TRAINING PROGRAM

Semafor
CONSEIL

Foundations
Network Security
OSINT
Threat Management
WebApp Security

Sessions

August 23rd

October 4th

2021

semafor-conseil.swiss

First set starts on August 23rd 2021: **Expand** your cybersecurity **knowledge**

Mondays

Network Security

5 days online

23th & 30th Aug.
6th, 13th & 20th Sept.

Tuesdays

Applications Security

5 days online

24th & 31th Aug.
7th, 14th & 21th Sept.

Wednesdays

Threat Management

5 days online

25th Aug.
1st, 8th, 15th & 22th Sept.

Thursdays

Open Source Intelligence

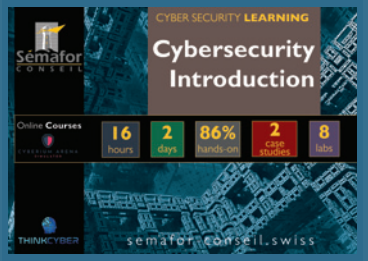
5 days online

26th Aug.
2nd, 9th, 16th & 23th Sept.

Fridays

Foundations

Theory



2 days online

27th Aug.
3rd Sept.

Technique

3 days online

4th , 17th & 11th Sept.

Second set starts on October 4th 2021: Taking your **knowledge** to the **next level**

Mondays

Network Security

5 days online

4th, 11th, 18th & 25th Oct.
1st Nov.

Tuesdays

Applications Security

5 days online

5th, 12th, 19th & 26th Oct.
2nd Nov.

Wednesdays

Threat Management

5 days online

6th, 13th, 20th & 27th Oct.
3rd Nov.

Thursdays

Open Source Intelligence

5 days online

7th, 14th, 21th & 28th Oct.
4th Nov.

Fridays

Foundations

Theory

2 days online

8th & 15th Oct.

Technique

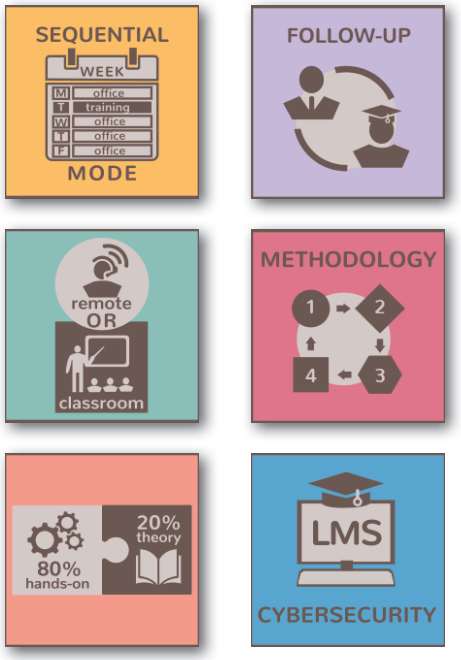
3 days online

22th & 29th Oct.
5th Nov.

OUR LEARNING MANAGEMENT APPROACH

Sémafor Conseil's learning management is participant centric. The enrollment of the practitioner is carefully planned and articulated in order to provide him with the best possible learning experience.

Once entered into the **participant management process (personalized coaching)**, the practitioner will be invited to come and get involved in the chosen training, in our **Cyberium Arena (LMS)**. The later is a virtual learning and training zone, disconnected from any system, which will allow the practitioner to **learn, test, train**, all the tips and tricks related to his profession. Without danger, the practitioner will spend **80 to 90% of his training** time in this Cyberium. Whether it is for the simulations or for the labs, the examples taken by the facilitator are the most recent and always as close to reality as possible.



Of course, all this practice will be supported by the most robust theories (20% of the remaining time).

As our trainings are delivered in **"sequential" mode** (one day per week over 5 weeks), thus enabling the participants to have time to harness the content of the courses in a much deeper fashion then with a block approach, as well as giving the opportunity to build a meaningful project

In addition, in order to provide maximum flexibility and comfort and to let the participant focus 100% on his training, it can be followed from the **place of his choice (home, office, nomad)**, in agreement with his employer.

