2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY CONFERENCE

云安全与物联网安全实践

主讲人：李雨航Yale Li，Fellow教授
云安全联盟CSA大中华区主席
中国科学院云安全首席科学家

CONTENTS
目 录

云安全联盟CSA

Our Community

100,000+
个人会员

80+
地方分会

500+
企业会员

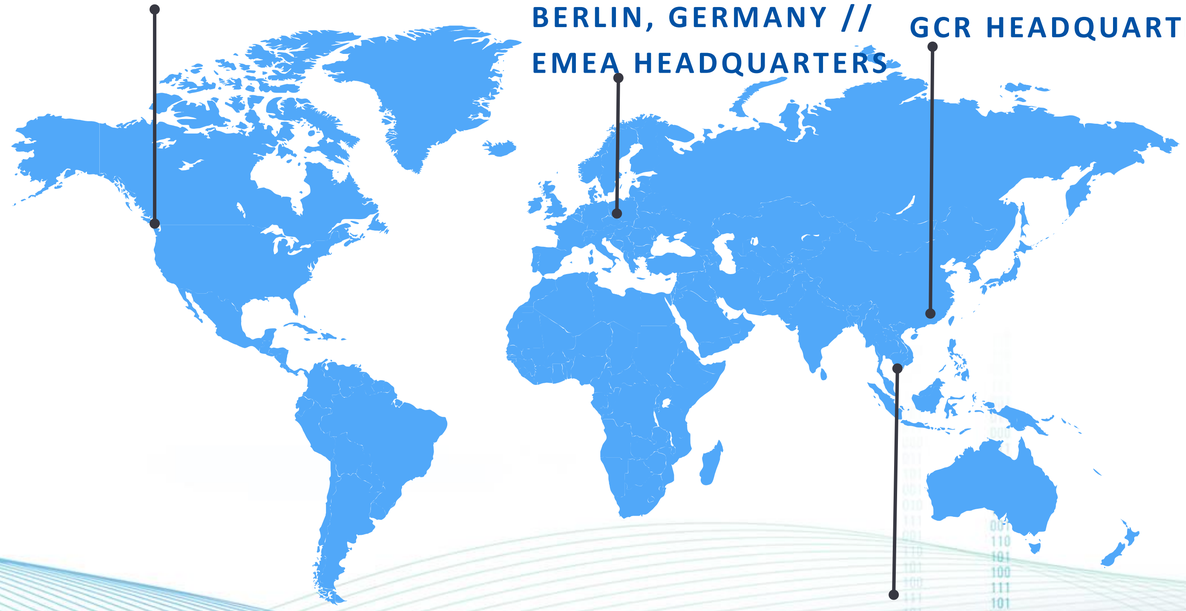
50+
研究工作组

与政府、研究机构、专业协会
和行业建立战略伙伴关系

CSA research is FREE!

