

FORMATION CYBERSÉCURITÉ



Programme

Automne

2021

Foundamentaux
Sécurité réseaux
OSINT (Renseignement)
Gestion des menaces
Sécurité des WebApp

semafor-conseil.swiss

Sécurité Réseau

5 Lundis

Sécurité des WebApp

5 Mardis

Gestion des menaces

5 Mercredis

Renseignement Sources Ouvertes

5 Jeudis

Foundamentaux

Sensibilisation
2 Vendredis

Compétences
3 Vendredis

Premier niveau : Développez vos connaissances en cybersécurité

Sécurité Réseau

Cours en ligne: 40 heures, 5 jours, 92% pratique, 5 études de cas, 13 labos

Sécurité réseau

Passer en revue toutes les failles d'un réseau en utilisant des techniques de hackers et des scans de réseaux pour découvrir les vulnérabilités.

Sécurité des WebApp

Cours en ligne: 40 heures, 5 jours, 85% pratique, 5 études de cas, 8 labos

Sécurité des WebApp

Comprendre les technologies et les langages utilisés pour la création d'applications et sites Web et apprendre à les sécuriser.

Analyse SOC

Cours en ligne: 40 heures, 5 jours, 90% pratique, 5 études de cas, 11 labos

Analyse SOC

Apprendre les méthodes et outils nécessaires à la mise en place d'un Centre des opérations de sécurité (SOC) performant.

OSINT

Cours en ligne: 40 heures, 5 jours, 88% pratique, 5 études de cas, 8 labos

OSINT

Apprendre la recherche d'information ciblée dans l'immensité des données publiques disponibles sur le Web, les réseaux sociaux et le Darkweb.

Introduction à la Cybersécurité

Cours en ligne: 16 heures, 2 jours, 86% pratique, 2 études de cas, 8 labos

Intro à la cybersécurité

Découverte du monde cyber et des menaces quotidiennes auxquelles nous sommes tous confrontés. Tout public.

Introduction à Linux

Cours en ligne: 24 heures, 3 jours, 90% pratique, 3 études de cas, 8 labos

Intro à Linux

Apprendre à utiliser Linux pour les débutants. Linux permet de sécuriser son informatique et peut s'installer sous un système Windows.

Deuxième niveau : Perfectionnez vos connaissances

Tests d'intrusion PenTest

Cours en ligne: 40 heures, 5 jours, 90% pratique, 5 études de cas, 10 labos

Tests d'intrusion

Apprendre à détecter les failles, prévenir les intrusions et maintenir l'activité avec différents outils au travers de simulations.

Piratage des WebApp

Cours en ligne: 40 heures, 5 jours, 85% pratique, 5 études de cas, 8 labos

Piratage des WebApp

Apprendre à pirater les applications et sites Web afin d'acquérir un haut niveau en protection pour les sécuriser au maximum du possible.

Traque aux menaces

Cours en ligne: 40 heures, 5 jours, 90% pratique, 5 études de cas, 11 labos

Traque aux menaces

Acquérir les compétences techniques pour prévenir des menaces de façon pro-active, détecter les intrusions à temps et collecter les preuves des intrusions.

OSINT Automatisation

Cours en ligne: 40 heures, 5 jours, 88% pratique, 5 études de cas, 8 labos

OSINT Automatisation

Apprendre à créer des automatisations de recherche d'information ciblée parmi les données publiques disponibles sur le Web, les réseaux sociaux et le Darkweb.

Cryptographie

Cours en ligne: 16 heures, 2 jours, 83% pratique, 2 études de cas, 4 labos

Cryptographie

Découverte des fondamentaux de la cryptographie et d'outils de chiffrement utilisés pour la sécurisation des données pour débutants.

