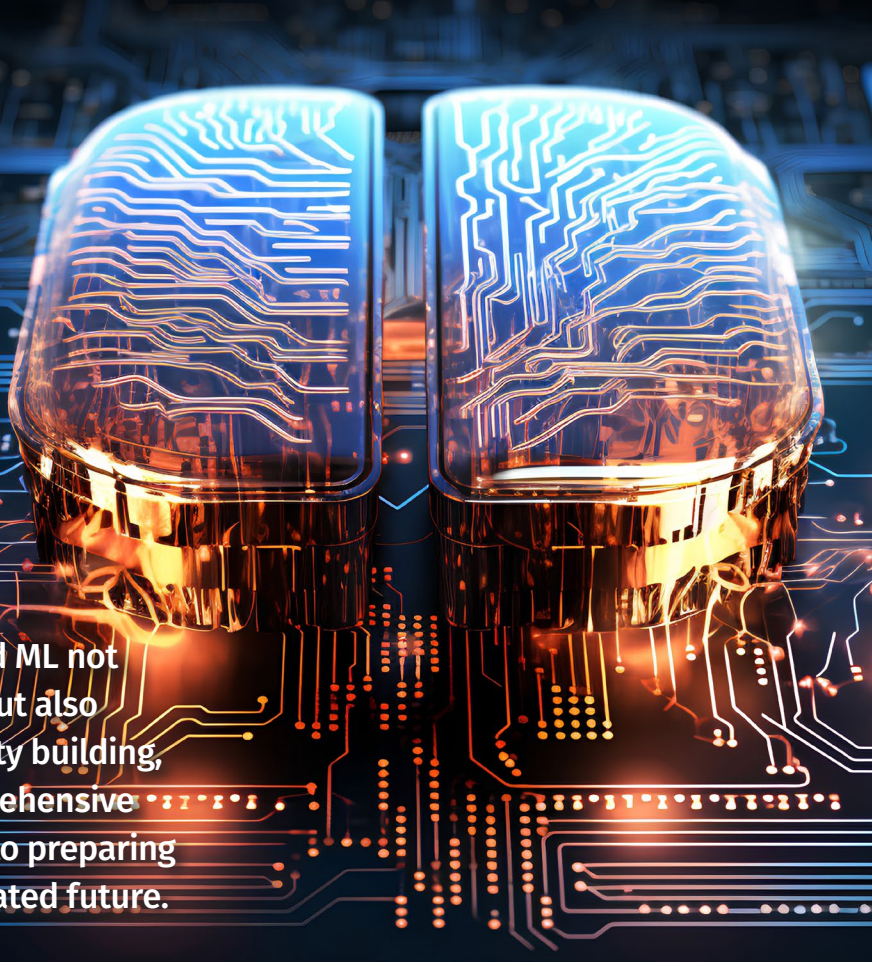
SANS

Leading Integrated Generative Artificial Intelligence (GenAI) and Machine Learning (ML) Cybersecurity



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.

Artificial Intelligence (AI) and Cybersecurity

Defending and Attacking GenAI/ML Technical Implementations

SANS is conducting thorough research that delves into the intricacies of exploiting and defending against the vulnerabilities of large language models (LLMs) and GenAI solutions. SANS explores the tactics, techniques, and procedures (TTPs) used by attackers to compromise LLMs and GenAI models and the countermeasures and defensive strategies organizations can employ to mitigate these risks.

Research across the industry is often inadequate and under-realized. SANS encourages research via its instructors, industry groups, summits, and the SANS college to increase research in this crucial area. We are actively bringing insights and best practices that provide actionable guidance on securely building and deploying internal or third-party LLMs and GenAI solutions, including implementing robust access controls, data encryption, and anomaly detection mechanisms. By exploring the intersection of LLMs and GenAI with cybersecurity, we aim to provide a deeper understanding of the associated risks and challenges and to identify effective strategies for securing these technologies.

Cybersecurity-Enhanced AI Capabilities

SANS is focusing on the application of GenAI and ML techniques to enhance cybersecurity-related job roles. Through courses, summits, forums, and webcasts, SANS showcases innovative and practical approaches to incorporating GenAI/ML into daily cybersecurity tasks, making them more efficient, accurate, and effective.

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. ***Courses that focus on the GenAI/ML attack space:***

AIS247: AI Security Essentials for Business Leaders

AIS247 teaches professionals how to integrate AI safely and effectively into business. It explores GenAI's principles, applications, and associated risks while emphasizing ethical usage and policy development. The course is designed for various professionals, ensuring they understand AI's transformative potential and implement it responsibly.

