Segurança em IoT é possível !

Desenvolvimento seguro de dispositivos IoT

Anchises Moraes
@anchisesbr @CSAbr
@RSASecurity @BSidesSP

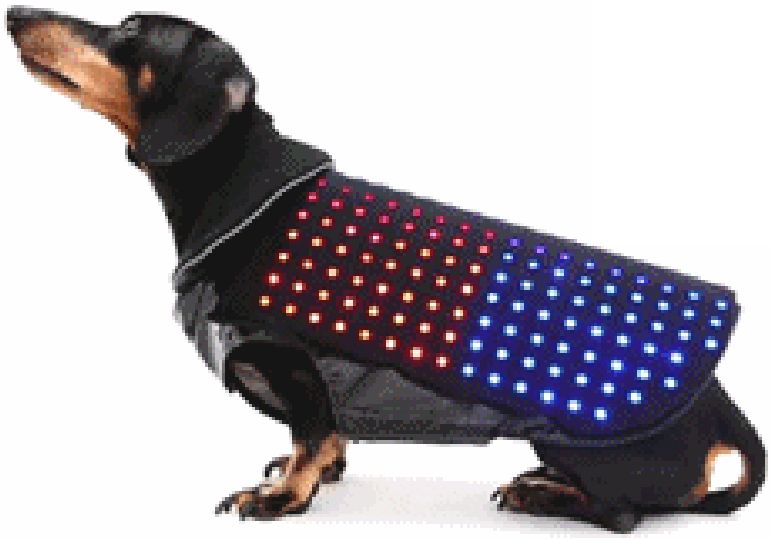
cloud security alliance SM
CSABR BRAZIL CHAPTER

Agenda

Internet of Things

Internet of Threats

Segurança em IoT



Picture source: Giphy

INTERNET OF THINGS

O que são? Aonde vivem? O que comem?

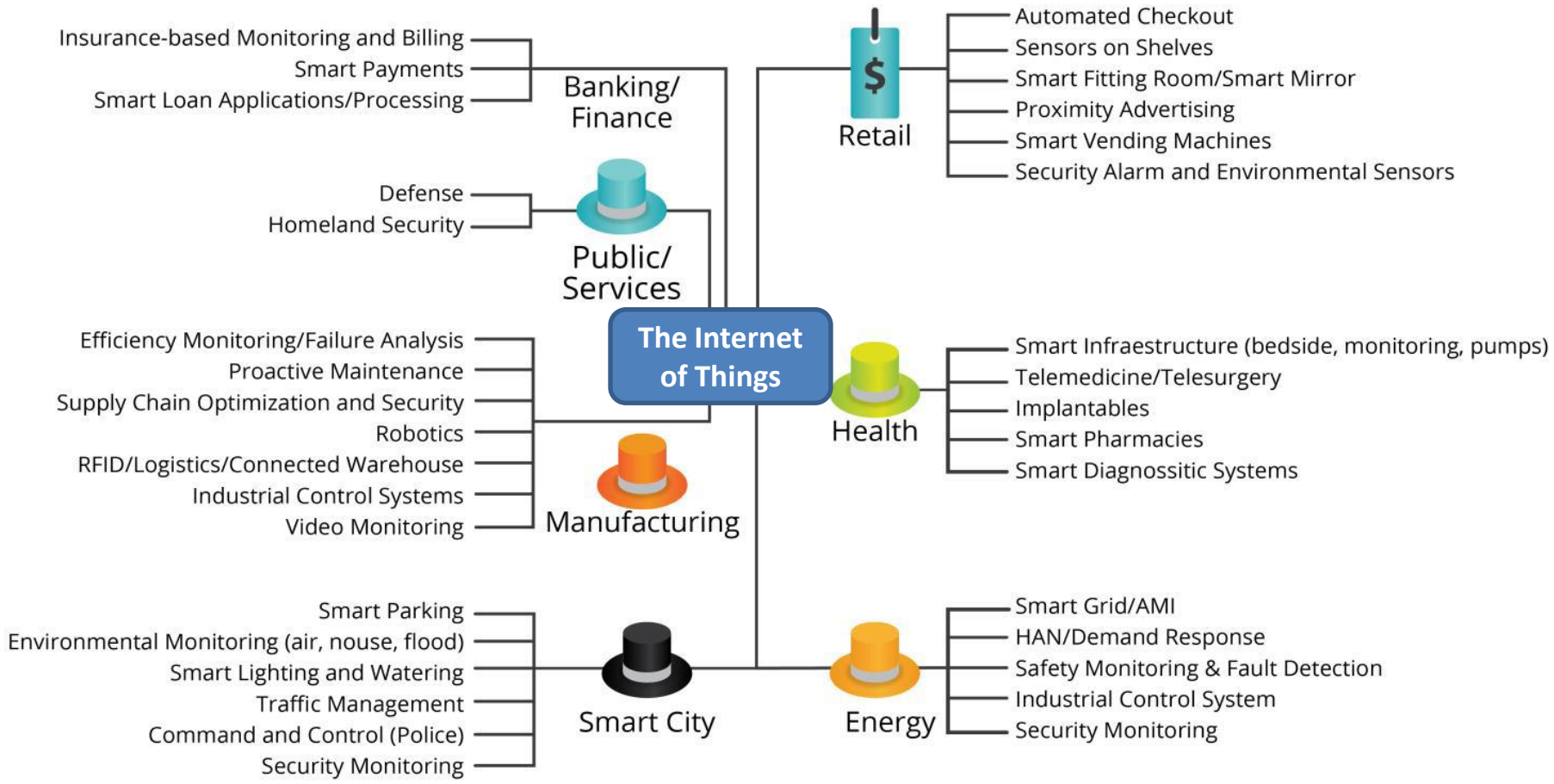
CSABR BRAZIL CHAPTER cloud security alliance SM

IoT ?

