



Construyendo arquitecturas zero trust sobre entornos cloud

José Manuel Ortega Candel

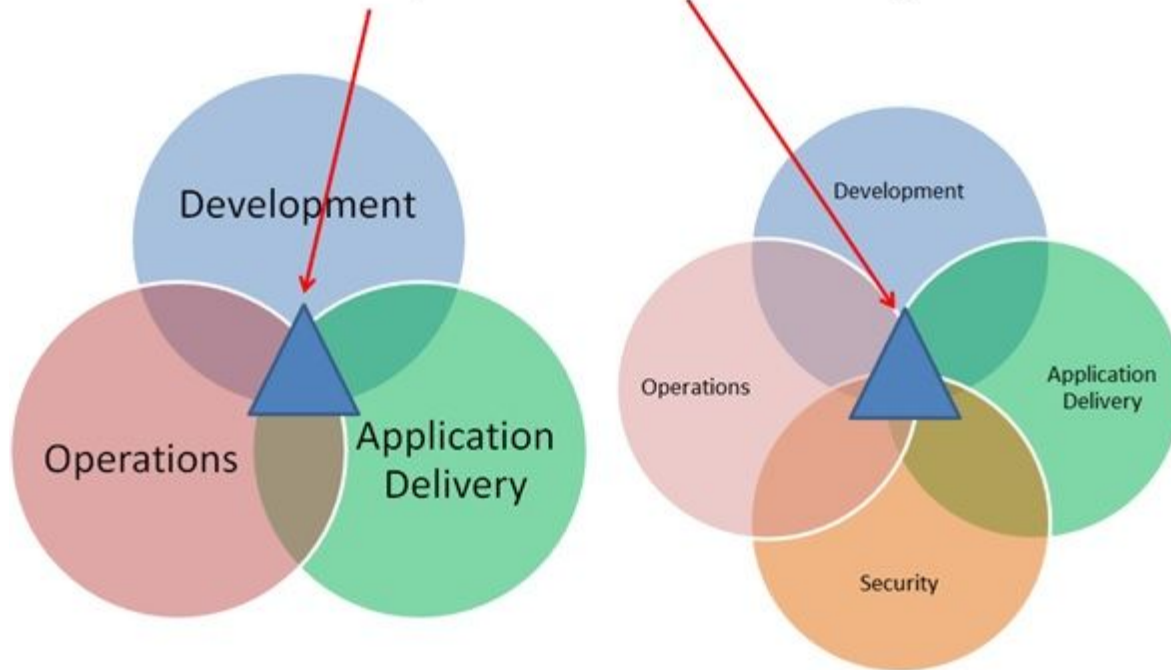
Agenda



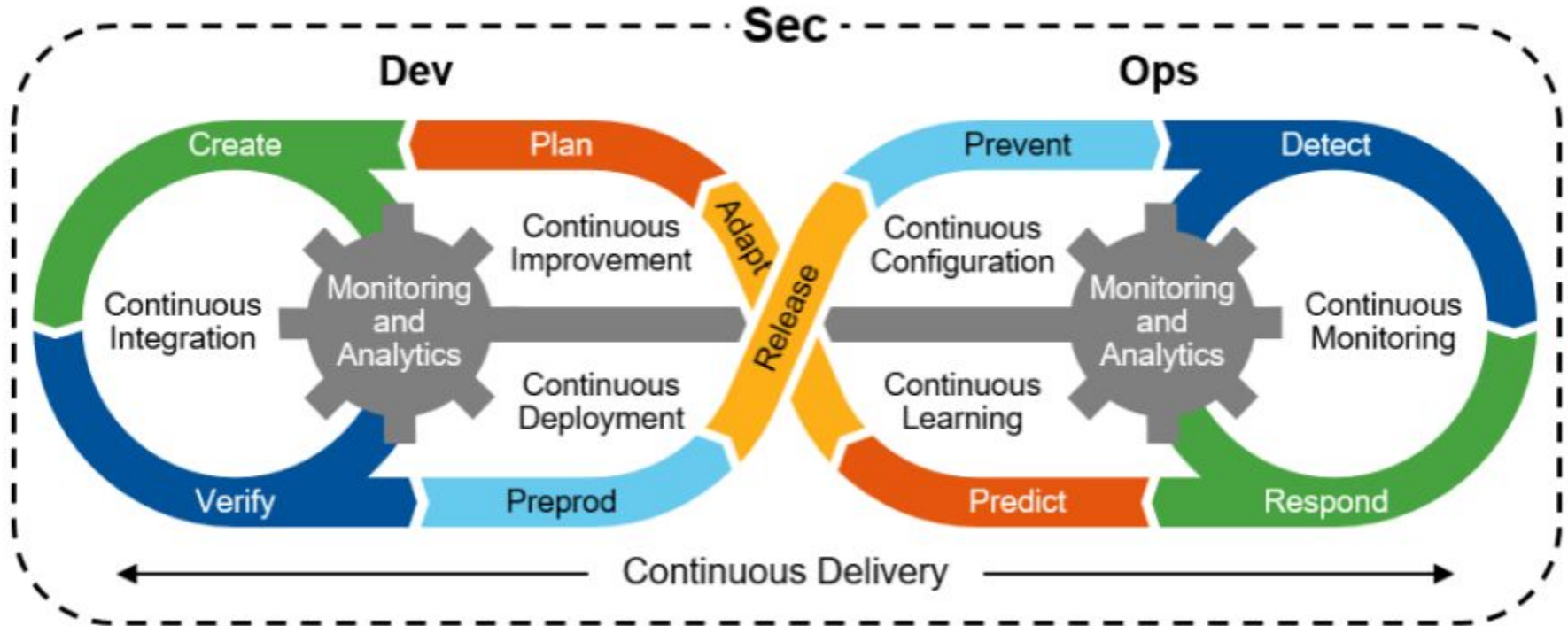
- **Introducción a DevSecOps y modelado de amenazas**
- **Modelo de confianza cero(zero trust) en la nube**
- **Mejoras prácticas a nivel de permisos y estrategias de seguridad al trabajar en entornos cloud**
- **Herramientas de análisis orientadas al pentesting en entornos cloud**

Introducción a DevSecOps

DevOps vs. DevSecOps



Introducción a DevSecOps



Introducción a DevSecOps



<https://www.cidersecurity.io/wp-content/uploads/2022/06/Top-10-CICD-Security-Risks-.pdf>

Top 10
CI/CD
Security
Risks

- CICD-SEC-1 Insufficient Flow Control Mechanisms
- CICD-SEC-2 Inadequate Identity and Access Management
- CICD-SEC-3 Dependency Chain Abuse
- CICD-SEC-4 Poisoned Pipeline Execution (PPE)
- CICD-SEC-5 Insufficient PBAC (Pipeline-Based Access Controls)
- CICD-SEC-6 Insufficient Credential Hygiene
- CICD-SEC-7 Insecure System Configuration
- CICD-SEC-8 Ungoverned Usage of 3rd Party Services
- CICD-SEC-9 Improper Artifact Integrity Validation
- CICD-SEC-10 Insufficient Logging and Visibility

A decorative graphic element in the bottom-left corner of the dark blue box. It consists of a teal-colored L-shaped line with a circular node at the corner, containing a white gear-like icon with a central dot.

