

# 2026

# CATALOGUE DE FORMATION



## Programme 2026

Dispensé par

**Asboth  
Laurent**

**Dicko  
Sabane**

**Scalabre  
Olivier**

# Table des matières

→	<b>01-02</b>	Introduction et modalités
→	<b>03</b>	VIG-CYBER001 : La sécurité du système d'information
→	<b>04</b>	VIG-CYBER002 - Panorama des menaces et attaques
→	<b>05</b>	VIG-CYBER003 - Les 10 règles d'hygiène
→	<b>06</b>	VIG-CYBER004 - Les 42 règles de l'ANSSI
→	<b>07</b>	VIG-CYBER005 - Les 10 Quick-Wins pour RSSI
→	<b>08</b>	VIG-CYBER006 - Comprendre internet
→	<b>09</b>	VIG-CYBER007 - Authentification et chiffrement
→	<b>10</b>	VIG-CYBER008 - Sécurité du poste de travail et nomadisme
→	<b>11</b>	VIG-CYBER009 - Gestion de la cybersécurité au sein d'une organisation
→	<b>12</b>	VIG-CYBER010 - RGPD

# Introduction et modalités



## La Cybersécurité une priorité en 2026

### Sensibilisez vos équipes

Véritable problème de société, la cybercriminalité est en pleine expansion et concerne tout le monde (tous types de systèmes, organisations, petites et grandes entreprises).

Que ce soit pour la protection de vos informations clients ou financières, la sécurité de vos opérations, la garantie de la propriété intellectuelle, ou la sécurité de toutes autres données sensibles, votre système doit être protégé. La sécurité de ces informations est fondamentale

**En mai 2018, les entreprises deviennent pénalement responsables.**

Suite aux nouveaux textes législatifs européens RGPD, les entreprises n'ayant pas sécurisé leur infrastructure informatique s'exposent à des sanctions pouvant aller jusqu'à 4% de leur chiffre d'affaires.

**58 K€**

Le coût médian d'une cyberattaque en France (Astères 2023)



**27 %**

On recense une perte moyenne de 27 % des chiffres d'affaires dans les PME suite à une cyberattaque. (CESIN 2022)



**60 %**

60 % des PME victimes de cyberattaques ne parviennent pas à remonter la pente et font faillite dans les 18 mois après l'attaque (CESIN 2022)



**95 %**

Dans 95 % des cyberattaques, la faille vient d'une erreur humaine. L'humain reste au coeur de tout. (Etude IBM)



## Modalités pédagogiques et logistiques

Formation réalisée dans nos locaux : nous disposons d'une salle équipée permettant l'accueil de 10 stagiaires en présentiel.

Formation dans les locaux de votre entreprise : Notre formateur s'adaptera aux systèmes informatiques et au matériel existant pour la formation. L'entreprise cliente garantit que le matériel est conforme en matière de sécurité. Elle se porte responsable d'établir, de diffuser et de porter à la connaissance des stagiaires, les instructions et consignes de sécurité incendie.

Formation à distance : En cas de besoin les formations peuvent également être proposées en visio-conférence.

Les repas des stagiaires ne sont pas compris dans le forfait formation.



## Organisme de formation

Vigilens est en cours de certification Qualiopi.

→ Lieu	Dans notre salle de formation - sur site client - en visio
→ Logistique	Supports distribués à tous les participants à l'issue de la formation
→ Validation	Fiche d'émargement, attestation de fin de stage
→ Moyens	Les stagiaires utilisent leur environnement de travail (PC, logiciels, etc.) Le formateur utilise le système de projection du client
→ Date	A définir

# VIG-CYBER001 : La sécurité du système d'information

## Public

Tout public

## Durée

3h à 3h30 selon le niveau du public et le temps d'échange

## Prérequis

Pas de prérequis

## Objectifs

Améliorer ses connaissances sur le système d'information en prenant conscience des risques qui le menacent.

## Sommaire de la formation

### 1°/ Notions et évolution de la sécurité du système d'information

L'objectif de ce chapitre est de montrer comment le système d'information a évolué avec désormais plus de 30 ans d'internet et l'utilisation massive des objets connectés. La sécurité du système d'information est devenu un enjeu.

### 2°/ Les parties prenantes

Quels sont les acteurs de la cybersécurité ? Les pirates (Black hats / White hats, les hacktivistes, et les autres)... Les acteurs de la protection cyber, nationaux, locaux, interne à l'entreprise...

