Join me in June for AWS re:Inforce 2023 in Anaheim, CA

I extend a warm invitation to you as registrations are now open for the AWS re:Inforce 2023 conference in Anaheim Convention Center which will commence in less than 50 days time!

I have especially prepared this attendee guide for Builders, Data Scientists, Data Analysts, Developers, Architects and Business Professionals to help you navigate the conference which commences on Tuesday 13 June and concludes on Wednesday 14 June and maximize your learning experience to build that security framework and innovate with new insights as you learn from AWS Customers with real use cases.

AWS re: Inforce 2023 conference is curated for your specific needs to educate AWS customers with technical deep dives, business enablement content for C-suite, decision makers and provides generalist content suitable for builders and non-technical audiences to meet your security needs. You will receive hands-on learning opportunities and be able to participate in interactive sessions to help you build a culture of security, acquire knowledge in best practice and implement solutions for your organization.

Over two-days you will be able to choose from six session tracks:

- Application Security
- Data Protection
- Governance, Risk and Compliance
- Identity and Access Management
- Network and Infrastructure Security
- Threat Detection and Incident Response

Build your own agenda

I recommend that you start building your customized agenda now from the session catalog that you may preview to ensure that won't miss any of the popular learning experiences that include breakout sessions, workshops, chalk talks, code talks and lightning talks that may fill up quickly. You may register at this link.

Highlights

This attendee guide is focussed on ensuring that you have a most enjoyable, interactive and memorable experience at the conference, allowing you to incorporate different tracks into your agenda for your use cases and speak to AWS security experts at the Expo.

Keynote - CJ Moses, AWS VP and Chief Information Security Officer

On Tuesday, 13 June, you will hear from AWS Vice President and Chief Information Security Officer CJ Moses provide a keynote in the morning at 9:00 am (PDT), be sure to check-in early to secure a good seat and be ready to take note of the latest announcements for your security needs.

Breakout Sessions

APS302 | From IDE to code review, increasing quality and security | Level 300

In this breakout session you will be hearing from speakers Ifeanyi Okafor, Omer Tripp and Jas Chhabra discuss how to improve the quality and security of your code early in the development cycle. Explore how you can integrate Amazon Code Whisperer, Amazon CodeGuru reviewer, and Amazon Inspector into your development workflow, which can help you identify potential issues and automate your code review process.

Don't forget to book into this interactive session if you would like to learn more about how to increase your developer productivity and explore the new tool AWS Code Whisperer an AI coding companion to understand how it can provide code suggestions for your security posture.

DAP401 | Security design of the nitro system | Level 400

In this breakout session you will hear from expert J.D. Bean discuss the AWS Nitro System and the underlying platform for all modern Amazon EC2 instances.

You learn about the inner workings of the Nitro System and discover how it is used to help secure your most sensitive workloads.

This session is fascinating to me for exploring the unique design of the Nitro System's purpose-built hardware and how the hardware provides root of trust and a cryptographic system to ensure data integrity.

Builders' Sessions

TDR353 | Detecting suspicious activity in Amazon S3 | Level 300
In this builders' session you will hear from speaker Steve de Vera provide a guided simulation of suspicious activity within an AWS account involving unauthorized data exfiltration and Amazon S3 bucket and object data deletion.

This is a highly recommended session that will help you to learn how to detect and respond to malicious activity using AWS services like AWS CloudTrail, Amazon Athena, Amazon GuardDuty, Amazon CloudWatch, and non-traditional threat detection services like AWS Billing to uncover evidence of unauthorized use.

DAP353 | Privacy-enhancing data collaboration with AWS Clean Rooms | Level 300

In this builders' session you will hear from speakers Ryan Malecky, Michael Santana, Akhil Aendapally, Ranjith Krishnamoorthy as they introduce AWS Clean Rooms to help you to protect sensitive data or eliminate raw data sharing.

I am looking forward to this session as you will be able to obtain hands-on experience with AWS Clean Rooms to learn how to query collective datasets and reduce the risk of exposing sensitive data from the underlying dataset.