Introducción a DevSecOps



- CICD-SEC-1: Insufficient Flow Control Mechanisms
- CICD-SEC-2: Inadequate Identity and Access Management
- CICD-SEC-3: Dependency Chain Abuse
- CICD-SEC-4: Poisoned Pipeline Execution (PPE)
- CICD-SEC-5: Insufficient PBAC (Pipeline-Based Access Controls)
- CICD-SEC-6: Insufficient Credential Hygiene
- CICD-SEC-7: Insecure System Configuration
- CICD-SEC-8: Ungoverned Usage of 3rd Party Services
- CICD-SEC-9: Improper Artifact Integrity Validation
- CICD-SEC-10: Insufficient Logging and Visibility

Modelado de amenazas



Modelado de amenazas



- El beneficio inmediato y más importante de implementar el modelado de amenazas es identificar las amenazas que pueden aparecer a lo largo del proceso de diseño para que se puedan implementar las contramedidas adecuadas.

Modelo de confianza cero en la nube



Behavioral Biometrics

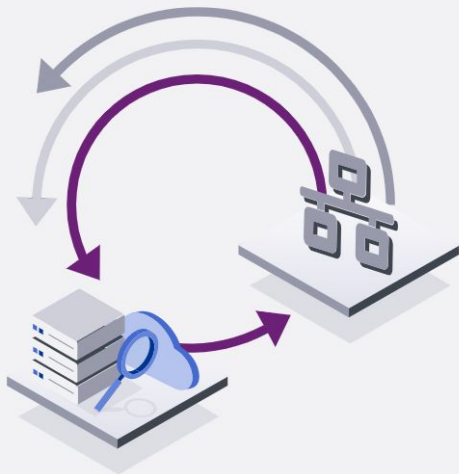


- User Behavior
- Velocity
- Geolocation



- Device Fingerprint
- Device Reputation

Adaptive Risk Engine



Risk-based
Adaptive



Access Control



Authorization

Apps



SaaS



On-Prem

Network



PAM

Infrastructure



Website



Platform

Data



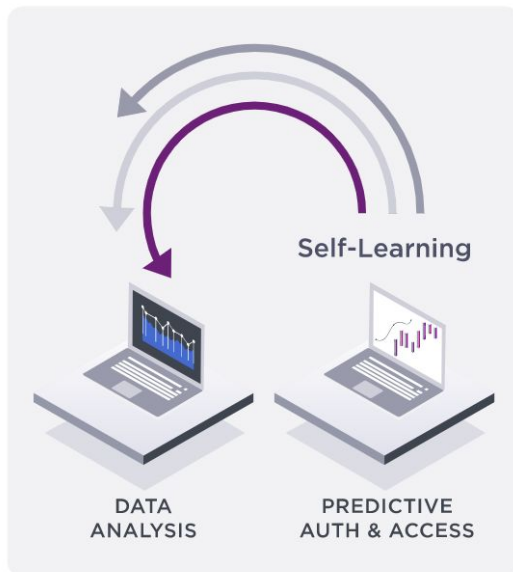
Modelo de confianza cero en la nube



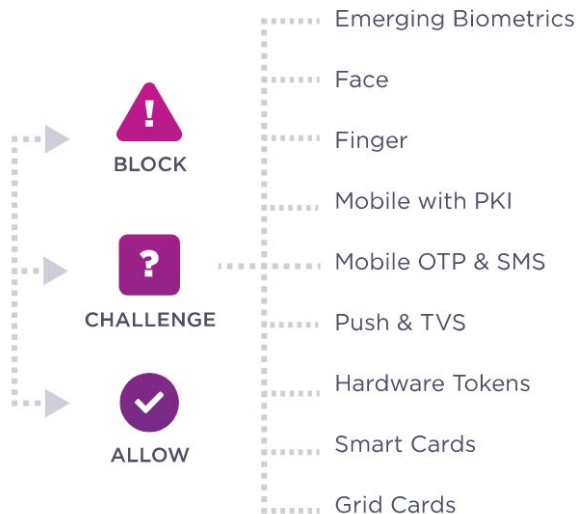
DATA AND CONTEXT (USERS, DEVICES AND THINGS)

- Emerging Contextual Elements
- Advanced Device Reputation
- User Behavior
- HTTP Traffic Analysis
- Geolocation
- Device Fingerprint
- Velocity

INSIGHT AND POLICY ENGINE



INTELLIGENT AUTHENTICATION



Modelo de confianza cero en la nube



- Zero Trust es un paradigma de ciberseguridad centrado en la protección de los recursos y la premisa de que la confianza nunca se otorga implícitamente, sino que debe evaluarse continuamente.
- El enfoque inicial debería estar en restringir los recursos para aquellos que necesitan acceder y otorgar sólo los privilegios mínimos necesarios para cumplir sus objetivos.

