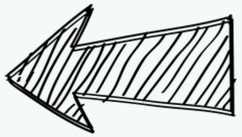
Cloud Computing - AWS

ACADEMIA CONSULTEC

Presentado por **Alejandro Chacón**
www.consultec-ti.com

Agenda

- Intro
- Almacenamiento S3
- Networking
- Cómputo y Almacenamiento
- Integración y Monitoreo
- Bases de Datos
- Seguridad



- Despliegues y Gestión de Infraestructura

ACADEMIA CONSULTEC

AWS Security

Agenda

- Intro
- DDOS, Shield & WAF
- Test de penetración
- KMS, CloudHSM, Secret Manager
- Certificate Manager
- Inspector
- GuardDuty
- Security Hub
- Config, Macie, Artifact
- Abuse
- Detective

ACADEMIA CONSULTEC

Seguridad en AWS

Modelo de Responsabilidad Compartida

- Responsabilidad de AWS - Seguridad de la Nube
  - Proteger la infraestructura (hardware, software, instalaciones y redes) que ejecuta todos los servicios de AWS.
  - Servicios gestionados como S3, DynamoDB, RDS, etc.
- Responsabilidad del cliente - Seguridad en la Nube
  - Para la instancia EC2, el cliente es responsable de la administración del sistema operativo (incluidos los parches de seguridad y las actualizaciones), la configuración de la red, el firewall y IAM.
  - Cifrado de datos de la aplicación.
- Controles compartidos:
  - Gestión de parches, gestión de la configuración, sensibilización y formación.

ACADEMIA CONSULTEC

Seguridad en AWS

Modelo de Responsabilidad Compartida - RDS

- Responsabilidad de AWS:
  - Administrar la instancia EC2 (Infra), deshabilita el acceso SSH
  - Aplicación de parches de base de datos automatizada
  - Parches automatizados del sistema operativo
  - Auditar la instancia (Infra) y los discos y garantizar que funcione
- Tu responsabilidad:
  - Verificar las reglas de entrada/puertos / IP / grupo de seguridad en DB's
  - Creación y permisos de usuarios en la base de datos
  - Creación de una base de datos con o sin acceso público
  - Asegúrese de que los grupos de parámetros o la base de datos estén configurados para permitir sólo conexiones SSL
  - Configuración de cifrado de base de datos

Seguridad en AWS

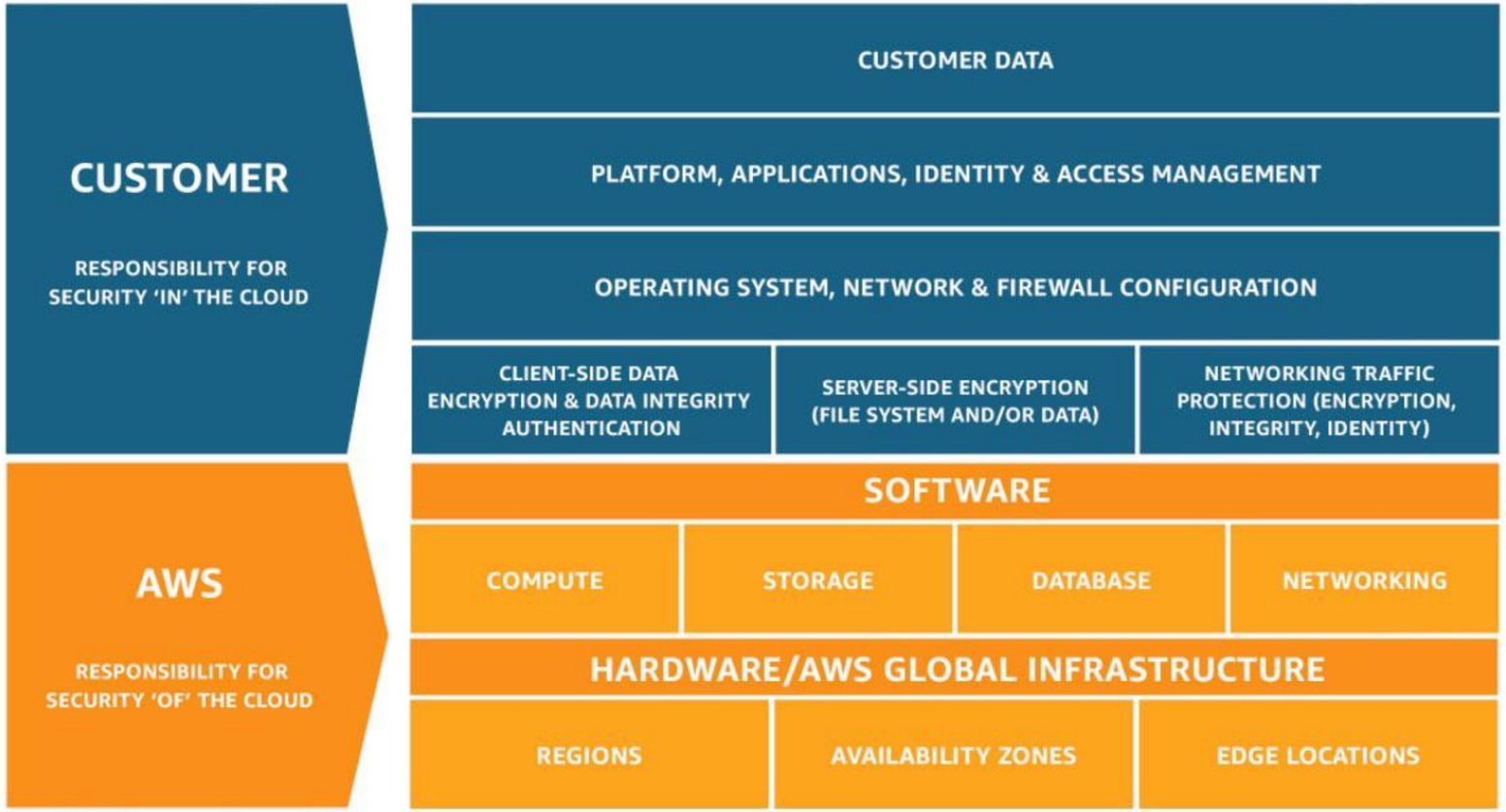
Modelo de Responsabilidad Compartida - S3

