Segurança e conformidade na AWS

Marcello Zillo Neto - mzillo@amazon.com
Security Lead / LATAM

Antes…

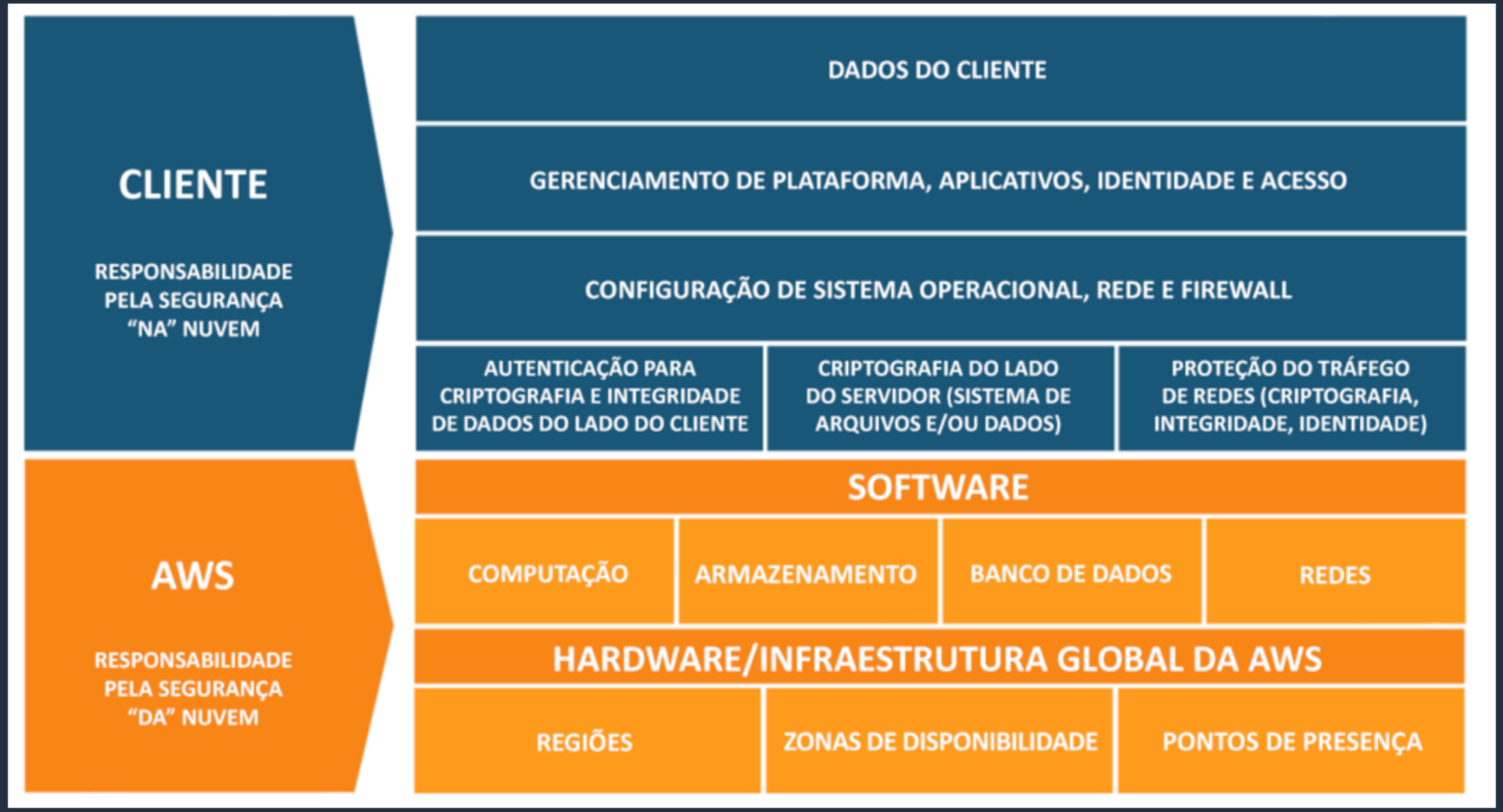
Ser ágil ou Estar seguro

Agora…

Ser ágil E Estar seguro

aws

Modelo de Responsabilidade Compartilhada



Base de Dados em ambiente tradicional

- App optimization
- Scaling
- High availability
- Database backups
- DB s/w patches
- DB s/w installs
- OS patches
- OS installation
- Server maintenance
- Rack & stack
- Power, HVAC, net
- Physical Security

aws

Base de Dados em Máquinas Virtuais (Amazon EC2)

