Cybersecurity



Cybersecurity Analyst (US Apprenticeship)

Personal mentor OpenClassrooms Certification

Become a fully-fledged junior cybersecurity analyst and embark on a fulfilling career in cybersecurity.

TRAINING PERIOD

12 months of full-time study

12 months in apprenticeship**

PATH DURATION:

402 hours supervised

OPENCLASSROOMS

This training program requires an estimated time commitment of 804 hours: 402 hours of supervised training (projects coached by mentors) and 402 hours of guided training (courses and educational resources). In apprenticeship, the total training duration does not include the time spent at the company.
The training period can be extended in the case of part time training. This estimated average duration depends on the student entry level into training, their time allocated per week, their availability, their capacity, and learning pace.

** Check training program eligibility based on the contract type (professional training contract or apprenticeship contract)

Training program last updated on Nov 16, 2026

Cybersecurity Analysts: What Are Their Responsibilities?

Cybersecurity professionals are instrumental in safeguarding organizations from cyber threats and ensuring their success. Your life as a cybersecurity professional can be very different, depending on the specific job you do:

- On the **offensive** side of cybersecurity, penetration testers and ethical hackers are here to **identify vulnerabilities** in systems, **simulate cyber attacks** to test the effectiveness of security measures, and **provide recommendations** for improving security.
- On the **defensive** side, SOC Analysts and incident responders typically **monitor and defend** networks against security threats, **analyze security breaches**, and ensure the integrity of information systems.
- **Governance**-wise, GRC analysts – for Governance, Risk, and Compliance – focus on ensuring that the organization **manages risks effectively**, maintains governance standards and complies with **regulatory requirements**.

As a cybersecurity analyst, you might actually find yourself involved in all these activities to varying extents and levels of autonomy, depending on the responsibilities of your team. That's why our program encompasses all three aspects and the associated skills.

Uncertain of a career in cybersecurity? Start with our Cybersecurity core mastery bootcamp!
You will practice recurrent cybersecurity activities, become proficient in them, and see for yourself if you're willing to make it your job!
Bonus: Bootcamp graduates directly qualify for our Cybersecurity Analyst apprenticeship!

What Skills Will You Learn During This Training?

Our program propels IT professionals directly into the heart of the cybersecurity arena. We will train you to be versatile, with operational competencies in the pivotal roles of SOC Analyst for **defensive security**, Ethical Hacker/Pentester for **offensive security**, and GRC Analyst for **governance, risks and compliance**.

Over the course of this training program, we'll thus teach you a variety of skills, including how to:

- Raise employees' awareness and commitment to cybersecurity

- Conduct a Web penetration test and share its results and recommendations
- Secure critical assets and infrastructure
- Automate recurrent activities by writing and running scripts in Python
- Investigate cybersecurity incidents and contain attacks
- Assess the compliance and risk level of a supplier

In addition to these technical skills, you'll also learn transversal or "soft" skills, which will help you grow in your career.

This holistic approach ensures you will not just be a specialist in one domain but a fully-fledged junior cybersecurity analyst, prepared to tackle diverse challenges head-on.

The value for your employer and your career is twofold:

- Initially, you will **bring an immediate proficiency in key cybersecurity activities**, executing tasks efficiently, proactively, and reliably.
- As you grow in your role over time, you will already possess the foundational knowledge to **specialize in any of the three core areas**, aligning your skills with the evolving needs of your organization.

General security concepts, security architecture, security operations, security program management & oversight, threats, vulnerabilities & mitigations: Our curriculum is meticulously mapped to the CompTIA Security+ certification, recognized by the DoDD 8140, ensuring a commitment to both excellence and ethics.



OpenClassrooms is an authorized CompTIA Delivery Partner. This training includes a voucher for the CompTIA Security+ exam, available upon completion.

How Do OpenClassrooms Apprenticeships Work?

Apprenticeship programs combine paid on-the-job learning with online project-based instruction that equips employees for high-demand careers in data, technology, and business development.

Here's how it works:

1. **Onboarding** (2-3 weeks prior to start of apprenticeship): Familiarizes both the apprentice and the employer with the training components and requirements.
2. **Pre-apprenticeship** (3 months of training): Provides the apprentice with scenario-based project learning coupled with weekly mentorship and skills building courses in preparation for the formal apprenticeship program. This cybersecurity core mastery bootcamp is ideal for those needing to develop and demonstrate their cyber-awareness and proficiency in key activities before starting their apprenticeship.
3. **Apprenticeship** (12 months on-the-job, with one day per week of instruction): Continues to build apprentice's skills via on-the-job training, corresponding online instruction, and weekly one-to-one mentoring sessions.
4. **Get certified**! Following completion of the apprenticeship program, apprentices earn an industry-recognized and nationally portable credential from the U.S. Department of Labor.