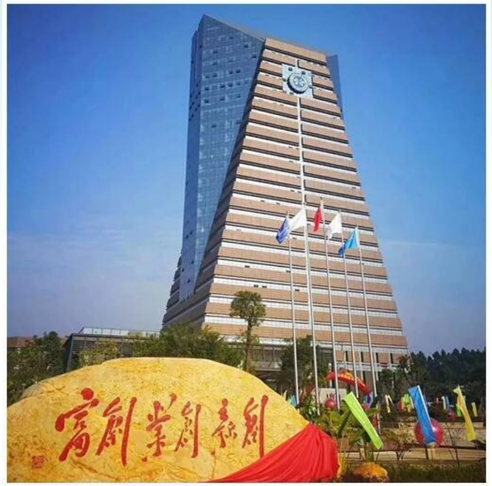
2009
CSA FOUNDED

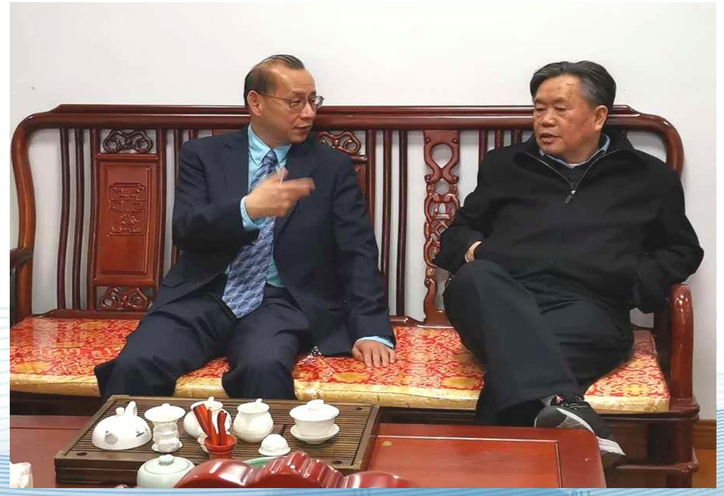
CSA®



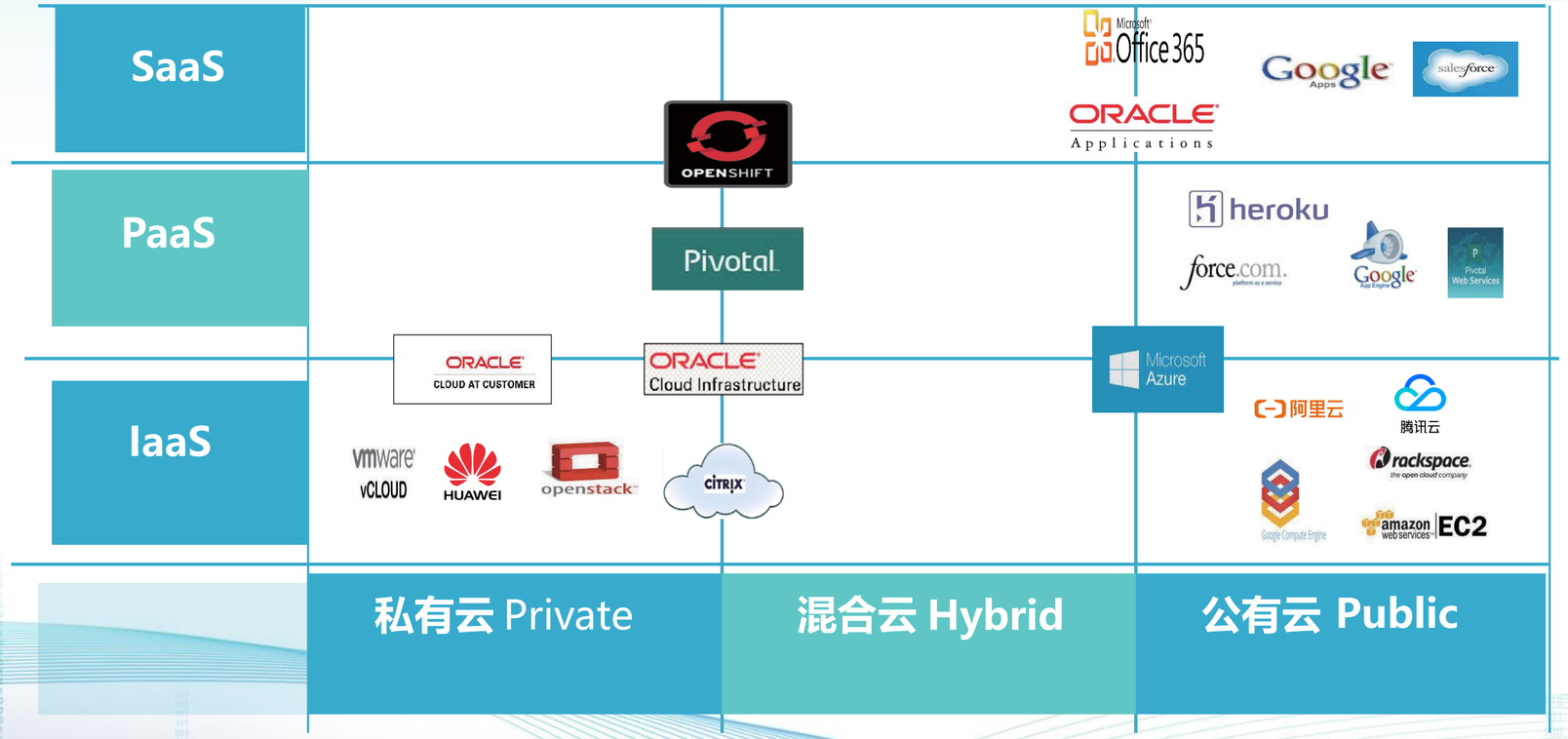
中科院云计算中心

中科院云计算中心是中国科学院直属的唯一一个以云计算、大数据为核心研发领域的大型研发机构，是中国科学院首次与地方政府共建的云计算专业研发机构，拥有国内首个完全自主产权的G-cloud云计算平台，技术处于国内领先地位。

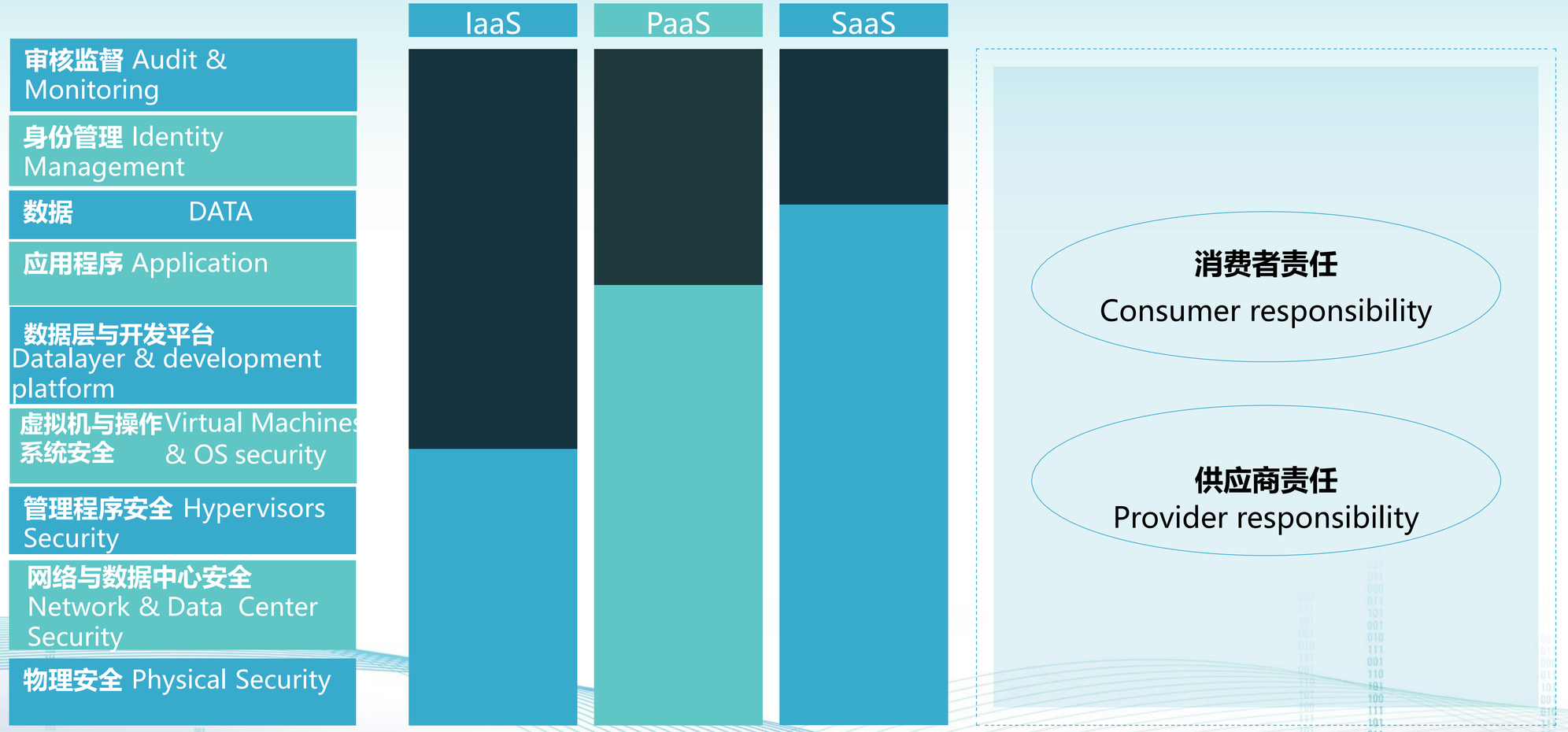




不同的云服务有着本质上的区别



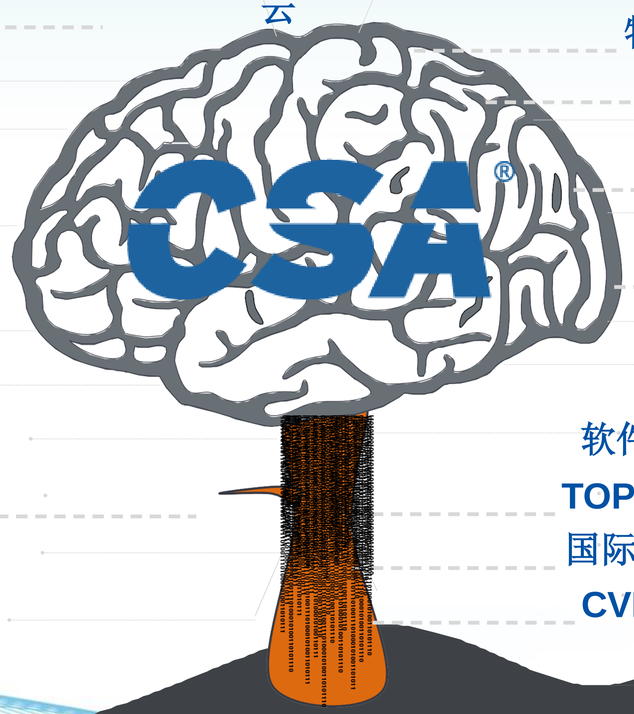
责任共担模型


审核监督 Audit & Monitoring
身份管理 Identity Management
数据 DATA
应用程序 Application
数据层与开发平台 Datalayer & development platform
虚拟机与操作系统安全 Virtual Machines & OS security
管理程序安全 Hypervisors Security
网络与数据中心安全 Network & Data Center Security
物理安全 Physical Security
IaaS
PaaS
SaaS
消费者责任
Consumer responsibility
供应商责任
Provider responsibility