Serviços de Infraestrutura

App optimization

Scaling

High availability

Database backups

DB s/w patches

DB s/w installs

OS patches

OS installation

Server maintenance

Rack & stack

Power, HVAC, net

Physical Security

aws

aws

Base de Dados no Amazon RDS / Aurora

Serviços en Contêiners

- Scaling
- High availability
- Database backups
- DB s/w patches
- DB s/w installs
- OS patches
- OS installation
- Server maintenance
- Rack & stack
- Power, HVAC, net
- Physical Security

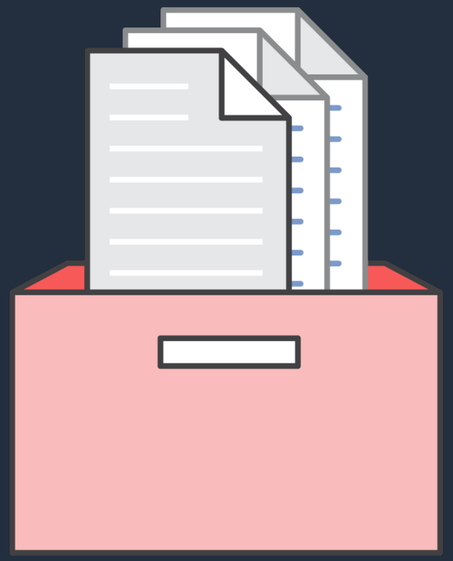
App optimization

aws

aws

O cliente é proprietário dos dados, controla o acesso e a localização

Propriedade



Acesso

Rastreabilidade

Você mantém a propriedade e o controle de seu conteúdo, e escolhe em que região o conteúdo reside.

aws

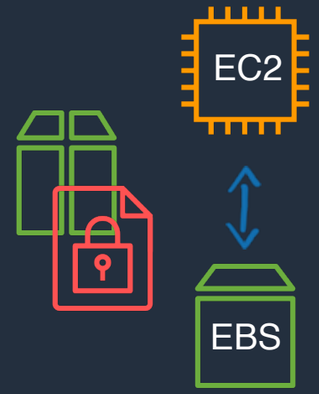
Criptografia de ponta a ponta: Em repouso

AWS Key Management Service (KMS) - CloudHSM

AWS KMS

Criptografia de Volume

- Criptografia de disco (EBS)
- Arquivos
- Soluções de Parceiros / Marketplace



Criptografia de Objetos

- Criptografia do lado do Servidor (SSE-S3)
- S3 SSE com chaves administradas pelo cliente (KMS)
- Criptografia do lado do cliente

