CyberSafe X SANS AI Security Fellowship

Application Guide

Everything you need to know before you apply

About the Fellowship

The CyberSafe x SANS AI Security Fellowship is a fully funded advanced training and certification programme for experienced African women in cybersecurity who want to specialise in securing AI systems, applications, and infrastructure.

The fellowship combines SANS OnDemand learning, hands-on labs, structured progression, mentorship, progress support and preparation for two GIAC certifications. It builds on an existing cybersecurity foundation as it is not an entry-level cybersecurity programme

Eligibility

This fellowship is designed for experienced cybersecurity professionals who are ready to specialise. You may be a strong fit if you can say yes to all of the following:

- You are a woman older than 21
- You are African, speak English, and currently resident in an African country.
- You have at least three years of hands-on cybersecurity experience.
- You have a genuine interest in AI security.
- You are able to meet the programme's technical requirements for the full duration (see Technical Requirements below).
- You can commit to the full programme, including certification preparation.
- You are willing to complete the prerequisite AI security course as part of the application process.

The Technical Requirements

Fellows are responsible for their own device and connectivity for the full duration of the programme. The requirements below reflect the most demanding course in the pathway, SEC545, unless otherwise noted.

Hardware

- Processor: x86/x64, 64-bit, 2.5 GHz or faster, multicore. Apple Silicon (M-series) is not supported for SEC598.
- Memory: 16 GB RAM minimum.
- Storage: An SSD is required for SEC545. SEC411 and SEC495 each require 20 GB of free space; SEC598 course media downloads may run 40 to 50 GB.
- Wireless: A wireless network adapter; SEC545 specifically requires 802.11 b/g/n/ac support.

Operating System and Access

- OS: A fully updated, supported 64-bit Windows, Linux, or Intel-based macOS. Apple Silicon Macs are not supported for SEC598.
- Admin rights: Local administrator or root privileges, and the ability to install and configure required software.
- Containers: Docker Desktop, Docker Engine, or a Docker Compose-compatible platform. SEC495 also supports Rancher Desktop.
- Browser: Firefox 120 or later with the SmartProxy extension for SEC545. SEC598 supports current versions of Edge, Chrome, or Firefox.
- Certificates: Ability to install a trusted root certificate, required for SEC545.

Network

- Connectivity: Reliable internet access with the ability to connect over HTTPS, SSH, and SOCKS5 on non-standard ports.
- VPNs and proxies: You must be able to configure or disable VPNs, intercepting proxies, or egress filtering if they interfere with SEC545 labs.

If you're unsure whether your current device meets these requirements, plan to confirm this before applying. The fellowship cannot provide loaner equipment.

Learning Path

Fellows move through four SANS courses in sequence. Each course must be completed before the next is unlocked, and two of the four leads to a GIAC certification.

SEC411	AI Security Principles and Practices: core AI literacy, how large language models work, tokenisation security, attack surface analysis, and the fundamentals of prompt injection and jailbreaking. No prior AI experience required. SEC411 completion unlocks SEC495.	-
SEC495	Leveraging LLMs: building and securing a complete Retrieval-Augmented Generation (RAG) system from the ground up, self-hosted end to end, including access controls and defence against prompt injection. SEC495 completion unlocks SEC545.	-
SEC545	GenAI and LLM Application Security: securing a real GenAI application end to end, vector databases, LangChain agents, MCP, and cloud hosting on Kubernetes, plus AI threat modelling using the MAESTRO framework and a capstone capture-the-flag exercise. GAIPS must be passed before SEC598 access is released.	GIAC AI Platform Security (GAIPS)
SEC598	AI and Security Automation for Red, Blue, and Purple Teams: automating security work, SOAR playbooks, infrastructure as code, and AI-driven detection and response across AWS and Azure. GASAE must be passed for full fellowship completion.	GIAC AI Security Automation Engineer (GASAE

Every fellow receives access to the first course, and completion of one course unlocks the next as courses are released sequentially. All courses are delivered through SANS OnDemand, self-paced with hands-on labs throughout. Courses are taught by practitioners, including instructors holding the GIAC Security Expert (GSE) certification.

How the Selection Process Works

- **Step 1 – Submit Your Application**

Complete the online application form between August 19 and September 10, 2026. Applications are reviewed on a rolling basis.

- **Step 2 – Complete the Prerequisite Course**

Upon completing the application form, applicants get access to a short AI Security prerequisite course. ***Applications proceed to formal review only once you've submitted the required course completion certificate within completed by your assigned deadline.***

- **Step 3 – Eligibility screening and shortlisting**

Your application is assessed against the published programme requirements and selection criteria. ***Selection is competitive. Completing the application and prerequisite does not guarantee an interview or fellowship place.***

- **Step 4 – Interview and Verification**

Shortlisted applicants will participate in an online blind interview and complete identity verification. To verify your identity, you must submit one valid government-issued ID from your country of residence. Examples of acceptable include International travel passport, National identity card, and Permanent residence permit (where applicable). The applicant's name on the submitted valid government-issued ID must match the same name on applicant's CV and LinkedIn profile.

Your submitted ID is used solely for verification purposes. We will not share or distribute your documents with third parties. If you are accepted, your ID will be securely stored for the duration of the programme. If you are not selected, your ID will be immediately deleted.

The interview focuses on your cybersecurity experience, motivation for AI security, learning readiness, and programme commitment.

- **Step 5 – Final Selection and Onboarding**

Selected fellows receive onboarding instructions and complete the required agreement before programme orientation.