CSA安全研究项目

人工智能
区块链与分布式
网络事件分享
云组件规范
云控制矩阵
云安全服务管理
一致性评价
容器与微服务
DevSecOps
组织架构
ERP 安全
金融服务
医疗保健

云

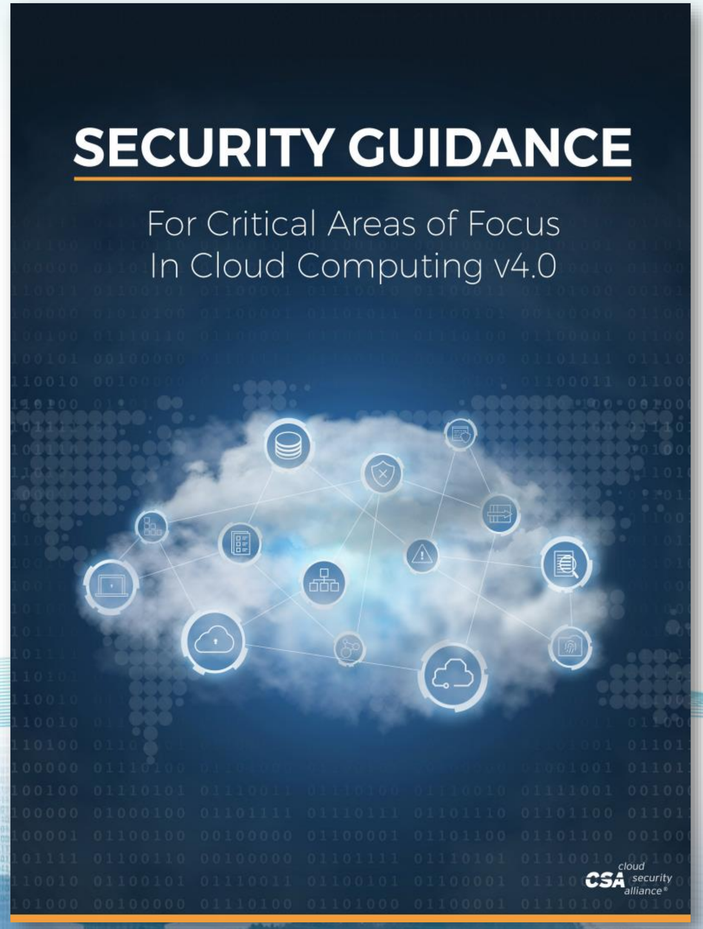


ICS安全
物联网
密钥管理
手机应用安全云测
开放认证框架
开放API
隐私水平协议
量子安全
安全即服务
软件定义边界
TOP威胁
国际标准
CVE

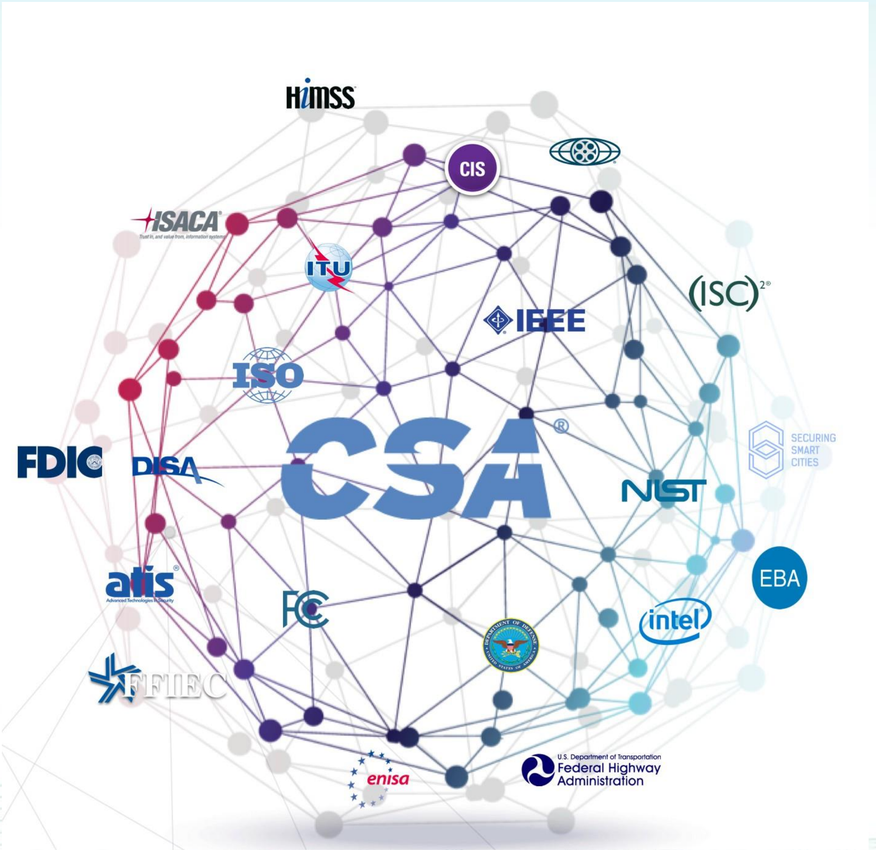
教育
思想先驱
工具和标准
合作
Best Practices
最优实践与
解决方案

云计算安全指南

报告下载地址： https://www.c-csa.cn



- 启动CSA的基础云安全研究
- 2017年7月发布第四版本
- 重要的企业经验教训
- 领域 1: 云定义 & 架构
- 领域 2-5: 云端治理
  - 企业风险管理和治理
  - 合法
  - 合规 & 审计管理
  - 信息治理
- 领域 6-14: 云端运营
  - 管理层面和业务连续性
  - 基础设施安全
  - 虚拟化和存储
  - 事件响应
  - 应用安全
  - 数据安全和加密
  - 身份管理
  - 安全服务
  - 相关技术



CCM 云控制矩阵

HRS	Human Resources Security
IAM	Identity & Access Management
IVS	Infrastructure & Virtualization
IPY	Interoperability & Portability
MOS	Mobile Security
SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
STA	Supply Chain Mgmt, Transparency & Accountability
TVM	Threat & Vulnerability Management
AIS	Application & Interface Security
AAC	Audit Assurance & Compliance
BCR	Business Continuity Mgmt & Op Resilience
CCC	Change Control & Configuration Management
DSI	Data Security & Information Lifecycle Mgmt
DSC	Datacenter Security
EKM	Encryption & Key Management
GRM	Governance & Risk Management

133 CONTROLS
Cloud Controls Matrix v3.0.1

- 为云供应链风险管理设计最基本的控制框架
- 划定控制所有权（供应商，客户）
- 为云供应商类型的排名提供实用性参考
- 能够作为安全态势和遵从态势测量的典范
- 包括16个控制域，133个控制项
- 包含了全球法规和安全标准与控制项的映射关系：例如：NIST, ISO 27001, COBIT, PCI, HIPAA, FISMA, FedRAMP – mappings growing virally
- 被政府和企业广泛应用