Introduction à Python

Cours en ligne: 24 heures, 3 jours, 90% pratique, 3 études de cas, 8 labos

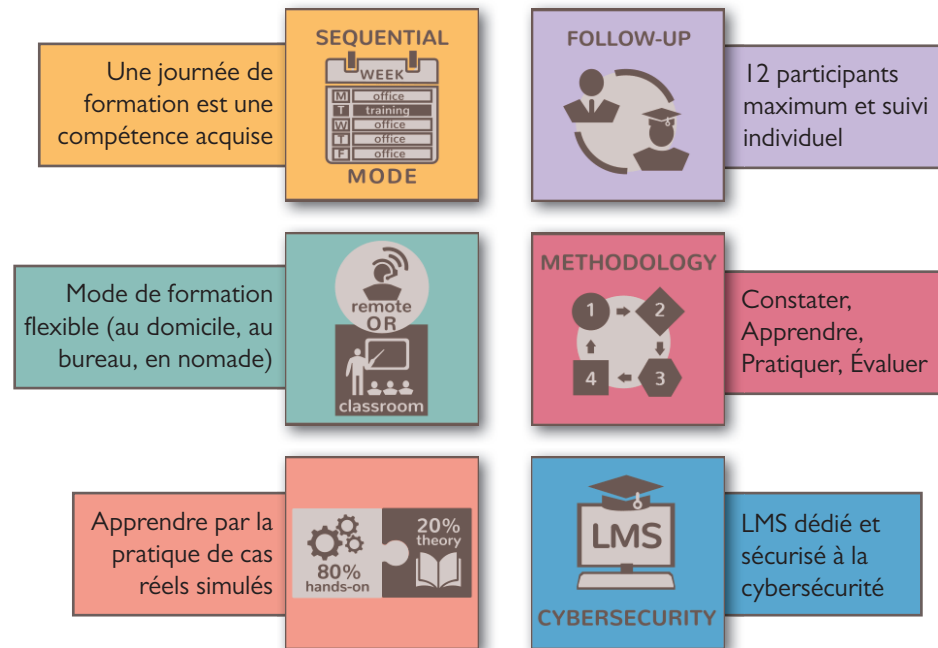
Intro à Python

Apprendre la base du langage Python, le langage le plus facile et pratique pour le développement, particulièrement utilisé pour la cybersécurité.

NOTRE APPROCHE PÉDAGOGIQUE

Chaque futur expert est au centre de la méthode de formation à la cybersécurité de Sémafor Conseil. Il établit son programme de formation selon les compétences qu'il souhaite développer. La formation choisie est **planifiée et articulée** de façon à procurer la meilleure expérience technique.

Le participant est invité à s'impliquer dans notre Cyberium Arena (LMS), un espace virtuel d'apprentissage et de formation, déconnecté de tout autre système, sur lequel il passera plus de **80% de son temps** de formation. Que ce soit pour les simulations ou les labos, les exemples choisis par le formateur sont des **cas d'actualité** les plus récents et au plus **près de la réalité**.



Naturellement, toute cette pratique s'appuie sur des **enseignements théoriques** (20% du temps). Les formations sont conduites à raison d'une journée par semaine sur une durée cinq semaines ce qui laisse **du temps pour s'approprier le contenu** de façon approfondie et permet de bâtir un **projet significatif**.

Tous les cours théoriques et pratiques dans le **Cyberium Arena (LMS)** sont accessibles **en ligne** depuis le lieu qui convient le mieux (bureau, maison, nomade).

Les avantages pour :

Ressources Humaines

Pour les responsables de ressources humaines, nous créons des parcours de formation, efficaces et tangibles, qui permettent aux participants de garder leur agenda professionnel ouvert. Ceci fournit ainsi un retour sur investissement immédiat à travers tout le cours, du premier au dernier jour, car le participant peut intégrer la formation apprise à ses activités quotidiennes.

Direction IT & Cybersécurité

Pour les responsables, nous offrons des modules de formation couvrant les connaissances dans tous les domaines d'expertise en cybersécurité, permettant aux membres de leur équipe en formation de mettre en pratique les compétences immédiatement.