Modelo de confianza cero en la nube



- **Desarrollo de aplicaciones**
- **Aprovisionamiento de infraestructura**
- **Conectividad de servicios**
- **Autenticación de personas**

Modelo de confianza cero en la nube



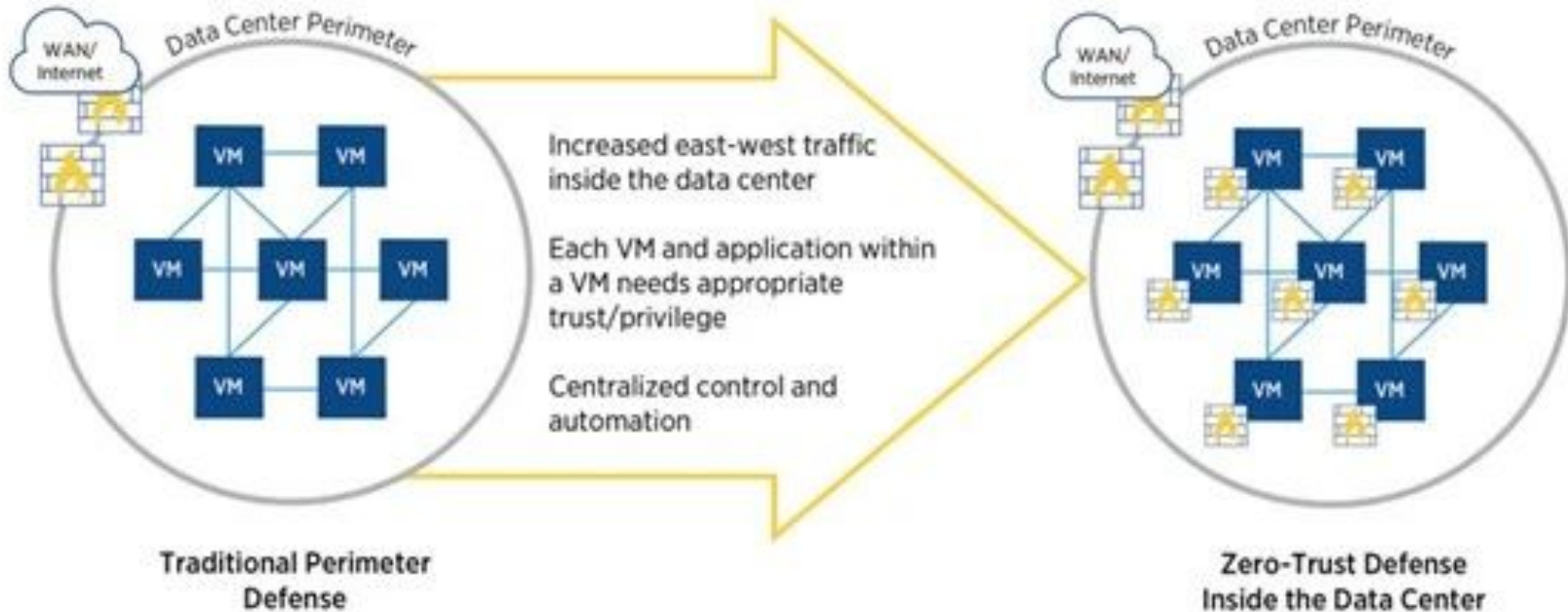
- **¿Qué están intentando proteger?**
- **¿De quién intentan protegerlo?**

Modelo de confianza cero en la nube



- **Uso de arquitecturas proxy**
- **Proteger los datos mediante políticas granulares basadas en el contexto**
- **Reducir el riesgo eliminando la superficie de ataque**
- **Acciones de defensa y protección**

Modelo de confianza cero en la nube



Modelo de confianza cero en la nube



- **Todas las entidades de una red suponen una amenaza**
- **Acceso a los recursos basado en autenticar y autorizar tanto el usuario como al host que va a acceder**

Modelo de confianza cero en la nube

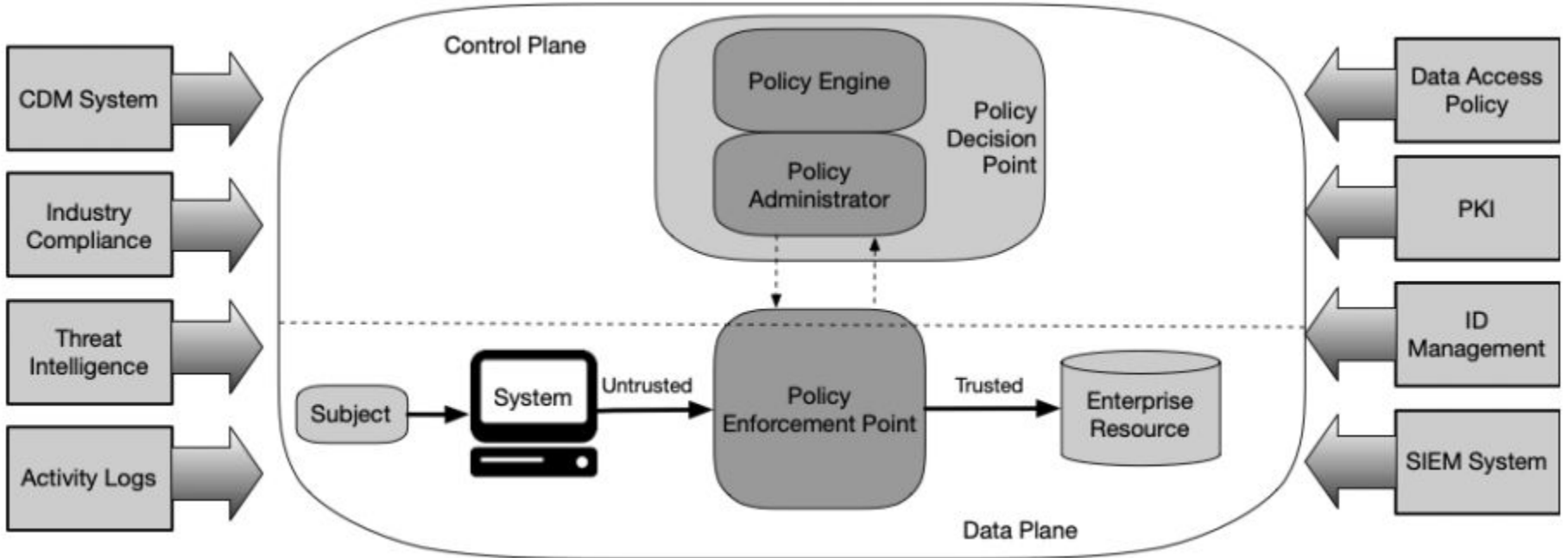


- **Ninguna parte de la red es confiable.** Debemos actuar como si el atacante estuviese siempre presente.
- **Nunca confiar en la conexión a la red.** Cualquier conexión que se establezca es insegura.
- **Verificar explícitamente.** Siempre hay que verificar, nunca confiar.
- **Privilegios mínimos.** Restringir los recursos para aquellos únicamente que necesitan acceder.
- **Microsegmentación.** Aplicar políticas dinámicas basadas en información de contexto.
- **Visibilidad.** Es importante inspeccionar y evaluar continuamente los riesgos.

