过开发创新的新产品，大规模的安全厂商将会提供更多的基于云计算的安全解决方案。

安全成为本地持续集成和持续部署的工具集

在云的基础设施，特别是随着越来越多的组织切换到DevOps式快速应用开发和部署在云计算，**安全不再被认为是开发和部署一个独立的实体**。云安全将成为更广泛的集成和本地的整体过程的连续集成和连续部署（CI/CD），例如詹金斯工具被用来验证代码和验证安全性作为标准的质量保证步骤。

更多的供应商提供安全检测和监控启用的DevOps工具，如采用SAST对应用程序源代码做静态分析，从内向外寻找安全漏洞；用DAST检测应用程序运行时安全漏洞。IT安全性在DevOps环境下变得更快、更敏捷。

云计算安全趋势分析

云安全的发展速度将超出我们的预期

对于云基础设施的攻击将变得更加复杂和自动化，这一趋势将持续增强，因为更多的组织在云基础设施中存储了越来越多有价值的数据。根据Gartner的研究，“到2020年，云计算遭受攻击事伯中，80%是由于客户配置错误，凭据管理不善或内部盗窃，而不是云服务提供商提供的产品的安全漏洞。”

IT组织需要提高他们的安全准备工作能力、实时警报和反应能力，同时也要考虑他们的内部操作、内部配置和员工的安全培训和认证的问题。

需要密切关注网络空间总体安全趋势

比较显著的几个特点是：

从威胁表现来看，主要是网络攻击的全球化与网络犯罪的运营化；

从产品形态来看，主要是安全产品的软件化服务化；

从核心能力来看，主要是安全分析的知识化与智能化。

目录

- 云安全现状与趋势
- CSA 国际云安全联盟介绍
- CSTR云安全技术标准介绍

关于国际云安全联盟

➢CSA（Cloud Security Alliance）

2008年12月在美国发起，是中立的非盈利世界性行业组织，致力于国际云计算安全的全面发展，2011年美国白宫在CSA峰会上宣布了美国联邦政府云计算战略。全球300多个单位会员，7万多个个人会员。全球500强中的科技类企业都是会员单位，包括：**亚马逊、微软、Google、FaceBook、IBM、Intel、Oracle、Vmware、HP、EMC、华为、阿里、腾讯、中兴通讯、Ucloud**等主要的云服务提供商、云计算解决方案提供商