Projects

At OpenClassrooms, learning is project-driven because that's the fastest way to become proficient. Projects offer hands-on experience so you can hit the ground running when you start your new job.

This path has nine projects that you'll need to complete, one at a time. You'll receive a detailed brief with the context, customer requirements, and additional details. Then it's up to you to go and make it real! To do this, you'll have to be creative, coming up with innovative solutions to the questions at hand.

Want to see an example of a project? Read our blog post here.

Online But Never Alone!

Before, during, and after the training program, you'll be accompanied by humans:

- One-to-one weekly mentorship sessions with a professional in the field, in partnership with

OpenClassrooms, who'll provide you with support and guidance to complete your projects.
- OpenClassrooms staff who'll help you succeed in your apprenticeship.
- Our global community of student peers with whom you'll be in regular contact through our online platform.



Thomas ROCCIA, Senior Security Researcher at Microsoft, and mentor on OpenClassrooms' Cybersecurity paths.

> "As a mentor, my role is to support students and share my professional experience in the field of cybersecurity. What's exciting is to guide and accompany enthusiastic and motivated students, as this allows us to develop our pedagogical skills and transmit our passion for this constantly evolving field." Thomas

Are You Eligible for This Apprenticeship?

To be eligible for this apprenticeship, you must demonstrate proof of the following prerequisites:

- Be over 18 years of age and have the right to work in the U.S.
- Have a high school/secondary school degree, vocational certificate, or equivalent.

Technical prerequisites:

To get the most out of this program, you should already have some level of **IT proficiency** and **cyber-awareness**.

IT Proficiency can be evidenced by having an Associate's level degree or equivalent in IT (like graduating from our Help Desk Technician training program) or possessing at least 2 years of professional experience in IT.

Cyber-awareness can be developed through our 3-month Cybersecurity core mastery bootcamp. Alternatively, already holding introductory certifications like the ISC2 CC or ISACA CFC will equip you with the necessary foundational knowledge to make a success of this apprenticeship program.

Language: a good level of English (for non-native speakers, a CEFR level of B2, an IELTS band score of 6.5, or a TOEFL score of 80 is recommended).

Equipment: access to a computer (PC or Mac with x86-64 CPU), headphones, a webcam, and a stable internet connection.

- At least 8GB of RAM and 50GB of free storage space available on your computer (16GB of RAM and 100GB of free storage space are recommended).
- Administrator rights to your computer in order to install required programs.

Important Information About Starting Your Apprenticeship

To begin your journey as a **Cyber Security Analyst Apprentice**, you'll need to be employed by a company that supports your apprenticeship. If you haven't yet secured an employer, don't worry—OpenClassrooms is here to help. Our team can provide guidance and resources to connect you with potential employers who align with your career aspirations.

Start your apprenticeship with confidence, knowing that we're committed to supporting you every step of the way.

Project 1 - 12 hours

Dive into Your Cybersecurity Analyst Training

Discover your projects and plan your training.

Skills

- Prepare for your training

Associated courses



Set Yourself Up for Success in Your OpenClassrooms Training

Easy 2 hours

This course will guide you through the first steps of your OpenClassrooms training program—showing you how to get started on your program and complete your first project.



Discover the World of Cybersecurity

Easy 4 hours

Understand the intricacies of a cyberattack—one of today's major challenges—and dive into the many roles within cybersecurity. One might just be your future career!



Improve Your Productivity With ChatGPT

Easy 4 hours

Learn how to use ChatGPT to improve your productivity and discover how “prompt engineering” can help you save time on your work tasks.

Project 2 - 50 hours

Raise Employees' Awareness and Commitment to Cybersecurity

Your organization’s employees’ cybersecurity habits have led to serious incidents in the past. Your mission: to draw up a user charter and organize its deployment to win everyone’s engagement.

Skills

- Communicate with policy violators to ensure future compliance
- Raise awareness within the company on cybersecurity issues
- Write a user charter supporting the global security policy

Associated courses



Discover the World of Cybersecurity

Easy 4 hours

Understand the intricacies of a cyberattack—one of today’s major challenges—and dive into the many roles within cybersecurity. One might just be your future career!