- Responsabilidad de AWS:
  - Garantiza almacenamiento ilimitado
  - Garantiza encriptación
  - Garantizar la separación de los datos entre diferentes clientes.
  - Asegúrese de que los empleados de AWS no puedan acceder a sus datos
- Tu responsabilidad:
  - Configuración del bucket
  - Política de depósito/configuración pública
  - Usuario y roles de IAM
  - Habilitación del cifrado

ACADEMIA CONSULTEC

Seguridad en AWS

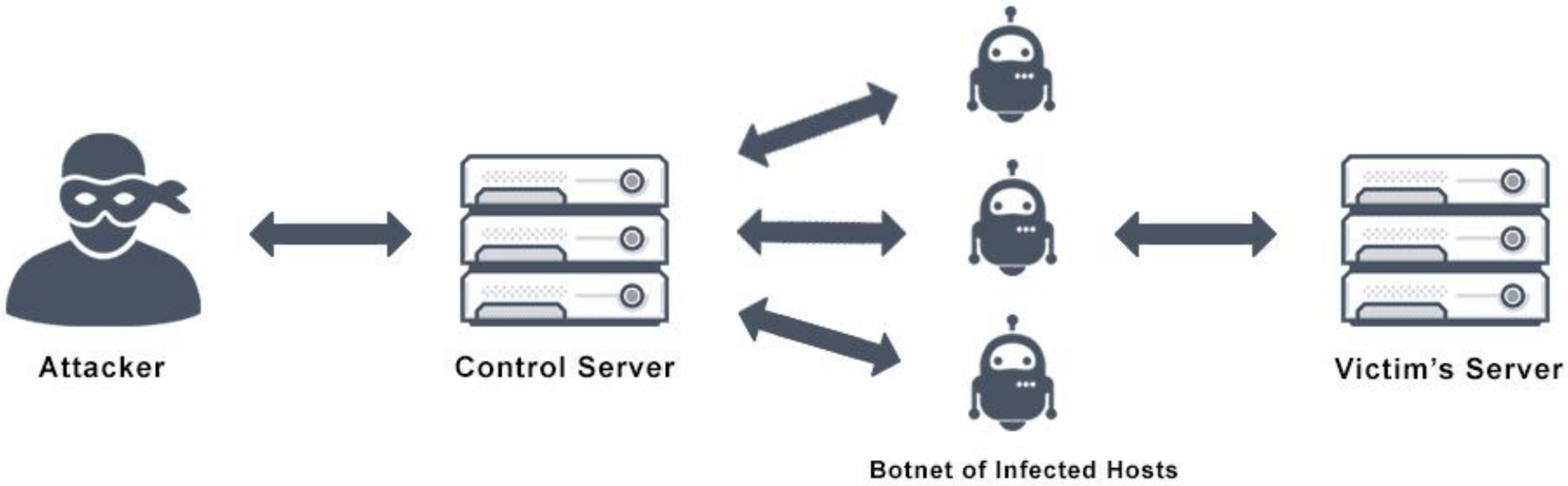
Modelo de Responsabilidad Compartida



ACADEMIA CONSULTEC

Seguridad en AWS

Ataques DDOS - Distribuidos



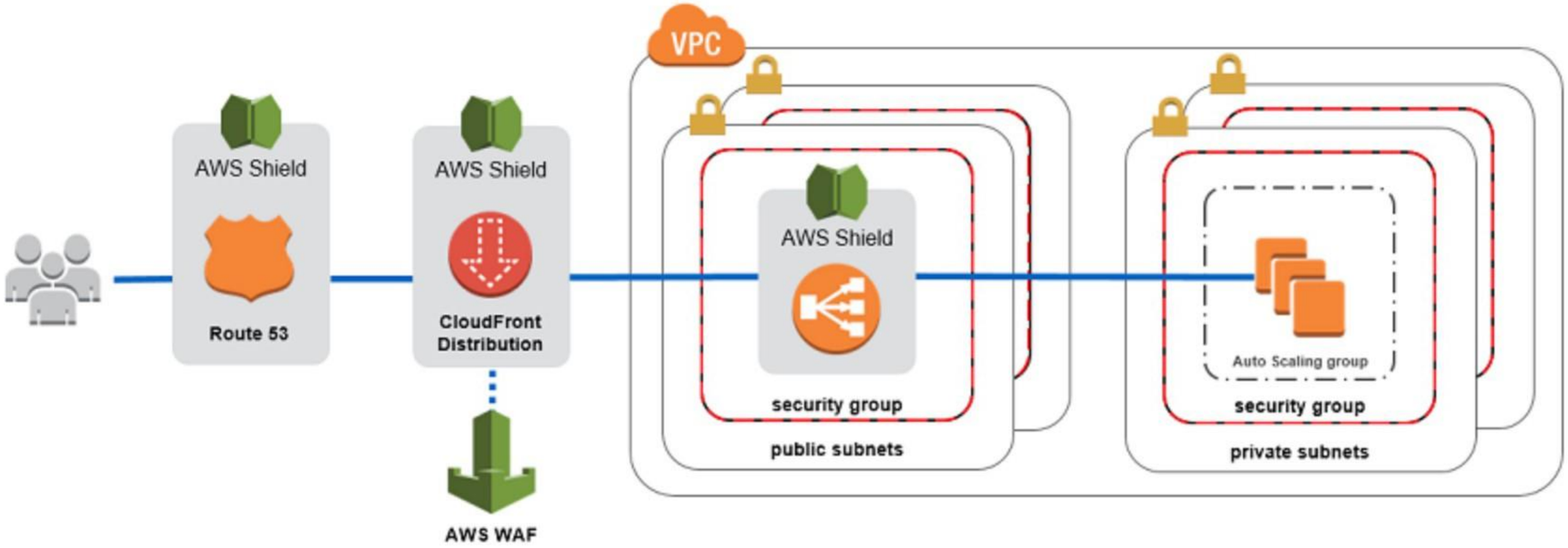
Seguridad en AWS

Ataques DDOS - Protección en la nube

- AWS Shield Standard
  - protege contra ataques DDOS para su sitio web y aplicaciones, para todos los clientes sin costo adicional
- AWS Shield Advanced
  - protección DDoS premium las 24 horas, los 7 días de la semana
- AWS WAF
  - filtre solicitudes específicas en función de las reglas predefinidas por AWS (Gratis) o mas avanzadas adquiridas en el MarketPlace
- CloudFront y Route 53:
  - Protección de disponibilidad mediante red perimetral global
  - Combinado con AWS Shield, proporciona mitigación de ataques en el perímetro

Seguridad en AWS

Ataques DDOS - Ejemplo de protección



ACADEMIA CONSULTEC

Seguridad en AWS

Shield

- AWS Shield Estándar:
    - Servicio gratuito que se activa para cada cliente de AWS
    - Brinda protección contra ataques como inundaciones SYN/UDP, ataques de reflexión y otros ataques de capa 3/capa 4
- AWS Shield avanzado:
    - Servicio opcional de mitigación de DDoS ($3000 por mes por organización)
    - Protéjase contra ataques más sofisticados en Amazon EC2, Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator y Route 53
    - Acceso 24/7 al equipo de respuesta DDoS (DRP) de AWS
    - Protéjase contra tarifas altas durante picos de uso debido a

Seguridad en AWS

WAF - Web App Firewall

- Protege sus aplicaciones web de vulnerabilidades web comunes (Capa 7)
- La capa 7 es HTTP (frente a la capa 4 es TCP)
- Implemente en Application Load Balancer, API Gateway, CloudFront

- Definir Web ACL (Lista de control de acceso web):
  - Las reglas pueden incluir direcciones IP, encabezados HTTP, cuerpo HTTP o cadenas URI