Criptografia de Banco de Dados

- MS SQL Server
- Oracle
- MySQL
- PostgreSQL
- Amazon Redshift

aws

Programa de conformidade AWS

CSA Cloud Security Alliance Controls

ISO 9001 Global Quality Standard

ISO 27001 Security Mgmt Controls

ISO 27017 Cloud Specific Controls

ISO 27018 Personal Data Protection

PCS DSS Level 1

+200

certificações e acreditações de segurança e conformidade

SOC 1 Audit Controls Report

SOC 2 Security, Availability & Confidentiality Report

SOC 3 General Controls Report

C5 (Germany) Operational Security Attestation

Cyber Essentials Plus (UK) Cyber Threat Protection

ENS High (Spain) Spanish Govt Standards

G-Cloud (UK) UK Govt Standards

IT-Grundschutz (Germany) Baseline Protection Methodology

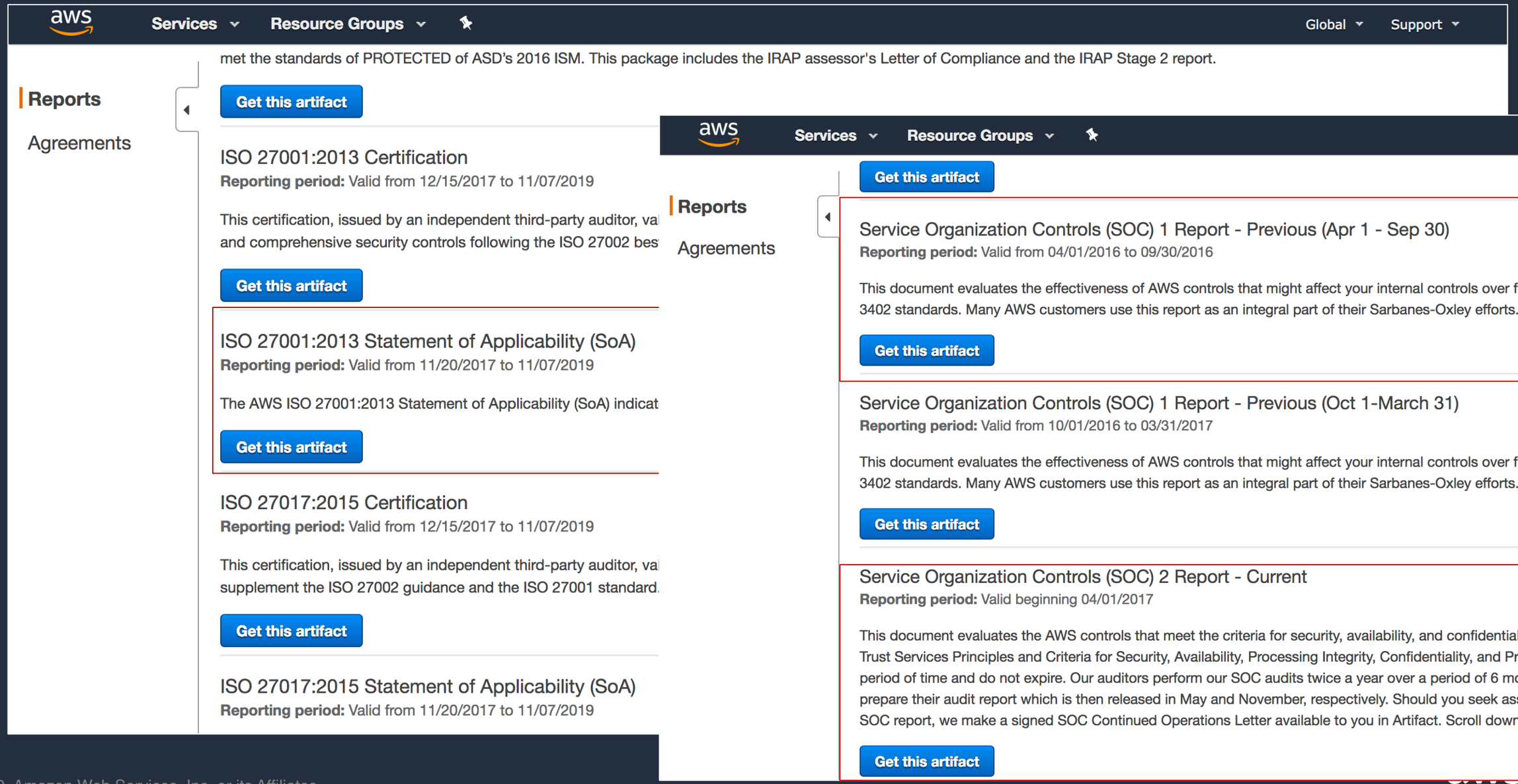
+2600

controles de segurança auditados anualmente

E muito mais em:

https://aws.amazon.com/compliance/

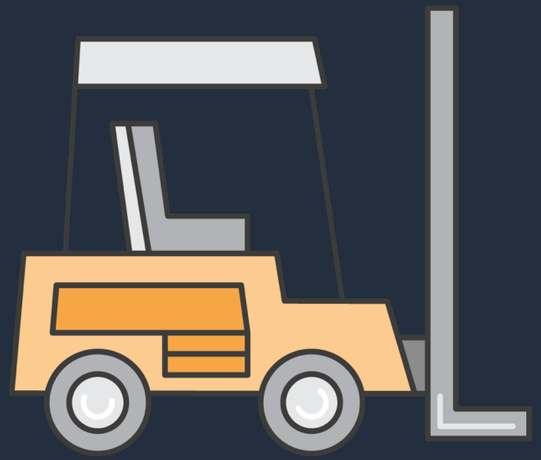
Relatórios de cumprimento regulatório - AWS Artifact