Arquitecturas zero trust



Arquitecturas zero trust



Arquitecturas zero trust

NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-207>



Table of Contents

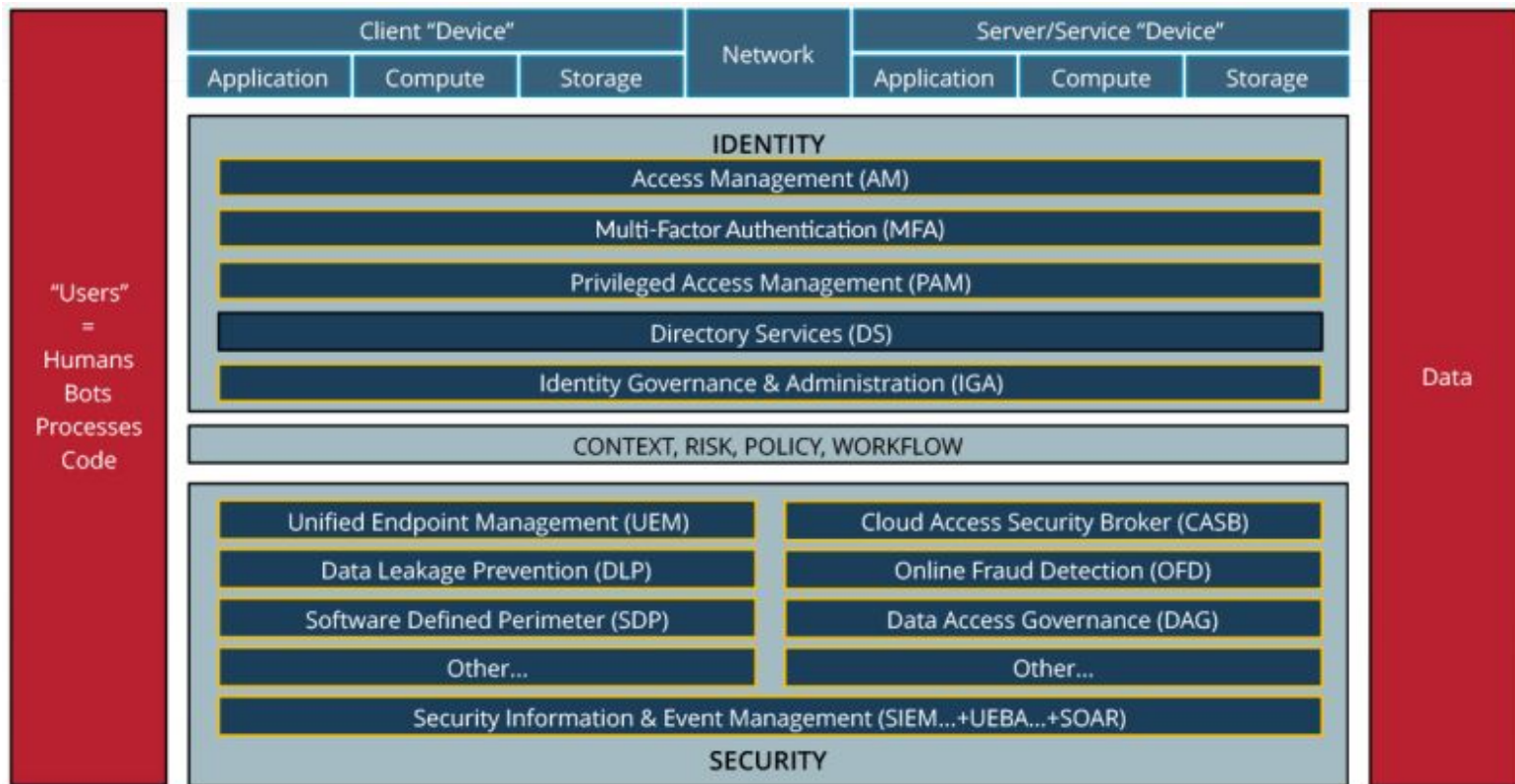
1	Introduction	1
1.1	History of Zero Trust Efforts Related to Federal Agencies	2
1.2	Structure of This Document	2
2	Zero Trust Basics	4
2.1	Tenets of Zero Trust	6
2.2	A Zero Trust View of a Network	8
3	Logical Components of Zero Trust Architecture	9
3.1	Variations of Zero Trust Architecture Approaches	11
3.1.1	ZTA Using Enhanced Identity Governance	11
3.1.2	ZTA Using Micro-Segmentation	12
3.1.3	ZTA Using Network Infrastructure and Software Defined Perimeters	12
3.2	Deployed Variations of the Abstract Architecture	13
3.2.1	Device Agent/Gateway-Based Deployment	13
3.2.2	Enclave-Based Deployment	14
3.2.3	Resource Portal-Based Deployment	15
3.2.4	Device Application Sandboxing	16
3.3	Trust Algorithm	17
3.3.1	Trust Algorithm Variations	19
3.4	Network/Environment Components	21

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>

Arquitecturas zero trust



IDENTITY DEFINED
SECURITY ALLIANCE



Arquitecturas zero trust



Fuente: Microsoft



IDENTITY DEFINED
SECURITY ALLIANCE

Uso de soluciones de IAM

- Normalización de las identidades en la organización
- Funcionalidades que garantizan unas políticas de contraseñas apropiadas
- Ágil aprovisionamiento de usuarios
- Privileged Session Management(PSM)
- Monitorizar en tiempo real las sesiones de los usuarios
- Si cualquier credencial se ve comprometida, se puede gestionar la revocación de secretos o sesiones