- **For Cybersecurity Teams—**Students understand the strategic importance, mechanisms, and risks of GenAI. They learn to enhance productivity and improve work quality while ensuring ethical use and alignment with organizational goals.
- **For Organizations—**The course equips teams to implement GenAI, focusing on cybersecurity risk management and responsible AI policies to ensure robust operations, manage risks, and maintain compliance.

> As a non-IT employee, I was concerned that the course may be too technical for me. However, after completing the AIS247 course, I feel confident that I understood the information and the way that it was organized and taught was very user friendly. Wonderful course!
> **—AIS247 student**

SEC535: Offensive AI – Attack Tools and Techniques

SEC535 provides students with a foundational understanding of using AI for offensive purposes, covering security bypassing, exploit development, social engineering, automated attacks, and malware creation, culminating in a comprehensive lab to apply their learning and navigate cybersecurity threats.

- **For Cybersecurity Teams—**Students taking SEC535 benefit from gaining practical skills in using AI for offensive cybersecurity operations, including security bypassing, exploit development, social engineering, automated attacks, and malware creation.
- **For Organizations—**Organizations benefit from having SEC535-trained professionals who can effectively use AI to enhance and automate their offensive cybersecurity strategies, improving their ability to detect, respond to, and mitigate sophisticated cyber threats.

SANS Educational Focus on AI Cybersecurity is essential as it bridges the gap between emerging AI technologies and their practical applications within cybersecurity.

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

SEC595 demystifies data science and machine learning, focusing over 70% on hands-on problem-solving to apply AI and Machine Learning (ML) in cybersecurity effectively. This course balances practical application with essential theory, preparing participants to implement and troubleshoot real-world security solutions using AI tools.

- **For Cybersecurity Teams—**Students gain essential machine learning skills, including practical threat detection, response applications, and data handling. They will have hands-on experience in building, training, and evaluating models.
- **For Organizations—**The course equips teams with advanced skills in threat detection, response, data handling, and model integration. It ensures compliance with ethical and legal standards, strengthening overall security.

> AI/ML for cybersecurity is poorly understood and misrepresented too often. SEC595 provides that balance between what management needs to know to grow its understanding of the technologies and hands-on experience.
> **—Thomas L, U.S. Military**

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. ***Courses that integrate GenAI/ML attack space:***

Forensic and Incident Response Courses

Digital Forensics and Incident Response (DFIR) are crucial in AI security as they provide the necessary tools and methodologies to investigate and mitigate breaches involving advanced AI technologies. These practices help organizations understand attack vectors, secure vulnerabilities, and strengthen defenses against increasingly sophisticated cyber threats driven by AI.

SANS DFIR

FOR518: Mac and iOS Forensic Analysis and Incident Response

FOR518 equips professionals with AI-enhanced tools and techniques to conduct detailed forensic investigations on Apple devices, improving accuracy in analyzing artifacts and identifying security incidents.

- **For Cybersecurity Teams—**The course teaches the use of GenAI/ML to analyze Mac artifacts and create user behavior patterns. Students gain practical skills in understanding and responding to user activities and potential threats.
- **For Organizations—**The course's AI integration enhances threat detection and response capabilities, leading to more accurate and efficient investigations and a stronger overall cybersecurity posture.

> "It was very interesting to learn that certain forensic tools could report data as being encrypted even though one could still get other data.
> **—Gary Titus, Stroz Friedberg LLC**

FOR577: LINUX Incident Response and Threat Hunting

FOR577 leverages AI to enhance forensic investigations on Linux systems, focusing on validating findings and streamlining processes to detect and respond to security incidents more effectively.

- **For Cybersecurity Teams—**The course teaches how to leverage AI, including ChatGPT, to validate Linux findings. Students learn how to enhance accuracy and efficiency in Linux forensics.
- **For Organizations—**The course's AI integration improves the ability to conduct thorough investigations and respond to security incidents effectively.

> "This course is very challenging and helps to up your game as an incident responder on Linux systems. The capstone exercise was both frustrating and amazing. I learned so much!"
> **—David Roman, Talos IR**

FOR585: Smartphone Forensic Analysis In-Depth

FOR585 equips cybersecurity professionals with advanced techniques and AI-enhanced tools for effectively analyzing and extracting forensic data from smartphones, improving the detection and investigation of mobile security incidents.

- **For Cybersecurity Teams—**The course enhances skills in AI detection on smartphones. It teaches how to trace interactions with browser and app-based AI, distinguishing between human and AI activities.
- **For Organizations—**The course's AI integration improves accuracy in tracing AI interactions and distinguishing human activities, enhancing detection and response to security breaches.

> FOR585 course content provides extremely relevant material, guiding examiners to crucial artifacts for investigations and validation. It outlines key details for every forensic challenge.
> **—Quinn L., U.S. Federal Agency**

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques

FOR610 delves into malware analysis, equipping cybersecurity teams with the knowledge and skills to dissect and counteract malware using advanced tools and methods, including AI-driven approaches for enhanced threat detection and response.

