

## **SANS Defines the Standards**

#### Setting the Global Benchmark for AI Security

Al adoption is moving faster than many security leaders can keep pace with. Enterprises are rolling out GenAl and agentic systems at scale, while adversaries exploit Al to accelerate attacks. Regulators are racing to set guardrails, but most organizations still lack a trusted roadmap for secure and compliant adoption.

For over 35 years, SANS has set the benchmark for cybersecurity training and practice. Now, as the AI landscape reaches an inflection point, SANS is defining the standards for organizations to adopt AI safely, responsibly, and with confidence.



**SANS Secure AI Blueprint:** A three-track model (Protect, Utilize, Govern) that outlines practical pathways for organizations to adopt AI securely, align with regulatory frameworks, and connect strategy directly to workforce training.



**SANS Critical AI Security Guidelines:** The first operations-driven framework for securing AI systems, organized into six domains: Access, Data, Deployment, Inference, Monitoring, and Governance.



**Global Standards Contributions:** Through partnership with OWASP AI Exchange, SANS faculty co-authored the OWASP Top 10 for LLMs and contributed substantial content adopted into ISO/IEC 27090 and the EU AI Act.



**Regulatory Engagement:** SANS experts brief U.S., EU, and APAC policymakers and translate frameworks such as the NIST AI Risk Management Framework, America's AI Action Plan, and the EU AI Act into field-tested controls.



**Comprehensive Leadership:** SANS delivers unmatched breadth and depth in shaping the future of secure AI through 22+ initiatives spanning training, standards, research, and policy.

### **SANS's AI Security Impact**

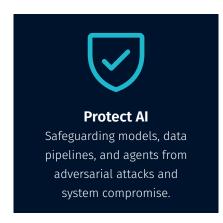
- > 3 tracks for safe AI adoption outlined in the SANS Secure AI Blueprint
- > 70+ pages contributed to ISO/IEC 27090
  Al Security Guidance

- > 40+ pages authored into EU AI Act security standards
- > 22+ major AI initiatives across training, standards, research, and policy
- **6** control domains in the Critical AI Security Guidelines

# The Secure AI Blueprint:

## From Policy to Practice

SANS translates global frameworks and policies into action through the Secure AI Blueprint, a three-track model that ensures AI adoption is secure, compliant, and operationally effective:







## **SANS AI Curriculum:**

#### Operationalizing the Blueprint

SANS's AI curriculum provides practitioners, engineers, and leaders with hands-on skills that directly support priorities outlined in the Secure AI Blueprint. Courses are authored by the same experts shaping AI security guidelines, standards, and regulatory frameworks worldwide.

#### **Protect Al**

**SEC495:** Leveraging LLMs — Building & Securing RAG and Agentic Systems

**SEC545:** GenAl and LLM Application Security

**SEC595:** Applied Data Science & AI/ML for Cybersecurity Professionals

#### **Utilize Al**

**SEC511:** Continuous Monitoring and Detection Engineering

**SEC503:** Network Monitoring and Threat Detection

**SEC598:** Security Automation for Offense, Defense, and Cloud

#### **Govern Al**

**AIS247:** AI Security Essentials for Business Leaders

**LDR512:** Security Leadership Essentials for Managers

**LDR514:** Security Strategic Planning,

Policy, and Leadership

Visit sans.org/artificial-intelligence for more information on SANS's AI curriculum >

### Ready to Own AI Securely?

SANS provides the frameworks and training your organization needs to adopt AI with confidence.

> Download the Secure AI Blueprint today.

