INFOSEC Boot Camps
CERTIFICATION TRAINING

Get live, expert instruction from anywhere.

Generative and Agentic AI for Cybersecurity Professionals Boot Camp

This intensive 5-day course equips cybersecurity professionals with practical knowledge of generative AI and agentic AI systems, focusing on their applications, risks and defensive strategies in cybersecurity contexts.

Course description

This intensive 5-day course equips cybersecurity professionals with practical knowledge of generative AI and agentic AI systems, focusing on their applications, risks and defensive strategies in cybersecurity contexts. Participants will gain hands-on experience with AI tools while understanding their implications for threat landscapes and defensive operations. By the end of this course, participants will have built and deployed a complete suite of autonomous AI security agents capable of:

- **Autonomous penetration testing:** AI agent that conducts comprehensive security assessments
- **Intelligent traffic analysis:** Real-time network traffic monitoring and threat detection
- **Malware detection and verification:** Automated malware identification with YARA rule matching and VirusTotal integration
- **Memory forensics analysis:** AI-powered memory dump analysis using Volatility framework
- **Orchestrated security operations:** Multi-agent system that coordinates all security functions

Who should attend

- Cybersecurity professionals with 2+ years of experience
- Security operations center (SOC) analysts
- Incident response team members
- Security architects and engineers
- Penetration testers
- Threat hunters
- Security managers and team leads
- General interest audience

Boot camp at a glance

What you'll learn

- AI fundamentals for cybersecurity
- Generative AI applications and risks
- Agentic AI and autonomous security systems
- Memory forensics and advanced analysis
- AI governance and compliance

Delivery methods

- Online

Training duration

- Immediate access to course materials
- 5-day boot camp
- 90-day extended access to all boot camp materials

The hands-on cybersecurity training platform that moves as fast as you do

Infosec Boot Camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to days of live training from an experienced pro, you'll get unlimited access to hundreds of additional hands-on cybersecurity courses and cyber ranges to help you advance your skills before, during and after your boot camp. Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, or get a head start on your next certification goal.

Start training immediately

Prepare for your boot camp with immediate access to the Infosec Skills on-demand training library.

Learn by doing in the cyber range

Put what you've learned into practice with 100s of browser-based labs and hands-on projects.

Get unlimited custom practice exams

Uncover knowledge gaps with unlimited practice exams attempts and skill assessments.

700+ IT and security courses

Earn CPEs and build new skills with hundreds of additional training courses.

What's included

- Five days of expert, live instruction in AI for cybersecurity
- 90-day extended access to boot camp components, including class recordings
- Free 90-day Infosec Skills subscription (access to 1,400+ additional courses and labs)
- Knowledge Transfer Guarantee

Prerequisites

2+ years of cybersecurity experience. Basic understanding of machine learning concepts. Familiarity with scripting (Python preferred). Understanding of common attack vectors and defensive frameworks.

Lab prerequisites: Basic AWS CLI and console familiarity. Docker container experience. Python programming skills. Linux command line proficiency.

Assessments and certification

Assessment methods:

- Daily practical exercises (40%)
- Capstone project presentation (30%)
- Written examination (20%)
- Participation and engagement (10%)

Certification requirements:

- Minimum 80% attendance
- Successful completion of all practical exercises
- Passing score on written examination (75%)
- Satisfactory capstone project presentation

What you'll learn

- Design and implement agentic AI systems for cybersecurity
- Build autonomous security workflows with human oversight
- Create AI-powered threat hunting and incident response capabilities

- Integrate multiple security tools into cohesive AI-driven platforms
- Deploy complete autonomous SOC with all developed agents
- Execute comprehensive red team exercise against agent-defended environment
- Demonstrate autonomous threat detection, analysis and response workflows
- Validate malware detection through traffic analysis and memory forensics

Required tools and infrastructure

AWS account (AWS Free Tier + additional resources ~$200/participant for week)

- EC2 instances (t3.large recommended for agent workloads)
- VPC with multiple subnets for isolated testing
- S3 buckets for evidence and artifact storage
- Lambda functions for serverless agent components

Core security tools

- Penetration testing: Metasploit, Nmap, OpenVAS, Maltego, Burp Suite Community
- Traffic analysis: Wireshark, Scapy, Suricata, Zeek (Bro)
- Malware analysis: YARA, radare2, Ghidra, Cuckoo Sandbox
- Memory forensics: Volatility 3, Rekall, LiME
- DFIR tools: Autopsy, Sleuth Kit, SANS SIFT Workstation

AI and automation frameworks

- LangChain, CrewAI, AutoGen for agent development
- Ollama with CodeLlama, Mistral, and security-focused models
- Apache Kafka for agent communication
- Redis and Celery for task orchestration

Development and deployment

- Docker and Kubernetes for containerized agents
- Terraform for Infrastructure as Code
- Git repositories for agent code management
- Grafana and Prometheus for monitoring

Specialized lab requirements

- VirusTotal API Keys (Community tier available)
- Maltego Community Edition accounts
- Sample malware repository (controlled and legal samples)
- Memory dump datasets for forensics training
- Vulnerable target environments (Metasploitable, DVWA, VulnHub VMs)

Recommended reading

- “AI-Powered Cybersecurity” by Sarkar and Sharma
- “Adversarial Machine Learning” by Biggio and Roli
- NIST AI Risk Management Framework
- MITRE ATT&CK Framework for AI

Additional resources

- AI security research papers and publications
- Vendor whitepapers and case studies
- Professional AI security communities and forums
- Certification pathways and continuing education opportunities

Learn from experts

We don’t just have great instructors, our instructors have years of industry experience and are recognized as experts. Over the past 15 years, we’ve helped tens of thousands of students get certified and advance their careers.