### 3°/ Focus sur les données

Les données : la source de tous nos maux ! Quels types de données, quelle valeur pour vos données, quels risques..

### 4°/ Conclusion

Questions / réponses sur la formation

# VIG-CYBER002 - Panorama des menaces et attaques

## Public

Tout public

## Durée

2h30 à 3h selon le niveau du public et le temps d'échange

## Prérequis

Pas de prérequis

## Objectifs

Acquérir une vision claire des principales menaces numériques qui pèsent sur les entreprises, en particulier les TPE/PME. Elle donne les clés pour identifier les vecteurs d'attaque, comprendre leur fonctionnement et adopter les bons réflexes pour s'en prémunir.

## Sommaire de la formation

### 1°/ Les notions

Dans ce chapitre sont abordées les différentes terminologies autour de la menace informatique. Qu'est ce qu'une vulnérabilité, qu'est ce qu'une menace, quel est le panorama des attaques en France avec quelques chiffres.

### 2°/ Panorama des attaques

Dans ce chapitre nous étudierons les 11 types d'attaques les plus fréquents. La violation de mot de passe, les virus, les vers, les trojans, le phishing, l'ingénierie sociale etc... afin d'en expliquer les rouages, pour permettre de mieux s'en prémunir. Nous verrons également les évolutions et quelques chiffres sur ces attaques.

### 3°/ Autres types de menaces

En complément des attaques les plus communes nous verrons ici, d'autres types d'attaques également utilisé par les pirates : Les injections SQL, l'usurpation d'identité, la cyberfraude, la cybercontrefaçon, le cyberharcèlement, le darkweb, etc..

### 4°/ Conclusion

Questions / réponses sur la formation

# VIG-CYBER003 - Les 10 règles d'hygiène

## Public

Tout public

## Durée

2h30 à 3h selon le niveau du public et le temps d'échange

## Prérequis

Pas de prérequis

## Objectifs

Connaitre les 10 règles indispensables pour se prémunir simplement mais efficacement des attaques cyber. Aussi bien à titre professionnel que personnel.

## Sommaire de la formation

### 1°/ Passage en revue des 10 règles d'hygiène

- Les mots de passe
- Les sauvegardes
- Les mises à jour
- L'antivirus
- Les téléchargements
- La messagerie
- Les achats en ligne
- Les réseaux sociaux
- Le Pro / Perso
- Le Wifi

### 2°/ Bonus

Les bons réflexes à adopter en cas de suspicion d'attaque.

### 3°/ Conclusion

Questions / réponses sur la formation

# VIG-CYBER004 - Les 42 règles de l'ANSSI

## Public

Responsable informatique

## Durée

3h à 3h30 selon le niveau du public et le temps d'échange

## Prérequis

Pas de prérequis

## Objectifs

Améliorer la sécurité de son SI par la mise en place des règles préconisées par l'ANSSI.

## Sommaire de la formation

### 1°/ Passage en revue des 42 règles de l'ANSSI

Pour chacune des 42 règles de l'ANSSI il sera présenté la problématique du sujet et les solutions concrètes à apporter.

### 2°/ Conclusion

Questions / réponses sur la formation

# VIG-CYBER005 - Les 10 Quick-Wins pour RSSI

## Public

RSSI, responsables IT, référents sécurité, DSI de TPE/PME

## Durée

2h30 à 3h selon le niveau du public et le temps d'échange

## Prérequis

Connaissances de base en sécurité des systèmes d'information.

## Objectifs

Identifier les actions rapides, concrètes et à fort impact à mettre en place dans votre organisation pour réduire significativement les risques opérationnels.

## Sommaire de la formation

### 1°/ Passage en revue des 10 quick-wins

Pour chacun des 10 quick-win seront présentés les recommandations, le risque et les points d'attention, ceci afin de permettre une mise en œuvre concrète.

### 2°/ Conclusion

Questions / réponses sur la formation

# VIG-CYBER006 - Comprendre internet

## Public

Tous les collaborateurs utilisant un ordinateur et Internet dans le cadre de leur activité professionnelle (aucune compétence technique requise).

## Durée

2h30 à 3h selon le niveau du public et le temps d'échange

## Prérequis

Savoir utiliser un navigateur web, une messagerie et les outils de base bureautiques.