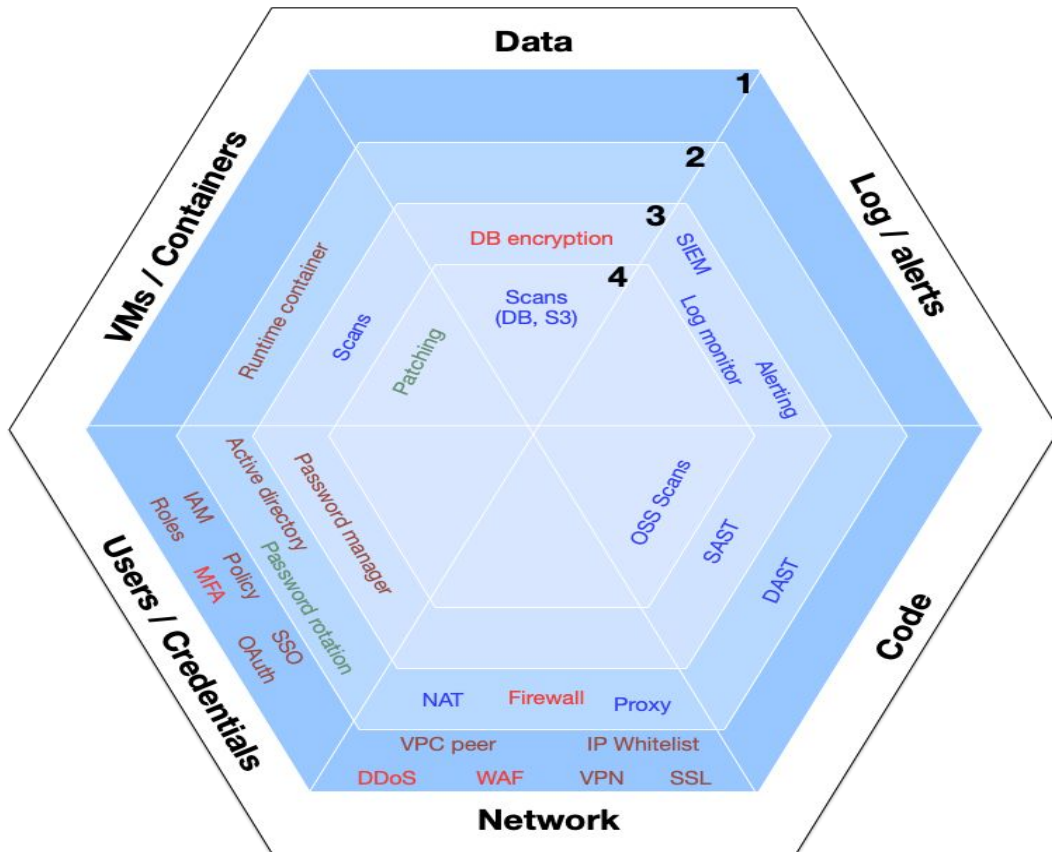


Uso de soluciones de IAM



- **Gobernanza de identidades:** gestiona el ciclo de vida de la cuenta de usuario, incluidos los derechos y su concesión.
- **Gestión de acceso:** controla las políticas de acceso unificado a menudo con la activación de la conexión única (SSO) y la autenticación multifactor (MFA).
- **Servicios de directorio:** gestión y sincronización de credenciales centralizadas y consolidadas.
- **Aprovisionamiento de usuarios:** automatiza la creación y la asignación de nuevas cuentas de usuario.
- **Análisis de identidades:** detecta y evita actividades de identidad sospechosas mediante el aprendizaje automático.
- **Conexión única (SSO):** consolida la contraseña de usuario y las credenciales de una única cuenta con una activación de contraseña segura para simplificar el acceso a los servicios.
- **Autenticación multifactor (MFA):** incrementa la autenticación con controles secundarios para garantizar la autenticidad de los usuarios y reducir la exposición a credenciales robadas.
- **Autenticación basada en riesgos:** utiliza algoritmos para calcular los riesgos de las acciones de los usuarios. Bloquea y denuncia actividades calificadas de alto riesgo.
- **Administración y gobernanza de identidades (IGA):** reduce el riesgo asociado a un acceso y privilegios excesivos mediante el control de derechos.

Estrategias de seguridad entornos cloud



Diaagnostic

Corrective

Defense

Prevent

Herramientas de análisis

<https://cloudcustodian.io>



Cloud
Custodian.



```
policies:
- name: my-aws-instances
  resource: aws.ec2
  filters:
    - type: value
      key: "tag:owner"
      value: "sam"
```

```
import boto3

client = boto3.client('ec2')

custom_filter = [{
  'Name': 'tag:owner',
  'Values': ['sam']}]

response =
client.describe_instances(Filters=custom_
filter)
```



```
policies:
- name: my-azure-instances
  resource: azure.vm
  filters:
    - type: value
      key: "tag:owner"
      value: "sam"
```

```
from azure.mgmt.compute import
ComputeManagementClient

compute_client =
ComputeManagementClient(credential,
Subscription_Id)

vm_list =
compute_client.virtual_machines.list_all(
)

response = [vm for vm in vm_list if
vm.tags.get('owner', '') == 'sam' ]
```



```
policies:
- name: my-gcp-instances
  resource: gcp.instance
  filters:
    - type: value
      key: "labels.owner"
      value: "sam"
```

```
import googleapiclient.discovery

service =
googleapiclient.discovery.build("comput
e", "v1")

response =
service.instances().list(project=projec
t, zone=zone,
filter='labels.owner=sam')
```



```
policies:
- name: my-k8s-deployments
  resource: k8s.deployment
  filters:
    - type: value
      key: "spec.metadata.labels.owner"
      value: "sam"
```

```
import yaml
import jmespath

with open('manifest.yaml', 'r') as m:
  yaml_manifest = yaml.safe_load(m)

expression =
jmespath.compile('metadata.labels.owner')
response = expression.search(yaml_manifest)

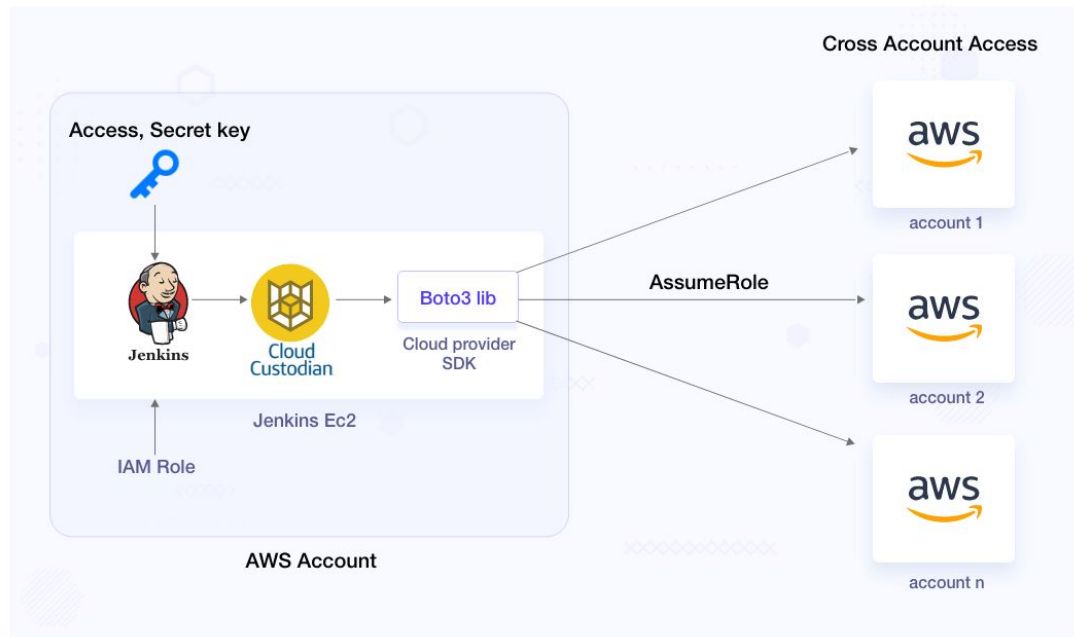
if response == 'sam':
  print("You nailed it!")
```

