



AWS
re:Inforce

JUNE 16 - 18, 2025 | PHILADELPHIA, PA

AWS re:Inforce A LA CARTA



where your presentation begins



ME PRESENTO:



Martín Ferrini - @martincho5

- Lead Cloud Engineer en Cloudhesive.
- +2 décadas trabajando en infraestructuras On-Premise y Cloud.
- Docente Universitario.
- Apasionado por la tecnología y la seguridad informática.
- Familiarero (5 hijos).



¿Qué es ^{AWS}re:Inforce ?

Evento anual de seguridad en la nube organizado por Amazon Web Services (AWS).

Está enfocado en proporcionar a los profesionales de seguridad las herramientas y conocimientos necesarios para proteger sus cargas de trabajo en la nube. El evento incluye sesiones técnicas, talleres, demostraciones y oportunidades para interactuar con expertos de AWS y otros profesionales del sector.

En 2025 se realizó en Philadelphia del 16 al 18 de Junio



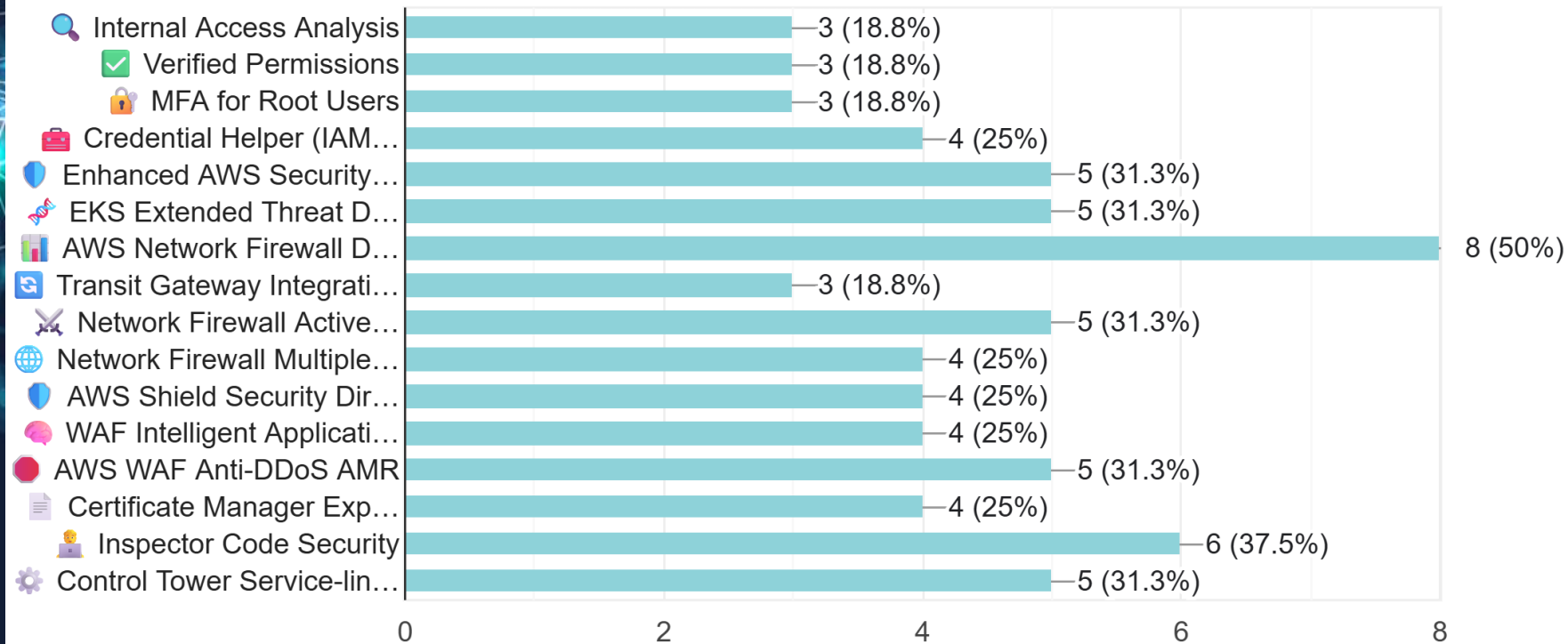
AWS re:Inforce 2025 Keynote with Amy Herzog



¿Cómo terminó la encuesta?

