



Segurança e conformidade na AWS

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

Antes...

Ser ágil

ou

Estar seguro

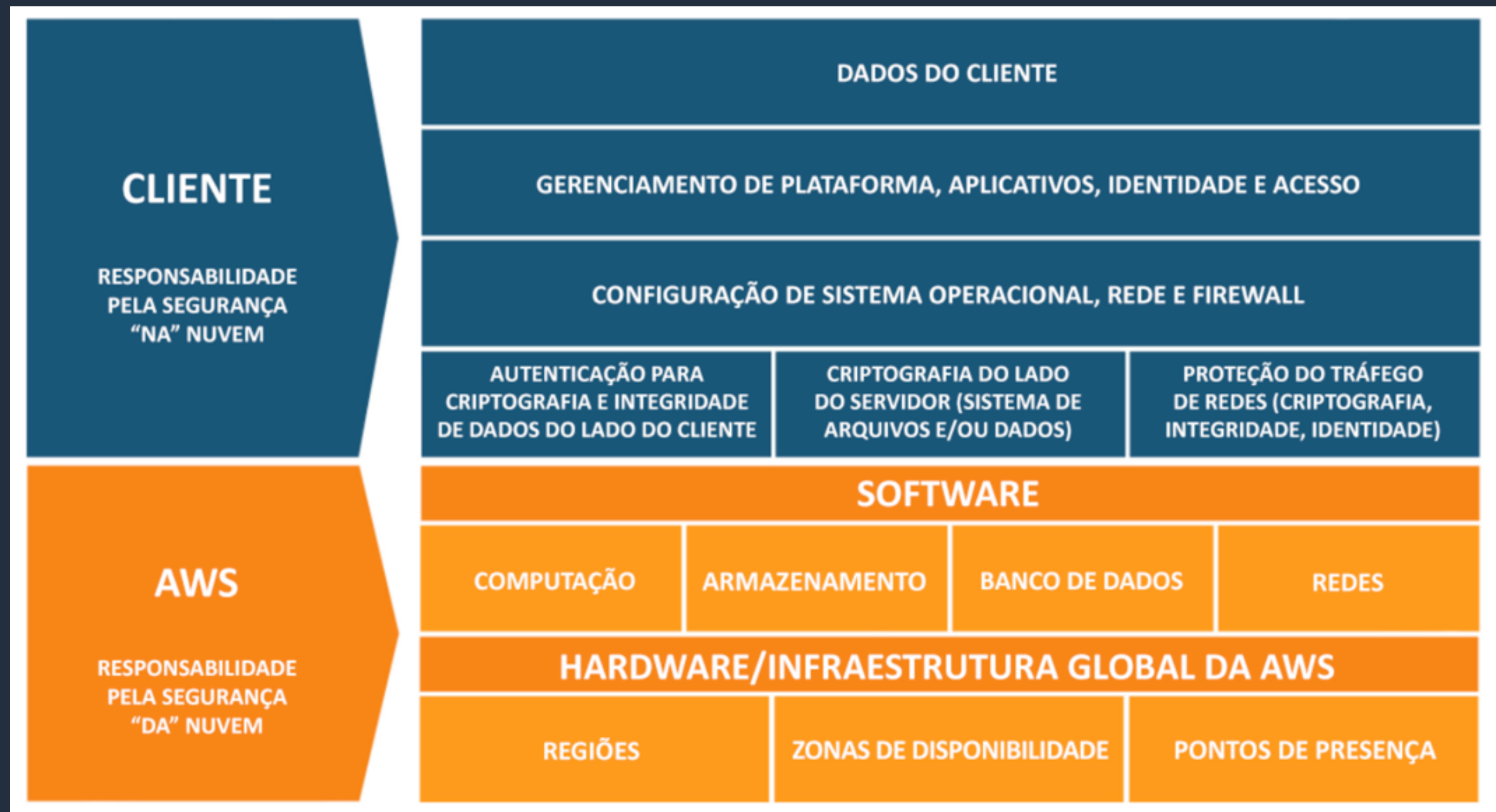
Agora...