➢ CSA的宗旨

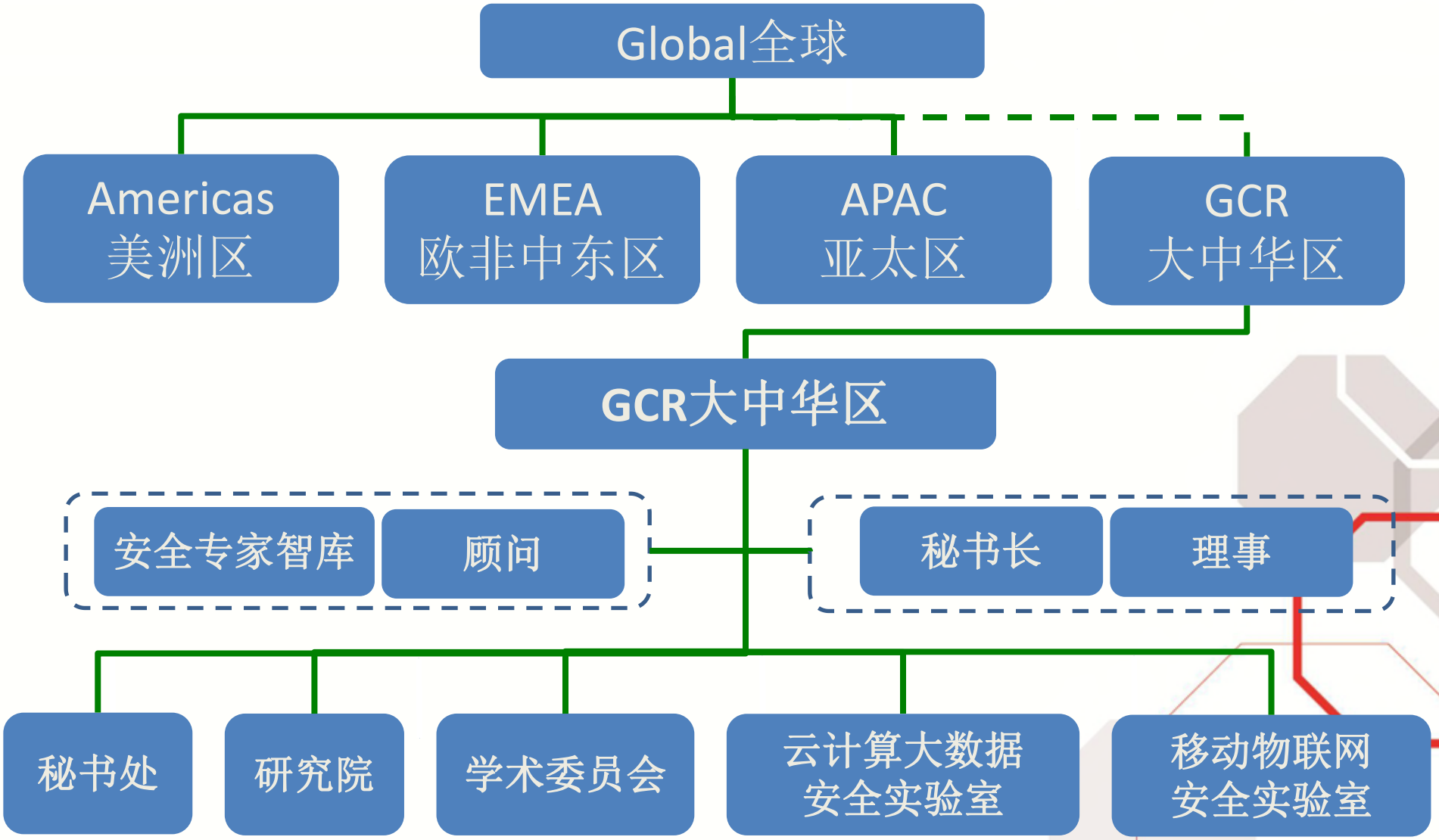
提供用户和供应商必要的云计算安全需求和保证证书，并达到同样的认识水平

促进对云计算安全最佳实践的独立研究

推广正确使用云计算和云安全解决方案的宣传和教育计划

创建有关云安全保证的问题和方针的明细表

CSA组织结构


Global全球
Americas
美洲区
EMEA
欧非中东区
APAC
亚太区
GCR
大中华区
GCR大中华区
安全专家智库
顾问
秘书长
理事
秘书处
研究院
学术委员会
云计算大数据
安全实验室
移动物联网
安全实验室

CSA持续从事新兴领域前瞻性安全研究

- CSA 研究院全球有**1000多**个安全专家，分布在美国、欧洲、中国主要的科技公司和研究机构，对新兴领域的安全进行前瞻性的研究，除了云计算，范围还涉及：**大数据、物联网、SDN/NFV、量子通讯等**
- CSA大中华区有**100多**个专家参与全球的安全研究，并在研究成果产业化方面作出独特的贡献。

CSA已经筹建的工作组有30多个如：

① 结构及框架工作组
② 安全即服务工作组
③ 一致性评估工作组
④ 法律及电子发现工作组
⑤ 虚拟化及技术分类工作组
⑥ 数据中心运行及事故响应工作组
⑦ 信息生命周期管理及存储工作组
⑧ 可移植性、互操作性及应用安全工作组
⑨ 身份与接入管理、加密与密钥管理工作组
⑩ GRC，Audit，Physical BCM，DR工作组

CSA 大中华区是世界标准的“连接器”！

CSA优秀实践概述

- 云安全指南
- 云安全威胁研究
- 可信云计算架构
- 云安全标准框架
- 量子安全框架
- 大数据安全威胁
- 物联网安全框架
- STAR 云安全评估认证
- CCSK 云安全培训认证
- 云审计协议
- 云管控、风险、合规工具
- 十大安全云设计实施指导
- SDP软件定义边界高度安全网络

Future: Mobile Application Security Test, Virtualization, Cloud Vulnerability, Cloud Security Eco-System , SDN/NFV , ...

The CSA Open Certification Framework is an industry initiative to allow global, accredited, trusted certification of cloud providers.

