# Les fondamentaux avancés de la cybersécurité

**Préparez votre entreprise pour les enjeux de la cybersécurité et la Directive NIS 2**

**Plongez au cœur de la cybersécurité avec notre formation intensive de deux jours**, spécialement conçue pour transformer théorie et pratique en compétences concrètes. Embarquez pour un voyage à travers les aspects fondamentaux et les défis actuels de la sécurité informatique.

**2 journées de formation pour :**

• **Approfondir les concepts techniques et les stratégies de cybersécurité** pour sécuriser les environnements IT complexes.

• **découvrir les fondamentaux et les aspects avancés de la cybersécurité**, intégrant les dernières pratiques en gestion des risques, en sécurité réseau, et en conformité avec les réglementations comme le GDPR et le NIS2.

• **apprendre à identifier et contrer les menaces internes et externes**, tout en comprenant les méthodes de cryptographie et les contre-mesures adaptées.

• **développer une expertise concrète en sécurité informatique**, avec des outils et des techniques pour sécuriser des environnements complexes

**Maîtrisez les bases essentielles et les techniques avancées de la cybersécurité pour protéger votre organisation face aux menaces modernes.**

La sécurité fait partie intégrante de l'environnement de travail d'un administrateur de réseaux et de systèmes. Celle-ci doit être pensée et intégrée dans les premières phases de la conception des réseaux et des systèmes, et ce bien avant leurs mises en œuvre. Mais pour cela, il faut absolument **comprendre les concepts de base et avancés de la sécurité**, qu'ils concernent l'environnement des menaces qui nous entourent ou les approches risques censées en évaluer la pertinence des protections ou des contremesures. De plus, les environnements hétérogènes de type Hybrid-Cloud et les **règlementations du type GDPR/NIS 2** doivent être mis en perspective face aux défis de la cyber-sécurité.

**Cette première formation permettra d'avoir une bonne connaissance des éléments clé de la cybersécurité et à préparer votre entreprise ou organisation pour l'entrée en vigueur de la Directive NIS 2. Vous pourrez ensuite suivre des formations plus avancées telles que ISO 27001, NIS 2, etc.**

## OBJECTIFS DE LA FORMATION

**Les participants à notre programme de formation en cybersécurité** démontreront leur compréhension des principes de bases qui sous-tendent et définissent la cybersécurité, ainsi que des rôles essentiels des professionnels de la cybersécurité dans **la protection des données et de l'infrastructure de l'entreprise**.

- Comprendre ce que signifie les mots « IT Security » & « Cyber Security »
- Comprendre la méthodologie « risk approach » ainsi que les méthodes d'évaluation de celui-ci (autant quantitatives que qualitatives) (ex. octave, cobit, ISO2700x, ...)
- Comprendre les menaces qui nous environnent et les attaques que subissent de manière continue les réseaux, les systèmes et les environnements Cloud
- Comprendre et mettre en oeuvre une approche efficace et appropriée de sécurité dans un environnement IT complexe (CSP, Security Wheel, ...)

## CONTENU DE LA FORMATION

- Security Definition
- The three A's of Security (including Auditing)
- Assessing Security Risks
    - Risk Concept
    - Risk Formula
    - Risk Assessment
    - Risk Objective
    - Risk Matrix
    - Risk Metrics
    - Risks from a business perspective
    - The Gap Approach
    - Risk Illusion
    - Data Risk Analysis

    - Data Risks Applied
    - Data Risks Management
- Security Threats
    - Internal Threats
    - Social Engineering
    - Accidental Security Breach
    - Exogenous Threats
    - Physical Threats
    - Mobile Users Threats
    - Outside Attacks
    - Historical Facs
    - New Trends in Threats
- Security Policy
    - CSP
    - PDCA
    - NIST
    - NIS2
- General Attack Methods (including Web Sites)
    - Authentication
    - Compromised Trusted Systems
    - Default Configurations
    - Improper Input Validation
    - Applications & Services
    - Denial of Services (DoS)
    - Viruses, Worms, Trojans Horses, Backdoors…
    - Wireless Network Attack
    - Physical Access
    - OT (Operation Technology)
- Security Countermeasures (including traffic flows, filtering, firewalling, security architecture, OT, …)
- Introduction to Cryptology :
    - History
    - Cryptographic Algorithms
    - PKI
- Other General Security Aspects:
    - hardware Security
    - Infrastructure Security
    - Backups
    - Anti-Malware
    - Disaster Recovery Plan (DRP & BCP)
    - Security Procedures

## A QUI S'ADRESSE CETTE FORMATION ?

Cette formation s'adresse à toute personne désireuse appréhender de manière globale la problématique de la Cybersécurité **afin de renforcer la sécurité de son organisation**.

- Administrateur de système ou de réseaux responsable d'infrastructure
- Personnes en charge de la définition des stratégies de sécurité informatique
- IT Manager, Infrastructure Manager ou CIO - DPO en charge de la protection des données médicales ou à caractère personnel (GDPR)

## PRÉ-REQUIS

- Compréhension technique des environnements informatiques
- Les éléments suivants sont des atouts pour comprendre tous les aspects techniques qui seront abordés :
    - Expérience technique dans au moins un OS serveur et une plateforme réseau
    - Connaissances approfondies de la communication réseau

## SUPPORT DE COURS

La présentation de la formation sera distribuée à tous les participants de la formation en format papier et numérique.

Les participants recevront pendant la formation une série de lectures pouvant les aider à comprendre les concepts présentés lors de la formation. Nous partagerons également avec vous les guides et règlementations européennes les plus importants en format électronique.

**Si votre entreprise compte plusieurs employés nécessitant une formation en cybersécurité ou si vous souhaitez former le COMEX et/ou management**, nos solutions de formation à la demande, permettent de personnaliser les contenus pour répondre aux besoins et aux objectifs spécifiques de vos équipes. Nos formateurs sont des praticiens ayant une grande expérience dans leur domaine, apportant leur expertise éprouvée en cybersécurité.