SG VIRTUAL CONFERENCE

Construyendo arquitecturas zero trust sobre entornos cloud

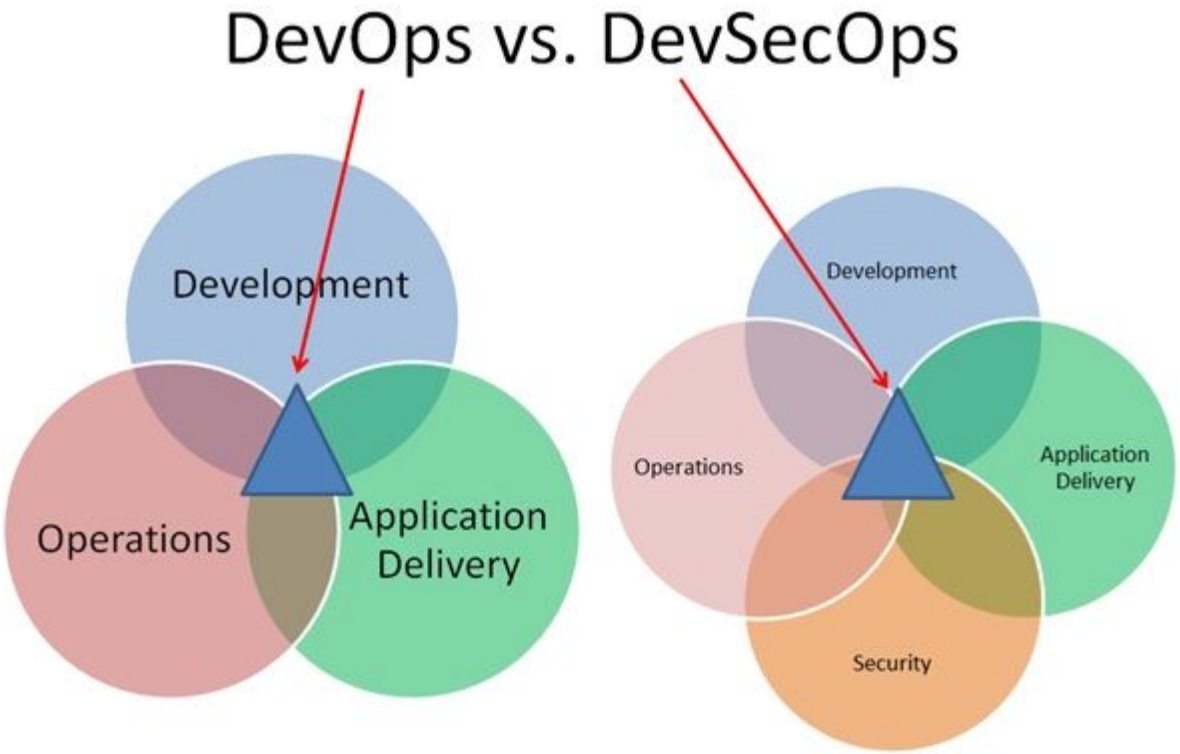
José Manuel Ortega Candel

Agenda

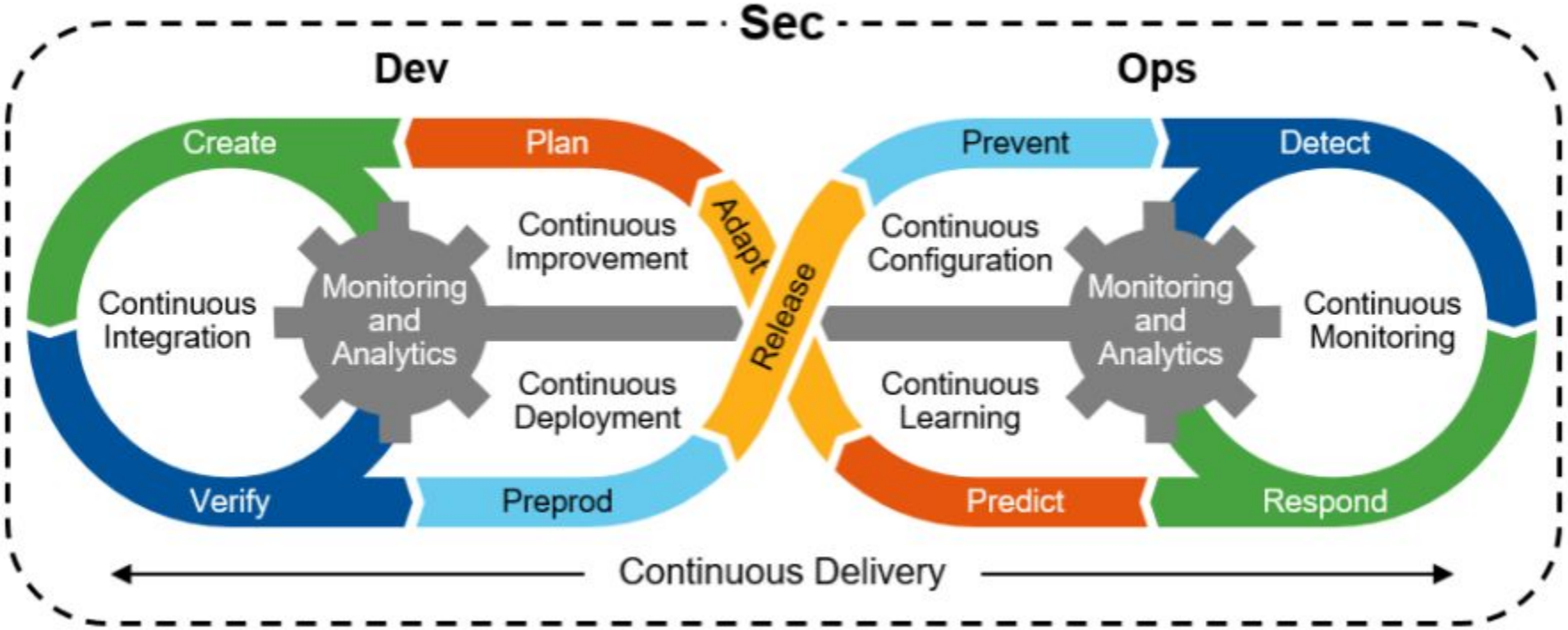
SG VIRTUAL CONFERENCE

- 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



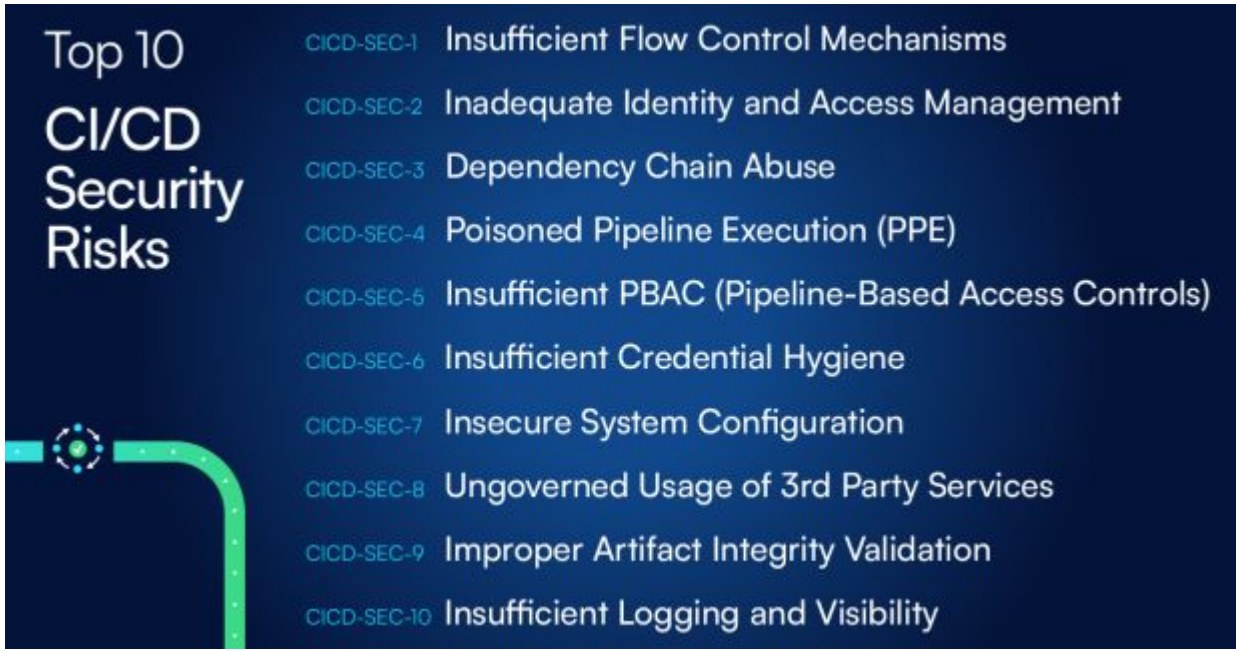
Introducción a DevSecOps



Introducción a DevSecOps

SG VIRTUAL CONFERENCE

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