Chalk Talks

TDR431| The anatomy of a ransomware event | Level 400

In this chalk talk will be hearing from speakers Megan O'Neil and Kyle Dickinson as they share the anatomy of a ransomware event that targets data residing in Amazon RDS and get detailed best practices for detection, response, recovery, and protection.

This is a much-anticipated session if you are interested in learning more about ransomware events and how to ensure that that you have appropriate measures for early detection and automated responses to limit your organization's exposure.

IAM431 | A tour of the world of IAM policy evaluation | Level 400

In this chalk talk you will hear from speakers Matt Luttrell and Daniel Peebles share beyond the basics of identity and access management (IAM) policy evaluation to focus on how policy evaluation works with some more advanced AWS features. I am keen to receive prescriptive guidance on what to do and what to avoid when designing authorization schemes and learn how policies are evaluated alongside AWS KMS key grants, Amazon S3 and Amazon EFS access points, Amazon VPC Lattice, and more.

Workshop

Session Number | Building a DDoS-resilient perimeter and automatic protection at scale | Level 300

In this workshop you will learn from speaker Dmitriy Novikov who will help you to acquire practical knowledge on how to build a DDoS-resilient perimeter, analyze logs to make informed decisions with Amazon Athena, and see how to use services like AWS Shield, AWS WAF, AWS Firewall Manager, and Amazon CloudFront to architect for DDoS resiliency and maintain robust operational capabilities that allow for rapid detection and engagement during high-severity events. This will an excellent session to help you learn how to detect and filter out malicious web requests, reduce the attack surface, and protect at scale with maximum automation and visibility.

Code Talks

DAP342 | Protecting data in use with Cryptographic Computing for Clean Rooms | Level 300

In this code talk, you will be hearing from speakers Andrew Kent and Bethany Rababy as they share cryptographic computing for clean rooms (C3R) which is a feature of AWS Clean Rooms that provides organizations the ability to protect data even while it is in use.

This will be a great code talk to further your learning with example queries and explanations of the C3R encryption client settings needed to run them to help you understand how to protect, use, collaborate and not share raw data.

GRC441| Proactive compliance in CI/CD pipelines with Amazon CodeCatalyst | Level 400

In this code talk you be hearing from speakers Isaiah Salinas and Nereida Woo discuss how to implement proactive compliance in CI/CD pipelines using Amazon CodeCatalyst and AWS Config. This interesting code talk will be beneficial to help you to integrate applications that comply with industry standards and regulations using continuous integration and continuous delivery (CI/CD) pipelines.

Lightning Talk

TDR371 | Security monitoring for connected devices across OT, IoT, edge & cloud | Level 200

In this lightning talk you will hear from speaker Ryan Dsouza teach you how to stay ahead of cybersecurity threats and help IT leaders, CIOs and CISOs manage cybersecurity risks for all connected devices that includes operational technology. This will be an important lightning talk to join as you will learn how AWS makes it easier to monitor, detect, and respond to threats across the entire attack surface, which includes OT, IoT, edge, and cloud, while protecting your security investments in existing third-party security tools.

Happy Hour | Tuesday June 13 - 4:00 PM– 5:00 PM (PDT)

Pencil into your calendar and socialize with us on Tuesday 13 June at 4:00pm-5:00pm (PDT) during the happy hour at the Expo to listen to lightning talks over drinks and network with your peers.

Closing reception

Sit back, relax and enjoy the closing remarks on the last day of the conference. Join us from 6:00pm (PDT) as AWS executive team share final tips, learnings and highlights from the conference to better prepare you as you head back into your workplace armed with confidence and security knowledge to build steps to secure your data against threats and implement with tools for threat detection.

AWS re:Inforce 2023 will commence on Tuesday 13 June and conclude on Wednesday 14 June. It will be Summer in sunny California and the weather in Arnaheim , CA is forecast to reach a high of 25 degrees celsius or 77 degrees fahrenheit.