Ser ágil



Estar seguro

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

Você

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

Você



Base de Dados no Amazon RDS / Aurora

Serviços em
Contêineres



Scaling

High availability

Database backups

DB s/w patches

DB s/w installs

OS patches

OS installation

Server maintenance

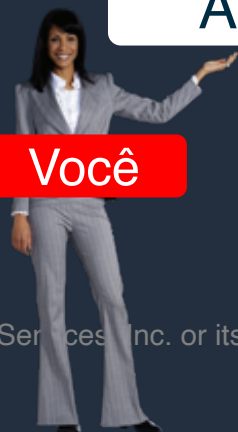
Rack & stack

Power, HVAC, net

Physical Security

App optimization

Você



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

Propriedade

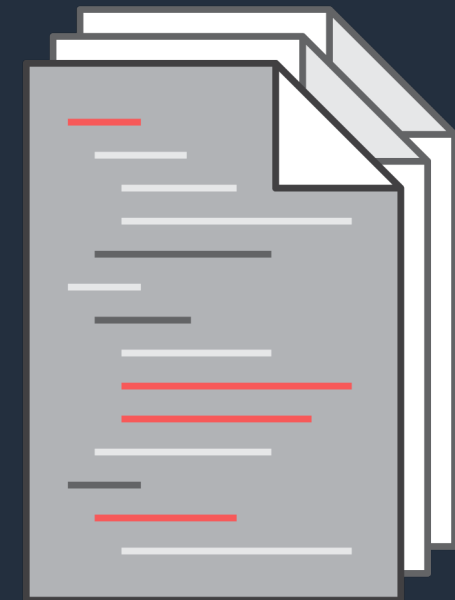


Acesso



Rastreabilidade

e



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

Criptografia de ponta a ponta: Em repouso

AWS Key Management Service (KMS) - CloudHSM



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

met the standards of PROTECTED of ASD's 2016 ISM. This package includes the IRAP assessor's Letter of Compliance and the IRAP Stage 2 report.

Get this artifact

ISO 27001:2013 Certification
Reporting period: Valid from 12/15/2017 to 11/07/2019

This certification, issued by an independent third-party auditor, validates and comprehensive security controls following the ISO 27002 best practices.

Get this artifact

ISO 27001:2013 Statement of Applicability (SoA)
Reporting period: Valid from 11/20/2017 to 11/07/2019

The AWS ISO 27001:2013 Statement of Applicability (SoA) indicates how the AWS services and resources are configured to meet the requirements of the ISO 27001 standard.

Get this artifact

ISO 27017:2015 Certification
Reporting period: Valid from 12/15/2017 to 11/07/2019

This certification, issued by an independent third-party auditor, validates and supplement the ISO 27002 guidance and the ISO 27001 standard.

Get this artifact

ISO 27017:2015 Statement of Applicability (SoA)
Reporting period: Valid from 11/20/2017 to 11/07/2019

Get this artifact

Service Organization Controls (SOC) 1 Report - Previous (Apr 1 - Sep 30)
Reporting period: Valid from 04/01/2016 to 09/30/2016

This document evaluates the effectiveness of AWS controls that might affect your internal controls over financial reporting (ICFR) and 3402 standards. Many AWS customers use this report as an integral part of their Sarbanes-Oxley efforts.

Get this artifact

Service Organization Controls (SOC) 1 Report - Previous (Oct 1-March 31)
Reporting period: Valid from 10/01/2016 to 03/31/2017

This document evaluates the effectiveness of AWS controls that might affect your internal controls over financial reporting (ICFR) and 3402 standards. Many AWS customers use this report as an integral part of their Sarbanes-Oxley efforts.

