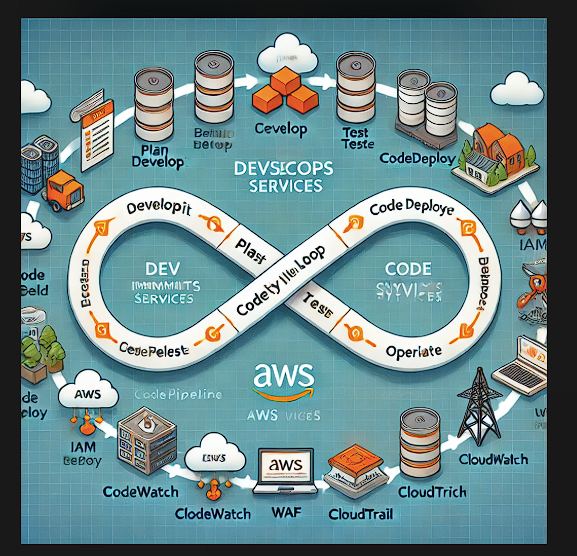
**Propuesta de migración Legacy, a DevSecOps, sobre AWS.**



**Itinerario.**

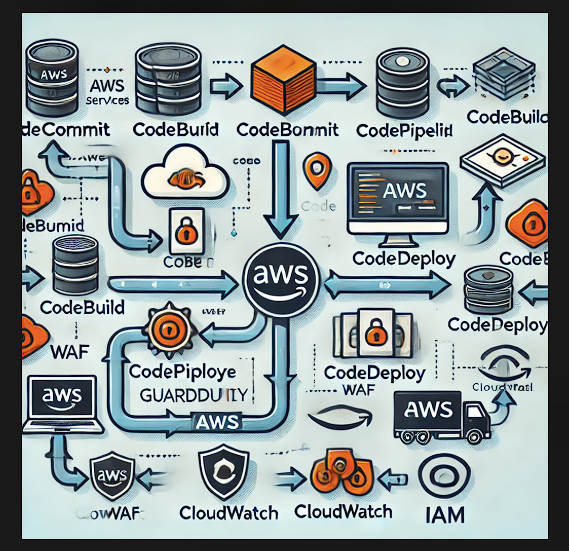
|  |  |  |
| --- | --- | --- |
| **Fase** | **Herramientas.** | |
| **Legacy** | **AWS** |
| **Planificación** | **GitLab** | **AWS IAM** |
| **Desarrollo** | **SonarQube GitLab Snyk Trivy** | **Amazon CodeGuru Amazon Inspector** |
| **Integración** | **Jenkins (SonarQube Snyk Trivy)** | **AWS CodePipeline AWS CodeBuild AWS Lambda** |
| **Despliegue** | **Jenkins** | **AWS CodeDeploy AWS Elastic Beanstalk Amazon ECS Amazon EKS**  **AWS CloudFormation** |
| **Operación** | **SonarQube Snyk Trivy** | **Amazon CloudWatch AWS CloudTrail AWS Config AWS Security Hub Amazon GuardDuty AWS WAF** |
| **Retroalimentación** | **GitLab** | **AWS CloudWatch Logs AWS X-Ray AWS Security Hub** |

* **Intensidad: 2 Horas diarias.**
* **Horario: lunes a sábado, durante cuatro semanas.**
* **Total: 44 Horas.**
* **Publico: Hasta 10 personas en reunión.**
* **Créditos estimados (USD): $495.23**

**Migración de Jenkins.**

**Desarrollo de Pipelines:**

* Desde **Python**, Escribir un **Jenkinsfile** simple, convertirlo a **YAML** de **CloudFormation**, y validar la salida para **CodePipeline**.
* Integración con WebHook de **GitLab**.

**Herramientas DevSecOps AWS.**

|  |  |  |
| --- | --- | --- |
| **AWS.** | **Herramienta.** | **Créditos USD.** |
| **CI/CD.** | **CodeBuild.** | **$ 1** |

**Integración continua.**



|  |  |  |
| --- | --- | --- |
| **AWS.** | **Herramienta.** | **Créditos USD.** |
| **Seguridad.** | **Secrets Manager.** | **$ 0.0130** |

**Cumplimiento.**

* Crear y consumir secretos en una aplicación.

|  |  |  |
| --- | --- | --- |
| **AWS.** | **Herramienta.** | **Créditos USD.** |
| **DevSecOps.** | **SonarQube.** | **$ 0** |
| **CodeGuru.** | **$ 0.3433** |

**SAST.**

* **Amazon CodeGuru**: Integrar y probar las herramientas de seguridad en un pipeline para monitoreo continuo.
* **CodeGuru Reviewer**: Analiza el código fuente en busca de errores comunes, vulnerabilidades de seguridad y malas prácticas de programación. Integra con servicios de repositorios como **GitHub**.
* **CodeGuru Profiler**: Proporciona recomendaciones sobre el rendimiento de las aplicaciones, ayudando a identificar cuellos de botella y optimizando el uso de los recursos.

|  |  |  |
| --- | --- | --- |
| **AWS.** | **Herramienta.** | **Créditos USD.** |
| **DevSecOps.** | **Snyk.** | **$ 0** |
| **Docker.** | **$ 0** |
| **Trivy.** | **$ 0** |
| **Hub Security.** | **$ 0** |

**Vulnerabilidades.**

* **Snyk**: Escanear dependencias de un proyecto y mostrar vulnerabilidades encontradas.
* **Hub Security:** Realizar un análisis de seguridad en una imagen.
* **ECR:** Subir imagen generada.