- “Internet dos Trecos”
- “Internet dos Trem”

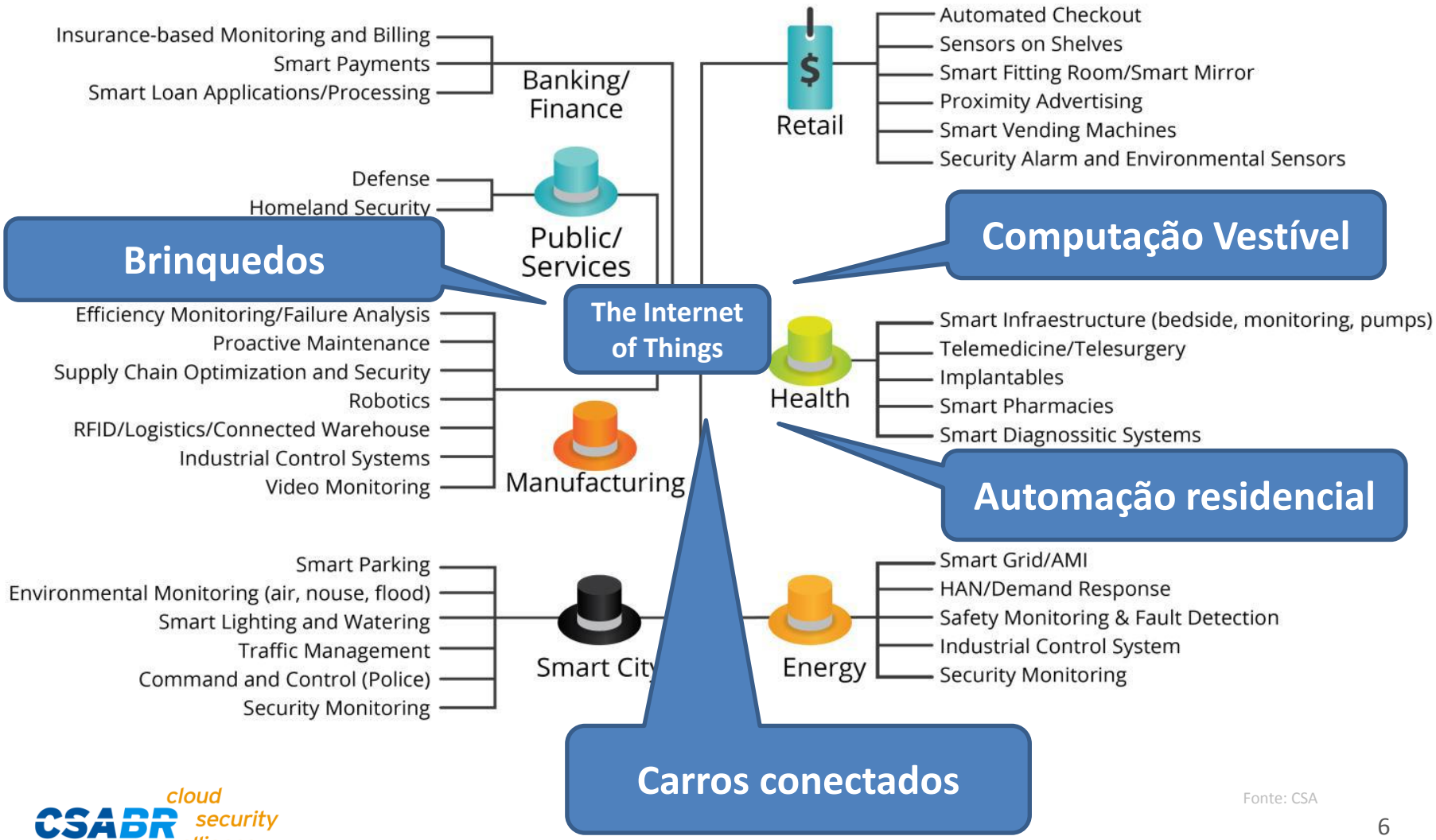
Fonte: Wikimedia Commons

IoT ?



Fonte: CSA

IoT ?