Generative and Agentic AI for Cybersecurity Professionals details

Our instructors give you 100% of their time and dedication to ensure that your time is well spent. You receive an immersive experience with no distractions!

Daily split: Day 1: 25% lecture, 75% hands-on labs | Day 2: 30% lecture, 70% hands-on labs | Day 3: 20% lecture, 80% hands-on labs | Day 4: 25% lecture, 75% hands-on labs

	Day 1	Day 2	Day 3	Day 4	Day 5
Morning session	Introductions Lecture: AI fundamentals for cybersecurity Hands-on lab 1A: Core agent architecture setup	Lecture: Generative AI for security operations Hands-on lab 2A: Intelligent traffic analysis agent	Lecture: Understanding agentic AI systems Hands-on lab 3A: AI-powered reconnaissance agent	Lecture: Memory forensics fundamentals Hands-on lab 4A: Volatility-based memory analysis agent	Lecture: AI governance and compliance Lecture: Measuring AI security effectiveness Lecture: Future trends and emerging threats
Afternoon session	Lecture: AI in the threat landscape Hands-on Lab 1B: Basic security agent development Lecture: AI ethics and legal considerations Hands-on lab 1C: Agent security and sandboxing	Lecture: Advanced prompt engineering & AI content threats Hands-on lab 2B: Malware detection and YARA integration agent Hands-on lab 2C: VirusTotal integration and verification agent	Lecture: Autonomous threat response & offensive AI Hands-on Lab 3B: Intelligent exploitation agent Hands-on Lab 3C: Penetration test reporting agent	Lecture: Advanced memory threats & AI security architecture Hands-on lab 4B: Advanced memory threat hunting agent Hands-on lab 4C: Forensics integration and evidence management	Capstone Labs - Integrated autonomous security operations center (Lab 5A: Multi-agent security orchestration platform; Lab 5B: End-to-end threat simulation and response; Lab 5C: Production deployment and monitoring) Skills verification Course wrap-up

Schedule may vary from class to class

Before your boot camp

Start learning now. You'll get immediate access to all the content in Infosec Skills the moment you enroll. Prepare for your live boot camp, uncover your knowledge gaps and maximize your training experience.

During your boot camp

AI fundamentals and architecture

- Introduction to machine learning, deep learning and neural networks
- Overview of generative AI: Large Language Models (LLMs), diffusion models, GANs
- Understanding agentic AI: autonomous decision-making systems
- Current AI landscape and key players (OpenAI, Anthropic, Google, Microsoft)

- Multi-agent systems and their architecture
- Decision-making frameworks in autonomous AI
- Tool use and API integration in AI agents
- Limitations and failure modes of agentic systems

Security applications and threat landscape

- AI-powered attacks: deepfakes, social engineering, automated vulnerability discovery
- Case studies: Recent AI-enabled cyber incidents
- Evolution of attack vectors with AI integration
- Attribution challenges in AI-assisted attacks
- Automated report generation and documentation
- Threat intelligence analysis and summarization
- Security policy creation and compliance checking
- Code review and vulnerability assessment assistance

Autonomous security operations

- Build and deploy complete suite of autonomous AI security agents
- Autonomous Penetration Testing with comprehensive security assessments
- Intelligent Traffic Analysis with real-time network traffic monitoring
- Malware Detection and Verification with YARA rule matching
- Memory Forensics Analysis using Volatility framework
- Orchestrated Security Operations with multi-agent coordination
- Automated incident response and containment
- AI-driven vulnerability discovery and exploitation

Technical implementation skills

- Deploy AWS EC2 instances with agent development environment
- Install LangChain, CrewAI and AutoGen frameworks
- Configure local LLMs (Ollama with CodeLlama and Mistral models)
- Set up agent communication infrastructure with Redis and Celery
- Create reconnaissance agent using Nmap and Python
- Build log analysis agent with pattern recognition
- Implement agent memory and state management
- Deploy secure execution environments using Docker containers

Memory forensics and advanced analysis

- Memory acquisition techniques and legal considerations
- Volatility framework architecture and plugin ecosystem
- Memory artifacts and attack technique detection
- Process hollowing, DLL injection and advanced persistence mechanisms
- Automated memory dump acquisition and processing workflows
- AI-powered Volatility plugin orchestration and analysis
- Malware detection in memory using pattern recognition and ML
- Timeline analysis and attack reconstruction workflows

AI governance and future readiness

- Establishing AI governance frameworks
- Compliance requirements for AI in regulated industries
- Audit trails and explainability requirements
- Privacy-preserving AI techniques
- Key performance indicators for AI security programs
- Testing and validation methodologies
- Quantum computing implications for AI and cybersecurity
- Advanced persistent AI threats and defense evolution

Lab deliverables

- Daily agent development: Functional autonomous agents for each security domain
- Day 3 milestone: Working penetration testing agent with full automation
- Day 4 milestone: Complete traffic analysis and memory forensics capabilities
- Final deliverable: Integrated multi-agent security operations platform with autonomous penetration testing with comprehensive reporting, real-time traffic analysis with malware detection, YARA rule matching and VirusTotal verification workflows, Volatility-based memory forensics with automated threat hunting and centralized orchestration and human oversight capabilities.

After your boot camp

Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, get a head start on your next certification goal or start earning CPEs.

About Infosec

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. Learn more at infosecinstitute.com.

INFOSEC