Introducción a DevSecOps

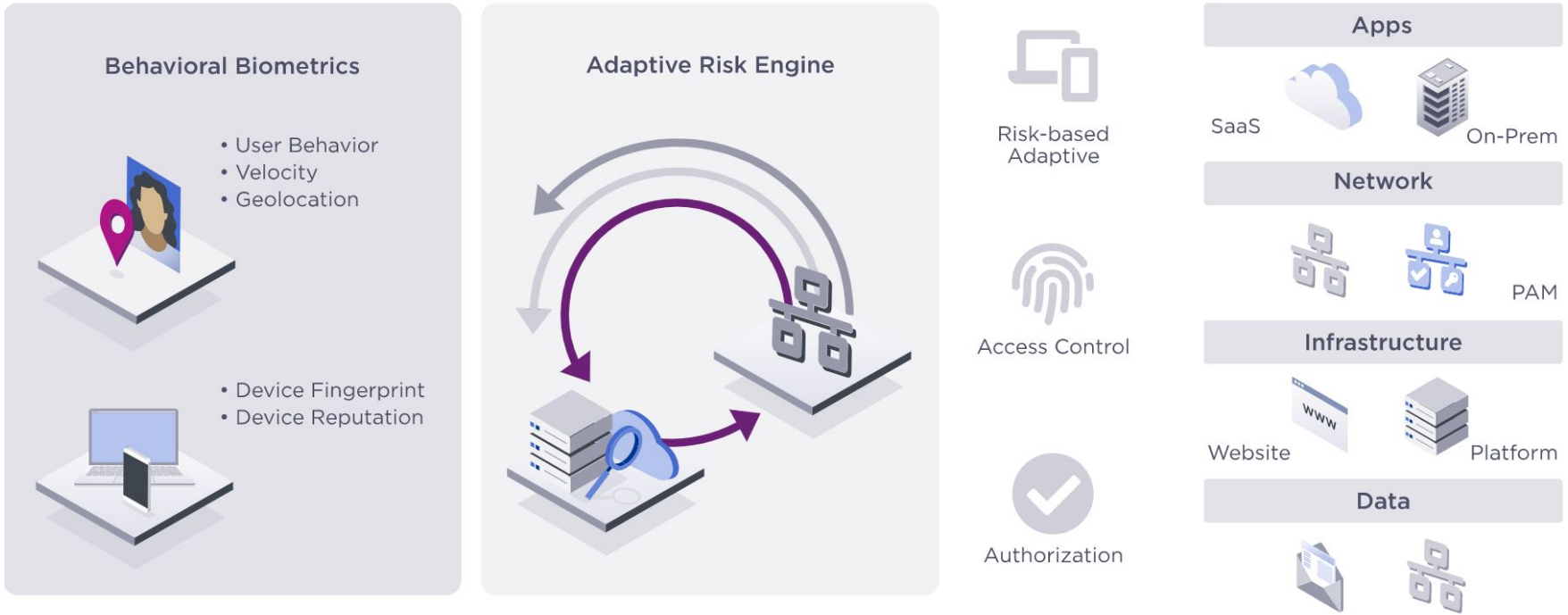
- CICD-SEC-1: Insufficient Flow Control Mechanisms
- CICD-SEC-2: Inadequate Identity and Access Management
- CICD-SEC-3: Dependency Chain Abuse
- CICD-SEC-4: Poisoned Pipeline Execution (PPE)
- CICD-SEC-5: Insufficient PBAC (Pipeline-Based Access Controls)
- CICD-SEC-6: Insufficient Credential Hygiene
- 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