Get this artifact

Service Organization Controls (SOC) 2 Report - Current
Reporting period: Valid beginning 04/01/2017

This document evaluates the AWS controls that meet the criteria for security, availability, and confidentiality in the AWS Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy. This report is issued for a specific period of time and do not expire. Our auditors perform our SOC audits twice a year over a period of 6 months – October and May. We prepare their audit report which is then released in May and November, respectively. Should you seek assurance that your AWS services meet the SOC 2 criteria, we make a signed SOC report available to you in Artifact. Scroll down to the bottom of the report for more information.

Get this artifact

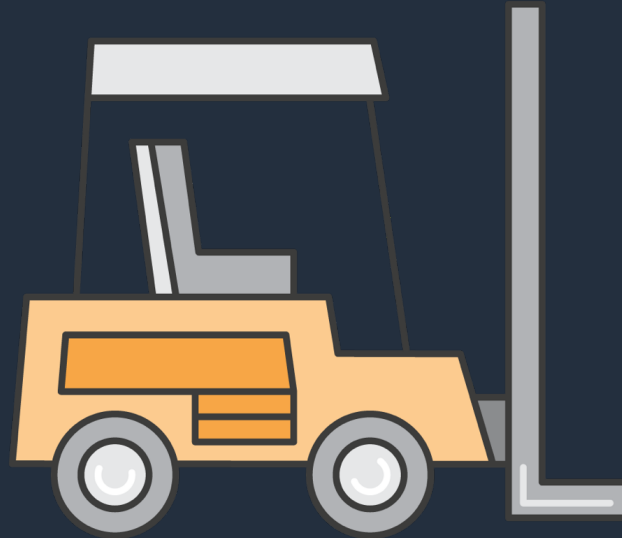


AWS e Cloud Security

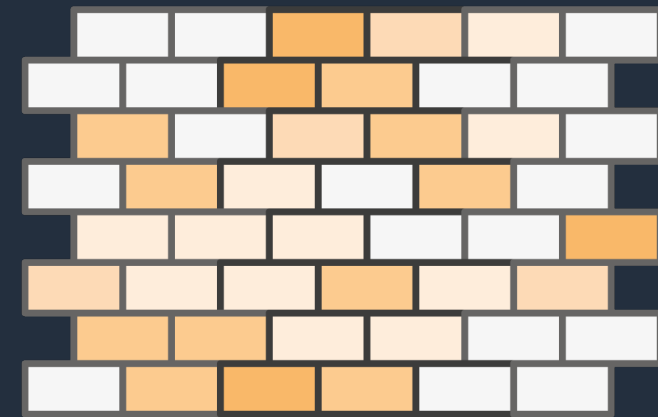
Visível



Automatizada

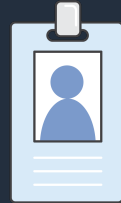