Herramientas de análisis

<https://cloudcustodian.io>



Cloud Custodian



AWS CloudWatch



AWS Lambda

Herramientas de análisis

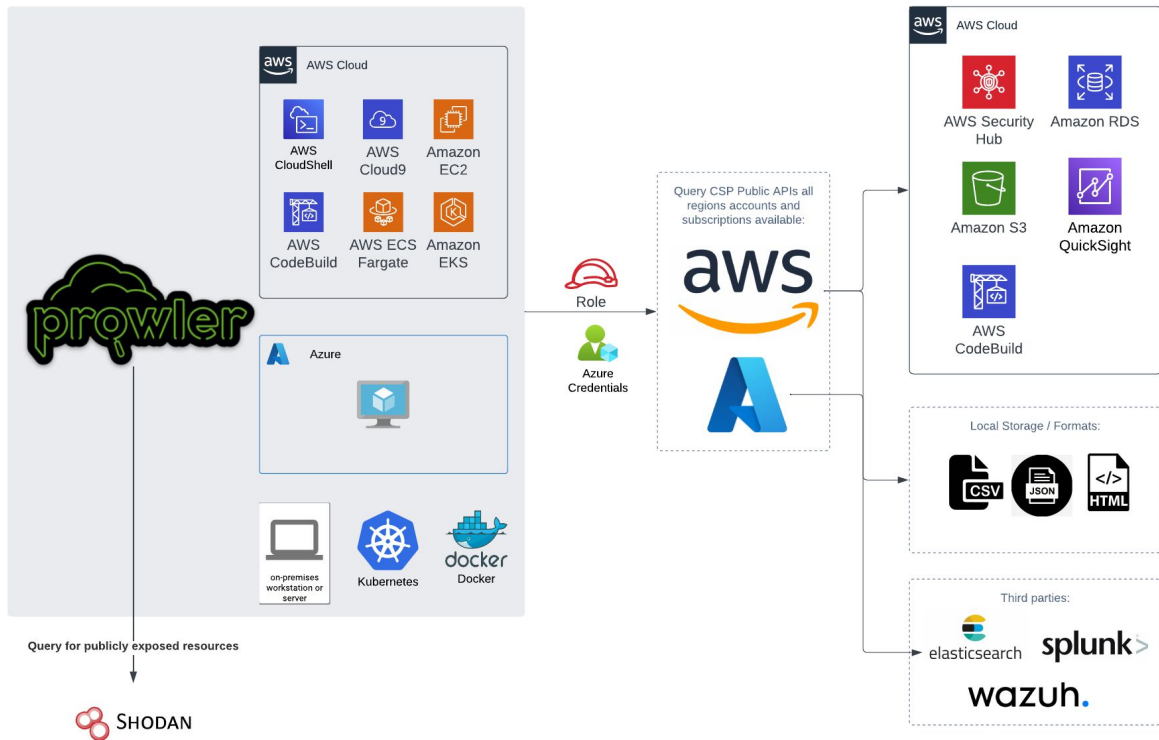


<https://github.com/prowler-cloud/prowler>

- Prowler es una herramienta de seguridad de código abierto para realizar evaluaciones de las mejores prácticas de seguridad de AWS y Azure
- Permite realizar auditorías, respuesta a incidentes, monitorización continua, hardening y gestionar la revocación de secretos.



Herramientas de análisis



Herramientas de análisis



```
aws configure
```

```
export AWS_ACCESS_KEY_ID="ASXXXXXXXX"  
export AWS_SECRET_ACCESS_KEY="XXXXXXXXXX"  
export AWS_SESSION_TOKEN="XXXXXXXXXX"
```

```
arn:aws:iam::aws:policy/SecurityAudit
```

```
arn:aws:iam::aws:policy/job-function/ViewOnlyAccess
```



Herramientas de análisis



Report Information

Version: 3.0.0

Parameters used: aws -p dev -s iam --log-level ERROR

Date: 2022-12-19T17:16:38.009578

AWS Assessment Summary

AWS Account: 10

AWS-CLI Profile: dev

Audited Regions: All Regions

AWS Credentials

User Id: AR0ARRZCC64WAISUBZ7Y

Caller Identity ARN: arn:aws:sts::100000000000:assumed-role/iam_administrative/8e6ebbad-e66d-41e8-bedd-2573649514c3

Assessment Overview

Total Findings: 74

Passed: 71

Failed: 3

Total Resources: 24

Filters Show 100 entries Search:

Status	Severity	Service Name	Region	Check Title	Resource ID	Check Description	Check ID	Status Extended	Risk	Recommendation	Recommendation URL
PASS	high	iam	us-east-1	Avoid the use of the root accounts	<root_account>	Avoid the use of the root account	iam_avoid_root_usage	Root user in the account wasn't accessed in the last 1 days.	The root account has unrestricted access to all AWS services. read more...	Follow the remediation instructions. read more...	read more...
PASS	critical	iam	us-east-1	Ensure no root account access key exists	<root_account>	Ensure no root account access key exists	iam_no_root_access_key	User <root_account> has no access keys.	The root account is the most p read more...	Use the credential report to read more...	read more...
FAIL	critical	iam	us-east-1	Ensure MFA is enabled for the root account	<root_account>	Ensure MFA is enabled for the root account	iam_root_mfa_enabled	MFA is not enabled for root account.	The root account is the most p read more...	Using IAM console navigate to read more...	read more...
PASS	medium	iam	us-east-1	Ensure access keys are rotated every 90 days or less	<root_account>	Ensure access keys are rotated every 90 days or less	iam_rotate_access_key_90_days	User <root_account> has no access keys.	Access keys consist of an acce read more...	Use the credential report to read more...	read more...
PASS	high	iam	us-east-1	Ensure multi-factor authentication (MFA) is enabled for all IAM users who have a console password.	<root_account>	Ensure multi-factor authentication (MFA) is enabled for all IAM users	iam_user_mfa_enabled	User <root_account> has not Console Password enabled.	Unauthorized access to this cr read more...	Enable MFA for users account. read more...	read more...
PASS	medium	iam	us-east-1	Do not setup access keys during setup for all IAM users that have password	<root_account>	Do not setup access keys during setup for all IAM users that have password	iam_no_root_access_key	User <root_account> has no access keys.	Access keys consist of an access key ID and secret. read more...	Avoid using long lived access keys. read more...	read more...
PASS	medium	iam	us-east-1	Check if IAM users have two active access keys	<root_account>	Check if IAM users have two active access keys	iam_check_saml_providers_sts	There are 2 active access keys for user <root_account>.	Access keys could be lost or stolen. It creates a cri read more...	Create an IAM role for managing incidents with AW read more...	read more...
PASS	critical	iam	us-east-1	Ensure that no custom IAM pol which allow permissive role ass (e.g. sts:AssumeRole on *)	<root_account>	Ensure that no custom IAM pol which allow permissive role ass (e.g. sts:AssumeRole on *)	iam_no_custom_policy_permissive_role_assumption	There are 1 custom policies for user <root_account>.	AWS console defaults the checkboxes for creating a read more...	Enable MFA for users account. MFA is a simple be read more...	read more...
PASS	high	iam	us-east-1	Ensure no Customer Managed allow actions that may lead into Escalation	<root_account>	Ensure no Customer Managed allow actions that may lead into Escalation	iam_no_customer_managed_policy_permissions	There are 1 customer managed policies for user <root_account>.	AWS provides a support center that can be used fo read more...	Enable SAML_provider and use temporary creden read more...	read more...
PASS	medium	iam	us-east-1	Ensure IAM policies that allow administrative privileges are not created	<root_account>	Ensure IAM policies that allow administrative privileges are not created	iam_no_administrative_privileges	There are 1 administrative policies for user <root_account>.	Administrative policies are the most p read more...	Administrative policies are the most p read more...	read more...



Principales servicios de seguridad en AWS



AWS WAF

Protect your web applications from common web exploits



AWS Shield

Managed DDoS protection



Amazon GuardDuty

A threat detection service that continuously monitors for compromised accounts, anomalous behavior, and malware



AWS Secrets Manager

Store credentials, API keys, tokens, and other secrets securely



AWS KMS

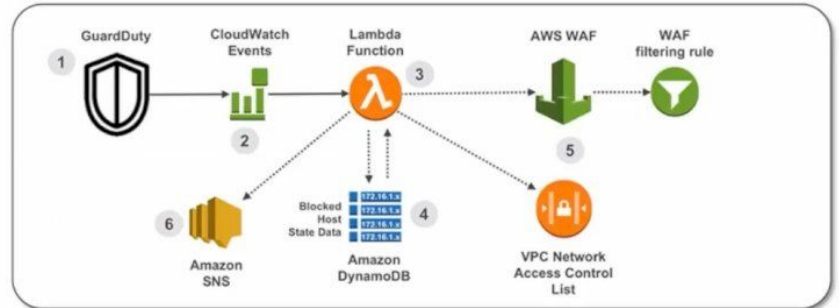
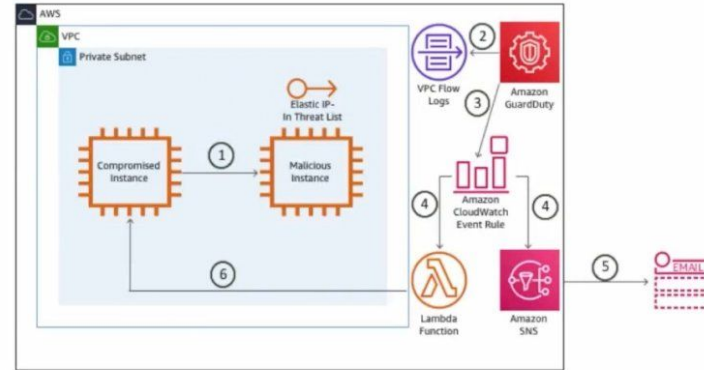
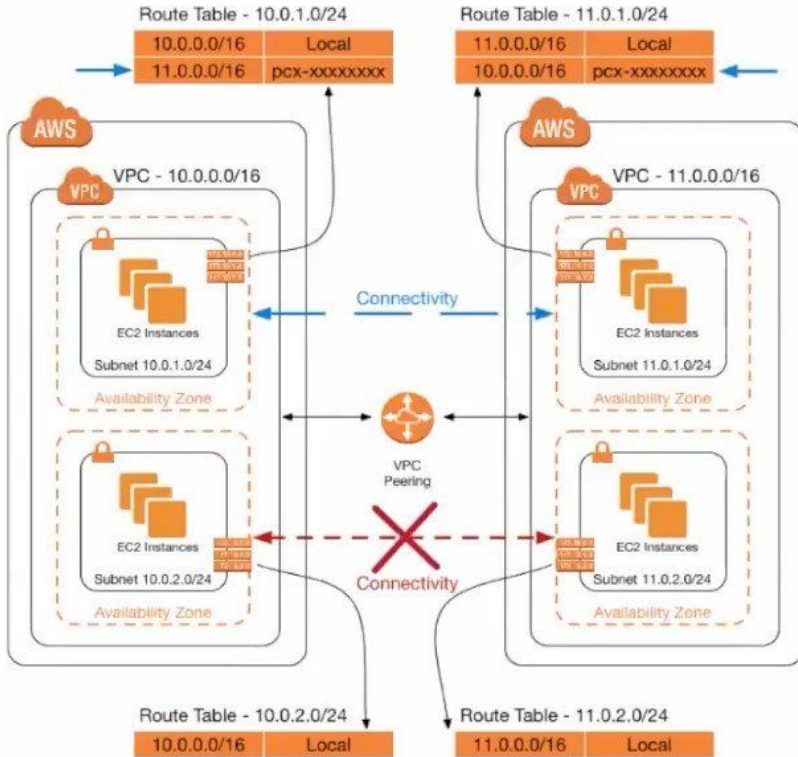
Create and control the cryptographic keys that protect your data