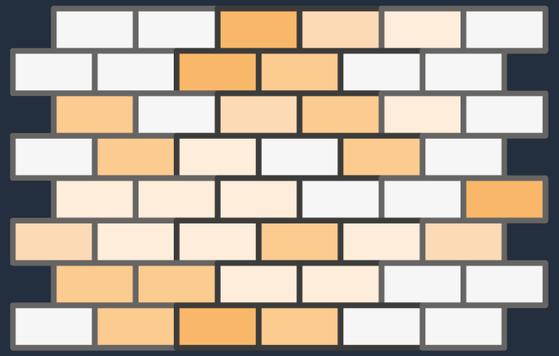
AWS e Cloud Security

Visível

Automatizada



Resiliente



A infra-estrutura global da AWS foi projetada para atender às exigências das empresas mais sensíveis do mundo em termos de segurança

aws

Serviços de Segurança Nativos na AWS

Gestão de Identidade e Acessos

AWS Identity & Access Management (IAM)

AWS Organizations

AWS Control Tower

AWS Cognito

AWS Directory Service

AWS Single Sign-On

AWS Secrets Manager

IAM Access Analyzer

Controles de Detecção

AWS CloudTrail

AWS Security Hub

AWS Config

Amazon CloudWatch

Amazon GuardDuty

VPC Flow Logs

Trusted Advisor

Segurança em Infraestrutura

AWS Systems Manager

AWS Shield

AWS Web Application Firewall (WAF)

Amazon Inspector

Amazon Virtual Private Cloud (VPC)

Image / AMI / Hardening

Bastion Host

Proteção de Dados

AWS Key Management Service (KMS)

AWS CloudHSM

Amazon Macie

AWS Certificate Manager

Server Side Encryption

S3 Block Public Access

Resposta a Incidentes

AWS Config Rules

AWS Lambda

Amazon Detective

Step Functions

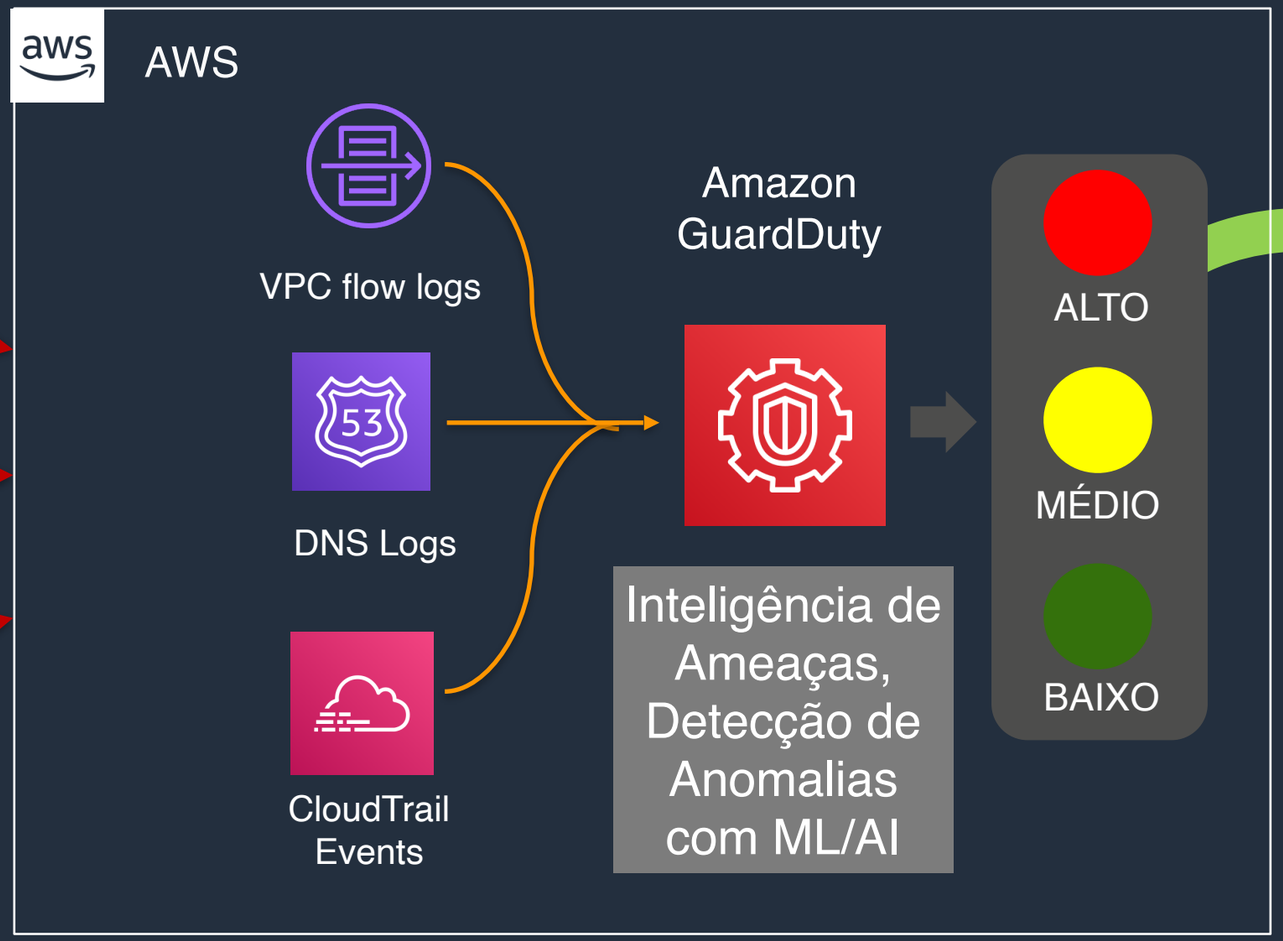
https://aws.amazon.com/pt/products/security/