Benefits for:

Human Ressources

For Human Resources Managers, we create efficient training paths, which are palatable and enabling participants to keep their agendas available 4 days a week for the duration of the course, thus providing an immediate return on investment throughout the course, from the first training day, as the practitioners can incorporate its learning into its daily practice .

IT & Cybersecurity Management

For managers, we offer training module that provides the most current topical knowledge in cybersecurity in order for the participants to deliver an immediate return on investment with strong and engageable technical skills, which the practitioners can leverage with confidence on the job.

Practitioners

For the company's practitioners, we create unique conditions for effective and innovative courses focused on cybersecurity, leveraging the most up-to-date training environment, where participants can explore and discover safely the uses of the tools they are exposed to. The practitioners are supported throughout the courses by a team of expert coaches and trainers, which will empower them to be successful; they can also leverage the acquired knowledge to pass related certifications.

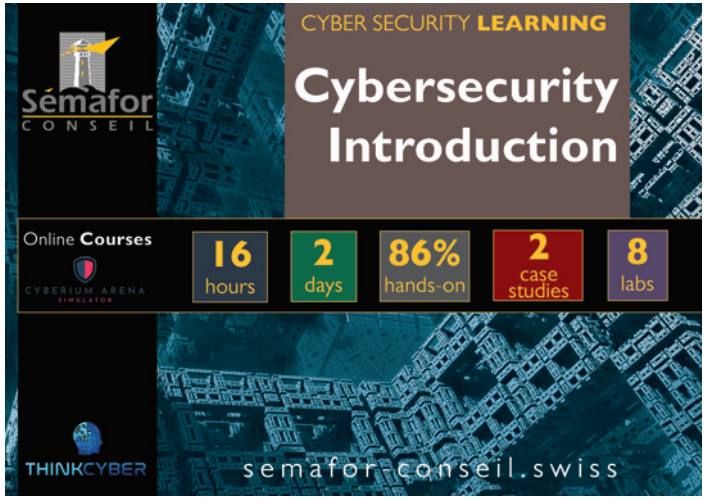
foundations

Cybersecurity Foundations

This track covers the fundamental concepts of cyber defense and practical understanding of basic tools and technics using our LMS, the CYBERIUM ARENA platform.
Participants learn the basics of the various concepts as they get to grips with basic cybersecurity technology products.

Sémafor CONSEIL

Expand your cybersecurity **knowledge**



Introduction to Cybersecurity is an essential course covering main topics from the cyber world and allows the participants to quickly view the complex world of digital crimes.

This training covers the core concepts of defense and understanding in the practical world using the CYBERIUM ARENA simulator. Participants will learn about different domain structures and security technology products.

This course is essential for:

Any Manager who wants to have basic knowledge in cybersecurity to understand the cyber world and foundation knowledge to make decision/investment to secure companies informations.

Complete syllabus online:
https://semafor-conseil.swiss/en/ns101-cybersecurity-introduction/

Taking your **knowledge** to the **next level**

Cryptography is an indispensable tool for protecting information in computer systems. In this course, you will learn the inner workings of cryptographic systems and how to use them in real-world applications correctly.

From ancient examples of secret messages and the spies that cracked them to modern cryptographic applications, you will have the opportunity to explore the foundations of data security.

This course is essential for:

- Cybersecurity beginners
- Anyone intersted in cryptography
- Anyone curious about how the datas are encrypted to be secured

Complete syllabus online:
https://semafor-conseil.swiss/en/bt216-cryptography/

foundations

Sémafor CONSEIL

Expand your cybersecurity knowledge

This training covers basic use in the Linux environment. Linux Introduction course is designed for non-experienced users, helping them become comfortable with Linux and basic automation scripting capabilities.

