AI SECURITY WORKSHOP

Unlock AI confidence: Identify AI security gaps

Position your organization at the forefront of responsible AI by embedding governance, security, and compliance into every stage of your AI journey.

As AI becomes central to digital transformation and business operations, organizations face new risks, including data exposure, regulatory compliance issues, model bias, and adversarial threats. Without robust planning and governance, AI can introduce vulnerabilities, breaches, and operational uncertainty.

The AI Security Workshop from GDT provides your organization with a clear, actionable pathway to securing AI by identifying vulnerabilities, aligning with global standards, and defining methods to build trust with stakeholders. Through expert facilitation and a framework-aligned discussion, you'll gain the insights needed to secure and future-proof your AI investments.

AI Security Workshop

The AI Security Workshop is a structured, interactive, half-day engagement led by a GDT cybersecurity expert. It is designed to evaluate your current AI posture and help your organization confidently navigate the complex landscape of AI risk, compliance, and responsible innovation. This workshop provides you with practical knowledge related to current AI security threats and can be tailored to address your organization's specific business and cybersecurity requirements. Following the workshop, a GDT cybersecurity expert will perform an analysis of information gathered during the workshop.

Scope
The workshop provides a structured, actionable approach to assessing and strengthening your organization's AI governance framework.

- **Explore the threat landscape:** Get an overview of AI security and the current threat landscape.
- **Explore your organization's needs:** Understand your organization's challenges, needs, and desired end state in relation to your AI efforts.
- **Align AI risks with global frameworks:** Align with OWASP Top 10 LLM and the OWASP LLM Governance Checklist.
- **Evaluate critical controls:** Review security, privacy, data management, and incident response.
- **Deliver tailored advice:** Get clear, actionable recommendations for the next steps in your AI journey.

Focus areas
- Privacy and data protection
- Security controls and threat mitigation
- Bias, fairness, and responsible AI use
- Incident response and business continuity
- Vendor and supply chain risk management

Outcomes
- **Proactive risk reduction:** Identification of AI-specific vulnerabilities, such as data leakage, prompt injection, and system prompt leakage, as well as gaps in controls for your AI systems related to the OWASP Top 10 for LLM and OWASP LLM Application Cybersecurity and Governance Checklist.
- **Tailored, actionable insights:** Recommendations and a prioritized roadmap based on your unique AI landscape, use cases, and risk profile.
- **Faster, safer AI Innovation:** Guardrails, best practices, and continuous improvement mechanisms to enable secure AI adoption and development.

Security is part of our DNA

GDT helps clients identify, prioritize, and execute next steps to accelerate digital transformation. Our deep expertise enables us to rapidly and expertly assess existing technology ecosystems and make strategic recommendations for effective transformation. Plus, benefit from our extensive partner ecosystem. GDT has forged deep relationships and aligned our strategies with top-tier security providers like Cisco, Fortinet, Palo Alto Networks, and many others.

Visit GDT.com to learn more.

Schedule your complimentary workshop at https://marcom.gdt.com/cybersecurity-workshop