GSDC
Global Skill Development Council

★ MOST TRUSTED AI SECURITY CERTIFICATION

GLOBALLY RECOGNIZED · VENDOR-NEUTRAL · ANSI-ALIGNED

Certified Agentic AI Cybersecurity Professional

(CAAICP)

Become a Globally Recognized Agentic AI Security Professional

Earn the CAAICP credential — gain the skills to build, deploy, and defend autonomous AI agents across modern security operations, and command a **20–60% higher salary**.

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

Enroll at **gsdcouncil.org/certified-agentic-ai-cybersecurity-certification**

Global Skill Development Council · US · Singapore · Switzerland

THE OPPORTUNITY

Why This Certification, Why Now

Security teams are racing to adopt autonomous AI agents for defense — while defending against the very risks those agents introduce. This is the skillset that bridges both sides.

Autonomous threats are here

Attackers are already using AI agents at machine speed — defense has to move at the same pace.

AI agents are entering the SOC

Security teams now use autonomous agents to triage alerts, enrich intel, and contain incidents in real time.

Agentic systems are a new attack surface

Prompt injection, tool misuse, and data poisoning create risks that traditional security training doesn't cover.

Leaders need governed AI, not just automation

Boards want autonomous defense that is auditable, compliant, and safely governed — not a black box.

FROM THEORY TO PRACTICE

What You'll Be Able to Do

- Explain Agentic AI architectures, reasoning, memory, and autonomous decision-making for security operations
- Apply Agentic AI for intelligent threat detection, monitoring, and behavioral analytics
- Automate SOC operations using Agentic AI for alert triage, incident response, and SOAR workflows
- Leverage Agentic AI for vulnerability assessment, attack surface management, and automated remediation
- Identify and mitigate security risks in autonomous AI systems, including prompt injection and tool misuse
- Secure Agentic AI deployments through governance, compliance, and responsible AI practices

TRUSTED CREDENTIAL

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 cybersecurity practitioners, agentic-systems experts, and security leaders advancing autonomous defense.

RECOMMENDED BY

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

🛡 **ABICB Accredited**

🌐 **ANSI Member**

⚖ **Vendor-Neutral**

See our **Wall of Fame & verified reviews →** · **trustpilot.com/review/gsdcouncil.org** · **reviews.io**

TRUSTED BY 2,50,000+ PROFESSIONALS

Our Global Clients

Professionals across technology, cloud, finance, and enterprise security hold GSDC certifications.

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

IS THIS FOR YOU?

Who Is This Certification For?

- Security analysts, SOC engineers, and incident responders
- Security architects and engineers
- Threat-intelligence and vulnerability-management professionals
- IT and security leaders adopting AI-driven defense
- Penetration testers exploring agentic AI for penetration testing
- Risk and compliance professionals working with AI-driven security programs
- Anyone pursuing a certification in agentic AI for cybersecurity to advance their career

PRE-REQUISITES

No mandatory prerequisites. Foundational cybersecurity knowledge and basic familiarity with AI concepts are helpful, but no formal AI background is required — the program builds from the fundamentals of Agentic AI up to real security operations workflows.

ADVISORY FACULTY & MENTORS

Learn from Experts

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

Ziggy Rafiq
CAPGEMINI
Software Engineering Lead

Trevor Wiseman
THE CIRCUIT
VP of Technology & AI Governance

Suvarsha Rai
AMAZON
Sr. Technical Product Manager

Caleb Jephunneh
BRICKLABSAI
CEO | Global AI Speaker

Swathi Adimulam
ORACLE
OCI Cloud & AI Architect

Leela VenkataSatish Kolla
LTIMINDTREE
Director, Program & Project Mgmt

Baris Dirim
CULTUREASY
Human Systems Architect

PROGRAM CURRICULUM

What You'll Learn

36+ hours across the full agentic AI security lifecycle, with hands-on demos and real frameworks built into every module. Each module pairs videos and e-books with templates and Learn-By-Doing activities.

1

Foundations of AI, Generative AI, and Agentic AI

Autonomy, goal-orientation, and the shift from content generation to autonomous action

2

Architecture of AI Agents and Multi-Agent Systems

LLM core, memory, planning, tool use, and orchestration frameworks

3

Agentic AI for Threat Detection and Monitoring

Autonomous threat hunting, SOC alert triage, and behavioral analytics

4

Agentic Incident Response and SOAR

Automated triage, containment, threat-intel agents, and AI-assisted forensics

5

AI-Assisted Vulnerability and Defense Management

Scanning, attack-surface mapping, and automated remediation workflows

6

Securing AI Agents and Defending Against AI Threats

Prompt injection, tool misuse, data poisoning, and zero-trust for agents

7

Governance, Compliance, and Responsible AI in Security

NIST, ISO 27001, MITRE ATT&CK, oversight, and trustworthy AI programs

8

Capstone Project — Applied Agentic Security Strategy

Design & present a real agentic incident-response workflow for a simulated breach

DETAILED CURRICULUM

Module-by-Module

Module 1 — Foundations of AI, Generative AI, and Agentic AI

- Evolution from Traditional AI to Generative AI to Agentic AI
- What makes AI “agentic”: autonomy, goal-orientation, decision-making
- Generative vs agentic AI
- Core concepts: agents, environments, goals, actions, feedback loops
- The agentic AI landscape and enterprise use cases