¿Qué tema te gustaría que abordemos en la próxima sesión? Seleccioná uno o más de los siguientes: 📍

16 respuestas



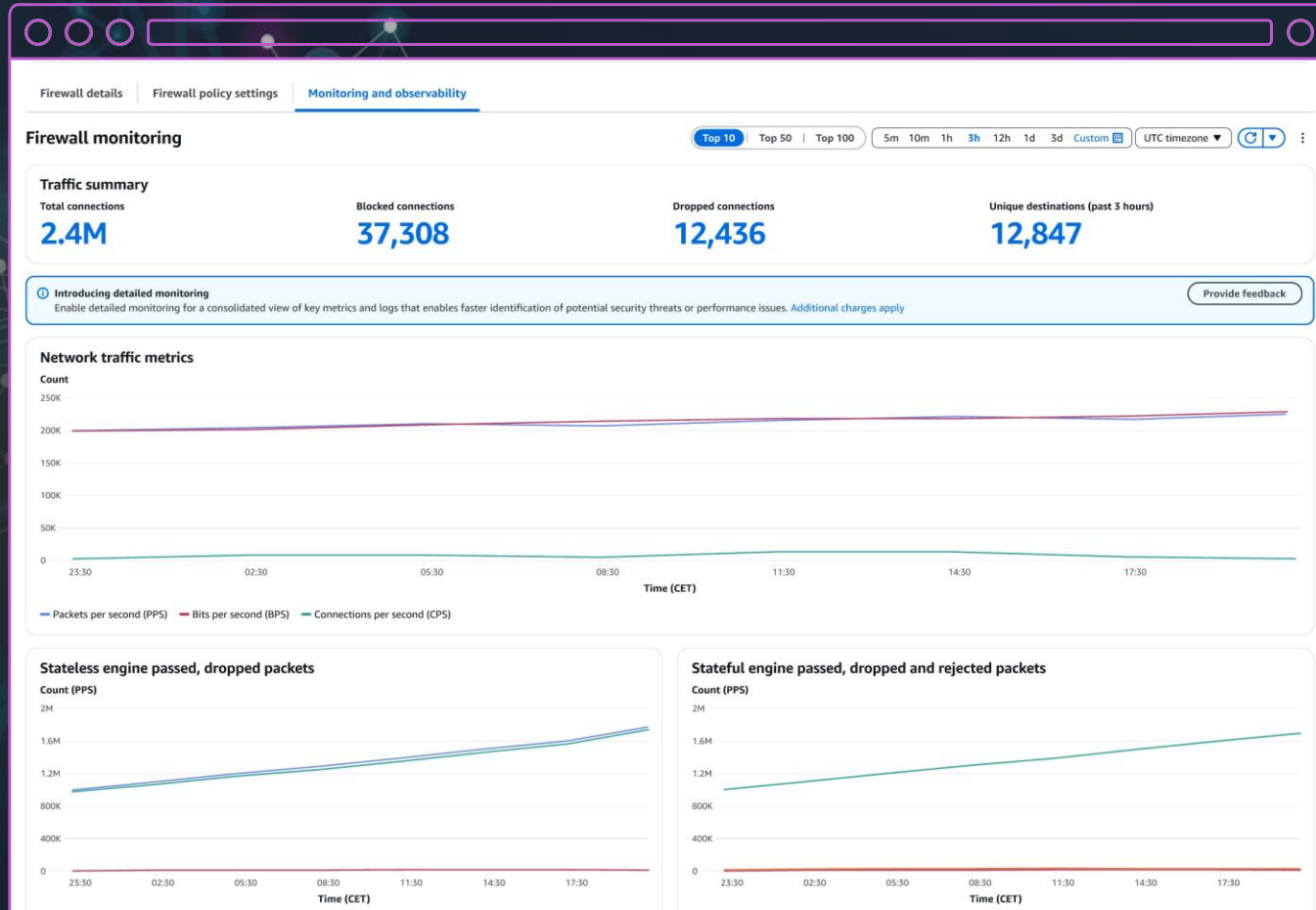
01



AWS Network Firewall Dashboard

AWS Network Firewall Dashboard para mejorar la Observabilidad

Mejor visibilidad de los principales generadores de tráfico y conteo de reglas aplicadas para ayudar a gestionar mejor las reglas del firewall



- ✓ Visibilidad de métricas y conocimiento del tráfico
- ✓ Optimización de la creación y validación de reglas
- ✓ Visualización de los principales generadores de tráfico, dominios bloqueados y conteo de reglas aplicadas

Más info

<https://aws.amazon.com/about-aws/whats-new/2025/06/aws-network-firewall-monitoring-dashboard/>



Demo



AWS Network Firewall Dashboard

02



Inspector Code Security

Amazon Inspector Code Security brinda seguridad en todo el stack de código



Escanea el código en todo el stack para encontrar vulnerabilidades

Identifica dependencias vulnerables en paquetes de código abierto

Genera correcciones de código alineadas con las mejores prácticas de seguridad, en tiempo real

Proporciona un panel unificado para gestionar la seguridad en todos los repositorios

Más info

<https://aws.amazon.com/blogs/security/shifting-vulnerability-detection-left-with-amazon-inspector-code-security-capabilities/>



Scan frequency

Specify how often the code is scanned.

- ☒ **Change-based and periodic scanning**
Scan code whenever it is modified and on a periodic basis.
Recommended

☐ Customize scanning types and triggers

Change-based and periodic scanning

- ✔ Scan code whenever there is a pull or merge request.
- ✔ Scan code on a recurring basis

Periodic scanning