Fonte: CSA

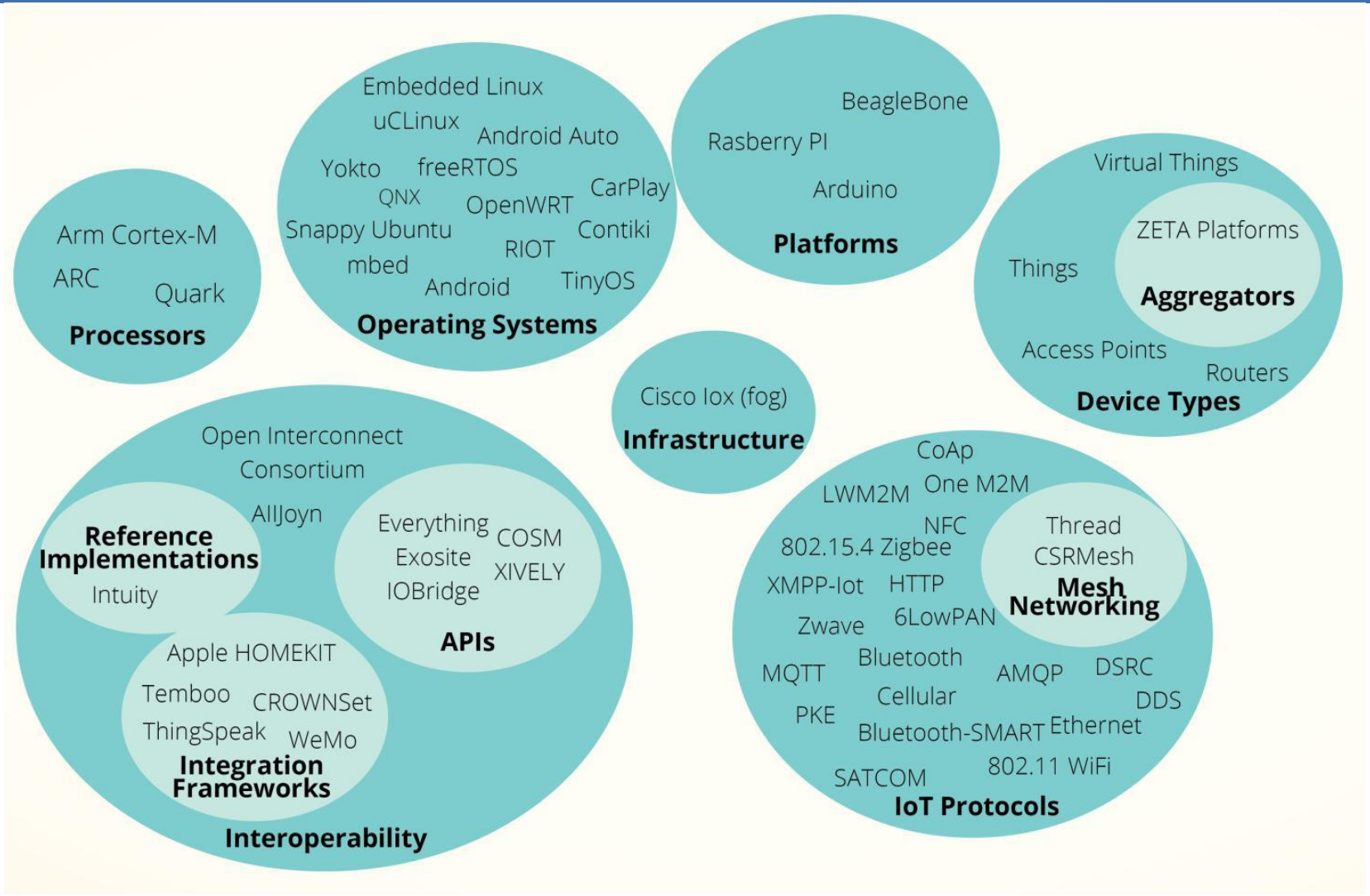
34bi

Dispositivos conetados na Internet em 2020

7,7 bilhões de pessoas em 2020

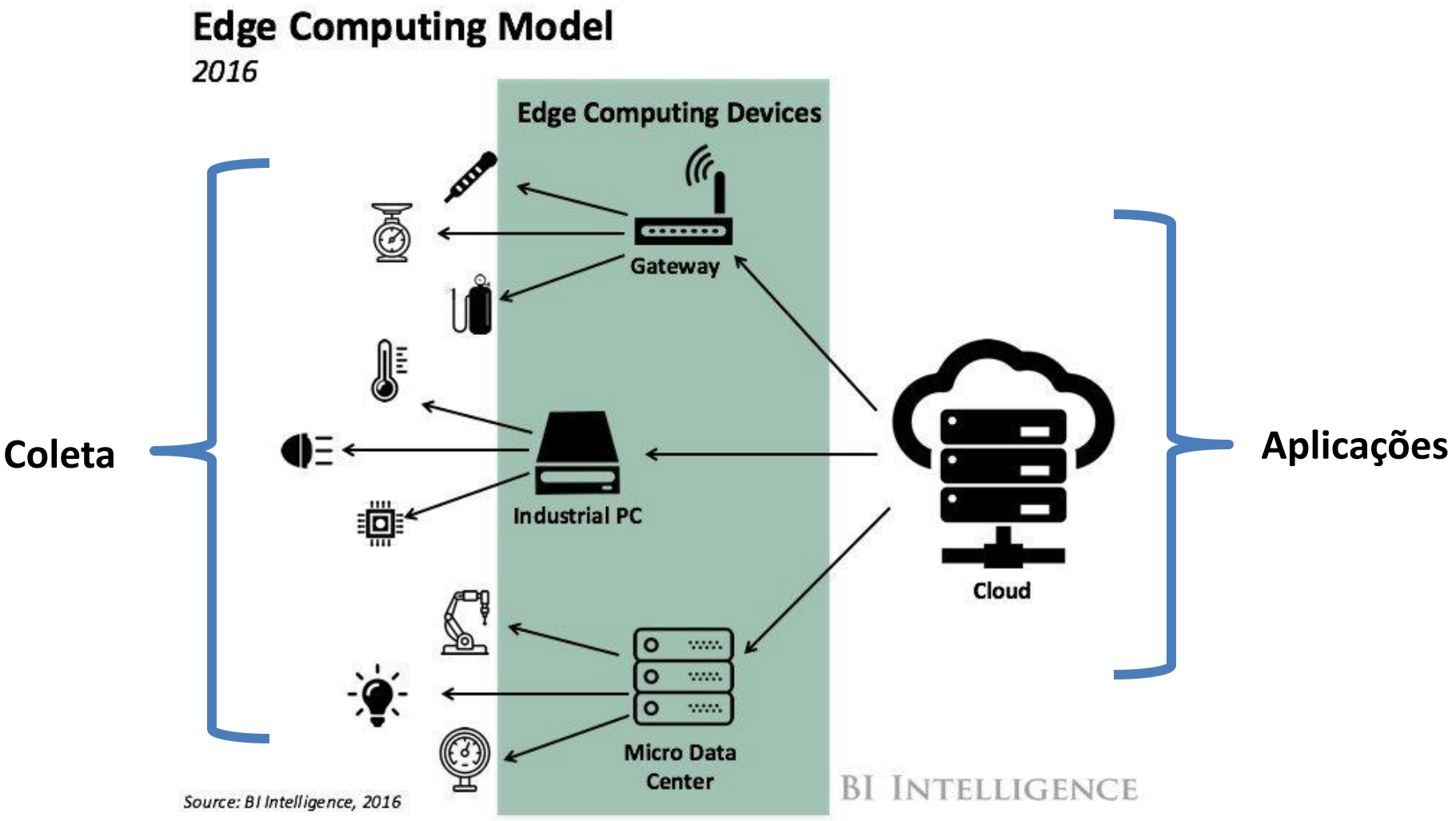
Fontes: http://www.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10
http://www.worldometers.info/world-population/

IoT Ecosystem



Fonte: CSA

Fog computing e IoT



Fonte: http://www.businessinsider.com/internet-of-things-cloud-computing-2016-10

INTERNET OF THREATS

Segurança em IoT ?

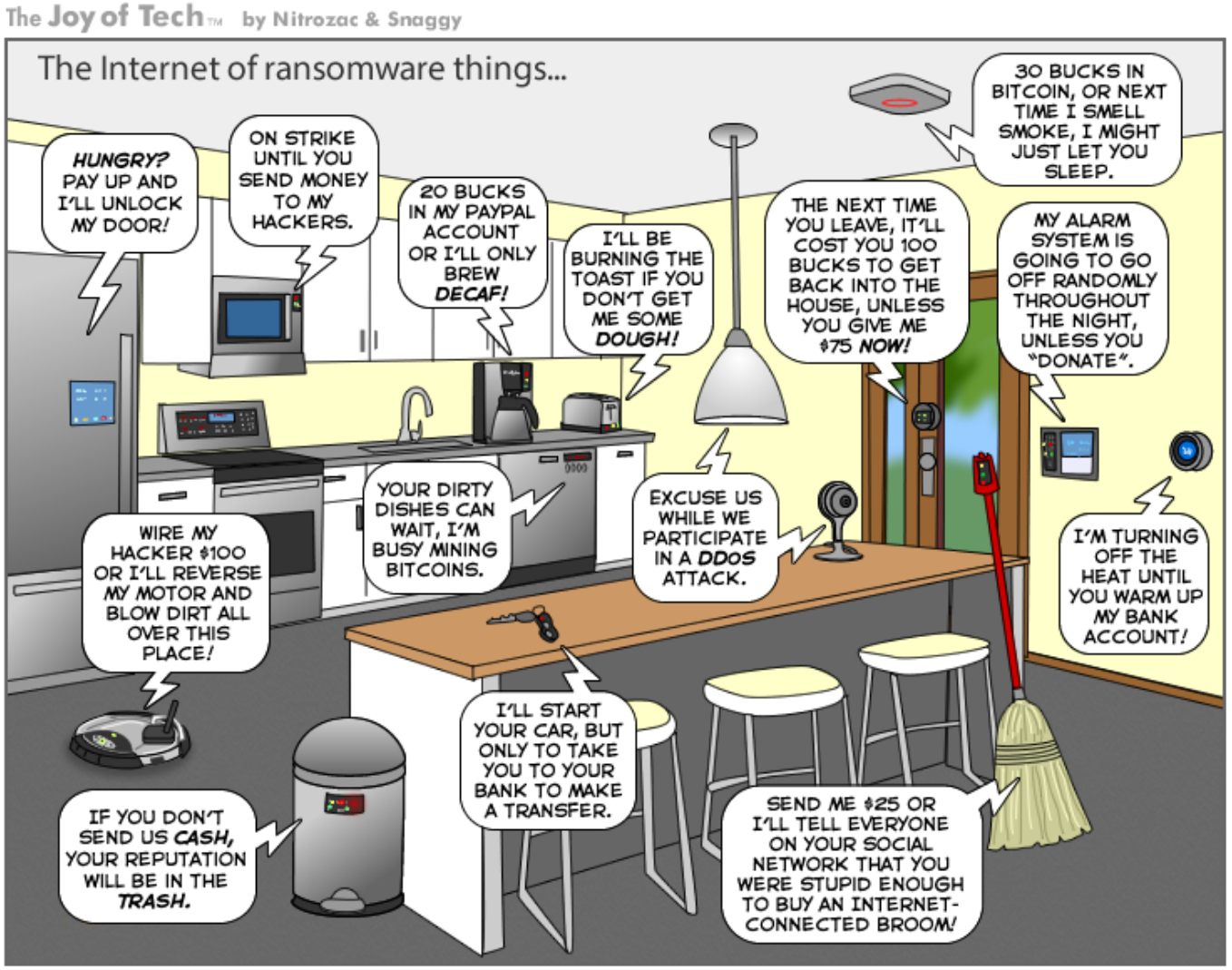
Segurança em IoT?

