QCon SAN FRANCISCO by InfoQ

Security at QCon San Francisco 2026

Sessions

The Freeze Paradox: Why Stopping Deployments Doesn't Stop Failures

Monday Nov 16

When systems fail at Netflix and in an environment this complex, they sometimes will, the instinctive response is to freeze deployments.

Prachi Jain

Senior Site Reliability Engineer @Netflix, Expert in Building and Managing Scalable, Reliable Services, Previously @Fastly and @Cisco

Sandhya Narayan

Expert in Information Security, Compliance, and Risk Management, Previously Technical Program Manager @Netflix, @Adobe, SAP, @eBay, and the Stanford Research Institute

---

How Airbnb Guardrailed Its AI Customer Support Agent

Monday Nov 16

When Airbnb launched its AI customer support assistant, the feature made the news — the guardrails built to make it safe to ship did not. Yet an AI agent that talks to millions of customers, remembers a conversation across turns, and can trigger account actions is a

Weiping Peng

Distinguished Engineer @Airbnb, Previously Principal Architect @Salesforce for AI platform

---

Silent Agent Failures: Detect and Fix Them Before Your Customers Notice

Monday Nov 16

An agent run can receive a success verdict, complete every tool call without an error, and still fail the customer. It skips a necessary step, cites the wrong evidence, or delivers a confident answer that doesn’t resolve the request.

Diane Lin
Staff Engineer @Datadog

Agentic Trust: Securing AI Agents in Production

Monday Nov 16

This session will cover practical measures that you can take now to run agents more securely in production. This will not cover topics like model training and alignment; rather it will focus on deploying an existing agent as safely as possible.

Amanda Walker
Sr. Director, Engineering - Privacy, Safety and Security @Google

---

Into the Labyrinth: What Distributed Systems Have Taught Us About Guardrails

Monday Nov 16

AI has changed everything about software engineering...or has it? We've spent the past few decades learning how to build web-scale applications: complex, distributed systems that are too complex to fit into one reviewer's brain, but too critical to just YOLO into production.

Akshay Shah
Field CTO @Antithesis

It's Never the Thing That Broke: Learning From Incidents at (AI) Speed

Monday Nov 16

When something breaks, our first instinct is to focus on the thing that failed. But in complex systems, the failure is usually the result of many things going right, changing, and interacting in ways we didn't anticipate.

Vanessa Huerta Granda
Resilience Engineering Manager @Enova, Co-Author of the Howie Guide on Post Incident Analysis, Board Member for the Resilience in Software Foundation

QCon
SAN FRANCISCO by InfoQ

No More Small Systems, How AI May Bring Large System Problems to Everyone

Wednesday Nov 18

Once you figure out how to use AI to make your organization productive, you will soon find you have a whole new set of problems. While some of those problems will be novel thanks to LLMs, many of them are just the result of there being "more stuff".

Adam Bender

Technical Lead for Enterprise Engineering @Google