Participants

Pour les praticiens, nous créons des conditions uniques pour ces cours de haut niveau et innovateurs focalisés sur la cybersécurité, utilisant un environnement de formation, dans lesquels les participants peuvent explorer et expérimenter les meilleures pratiques en toute sécurité. Les praticiens sont accompagnés tout au long du cours par une équipe de coaches experts et de formateurs qui les conduisent à la réussite. Les connaissances acquises peuvent aussi être utilisées pour passer des certifications en relation avec le sujet.

Développez vos connaissances en cybersécurité

foundations



Fondamentaux de la cybersécurité

Ce domaine couvre les concepts fondamentaux de la cyberdéfense et la pratique des outils et techniques de base au travers de la plateforme Cyberium Arena. Les participants apprennent les fondamentaux de nombreux concepts de la cybersécurité et la prise en main des outils courants.



FORMATION CYBERSÉCURITÉ
Introduction à la Cybersécurité

Cours en line
16 heures | 2 jours | 86% pratique | 2 études de cas | 8 labos

THINKCYBER | semafor-conseil.swiss

Le cours d'introduction à la cybersécurité couvre tous les domaines du monde cyber et offre aux participants une vue globale de la complexité de la cybercriminalité.

Ce cours ne nécessite pas de compétence technique spécifique en informatique. Il est conçu pour que tout à chacun puisse découvrir le monde cyber et les menaces quotidiennes auxquelles nous sommes tous confrontés. Les participants apprendront différents domaines et technologies de la cybersécurité.

Ce cours s'adresse à :

Tout dirigeant, responsable de service, manager qui veut acquérir les connaissances de base en cybersécurité, comprendre le monde de la cybercriminalité et prendre toute décision afin de sécuriser son entreprise et sensibiliser ses équipes.

Détails du cours sur le site :
<https://semafor-conseil.swiss/en/ns101-cybersecurity-introduction/>

Perfectionnez vos connaissances

FORMATION CYBERSÉCURITÉ
Cryptographie

Cours en line
16 heures | 2 jours | 83% pratique | 2 études de cas | 4 labos

THINKCYBER | semafor-conseil.swiss

La cryptographie est un outil indispensable dans la protection des données numériques. Dans ce cours, les participants apprennent les mécanismes de la cryptographie et comment les utiliser correctement.

Des antiques messages secrets décodés par les espions à la cryptographie moderne, vous explorez les fondements de la sécurité des données.

Ce cours s'adresse aux :

Débutants en cybersécurité
Tous ceux qui sont intéressés par la cryptographie
Tous les curieux qui veulent découvrir comment les données numériques sont sécurisées

Détails du cours sur le site :
<https://semafor-conseil.swiss/en/bt216-cryptography/>

Développez vos connaissances en cybersécurité

foundations



Fondamentaux de la cybersécurité

Linux Introduction

Online Courses

- 24 hours
- 3 days
- 90% hands-on
- 3 case studies
- 8 labs

THINKCYBER semafor-conseil.swiss

Le cours Introduction à Linux couvre les fondements du système Linux. Ce cours est conçu pour les débutants. Les participants sont entraînés à l'utilisation de Linux et des bases de l'automatisation des scripts.

Il est inutile de supprimer votre système Windows et toutes vos applications habituelles pour utiliser Linux sur votre ordinateur. Nous vous apprendrons à installer Linux en sous-système de Windows.

Ce cours s'adresse à :

- Toute personne à l'aise avec l'informatique qui souhaite connaître le système Linux
- Ceux qui veulent débiter une carrière orientée vers la cybersécurité
- Tout chef de projet ou responsable impliqué dans la sécurité informatique

Détails du cours sur le site :
<https://semafor-conseil.swiss/en/ns103-linux-introduction/>

Perfectionnez vos connaissances

Introduction à Python

Cours en ligne

- 24 heures
- 3 jours
- 90% pratique
- 3 études de cas
- 8 labos

THINKCYBER semafor-conseil.swiss

Toute personne qui souhaite débiter dans la cybersécurité et créer les outils nécessaires doit apprendre à programmer. Python est le langage facile utilisé pour beaucoup d'outils dans différents domaines, dont la sécurité informatique.