aws

Detecção de Ameaças - AWS GuardDuty

Tipos de Detecção de Ameaças

- Reconhecimento
- Instância comprometida
- Conta Comprometida



Resposta a incidentes – Automação simplificada

GuardDuty → CloudWatch Events → Lambda

Amazon GuardDuty

Amazon CloudWatch

CloudWatch Event

AWS Lambda

Lambda Function

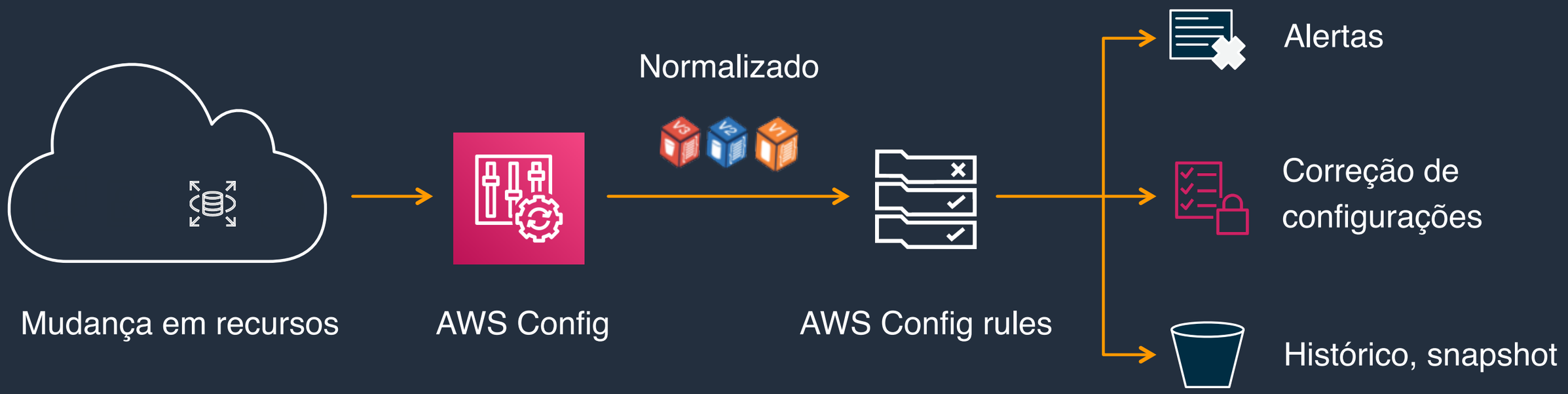
Detectar → **Reportar** → **Atuar**

Detecção de ameaças e anomalias → Ativa Lambda no evento GuardDuty TOR Cliente → Execução do Lambda que contém a ameaça alterando Security Groups