云安全顶级威胁-CSA Cloud Security Top Threats

1.数据泄露
2.被盗用的证书以及身份管理系统
3.不安全的程序接口
4.系统和App漏洞
5.账号劫持
6.内部恶意人员

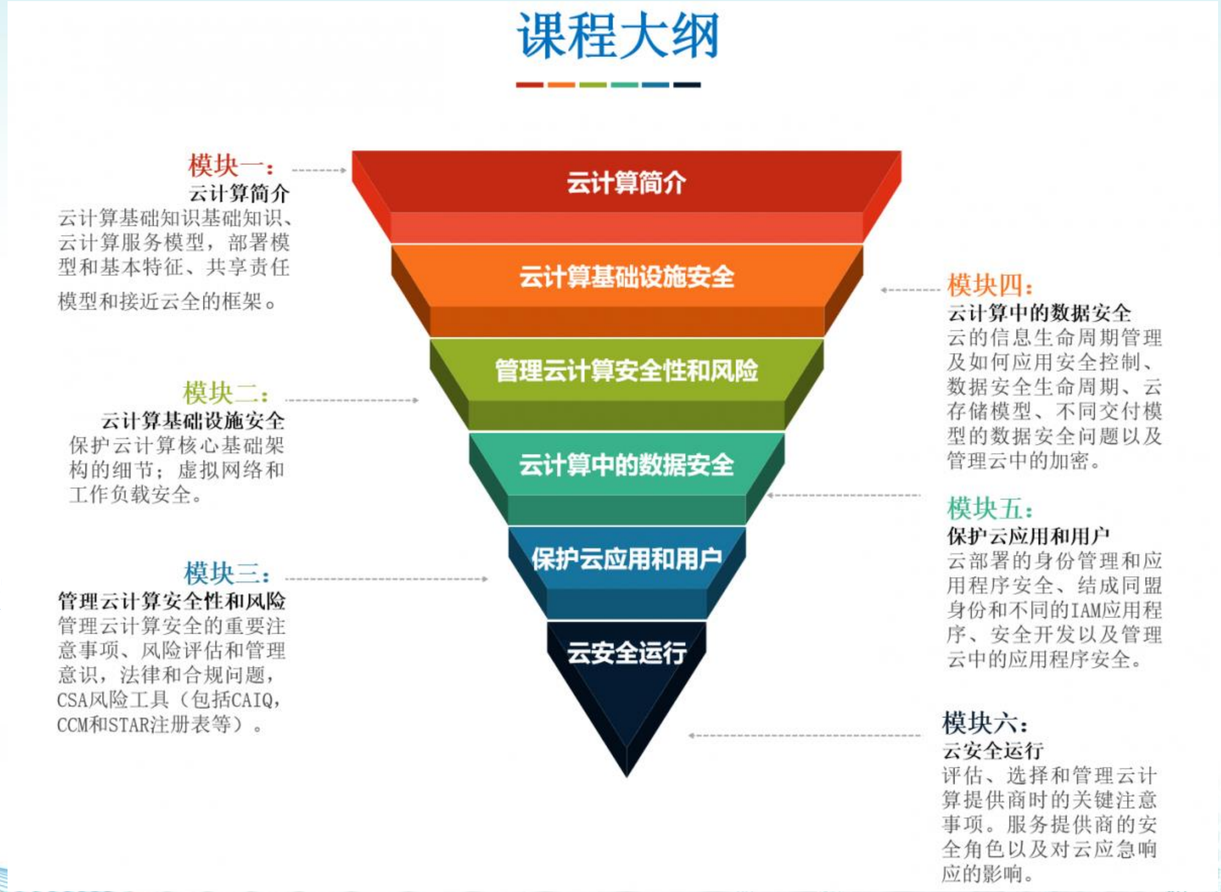
7.高级持续性威胁
8.数据丢失
9.不充分的尽职调查
10.恶意使用和滥用
11.拒绝攻击服务DoS
12.共享技术中的漏洞

报告下载地址：https://www.c-csa.cn

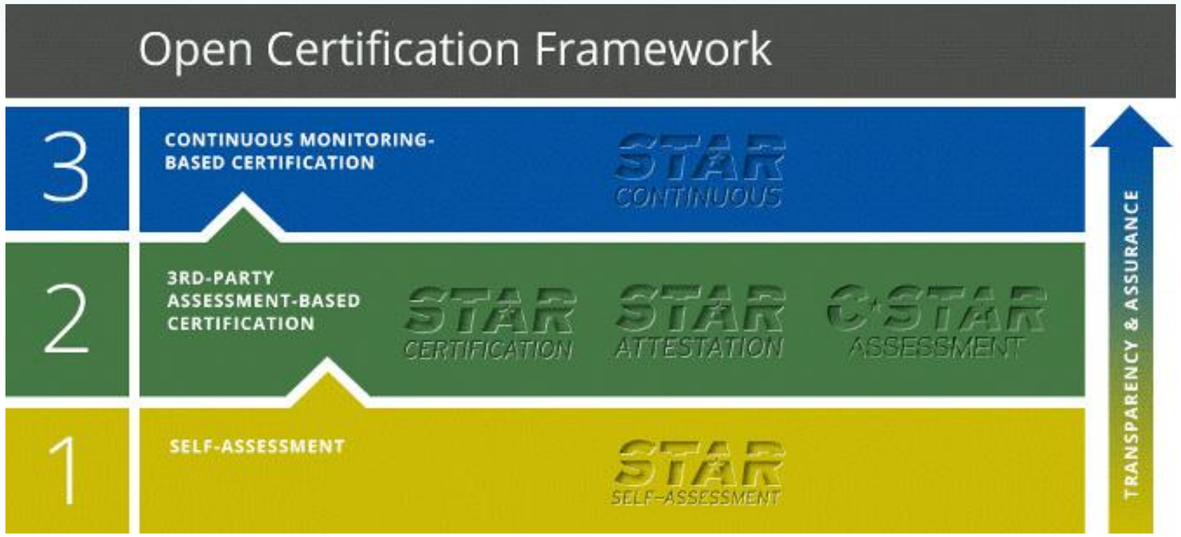
个人云安全认证 CCSK

- 最有价值的IT认证 2016 – Certification Magazine
- 云安全竞争力的衡量标准
- 基于CSA的指南和云控制矩阵
- 在线考试
- 不断涌现关于云安全，风险管理和审计的需求

CCSK™
Certificate of
Cloud Security Knowledge



CSA OCF（开放认证框架）



第一级----自我评估

云厂商在CSA官网注册并提交自评估报告。

第二级----第三方认证

由第三方机构进行认证，确保云厂商满足CSA云安全控制矩阵CCM要求。例如: CSA STAR和C-STAR认证

第三级----持续监控

云厂商公布基于CSA云计算信任协议（The Cloud Trust Protocol，CTP）的安全监控结果，对云服务相关安全要求进行持续的审计和评估。

云厂商安全认证 CSA C-STAR

针对云厂商安全管理的一种严格的第三方独立评估。

该评估主要参考GB/T 22080-2008管理体系标准及CSA云控制矩阵（Cloud Control Matrix）的要求，以及29个国标GB/T 22239-2008（信息安全技术—信息系统安全等级保护基本要求）和GB/Z 28828-2012（信息安全技术—公共及商用服务信息系统个人信息保护指南）的相关控制措施