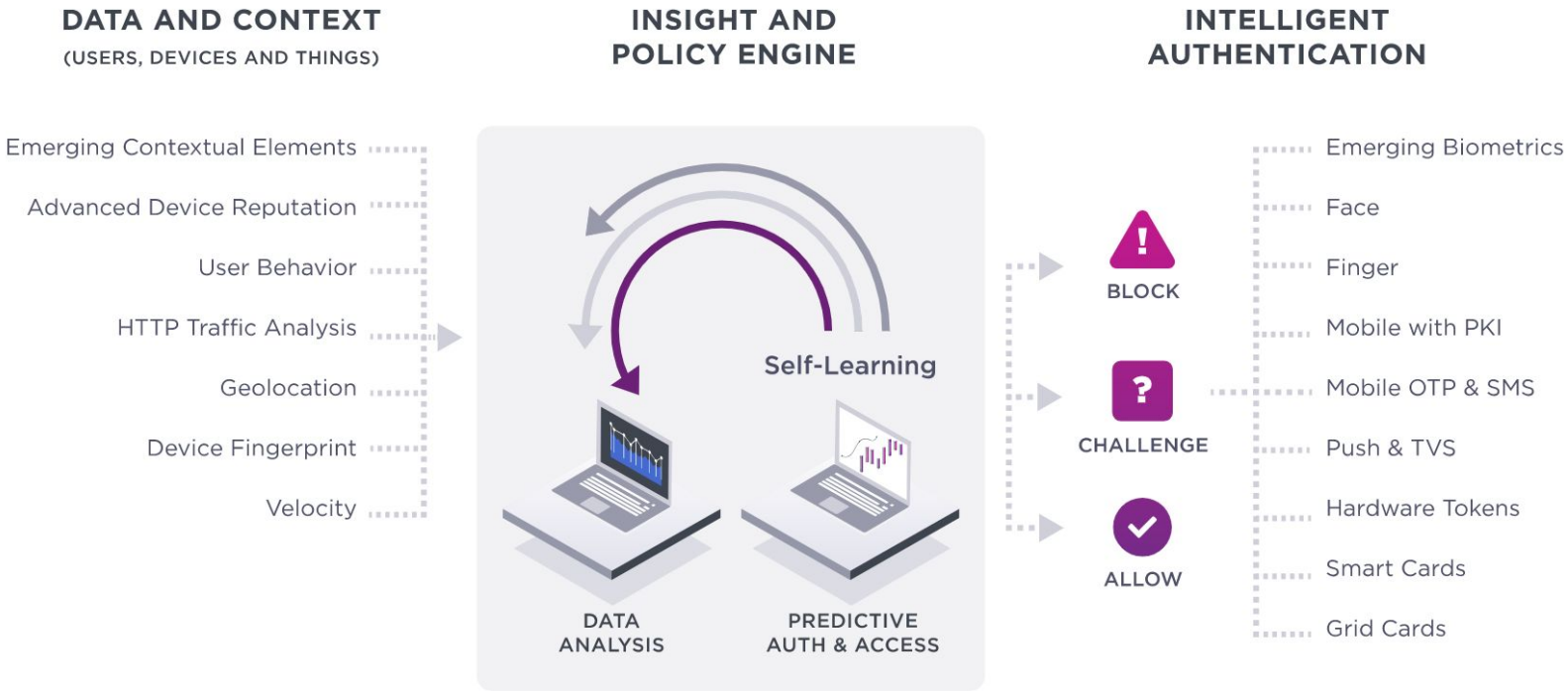
Modelado de amenazas

- 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



Modelo de confianza cero en la nube



Modelo de confianza cero en la nube

SG VIRTUAL CONFERENCE

- **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

SG VIRTUAL CONFERENCE

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

Modelo de confianza cero en la nube

SG VIRTUAL CONFERENCE

- ¿Qué están intentando proteger?

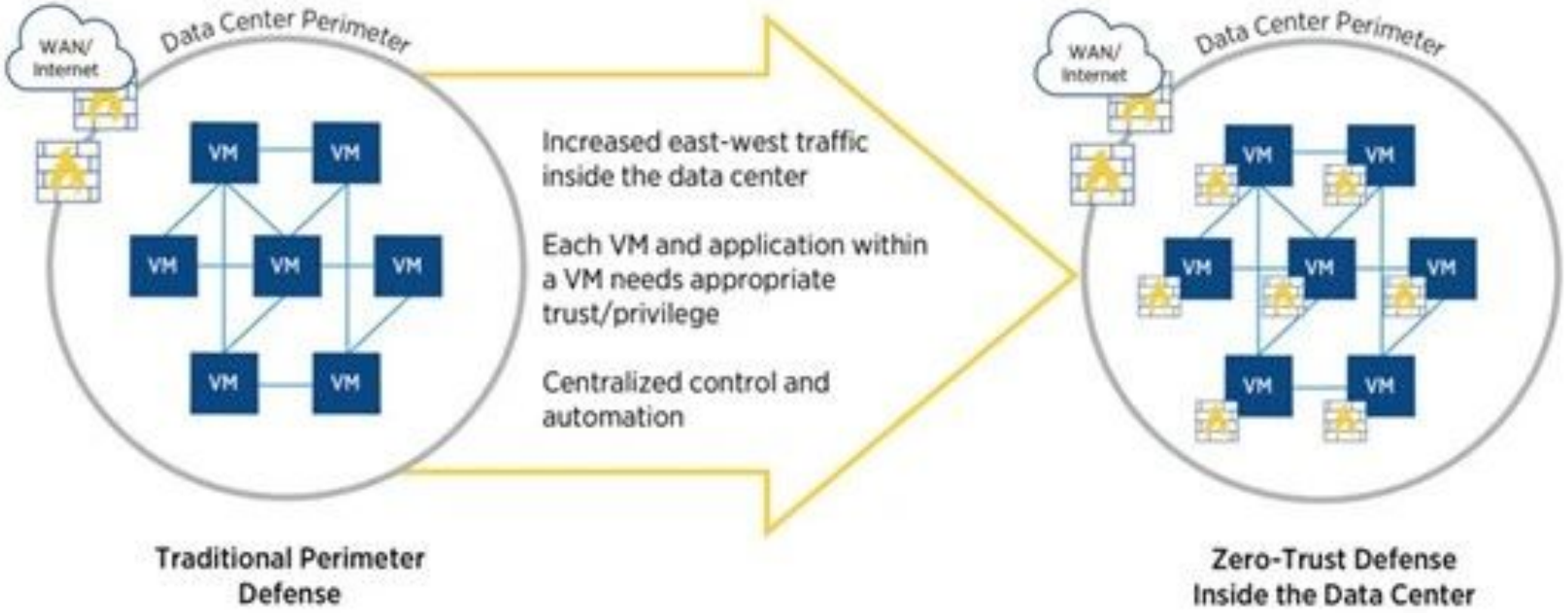
- ¿De quién intentan protegerlo?