Resiliente



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

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

Detecção de Ameaças - AWS GuardDuty

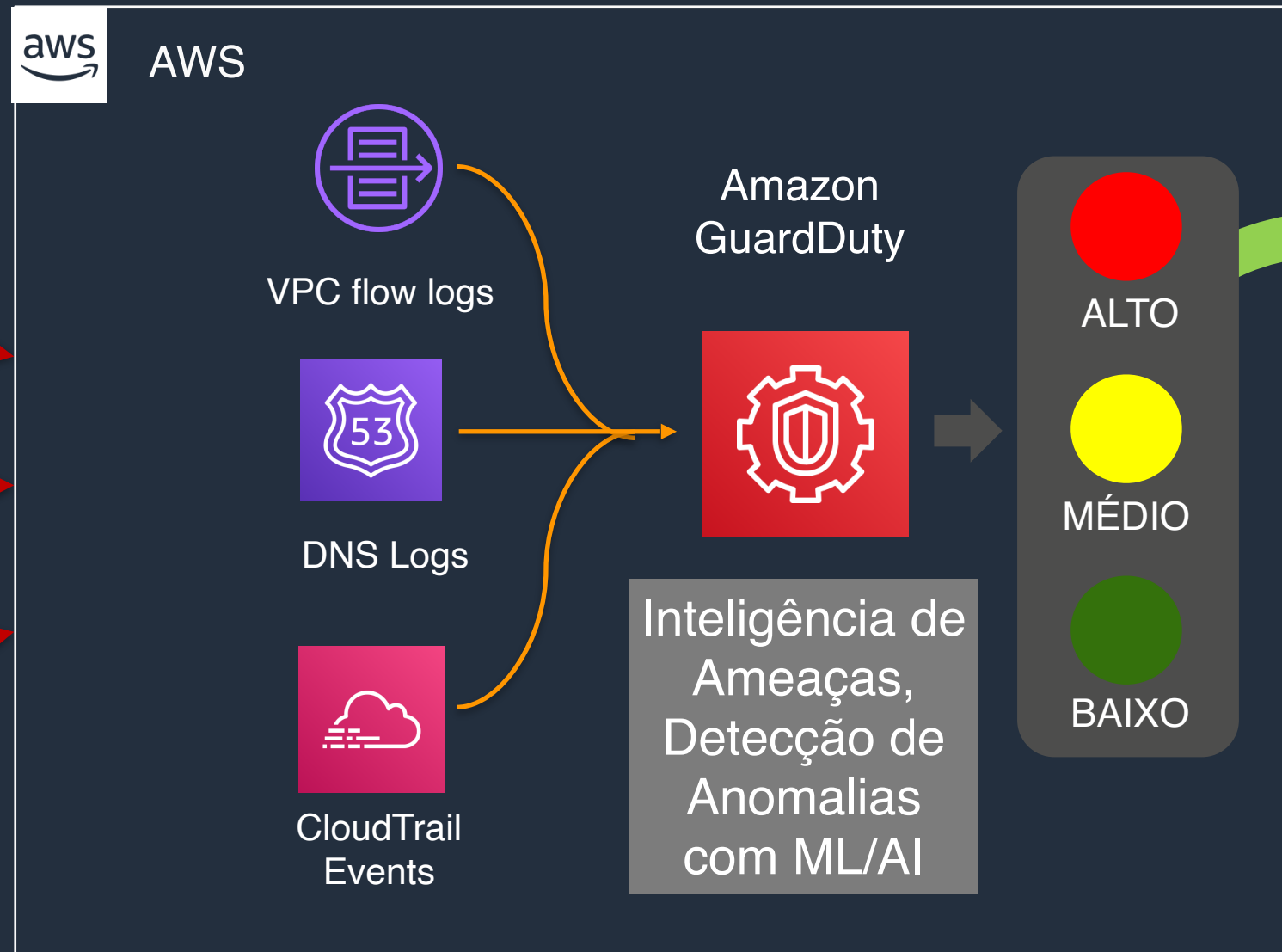
Tipos de Detecção de Ameaças

Reconhecimento

Instância comprometida

Conta Comprometida

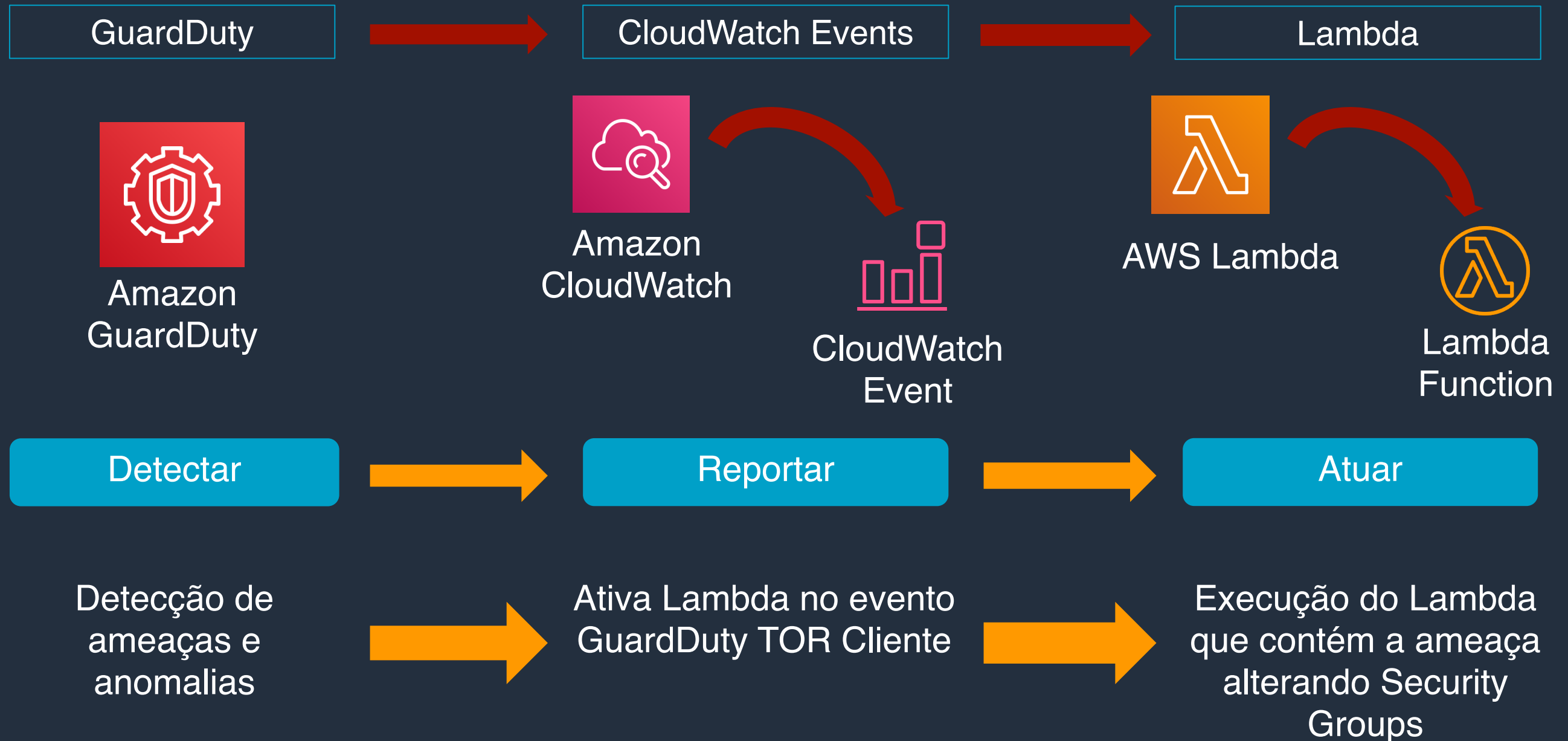
Fontes de dados



Descobertas

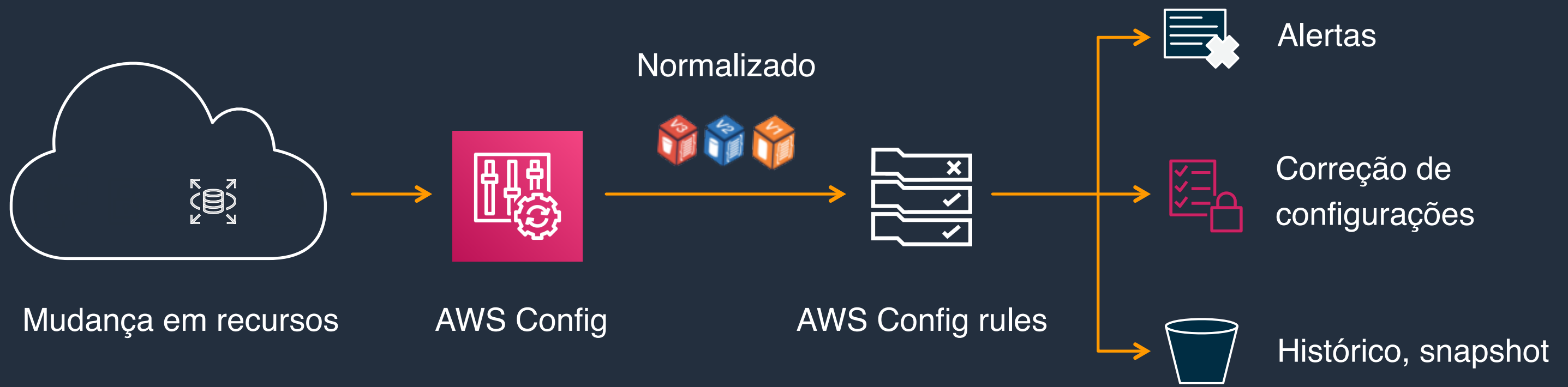
Resposta automática, e/ou Alertas no SIEM

