CIBERSEGURIDAD
COMO MOTOR DE CONFIANZA EN LAS TELECOMUNICACIONES

Amenazas Emergentes

Construyendo confianza en un panorama digital en evolución.

Mauricio Romero
eddyesco@amazon.com

LATAM – NOLA – Sector Público

La seguridad es ahora un imperativo empresarial

91% Organizaciones que informan al menos un incidente o violación cibernética

56% Organizaciones que informan que sufrieron consecuencias relacionadas en una medida moderada o grande.

70% Organizaciones que informan que la seguridad cibernética estaba en la agenda de su junta directiva de forma regular, ya sea mensual o trimestralmente

Deloitte 2023 Global Future of Cyber Survey

"Hoy en día, estamos viendo el surgimiento de nuevas actitudes poderosas en lo que respecta a la cibernética. Los líderes están mirando la cibernética a través de una lente nueva y nítida, una que revela el valor comercial inherente que puede surgir al incorporar la cibernética. No solo en toda la empresa, sino como parte crucial de una poderosa estrategia de crecimiento".

Emily Mossburg,
Líder Cibernética Global de Deloitte

Panorama de seguridad de las telecomunicaciones

- Existe una expansión de las redes de telecomunicaciones impulsadas por tendencias como BYOD, nuevos tipos de dispositivos conectados y redes de comunicación más amplias.
- Las empresas de telecomunicaciones son atacadas directamente o como un medio para afectar industrias como finanzas, servicios públicos, atención médica y gobierno.
- Cada vez cobra mas relevancia a estas empresas considerar estándares de seguridad de industria (PCI, HIPPA) aplicar controles de seguridad (SOC, ISO) y estándares nacionales de gobierno e industria.

Algunos datos relacionados:

Un tercio de todos los ataques de denegación de servicio distribuido (DDOS) se dirigieron a las empresas de telecomunicaciones *

Se espera que el tamaño del mercado de ciberseguridad de telecomunicaciones alcance los USD 82,64 mil millones para 2030.

En 2021, el 76% de los 500 principales ataques de ciberseguridad se lanzaron contra la infraestructura de telecomunicaciones *.

** Lumen and Deloitte research.*
*** ResearchAndMarkets*

Voz del cliente...

- Se enfrentan a barreras para mantener su postura de seguridad, ya que **carecen de visibilidad de las amenazas cibernéticas** en su patrimonio digital.
- Los actores de **amenazas están utilizando IA, aprendizaje automático y otras tecnologías** para lanzar ataques cada vez más sofisticados.
- Necesitan **consolidar herramientas y plataformas de seguridad** para obtener información procesable de los datos de seguridad.
- La escasez global de **talento cibernético** agrava los desafíos para detectar y responder rápidamente a las amenazas cibernéticas.

Las amenazas cibernéticas están evolucionando rápidamente. El robo de identidad, el fraude, el ransomware, el espionaje y el lavado de dinero están en constante crecimiento.

$4.45M Costo promedio de una violación de datos en 2023.

51% de las organizaciones que planean aumentar las inversiones en seguridad como resultado de la infracción.

Sources: Gartner, Global Enterprise Cyber Security Industry Research Report 2023.
IBM Cost of Data Breach Report 2023

Evolución de las amenazas

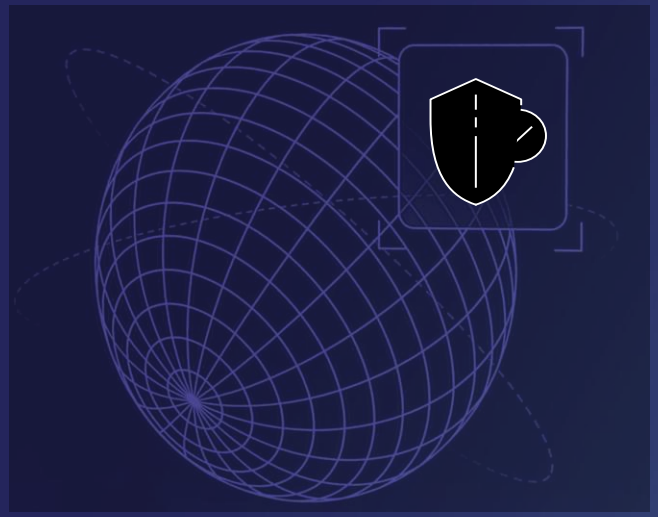
Ataques puntuales

Actores individuales

Desde un garaje

Vectores simples

Habilidades raras



Ataques sostenidos

Grupos organizados

Infraestructura global

Múltiples vectores

Acelerados con IA

Escala de peticiones y amenazas globales

Más de 1 billón de solicitudes de DNS en todas las regiones de AWS todos los días