Module 2 — Architecture of AI Agents and Multi-Agent Systems

- Anatomy of an AI agent: LLM core, memory, planning, tool use
- Reasoning and planning techniques (ReAct, Chain-of-Thought, Reflection)
- Memory systems: short-term, long-term, RAG
- Tool/function calling and API integration
- Multi-agent orchestration
- Popular frameworks (LangChain, LangGraph, AutoGen, CrewAI)

Module 3 — Agentic AI for Threat Detection and Monitoring

- Autonomous threat detection and anomaly hunting
- AI agents in SOC operations and alert triage
- Log analysis, SIEM augmentation, event correlation
- Behavioral analytics and insider-threat detection

Module 4 — Agentic Incident Response and SOAR

- Automated incident triage, enrichment, and containment
- Agentic playbooks and SOAR orchestration
- Threat-intelligence gathering and summarization agents
- AI-assisted forensics and root-cause analysis

Module 5 — AI-Assisted Vulnerability and Defense Management

- AI-assisted vulnerability scanning and prioritization
- Attack-surface mapping and continuous security assessment
- Red-team and blue-team augmentation concepts
- Patch intelligence and automated remediation workflows

Module-by-Module

Module 6 — Securing AI Agents and Defending Against AI Threats

- Threats to agentic systems: prompt injection, tool misuse, data poisoning
- Securing agent tool access, permissions, and guardrails
- Defending against AI-powered attacks and deepfakes
- Identity, access, and zero-trust for autonomous agents

Module 7 — Governance, Compliance, and Responsible AI in Security

- Security frameworks and AI (NIST, ISO 27001, MITRE ATT&CK)
- Auditability, human oversight, and safe levels of autonomy
- Privacy, data handling, and ethical use
- Building a trustworthy AI-driven security program

Capstone Project · Applied Agentic Security Strategy
— Build, implement & present a real agentic incident-response workflow applying detection, triage, containment & escalation design — SME-reviewed, portfolio-ready. Plus 1-on-1 and daily expert sessions.

YOUR LEARNING JOURNEY

A Guided 4-Week Path to Certification

Self-paced study, daily live sessions, personal mentoring, and hands-on practice — finish in as little as one week.

📘

WEEK 1 · FOUNDATION

Self-paced modules

36+ hrs expert-led video, e-books, templates & toolkits · lifetime access

🖥

WEEK 2 · DAILY LIVE

GSDC Studio

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

🛠

WEEK 3 · PRACTICE

Learn by Doing + 1-on-1 SME

Build an alert-triage agent & an incident-summarization agent, with personal SME reviews

🏅

WEEK 4 · CERTIFICATION

Apply & Get Certified

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

⚡ **Move at your own pace.** This is a suggested roadmap — driven learners can finish in as little as one week.

ALL IN ONE ENROLLMENT

Everything Included

🎥 **Expert-Led Videos**
36+ hours, self-paced

🖥 **GSDC Studio**
100+ live monthly sessions

💬 **SME Connect**
1-on-1 with industry experts

🛠 **Learn By Doing**
Hands-on demos: alert-triage & incident-summarization agents

🎯 **Capstone Project**
Design a real agentic incident-response workflow

💼 **Job Support**
Career help + free GSDC membership

KNOW BEFORE YOU ENROLL

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 Questions	**MCQ** Format	**English** Language	**65%** Pass score
90 min Duration	**No** Open Book	**5 yrs** Validity	**Yes** Complimentary Retake

IS THIS FOR YOU?

Who Is This Certification For?

YOUR ROLE	HOW CAAICP HELPS YOU	CAREER OUTCOME
Security Analyst / SOC Engineer	Move from manual triage to agent-assisted detection, enrichment, and response.	→ **SOC Lead / Threat Detection Engineer**
Incident Responder	Apply agentic playbooks for containment, forensics, and root-cause analysis.	→ **Senior IR / SOAR Specialist**
Security Architect / Engineer	Design and govern multi-agent security systems with proper guardrails.	→ **AI Security Architect**
Threat Intel / Vulnerability Mgmt	Automate intel gathering, attack-surface mapping, and remediation prioritization.	→ **Threat Intel Lead**
Penetration Tester	Explore agentic AI for offensive security and red/blue-team augmentation.	→ **AI-Augmented Pentest Lead**
Risk & Compliance Professional	Apply NIST, ISO 27001, and MITRE ATT&CK to autonomous AI programs.	→ **AI Governance & Risk Lead**

No prior AI experience required. Security professionals at every level — from analysts to leaders — are welcome.

ENROLLMENT OPTIONS

Choose Your Plan

Single Access

1

CERTIFICATION

- ✓ Self-paced expert-led videos + GSDC Studio
- ✓ 3 SME Connect (1-on-1) sessions
- ✓ Capstone Project + Job Support + membership
- ✓ Exam + 1 free retake & practice

Bundle Access

MOST POPULAR

3

CERTIFICATIONS

- ✓ Everything in Single, across 3 certifications
- ✓ 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.

7-DAY

7-Day Money-Back Guarantee

Enroll with zero risk — full 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

Enroll Now → gsdcouncil.org/certified-agentic-ai-cybersecurity-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