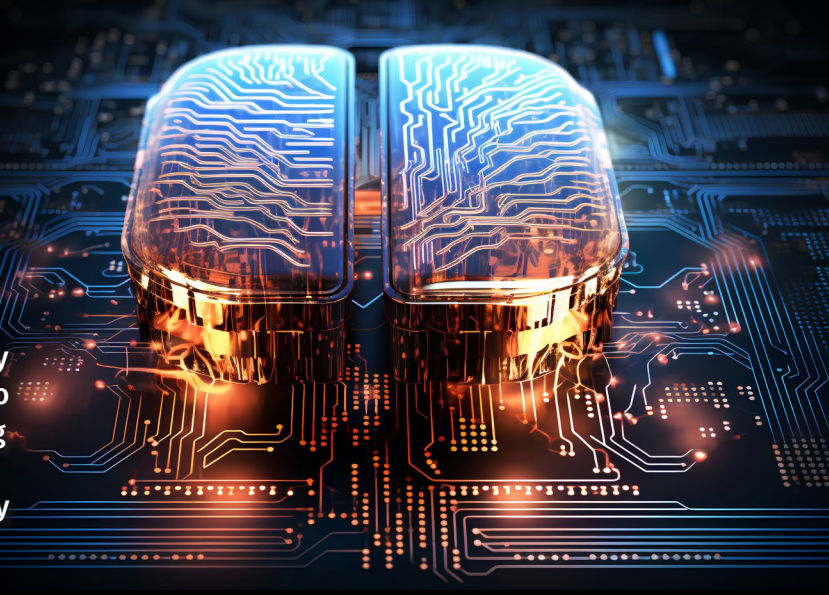
SANS

Generative Artificial Intelligence (GenAI) and Machine Learning (ML) Courses Road Map



SANS Institute's engagement with GenAI and ML not only encompasses training and education but also extends to cutting-edge research, community building, and shaping industry standards. This comprehensive involvement underscores our commitment to preparing cybersecurity professionals for an AI-integrated future.

GenAI/ML Technology-Focused Courses

SANS Institute develops specialized courses that equip professionals and organizations with the skills and knowledge needed to address AI-related complexities.

AIS247
AI Security Essentials for Business Leaders

AIS247 trains professionals to integrate AI into business safely and effectively, covering GenAI principles, applications, risks, ethics, and policy for responsible implementation.

SEC535
Offensive AI – Attack Tools and Techniques

SEC535 teaches AI for offensive purposes, covering security bypassing, exploit development, social engineering, automated attacks, and malware creation, with hands-on labs for practical application.

SEC595
Applied Data Science and AI/Machine Learning for Cybersecurity Professionals

SEC595 demystifies data science and machine learning with 70% hands-on problem-solving, focusing on practical AI/ML applications in cybersecurity and balancing theory with real-world solutions.

GenAI/ML Integration-Enhanced Courses

SANS incorporates GenAI/ML training across its broader cybersecurity education courses, equipping professionals with the necessary expertise to tackle AI-related complexities and effectively defend against sophisticated cyber threats.

CYBER DEFENSE

SEC497
Practical Open-Source Intelligence (OSINT)

SEC497 teaches cybersecurity professionals to use AI-enhanced techniques and tools for gathering and analyzing publicly available data for security intelligence and threat assessment.

SEC503
Network Monitoring and Threat Detection In-Depth

Delivers the technical knowledge, insight, and hands-on training you need to confidently defend your network

SEC587
Advanced Open-Source Intelligence (OSINT) Gathering and Analysis

SEC587 trains professionals to use GenAI/ML for OSINT, focusing on advanced techniques to analyze and validate data from various sources.

FORENSIC & INCIDENT RESPONSE

FOR518
Mac and iOS Forensic Analysis and Incident Response

FOR518 teaches professionals AI-enhanced forensic techniques for Apple devices, improving accuracy in artifact analysis and security incident identification.

FOR577
LINUX Incident Response and Threat Hunting

FOR577 uses AI to enhance forensic investigations on Linux systems, improving validation and streamlining processes for more effective security incident detection and response.

FOR585
Smartphone Forensic Analysis In-Depth

FOR585 trains cybersecurity professionals in advanced, AI-enhanced techniques for analyzing and extracting forensic data from smartphones, enhancing mobile security incident detection and investigation.

OFFENSIVE OPERATIONS

SEC504
Hacker Tools Techniques and Incident Handling

SEC504 trains cybersecurity professionals in identifying and responding to threats, using AI to enhance detection, analysis, and automated response capabilities.

SEC598
Security Automation for Offense Defense and Cloud

SEC598 trains professionals to use advanced AI and automation to enhance offensive and defensive cybersecurity strategies in cloud environments.

FOR610
Reverse-Engineering Malware: Malware Analysis Tools and Techniques

FOR610 teaches malware analysis, equipping cybersecurity teams with advanced tools and AI-driven methods to dissect and counteract malware, enhancing threat detection and response.

CYBERSECURITY LEADERSHIP

LDR512
Security Leadership Essentials for Managers

LDR512 trains leaders to manage cybersecurity defenses strategically, using AI insights to improve decision-making and security policy development.

LDR514
Security Strategic Planning, Policy, and Leadership

LDR514 trains cybersecurity leaders in advanced strategies and policy development, using AI-driven data analysis to improve security governance and decision-making.

FOR710
Reverse-Engineering Malware: Advanced Code Analysis

FOR710 provides intensive hands-on training on dissecting complex malware, using AI tools for analysis, and developing robust malware defense strategies for organizations.