  - Protege contra ataques comunes: inyección SQL y Cross-Site Scripting (XSS)
  - Restricciones de tamaño, coincidencia geográfica (bloquear países)
  - Reglas basadas en tasas (para contar ocurrencias de eventos) – para protección DDoS

Seguridad en AWS

Penetration tests

- Los clientes de AWS pueden realizar evaluaciones de seguridad o pruebas de penetración en su infraestructura de AWS sin aprobación previa para 8 servicios:
  - Instancias Amazon EC2, NAT Gateways y Elastic Load Balancers
  - RDS de Amazon
  - Amazon CloudFront
  - amazona aurora
  - Puertas de enlace API de Amazon
  - Funciones de AWS Lambda y Lambda Edge
  - Recursos de Amazon Lightsail
  - Entornos de Amazon Elastic Beanstalk

Seguridad en AWS

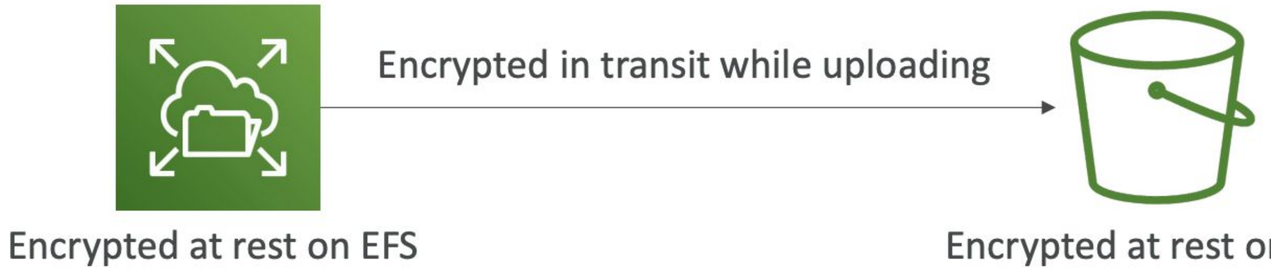
Penetration tests

- Actividades Prohibidas
  - Zona DNS a través de Amazon Route 53 Hosted Zones
  - Denegación de servicio (DoS), Denegación de servicio distribuida (DDoS), DoS simulado, DDoS simulado
  - inundación del puerto
  - Inundación de protocolo
  - Inundación de solicitudes (inundación de solicitudes de inicio de sesión, inundación de solicitudes de API)
- Para cualquier otro evento simulado, comuníquese con aws-security-simulated-event@amazon.com

ACADEMIA CONSULTEC

Seguridad en AWS

Datos en reposo y tránsito



- En reposo:
  - En un disco duro, en una instancia RDS, en S3 Glacier Deep Archive, etc.
- En tránsito (en movimiento): datos que se mueven de un lugar a otro
  - Transferencia desde las instalaciones a AWS, EC2 a DynamoDB, etc.
  - Significa datos transferidos en la red.
- ¡Queremos cifrar los datos en ambos estados para protegerlos!
- Para ello aprovechamos las claves de cifrado

ACADEMIA CONSULTEC

Seguridad en AWS

KMS

- Cada vez que escuche "cifrado" para un servicio de AWS, lo más probable es que sea KMS
- KMS = AWS administra las claves de cifrado por nosotros
- Opción de cifrado:
  - Volúmenes de EBS: cifrar volúmenes
  - S3 buckets: Cifrado de objetos del lado del servidor
  - Base de datos Redshift: encriptación de datos
  - Base de datos RDS: cifrado de datos
  - Unidades EFS: cifrado de datos
- Cifrado activado automáticamente:
  - Registros de CloudTrail
  - Glaciar S3
  - Storage Gateway