- **Step 6 – Begin Your AI Security Journey**

Orientation takes place on October 21, 2026. The fellowship learning journey begins October 26, 2026.

How the Selection Process Works

Applications open	August 19, 2026, 12:00 PM WAT
Applications close	September 10, 2026, 12:00 PM WAT
Applications reviewed	Rolling basis
Selection and feedback	September 30, 2026
Documentation deadline	October 14, 2026
Orientation	October 21, 2026
Training begins	October 26, 2026
Fellowship completion	July 30, 2027

Programme Journey

Oct 2026	Orientation, onboarding, and programme launch
October 26 – November 24, 2026	SEC411
November 27 – December 20, 2026	SEC495
January 4 – April 16, 2027	SEC545 + GAIPS certification
April 19 – July 30, 2027	SEC598 + GASAE certification

What You Need to Prepare Before Applying

Please have the following information and documents ready before you begin your application:

- Personal and professional information, your CV clearly demonstrating your cybersecurity experience, technical responsibilities and relevant professional achievements.
- The application includes questions about your cybersecurity experience, your interest in AI security, your career goals and your readiness to participate in the fellowship.
- Please answer all application questions in your own words and based on your own experiences. We are interested in understanding your individual journey, perspective, motivations and readiness for the fellowship.

How Applications are Assessed

The selection process considers evidence of both cybersecurity experience and readiness for advanced AI security learning.

- Hands-on cybersecurity experience
- Technical depth and practical problem-solving
- Motivation for specialising in AI security
- Evidence of initiative and independent learning
- Readiness for advanced SANS training
- Career goals alignment and potential value of the fellowship
- Communication and ability to explain technical work clearly
- Ability to commit to programme requirements

Frequently Asked Questions

- **Is the fellowship free?**

Yes. It's fully funded, and fellows pay no tuition. Fellows are, however, expected to provide their own laptop meeting the technical requirements and internet access for the programme duration.

- **Who can apply?**

Women aged 21 to 35 who are African, able to participate effectively in an English-language training programme, resident in an African country, with at least three years of hands-on cybersecurity experience.

- **Do I need previous AI experience?**

No prior AI experience is required. A cybersecurity foundation is required.

- **Do I need to be a CyberSafe Foundation alumna?**

No. The fellowship is open to any eligible applicant who meets the stated criteria.

- **Can I apply if I live outside Africa?**

No. Applicants must be African citizens and currently reside in an African country, from the time of application until the completion of the programme.

- **Do I have to complete the prerequisite course?**

Yes. Your application only proceeds to formal review once you've submitted evidence of completing it. Only submissions made through the appropriate channel by your assigned deadline will be considered.

- **Is the training live or self-paced?**

SANS learning is OnDemand and self-paced, but the fellowship has deadlines and progress requirements you're expected to meet.

- **Are all four courses available from the start?**

No. Courses are released sequentially: completing one unlocks access to the next.

- **Can I work full-time while doing the fellowship?**

The programme is designed for working cybersecurity professionals, but you'll need to protect regular study time and meet deadlines, particularly during certification preparation.

- **Can students apply?**

Yes. Students are eligible provided they meet the minimum work experience requirement and agree to all programme commitments.

- **How much time should I plan for?**

Approximately 4 to 6 hours per week during standard learning periods, with more required during certification preparation and exam periods. Some weeks may need more time depending on your pace, lab work, and exam readiness.

- **What are the technical requirements to participate?**

You'll need a personal laptop meeting the programme's minimum specifications (16 GB RAM, a 64-bit OS, admin rights, and enough free storage for course labs), plus reliable internet access. Full details are in the Technical Requirements section above.

- **Can I use a Mac for the fellowship?**

An Intel-based Mac is supported. Apple Silicon (M-series) Macs are not supported for SEC598, the fellowship's final course, so if your only device is an M-series Mac, you'll need another option for that stage.

- **What if my laptop doesn't meet the requirements?**

You're responsible for ensuring your device meets the technical requirements before you apply. The fellowship is unable to provide loaner equipment, so this is worth confirming early rather than after you've been selected.

- **Do I need administrator access on my laptop?**

Yes. Several courses require you to install and configure software, including container platforms and browser extensions, which needs local administrator or root privileges.

- **Will I have costs beyond my time?**

Course access, labs, and GIAC exam attempts included in the pathway are fully funded. You are responsible for your device, internet access, and any costs of meeting the technical requirements.

- **What happens if I fall behind on a course?**

The fellowship includes biweekly progress reviews. If you're falling behind, CyberSafe Foundation and SANS will work with you on a documented recovery plan with clear deadlines.

- **What happens if I fall behind on a course?**

The fellowship includes biweekly progress reviews. If you're falling behind, CyberSafe Foundation and SANS will work with you on a documented recovery plan with clear deadlines.

- **What if I don't pass a GIAC exam on my first attempt?**

This is handled case by case with SANS and CyberSafe Foundation. Reach out as soon as you know you're at risk so a plan can be put in place before it affects your progression

- **Can I use AI to help write my application answers?**

No. The application questions must be answered in your own words. We ask you not to use AI writing tools, such as ChatGPT or similar, to generate your responses. Reviewers are assessing your personal experience, reasoning, and communication style, and applications that appear to be AI-generated will be disqualified.

Questions

Email aisecurity@cybersafefoundation.org

Connect With Us

Instagram: https://instagram.com/cybersafehq

Twitter: https://twitter.com/cybersafehq

LinkedIn: https://linkedin.com/company/cybersafefoundation

Facebook: https://facebook.com/cybersafefoundation