124.000 nuevos dominios maliciosos detectados de media diaria

Inspeccionado más de
360T
eventos en promedio por día

Observa
750M+
Interacciones de amenazas potenciales diarias

Cada día
400M
Actividades clasificadas como maliciosas diarias

Tendencias de la industria que observamos para DDoS

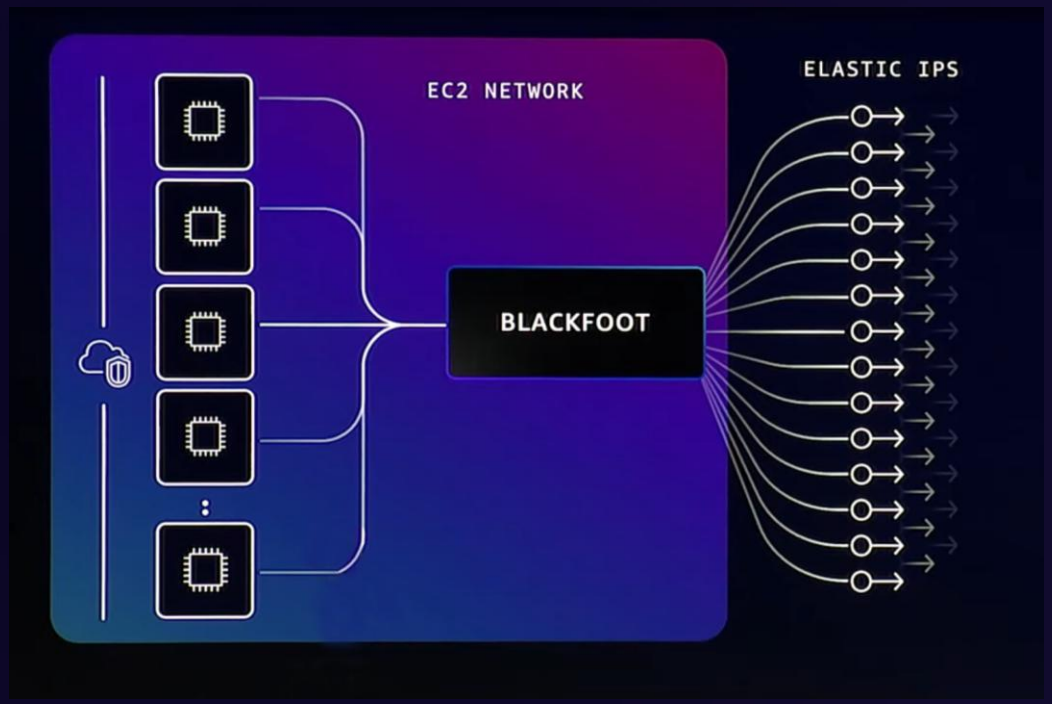
- **Extorsión:** Negocios nativos digitales como el comercio electrónico o los juegos en línea
- **Competencia:** individuo/empresa utiliza el evento DDoS contra el sitio web de la competencia para apoderarse de sus clientes. Esto es común en la industria del juego.
- **Hacktivismo:** objetivos DDoS con fines políticos o sociales, por ejemplo: Operación Megaupload, Universal Music Group, Departamento de Justicia de EE. UU., RIAA
- **Guerra cibernética:** actor estatal lanza evento DDoS contra oponente

Takeaway:

El volumen de amenazas está aumentando y la naturaleza de las amenazas está evolucionando para centrarse más en las aplicaciones

Escala de las amenazas en la red de AWS

PROTECCION E INTELIGENCIA DE RED DE HONEYPOT DINÁMICO



13T
Flujos por hora

10K+
Madpots concurrentes en cualquier momento

90s/3min
Inicia escaneo / completa exploit

12.5%
IP bloqueadas cambian cada 3 minutos

2.4T
Solicitudes de análisis maliciosas evitadas en 6 meses

Hallazgos de secuencias de ataque en los principales escenarios de amenazas

Identidad comprometida

Credenciales de IAM utilizadas para realizar múltiples solicitudes sospechosas que se alinean con comportamientos de ataque conocidos, como persistencia, evasión y creación de cargas de trabajo

Datos comprometidos

Secuencia de acciones que sugieren el compromiso o la exfiltración de datos en uno o más buckets de S3 mediante credenciales potencialmente utilizadas indebidamente

Host comprometido

Secuencia detectada en una instancia EC2, como ejecuciones de comandos sospechosas seguidas de la ejecución de archivos maliciosos y conexión con un grupo de criptominería conocido