云安全的最大收益

- 安全和规模效益
  - 规模越大，实施安全控制的成本越低
- 安全导致市场差异化
  - 安全性成为云消费者的首要考虑事项
- 快速智能的资源伸缩
  - 资源伸缩使安全防御措施也具备弹性
- 审计和取证
  - 虚拟镜像取证减少停机时间
  - 更具成本效益的云日志存储
- 资源集中的优势
  - 每单位资源更便宜的物理边界限制和物理访问控制
- 更及时的发布更新与有效的默认安全配置
  - 通过默认加固的镜像模板管理安全基线
  - 比传统修补模式更及时的发布更新
- 标准化的安全管理接口
  - 大型云提供者的安全管理能力可以通过标准接口对外开放
- 审计和SLA促进更好的风险管理
  - 需要量化SLA中各种风险场景的处罚以及安全漏洞对声誉的可能影响，激发更为严格的内部审计和风险评估程序

企业上云安全实践----上云是常态、不上是例外

需求调研

什么系统要上云，涉及哪些数据、密级如何、是结构化数据还是非结构化数据、数据量有多大，系统对环境及硬件资源的要求是什么（CPU、内存、网络、I/O的要求都是什么样的，分别需要多少资源），业务系统的SLA要求都是什么……

厂商选型

厂商规模与技术实力、公开的故障与历史可用性、厂商整体经营风险、厂商的安全合规状况、标杆客户、业界口碑、互换性与可移植性（厂商琐定的风险）、是否可以协商合同（包括SLA、保密协议等）……

CSA软件定义边界SDP(1)

传统企业安全：基于防火墙的边界防御

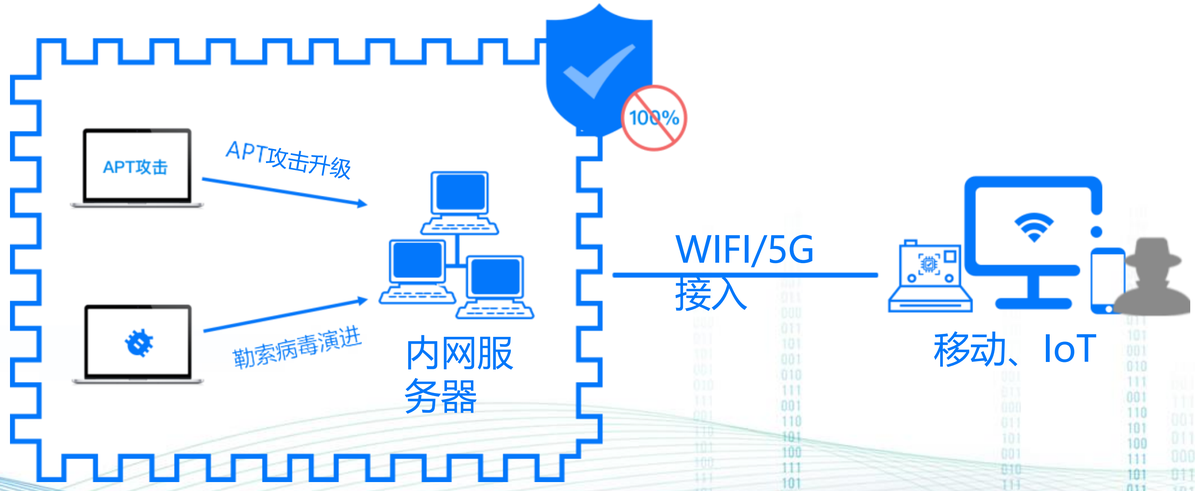
- Firewall防火墙
- IDS 入侵检测
- IPS 入侵防护
- …

行业趋势 — 变革

CSA软件定义边界SDP(2)

变革1：云/移动/IoT等新技术出现让企业数据不再局限在墙内，传统安全边界在瓦解

变革2：APT攻击、勒索病毒等黑客技术的演进以及WIFI/5G等无线方式接入，让企业内网不再100%安全



CSA软件定义边界SDP(3)

企业安全无法再100%依赖防火墙，国际云安全联盟CSA定义了万物互联代的网络安全模型

Software-Defined-Perimeter(SDP) 软件定义边界

SDP有效防止十大安全威胁*

1. 数据泄露
2. 弱身份、密码与访问管理
3. 不安全的界面 和API 接口
4. 系统和应用程序漏洞
5. 账号劫持
6. 内部恶意人员威胁
7. 高级持续威胁攻击（APTS）
8. 数据丢失
9. DDoS拒绝服务
10. 共享技术问题

* 来自云安全联盟CSA白皮书《SDP for IaaS》

- Gartner

  SDP入选《 2017年11大信息安全技术》，《 2018最应投入的10大安全项目》，《网络服务隔离指南》：“到2021年底，60%的企业将用SDP取代VPN”

- zscaler

  2018年纳斯达克上市的硅谷独角兽，专攻SDP产品，市值已超过60亿美金

- CISCO Symantec. Akamai verizon CITRIX

  国外众多老牌安全产商、CDN产商、电信运营商都推出自己的SDP产品

- RSAConference

  连续4年举办SDP黑客破解大赛，无人攻破

SDP — CSA技术创新

CSA软件定义边界SDP(4)

安全思路的转变

传统安全：攻防

挑战：你永远不知道敌人明天是否有更高级的武器

SDP安全：隐身

优势：敌人无法攻击看不见的目标

CSA软件定义边界SDP(5)

基于零信任(Zero-Trust)安全理念的软件定义边界(SDP)的安全模型

SDP核心优势

网络隐身 Information Hiding
隐藏服务器地址、端口，使之不被扫描发现

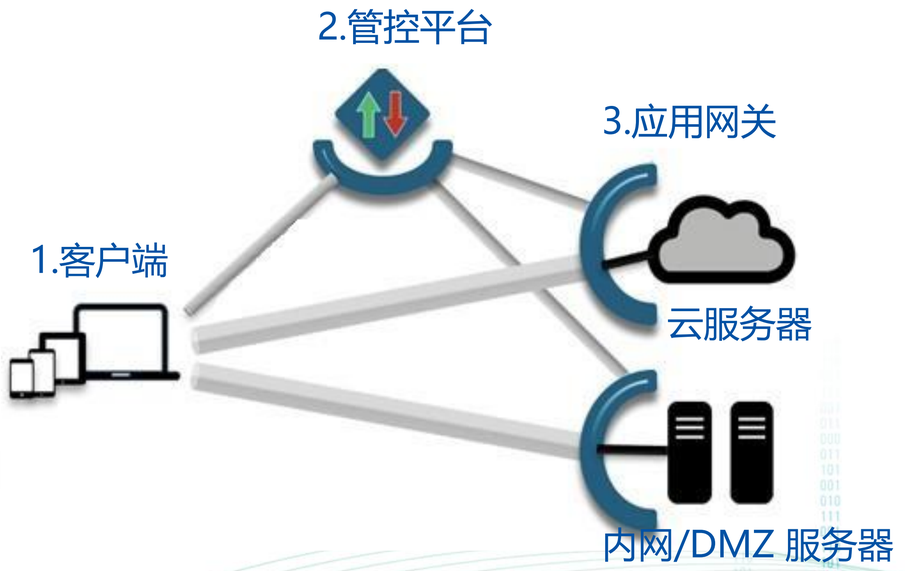
预验证 Pre-authentication
在连接服务器之前，先验证用户和设备的合法性

预授权 Pre-authorization
用户只能看到被授权访问的应用（最小权限原则）

应用级的访问准入 Application Layer Access
用户只有应用层的访问权限，无网络级的访问

扩展性 Extensibility
基于标准协议，可以方便与其它安全系统集成

SDP安全模型架构图



SDP使用场景

SDP for IoT
SDP for IaaS
SDP for HTTP
SDP for Enterprise
...