Seguridad en AWS

CloudHSM

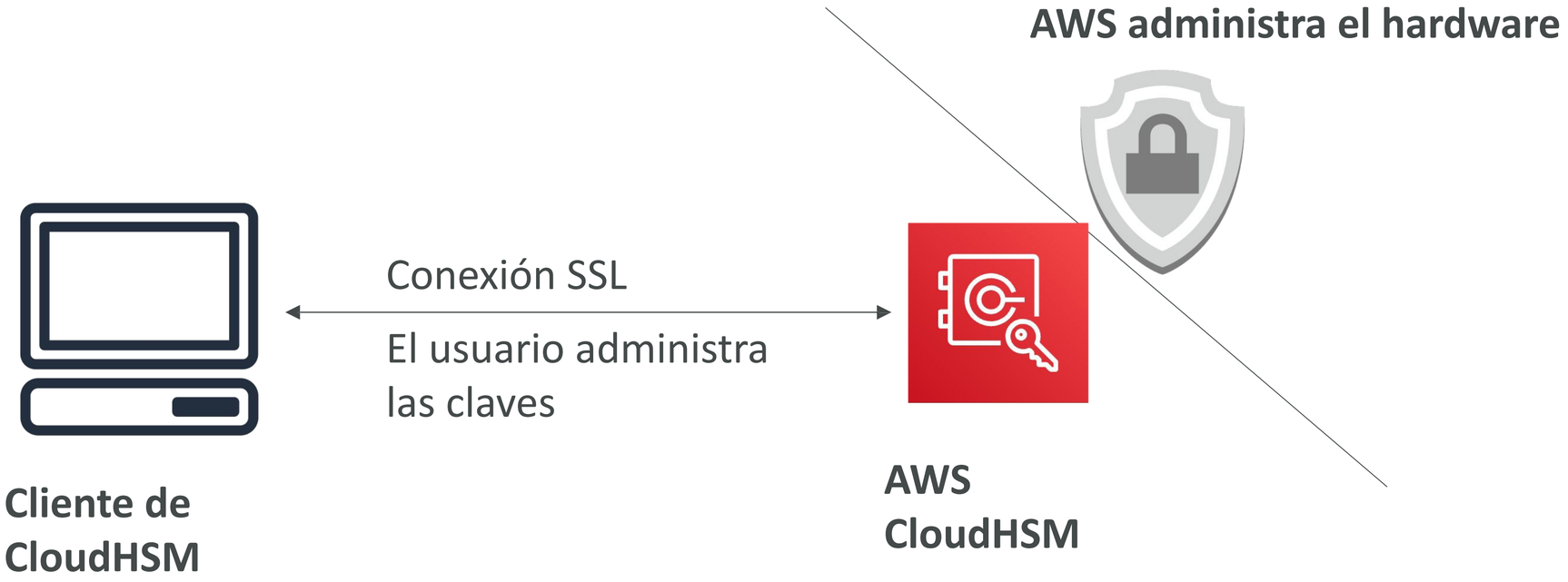
- KMS => AWS administra el software para el cifrado
- CloudHSM => AWS aprovisiona hardware de cifrado
- Hardware dedicado (HSM = Módulo de seguridad de hardware)
- Usted administra sus propias claves de cifrado por completo (no AWS)
- El dispositivo HSM es resistente a manipulaciones, cumple con FIPS 140-2 Nivel 3

Ejemplo de dispositivo HSM

ACADEMIA CONSULTEC

Seguridad en AWS

CloudHSM Esquema



Seguridad en AWS

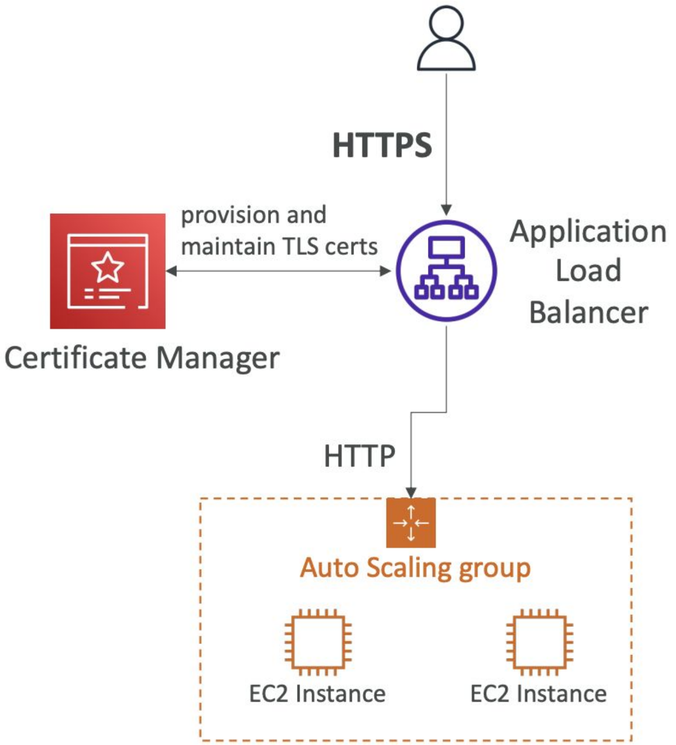
Client Master Keys (CMK)