Tres enfoques de seguridad de IA generativa - 1

- Tres formas de pensar en la IA generativa + seguridad

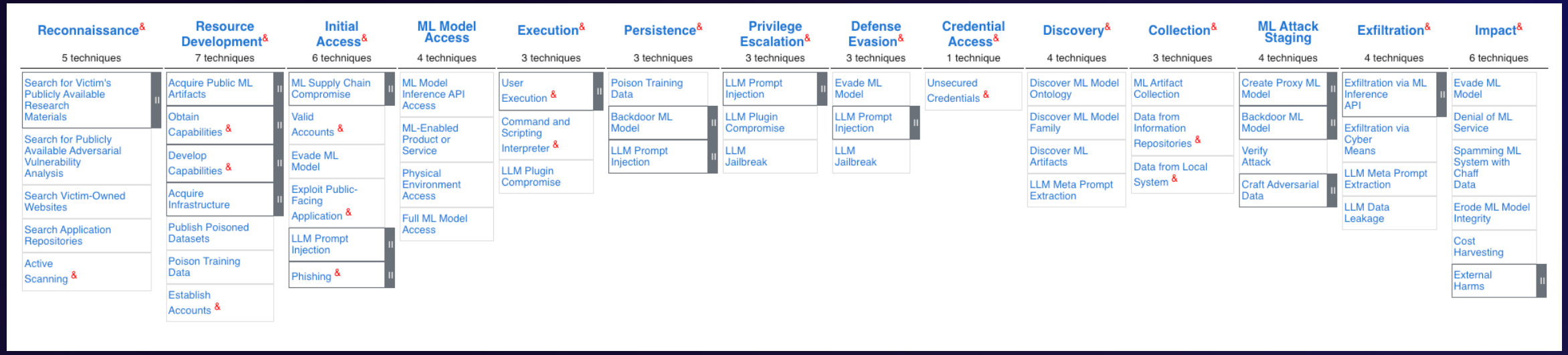
Seguridad de la IA generativa

¿Cómo protejo mis aplicaciones empresariales que aprovechan la IA generativa?

MITRE ATLAS™

MITRE ATLAS™ (ADVERSARIAL THREAT LANDSCAPE FOR ARTIFICIAL-INTELLIGENCE SYSTEMS)

MITRE ATLAS™ es una base de conocimientos viva y accesible a nivel mundial de las tácticas y técnicas de los adversarios contra los sistemas habilitados para IA basada en observaciones de ataques del mundo real y demostraciones realistas de equipos y grupos de seguridad de IA.



Source: https://atlas.mitre.org/

OWASP® Top for 10 Large Language Models

- Algunos artículos requieren algo más que contramedidas técnicas

LLM01

Prompt Injection

Esto manipula un lenguaje grande (LLM) a través de entradas astutas, causando acciones no deseadas por parte del LLM. Las inyecciones directas sobrescriben los avisos del sistema, mientras que las indirectas manipulan las entradas de fuentes externas.

LLM02

Insecure Output Handling

Esta vulnerabilidad ocurre cuando se acepta una salida de LLM sin escrutinio, exponiendo los sistemas backend. El uso indebido puede tener consecuencias graves como XSS, CSRF, SSRF, escalada de privilegios o ejecución remota de código.

LLM03

Training Data Poisoning

Esto ocurre cuando se manipulan los datos de entrenamiento de LLM, introduciendo vulnerabilidades o sesgos que comprometen la seguridad, la eficacia o el comportamiento ético.

LLM04

Model Denial of Service

Los atacantes provocan operaciones que consumen muchos recursos en los LLM, lo que lleva a la degradación del servicio o a altos costos. La vulnerabilidad se magnifica debido a la naturaleza intensiva en recursos de los LLM y la imprevisibilidad de las entradas de los usuarios.

LLM05

Supply Chain Vulnerabilities

El ciclo de vida de las aplicaciones de LLM puede verse comprometido por componentes o servicios vulnerables, lo que lleva a ataques de seguridad. El uso de conjuntos de datos de terceros, modelos preentrenados y complementos puede agregar vulnerabilidades.

LLM06

Sensitive Information Disclosure

Los LLM pueden revelar inadvertidamente datos confidenciales en sus respuestas, lo que lleva a un acceso no autorizado a los datos, violaciones de la privacidad y violaciones de seguridad. Es crucial implementar la desinfección de datos y políticas estrictas de usuario para mitigar esto.

LLM07

Insecure Plugin Design

Los complementos LLM pueden tener entradas inseguras y un control de acceso insuficiente. Esta falta de control de aplicaciones hace que sean más fáciles de explotar y puede tener consecuencias como la ejecución remota de código

LLM08

Excessive Agency

Los sistemas basados en LLM pueden emprender acciones que conducen a consecuencias no deseadas. El problema surge de la funcionalidad, los permisos o la autonomía excesivos otorgados a los sistemas basados en LLM.

LLM09

Overreliance

Los sistemas o las personas que dependen demasiado de los LLM sin supervisión pueden enfrentar información errónea, falta de comunicación, problemas legales y vulnerabilidades de seguridad debido a contenido incorrecto o inapropiado generado por los LLM.

LLM10

Model Theft

Esto implica el acceso no autorizado, la copia o la exfiltración de modelos LLM patentados. El impacto incluye pérdidas económicas, ventaja competitiva comprometida y acceso potencial a información confidencial.