"Fazemos segurança em IoT como fazíamos segurança na Web nos anos 90"

Julio Cesar Fort

@juliocesarfort

Internet of Threats



Fonte: http://www.joyoftech.com/joyoftech/joyarchives/2340.html

Necessidade de segurança em IoT

- Privacidade e proteção de dados
- Uso por agentes maliciosos
- Pontos de lançamento de ciber ataques
- Danos resultantes do comprometimento de sistemas físicos

Desafios de segurança em dispositivos IoT

- Produtos implantados em ambientes inseguros ou fisicamente expostos
- A segurança é nova para fabricantes de IoT
  - Segurança não é prioridade de negócios
  - Metodologias de desenvolvimento sem abordagem de segurança
  - Falta de padrões e arquiteturas de referência para o desenvolvimento seguro de IoT
  - Falta de desenvolvedores de IoT com habilidades de segurança

COMO PROTEGER O SEU IOT

Dicas de segurança em IoT para usuários finais

CSA BR BRAZIL CHAPTER cloud security alliance SM

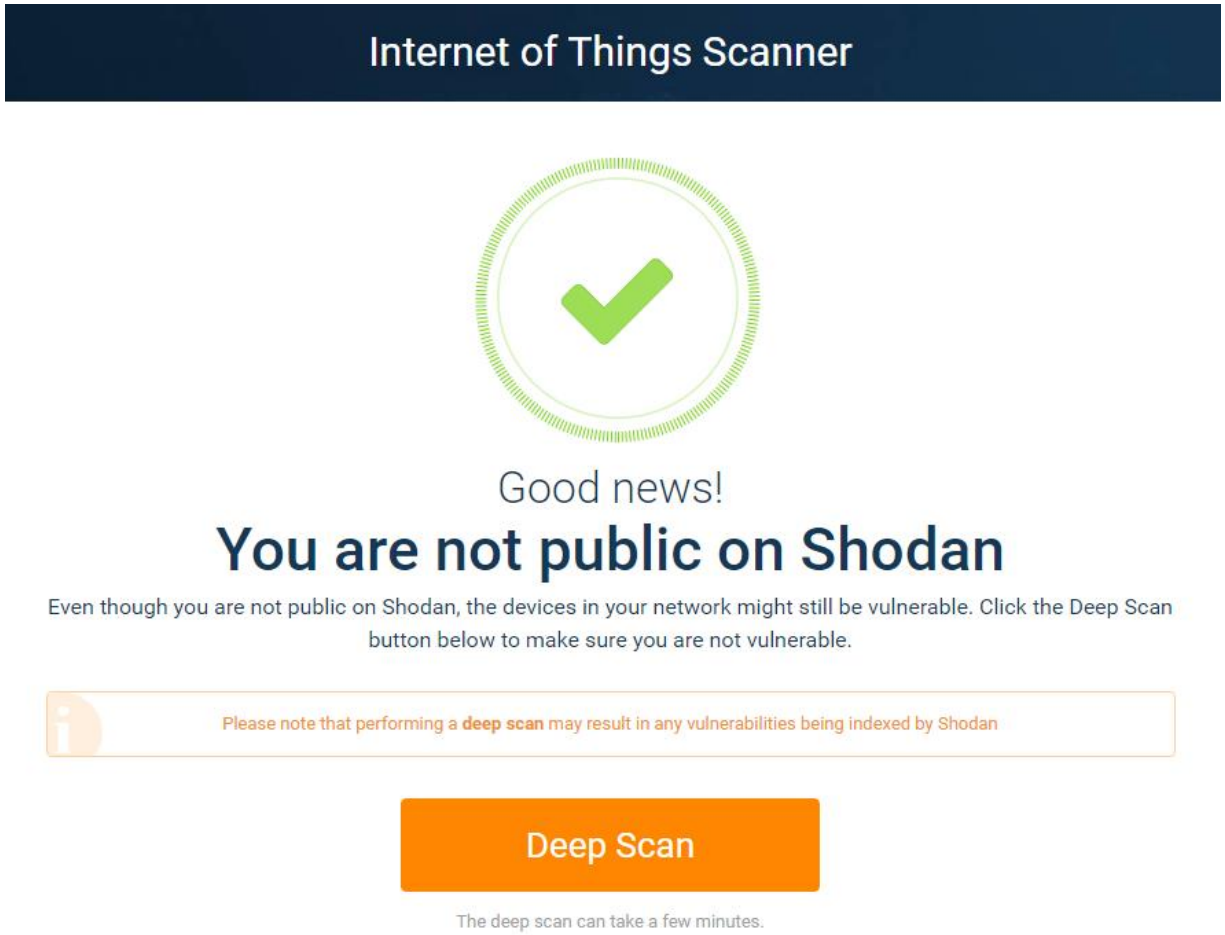
Dicas rápidas

- Altere as senhas padrão de seus dispositivos conectados
- Desativar o recurso Universal Plug-and-Play (UPnP)
- Revisar as restrições de Gerenciamento Remoto
- Verifique as atualizações de software