## Objectifs

Familiariser les utilisateurs avec le fonctionnement d'Internet et les bonnes pratiques de sécurité liées à ses principaux usages. Comprendre les risques associés à la navigation, à l'usage des mails, des réseaux sociaux et des messageries.

## Sommaire de la formation

### 1°/ Présentation d'Internet

Définition, fonctionnement (client-serveur, adresse IP, protocoles)  
Différences entre Internet, Web, Intranet, Extranet

Usages d'Internet dans la vie personnelle et professionnelle

### 2°/ Le surf et ses dangers

Tracking, cookies, publicité ciblée  
Fichiers suspects, extensions à risque..  
Rançongiciels : fonctionnement et bonnes pratiques de prévention  
Où et comment télécharger en toute sécurité

### 3°/ La navigation web

Fonctionnement des navigateurs et moteurs de recherche  
Navigation privée, historique, mots de passe enregistrés  
Typosquatting et faux sites web : comment les repérer.

### 4°/ La messagerie électronique

Différences entre spam, malware, phishing  
Reconnaître un message frauduleux  
Bonnes pratiques pro/webmail  
Gestion des pièces jointes, liens et mots de passe

### 5°/ La messagerie instantanée

Outils de chat d'entreprise et apps mobiles  
Risques : usurpation, virus via MMS, liens piégés

Paramétrage de la confidentialité

Bonnes pratiques sur mobile et ordinateur

### 6°/ Les réseaux sociaux

Ingénierie sociale : exploitation de vos publications  
Atteinte à l'e-réputation, fausses informations, piratage de compte  
Paramétrage de la confidentialité et contrôle des partages, comportements à adopter pour un usage professionnel sécurisé

# VIG-CYBER007 - Authentification et chiffrement

## Public

Tous les collaborateurs utilisant un ordinateur et Internet dans le cadre de leur activité professionnelle (aucune compétence technique requise).

## Durée

3h à 3h 30 selon le niveau du public et le temps d'échange

## Prérequis

Savoir utiliser un navigateur web, une messagerie et les outils de base bureautiques.

Aucun prérequis technique nécessaire.

## Objectifs

Comprendre les mécanismes d'authentification (mots de passe, MFA, etc.) et leurs vulnérabilités. Elle aborde également les fondamentaux de la cryptographie pour mieux protéger les données échangées dans l'environnement professionnel.

## Sommaire de la formation

### 1°/ Le principe de l'authentification

Définition : identification vs authentification  
Les différents facteurs d'authentification (connaissance, possession, biométrie)  
Authentification simple, forte (2FA/MFA) et sans mot de passe (FIDO)  
Risques d'une compromission : impacts personnels et professionnels.

### 2°/ Les attaques d'authentification

Attaques directes : force brute, permutation, dictionnaire  
Attaques de proximité : keyloggers, observation malveillante, usurpation  
Ingénierie sociale, réutilisation de mots de passe, phishing, etc..  
Que faire en cas d'attaque ou de suspicion

### 3°/ Sécuriser et gérer ses mots de passe

Définir un mot de passe fort et mémorisable  
Séparer les usages pro/perso.  
Gestionnaires de mots de passe.  
Notions de SSO, IAM, IDaaS : centralisation et limites

### 4°/ Notions de cryptographie

Cryptographie : objectifs (confidentialité, intégrité, authenticité, non-répudiation)  
Chiffrement symétrique et asymétrique  
Signature numérique et certificats électroniques (AC/IGC)  
Mécanismes de sécurisation des échanges

### 5°/ Conclusion

Synthèse sur l'importance croissante de l'authentification forte et du chiffrement  
Intégration des bonnes pratiques dans le quotidien professionnel

# VIG-CYBER008 - Sécurité du poste de travail et nomadisme

## Public

Tout collaborateur utilisant un ordinateur, un smartphone ou une connexion internet dans le cadre de son activité.

## Durée

3h à 3h30 selon le niveau du public et le temps d'échange

## Prérequis

Savoir utiliser un navigateur web, une messagerie et les outils de base bureautiques.

Aucun prérequis technique nécessaire.

## Objectifs

Comprendre les principaux risques liés à l'usage quotidien de leur poste de travail ainsi que les bonnes pratiques à adopter dans un contexte de mobilité (télétravail, déplacements, usage personnel / professionnel).

## Sommaire de la formation

### 1°/ Les mises à jour

Pourquoi les mises à jour sont critiques ?  
MAJ du système, des applications et vigilance sur les fausses MAJ  
Gestion du cycle de vie des équipements  
Bonnes pratiques lors de l'installation de nouvelles applications.