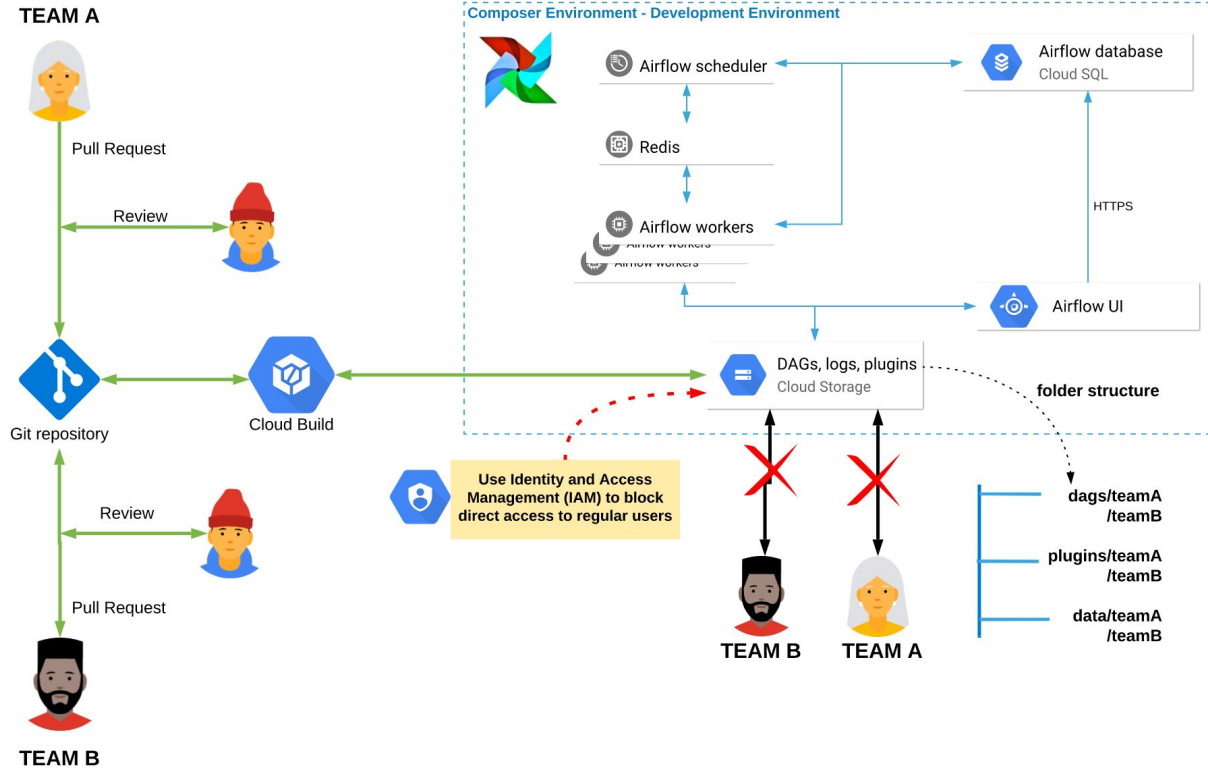
Amazon Inspector

An automated security vulnerability management service that continually evaluates your resources for software vulnerabilities and unintended network exposure

Principales servicios de seguridad en AWS



Mejores prácticas de seguridad



Mejores prácticas de seguridad



- **Funciones y permisos de IAM**
- **Funciones y permisos específicos de Cloud Compose**
- **Uso compartido restringido al dominio (DRS)**



Conclusiones



- **Estrategia de empresa a largo plazo**
- **Gestión centralizada de la seguridad**
- **Solución centrada en la identidad del usuario**

Conclusiones



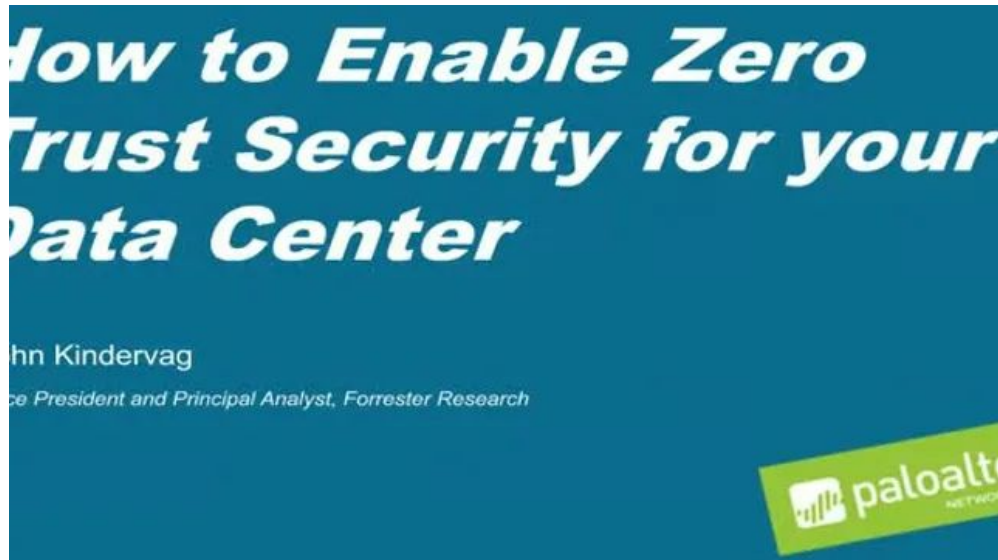
- Zero Trust Container Security
- <https://more.suse.com/zero-trust-security-for-dummies.html>



Conclusiones



- How to Enable Zero Trust Security for Your Data Center
- <https://www.brighttalk.com/webcast/10903/235239>



¡Gracias!

¿Preguntas?

@jmortegac

<https://www.linkedin.com/in/jmortega1>

<https://jmortega.github.io>

