SEC573: AI-Powered Security Automation: Building Tools with Python, LLMs, and MCP™

GPYC Python Coder giac.org/gpyc

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Leverage AI to develop new tools to perform routine tasks quickly and efficiently
- Automate log analysis and packet analysis with AI agents, file operations, regular expressions, and analysis modules to detect threats
- Develop forensics tools to carve binary data, process unstructured AI data, and extract new artifacts
- Read data from databases and the Windows Registry to support AI-driven for investigations and tool development
- Interact with websites and APIs to enrich logs and AI prompts to accomplish information security tasks
- Develop MCP servers and OpenAI agents for advanced automation and threat identification and response
- Understand prompt injection attacks and build secure AI integrations

GPYC Python Coder giac.org/gpyc

GIAC Python Coder

The GIAC Python Coder (GPYC) certification validates a practitioner's understanding of core programming concepts, and the ability to write and analyze working code using the Python programming language. GPYC certification holders have demonstrated knowledge of common python libraries, creating custom tools, collecting information about a system or network, interacting with websites and databases, and automating testing.

- Python essentials: variable and math operations, strings and functions, and compound statements
- Data structures and programming concepts, debugging, system arguments, and argparser
- Python application development for pen testing: backdoors and SQL injection

Are you ready to supercharge your cybersecurity career with AI-driven automation and tackle the evolving threats in today's digital landscape? The key is mastering AI integration through practical tools like message context protocol (MCP) and OpenAI agents, all built on accessible Python foundations. Do you want to leverage AI for real-time anomaly detection, automate analysis of forensic artifacts, or develop custom agents that uncover hidden attack patterns and outpace adversaries? From building AI-powered log analysts to integrating automation frameworks like n8n to writing stand along autonomous AI agents, this course equips you with the skills to harness massive data streams, enhance forensics, and create intelligent defenses that keep you ahead.

SEC573: AI-Powered Security Automation positions AI as the core of modern InfoSec. You will be taught to write and debug Python code. And when the code gets a little too complex, you will learn to leverage AI code writing agents to "Vibe code" a solution to today complex problems. Have you ever wondered why so many SANS courses touch on the Python basics? It's because mastering Python is essential for completing advanced labs and staying relevant in fields like data science, machine learning, and penetration testing. This class will teach you the essentials and how to leverage AI to write, explain, and enhance your Python programs to solve real-world problems.

When you're ready to elevate AI from a buzzword to your InfoSec superpower, SEC573 delivers exactly what you need to get started. This course also prepares you for the GPYC certification (GIAC Python Coder), validating your ability to apply AI and Python to solve real-world cybersecurity challenges.

Author Statement

The ability to leverage AI skills to develop new tools is essential for professionals working in all aspects of InfoSec. Understanding how to integrate AI into your workflows means you can automate complex tasks and achieve more, with fewer resources, in less time. SEC573 is designed for network defenders, forensics examiners, penetration testers, and other security professionals who want to learn how to apply AI-driven automation to do their job more efficiently. This course will help take your career to the next level by teaching you this highly sought-after skill. We will focus on the most important skills for security professionals, such as building AI agents, integrating with automation frameworks, and handling prompt injections, all while interacting with networks, websites, databases, and file systems. We will cover these essential skills as we build practical AI applications that you can immediately put into use in your place of work.
—Mark Baggett

Business Takeaways

- Automate system processes with AI to handle inputs quickly and efficiently
- Create AI-driven programs that increase efficiency and productivity
- Develop intelligent tools to provide the vital defenses our organizations need
- Integrate AI agents for proactive threat detection and response
- Streamline forensics and incident response with custom AI automations
- Enhance cloud and network security through AI-powered monitoring and analysis
- Build resilient systems against emerging threats using MCP and OpenAI technologies

Section Descriptions

SECTION 1: Essential Skills Workshop

The course starts with an intro to Python and the pyWars capture-the-flag challenge. Students learn at their own pace in the pyWars lab, with over 100 hands-on labs to build life-changing skills. Advanced students tackle Python bonus challenges, while beginners start with Python essentials

TOPICS: Leveraging AI and Vibe Coding; The Essentials of Python Coding; Variables and Math Operators; Strings and Functions; Visual Studio Code and Debugging Code

SECTION 2: Essentials Knowledge Workshop

You won't learn programming from slides. This section builds on the hands-on approach, covering data structures and programming concepts. Learn to use Python Virtual Environments to resolve library conflicts and organize your setup. We also cover debugging with Visual Studio Code and share tips to become a better Python programmer.

TOPICS: Python Virtual Environments; Python Modules; Lists, Loops, and Tuples; Dictionaries; Tips, Tricks, and Shortcuts

SECTION 3: Automated Defense with AI

In this section, we take on the role of network defenders, using AI to develop code and access data to solve complex challenges. We'll explore AI's limitations and the need for offline analysis, including regex and file analysis. Forensics and offensive security pros will also benefit, as skills like file reading and data parsing are essential for them.

TOPICS: File Operations; Leveraging Code writing Agents and "Vibe Coding"; Developing MCP Server Leveraging Automation Frameworks like n8n; Targeting Useful data with Regular Expressions; Log Parsing, Data Analysis Tools, and Techniques

SECTION 4: Automated Forensics with AI

In our forensics-themed section, we will assume the role of a forensic analyst who has to carve evidence from artifacts when no tool exists to do so.

TOPICS: Processing Unstructured and Structured Data; Developing AI Agents with Chat Completion and Tool Calling; Developing AI Agents with the Responses API; Giving Access to Data Sources such as JSON, Windows Registry, and SQL Data; Accessing Web APIs and Web Applications

SECTION 5: Automated Offense with AI

In this offensive-themed section, we become penetration testers whose attempts have been blocked by modern defenses. You will build an agent to bypass these defenses and gain remote access. We'll also learn how AI agents can be turned against us by exploring AI guardrails, their limitations, and applying them in offensive exercises.

TOPICS: AI Prompt Injection Attacks and Techniques; OpenAI Agent Input and Output Guardrails; Network TCP and UDP Socket Operations; Exception Handling and Process Execution; Blocking and Non-blocking Sockets

SECTION 6: Capstone Workshop

In the final section, you'll team up with other students to apply your skills in programming challenges. You'll solve problems, exploit vulnerable systems, analyze packets, parse logs, and automate code execution on remote systems. Test your skills, tackle challenges, and prove your expertise!

"I have had a few Python courses in the past in school, but I am already learning new things and ways to find new information on Day 1."

—Vergil Daughtery

"Excellent class for learning how to construct automated and advanced discovery analytics for information systems."

— Mary Gutierrez, **Booz Allen Hamilton**

Who Should Attend

- Security professionals who benefit from automating routine tasks so they can focus on what's most important
- Forensic analysts who can no longer wait on someone else to develop a commercial tool to analyze artifacts
- Network defenders who sift through mountains of logs and packets to find evil-doers in their networks
- Penetration testers who are ready to advance from script kiddie to professional offensive computer operations operator
- Security professionals who want to evolve from security tool consumer to security solution provider

NICE Framework Work Roles

- Secure Software Assessor (OPM 622)
- Research & Development Specialist (OPM 661)
- Data Analyst (OPM 422)
- Cyber Defense Analyst (OPM 511)
- Cyber Operator (OPM 321)
- Law Enforcement/CounterIntelligence Forensics Analyst (OPM 211)
- Cyber Defense Forensics Analyst (OPM 212)