Modelo de confianza cero en la nube

SG VIRTUAL CONFERENCE

- 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

SG VIRTUAL CONFERENCE

- 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

SG VIRTUAL CONFERENCE

- **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

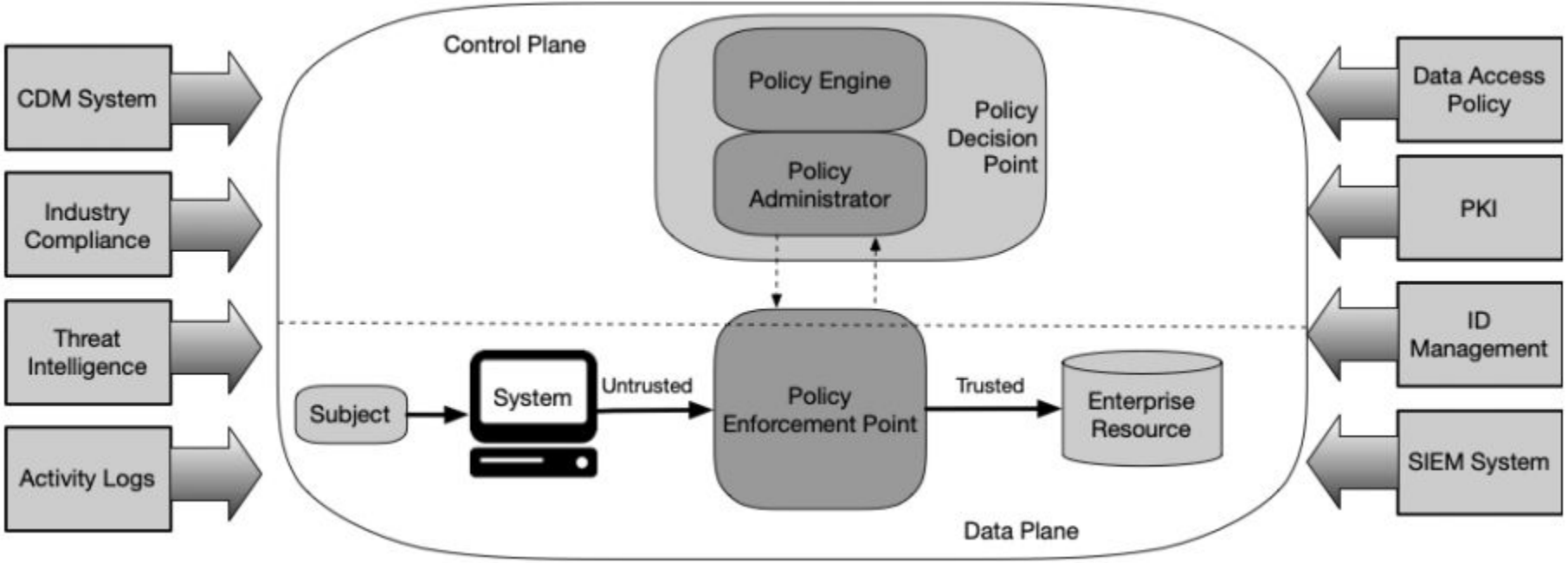
Fuente: NIST SP 800-207

National Institute of Standards and Technology

Arquitecturas zero trust

National Institute of Standards and Technology