CSA软件定义边界SDP(6)

Google BeyondCorp：基于SDP的安全办公平台

https://cloud.google.com/beyondcorp/

BeyondCorp 一开始是 Google 内部的一项举措，旨在让每个员工都能在 不借助 VPN 的情况下通过零信任的网络工作，如今它已融入大部分 Google 员工的日常工作。 BeyondCorp通过将访问权限控制措施从网络 边界转移至具体的设备，让员工可以更安全地在任何地点工作，而不必借 助于传统的 VPN。

2009年Google内网遭受了代号为“极光行动” 的APT攻击，推动Google 重新搭建整体安全架构，从而诞生了BeyondCorp项目。自2012年 Google开始在内部实施BeyondCorp，共发表了6篇相关的论文。

美国国防部与中情局的实践

美国国防部在《Department of Defense Global Information Grid Architectural Vision》信息化架构指南中提出，所有敏感信息 的访问必须严格遵守“need to know”（最小权限原则）的信息安 全原则。而SDP可以有效实施该原则。

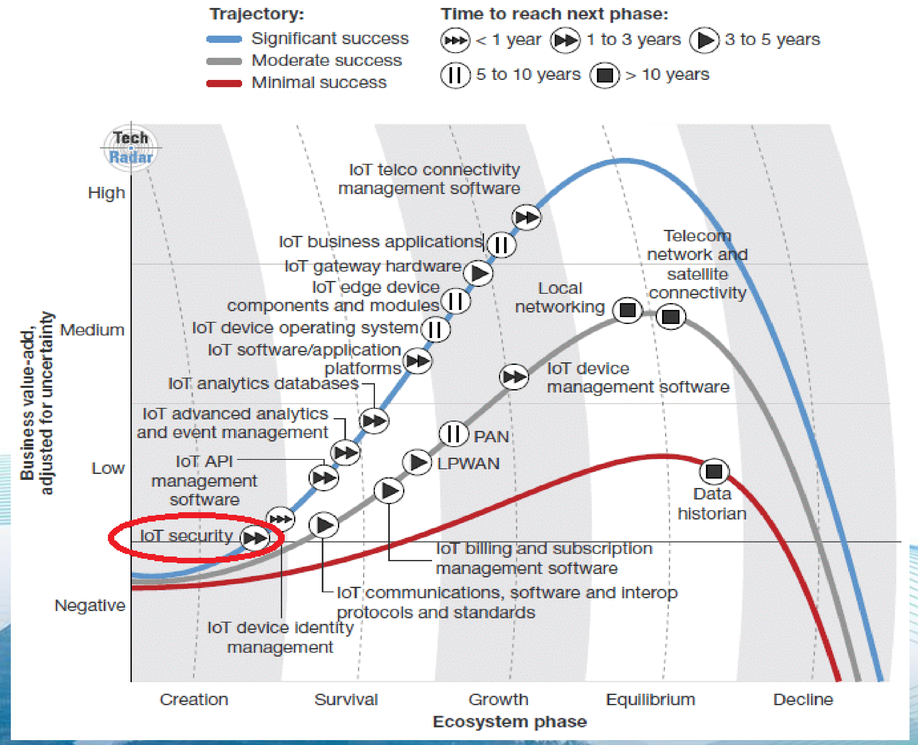
美国中情局的前CTO、著名安全专家Bob Flores是国际云安全联盟SDP标准工作组的联席主席.

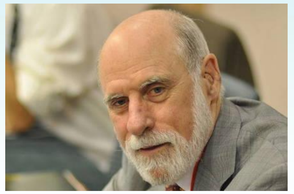
https://cloudsecurityalliance.org/working-groups/software-defined-perimeter/

物联网安全趋势与观点

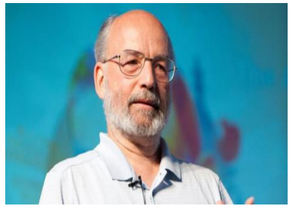
Forrester: 安全是IoT发展的关键

大部份IoT技术仍然在生存及成长阶段，标准和安全是成功的关键因素。IoT安全技术仍然在创建阶段，没有成熟的产品。

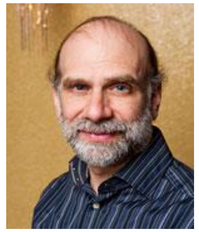




Vint Cerf, 互联网之父，谷歌首席布道师
“让我们保持万物互联，同时保证互联系统的安全与可靠性。”



Adi Shamir @ FC ‘2016: “物联网将是安全大灾难."



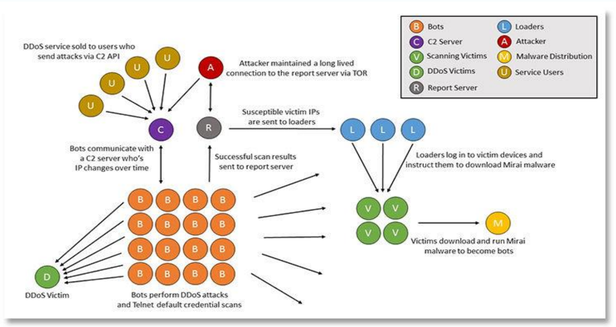
Bruce Schneier：现在大多数的“物”都是不安全的，有可能变成监视工具，要解决这问题会很困难... 物联网安全不能由市场经济原则驱动，政府要扮演主要角色，成立跨部门标准规范组织制定相应的安全规范.

Ross Anderson（剑桥大学）：物联网安全不单纯是一个技术问题，而是牵涉到心理学、道德、法律、保险等多方面的问题，安全工程将会很复杂，Safety将在未来一段时间比隐私更重要。