Source: https://owasp.org/www-project-top-10-for-large-language-model-applications/

Tres enfoques de seguridad de IA generativa - 2

- Tres formas de pensar en la IA generativa + seguridad

Seguridad de la IA generativa

IA generativa en la seguridad

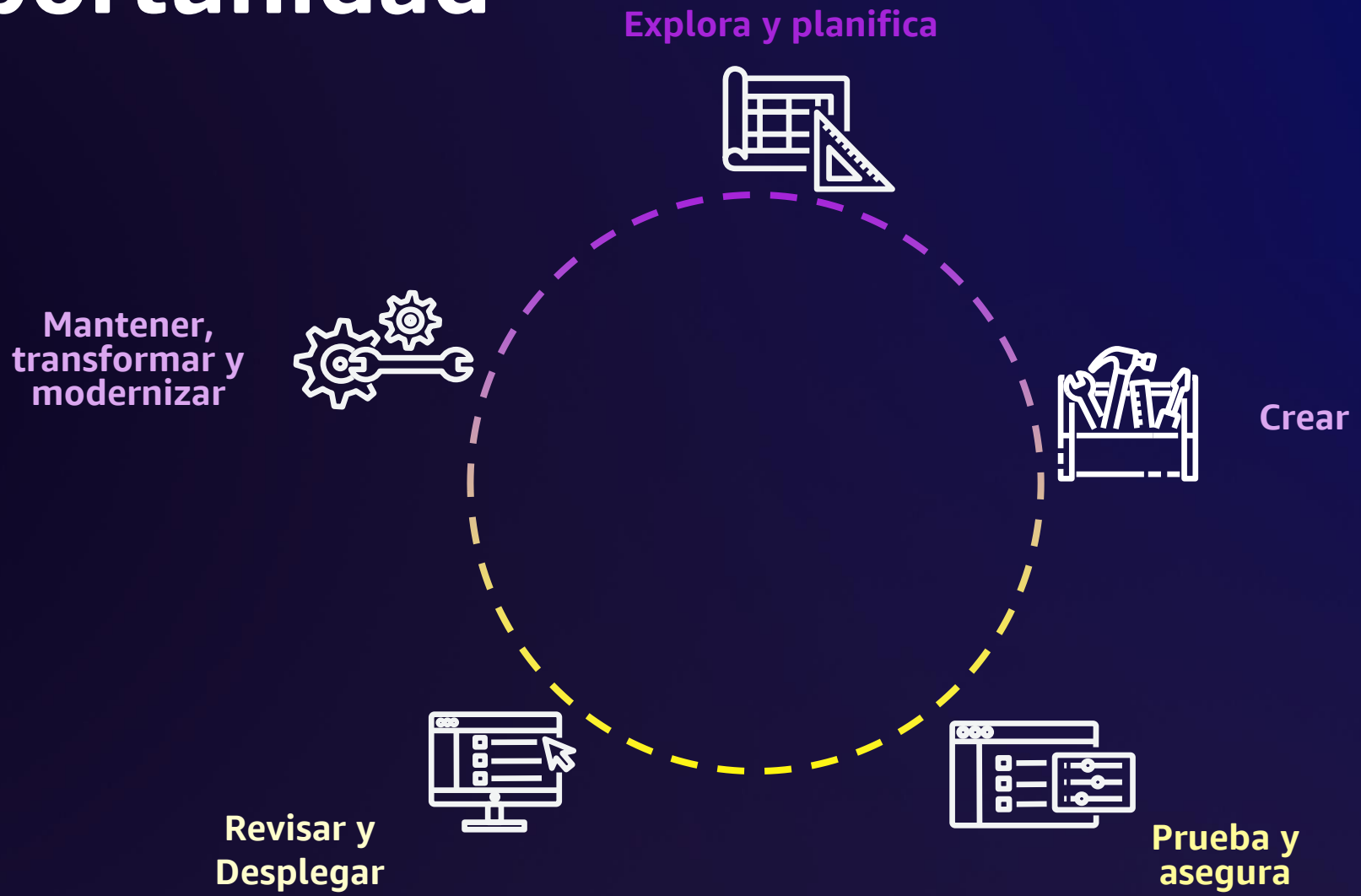
¿Cómo utilizar la IA generativa?
para minimizar las vulnerabilidades,
las amenazas y los riesgos?

La IA generativa puede empoderar a los equipos

Source: IDC - New Use Cases for Generative AI in Security Analytics

Amenaza y oportunidad

IA Generativa en el ciclo de vida del software



Tres enfoques de seguridad de IA generativa - 3

- Tres formas de pensar en la IA generativa + seguridad

Seguridad de la IA generativa

IA generativa en la seguridad

Seguridad frente a amenazas generativas impulsadas por IA

¿Cómo protegerme contra los actores de amenazas que emplean la IA generativa?

Potenciales amenazas impulsadas por IA

UNA LISTA NO EXHAUSTIVA

Denegación de servicio

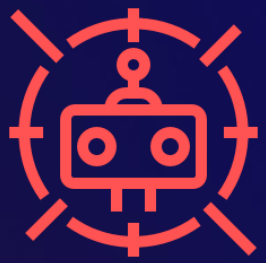
- SYN Floods
- Reflection Attacks
- Web Request Floods

Vulnerabilidades de aplicaciones

- SQL Injection
- Cross-site Scripting (XSS)
- OWASP Top 10
- Common Vulnerabilities and Exposures (CVE)
- Privilege Escalation
- Data Exfiltration

Buenos bots

- Search Engine Crawling
- Website Health Monitoring
- Vulnerability Scanning



Bad Bots

- Comment Spam
- SEO Spam
- Fraud
- Account Takeover

Threath Intelligence como estrategia

COMO GUARDDUTY APROVECHA IA PARA PREVENIR LOS ATAQUES IMPULSADOS POR AI Y ESCALA GLOBAL

Alerta temprana

Una red neuronal proporciona inteligencia de amenazas de 182k nuevos dominios maliciosos por día a Amazon GuardDuty

Tácticas emergentes

Observamos más de 100 millones de amenazas potenciales todos los días en todo el mundo, con aproximadamente 500,000 de esas actividades observadas clasificadas como maliciosas.

