AWS re:Inforce 2025 recap

Ashish Ghodake

- Cloud Security
- Motorcyclist
- Hiker

Agenda

- Announcements
- Talks
- Workshops

Announcements

- Verify internal access to critical AWS resources with new IAM Access Analyzer capabilities
- AWS IAM now enforces MFA for root users across all account types
- Improve your security posture using Amazon threat intelligence on AWS Network Firewall
- AWS Certificate Manager introduces exportable public SSL/TLS certificates to use anywhere
- AWS WAF reduces web application security configuration steps and provides expert-level protection
- Amazon GuardDuty expands Extended Threat Detection coverage to Amazon EKS clusters
- Updates to the AWS MSSP Competency: Deliver Turnkey Security Solutions for Customers
- Secure your Express application APIs in minutes with Amazon Verified Permissions
- Beyond compute: Shifting vulnerability detection left with Amazon Inspector code security capabilities
- AWS Backup adds new Multi-party approval for logically air-gapped vaults

Talks

Where are your secrets? Monitor keys, secrets, and certs usage on AWS (DAP441)

- Focused Mainly on Observability around Secret Manager, KMS and ACM
- Solution basically focuses around collecting logs from Cloudtrail, Config and SecurityHub and ingesting it into SecurityLake and provide insights using Athena queries and Quicksight
- https://github.com/aws-samples/sample-crypto-asset-monitoring

Sticky situations: Building advanced AWS WAF honeypots for better security

- Focused on building Honeypots using AWS Native Services
- MadPot - https://www.aboutamazon.com/news/aws/amazon-madpot-stops-cybersecurity-crime
- Solution focuses on building honeypot by using CloudFront & S3 for frontend, Lambda@Edge for dynamic baits and API Gateway for capturing request body
- Also utilizes WAF for making actionable threat intel lists from the honeypot
- https://docs.aws.amazon.com/solutions/latest/security-automations-for-aws-waf/solution-overview.html

Talks

I didn't know Network Firewall could do that! (NIS322)

- Covered different Deployment models for AWS Network Firewall
- New Easy Integration with Transit Gateway
- Firewall routing for Local Traffic
- New Multiple VPC endpoints with single firewall
- Layer 7 metadata filtering capabilities, TLS inspections, IDS and IPS
- Automated Domain List feature
- New Flow management features to capture, flush and filter flows

Multi-stage threat detection using Amazon GuardDuty and MITRE (TDR302)

- Explained MITRE ATT&CK, D3FEND and Engage
- Guardduty now gives out MITRE ATT&CK sequence details in findings
- Gives timeline of corelated signals related to the finding
- https://aws-samples.github.io/threat-technique-catalog-for-aws/

Workshop - SEC271: Red Team approaches to practical generative AI defenses

- Attack Techniques for Gen AI applications
  - Prompt Injection
  - Data Poisoning
  - Guardrail Bypass
  - Context Window Overflow
  - Data Leaks
  - Supply Chain Issues
  - Model Generated SQL

References

- https://aws.amazon.com/blogs/aws/aws-reinforce-roundup-2025-top-announcements/
- https://reinforce.awsevents.com/on-demand/

Thank You !

LinkedIn

Content