This course is essential for:

- Anyone comfortable with computers who wants to have basic knowledge with Linux System
- Anyone who wants to start a carreer in cybersecurity
- Any Manager who has to deal with IT & Security teams

Complete syllabus online:
https://semafor-conseil.swiss/en/ns103-linux-introduction/

Taking your knowledge to the next level

Any person wanting to automate stages and create cyber-tools must learn to program. Python is an easy language used by many to build tools in different fields, including cyber.

This training will provide the participant with a stepping-stone on understanding programming logic and creating basic scripts to take his skills to the next level.

This course is essential for:

- Anyone comfortable with computers who wants to learn the foundation of the most common cybersecurity language
- Softwares and Apps developers

Complete syllabus online:
https://semafor-conseil.swiss/en/ns105-python-intro/

Sémafor CONSEIL

network security

Network Security

Network security encompasses a wide number of technologies, devices and processes. After theses courses, you will be able to discover security vulnerabilities throughout the network using exploration & discovery and vulnerability analysis techniques. You will understand the different types of firewalls available and master hardening for Windows and Linux servers.

Sémafor CONSEIL

Expand your cybersecurity **knowledge**

Network security is a broad term that covers multiple technologies, devices, and processes. Nowadays, every organization, regardless of size, industry, or infrastructure, requires a network security expert in place to protect it from the ever-growing landscape of cyber threats today.

After this course, you will discover security vulnerabilities across the entire network using network hacking techniques and vulnerability scanning. You will understand the various types of firewalls available and master both Windows and Linux servers' hardening.

This course is essential for:

- Computer or network specialists who want to turn their knowledge into security perspectives
- Network operatives
- Programmers & Developers

Complete syllabus online:
https://semafor-conseil.swiss/en/bt208-network-security/

Taking your **knowledge** to the **next level**

Penetration testers face a combination of intrusion detection systems, host-based protection, hardened systems, and analysts that pour over data collected by their security information management systems.

Penetration tests help find flaws in the system to take appropriate security measures to protect the data and maintain functionality. This training will provide the participant with a stepping stone on running penetration testing in practice and taking on the complex task of effectively targeting and planning a penetration attack on a traditionally secured environment.

This course is essential for:

This course targets people from the IT world that want to upgrade their careers and master the art of penetration testing.

- Network & IT operatives
- Incident responders
- Pen Testers who want to update or upgrade their skills

Complete syllabus online:
https://semafor-conseil.swiss/en/bt212-penetration-testing/

Expand your cybersecurity knowledge

OSINT

intelligence

Open Source INTelligence (OSINT)

Open Source Intelligence (OSINT) covers the techniques and procedures used to retrieve targeted information from freely accessible networks containing vast amounts of data.

Sémafor CONSEIL

Network security is a broad term that covers multiple technologies, devices, and processes. Nowadays, every organization, regardless of size, industry, or infrastructure, requires a network security expert in place to protect it from the ever-growing landscape of cyber threats today.

After this course, you will discover security vulnerabilities across the entire network using network hacking techniques and vulnerability scanning. You will understand the various types of firewalls available and master both Windows and Linux servers' hardening.

This course is essential for:

- Intelligence officers
- Police officers
- Private/public Investigators
- Forensics investigators
- Reporters/Journalists

Complete syllabus online:
https://semafor-conseil.swiss/en/bt214-osint/

Taking your knowledge to the next level

Open-source intelligence (OSINT) Automation covers the techniques and procedures practiced retrieving targeted information from open-source networks containing immense amounts of data using automatic tools to achieve maximum results.

This course teaches participants how to collect and analyze information using different tools and creating automation. Participants will be further exposed to collecting information from the Darknet, social networks, and other sources.

This course is essential for:

This course targets mostly law-enforcement wanting to master the art of finding data around the internet.

