SEC598

AI and Security Automation for Red, Blue, and Purple Teams

SEC598: AI and Security Automation for Red, Blue, and Purple Teams empowers the student to elevate their security program across offensive and defensive domains. Whether they are automating adversary emulation campaigns, building intelligent response workflows, or engineering detection-as-code pipelines, this course teaches how to harness AI-driven automation to outpace modern threats.

Extensive use of AI and automation in security workflows saved organizations an average of $2.2 million per breach compared to those without such investments.

Source: IBM Cost of a Data Breach 2024

2025 UPDATE

The 2025 update to SEC598 delivers the most advanced evolution of the course to date, featuring a 40% refresh focused on integrating Generative AI, agentic automation, and full-spectrum team collaboration. Students now engage in hands-on labs with LLMs, autonomous agents, SOAR platforms, Terraform deployments, and cloud-native detection tools across red, blue, and purple team scenarios.

The course has been renamed to reflect its broadened scope from "Security Automation for Offense, Defense, and Cloud" to "AI and Security Automation for Red, Blue, and Purple Teams", and with over 25 updated and expanded labs, SEC598 empowers students to automate offensive and defensive workflows using modern AI-enhanced techniques and secure-by-design infrastructure.

NEW CONTENT

- Generative AI, LLMs, and Agentic AI fundamentals
- Detection-as-Code workflows with CI/CD integration
- Multi-agent orchestration for security operations
- Adversary Emulation powered by AI
- Red team automation using Caldera, Atomic Red Team, CrewAI
- Purple teaming workflows mapped to MITRE ATT&CK
- Defensive automation with Microsoft Sentinel, Azure Logic Apps, and Tines
- AI-augmented IR playbooks and detection validation pipelines

UPDATED FEATURES

- Fully revised course structure and title reflecting AI integration
- Enhanced support for hybrid and cloud-native environments
- Real-world SOAR workflows using Microsoft Sentinel and Cortex XSOAR
- Deep dive into IaC with Terraform, Ansible, and Bicep
- Tools included: LangChain, AutoGen, CREWAI, Caldera, PurpleSharp, CloudGoat
- Integrated MITRE ATT&CK mapping across red and blue use cases

LAB REFRESH

- AI-powered Detection-as-Code with LLMs
- Amazon Bedrock Offensive AI Agents with MCP
- Cloud-native adversary simulations in AWS & Azure
- Continuous Attack Surface and Vulnerability Management with AI
- Adversary Emulation as Code using Tines
- Jupyter-based email threat analysis with AI integration
- Red team agent deployment with CrewAI
- Continuous testing with Terraform and security IaC
- IR playbook automation using PowerShell, Tines, and Sentinel
- Bonus lab: Always-On Purple Team agents (autonomous SOC simulation)

"I am very excited to release SEC598, which has a clear and in-depth focus on security automation leveraging GenAI to tackle the challenges we face daily. I am convinced that SEC598 gives you an in-depth understanding of automation concepts, technologies and how to apply them for offense and defense. This course is your game-changer to begin your journey into continuous purple teaming!" – SEC598 course author Jeroen Vandeleur

For more information:
sans.org/SEC598

SANS | GIAC CERTIFICATIONS