- **For Cybersecurity Teams—**The course teaches the use of AI and large language models like ChatGPT and ClaudeAI for malware forensics. This integration automates security alert management, establishes robust policies, and improves user interactions with AI-driven bots.
- **For Organizations—**The course's AI integration strengthens malware forensics capabilities, increasing efficiency, accuracy, and responsiveness in threat detection and mitigation.

> This course has helped me to improve my knowledge of malware techniques, to understand how to better protect assets, and how to successfully complete the eradication steps.
> **—Eric B., Nestle**

FOR710: Reverse-Engineering Malware: Advanced Code Analysis

FOR710 offers intensive, hands-on training aimed at teaching students how to dissect complex malware, utilize innovative AI tools for analysis, and develop robust malware defense strategies for their organizations.

- **For Cybersecurity Teams—**The course teaches students how to utilize AI tools for malware analysis, understanding their limitations and potential applications.
- **For Organizations—**The course's AI integration enhances malware detection and analysis, improving overall cybersecurity capabilities and staying ahead of evolving threats.

> The labs and exercises for the automation were excellent and really showed off what is needed to perform RE [reverse engineering] through automation.
> **—Daniel T., U.S. DOJ**

Offensive Operations Courses

AI-powered tools and techniques significantly enhance penetration testing and offensive operations by automating and optimizing various stages. They improve efficiency and accuracy in vulnerability scanning, quickly identifying and prioritizing vulnerabilities. During exploitation, AI assists in crafting and executing sophisticated exploits, increasing the likelihood of successful penetration. Post-exploitation activities are streamlined with AI-driven tools automating tasks such as privilege escalation and lateral movement, ultimately making the entire penetration testing process more efficient and effective. ***The following courses currently offer AI integration:***

SEC504: Hacker Tools Techniques and Incident Handling

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

- **For Cybersecurity Teams—**The course teaches how to apply AI in incident response and advanced threat detection. It shows how to automate repetitive tasks, enhance data analysis, and improve threat identification accuracy.
- **For Organizations—**The course's AI integration enhances security operations by leveraging AI for incident response and threat detection, increasing efficiency and accuracy.

> Great content! As a developer it is extremely useful to understand exploits and how better coding practices help your security position.
>
> **—Jeremy Bramson, Bramson Welch & Associates**

SEC598: Security Automation for Offense Defense and Cloud

SEC598 equips professionals with the skills to utilize advanced AI and automation technologies to enhance offensive and defensive cybersecurity strategies within cloud environments.

- **For Cybersecurity Teams—**The course integrates AI technologies, specifically Amazon Web Services AI/ML Large Language Model service offerings. Students gain expertise in automating threat detection, risk assessment, and incident response.
- **For Organizations—**The course's AI integration uses advanced AI tools for natural language processing and machine learning in modern web applications, making cybersecurity efforts more robust, innovative, and efficient.

> I'd recommend this course to those who want to understand how to manage a SOAR and SIEM. It's very good for teaching students how to understand playbooks for alerts.
>
> **—David Ahmad, Fox Corporation**

Cyber Defense Courses

AI and ML technologies enhance cybersecurity and cloud defenses by automating threat intelligence, improving anomaly detection, and enabling predictive analytics. These advancements allow for the identification and mitigation of potential threats, optimizing resource allocation, reducing response times, and increasing overall security effectiveness in cloud environments. ***The following courses currently offer AI integration:***

SANS
CYBER DEFENSE

SEC497: Practical Open-Source Intelligence (OSINT)

SEC497 teaches cybersecurity professionals how to use AI-enhanced techniques and tools to gather and analyze publicly available data for security intelligence and threat assessment purposes.

- **For Cybersecurity Teams—**The course covers AI applications like generative adversarial networks, ChatGPT, and Gemini. It teaches how to automate sentiment analysis and manage email communications using AI technologies.
- **For Organizations—**The course's AI integration enhances the organization's operational efficiency, decision-making, and overall data management.

> This class is amazing so far! It's exactly what I want - a hands-on, real-world deep dive into OSINT challenges, techniques, strategies, and actual tools to use.
> **—Mattie Swain**

SEC503: Network Monitoring and Threat Detection In-Depth

SEC503 trains cybersecurity professionals on how to effectively monitor networks and detect threats using advanced security tools and AI-enhanced techniques.

- **For Cybersecurity Teams—**The course teaches how to use AI for network monitoring and threat detection. Students use AI technology to analyze network traffic, identify zero-day threats, and improve incident response.
- **For Organizations—**The course's AI integration enhances an organization's ability to distinguish between normal and suspicious activities, it helps customize AI-driven security tools to protect against cyber threats.