- ☒ Enable periodic scanning
- ☐ Disable periodic scanning

Set the scan frequency

Weekly ▼

On day

Monday ▼

Scan analysis

Choose at least one type of analysis.

- ☒ **Complete scanning analysis**
Recommended

☐ Customized scanning analysis

Complete analysis

All scanning analysis options will be applied.

- ✔ Static Application Security Testing
- ✔ IaC scanning
- ✔ Software composition analysis

CWE-284 - Public READ bucket ACL

Finding ID: [arn:aws:inspector2:us-east-1:](#)

The Bucket ACL allows public READ permission. Make sure that bucket ACL prohibits READ permission to everyone.

Finding overview

AWS account ID	
Severity	Critical
Type	Code Vulnerability
Detector name	Public READ bucket ACL
Relevant CWE	CWE-284
Rule ID	cloudformation-public-read-bucket-acl
Detector tags	#aws-cloudformation, #security
Fix available	Yes
Created at	June 10, 2025 8:13 PM (UTC+01:00)

Vulnerability details

File path	cloudformation/template.yaml
-----------	------------------------------

Vulnerability location

```
89     DBSubnetGroupDescription: Subnet group for vulnerable DB
90     SubnetIds:
91       - !Ref VulnerablePublicSubnet
92       - !Ref VulnerableSecondarySubnet
93     # VULNERABILITY: S3 bucket with public access
94     VulnerableBucket:
95       Type: AWS::S3::Bucket
96       Properties:
97         BucketName: vulnerable-demo-bucket-cf
98         AccessControl: PublicRead
99       # VULNERABILITY: No encryption configured
100      # VULNERABILITY: No versioning configured
101
102     # VULNERABILITY: Overly permissive bucket policy
103     VulnerableBucketPolicy:
```

Suggested remediation: Showing 1/1
fixes

[Download](#) < 1 >

Why are we recommending the following fix?