|  |  |  |
| --- | --- | --- |
| **AWS.** | **Herramienta.** | **Créditos USD.** |
| **Contenedores.** | **ECR.** | **FREE TIER.** |

**Entrega continua.**

|  |  |  |
| --- | --- | --- |
| **AWS.** | **Herramienta.** | **Créditos USD.** |
| **Automatización.** | **RDS.** | **FREE TIER.** |
| **EC2.** | **FREE TIER.** |
| **Contenedores.** | **Fargate.** | **$ 0.1000** |
| **ECS.** | **$ 0** |
| **Elastic Benstalk.** | **$ 0** |
| **Orquestación.** | **EKS.** | **$ 0.2000** |

* **Automatización de despliegue**: Código desplegado desde el repositorio, pasa por las fases de construcción, pruebas, seguridad, y finalmente el despliegue a ambientes de producción o staging (a través de **EC2**).
* **ECS**: Configurar auto-scaling.
* **Fargate**: Desplegar una aplicación con Fargate desde ECR.
* **Elastic Benstalk:** Despliegue simplificado de aplicaciones web y contenedores.
* **AWS Lambda**: Para la ejecución de funciones que pueden formar parte de la integración.
* **EKS**: Desplegar una aplicación de múltiples contenedores.

|  |  |  |
| --- | --- | --- |
| **AWS.** | **Herramienta.** | **Créditos USD.** |
| **Networking.** | **API Gateway.** | **$ 0.1500** |
| **CloudFront.** | **$ 0.0035** |
| **Contenedores.** | **ALB.** | **$ 0.0610** |

**Escalabilidad.**

* Integrar con **CloudFront, API Gateway** para proteger aplicaciones desplegadas.
* **ALB:** Configurar balanceo de carga.

|  |  |  |
| --- | --- | --- |
| **AWS.** | **Herramienta.** | **Créditos USD.** |
| **Gobernanza.** | **IAM.** | **$ 0** |
| **S3.** | **FREE TIER.** |

**Gobernanza.**

**IAM.**

* Configuración de la **CLI** de AWS en local.
* Subir el YAML al **Bucket**.

|  |  |  |
| --- | --- | --- |
| **AWS.** | **Herramienta.** | **Créditos USD.** |
| **CI/CD.** | **CodePipeline.** | **$ 1** |

* Desde CLI, Crear un **stack** de CloudFormation.

|  |  |  |
| --- | --- | --- |
| **AWS.** | **Herramienta.** | **Créditos USD.** |
| **Automatización.** | **CloudFormation.** | **$ 0** |

**Infraestructura como código.**

**CloudFormation**:

* Establecer en el YAML la **retención** de backup del Bucket.

|  |  |  |
| --- | --- | --- |
| **AWS.** | **Herramienta.** | **Créditos USD.** |
| **Gobernanza.** | **AWS Backup.** | **$ 0.0016** |

.

* Deployar cambios en la pila existente.

|  |  |  |
| --- | --- | --- |
| **AWS.** | **Herramienta.** | **Créditos USD.** |
| **CI/CD.** | **CodeDeploy.** | **$ 0** |

|  |  |  |
| --- | --- | --- |
| **AWS.** | **Herramienta.** | **Créditos USD.** |
| **Seguridad.** | **AWS Config.** | **$ 0.0002** |
| **AWS Inspector.** | **$ 0.0130** |
| **AWS WAF.** | **$ 0.1867** |
| **Observabilidad.** | **X-Ray.** | **$ 0.0166** |

**Cumplimiento.**

* **AWS Inspector:** Escaneo de vulnerabilidades para instancias.
* **AWS Config:** Configurar reglas de conformidad para monitorear recursos.
* **AWS WAF:** Crear y aplicar reglas básicas para proteger aplicaciones desplegadas.
* Monitorear logs de seguridad de **WAF**, **VPC** **Flow** **Logs** o eventos detectados.
* **X-Ray:** Configurar una traza para una aplicación web.

|  |  |  |
| --- | --- | --- |
| **AWS.** | **Herramienta.** | **Créditos USD.** |
| **Seguridad.** | **AWS CloudWatch.** | **FREE TIER.** |
| **Observabilidad.** | **AWS CloudTrail.** | **FREE TIER.** |

**Observabilidad.**

* **CloudWatch**: Crear métricas personalizadas y alertas de seguridad.

|  |  |  |
| --- | --- | --- |
| **AWS.** | **Herramienta.** | **Créditos USD.** |
| **Automatización.** | **Lambda.** | **FREE TIER.** |

* **Lambda:** Lanzar el evento de seguridad.
* **SNS:** Uso para notificaciones de eventos.

|  |  |  |
| --- | --- | --- |
| **AWS.** | **Herramienta.** | **Créditos USD.** |
| **Observabilidad.** | **SNS.** | **FREE TIER.** |
| **SQS.** | **FREE TIER.** |

* **SQS:** Uso como sistema de mensajería confiable.
* **CloudTrail**: Generar y revisar logs para auditoría de acceso a recursos.
* Usar **CloudWatch Logs Insights** para analizar errores en la compilación o despliegue.
* Evaluar la conformidad con estándares de seguridad como **CIS AWS Foundations Benchmark** o normativas específicas del cliente.

|  |  |  |
| --- | --- | --- |
| **AWS.** | **Herramienta.** | **Créditos USD.** |
| **Mejora Continua.** | **GuardDuty.** | **$ 1** |

**Mejora Continua.**

* **GuardDuty**: Analizar las alertas generadas.
* Implementar políticas automatizadas contra ataques DDoS con **AWS Shield Advanced**.