

GLOBALLY RECOGNIZED · VENDOR-NEUTRAL · ANSI-ALIGNED

Certified AI Security Professional

— (CAISP)

Become a Globally Recognized AI Security Professional

Earn the CAISP credential — secure models, data pipelines, LLMs, RAG systems, and AI agents against adversarial attacks, prompt injection, and supply-chain risk across the full AI lifecycle. **Today's offer: \$800 → \$400.**



4.8/5 Reviews.io (96%) · **4.4/5** Trustpilot · **2,50,000+** certified

Enroll at gsdcouncil.org/ai-security-certification

Why This Certification, Why Now

Enterprises are shipping LLMs, RAG systems, and autonomous agents into production faster than security teams can cover them. Traditional AppSec never accounted for models that can be poisoned, extracted, or talked into misbehaving.



AI created a new attack surface

Training data, model weights, embeddings, vector stores, prompts, and tool calls are all attackable — and none are covered by legacy controls.



LLM attacks are already mainstream

Prompt injection, jailbreaking, system-prompt leakage, insecure output handling, and model theft now appear in real incidents.



Frameworks have caught up

OWASP Top 10 for LLMs, MITRE ATLAS, NIST AI RMF and Adversarial ML, and ISO/IEC 42001 are now the assessment baseline.



Agents and supply chains raise the stakes

Tool use, plugins, open-source models, and third-party datasets extend trust boundaries far beyond your own environment.

FROM THEORY TO PRACTICE

What You'll Be Able to Do



Master AI security fundamentals — threats, attack surfaces, and core security principles



Build AI security strategy aligned with enterprise cybersecurity and risk objectives



Apply NIST, OWASP, MITRE ATLAS, and ISO standards to enterprise AI security practice



Protect AI data, ML pipelines, models, and development environments



Identify and mitigate adversarial ML attacks, model vulnerabilities, and emerging AI threats



Secure LLMs, RAG systems, AI agents, APIs, and Generative AI applications



Run AI security testing, red teaming, vulnerability assessment, and incident response



Lead enterprise AI security initiatives across the complete AI lifecycle

Why GSDC

**4.4 / 5**

Trustpilot · Excellent

**4.8 / 5**

Reviews.io · 96% recommend

2,50,000+

professionals certified

500+

Fortune clients

190+

countries served

Since 2016

US · SG · Switzerland

- ✓ Independent, vendor-neutral certification body established in 2016 — offices in the US, Singapore, and Switzerland.
- ✓ Accredited by ABICB (Accreditation Board for International Certification Bodies) and a proud member of ANSI.
- ✓ Alumni work at 500+ Fortune companies across 190+ countries; 100+ Authorized Training Partners worldwide.
- ✓ Certification built and reviewed with AI security professionals, cybersecurity practitioners, and technology leaders protecting production AI systems.

RECOMMENDED BY

Forbes · Indeed · TechTarget · CareerSidekick · LeanIX · People Managing People · Authentic

**ABICB Accredited****ANSI Member****Vendor-Neutral**Read verified reviews: trustpilot.com/review/gsdccouncil.org · reviews.io

Our Global Clients

Professionals across technology, cloud, finance, and regulated enterprises hold GSDC certifications.

Oracle**Amazon****Microsoft****Cisco****Veritas****HP****Bank of America****Deloitte****Volkswagen**

IS THIS FOR YOU?

Who Is This Certification For?

- AI security professionals and cybersecurity practitioners
- Information security managers and IT security architects
- AI and machine learning engineers building production systems
- Security operations (SOC) teams, penetration testers, and red teamers
- Risk management, data privacy, and data protection professionals
- IT and technology managers, compliance and governance professionals

PRE-REQUISITES

There are no mandatory prerequisites. Basic familiarity with cybersecurity, information security, risk management, or technology concepts is helpful, along with an interest in securing AI systems in real-world environments. No advanced AI or technical background is required — the program starts with AI security fundamentals and builds toward practical skills for identifying threats, managing risks, and implementing secure AI practices.

Learn from Experts

Learn from experienced practitioners and industry leaders who design, update, and teach the program — bringing real-world AI security, adversarial ML, and enterprise cybersecurity expertise to every module.



Maxim Salnikov
MICROSOFT

Digital and App Innovation Business
Lead, Western Europe



Trevor Wiseman
THE CIRCUIT

VP of Technology & AI Governance



Swathi Adimulam
ORACLE

OCI Cloud & AI Architect



Hayk Hakobyan
INSIGHTGENIE

Co-Founder



Baris Dirim
CULTUREASY

Human Systems Architect

What You'll Learn

16+ hours across 13 modules covering the full AI security lifecycle — from threat modeling to red teaming — with real frameworks, toolkits, and Learn-By-Doing activities built into every module.