攻击面扩大，攻击方法推陈出新

物联网安全威胁从数字世界到物理世界，危及人身安全

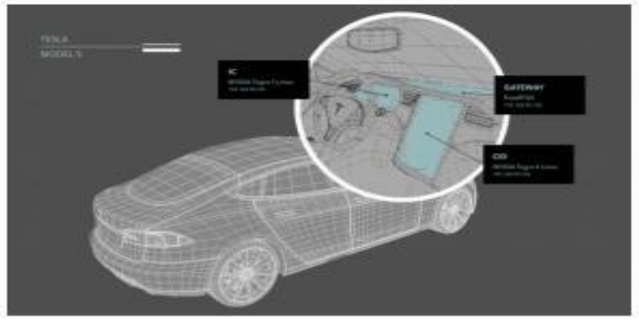
海量物联网设备感染病毒形成僵尸网络，发起美国史上最大规模DDoS攻击



1、利用TCP端口漏洞，绕过防火墙
2、停止telnet服务并关闭漏洞端口
3、端口嗅探，等待CC命令并发起DDoS攻击。

物联网小设备受制于**软件漏洞**，一旦联网会被黑客所利用，形成受控制的**僵尸网络**。

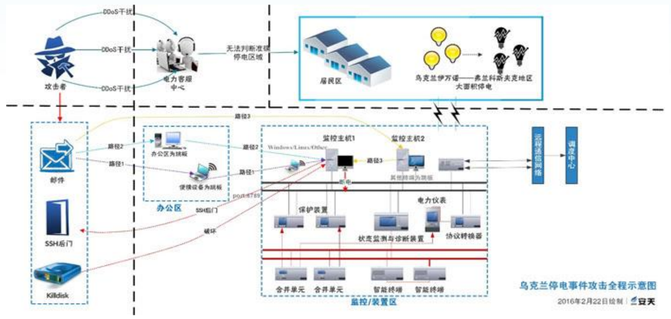
智能网联车遭受远程攻击，不但威胁车辆信息安全，更直接威胁人身安全



1、远程无线攻入车载HMI
2、多个漏洞提权，root权限登陆CID和IC上
3、连接到CAN总线，任意车身和行车控制

对联网智能设备的攻击不仅局限于虚拟世界，也直接危害到物理世界，甚至危及**生命安全**。

智能电网、工业物联网等关键基础设施面临黑客组织定点攻击，造成巨大经济损失



1、黑客通过钓鱼邮件，植入恶意代码
2、横向渗透，发送恶意载荷向受控SCADA节点发送断电指令
3、导致变电站中断了三个小时，22.5万用户停电

针对工业物联网的安全漏洞一旦被利用，会**瘫痪关键基础设施**的运行，对日常生活影响巨大。

欧美高度关注物联网安全威胁，跨政府部门协作

法案

A BILL

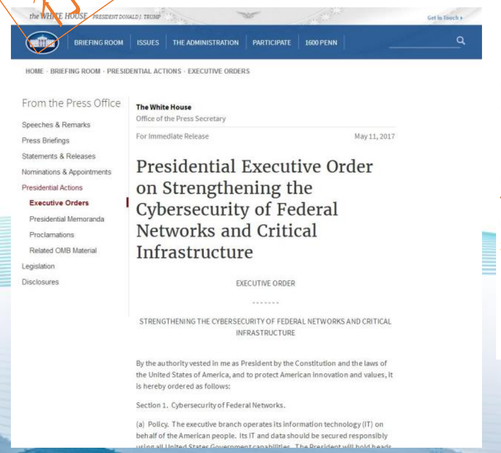
To provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Internet of Things (IoT) Cybersecurity Improvement Act of 2017".