- Threat intelligence analysts
- Cybersecurity professionals
- Law enforcement personnel
- Private/public Investigators
- Forensics investigators

Complete syllabus online:
https://semafor-conseil.swiss/en/bt221-osint-automation/

Threat Management

At the core of any cybersecurity implementation there is threat management, by setting up the structures, such as a SOC enabling the organisation to face threats, and by giving the means to hunt them efficiently to reduce the risks and improve the organisation's overall posture.

Sémafor CONSEIL

Expand your cybersecurity **knowledge**

Nowadays, a Security Operation Centers (SOC) should have everything it needs to mount a competent defense of the constantly changing IT enterprise. The SOC includes a vast array of sophisticated detection and prevention technologies, cyber intelligence reporting, and access to a rapidly expanding workforce of talented IT professionals.

This SOC Operation course is designed for SOC organizations to implement a SOC solution and provide full guidance on the necessary skills and procedures to operate it. The training will provide participants with all aspects of a SOC team to keep the enterprise's adversary.

This course is essential for:

- Computer specialists to begin or evolve in cybersecurity with network foundation knowledge
- People implicated in internal security policy

Complete syllabus online:
https://semafor-conseil.swiss/en/bt222-soc-analyst/

Taking your **knowledge** to the **next level**

In today's cybersecurity landscape, it isn't possible to prevent every attack. Threat hunting is the proactive technique that focuses on pursuing attacks and the evidence that attackers leave behind when they patrol an attack using malware or expose sensitive data.

The process is important and is based on thinking that the attacker has already managed to infiltrate and test everything possible to detect intrusion earlier to stop them before intruders can carry out their attacks and exploit them illegally.

This course is essential for:

Specialists and operatives with networking knowledge who want to acquire the threat hunting capabilities to protect their organization better.

- Network administrators/specialists
- Security Testers
- Cybersecurity consultants
- Ethical Hackers

Complete syllabus online:
https://semafor-conseil.swiss/en/bt223-threat-hunting/

WebApp security

Web Applications Security

Applied web security is specifically about the security of websites, web applications (WebApp). At a higher level, Web security covers the principles of cybersecurity applied to the Internet and Web systems.

Sémafor CONSEIL

Expand your cybersecurity **knowledge**

The Web Application Security course will help participants understand web application languages and their exploitation. Participants will learn a proven process for locating these flaws consistently.

This training program's primary goal is to help security specialists understand web application risks in their organization and learn how to conduct web application security assessments.

This course is essential for:

- Webmasters
- Web Apps/Services Designers
- PHP Developers
- Intranet/Internet Developers

Complete syllabus online:
https://semafor-conseil.swiss/en/rt422-web-application-security-intermediate/

Taking your **knowledge** to the **next level**

During this training, participants will get knowledge and skills of the pentesters procedure to detect security vulnerabilities in web applications using a combination of manual and automated techniques and methods.

Testing web-application security is not intuitive, and to be useful, you need an understanding of web application design, HTTP, JavaScript, browser behavior, and potentially other technologies.

This course is essential for:

- Internet/intranet developers to secure datas
- Penetration Testers
- Cybersecurity consultants
- Security architects
- Red team specialists
- Ethical hackers

Complete syllabus online:
https://semafor-conseil.swiss/en/rt423-webapp-security-advanced/

TRAINING PROGRAM

Sémafor CONSEIL

Our current practitioner training courses offering covers 5 key areas of cybersecurity, Network Security, Web Application Security, Threat Management and OSINT, as well as Fundamentals in Cybersecurity, Cryptography, Linux system engineering and also an introduction to Python.

Sémafor Conseil has a much broader catalog encompassing 30 courses, which go well beyond the above knowledge areas, covering forensics, exploit development, and as well industrial control systems.

Guillaume Ibsaïenne

Learning & Development Manager

+41 79 548 67 85

guillaume.ibsaienne@
semafor-conseil.swiss

Guillaume Saouli

Managing Partner

+41 78 921 37 40

guillaume.saouli@
semafor-conseil.swiss

semafor-conseil.swiss

+41 21 728 19 65