databricks

Databricks AI Risk Workshop

Navigate AI with speed, safety and confidence

Overview

While many business leaders and data teams are excited about the transformative potential of AI, governance and risk leaders — spanning compliance, security, privacy, legal and ethics — are often more focused on the unintended adverse consequences of these systems. This disconnect is a significant factor slowing AI adoption.

To address this divide, this half-day workshop is designed to equip leaders with a comprehensive understanding of AI and ML systems, including their components, risks and actionable mitigation strategies based on the content of the open Databricks AI Security Framework. The workshop is available in person and tailored to your organization's industry, size and maturity.

If you want to join a scheduled workshop or arrange one for your organization, contact us at dasf@databricks.com.

You'll learn how to:

- **Understand AI systems:** Break down the 12 components of AI and learn how they work together as a cohesive system to deliver business outcomes, including enhanced security
- **Assess AI risks:** Explore the 62 specific risks tied to each component of AI, the threats that can realize those risks, and 64 actionable controls to mitigate each of them
- **Implement AI controls:** Explore compliance frameworks like HITRUST and NIST to understand how they can be used to manage AI risks effectively
- **Operationalize AI governance:** Identify which controls to apply, where in the AI lifecycle to apply them and who is responsible for deploying them

Plus, you'll hear from experts with 20+ years of industry experience on key approaches and controls to managing cybersecurity risks associated with AI.

CO-CREATED WITH THE FOLLOWING ORGANIZATIONS

árhasi · Barracuda · complyleft · ethriva · HIDDENLAYER · NAVY FEDERAL Credit Union · ROBUST INTELLIGENCE · SAFE

Target Audience

Leaders at the director level and above in governance, data, privacy, legal, IT and security functions

Agenda

DURATION

3.5 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