Ensure the S3 bucket does not allow READ permissions to everyone Make sure that AccessControl is not set toPublicReadWrite or PublicRead.

97	97	BucketName: vulnerable-demo-bucket-cf
98	-	AccessControl: PublicRead
98	+	AccessControl: <set value other than PublicRead or PublicReadWrite>
99	99	# VULNERABILITY: No encryption configured

Resource affected

Demo



Inspector Code Security

03



Enhanced AWS Security Hub

Unified security with enhanced AWS Security Hub (public preview)

- ✓ Proporciona visibilidad integral en todo tu entorno de AWS
- ✓ Ayuda a comprender el alcance completo de los posibles impactos
- ✓ Utiliza análisis avanzados para identificar lo que realmente importa
- ✓ Acelera el tiempo de remediación de los problemas de seguridad



Summary

Region: us-east-1 (home Region)

[Reset to default layout](#)

[+ Add widget](#)

[+ Create Custom Widget](#)

Save filter sets

[Choose a filter set](#)

[Add filter](#)

Threat summary

A threat finding is an event with the potential to adversely impact operations, assets, or individuals. Top severity detections are listed below.



Findings

Severity ▾

🔗 Potential data compromise of one or more S3 buckets involving a sequence of actions associated with AssumedRole/GenerateAttackSequence-attacksequencesroleBD719EC5-hiNhuBhXL3wh.

Critical

🔗 Potential data compromise of one or more S3 buckets involving a sequence of actions associated with AssumedRole/GenerateAttackSequence-attacksequencesroleBD719EC5-hiNhuBhXL3wh.

Critical

[View all threats](#)

Exposure summary

An exposure finding is a correlation of multiple security findings, resource relationships and configurations. The exposure findings with the greatest severity and most findings are listed below.



Exposure

Severity ▾

Count ▾

🔗 Potential Unauthorized Access: IAM user has administrative access policy, weak password policies, and MFA disabled

Critical

[More](#)

5

🔗 Potential Credential Stealing: Internet reachable EC2 instance with administrative instance profile has network-exploitable software vulnerabilities with a high likelihood of exploitation

Critical

4

[View all exposure findings](#)

Resource summary

View resources prioritized by exposures, threats, and severity of findings. This widget cannot be filtered. To apply filters, see our Resources page.

Resource	Resource type	Findings
attacked-bucket-us-east-1-ojkt5h	AWS::S3::Bucket	2 exposure findings 1 attack sequence finding 29 other findings
attacked-bucket-us-east-1-liikdp	AWS::S3::Bucket	2 exposure findings 1 attack sequence finding 28 other findings
attacked-bucket-us-east-1-v49qdg	AWS::S3::Bucket	2 exposure findings 1 attack sequence finding 28 other findings
attacked-bucket-us-east-1-	AWS::S3::Bucket	2 exposure findings 1 attack sequence finding

[View all resources](#)

Security coverage

Track the status of AWS security capabilities across your environment.

Security capability	Account coverage	Actions
Vulnerability management By Amazon Inspector	<div><div></div></div> 33% covered	⋮
Threat detection By Amazon GuardDuty	<div><div></div></div> 86% covered	⋮
Sensitive data discovery By Amazon Macie	<div><div></div></div> 50% covered	⋮
Posture management By AWS Security Hub	<div><div></div></div> 75% covered	⋮

Covered Not covered

AWS Security Hub

Consola Unificada

Vista centralizada de las capacidades de seguridad con un panel integrado para amenazas, exposiciones y operaciones de seguridad



Potential Credential Stealing: Internet reachable EC2 instance with administrative instance profile has network-exploitable software vulnerabilities with a high likelihood of exploitation

[View JSON](#)[Actions](#)[Create ticket](#)

The EC2 instance in question is directly accessible from the internet, which significantly increases its exposure to potential attacks. It has a high-severity software vulnerabilities that can be exploited remotely over the network without requiring any user interaction or special privileges. This vulnerability has a known exploit available, making it easier for attackers to compromise the instance. Furthermore, the instance has an administrative access policy attached to it, meaning if compromised, an attacker could gain powerful privileges within your AWS environment. This combination of factors - internet accessibility, a severe and easily exploitable vulnerability, and administrative access - creates a critical risk scenario where an attacker could potentially steal credentials and gain unauthorized access to your AWS resources with minimal effort.