- CMK administrada por el cliente:
  - Crear, administrar y utilizar por el cliente, puede habilitar o deshabilitar
  - Posibilidad de política de rotación (clave nueva generada cada año, clave antigua conservada)
  - Posibilidad de traer su propia llave
- CMK administrada por AWS:
  - Creado, administrado y utilizado en nombre del cliente por AWS
  - Utilizado por los servicios de AWS (aws/s3, aws/ebs, aws/redshift)
- CMK propiedad de AWS:
  - Colección de CMK que un servicio de AWS posee y administra para usar en varias cuentas
  - AWS puede usarlos para proteger los recursos en su cuenta (pero no puede ver las claves)
- Claves de CloudHSM (almacén de claves personalizado):
  - Claves generadas desde su propio dispositivo de hardware CloudHSM
  - Las operaciones criptográficas se realizan dentro del clúster de CloudHSM

Seguridad en AWS

Administrador de Certificados SSL

- Permite aprovisionar, administrar e implementar fácilmente
- Certificados SSL/TLS
- Se utiliza para proporcionar cifrado para sitios web (HTTPS)
- Admite certificados TLS públicos y privados
- Gratis para certificados TLS públicos
- Renovación automática del certificado TLS
- Integraciones con (cargar certificados TLS en)
    - Balanceadores de carga elásticos
    - Distribuciones de CloudFront
    - API en API Gateway



Seguridad en AWS

Secret Manager

- Servicio más nuevo, destinado a almacenar secretos
- Capacidad para forzar la rotación de secretos cada X días
- Automatiza la rotación de secretos (usa Lambda)
- Integración con Amazon RDS (MySQL, PostgreSQL, Aurora)
- Los secretos se cifran mediante KMS
- Principalmente destinado a la integración de RDS

Seguridad en AWS

Artifact*

- Portal que brinda a los clientes acceso a pedido a la documentación de cumplimiento de AWS y los acuerdos de AWS
- Informes de artefactos
    - Permite descargar documentos de cumplimiento y seguridad de AWS de auditores externos, como certificaciones ISO de AWS, industria de tarjetas de pago (PCI) e informes de control de sistemas y organizaciones (SOC).
- Acuerdos de artefactos
    - permite revisar, aceptar y realizar un seguimiento del estado de los acuerdos de AWS, como el Anexo para socios comerciales (BAA) o la Ley de portabilidad y responsabilidad de seguros médicos (HIPAA) para una cuenta individual o en su organización
- Se puede utilizar para respaldar la auditoría interna o el cumplimiento

ACADEMIA CONSULTEC

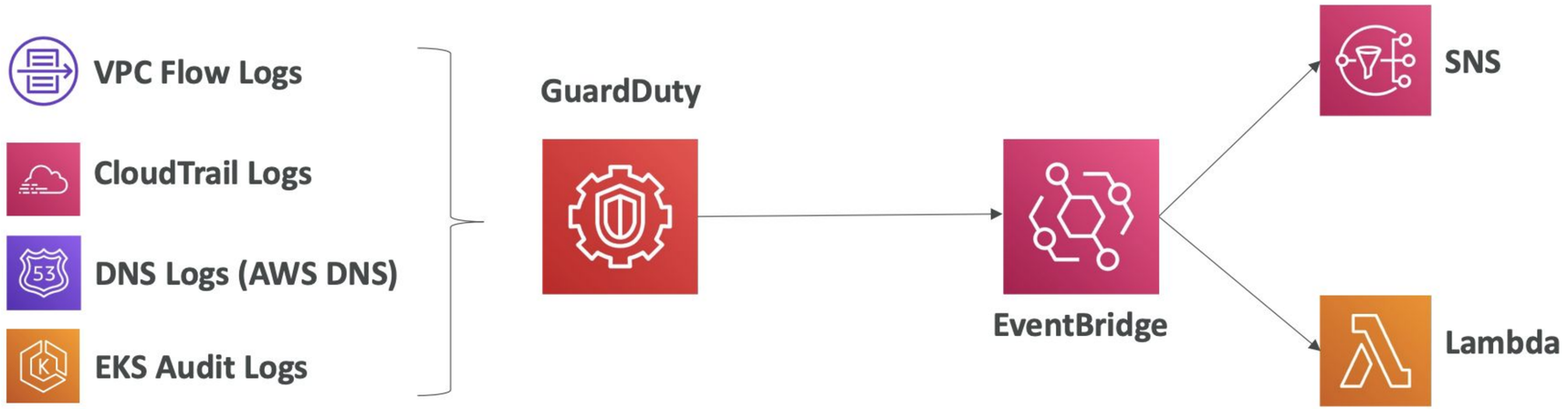
Seguridad en AWS

GuardDuty

- Descubrimiento inteligente de amenazas para proteger su cuenta de AWS
- Utiliza algoritmos de aprendizaje automático, detección de anomalías, datos de terceros
- Habilitar con un clic (prueba de 30 días), sin necesidad de instalar software
- Los datos de entrada incluyen:
    - Registros de eventos de CloudTrail: llamadas API inusuales, implementaciones no autorizadas
        - Logs de CloudTrail
        - Eventos de datos de CloudTrail S3
    - VPC Flows: tráfico interno inusual, dirección IP inusual
    - DNS Logs: instancias EC2 comprometidas que envían datos codificados dentro de consultas de DNS
    - Logs de auditoría de Kubernetes: actividades sospechosas y posibles compromisos del clúster de EKS
- Puede configurar reglas de EventBridge para recibir notificaciones en caso de hallazgos
- Las reglas de EventBridge pueden apuntar a AWS Lambda o SNS
- Puede proteger contra ataques de criptomonedas (tiene un "hallazgo" dedicado para ello)