Prevención automática

Activamos protecciones automatizadas con una precisión del 99,998 % en AWS Shield, Amazon Virtual Private Cloud (2,6T), Amazon S3 (24B) y AWS WAF

“Todo falla, todo el tiempo”

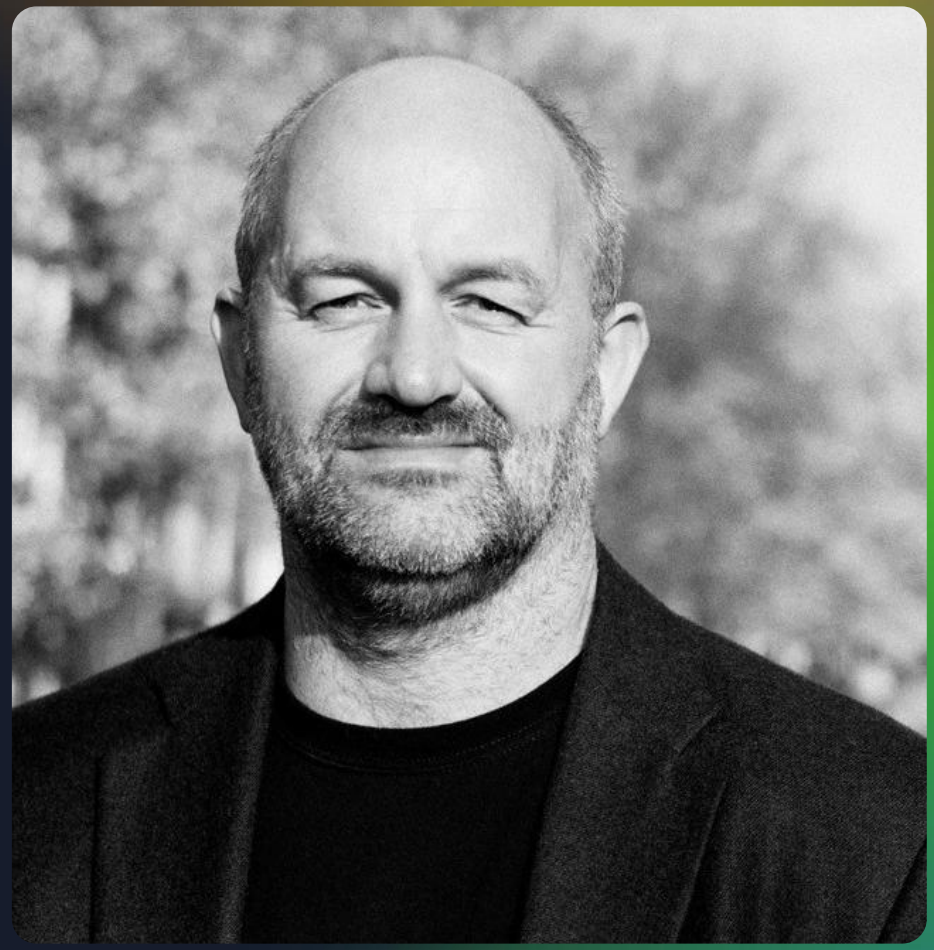
Puntos únicos de falla

Carga excesiva

Configuración incorrecta y errores

Amenazas

Destino compartido



Werner Vogels CTO, Amazon.com

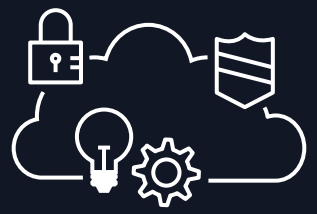
Resiliencia

CAPACIDAD DE UNA CARGA DE TRABAJO PARA
RECUPERARSE DE INTERRUPCIONES DE INFRAESTRUCTURA O SERVICIO

El modelo mental

Alta disponibilidad

Resistencia a fallas comunes a través de mecanismos de diseño y operación en un sitio primario



Servicios principales, objetivos de diseño para cumplir con los objetivos de disponibilidad

Recuperación ante desastres

Volver al funcionamiento dentro de destinos específicos en un sitio de recuperación para fallas que HA no puede manejar

Objetivos de copia de seguridad y recuperación, abastecimiento de datos, recuperación gestionada