1

Foundations of AI Security

Principles, ML fundamentals, attack surfaces, threat landscape, security roles

2

AI Threat Modeling & Risk

Asset and threat identification, risk scoring, controls, registers, monitoring

3

Frameworks & Standards

NIST AI RMF, OWASP LLM Top 10, MITRE ATLAS, ISO 27001/23894/42001/5338

4

AI Data & Pipeline Security

Training data protection, provenance, poisoning, leakage, MLOps security

5

Adversarial Machine Learning

Evasion, poisoning, extraction, inversion, backdoors, and defenses

6

Secure AI Development

Secure training, hardening, robustness, versioning, and secure deployment

7

Generative AI & LLM Security

Prompt injection, jailbreaking, output handling, model theft, LLM controls

8

RAG & AI Agent Security

Vector DB and embedding security, agentic risks, tool, plugin, and API security

9

Infrastructure & Cloud Security

GPU and compute security, containers, secrets, isolation, deployment

10

Security Testing & Red Teaming

AI red teaming, attack simulation, jailbreak and RAG testing, remediation

11

Supply Chain & Third-Party

Model and dataset supply chain, open-source risk, provenance, vendor risk

12

Privacy, IAM & Security Ops

PII protection, privacy-preserving ML, access control, logging, incident response

13

Enterprise AI Security

Strategy, policies, architecture, maturity, roadmap, metrics, improvement

Module-by-Module

Module 1 — Foundations of AI Security

- Introduction to AI Security
- AI Security Principles
- AI and ML Fundamentals
- AI Lifecycle
- AI Attack Surfaces
- AI Threat Landscape
- AI Security Architecture
- AI Security Challenges
- AI Security Roles
- AI Security Best Practices

Module 3 — AI Security Frameworks & Standards

- NIST AI RMF
- NIST Adversarial ML
- OWASP AI Exchange
- OWASP Top 10 for LLMs
- MITRE ATLAS
- ISO/IEC 27001
- ISO/IEC 23894
- ISO/IEC 42001
- ISO/IEC 5338
- AI Security Control Mapping

Module 5 — Adversarial Machine Learning

- Adversarial ML Fundamentals
- Evasion Attacks
- Poisoning Attacks
- Model Extraction
- Model Inversion
- Membership Inference
- Adversarial Examples
- Backdoor Attacks
- Model Manipulation
- Adversarial Defenses

Module 7 — Generative AI & LLM Security

- GenAI Security Fundamentals
- LLM Attack Surfaces
- Prompt Injection
- Jailbreaking
- Sensitive Data Disclosure
- Insecure Output Handling
- System Prompt Leakage
- Model Poisoning
- Model Theft
- LLM Security Controls

Module 2 — AI Threat Modeling & Risk

- AI Threat Modeling
- AI Asset Identification
- AI Threat Identification
- AI Risk Assessment
- AI Risk Classification
- AI Risk Scoring
- AI Risk Treatment
- AI Security Controls
- AI Risk Register
- AI Risk Monitoring

Module 4 — AI Data & Pipeline Security

- AI Data Security
- Training Data Protection
- Data Classification
- Data Provenance
- Data Lineage
- Data Integrity
- Data Poisoning
- Data Leakage
- ML Pipeline Security
- MLOps Security

Module 6 — Secure AI Development

- Secure AI Development
- Secure Model Training
- Model Validation
- Model Hardening
- Model Robustness
- Model Integrity
- Model Versioning
- Model Access Control
- Secure Model Storage
- Secure Deployment

Module 8 — RAG & AI Agent Security

- RAG Security
- RAG Attack Surfaces
- Vector Database Security
- Embedding Security
- Knowledge Base Security
- AI Agent Security
- Agentic AI Risks
- Tool and Plugin Security
- AI API Security
- Agent Access Controls

Module-by-Module

Module 9 — AI Infrastructure & Cloud Security

- AI Infrastructure Security
- GPU Security
- AI Compute Security
- Container Security
- Cloud AI Security
- AI Network Security
- API Gateway Security
- Secrets Management
- AI Environment Isolation
- AI Deployment Security

Module 11 — AI Supply Chain & Third-Party Security

- AI Supply Chain Security
- Model Supply Chain
- Dataset Supply Chain
- Open-Source AI Risks
- Third-Party Models
- AI Vendor Risk
- AI Dependency Security
- Model Provenance
- AI Procurement Security
- Supply Chain Monitoring

