Formez-vous à la cybersécurité avec ENI Service

À l'ère numérique, la cybersécurité est devenue bien plus qu'une nécessité ; c'est un impératif. Les enjeux sont colossaux : la protection des données sensibles, la préservation de la réputation de l'entreprise, et la confiance des clients sont en jeu. Dans un monde interconnecté, où les menaces évoluent constamment, notre engagement envers la cybersécurité est notre priorité.

Découvrez comment ENI Service peut vous aider à naviguer dans cette ère de défis, à vous former et à défendre votre entreprise contre les cybermenaces.

NOS PARCOURS **DE FORMATION**

Nos conseillers formation vous accompagnent dans l'élaboration d'un parcours personnalisé. Choisissez entre nos **offres clé en main**, tirées de notre catalogue de formations en cybersécurité, ou un **cursus sur mesure**, totalement adapté à vos besoins spécifiques (enjeux, moyens, profils des apprenants, etc.).

Découvrez un exemple de parcours personnalisé clé en main au dos de cette page.

NOS FORMATIONS **EN CYBERSÉCURITÉ**

Notre catalogue comprend une vaste diversité de formations dans le secteur de la sécurité informatique, dispensées par des formateurs experts dans leur domaine en présentiel ou à distance.

Cours officiels Microsoft Sécurité, ISO 27001 / 27005, EBIOS, F5, pfSense, SonicWALL et Stormshield ; formations spécifiques pour tous les besoins et profils, utilisateurs comme techniques. De la sensibilisation à la cybersécurité à l'administration de réseaux sécurisés en passant par l'investigation numérique, la conduite d'audit, la sécurisation de sites Web, le Ethical Hacking ou le déploiement d'un Firewall et d'un VPN…

Parcourez notre catalogue !

SÉCURITÉ DES RÉSEAUX ET DES SYSTÈMES D'INFORMATION

FOCUS **SUR LA DIRECTIVE NIS2**

Ambitieuse et visionnaire, la directive NIS2 a pour objectif d'établir un niveau de maturité cybernétique uniforme dans toute l'Union Européenne, en renforçant la cybersécurité des tissus économiques et administratifs des pays membres.

Plus de 10 000 entités réparties sur 18 secteurs d'activité seront concernées !

Pour vous permettre d'appréhender tous les enjeux liés à cette directive, formez-vous en présentiel ou à distance avec la formation
NIS2 – Fondamentaux et Implémentation (2 jours)

Exemple de parcours de formation en **cybersécurité**

Dans cet exemple, notre client a opté pour un parcours de formation clé en main pour former des spécialistes de la cybersécurité.

En parallèle de son expertise en développement informatique, le spécialiste maîtrise les différents systèmes d'exploitation (Windows, Linux) et le fonctionnement d'un réseau.

Le parcours de formation ci-dessous permet donc d'acquérir les connaissances et compétences nécessaires pour analyser, diagnostiquer, prévenir et protéger les systèmes d'informations de l'entreprise. Il allie théorie, pour acquérir les connaissances de base, et pratique, par la réalisation d'exercices de mise en application permettant de consolider les connaissances.

PRÉREQUIS

Pour suivre ce parcours de formation, les apprenants devront avoir une forte capacitée d'adaptation, être autonomes et motivés pour intégrer un parcours riche avec un rythme soutenu, disposer de connaissances de base en systèmes et réseau et savoir lire et comprendre de l'anglais technique.

OBJECTIFS

Le parcours de formation a pour but de faire monter en savoir-faire sur la cybersécurité des informaticiens déjà expérimentés et ayant une compétence sur le domaine administration des systèmes et réseaux.

À l'issue de leur formation, les participants doivent être en mesure :

- De déployer sur leur établissement les dispositions techniques acquises pendant la formation pour atteindre un niveau d'exposition au risque cyber le plus limité possible.
- De réagir efficacement sur les composants du système en cas de cyber attaque pour en limiter autant que faire se peut les impacts.
- D'évaluer régulièrement le niveau de robustesse du SI aux agressions de tiers.
- D'accompagner les membres de la Direction du Système d'Information sur l'état de l'art en termes de cybersécurité pour la mise en œuvre et le maintien en condition opérationnelle des composants SI afin d'en assurer la robustesse et la fiabilité.
- D'assurer une veille technologique efficace pour appréhender les nouvelles approches en matière de cyber-malveillance et adapter les dispositions techniques pour s'en prémunir.

MODULES DU PARCOURS DE FORMATION

1) **Panorama de la cybersécurité – Menaces & Enjeux et Cyber Défense (2 jours)**
2) **Architecture Réseau (3 jours)**
3) **PKI : Mise en œuvre et utilisation d'une infrastructure à clé publique en environnement Windows (2 jours)**
4) **Sécurité informatique – Ethical Hacking – Apprendre l'attaque pour mieux se défendre (5 jours)**
5) **Investigation numérique – Réseau et Windows (5 jours)**
6) **Déploiement d'un réseau VPN (2 jours)**
7) **Continuité / Reprise d'activité / Sauvegarde & restauration (2 jours)**
8) **Déploiement d'un Firewall (2 jours)**
9) **EDR/MDR/XDR (3 jours)**
10) **SOC – Security Manager (5 jours)**
11) **Cybersécurité – Sondes IDS et Honeypots (2 jours)**
12) **Mise en œuvre d'un reverse proxy avec Apache (2 jours)**
13) **Microsoft Sécurité – Administrer les identités et les accès (4 jours)**