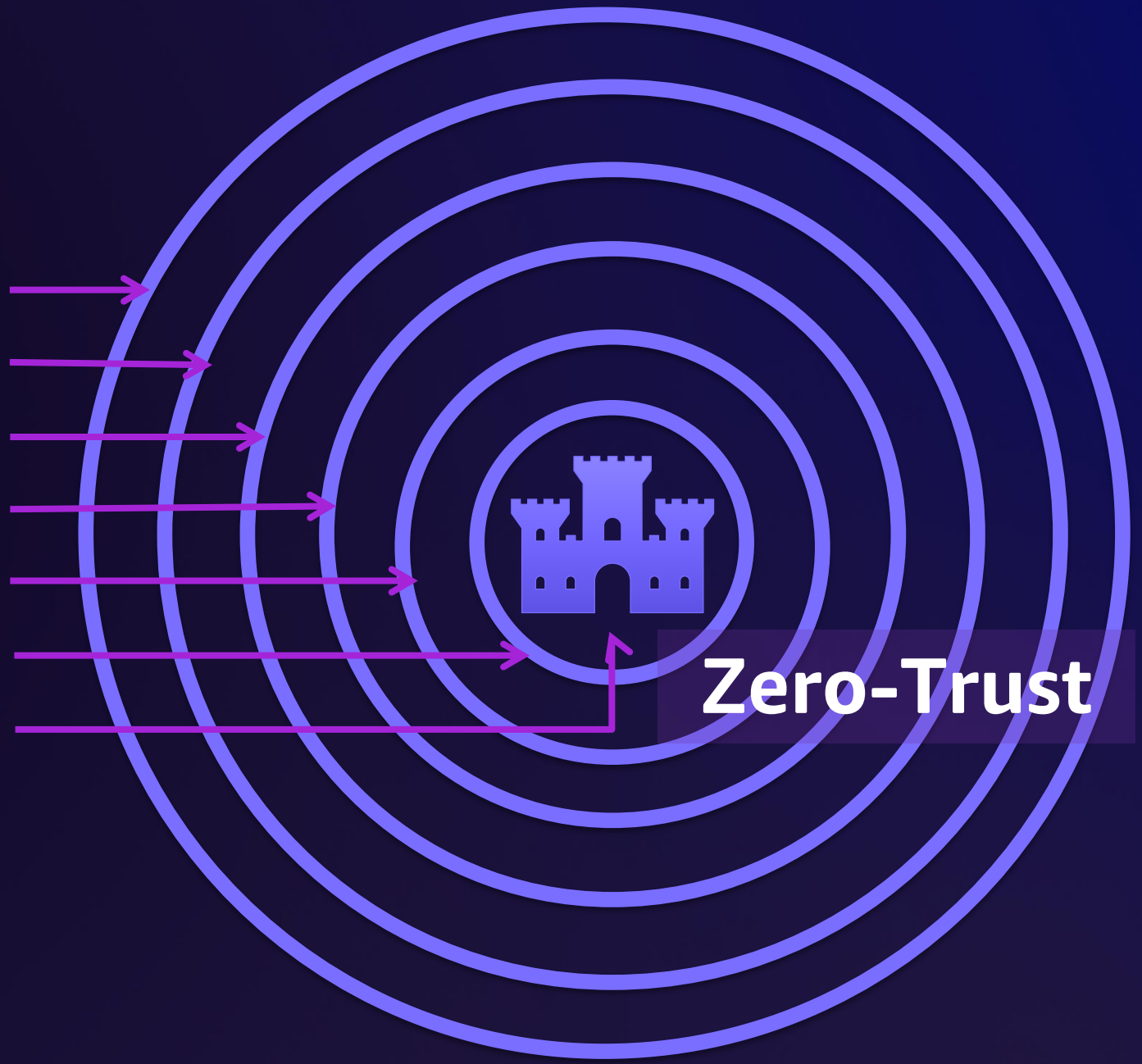
Mejora continua

CI/CD, observabilidad, más allá de las pruebas hacia patrones de ingeniería del caos

Estrategia de defensa

DEFENSA EN PROFUNDIDAD + ZERO-TRUST

- Policies, Procedures & Awareness
- Network & Edge Protection
- Identity & Access Management
- Threat Detection & Incident Response
- Infrastructure Protection
- Application Protection
- Data Protection



Matriz de alcance de seguridad de IA generativa

SCOPE 1	SCOPE 2	SCOPE 3	SCOPE 4	SCOPE 5
APLICACIÓN PARA EL CONSUMIDOR	APLICACIÓN EMPRESARIAL	MODELOS PREENTRENADOS	MODELOS AJUSTADOS	MODELOS AUTOENTRENADOS

GOBERNANZA Y CUMPLIMIENTO | LEGAL Y PRIVACIDAD | GESTIÓN DE RIESGOS | CONTROLES | RESILIENCIA

PROTECCIÓN DE LA IA GENERATIVA

EVALUAR EL RIESGO DE TERCEROS EMPLEANDO LOS MARCOS DE GESTIÓN DE RIESGOS Y MECANISMOS DE ADQUISICIÓN

"Brindar servicios seguros y operativamente excelentes para nuestros clientes es, y siempre será, nuestra principal prioridad."