C-CCSK
China-Certificate of
Cloud Security Knowledge

CSA优秀实践1：云安全指南V4.0

- CSA “Security Guidance for Critical Areas of Focus in Cloud Computing云计算关键领域安全指南”从2009年推出开始，到2017年已持续更新到V4.0版本
- 是**云安全领域奠基性的理论基础**，得到全球普遍认可，具有广泛的影响力，被翻译成6国语言，成为业界云安全研究、各个国家和地区建立云安全标准和云安全战略最权威的理论和实践基础

CSA优秀实践2：云安全控制矩阵

CCM Cloud Controls Matrix

Microsoft Excel - CSA_Controls Matrix (CM)_v2.0.xlsx [Read-Only]

A1 Control Area

	A	B	C	D	E	F	G	H	
1	Control Area	Control ID	Control Specification	Cloud Service Delivery Model Applicability			Scope Applicability		
2				SaaS	PaaS	IaaS	Service Provider	Customer	
59	Information Security - Portable / Mobile Devices	IS-32	Policies and procedures shall be established and measures implemented to strictly limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).	X	X	X	X	X	C C
60	Information Security - Source Code Access Restriction	IS-33	User access to program source code shall be restricted to authorized personnel.	X	X	X	X		
61	Information Security - Utility Programs Access	IS-34	The use of utility programs that might be capable of overriding system and application controls shall be restricted.	X	X	X	X	X	C
62	Legal - Non-Disclosure Agreements	LG-01	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of data shall be identified and reviewed at planned intervals.	X	X	X	X	X	
	Legal - Third Party Agreements	LG-02	Agreements with third parties involving accessing, processing, communicating or managing the organization's information assets, or adding products or services to information assets shall cover all relevant security requirements. Agreements provisions shall include security (e.g., encryption, access controls, and leakage prevention) and integrity controls for data exchanged to prevent improper disclosure, alteration or destruction.	X	X	X	X		C

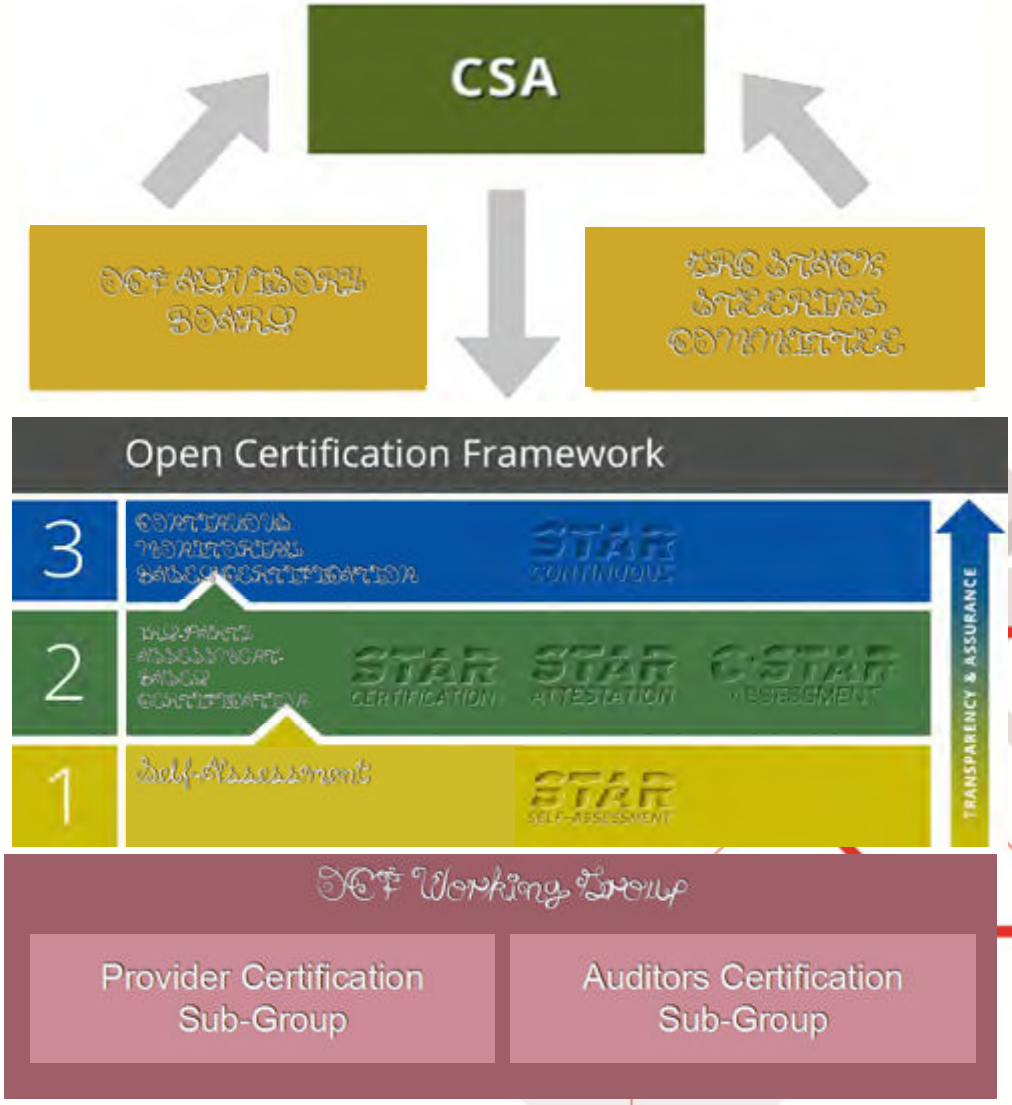
CSA Controls Matrix (CM) v2.0 / Compliance Mapping Reference /