行政令

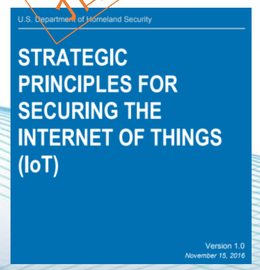


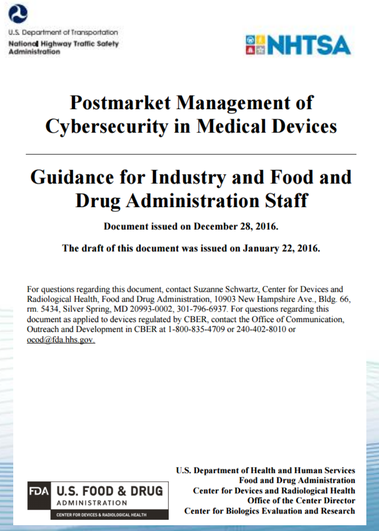
建议书

白皮书

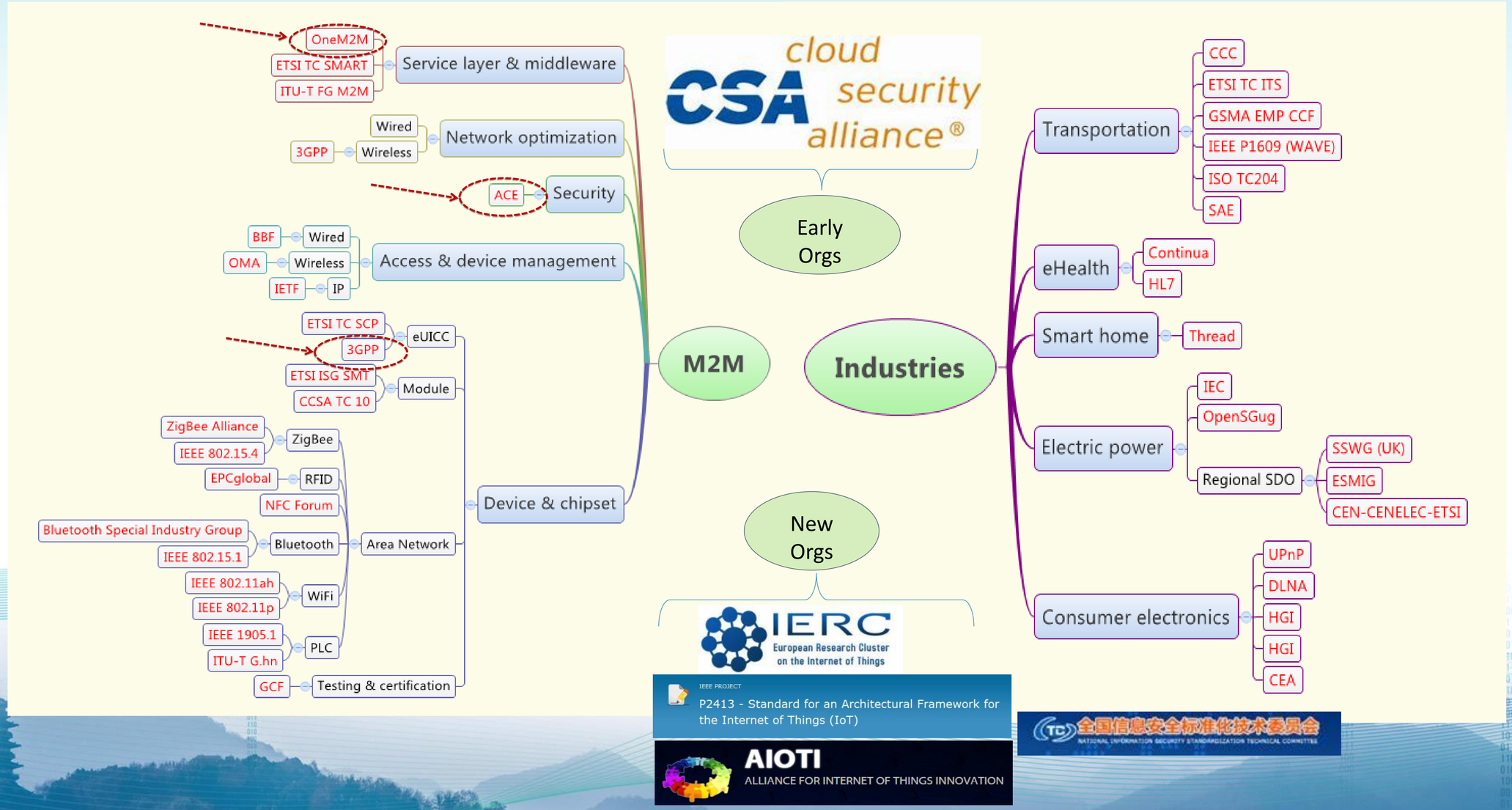
最佳实践

指导手册

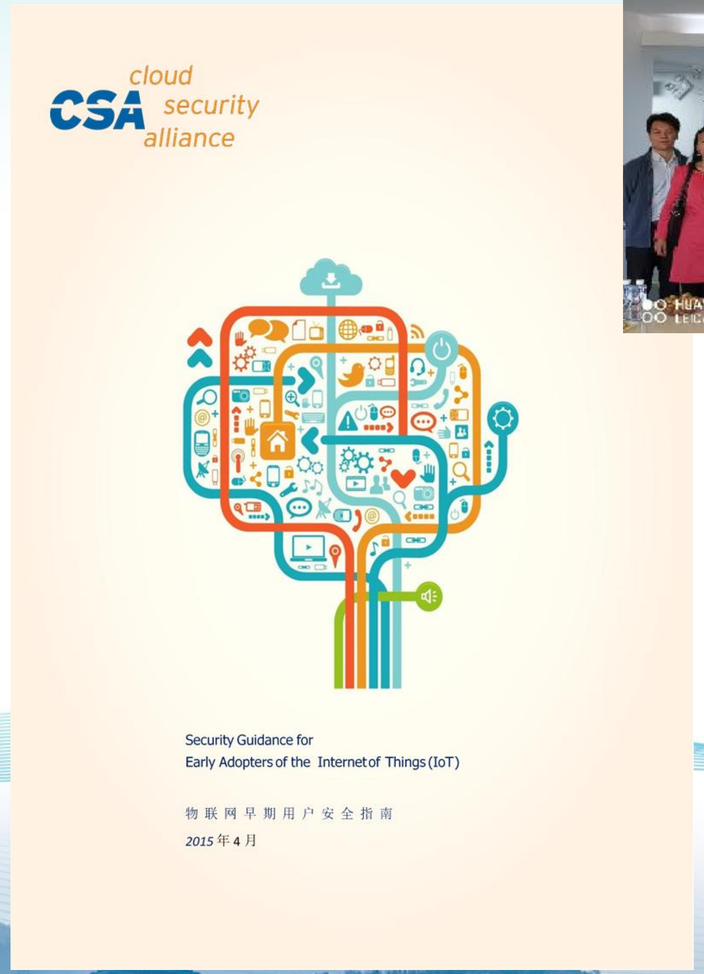


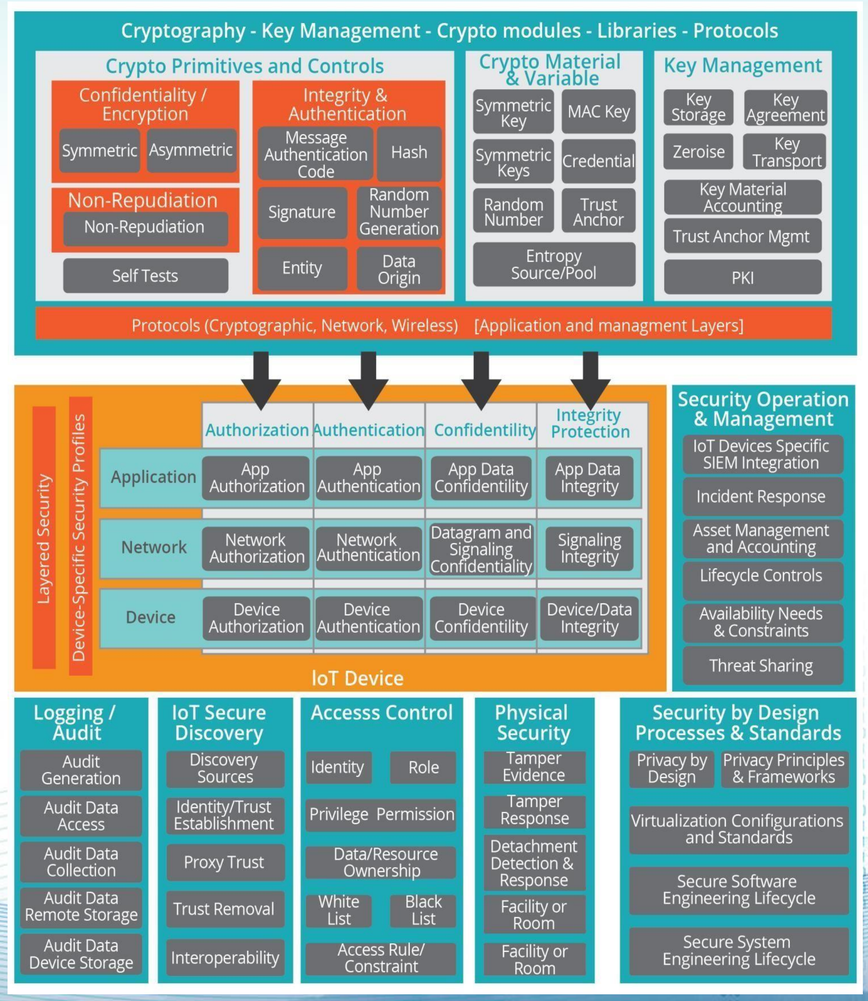


物联网标准组织与安全工作组



CSA物联网安全研究成果





发布：
CSA《物联网控制框架》与《物联网安全控制框架指南》

IoT Controls Framework and Guide to the IoT Security Controls Framework

iot CONTROLS FRAMEWORK	For more details about the framework, download the "Guide to the CSA IoT Controls Framework" at: https://cloudsecurityalliance.org/artifacts/guide-to-the-iot-security-controls-framework			IoT System Risk Impact Levels		
Control Domain	**Control ID**	**CCM ID**	**Control Specification**	**Confidentiality**	**Integrity**	**Availability**
Risk Mitigation *Risk Management Approach*	**RSM-01**	GRM-01	Adopt a standardized industry recognized risk management approach. Baseline security requirements should be established for developed or acquired IoT components to comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations should be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements should be reassessed based on business needs.	Low	Low	Low
Risk Mitigation *Risk Assessment*	**RSM-02**	GRM-02	Perform a risk assessment. Analyze sources, storage and transmissions of sensitive data across devices, gateways, applications, data stores, mobile applications, cloud services, fog computing services and network infrastructure. Analyze data classification mechanisms and data security capabilities to protect sensitive data from unauthorized use, access, loss, destruction, and falsification. Analyze the potential for trusted insiders to misuse their privileged access to data. Analyze data retention periods and end-of-life disposal requirements. Identify safety risks. Prioritize risks based on impact and likelihood. Decide on risk migitations for each risk - mitigate, defer or accept the risk. Perform a risk assessment as follows: •Analyze potential risk if the security of each of the following components would be compromised: sources, storage and transmissions of sensitive data across devices, gateways, applications, data stores, mobile applications, cloud services, fog computing	Low	Low	Low

cloud security alliance®

- IoT Controls Framework
  - Security controls framework
  - Continuation of CCM, specific to IoT
  - Flexible design
- Guide to IoT Security Controls Framework
  - Explains how to use the matrix

报告下载地址：https://www.c-csa.cn (研究项目-文件下载)

THANK YOU

谢　　谢　　观　　看

邮箱：info@c-csa.cn
微信：csagcr
网站：http://c-csa.cn