Le cours Introduction à Python fournira aux participants une première pierre dans la compréhension de la logique de programmation en Python et un niveau de base de programmation permettant de facilement progresser.

Ce cours s'adresse à :

- Personne à l'aise avec l'informatique qui souhaite apprendre les fondamentaux de Python, le langage le plus utilisé dans la cybersécurité
- Développeur de logiciel, d'Apps et d'application web

Détails du cours sur le site :
<https://semafor-conseil.swiss/en/ns105-python-intro/>

Développez vos connaissances en cybersécurité

Perfectionnez vos connaissances

network security

Sécurité Réseau

Sécurité Réseau englobe un grand nombre de technologies, appareils, et processus. Après ces cours, vous serez en mesure de détecter les vulnérabilités d'un réseau grâce à des techniques et outils d'exploration et d'analyse. Vous comprendrez les différents types de pare-feu et maîtriserez le matériel des serveurs sous Windows et Linux.



FORMATION CYBERSÉCURITÉ

Sécurité Réseau

Cours en line

40 heures	5 jours	92% pratique	5 études de cas	13 labos
-----------	---------	--------------	-----------------	----------

THINKCYBER

semafor-conseil.swiss

Sécurité Réseau vise de multiples technologies, appareils et processus. De nos jours, chaque organisation, entreprise industrielle et de service, peu importe sa taille, est responsable de la sécurité de ses réseaux nécessairement intégrés à Internet. Face aux cybermenaces toujours plus nombreuses, les responsables ont besoin de spécialistes bien formés.

Ce cours permet de comprendre et d'identifier les vulnérabilités des réseaux et d'apprendre, avec les mêmes techniques utilisées par les hackers, à sécuriser toutes les machines de réseaux, les pare-feu, les serveurs Linux ou Windows et les ordinateurs.

Ce cours s'adresse à :

- Informaticien avec compétence réseau qui débute ou évolue vers la cybersécurité
- Gestionnaire de réseaux
- Développeur

Détails du cours sur le site :
<https://semafor-conseil.swiss/en/bt208-network-security/>

FORMATION CYBERSÉCURITÉ

Tests d'intrusion PenTest

Cours en line

40 heures	5 jours	90% pratique	5 études de cas	10 labos
-----------	---------	--------------	-----------------	----------

THINKCYBER

semafor-conseil.swiss

Les tests d'intrusion, c'est simple ! Un ensemble d'outils de détection et d'analyse pris en main avec bon sens. Le cours Tests d'intrusion enseigne à trouver les failles et prendre les mesures appropriées pour protéger les données tout en maintenant l'activité.

Ce cours entraîne le participant à la maîtrise des tests d'intrusion dans des situations réelles sur un simulateur virtuel sécurisé.

Ce cours s'adresse à :

- Tout spécialiste ayant des connaissances en réseau
- Administrateur de réseau
- Testeur de sécurité
- Hacker éthique

Détails du cours sur le site :
<https://semafor-conseil.swiss/en/bt212-penetration-testing/>

Développez vos connaissances en cybersécurité

Perfectionnez vos connaissances



Renseignement en sources ouvertes (OSINT)

Le Renseignement Sources Ouvertes (Open Source INTelligence) couvre les techniques et processus utilisés pour récupérer les informations ciblées accessibles librement en ligne parmi le large spectre des données publiées.