Fonte: The Hacker News

Online Scan

http://iotscanner.bullguard.com



COMO FAZER SEGURANÇA EM IOT

Guia para segurança em IoT para desenvolvedores

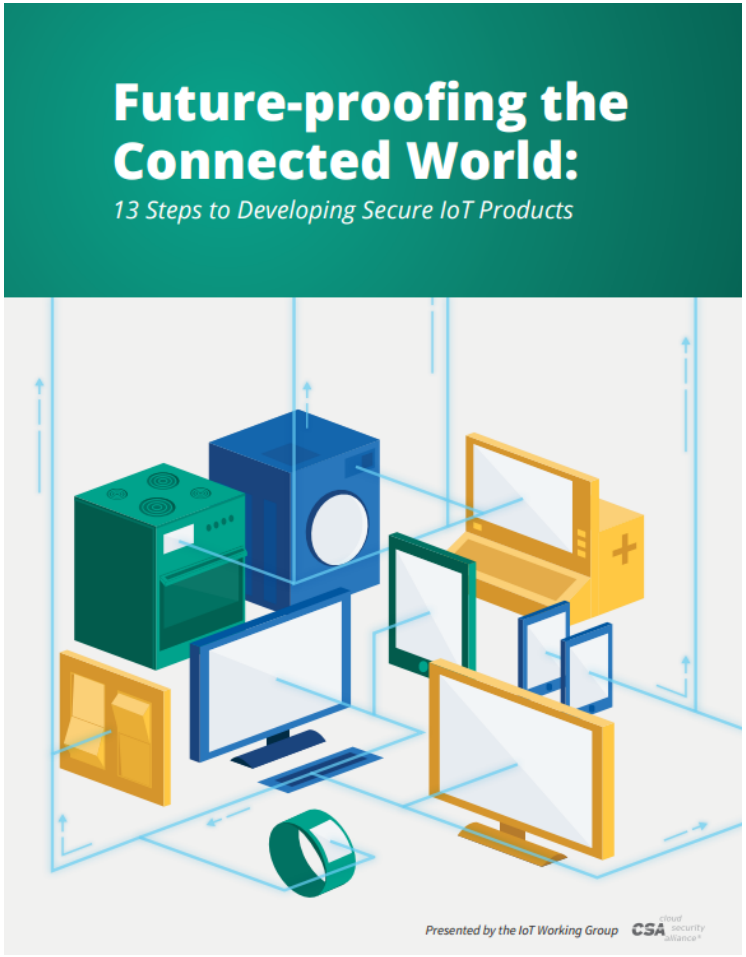
CSA BR BRAZIL CHAPTER cloud security alliance SM

Guia para Segurança em IoT

"Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products“

Cloud Security Alliance

07/outubro/2016



https://cloudsecurityalliance.org/download/future-proofing-the-connected-world/

13 passos para segurança em IoT


Picture source: http://www.freeimages.com

1. Metodologia de desenvolvimento seguro
2. Ambiente seguro de desenvolvimento
3. Recursos de segurança da plataforma
4. Definir proteções de Privacidade
5. Controles de segurança em hardware
6. Proteger dados
7. Proteger aplicativos e serviços associados
8. Proteger interfaces e APIs
9. Atualização segura
10. Autenticação, Autorização e Controle de Acesso
11. Gerenciamento seguro de chaves
12. Fornecer mecanismos de Log
13. Revisões de segurança

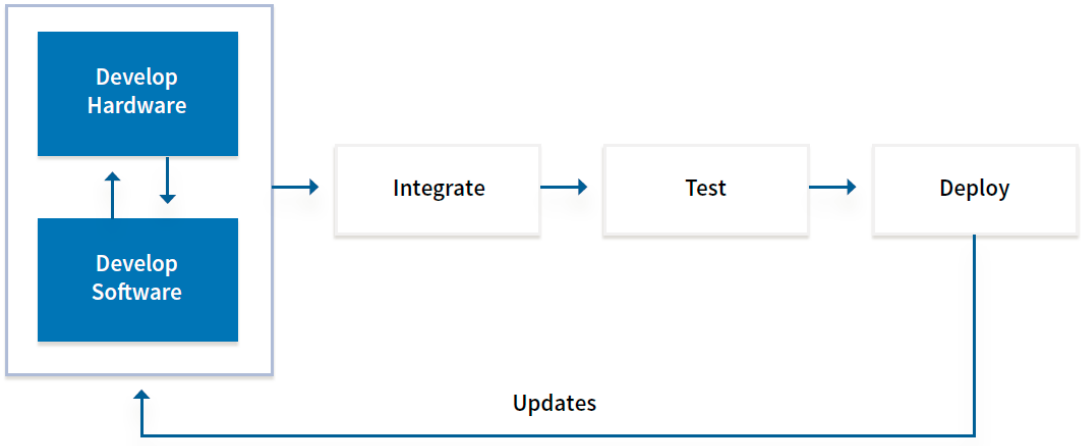
1- Metodologia de desenvolvimento seguro

- Modelagem de ameaças
- Requisitos e processos de Segurança nas metodologias de desenvolvimento
- Avaliação de impacto de segurança

Picture source: Giphy

2- Ambiente seguro de desenvolvimento e integração

- Avaliar as linguagens de programação
- Ambientes de Desenvolvimento Integrado
  - Plugins e ferramentas de teste de segurança



- Testes e Qualidade do código

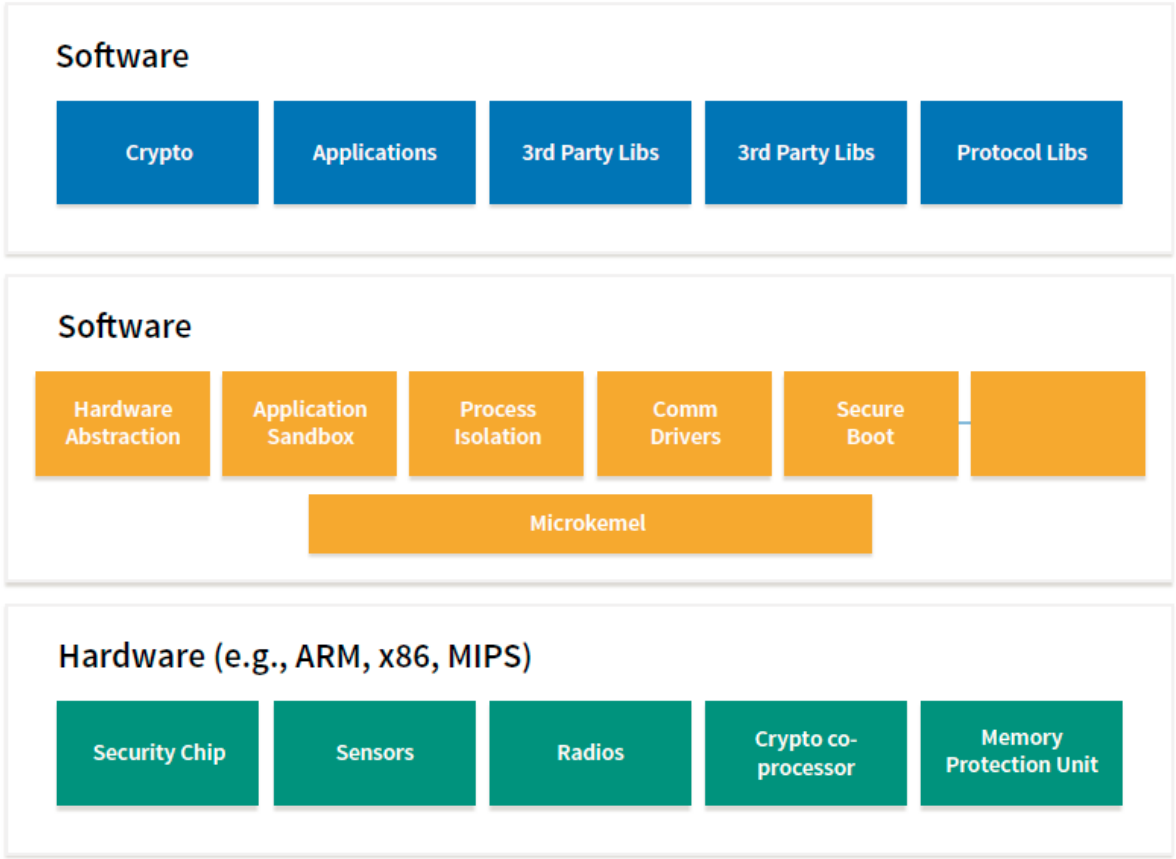
3- Recursos de segurança da plataforma e do Framework