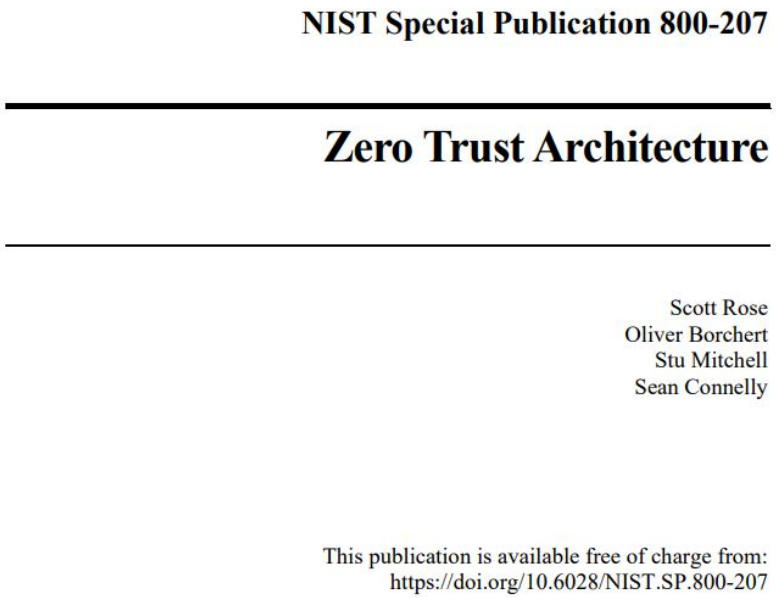
SG VIRTUAL CONFERENCE



Arquitecturas zero trust

National Institute of Standards and Technology

SG VIRTUAL CONFERENCE



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

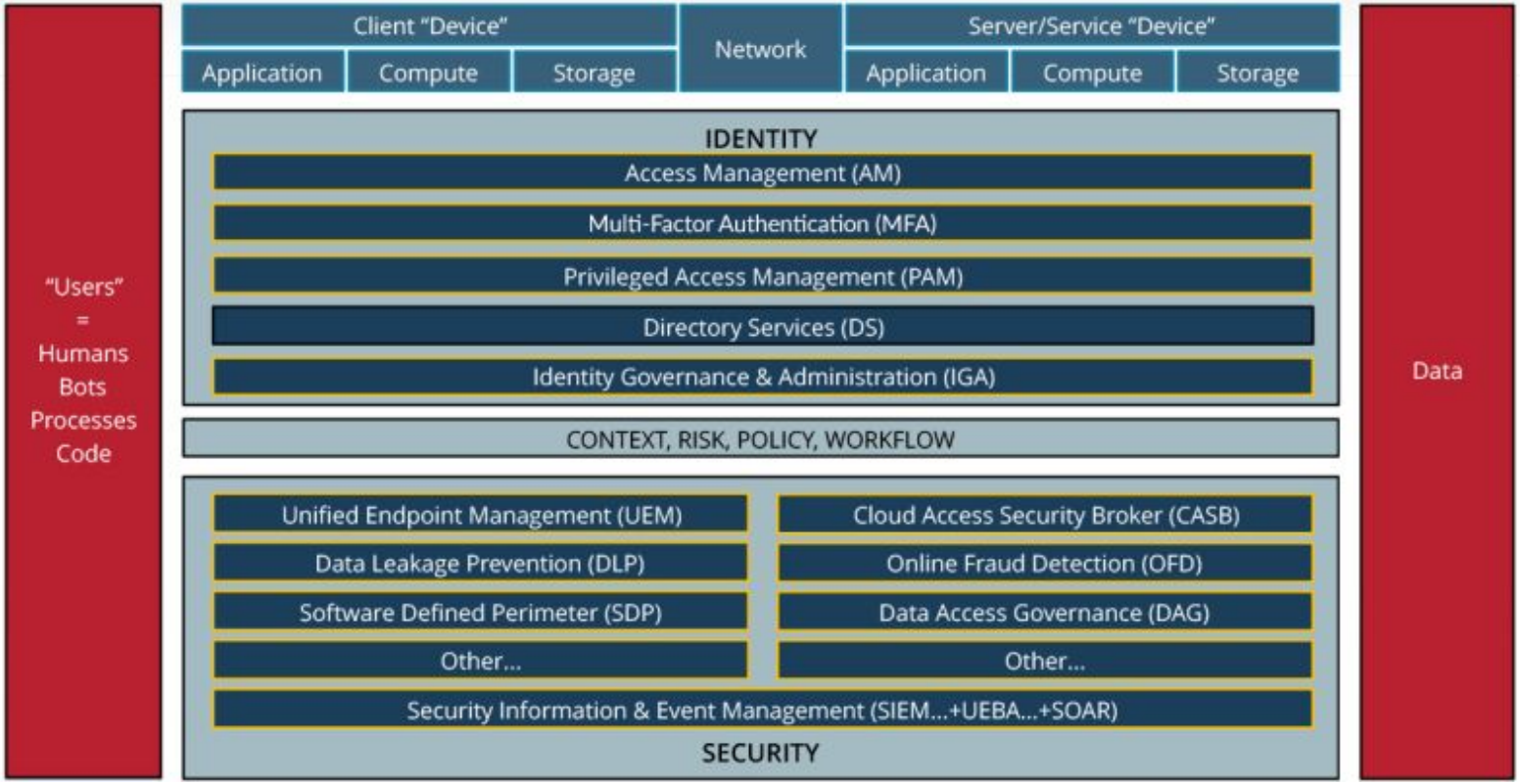
Table of Contents

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

Arquitecturas zero trust

IDENTITY DEFINED SECURITY ALLIANCE

SG VIRTUAL CONFERENCE



Arquitecturas zero trust

IDENTITY DEFINED SECURITY ALLIANCE