FORMATION CYBERSÉCURITÉ
Renseignement sources ouvertes
OSINT

Cours en line
CYBERIUM ARENA SIMULATOR

40 heures	5 jours	88% pratique	5 études de cas	8 labos
-----------	---------	--------------	-----------------	---------

THINKCYBER
semafor-conseil.swiss

Le Renseignement Sources Ouvertes (OSINT) couvre les techniques et méthodes de collecte ciblée d'information dans l'immensité des données, à partir de sources ouvertes, accessibles au public.

Le cours OSINT (Renseignement Sources Ouvertes) apprend aux participants à collecter et analyser les informations en utilisant toutes les sources publiques accessibles. Les participants seront amenés à collecter des informations sur le Darknet, les réseaux sociaux et d'autres sources.

Ce cours s'adresse à :

- Officier du renseignement
- Officier de police
- Enquêteur public et privé
- Enquêteur en criminalistique
- Journaliste/reporter en investigation

Détails du cours sur le site :
<https://semafor-conseil.swiss/en/bt214-osint/>

FORMATION CYBERSÉCURITÉ
Renseignement Sources Ouvertes
Automatisation OSINT

Cours en line
CYBERIUM ARENA SIMULATOR

40 heures	5 jours	88% pratique	5 études de cas	8 labos
-----------	---------	--------------	-----------------	---------

THINKCYBER
semafor-conseil.swiss

Le cours d'automatisation de l'OSINT (Renseignement Open Source) couvre les techniques et méthodes afin de collecter des informations ciblées dans l'immensité des données en sources ouvertes en utilisant des outils d'automatisation afin de maximiser les résultats.

Le cours OSINT Automatisation enseigne aux participants comment collecter et analyser les informations en utilisant différents outils et créer des automatisations. Les participants seront confrontés à la collecte d'information sur le Darkweb, les réseaux sociaux et d'autres sources.

Ce cours s'adresse à :

- Analyste en renseignement
- Praticien judiciaire
- Officier du renseignement
- Enquêteur privé et public
- Enquêteur en criminalistique

Détails du cours sur le site :
<https://semafor-conseil.swiss/en/bt221-osint-automation/>

Développez vos connaissances en cybersécurité



Gestion des menaces

Au centre de la mise en place de la cybersécurité, il y a la structure SOC (Centre des Opérations de la Sécurité) qui permet à l'organisation de faire face aux cybermenaces en fournissant les moyens efficaces de réduire les risques et perfectionner l'ensemble des processus et services.



FORMATION CYBERSÉCURITÉ

Sémafor CONSEIL

Analyse SOC

Cours en line

40 heures

5 jours

90% pratique

5 études de cas

11 labos

CYBERIUM ARENA SIMULATOR

THINKCYBER

semafor-conseil.swiss

De nos jours, un Centre des Opérations de Sécurité (SOC) devrait avoir tout ce qui est nécessaire afin de monter une défense efficace dans un service IT. Le SOC inclut une large gamme d'outils de détection et prévention sophistiqués, de reporting et de renseignement ainsi qu'une équipe de professionnels IT compétents.

Le cours Analyse SOC est conçu pour les services des opérations afin de mettre en œuvre une solution SOC. Le cours permet l'acquisition des compétences et méthodes nécessaires pour son implémentation. Le cours forme le participant à tous les aspects d'une équipe SOC performante.

Ce cours s'adresse à :

- Informaticien avec compétence réseau qui débute ou évolue vers la cybersécurité
- Personne impliquée dans la politique interne de sécurité de l'information

Détails du cours sur le site :
<https://semafor-conseil.swiss/en/bt222-soc-analyst/>

Perfectionnez vos connaissances

FORMATION CYBERSÉCURITÉ

Sémafor CONSEIL

Traque aux menaces

Cours en line

40 heures

5 jours

90% pratique

5 études de cas

11 labos

CYBERIUM ARENA SIMULATOR

THINKCYBER

semafor-conseil.swiss

Dans le monde de la cybersécurité d'aujourd'hui, il est possible de se prévenir de toutes les attaques. La traque aux cybermenaces est une technique pro-active de recherche d'attaque et de collecte des preuves laissées par les hackers lors d'attaques utilisant des malwares ou accédant à des données confidentielles.