Critical **New** First detected 1 day ago, last updated 5 minutes ago

Overview

Ticket	d4a796e7c32d2690730af
Type	Exposure/Potential Impact/Resource Hijacking
Primary resource	EC2 instance: i-045e5e28814812022
Region	us-east-1
Account	284561945518
Age	1 day
Created time	June 6, 2025, 14:32:3...

[View more](#)

Contributing traits (6) [Info](#)

Contributing traits provide the severity of the exposure finding.

Reachability

The EC2 instance is reachable within the VPC

[Security groups should not allow unrestricted access to ports with...](#) Finding

[Security groups should only allow unrestricted incoming traffic for...](#) Finding

The EC2 instance is reachable over the internet

Vulnerability

The EC2 instance has a software vulnerability with a known exploit

Misconfiguration

The IAM Role associated with the EC2 instance has an Administrative access policy

The EC2 instance has an open Security Group

The EC2 instance has a public IP address

[View all traits](#)

Remediation [Info](#)

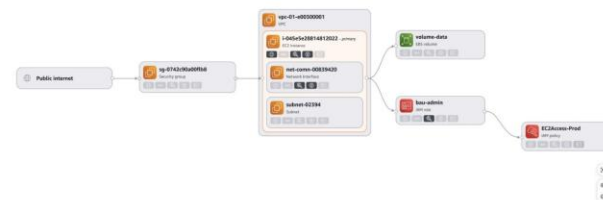
We recommend that you start remediating the top traits [internet reachable remediation](#), [exploit available](#) and [administrative access policy remediation](#).

Potential attack path

[Traits](#)[Resources](#)

Potential attack path [Info](#)

A visualization of AWS resources associated with this exposure finding. The graph indicates how potential attackers could access and take control of your resources.



☒ Primary resource ☐ Involved resource ☒ Contributing trait count

Trait types [Internet reachability](#) [AWS Sensitive data](#) [Vulnerability](#) [Misconfiguration](#) [Assumability](#)

AWS Security Hub

Hallazgos de exposiciones

Correlación automatizada de señales de seguridad en los servicios de AWS para identificar y priorizar riesgos críticos provenientes de vulnerabilidades y configuraciones incorrectas

Potential attack path

Traits

Resources

EC2 instance

ID

i-045e5e28814812022

Account ID

098765432109

Contributing traits

Reachability

Publicly invocable (1)

Vulnerability

Attack vector network (2)

Exploit available (1)

View more details

h this exposure finding. The graph indicates how potential attackers could

Primary resource Involved resource Contributing trait count

Trait types Internet reachability Sensitive data Vulnerability Misconfiguration Assumability

AWS Security Hub

Ruta de ataque

Visualiza posibles rutas de ataque comprendiendo cómo un adversario podría encadenar vulnerabilidades y configuraciones incorrectas para comprometer recursos críticos

Security Hub

Dashboard

Summary

Threats

Exposure

Vulnerabilities

Posture management

Sensitive data

Inventory

All findings

Resources

▼ Management

Integrations

Automations

▼ Settings

General

Configurations

Account coverage

Usage

▼ Detection engines

GuardDuty

Inspector

Security Hub

Macie

Documentation

What's new

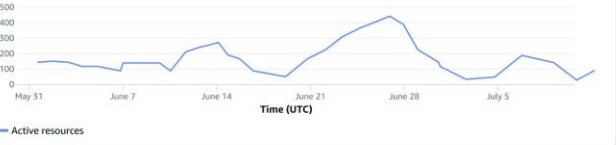
Security Hub > Resources

Resources

▼ Overview

Resource trends are displayed for the last 90 days. Apply filters from the graph to the resource table to view the resources represented in the visualization.