Project 3 - 20 hours

Let's Capture Flags - CTF Challenges

As a cybersecurity enthusiast, discover Root-Me and solve challenges in different categories in order to adopt the mindset of an attacker.

Skills

- Perform penetration tests on web applications

Project 4 - 40 hours

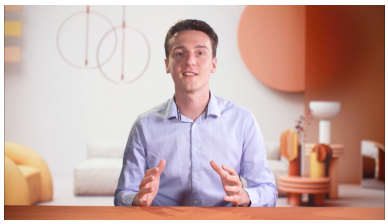
Conduct a Web Penetration Test

Assess the security of a client's information system by conducting a web penetration test, from enumeration to the exploitation of vulnerabilities, in order to provide a detailed report.

Skills

- Compile your findings into a clear and professional report for your supervisor
- Conduct penetration tests to evaluate the risks associated with those vulnerabilities
- Explore a website to map its structure and functionalities
- Identify potential vulnerabilities that could compromise its security

Associated courses



Conduct a Web Penetration Test

Medium 10 hours

Put yourself in the shoes of an attacker and perform a full penetration test on a web application, using the methods and tools of a professional pentester!

Project 5 - 60 hours

Secure Critical Assets and Infrastructure

An audit has been conducted on your company's Active Directory infrastructure. Based on the raw recommendations provided by the auditor, you are tasked with creating an efficient and prioritized action plan.

Skills

- Secure the company infrastructure
- Translate audit recommendations into a comprehensive action plan

Associated courses



Secure Your Active Directory and Windows Domains

Medium 6 hours

Learn the techniques used by attackers so you can resolve the vulnerabilities they exploit and monitor your Active Directory environment.

Project 6 - 30 hours

Write and Run Scripts in Python

A web hosting company supervising its public IPs wants to automate the neutralization of compromised files. Automate the cleaning of compromised files with Python.

Skills

- Contain a simple security incident
- Solve a security incident by following SOC procedures

Associated courses



Learn Python Basics

Easy 6 hours

Python is user-friendly for beginners and in high demand. Even the basics of data and program logic will empower you to write simple, powerful code. We'll practice a useful automation task called web scraping, an extract-transform-load process (ETL).

Project 7 - 80 hours

Investigate cybersecurity incidents and contain attacks

Based on observable elements collected, you will carry out in-depth analyses of several security incidents and identify possible containment actions.

Skills

- Investigate a cybersecurity incident
- Respond to an email phishing attack
- Write an incident report with recommendations for the company

Associated courses



Dive Into the World of Cybersecurity Incident Detection and Response

Medium 6 hours

Learn how to detect and address cybersecurity incidents by contributing to the creation and enhancement of a Security Operations Center (SOC).

Project 8 - 60 hours

Assess the Compliance and Risk Level of a Supplier

Find a partner contractor with whom your organization works and perform a third party compliance assessment and a risk assessment on them to reduce the risk of a supply-chain attack.

Skills

- Assess an organization 's compliance with a cybersecurity framework (NIST CSF/ISO 27001)
- Perform a risk assessment

Project 9 - 50 hours

Keep Your Exposure to Compromise Under Control

Perform a vulnerability watch and extract patches to be deployed, fixes to be applied and IOCs to be hunted. From this, develop a pragmatic action plan to maintain control over the risks of compromise.

Skills

- Analyse packet capture file
- Identify IS security breaches and risk of compromise
- Write scripts to find IOCS / automate blocking of IOCs
- Contribute to cybersecurity watch and threat activities

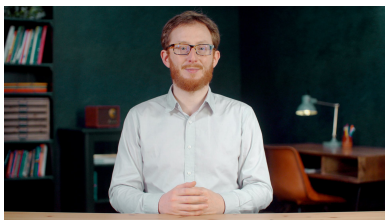
Associated courses



Learn Python Basics

Easy 6 hours

Python is user-friendly for beginners and in high demand. Even the basics of data and program logic will empower you to write simple, powerful code. We'll practice a useful automation task called web scraping, an extract-transform-load process (ETL).



Learn Programming With Python

Easy 12 hours

Are you a Python beginner? Take your basic coding skills to the next level with object-oriented programming. Practice using methods, classes, inheritance, and modules, and start coding your own applications!



Conduct Your Cybersecurity Watch

Easy 4 hours

Discover the essential techniques and tools for conducting effective cybersecurity monitoring!