- Selecione o Framework de integração

Framework	Transports	Languages Supported	Platforms	On-Boarding	Asset Mgmt	Config Mgmt	Secure Connection
AllJoyn	WiFi Ethernet Serial PLC	C C++ Obj-C Java	Arduino Linux Android iOS Windows MAC	●	●	●	●
HomeKit	WiFi Bluetooth-LE (on top of HomeKit Accessory Protocol (HAP)	Objective-C	iOS				●
IoTivity		C C++ Java JavaScript		●		●	●
ThingWorx		Java JavaScript					●
Xively		JavaScript	Android iOS	●	●	●	●
Oracle Java Embedded		Java JavaScript					●

3- Recursos de segurança da plataforma e do Framework *(cont.)*

- Avalie as funcionalidades de segurança da plataforma



4- Definir proteções de Privacidade

Picture source: Giphy

- Reduzir a coleta de dados ao mínimo necessário
- Suportar anonimato quando possível
- Verificar regulamentações de proteções de dados

5- Controles de segurança em hardware

- Segurança do Microcontrolador
- Trusted Platform Modules
- Proteção de Memória
- Chips especializados em segurança
- Módulos criptográficos
- Proteção física
- Supply chain (fornecedores)

Picture source: Giphy

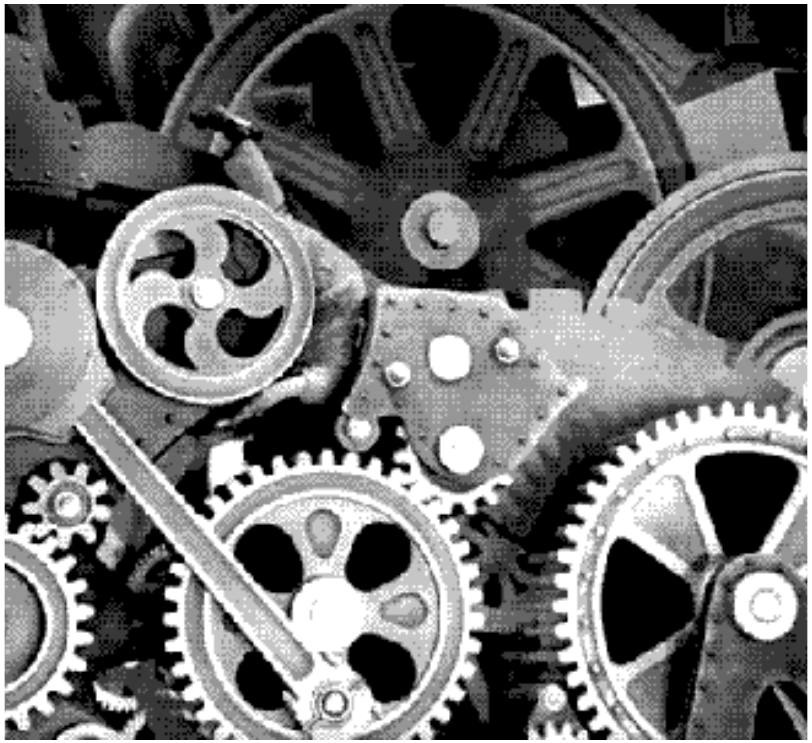
6- Proteger os dados

Picture source: Giphy

- Escolha dos protocolos de comunicação
  - Varredura de redes
  - Escuta de tráfego
  - Spoofing e masquerading
  - Negação de serviço e jamming
  - Pareamento de dispositivos

7. Proteger aplicativos e serviços associados

- Pontos de integração, apps e serviços
- Privilégios de acesso entre dispositivo e aplicações
- Uso de serviços em nuvem



Picture source: Giphy

8- Proteger interfaces e APIs

Picture source: Giphy

- Validação de mensagens
- Tratamento de erros
- Proteção contra ataques de replay
- Proteja a comunicação via API
  - Criptografia, autenticação
- Certificate Pinning

9- Atualização segura

- Updates de firmware e de software
- Considerar todo o ciclo de instalação e atualização
- Proteger contra modificações não autorizadas

Picture source: Pinterest

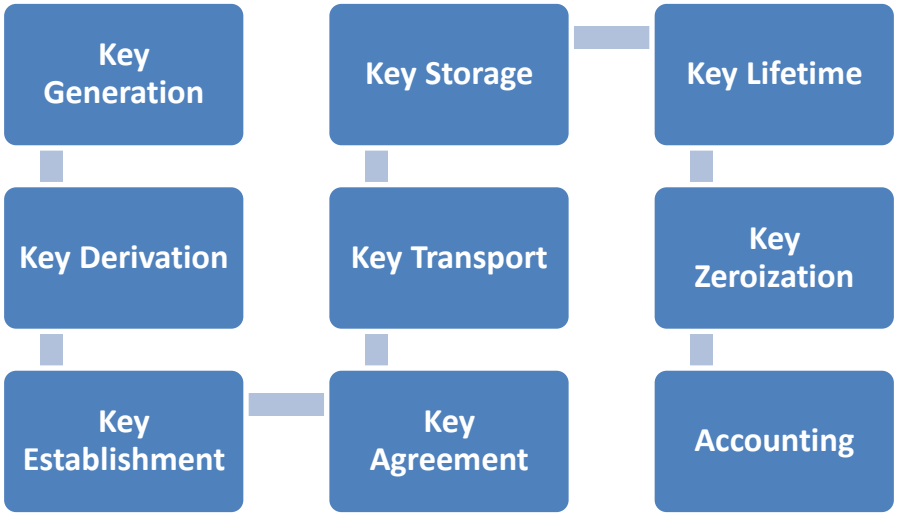
10- Autenticação, Autorização e Controle de Acesso