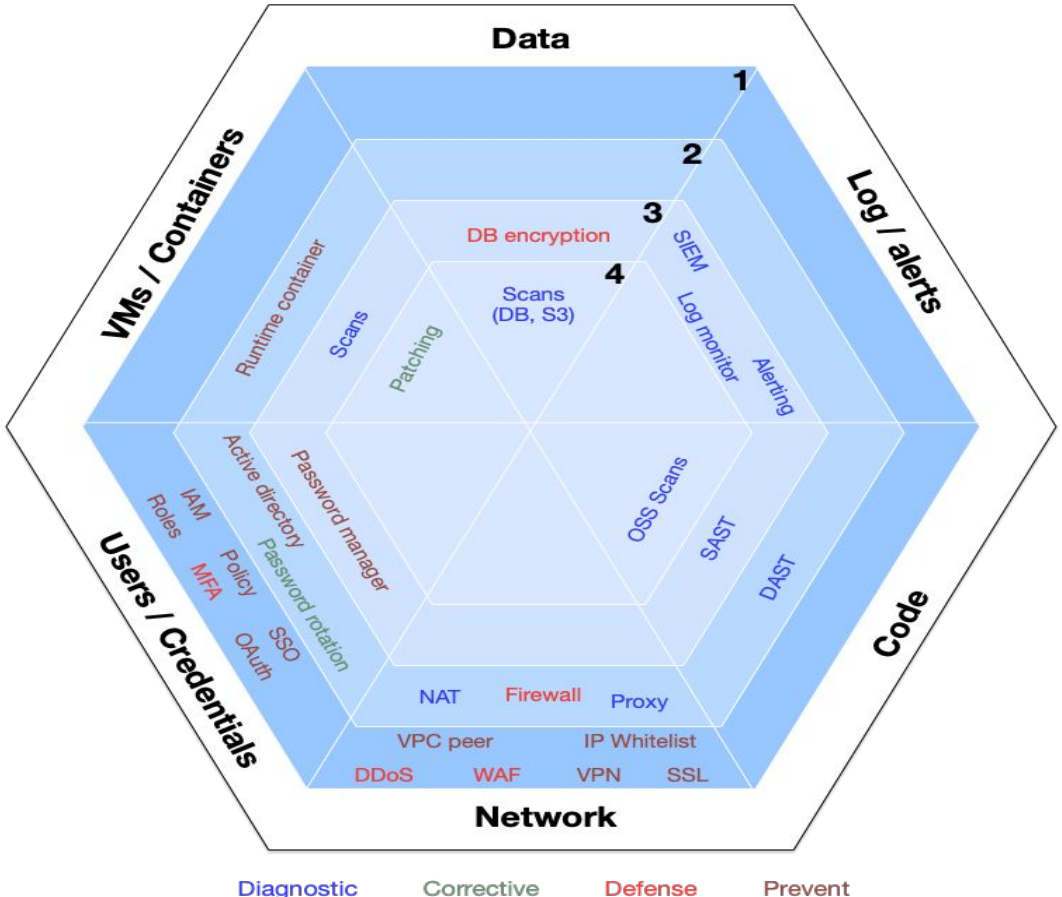
Uso de soluciones de IAM

- 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



Herramientas de análisis

https://cloudcustodian.io

Cloud Custodian

SG VIRTUAL CONFERENCE

aws

```
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)
```

Azure

```
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' ]
```

Google Cloud

```
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')
```

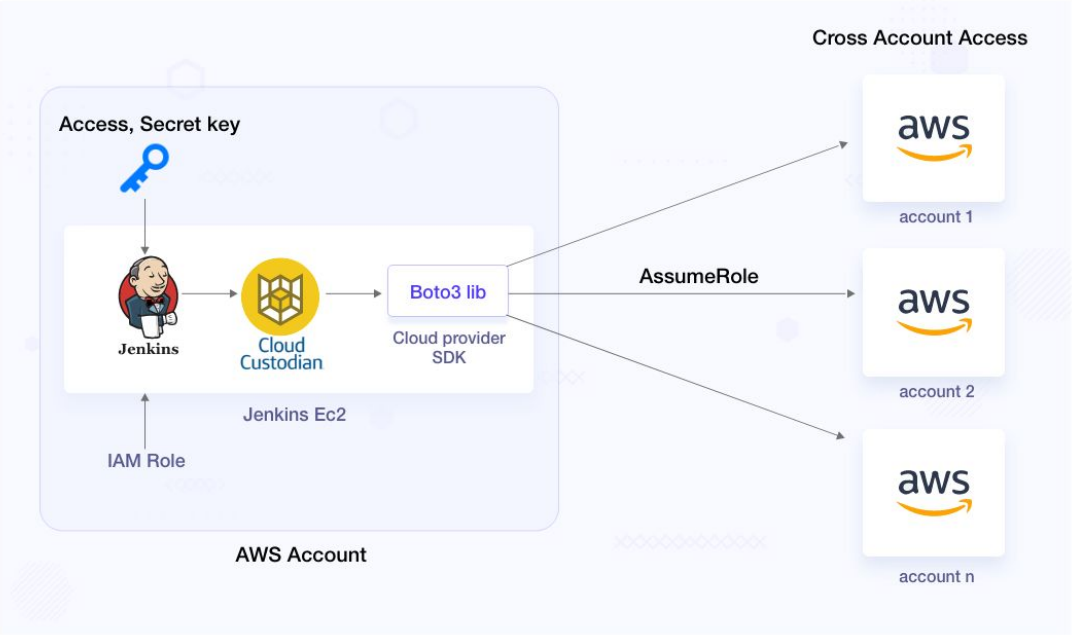