Resposta a incidentes – Automação simplificada



Inventário de ativos - AWS Config

Inventário, monitoramento e notificação de mudanças de configuração



Segurança e Conformidade - AWS Security Hub

The screenshot displays the AWS Security Hub console interface. At the top, the navigation bar includes the AWS logo, 'Services', 'Edit', and user information for 'security-admin@example.com' in the 'Oregon' region. The main content area is titled 'Summary' and features a sidebar with navigation options: Summary, Standards, Insights, Findings, and Settings.

The central dashboard contains several key components:

- CIS AWS Foundations:** A bar chart showing that 49% of rules are compliant. It details 22 non-compliant rules (orange) and 21 compliant rules (blue).
- Provider status:** A table listing the status of various services:

Service	Last finding received
Amazon GuardDuty	just now
Amazon Inspector	20 seconds ago
Amazon Macie	not enabled
Acme Endpoint protection	22 minutes ago
- Top insights by finding count:** A table listing the most frequent findings:

Insight	# Findings
EC2 instances that have missing security patches for important vulnerabilities	2.4 K
AWS Users with the most suspicious activity	744
AWS resources associated with potential data exfiltration	114
EC2 instances with general unusual behavior	25
S3 buckets that don't meet security standards / best practices	12
- Finding volume by create date:** A line chart showing the volume of findings over time from 2018-09-17 to 2018-10-17, with a peak of 140k.
- Top S3 buckets by finding severity:** A stacked bar chart showing the severity of findings across different S3 buckets.
- Finding volume over time by severity:** A line chart showing the volume of findings over time, categorized by severity.

At the bottom of the console, there are links for 'Feedback' and 'English', and a footer indicating 'Amazon Confidential'.

Segurança e Conformidade - AWS Security Hub

aws Services Edit security-admin@example.com Oregon Support

AWS Security Hub Security Hub > Standards > CIS AWS Foundations Updated: 2018-10-08 11:33 AM

CIS AWS Foundations info Sort by Default

Filter Insights

- 1.1 Avoid use of root account**
2 accounts failed
2018-11-09 11:20 AM
- 1.2 Ensure multi-factor authentication is enabled for all IAM users with console passwords**
5 IAM users failed
2018-11-09 11:20 AM
- 1.3 Ensure credentials unused for 90 days or greater are disabled**
2 credentials failed
2018-11-09 11:20 AM
- 1.4 Rotate access keys every 90 days or less**
12 access keys have warnings
2018-11-09 11:20 AM
- 1.5 Ensure IAM password policy requires at least one uppercase letter**
Pass
All IAM password policies passed
2018-11-09 11:20 AM
- 1.6 Ensure IAM password policy requires at least one lowercase letter**
Pass
All IAM password policies passed
2018-11-09 11:20 AM
- 1.7 Ensure IAM password policy requires at least one symbol**
Pass
All IAM password policies passed
2018-11-09 11:20 AM
- 1.8 Ensure IAM password policy requires at least one number**
18 password policies failed
2018-11-09 11:20 AM

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!