Ready NUM

- 在CSA云安全指南基础上推出“云安全控制矩阵CCM”，成为**云计算安全行业国际公认标准**
- CCM结合云计算业务特点，匹配了国际主要的信息安全标准和行业标准：ISO 27001, COBIT, PCI, HIPAA, FISMA, FedRAMP, Countries
- CCM核心内容**被ISO 27017**（信息安全治理架构）与**ISO 27036**（供应商关系的信息安全）**采纳**

CSA优秀实践3：OCF和STAR认证体系

- 基于CCM，CSA建立了“开放认证框架”OCF（ Open Certification Framework ）和STAR认证体系（ Security, Trust and Assurance Registry ）
- CSA与英国标准协会BSI强强联合，在全球开展CSA STAR认证；CSA在中国，结合等保，推出针对中国市场的CSA C-STAR认证。
- CSA STAR认证是**全球最权威的云安全管理体系认证**，主流的云服务商都遵守CCM，并通过了STAR和C-STAR认证：亚马逊、微软、HP、阿里、华为等



CSA优秀实践4：云安全标准 CSTR

CSA security alliance℠

CSA云安全联盟标准

➢CSA CSTR（Cloud Computing Security Technology Requirements）是**全球第一个**针对云计算产品与解决方案的技术标准，系统呈现了全球主要云服务商和云计算解决方案提供的优秀实践

➢CSTR由CSA**大中华区主导**，全球主流云计算厂家和研究机构共同制定，发源于中国，贡献到全球的**原创性标准**：亚马逊、微软、Intel、Oracle、华为、阿里、腾讯、百度、中国移动、中国电信、中兴、金蝶、京东云、Ucloud、浪潮、中科院、公安三所、武汉大学、深圳标准技术研究院等。

➢CSTR标准2016年10月25日CSA大中华区峰会上发布，基于CSTR标准（草案），CSA 全球将推出CSA STAR Tech国际认证。

CSA优秀实践5：

STAR Tech云计算产品安全认证体系

STAR Tech
Security, Trust and Assurance Registry Tech

- 基于CSTR,CSA在“开放认证框架”OCF（ Open Certification Framework ）基础上，开展STAR Tech认证体系
- CSA在中国联合赛宝实验室开展CSA STAR Tech认证。
- CSA STAR Tech认证是**全球最权威的云计算产品安全认证。**

CSA优秀实践6：

国际注册云计算安全专家认证体系

初级	**C-CCSK (Foundation)** China - Certification of Cloud Security Knowledge 云计算安全基础知识认证
中级	**C-CCSK** China - Certification of Cloud Security Knowledge 云计算安全知识认证
高级	**CCSMP** Certified Cloud Security Management Professional 国际注册云安全管理认证专家
高级	**CCSSP** Certified Cloud Security Systems Professional 国际注册云安全系统认证专家。