```
policies:
  - name: my-k8s-deployments
    resource: k8s.deployment
    filters:
      - type: value
        key: "spec.metadata.labels.owner"
        value: "sam"
```

```
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

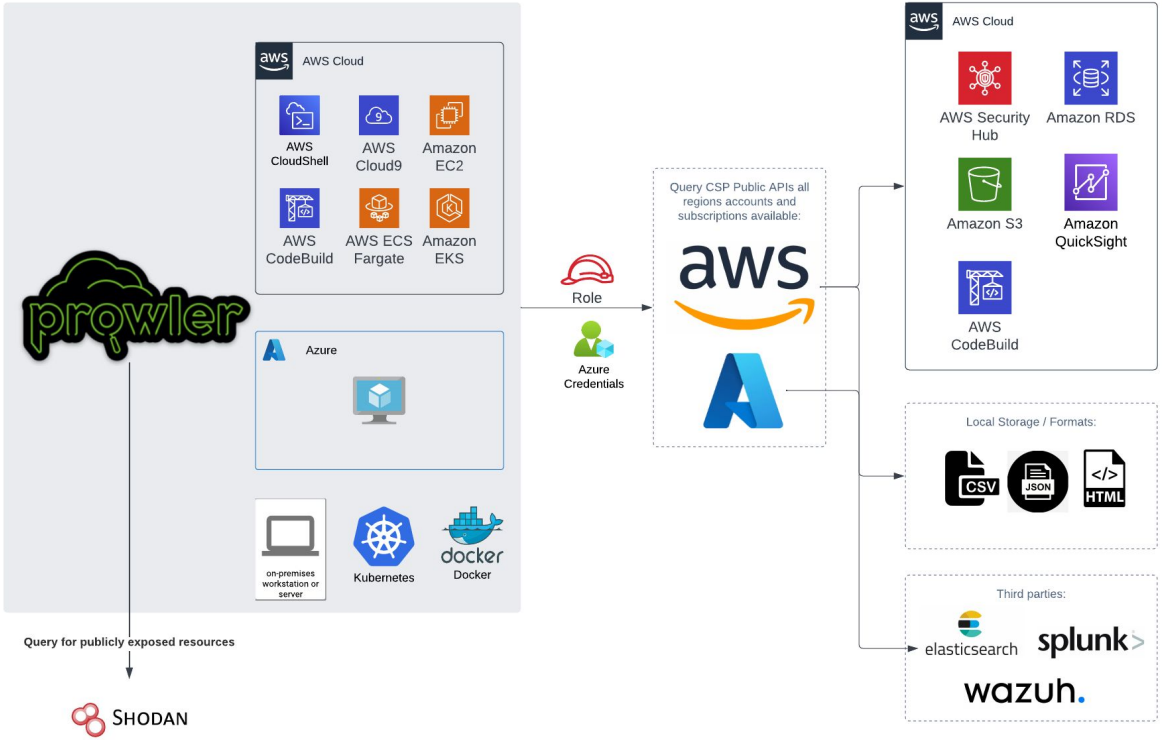
AWS Lambda

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

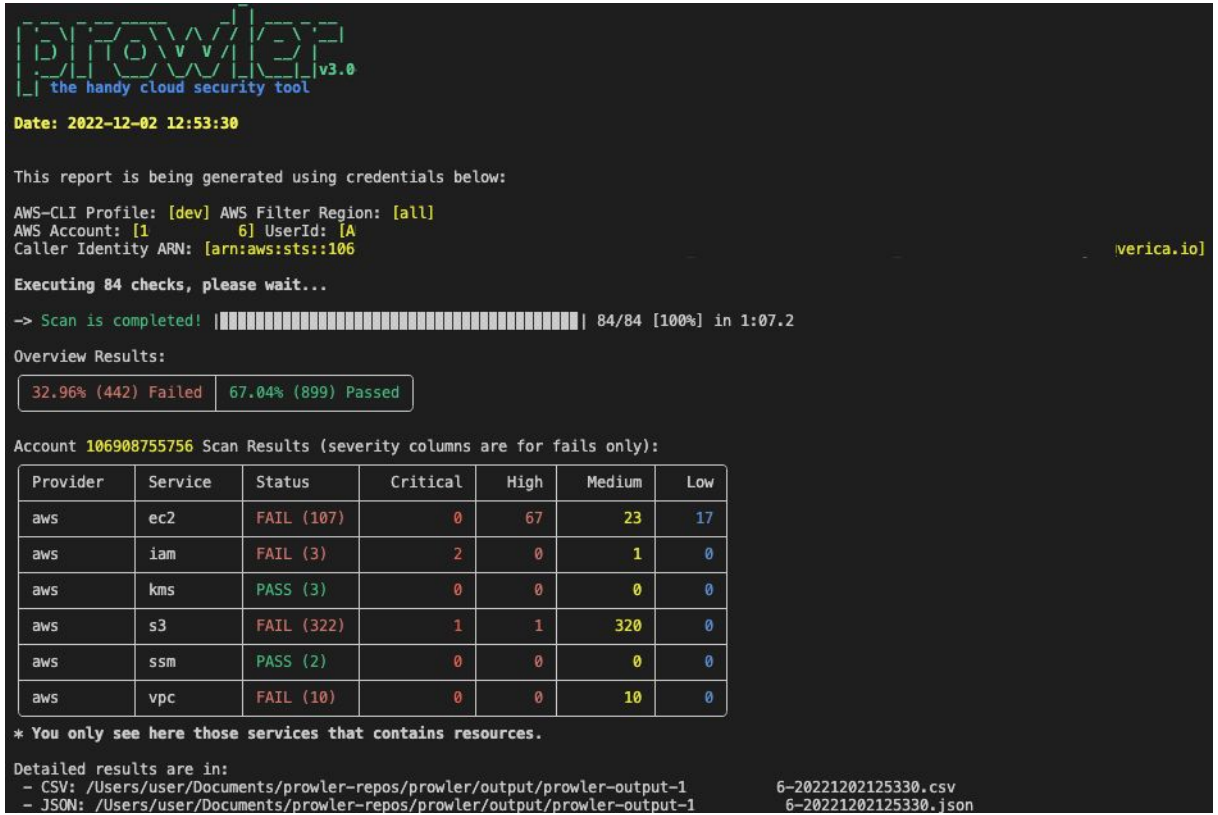


Herramientas de análisis

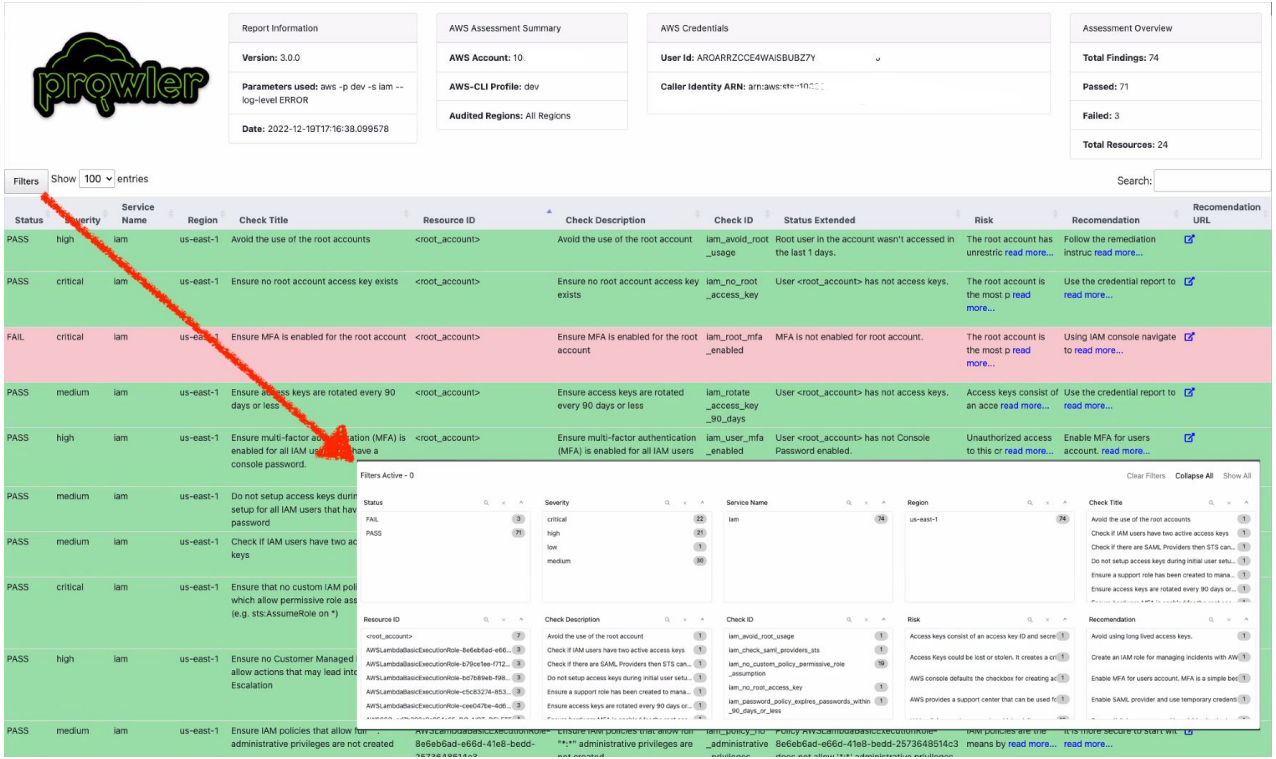