Seguridad en AWS

GuardDuty

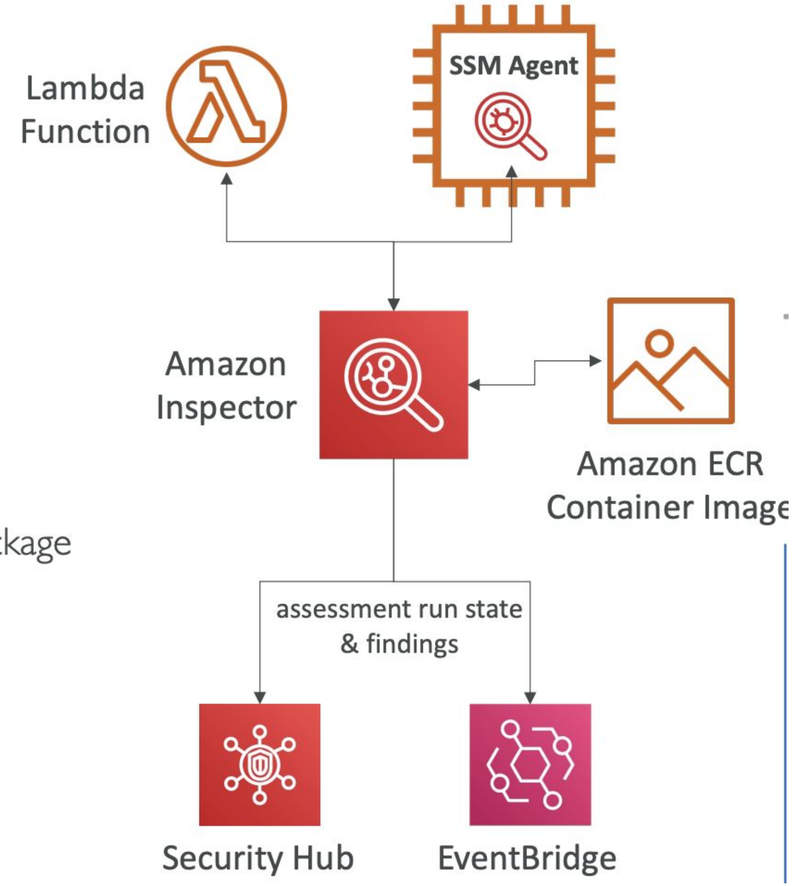


ACADEMIA CONSULTEC

Seguridad en AWS

Amazon Inspector

- Evaluaciones de seguridad automatizadas
- Para instancias EC2
  - Aprovechamiento del agente de AWS System Manager (SSM)
  - Analizar contra la accesibilidad de red no deseada
  - Analice el sistema operativo en ejecución frente a vulnerabilidades conocidas
- Para imágenes de contenedores, envíe a Amazon ECR
  - Evaluación de imágenes de contenedores a medida que se envían
- Para funciones lambda
  - Identifica vulnerabilidades de software en código de función y dependencias de paquetes
  - Evaluación de las funciones a medida que se implementan
- Informes e integración con AWS Security Hub
- Enviar hallazgos a Amazon Event Bridge



ACADEMIA CONSULTEC

Seguridad en AWS

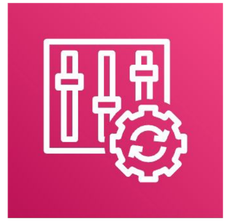
Amazon Inspector

- Recuerde: solo para instancias EC2, imágenes de contenedores y funciones Lambda
- Escaneo continuo de la infraestructura, solo cuando es necesario
- Vulnerabilidades de paquetes (EC2, ECR y Lambda) – base de datos de CVE
- Accesibilidad de red (EC2)
- Una puntuación de riesgo está asociada con todas las vulnerabilidades para la priorización

ACADEMIA CONSULTEC

Seguridad en AWS

AWS Config

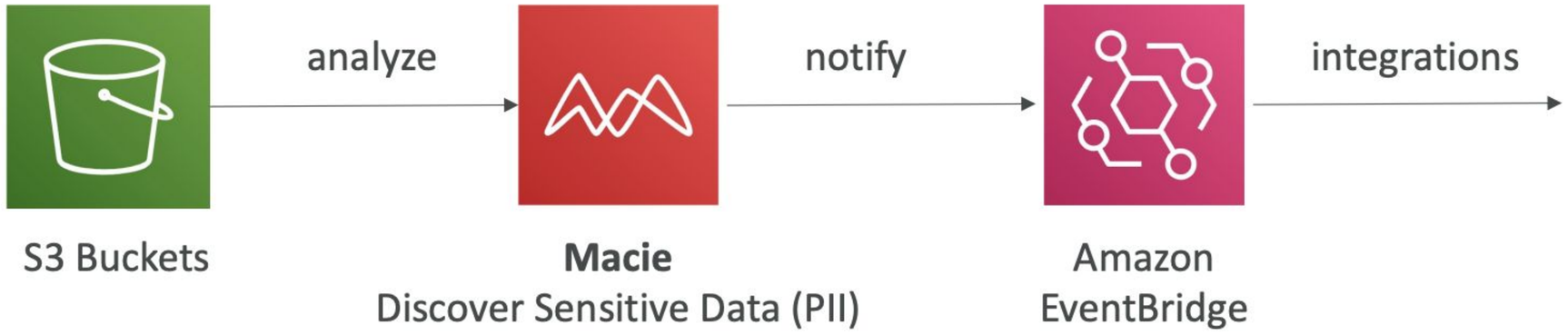


- Ayuda con la auditoría y el registro del cumplimiento de sus recursos de AWS
- Ayuda a registrar configuraciones y cambios a lo largo del tiempo.
- Posibilidad de almacenar los datos de configuración en S3 (analizados por Athena)
- Preguntas que puede resolver AWS Config:
  - ¿Hay acceso SSH sin restricciones a mis grupos de seguridad?
  - ¿Mis buckets tienen acceso público?
  - ¿Cómo ha cambiado mi configuración de ALB con el tiempo?
- Puede recibir alertas (notificaciones SNS) para cualquier cambio
- AWS Config es un servicio por región
- Se puede agregar entre regiones y cuentas

