databricks

# Databricks AI Security Workshop

Take the safest path on your AI journey

## Overview

This half-day workshop is designed to help security leaders understand the workings of AI and ML systems — including risk factors and how to mitigate those risks. Available as an in-person or virtual workshop, the content is crafted based on your organization's industry, maturity and size.

If you're interested in attending one of our scheduled workshops — or arranging one for your organization — please reach out to dasf@databricks.com.

You'll learn:

- How AI models work and their underlying concepts
- How AI models deliver business outcomes, including security
- Insights into how compliance frameworks like HITRUST and NIST play a crucial role in effectively mitigating risks associated with AI

Plus, you'll hear from the experts on key approaches and controls to manage cyber risks associated with AI.

**Omar Khawaja**
VP and Field CISO

**Arun Pamulapati**
Senior Staff Security Engineer

## Target Audience

- CISOs
- Security executives
- Governance leaders

## Agenda

DURATION
4 hours

FORMAT
Presentation, guided discussion

AI and Machine Learning Essentials

- Introduction to the machine learning lifecycle and AI system components
- Overview of machine learning operations (MLOps)
- Who manages AI and ML models

Risks Associated With AI and ML Models

- Top technical risks
- Top organizational risks

Overview of Controls for Mitigating AI Risks

- Group discussion on best practices