Le processus est important et basé sur l'idée que l'attaque a déjà eu lieu, donc le hacker s'est déjà infiltré. Il s'agit de tester tout ce qui est possible afin de détecter l'intrusion au plus tôt et de contrer les effets de l'intrusion.

Ce cours s'adresse à :

- Analyste SOC
- Administrateur réseau
- Testeur de sécurité
- Consultant en cybersécurité
- Hacker éthique

Détails du cours sur le site :
<https://semafor-conseil.swiss/en/bt223-threat-hunting/>

Développez vos connaissances en cybersécurité

WebApp security

Sécurité des Applications Web

La sécurité appliquée au Web est spécifique aux sites Internet et applications Web (WebApps). A un niveau supérieur, la sécurité des WebApps englobe les principes de la cybersécurité appliquée aux sites Internet : e-commerce, banque en ligne et tout service interactif.



FORMATION CYBERSÉCURITÉ

Sémafor CONSEIL

Sécurité des WebApp

Cours en line

40 heures

5 jours

85% pratique

5 études de cas

8 labos

THINKCYBER

semafor-conseil.swiss

Le cours Sécurité des Applications Web entraîne les participants à comprendre les langages dédiés au Web et leurs applications. Les participants apprennent, via un processus éprouvé, l'identification des failles courantes.

L'objectif principal de ce cours est de permettre aux professionnels du Web et de la sécurité de mesurer les risques des applications Web et d'apprendre comment mettre en place une évaluation des risques et une sécurité adaptée.

Ce cours s'adresse à :

- Webmaster / Créateur de site Web
- Concepteur d'application et/ou de service Web
- Développeur PHP
- Développeur Intranet/Internet
- Professionnel de la cybersécurité

Détails du cours sur le site :

<https://semafor-conseil.swiss/en/rt422-web-application-security-intermediate/>

Perfectionnez vos connaissances

FORMATION CYBERSÉCURITÉ

Sémafor CONSEIL

Piratage des WebApp

Cours en line

40 heures

5 jours

85% pratique

5 études de cas

8 labos

THINKCYBER

semafor-conseil.swiss

Ce cours permet tout d'abord de comprendre la conception des applications et sites Web, le HTTP, le JavaScript, les comportements des navigateurs et d'autres technologies afin de construire la sécurité par défaut (security by design).

Les participants acquièrent ensuite des compétences en procédures de tests d'intrusion afin de détecter des vulnérabilités dans les applications et sites Web en combinant manipulations manuelles et automatisées.

Ce cours s'adresse à :

- Développeur Internet/intranet pour la sécurisation des données
- Testeur d'intrusion
- Consultant en cybersécurité
- Architecte cybersécurité
- Hacker éthique

Détails du cours sur le site :

<https://semafor-conseil.swiss/en/rt423-webapp-security-advanced/>

PROGRAMME



FORMATIONS

Notre offre de cours orientés vers les praticiens couvre tous les domaines clés de la cybersécurité : la **sécurité des réseaux**, la sécurité des **applications Web**, la **gestion des menaces**, et **OSINT** (INTelligence Open Source, Renseignement Sources Ouvertes), aussi bien que la série de cours sur les **fondamentaux** comme l'introduction cybersécurité, cryptographie, l'ingénierie des systèmes Linux et aussi une introduction à Python.

Sémafor Conseil a un catalogue de formations beaucoup plus étendu avec 30 cours qui couvrent des sujets bien au-delà des thèmes ci-dessus, avec la **criminalistique** (forensique), le **développement d'exploits**, et aussi la sécurité des **systèmes de contrôle industriels** (ICS, SCADA).



Guillaume Ibsaïenne

Learning &
Development Manager

+41 79 548 67 85

guillaume.ibsaïenne@
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