Matt Garman
Chief Executive Officer
Amazon Web Services

Gracias

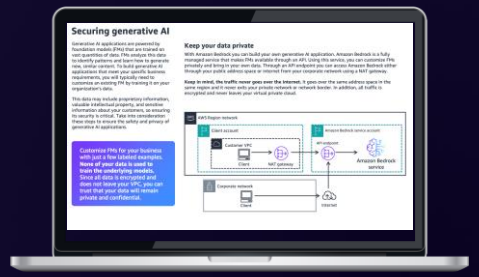
Feedback
https://pulse.aws/survey/WQURD8TF

Mauricio Romero
eddyesco@amazon.com
LinkedIn: RomeroGT

Apéndice
Recursos adicionales

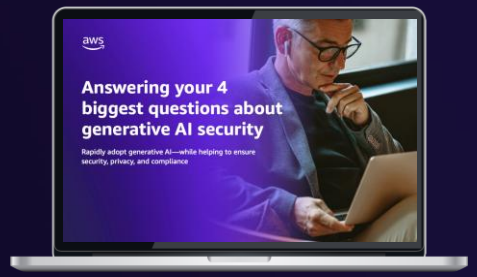
Recursos adicionales de AWS para comenzar

INFOGRAFÍAS, LIBROS ELECTRÓNICOS Y BLOGS DE AWS



Infographics

How AWS Securing the Future of Generative AI

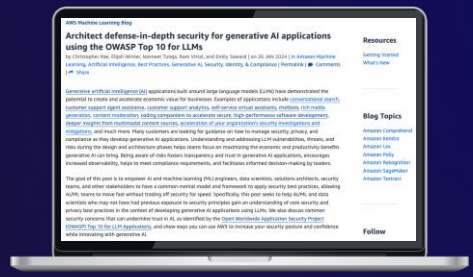


eBooks

Answering your 4 biggest questions about generative AI Security

The future of generative AI is secure - With AWS

Accelerate machine learning innovation through security

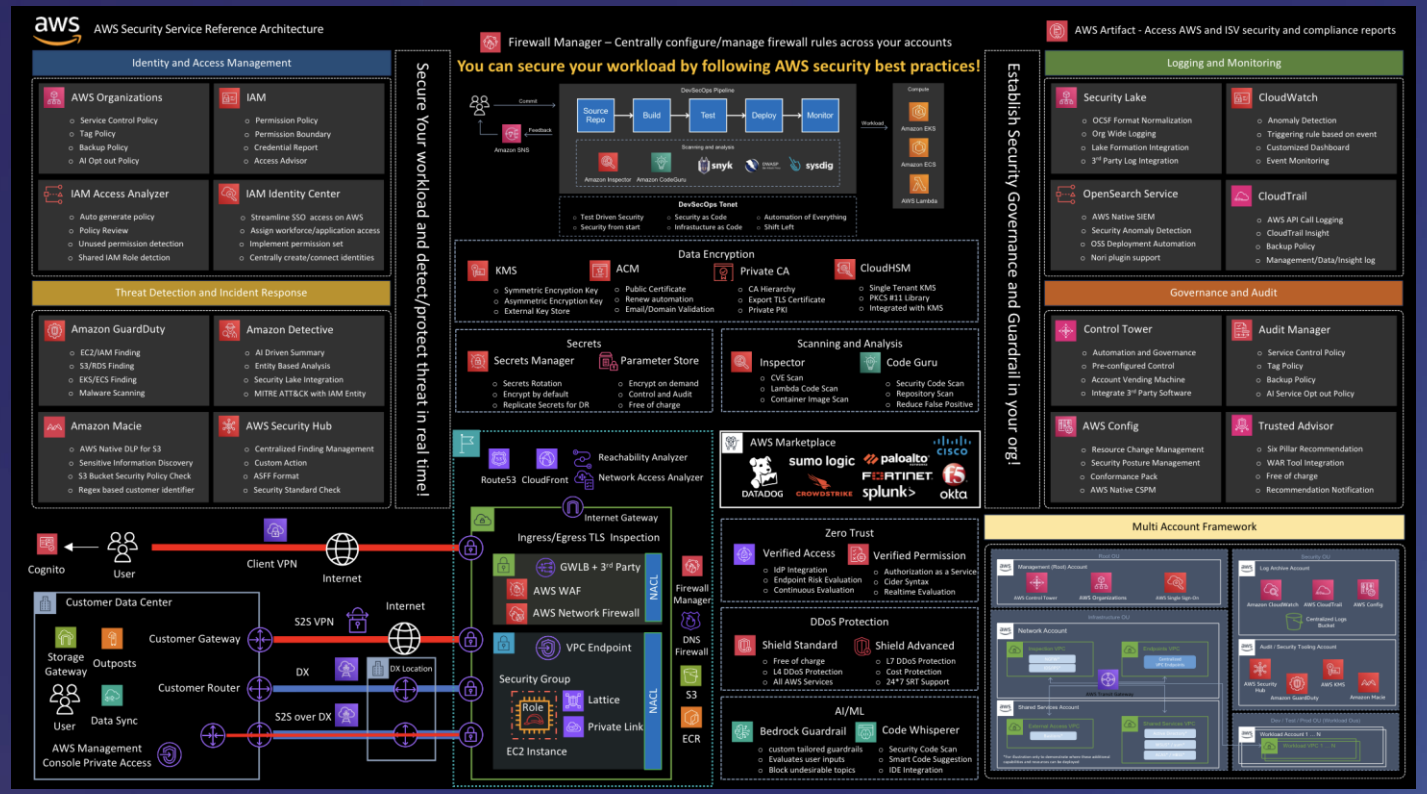


AWS Blogs

- Securing generative AI: An introduction to the Generative AI Security Scoping Matrix
- Architect defense-in-depth security for generative AI applications using the OWASP Top 10 for LLMs
- Securing generative AI: Applying relevant security controls
- Automate and enhance your code security with AI powered services