Picture source: Giphy

- Comunicação entre dispositivos
- Autenticação fim-a-fim
- Uso de TLS e de certificados para autenticação
- OAuth 2.0 para autorização

11- Gerenciamento seguro de chaves criptográficas

- Interação com PKI
- Provisionamento de chaves
- Características das chaves
- Armazenamento seguro
- Validação do certificado
- Boot seguro



12- Mecanismos de Log

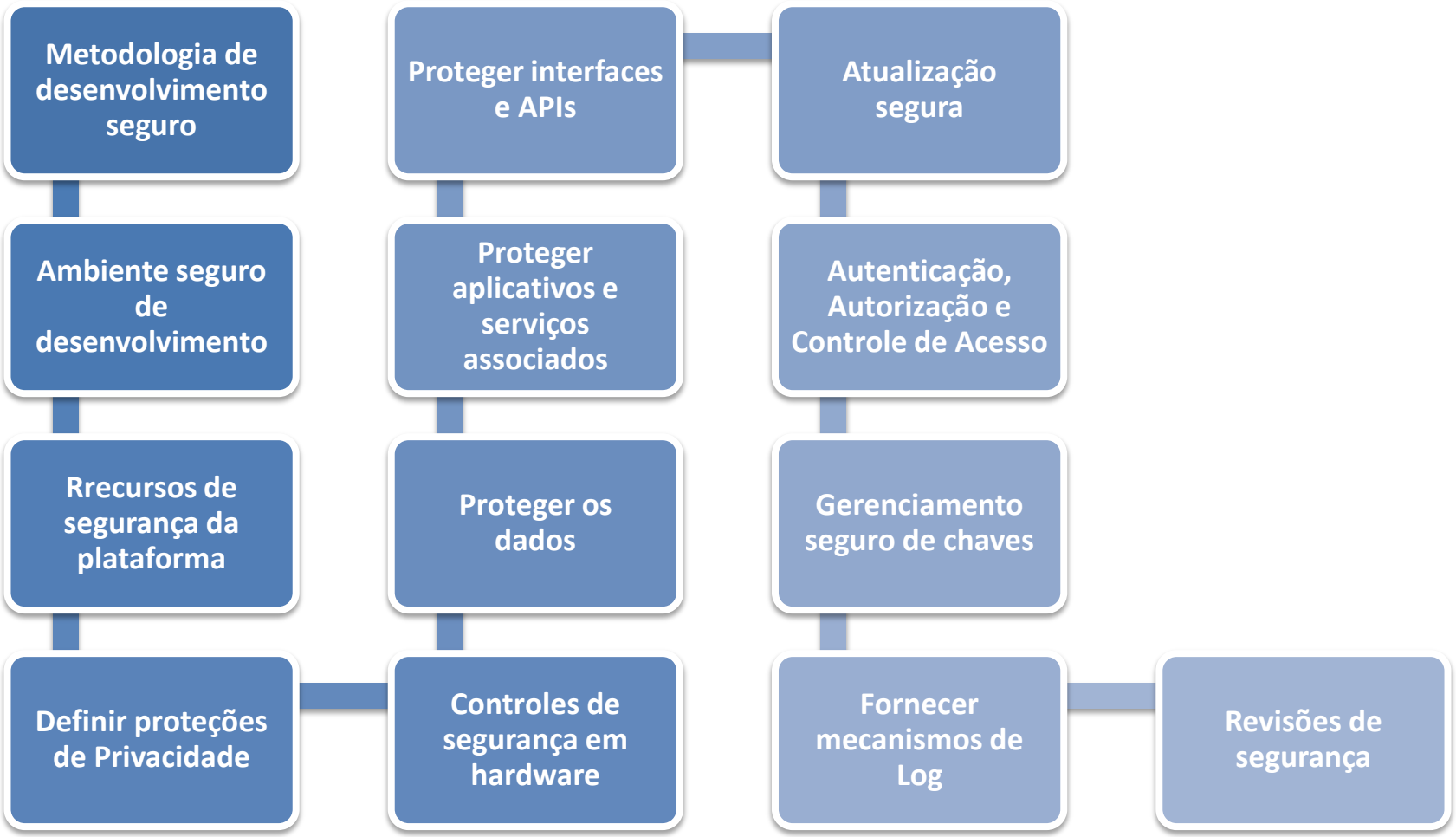
Picture source: Giphy

- Visibilidade das ações que ocorrem no dispositivo, ex:
  - Solicitação de Conexão
  - Autenticação (falha / sucesso)
  - Tentativas de abuso e elevação de privilégios
  - Mensagens malformadas
  - Atualizações de firmware e software
  - Tentativas de acesso
  - Mudanças de configuração
  - Acesso à memória protegida
  - Acesso físico indevido

13- Revisões de segurança

- Feedback contínuo
- Testes de Segurança
  - Static Application Security Testing (SAST)
  - Dynamic Application Security Testing (DAST)
  - Interactive Application Security Testing (IAST)
  - Superfície de ataques
  - Bibliotecas de terceiros
  - Fuzzing
  - Testes Customizados

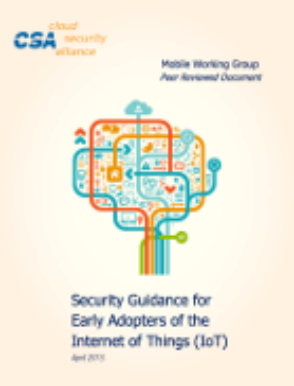
Relembrando...



Para saber mais

Internet of Things Working Group
https://cloudsecurityalliance.org/group/internet-of-things/

“Security Guidance for Early Adopters of the IoT”



https://cloudsecurityalliance.org/download/new-security-guidance-for-early-adopters-of-the-iot/

Quem é a CSA?