```
aws configure

export AWS_ACCESS_KEY_ID="ASXXXXXXX"
export AWS_SECRET_ACCESS_KEY="XXXXXXXXX"
export AWS_SESSION_TOKEN="XXXXXXXXX"
```


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

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

Herramientas de análisis



Herramientas de análisis



Principales servicios de seguridad en AWS

SG VIRTUAL CONFERENCE

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

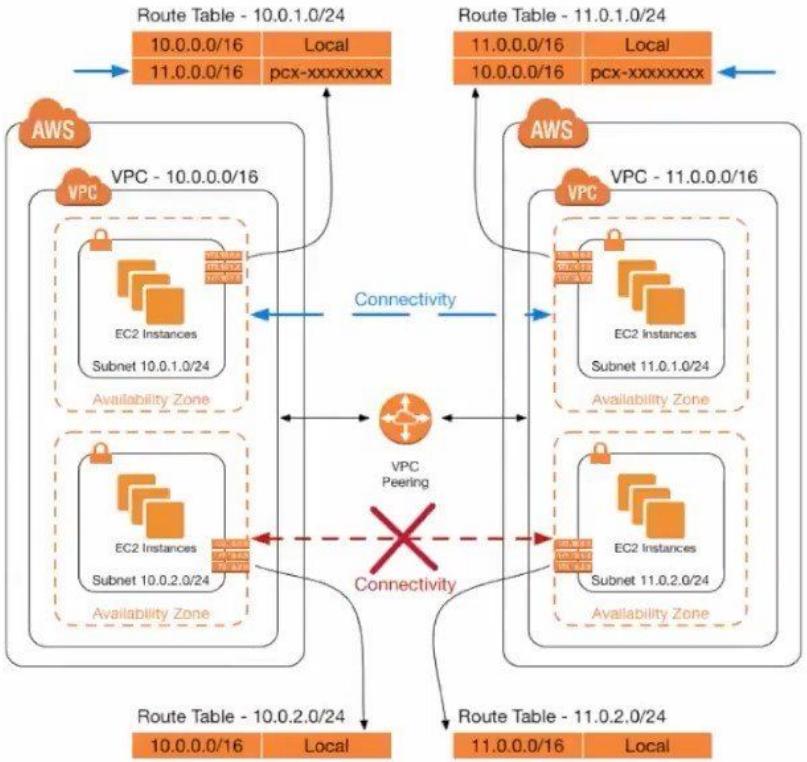
AWS KMS

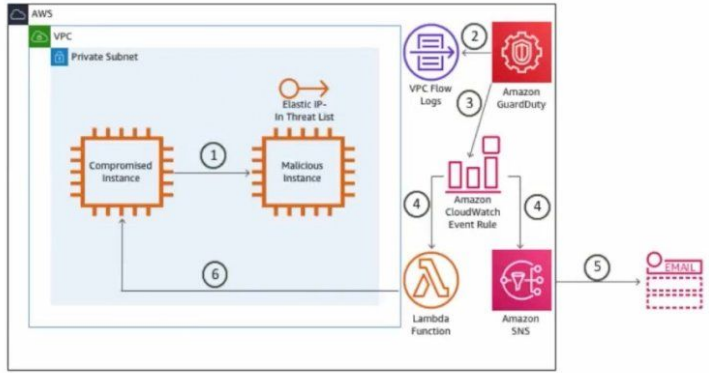
Create and control the cryptographic keys that protect your data

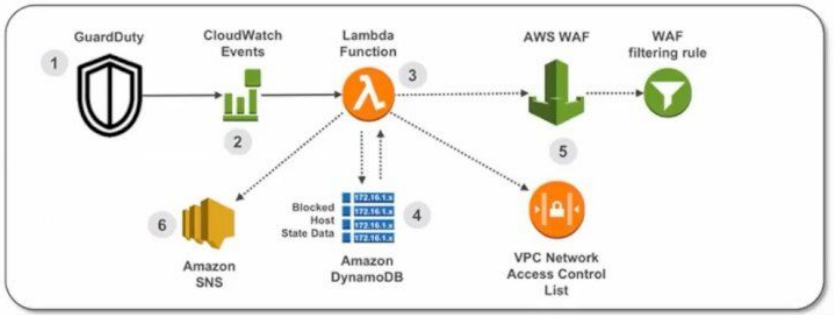
Amazon Inspector

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

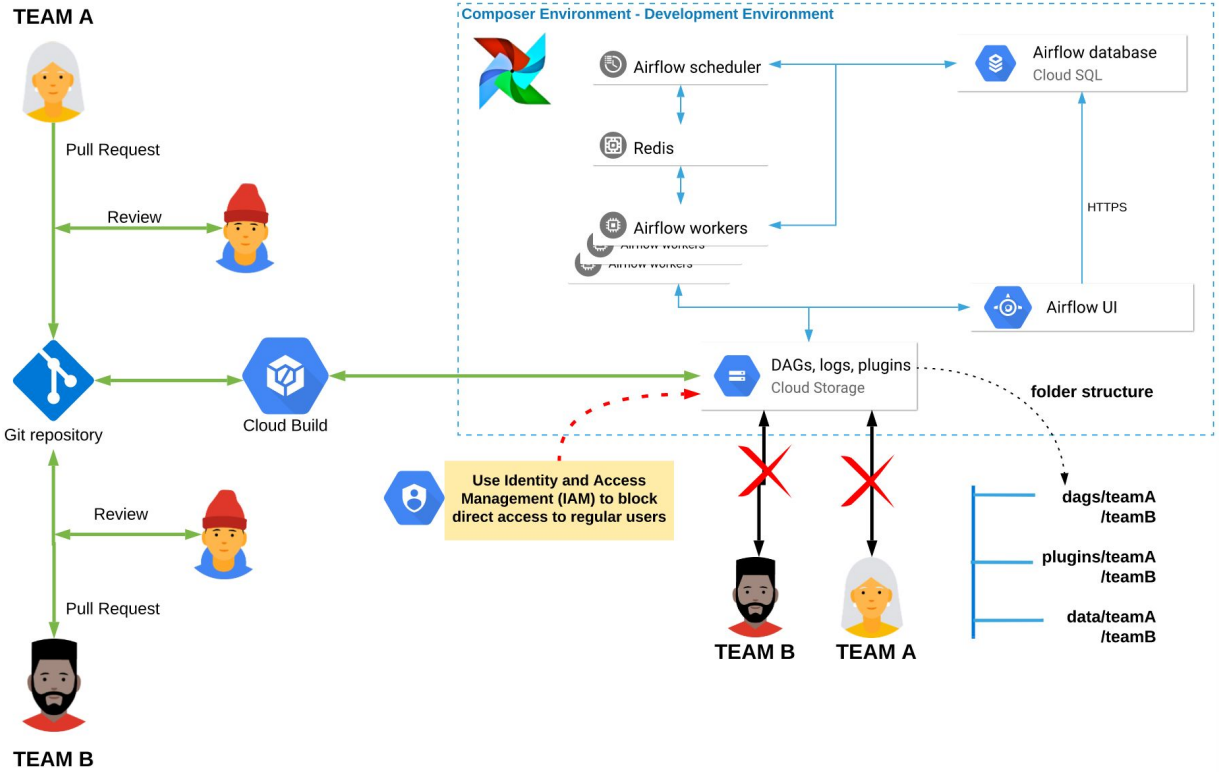
Principales servicios de seguridad en AWS







Mejores prácticas de seguridad



Google Cloud Composer

Mejores prácticas de seguridad

SG VIRTUAL CONFERENCE

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

Conclusiones

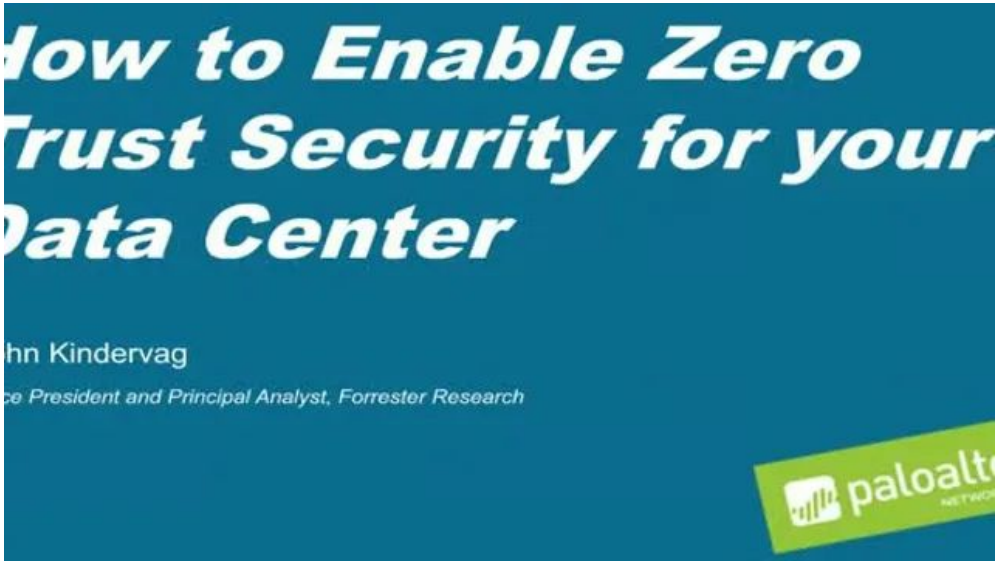
- Estrategia de empresa a largo plazo
- Gestión centralizada de la seguridad
- Solución centrada en la identidad del usuario

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