### 2°/ Configurations de base

Paramétrage à l'achat ou à l'initialisation d'un appareil  
Déverrouillage, mots de passe, biométrie  
Logiciels de sécurité (antivirus, pare-feu), configuration pour mobiles.

### 3°/ Configurations complémentaires

Comptes utilisateurs (admin, utilisateur, invité)  
Politique de sauvegarde.  
Sécurisation des connexions : Wi-Fi public/domicile, VPN, protocoles

### 4°/ Les périphériques amovibles

Risques liés aux clés USB, disques durs externes et autres supports  
Séparer usages perso/pro.  
Suppression sécurisée, formatage, destruction

### 5°/ Nomadisme & BYOD

Risques du nomadisme : vol, perte, rebond, confidentialité  
Bonnes pratiques : VPN, antivirus mobile, mots de passe distincts  
Risques spécifiques des smartphones et tablettes

### 6°/ Conclusion & rappel des bonnes pratiques

# VIG-CYBER009 - Gestion de la cybersécurité au sein d'une organisation

## Public

Responsables informatique, DSI, RSSI, chefs de projet, responsables qualité, dirigeants de TPE-PME.

## Durée

3h à 3h30 selon le niveau du public et le temps d'échange

## Prérequis

Connaissance générale des systèmes d'information et de leur fonctionnement.

## Objectifs

Comprendre comment intégrer la cybersécurité dans la gouvernance globale d'une entreprise, à travers les normes, les responsabilités et les processus adaptés.

## Sommaire de la formation

### 1°/ Intégrer la sécurité au sein d'une organisation

Panorama des normes ISO 2700x  
Système de management de la sécurité de l'information (SMSI)  
Gestion des risques et classification des informations  
Politique de sécurité.  
Rôle du RSSI et importance de la gouvernance

### 2°/ Intégrer la sécurité dans les projets

Intégration de la sécurité tout au long du cycle de vie d'un projet  
Analyse de risques (EBIOS, MEHARI, OCTAVE)  
Plan d'action SSI basé sur la défense en profondeur  
Prise en compte du SI, des contraintes légales et opérationnelles

### 3°/ Difficultés liées à la prise en compte de la sécurité

Manque de culture sécurité dans la direction  
Arbitrage difficile entre confort d'usage et exigences sécuritaires  
Shadow IT, Cloud, SaaS et évolution des technologies  
Problèmes de périmètre et frontières floues entre sphères privée et pro  
Rôle central de l'humain dans la sécurité

### 4°/ Métiers liés à la cybersécurité

Cartographie des fonctions clés : RSSI, auditeurs, analystes, architectes  
Profils types et parcours : reconversions, certifications, formations

### 5°/ Conclusion & rappel des bonnes pratiques

# VIG-CYBER010 - RGPD

## Public

Tout collaborateur d'entreprise, notamment RH, marketing, commercial, informatique, direction

## Durée

2h à 2h30 selon le niveau du public et le temps d'échange

## Prérequis

Aucun prérequis technique.

## Objectifs

Comprendre le cadre réglementaire du RGPD et ses implications.  
Identifier les données personnelles et les obligations de traitement associées.  
Appliquer les bonnes pratiques pour se conformer à la réglementation.

## Sommaire de la formation

### 1°/ Une réglementation à large portée

Origines, portée européenne et mondiale du RGPD

Définition des données personnelles (simples et sensibles)

Les responsabilités des entreprises et des sous-traitants

Sanctions encourues (administratives, pénales, réputationnelles)

### 2°/ Le traitement des données

Principes fondamentaux : les conditions de licéité

Le droit des personnes : accès, rectification, effacement, portabilité, etc..

Gestion du consentement et cas de traitement sans consentement

Exemples d'exercice de ces droits (Google, Apple, Facebook, etc.)

### 3°/ La mise en conformité

Démarche de mise en conformité : les obligations en pratique (registre, cartographie, analyse d'impact, etc.)

Rôles du DPO / responsable RGPD interne

Sécurisation des données et politique documentaire

Plan d'action en cas de fuite de données

### Check list RGPD

# Nous contacter

Téléphone

**+33 (0)6 76 28 11 60**



Email

**team-cyber@vigilens.fr**



Site web

**<https://cyberveillance.vigilens.fr>**



Adresse

**9 Avenue des Saules - 69600 OULLINS**