CSA物联网安全技术标准启动

2017.2.24　深圳 科技园 CSA物联网安全标准工作启动

CSA大数据安全技术标准启动

2017.4.22　北京 360 CSA 大数据安全标准工作启动

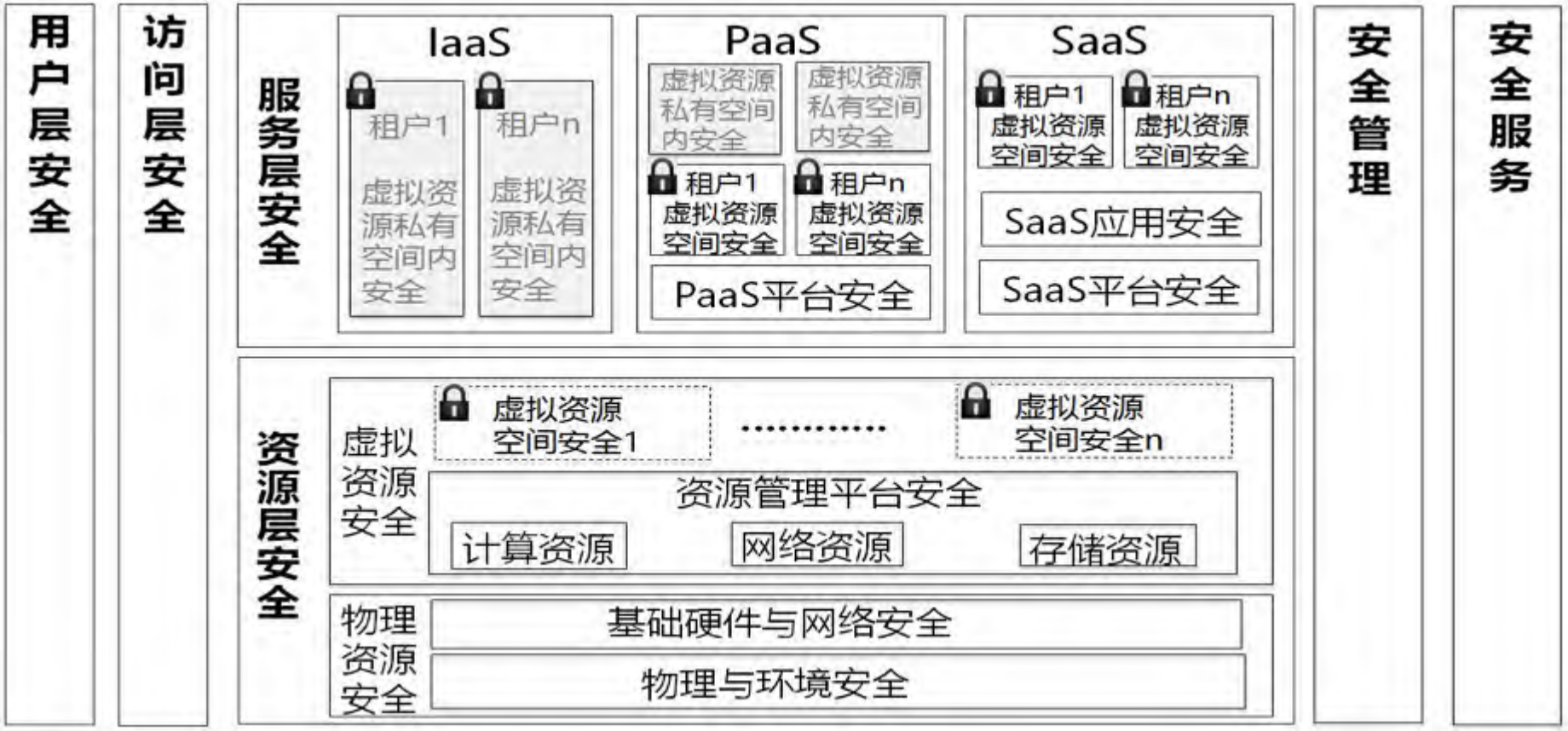
目录

- 云安全现状与趋势
- CSA 国际云安全联盟介绍
- CSTR云安全技术标准介绍

CSA CSTR标准工作背景

- CSA推出的STAR认证采用中立性认证技术对云服务供应商安全性开展缜密的第三方独立评估，并充分运用ISO/IEC 27001:2013管理体系标准以及CSA CCM云控制矩阵，帮助企业满足客户的安全需求。
- 实践中发现，《云安全指南》和STAR、C-STAR认证，对云计算服务的管理体系，运维运营，总体技术是业界的最佳实践和认证标准，但是云计算平台底层产品和SaaS上层应用的安全技术要求细节还需要更加系统和完整的定义，使云计算解决方案提供商能够在云计算产品开发过程中直接参考，第三方测评认证机构也能够对云计算产品级安全能力有认证的标准。
- 云服务客户和云计算解决方案提供商呼吁CSA推出云计算产品安全技术要求，为STAR系列认证锦上添花，作为产品开发、认证的标准。