Seguridad en AWS

AWS Macie

- Amazon Macie es un servicio de seguridad y privacidad de datos completamente administrado que utiliza el aprendizaje automático y la coincidencia de patrones para descubrir y proteger sus datos confidenciales en AWS.
- Macie lo ayuda a identificar y alertar sobre datos confidenciales, como información de identificación personal (PII)



Seguridad en AWS

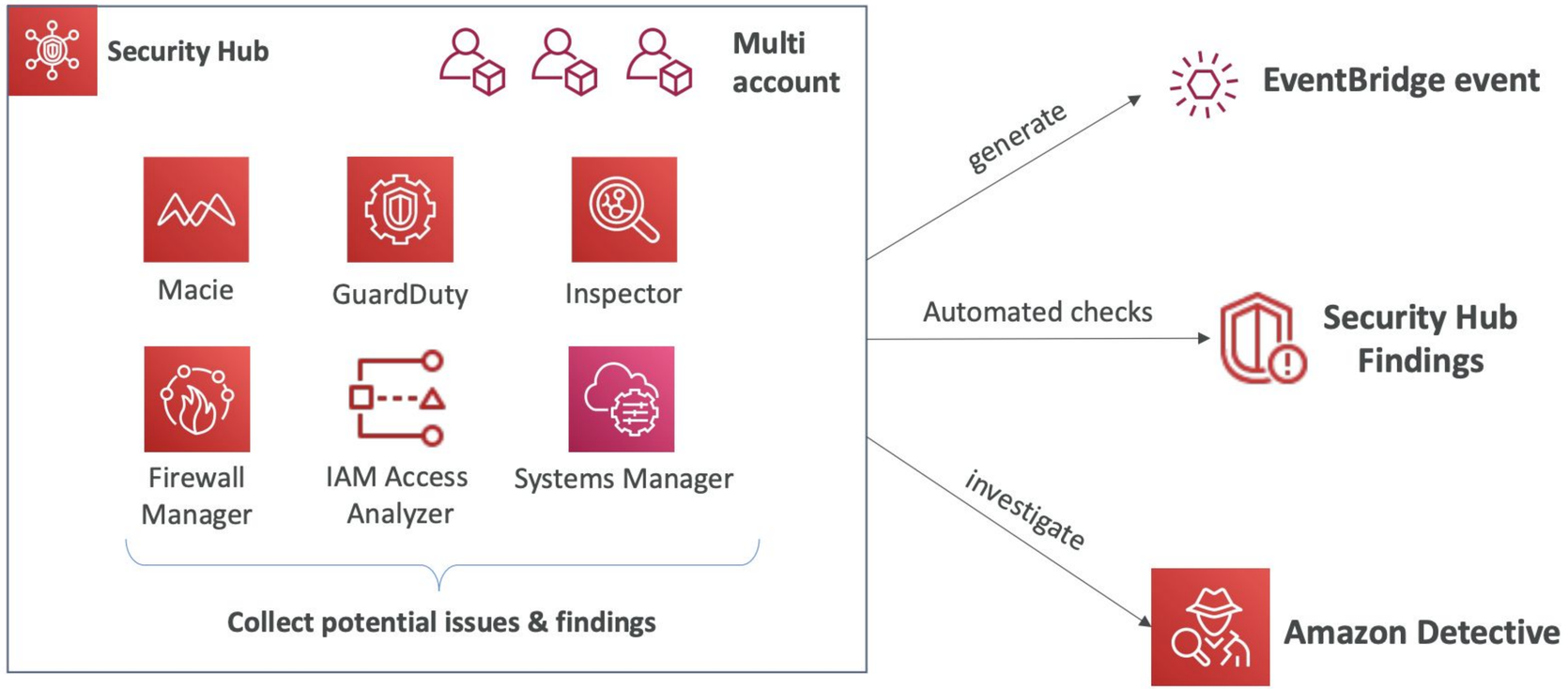
Security Hub

- Herramienta de seguridad central para administrar la seguridad en varias cuentas de AWS y automatizar los controles de seguridad.
- Tableros integrados que muestran el estado actual de seguridad y cumplimiento para tomar medidas rápidamente.
- Agrega automáticamente alertas en formatos de hallazgos personales o predefinidos de varios servicios de AWS y herramientas de socios de AWS:
    - GuardDuty
    - Inspector
    - macie
    - Analizador de acceso de IAM
    - Administrador de sistemas de AWS
    - Administrador de cortafuegos de AWS
    - Soluciones de red de socios de AWS
- Primero debe habilitar el servicio AWS Config

ACADEMIA CONSULTEC

Seguridad en AWS

Security Hub



ACADEMIA CONSULTEC

Seguridad en AWS

Detective

- GuardDuty, Macie y Security Hub se utilizan para identificar posibles problemas de seguridad o hallazgos
- A veces, los hallazgos de seguridad requieren un análisis más profundo para aislar la causa raíz y tomar medidas; es un proceso complejo.
- Amazon Detective analiza, investiga e identifica rápidamente la causa raíz de los problemas de seguridad o actividades sospechosas (usando ML y gráficos)
- Recopila y procesa automáticamente eventos de VPC Flow Logs, CloudTrail, GuardDuty y crea una vista unificada
- Produce visualizaciones con detalles y contexto para llegar a la causa raíz

Seguridad en AWS

Abuse

- Denuncie los recursos de AWS que sospeche que se utilizan con fines abusivos o ilegales
- Los comportamientos abusivos y prohibidos son:
    - Spam: recepción de correos electrónicos no deseados de direcciones IP, sitios web y foros propiedad de AWS enviados como spam por los recursos de AWS
    - Escaneo de puertos: envío de paquetes a sus puertos para descubrir los no seguros
    - Ataques DoS o DDoS: direcciones IP propiedad de AWS que intentan abrumar o bloquear sus servidores/softwares
    - Intentos de intrusión: iniciar sesión en sus recursos
    - Alojamiento de contenido objetable o con derechos de autor: distribución de contenido ilegal o con derechos de autor sin consentimiento
    - Distribución de malware: recursos de AWS que distribuyen software para dañar computadoras o máquinas
- Comuníquese con el equipo de abuso de AWS: Formulario de abuso de AWS, o abuse@amazonaws.com