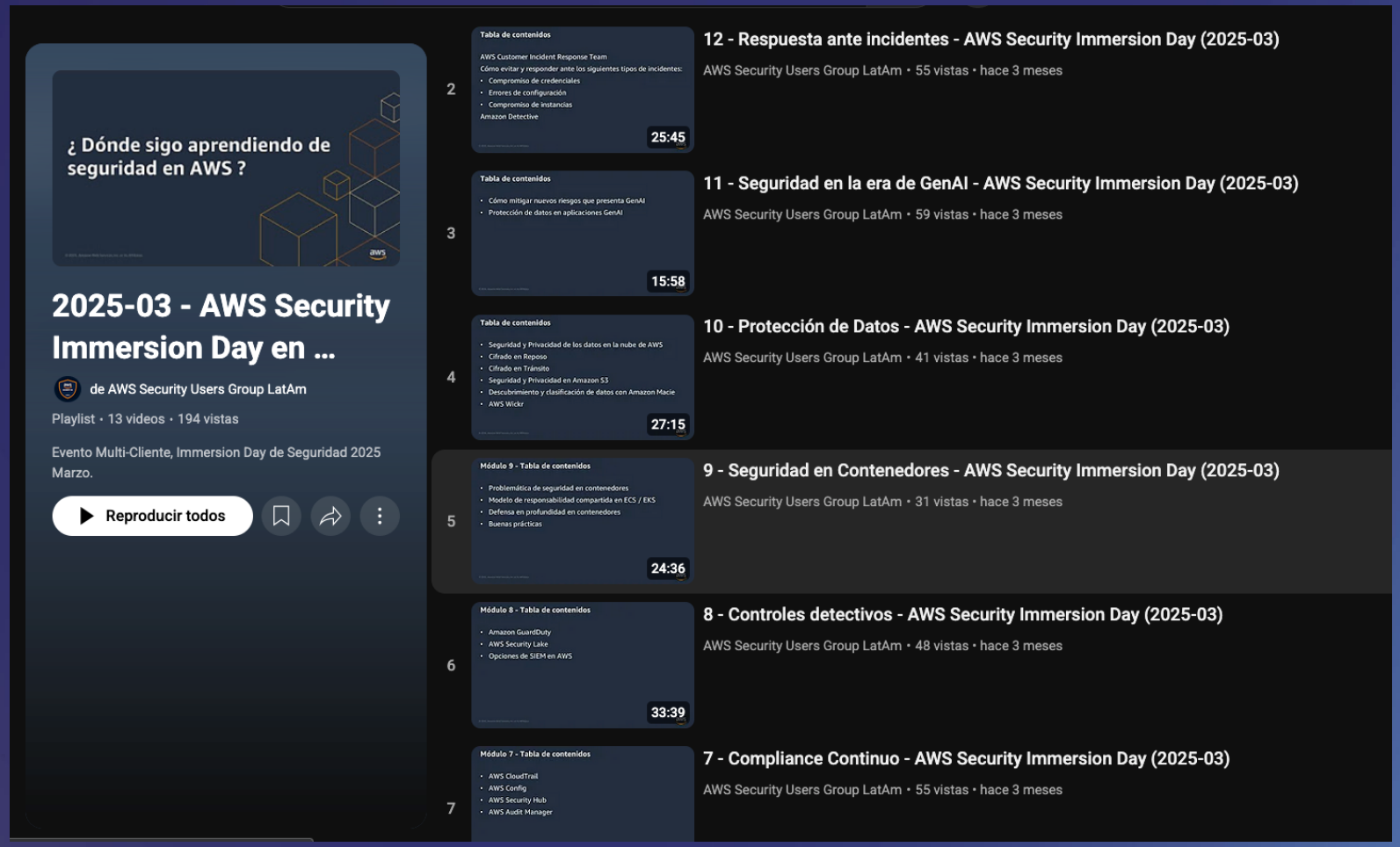
https://aws.amazon.com/ai/generative-ai/security/

Recurso: Arquitectura de referencia de seguridad



- Definir arquitectura de seguridad estado objetivo
- Revisar e implementar seguridad ya existente
- Implementar infraestructura como código de inicio
- Impulsar discusiones sobre gobernanza de seguridad

AWS Security Immersion Day en español



https://bit.ly/46kaDGX

Otros recursos disponibles

Top re:Inforce 2025 Announcements Blog

AWS Security Activation Days

Session Replays on AWS Events YouTube

Become an AWS Security Champion

AWS LEARNING PLAN

- Earn the AWS Digital Knowledge Security Champion Badge
- Deepen your security skills with digital learning on demand and hands-on interactive content
- Join the **AWS learners community** and get exclusive benefits

TRAIN NOW