CSA CSTR标准框架



CSA CSTR标准框架举例：IaaS安全要求

访问层安全

- 网络访问安全
- API访问安全
- WEB访问安全

资源层安全

- 物理资源安全
  - 基础硬件与网络安全
    - 设备硬件结构安全
    - 设备硬件软件安全
    - 网络架构安全
    - 网络边界安全
    - 网络授权及审计
- 虚拟资源安全
  - 资源管理平台安全
    - 云计算资源管理软件安全
    - 云存储资源管理软件安全
  - 虚拟资源空间安全
    - 虚拟化计算安全
    - 虚拟化网络安全
    - 虚拟化存储安全
    - 迁移安全
    - 虚拟化组件安全加固
    - 剩余数据保护

服务层安全

安全管理

- 身份鉴别和访问管理
- 安全审计
- 存储与备份管理
- 安全运维
- 威胁与脆弱性管理
- 密钥与证书管理

安全服务

- 网络安全服务
- 主机安全服务
- 应用安全服务
- 数据安全服务
- 审计与合规安全服务
- 安全情报服务

共218条要求，其中基础要求149条，增强要求69条

CSA CSTR标准框架举例：SaaS安全要求

访问层安全	资源层安全	服务层安全	安全管理	安全服务
• 网络访问安全 • API访问安全 • WEB访问安全		• 网络安全 • 主机安全 • SaaS资源管理平台和应用安全 • 租户虚拟资源空间安全	• 身份鉴别和访问管理 • 安全审计 • 存储与备份管理 • 安全运维 • 威胁与脆弱性管理 • 密钥与证书管理	

共136条要求，其中基础要求102条，增强要求34条

标准条款（样例）

- 6.2 虚拟资源安全
- 6.2.1 资源管理平台安全

6.2.1.1 计算资源管理平台安全

6.2.1.1.1 基础要求

计算资源管理平台应符合的基础要求如下：

a) 应支持对代码进行安全测试并进行缺陷修复的能力；

b) 应支持限制虚拟机对物理资源的直接访问，支持对物理资源层的调度和管理均受虚拟机监视器控制的能力；

c) 应支持对计算资源管理平台的攻击行为进行监测和告警的能力，检测到攻击行为时，应能够记录攻击的源IP、攻击的类型、攻击的目的、攻击的时间；

d) 应支持最小安装的原则，仅安装必要的组件和应用程序的能力；

e) 应支持禁用无需使用的硬件能力；

f) 应支持虚拟机和虚拟化平台间内部通信通道的受限使用能力；

g) 应支持组件间通信采用安全传输的能力；

h) 应支持管理命令采用安全传输的能力；

i) 应支持内核补丁更新、加固及防止内核提权的能力；

j) 应支持对恶意代码进行检测和处置的能力；

k) 应支持监视计算资源管理平台远程管理连接，中断未授权管理连接的能力；

l) 应支持对远程执行计算资源管理平台特权管理命令进行限制的能力；

m) 应支持资源监控的能力，资源监控的内容包括 CPU 利用率、带宽使用情况、内存利用率、存

标准解读（样例）

【标准条款】

(6.2 虚拟资源安全

-- 6.2.2 虚拟资源空间安全

--6.2.2.2 虚拟化网络安全

云计算平台应符合的基础要求如下：J) **应支持防止虚拟机使用虚假的IP或MAC地址对外发起攻击的能力**；

【安全威胁场景】

在云计算虚拟化网络中，虚拟机使用虚假的IP或MAC地址对外发起的攻击，存在两种场景，一个是对同一物理服务器上其他虚拟机的攻击，如ARP欺骗；另一个是对物理服务器外部的网络发起攻击，如DoS攻击。这种攻击，可能是恶意用户有意为之，也可能是虚拟机受到攻击，中了木马等，成为僵尸网络的一部分，被动发起的攻击。

对公有云、社区云、混合云、私有云都适用。

【条款解读】

虚拟机IP和MAC地址都是云计算系统分配的，系统应提供限制在虚拟机上修改IP或MAC地址的能力。

【参考方案】

在虚拟交换机上，收到虚拟机发出的报文，判断与系统分配的IP和MAC地址是否一致，不一致，则丢弃，并根据告警规则告警或自动隔离虚拟机等。

【测试方案】

在测试虚拟机上修改IP或MAC地址，

1.) 检查是否能对同一物理机上的同一VLAN的虚拟机发送IP报文；

2.) 检查是否能对不同物理机上的其他虚拟机发送IP报文;

3.) 检查云计算平台，是否检测到这类报文并记录日志或告警。

CSA = 公益 + 共享

钱晓斌 13801355522