> From a heavy background in host forensics and limited knowledge in network analysis and forensics, SEC503 has filled in a lot of the gaps in knowledge I have had throughout my career.
> **—Jared H., U.S. Military**

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

SEC587 trains professionals to use AI and machine learning in enhancing OSINT tasks, focusing on sophisticated techniques for analyzing and validating data from various sources.

- **For Cybersecurity Teams—**The course teaches AI and ML in OSINT tasks. Students learn prompt engineering, code analysis, and identify AI-generated disinformation and deepfake imagery.
- **For Organizations—**The course's AI integration facilitates OSINT automation tasks, improves efficiency and accuracy in data processing to manage digital threats effectively.

> This content is the next level for OSINT researchers. It fills in the areas that I have not been using but wanted to learn.
> **—Janie Brewer, Oracle**

Cybersecurity Leadership Courses

AI and ML can enhance policy and key cybersecurity decisions across an organization by providing data-driven insights, automating threat detection, and predicting future risks. These technologies enable more informed decision-making, streamline compliance with security policies, and improve the efficiency of security operations. By continuously analyzing data and adapting to new threats, AI and ML ensure that cybersecurity strategies remain effective and responsive to emerging challenges.

The following courses currently offer AI integration:

SANS CYBERSECURITY LEADERSHIP

LDR512: Security Leadership Essentials for Managers

LDR512 prepares leaders to strategically manage cybersecurity defenses, incorporating AI insights to enhance decision-making and security policy development.

- **For Cybersecurity Teams—**The course covers GenAI fundamentals, AI application architecture, and AI-specific attacks and defenses. Students gain practical experience in identifying and defending against AI-specific threats.
- **For Organizations—**The course's AI integration helps automate and streamline security processes, enhance threat detection, and develop accurate and responsive policies.

> This course continues to challenge and develop leadership capabilities to better prepare individuals to help their organizations thrive within the cyberspace.
>
> **—Christopher Burk, Southern California Edison**

LDR514: Security Strategic Planning, Policy, and Leadership

LDR514 equips cybersecurity leaders with advanced strategies and policy development skills, incorporating AI-driven data analysis to enhance organizational security governance and decision-making.

- **For Cybersecurity Teams—**The course helps students develop and manage comprehensive security policies for AI technologies. They will learn regulatory requirements, policy development, governance structures, risk management, ethical AI use, and incident response.
- **For Organizations—**The course's AI integration ensures robust AI security policies, responsible AI deployments, efficient risk management, and effective responses to security incidents.

> The course is one of the best classes I have taken to date. The content and labs are very well thought out and help hone in the skills you learned in class or those you've developed over the course of your career.
>
> **—Stephane Denis**

Courses Planned to Integrate AI in 2024

Cyber Defense

SEC401: Security Essentials – Network, Endpoint, and Cloud
SEC450: Blue Team Fundamentals: Security Operations and Analysis
SEC511: Continuous Monitoring and Security Operations
SEC530: Defensible Security Architecture and Engineering
SEC573: Automating Information Security with Python

DFIR

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics
FOR509: Enterprise Cloud Forensics and Incident Response
FOR528: Ransomware and Data Extortion
FOR589: Cybercrime Intelligence
FOR608: Enterprise-Class Incident Response & Threat Hunting

Offensive Operations

SEC542: Web App Penetration Testing and Ethical Hacking
SEC560: Enterprise Penetration Testing
SEC565: Red Team Operations and Adversary Emulation
SEC575: iOS and Android Application Security Analysis and Penetration Testing
SEC588: Cloud Penetration Testing
SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
SEC699: Advanced Purple Teaming – Adversary Emulation & Detection Engineering
SEC760: Advanced Exploit Development for Penetration Testers

Cloud Security

SEC488: Cloud Security Essentials
SEC510: Cloud Security Controls and Mitigations
SEC522: Application Security: Securing Web Applications, API, and Microservices
SEC540: Cloud Security and DevSecOps Automation
SEC541: Cloud Security Attacker Techniques, Monitoring, and Threat Detection
SEC549: Cloud Security Architecture

Leadership Curriculum

LDR433: Managing Human Risk

PHONE
301-654-SANS (7267)
Mon–Fri: 9:00 AM–8:00 PM ET

EMAIL
General Inquiries:
support@sans.org
Mon–Fri: 9:00 AM–8:00 PM ET
Sat: 9:00 AM–5:00 PM ET

MAILING ADDRESS
SANS Institute
11200 Rockville Pike, Suite 200
North Bethesda, MD 20852

By focusing on these key areas, SANS Institute continues to lead the industry in integrating AI into cybersecurity training and practices, ensuring that professionals and organizations are well-equipped to handle the complexities of AI and defend against advanced cyber threats.