Cloud Security Alliance (CSA)

- Associação sem fins lucrativos
- Reúne pessoas físicas e Empresas
- Oficializada em Dezembro de 2008
- **+65mil** Membros, **+190** membros corporativos
- Presente em **+40** países através de **+70** Chapters locais

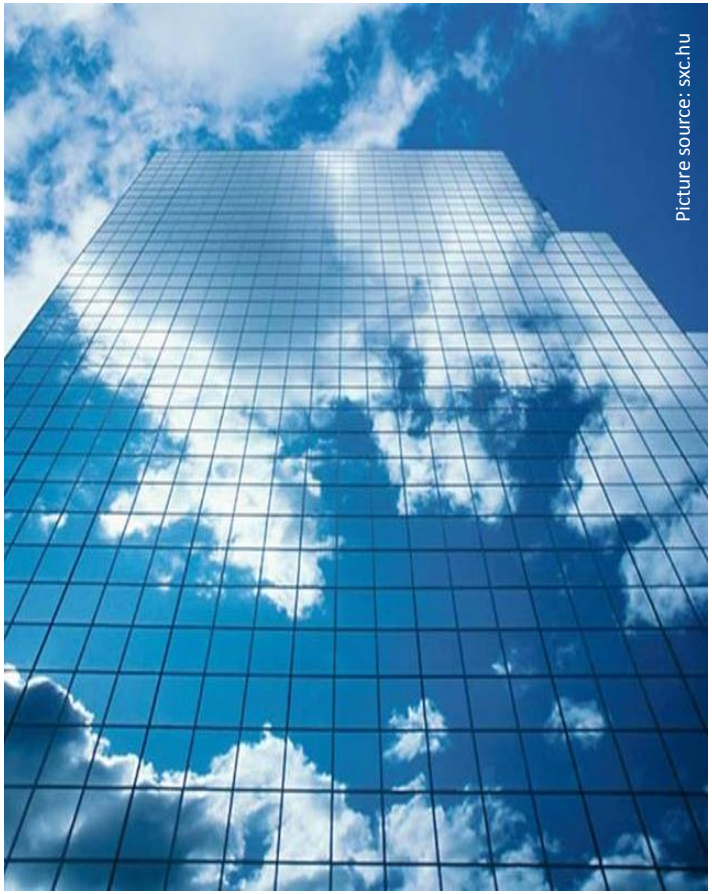
CSA Brasil

- Segundo Chapter oficial da CSA
  - Oficializado em 27 de Maio de 2010
- Segue Missão e Objetivos da CSA Global
  - Promover a Segurança em Cloud Computing
  - Promover pesquisas e iniciativas locais

CSABR BRAZIL CHAPTER cloud security alliance SM

Missão

"Promover a utilização das melhores práticas para fornecer garantia de segurança dentro de Cloud Computing, e oferecer educação sobre os usos de Cloud Computing para ajudar a proteger todas as outras formas de computação."



Diversas iniciativas de pesquisa

https://cloudsecurityalliance.org/research

Dezenas de Papers

https://cloudsecurityalliance.org/research

Educação

https://cloudsecurityalliance.org/education

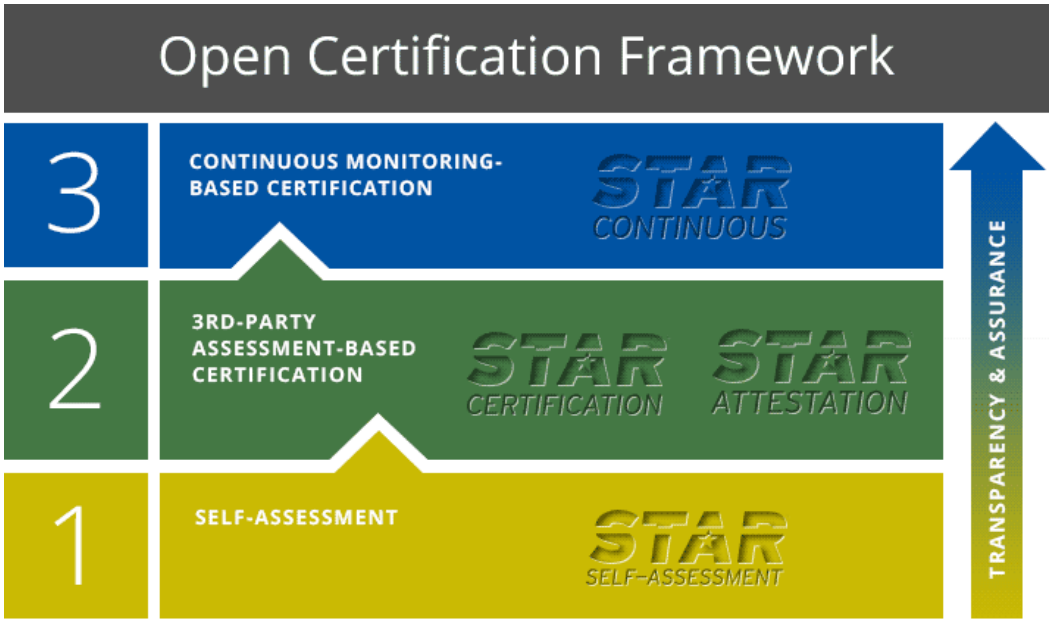
- Certificação “Certificate of Cloud Security Knowledge (CCSK)”
  - Exame online
- Treinamento
  - CCSK training (Basic / Plus)
  - PCI Cloud training
  - GRC Stack training

https://ccsk.cloudsecurityalliance.org

Outras Iniciativas

https://cloudsecurityalliance.org/star

- CSA Security, Trust & Assurance Registry (STAR) Program
  - Avaliação da segurança e maturidade dos provedores de Cloud Computing
  - Baseado nas melhores práticas da CSA
  - Registro e acesso público gratuitos



CSA BR BRAZIL CHAPTER cloud security alliance SM

Como se Associar

- Pessoa Física
  - Participação no grupo do LinkedIn
  - Participação na lista de discussões dos projetos (http://br.groups.yahoo.com/group/csabrasil)
  - Sem custo
- Pessoa Jurídica
  - Contato diretamente com a CSA Internacional
  - Taxa anual

Contato

- Cloud Security Alliance
  https://www.cloudsecurityalliance.org
  http://www.linkedin.com/groups?gid=1864210
  @cloudsa

- Cloud Security Alliance Brasil
  https://chapters.cloudsecurityalliance.org/brazil
  https://www.linkedin.com/groups?gid=3079437
  @csabr

OBRIGADO

Anchises Moraes
@anchisesbr @CSAbr @RSASecurity @BSidesSP

CSABR BRAZIL CHAPTER cloud security alliance SM

Nota sobre o uso de imagens

LEI Nº 9.610, DE 19 DE FEVEREIRO DE 1998.

Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências.

https://www.planalto.gov.br/ccivil_03/leis/L9610.htm

- Art. 44. O prazo de proteção aos direitos patrimoniais sobre obras audiovisuais e fotográficas será de setenta anos, a contar de 1° de janeiro do ano subseqüente ao de sua divulgação.
- Art. 46. Não constitui ofensa aos direitos autorais:
- VIII - a reprodução, em quaisquer obras, de pequenos trechos de obras preexistentes, de qualquer natureza, ou de obra integral, quando de artes plásticas, sempre que a reprodução em si não seja o objetivo principal da obra nova e que não prejudique a exploração normal da obra reproduzida nem cause um prejuízo injustificado aos legítimos interesses dos autores.