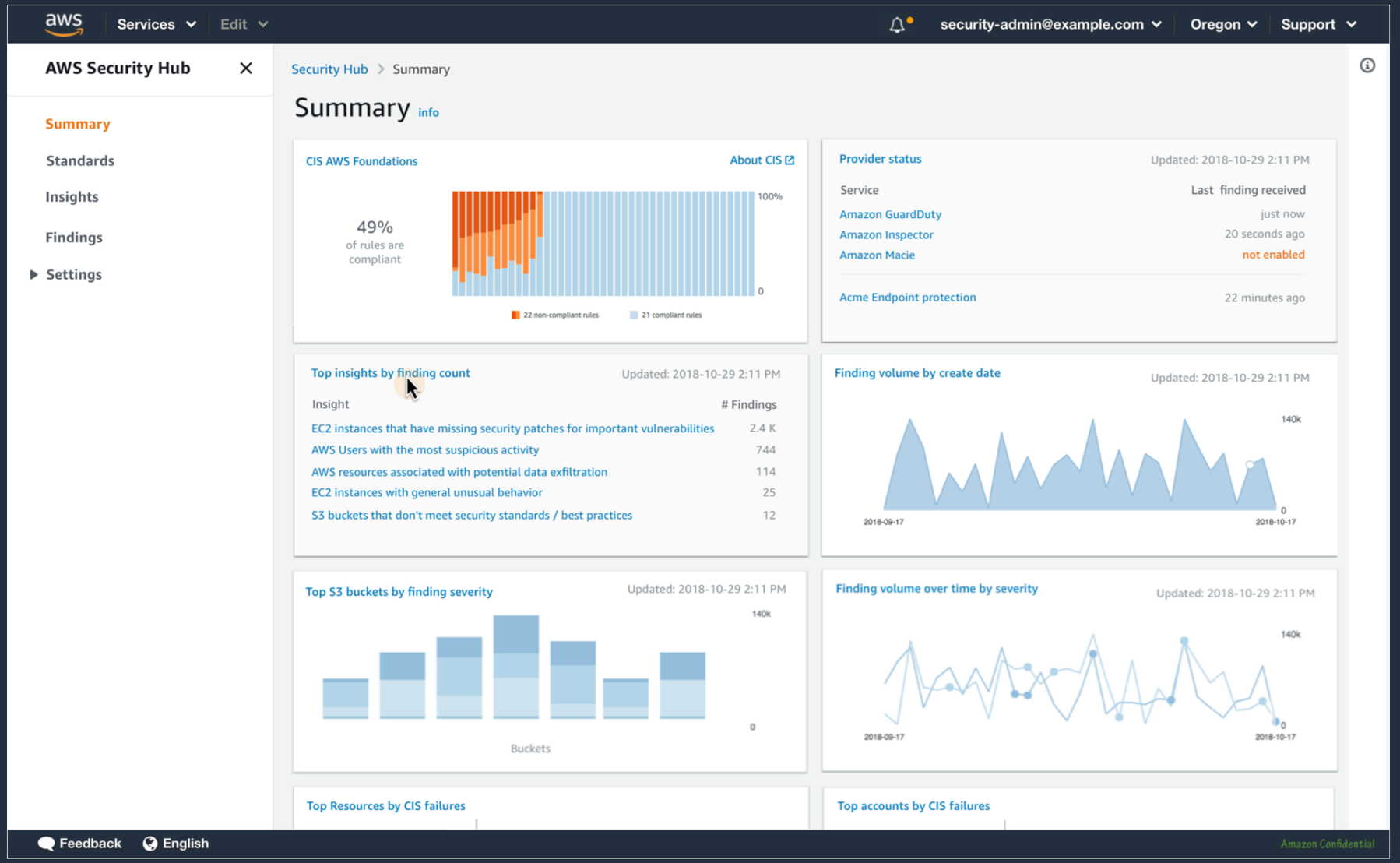
aws

Inventário de ativos - AWS Config

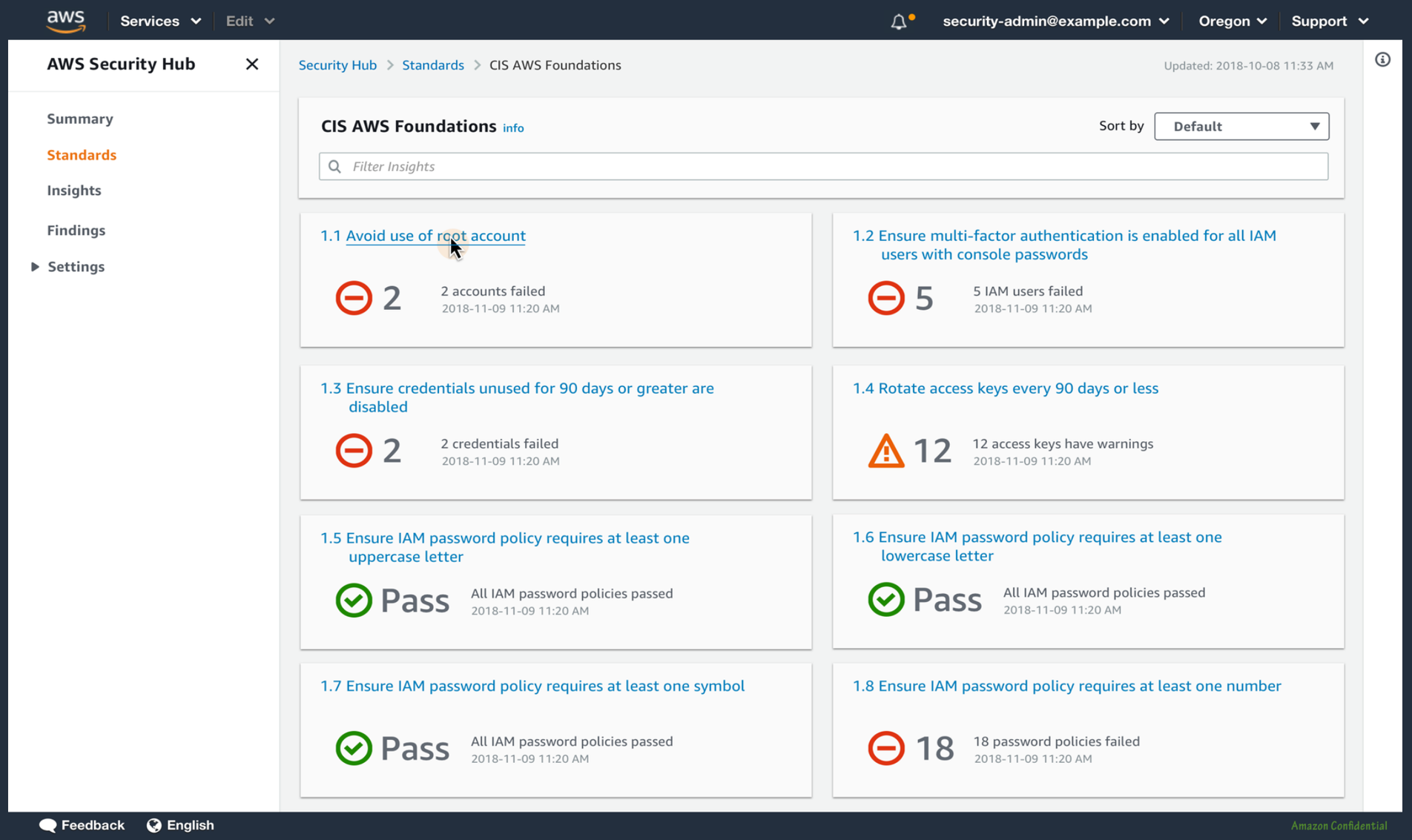
Inventário, monitoramento e notificação de mudanças de configuração



Segurança e Conformidade - AWS Security Hub



Segurança e Conformidade - AWS Security Hub



Na nuvem podemos alcançar melhores níveis de segurança, com menores custos operacionais

1. Modelo de Responsabilidade Compartilhada
2. Integração entre os serviços
3. Soluções AWS e de parceiros com pagamento por uso
4. Automação

Obrigado!