Active resources count



Time (UTC)

Saved filter set

Choose a filter set

Filter assets

Reset

Quick filters

Category

Clear filter

► Compute (260)

► Storage (200)

► Database (150)

► CI/CD (125)

► Identity (200)

► Network (125)

▼ Top 10 accounts

295562301397 (280)

284561945518 (211)

734551835194 (146)

107348332719 (52)

364823190652 (47)

View more (+5)

▼ Top 10 finding types in resources

Network reachability (50)

Software and Config (45)

Checks/Vulnerabilities/CVE

Package vulnerability (40)

Exposure (35)

Threat (30)

Attack sequence (25)

Code vulnerability (20)

Software config checks (15)

Coverage (10)

Resource type

► IAM role

► ECR container image

► S3 bucket

► Security Group

► IAM policy

► AWS Account

▼ EC2 instance

Resource

prod-webserver-01

aws-cloud-prep-01234

staging-auth-service

prod-payment-api

test-redis-cluster

dev-elasticsearch-01

uat-backend-service

prod-load-balancer

staging-kafka-broker

EC2 instance

aws-cloud-prep-01234

Open EC2

The resource is involved in 1 attack sequence finding, 1 exposure finding, and 8 other findings.

Details

Findings (10)

Instance name

aws-cloud-prep-01234

Instance ID

i-045e5e28814812022

ARN

arn:aws:ec2:us-east-1:522536594833:instance/...

Resource type

EC2 instance

Account ID

295562301397

AWS Region

us-east-1

Created time

February 6, 2024, 14:32:30 (UTC+3:30)

▼ Tags (3)

Key

Value

Name

aws-cloud-prep-01234

Environment

Prod

Image ID

ami-0db8018400e7fe1c9

IAM Instance profile ARN

arn:iam:instanceprofile:09823094809384

Private IP address

123.12.12.12 (DnsName1 if applicable)

Security Hub > Inventory > EC2 instance: i-3492g7k30911vnl

EC2 instance: i-3492g7k30911vnl

Last updated: 2 hours ago

Export

Attack path

2

Flat MoM

Findings

32

Flat MoM

Threat

Vulnerability

Sensitive data

Public exposure

Flagged

Details

Attack path

Findings

Installed software

Software applications

Filter by application

Name	Type	Version	Package URL
AMAZON_LINUX_2023	Operating system	1	pkg:rpm/gdisk@1.0.8-1.amzn2023.0.2?arch=X86_64&epoch=0&upstr=gdisk-1.0.8-1.amzn2023.0.2.src.rpm
gdisk	Application	1.0.8	pkg:rpm/gdisk@1.0.8-1.amzn2023.0.2?arch=X86_64&epoch=0&upstr=gdisk-1.0.8-1.amzn2023.0.2.src.rpm
openssl	Library	3.4	pkg:rpm/gdisk@1.0.8-1.amzn2023.0.2?arch=X86_64&epoch=0&upstr=gdisk-1.0.8-1.amzn2023.0.2.src.rpm
python3-pyserial	Application	2.5.0	pkg:rpm/gdisk@1.0.8-1.amzn2023.0.2?arch=X86_64&epoch=0&upstr=gdisk-1.0.8-1.amzn2023.0.2.src.rpm
json-c	Application	0.14	pkg:rpm/gdisk@1.0.8-1.amzn2023.0.2?arch=X86_64&epoch=0&upstr=gdisk-1.0.8-1.amzn2023.0.2.src.rpm

AWS Security Hub

Inventario de recursos enfocado en seguridad

Visibilidad integral de los recursos, destacando los activos accesibles desde internet, los hallazgos de seguridad y el contexto de las aplicaciones para identificar los recursos críticos en su entorno.



Demo



Enhanced AWS Security Hub



ENCUESTA



MUCHAS GRACIAS