Module 13 — Enterprise AI Security

- AI Security Strategy
- AI Security Policies
- AI Security Governance
- AI Security Architecture
- AI Security Program
- AI Security Maturity
- AI Security Gap Assessment
- AI Security Roadmap
- AI Security Metrics
- Continual Improvement

Module 10 — AI Security Testing & Red Teaming

- AI Security Testing
- AI Security Assessment
- AI Red Teaming
- Attack Simulation
- Prompt Injection Testing
- Jailbreak Testing
- Model Security Testing
- RAG Security Testing
- Agent Security Testing
- Security Findings and Remediation

Module 12 — AI Privacy, IAM & Security Operations

- AI Privacy Security
- PII Protection
- Sensitive Data Protection
- Privacy-Preserving ML
- AI Identity Management
- AI Access Control
- Least-Privilege Access
- AI Security Monitoring
- AI Security Logging
- AI Incident Response

A Guided Path to Certification

Self-paced study, daily live sessions, personal mentoring, and hands-on practice — finish at your own pace.



STEP 1 · FOUNDATION

Self-paced modules

16+ hrs expert-led video, e-books, templates, cheat sheets & toolkits · lifetime access



STEP 2 · DAILY LIVE

GSDC Studio

Daily live sessions with global experts · 100+ monthly · free recordings



STEP 3 · PRACTICE

Learn by Doing + 1-on-1 SME

Threat-model an LLM application and run prompt-injection & jailbreak tests, with personal SME reviews



STEP 4 · CERTIFICATION

Apply & Get Certified

2 practice exams + capstone project, final proctored exam · portfolio-ready deliverables

Move at your own pace. Study self-paced with lifetime access to all materials, live sessions, and recordings.

ALL IN ONE ENROLLMENT

Everything Included



Expert-Led Videos

16+ hours, self-paced



SME Connect

3 personalized 1-on-1 sessions



Capstone Project

Secure an end-to-end AI system



GSDC Studio

100+ live monthly sessions



Learn By Doing

Hands-on AI security assignments



Job Support

LinkedIn Enhancer, Resume Builder + free membership

Exam & What to Expect

This is a certification, not a course. Study self-paced with the materials provided (plus live support), then sit a proctored online exam. Lifetime access to materials, plus 2 practice exams.

40
EXAM QUESTIONS

MCQ
EXAM FORMAT

65%
PASSING SCORE

90 min
DURATION

English
LANGUAGE

No
OPEN BOOK

5 Years
VALIDITY

Yes
FREE RETAKE

IS THIS FOR YOU?

Where CAISP Takes You

YOUR ROLE	HOW CAISP HELPS YOU	CAREER OUTCOME
Cybersecurity Professional	Extend AppSec and threat modeling to models, pipelines, and LLM apps.	→ AI Security Engineer
SOC Analyst / Incident Responder	Monitor, log, and respond to AI-specific incidents and abuse patterns.	→ AI Security Operations Lead
Penetration Tester / Red Teamer	Run AI red teaming, prompt-injection, jailbreak, and RAG testing.	→ AI Red Team Lead
AI / ML Engineer	Harden training, validation, storage, and deployment of your models.	→ Secure AI Engineer
Security / Cloud Architect	Design isolated, secrets-safe AI infrastructure and API boundaries.	→ AI Security Architect
Risk / Compliance Professional	Map NIST, OWASP, MITRE ATLAS, and ISO controls to AI systems.	→ AI Security Assurance Lead



7-Day Money-Back Guarantee

Enroll with zero risk — full 100% refund within 7 days if you feel you haven't gained the skills you're looking for. Includes a complimentary exam retake and lifetime access to your materials.

 Chat on WhatsApp

 Book a 10-min advisor call

Choose Your Plan

Single Access

~~\$800~~ **\$400**

1

CERTIFICATION

- ✓ Self-paced expert-led videos + GSDC Studio
- ✓ 3 SME Connect (1-on-1) sessions
- ✓ Book of Knowledge + Capstone + Job Support
- ✓ Exam + 1 free retake & practice · membership (\$109 free)

Bundle Access

MOST POPULAR

~~\$1200~~ **\$600**

3

CERTIFICATIONS

- ✓ Everything in Single, across 3 certifications — just \$200 each
- ✓ Unlimited SME Connect (1-on-1)
- ✓ Exam + 2 free retakes & practice
- ✓ Most-chosen by serious learners

Region-specific pricing shown at enrollment · Teams? Ask about GSDC for Business.

Enroll Now → gsdcouncil.org/ai-security-certification

WhatsApp +1 251-333-1717 · Global Skill Development Council · US · Singapore · Switzerland

LIMITED-TIME OFFER — EXTRA 10% OFF

Use code **UPSKILL10** at checkout — valid for 72 hours only