Seguridad en AWS

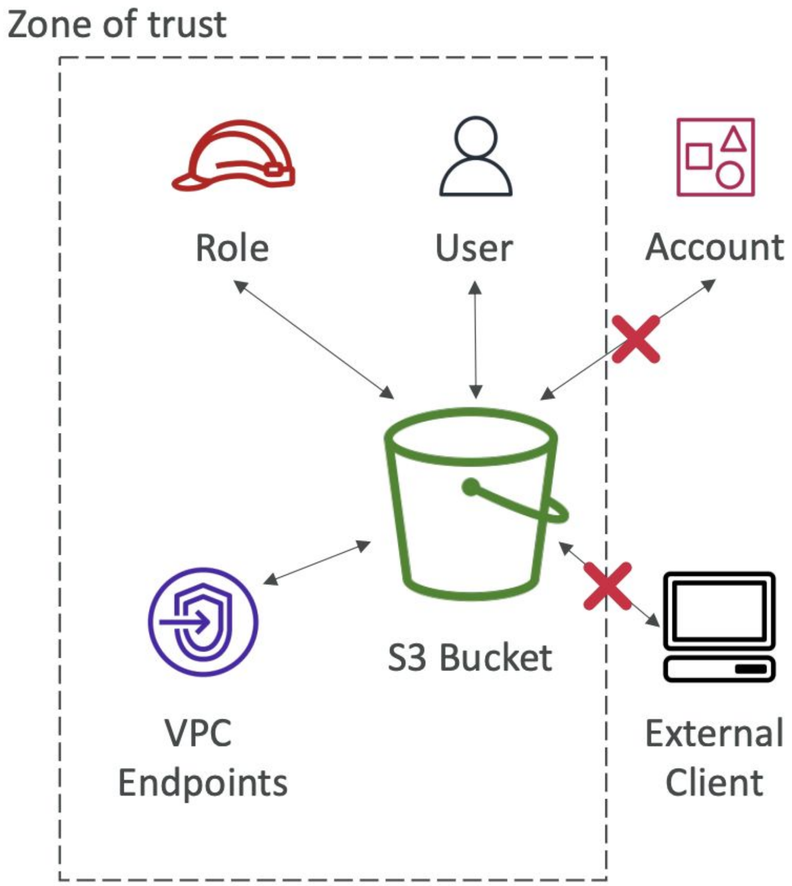
Root Account

- Usuario raíz = Propietario de la cuenta (creado cuando se crea la cuenta)
- Tiene acceso completo a todos los servicios y recursos de AWS
- ¡Guarde bajo llave las claves de acceso de usuario raíz de su cuenta de AWS!
- No utilice la cuenta raíz para tareas cotidianas, incluso tareas administrativas
- Acciones que solo puede realizar el usuario root:
    - Cambiar la configuración de la cuenta (nombre de cuenta, dirección de correo electrónico, contraseña de usuario raíz, claves de acceso de usuario raíz)
    - Ver ciertas facturas de impuestos
    - Cierre su cuenta de AWS
    - Restaurar permisos de usuario de IAM
    - Cambiar o cancelar su plan de AWS Support
    - Regístrese como vendedor en el Marketplace de instancias reservadas
    - Configure un depósito de Amazon S3 para habilitar MFA

Seguridad en AWS

IAM Access Analyzer

- Averigüe qué recursos se comparten externamente
  - Buckets S3
  - Funciones de gestión de identidades y accesos
  - Claves KMS
  - Funciones y capas lambda
  - Colas SQS
  - Secret Manager
- Definir zona de confianza = cuenta de AWS u organización de AWS
- Acceso fuera de la zona de confianza => hallazgos



Seguridad en AWS

Resumen

- Responsabilidad compartida en AWS
- Shield: protección automática contra DDoS + soporte 24/7 para avanzados
- WAF: cortafuegos para filtrar las solicitudes entrantes en función de las reglas
- KMS: claves de cifrado administradas por AWS
- CloudHSM: Cifrado por hardware, gestionamos las claves de cifrado
- AWS Certificate Manager: aprovisiona, administre e implemente certificados SSL/TLS
- Artefact: obtenga acceso a informes de cumplimiento como PCI, ISO, etc.
- GuardDuty: busque comportamientos maliciosos con registros de VPC, DNS y CloudTrail
- Inspector: encuentre vulnerabilidades de software en las funciones EC2, ECR Images y Lambda

Seguridad en AWS

Resumen

- Config: realice un seguimiento de los cambios de configuración y el cumplimiento de las reglas
- Macie: Encuentre datos confidenciales (p. ej., datos PII) en depósitos de Amazon S3
- CloudTrail: rastrea las llamadas a la API realizadas por los usuarios dentro de la cuenta
- Security Hub AWS: recopile hallazgos de seguridad de varias cuentas de AWS
- Amazon Detective: encuentre la causa raíz de los problemas de seguridad o actividades sospechosas
- AWS Abuse: Reporte los recursos de AWS utilizados con fines abusivos o ilegales
- Privilegios de usuario raíz:
    - Cambiar la configuración de la cuenta
    - Cierre su cuenta de AWS
    - Cambiar o cancelar su plan de AWS Support
    - Regístrese como vendedor en el Marketplace de instancias reservadas

Contacto

achacon@consultec-ti.com

info@consultec-ti.com

@consulteclatam

@consultec-ti

consultec-ti.com

Gracias

¡Nos vemos pronto!