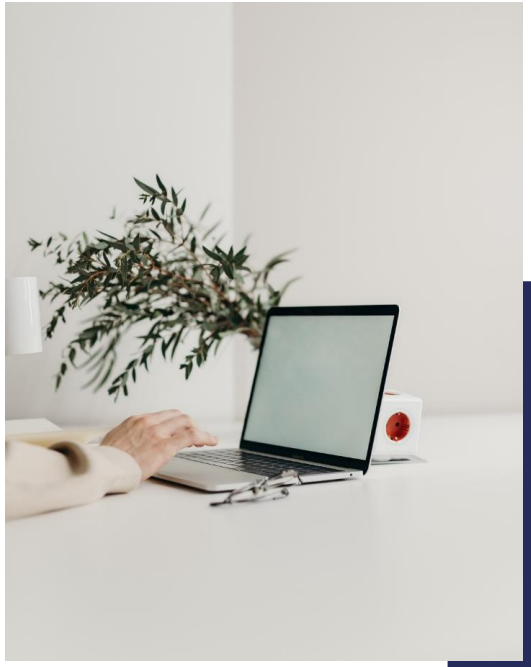
MOON TECH

CONSEIL ET SÉCURITÉ INFORMATIQUE

PROTÉGEONS ET SÉCURISONS VOS SYSTÈMES D'INFORMATION

Notre savoir-faire



MOONTECH
est spécialisée dans le conseil et la sécurité informatique, intervenant auprès des ETI et des PME de tous secteurs ainsi que des fonds d'investissement.

Nos experts vous accompagnent dans la **protection de vos données** et la **sécurisation de votre système d'information**, en vous proposant une **offre complète de prestations** afin d'aborder globalement la **sécurité de votre entreprise** :

- Evaluation de votre exposition aux risques Cyber et estimation de leur impact financier sur votre entreprise
- Campagnes de phishing
- Sensibilisation et formation des équipes
- Examen des vulnérabilités
- Tests d'intrusion physiques
- Social engineering (tentatives de prise en main à distance)
- Examen de conformité au RGPD
- Détermination de différents scénarii d'attaques possibles

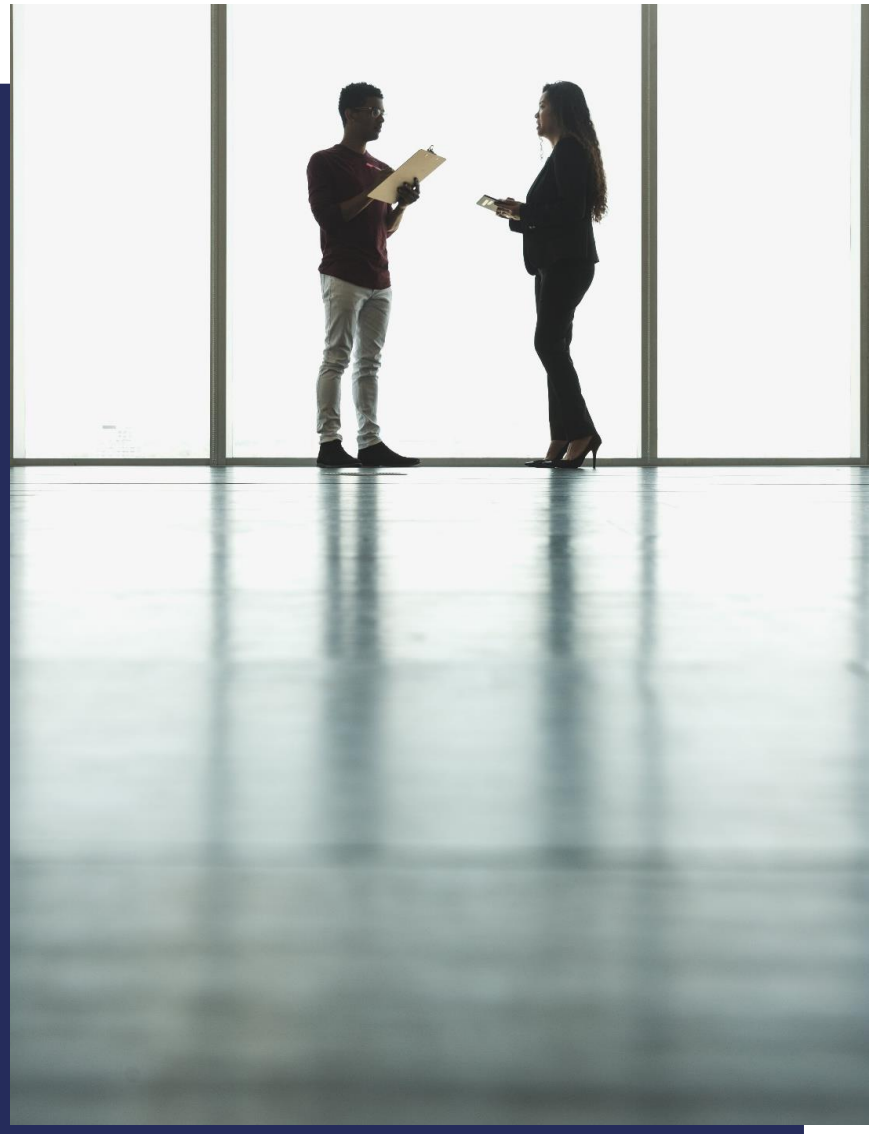
MOONTECH

Notre engagement à vos côtés

Nous garantissons des **prestations sur-mesure**, **adaptées à vos besoins** et à votre organisation, en toute **objectivité** et **indépendance vis-à-vis des éditeurs de solutions**.

Chaque mission est accompagnée de **recommandations détaillées** avec des éléments concrets pour améliorer la sécurité de votre entreprise et de votre système d'information.

Notre équipe partage son expertise en proposant des **formations adaptées aux besoins spécifiques de votre société** et de ses membres (dirigeants, équipe informatique, salariés), pour en sensibiliser tous les acteurs, leur apprendre à détecter et déjouer les attaques, en renforçant leurs connaissances en la matière et leur niveau de vigilance.



MOON TECH

Nos atouts : les 5 E

L'**expertise** et le savoir-faire de notre équipe

L'**exigence** dans la qualité de la réalisation de nos missions

L'**expérience** sur des missions auprès de tous types et de toutes tailles de structures

L'**échange**, pour évaluer les risques, exposer nos préconisations et sensibiliser les salariés

L'**écoute** des besoins de nos clients, afin de proposer une mission sur-mesure

Evaluation de l'exposition aux risques Cyber

Notre mission d'évaluation de l'exposition aux risques Cyber de votre entreprise a été conçue pour vous apporter des réponses concrètes aux potentielles failles de votre système d'information, renforcer votre sécurité et réduire vos risques de cyberattaques.

Notre mission se décompose ainsi :

1. **Entretien** avec la direction et votre DSI (le cas échéant)
2. **Compréhension de l'environnement** de vos systèmes d'information
3. **Evaluation de l'exposition** de l'entreprise face aux **risques Cyber** sur les points de sécurité jugés comme sensibles
4. Analyse de la **sensibilisation** et de la **formation** de votre personnel, ainsi que du **niveau de maturité numérique**
5. Vérification de la bonne **sécurisation des données** de votre structure : analyse documentaire complétée par des entretiens
6. **Elaboration de scénarii possibles d'attaques**, et **mesure de votre maturité** pour répondre à ces menaces
7. **Chiffrage du coût d'une éventuelle cyberattaque**

A l'issue de la mission, nos experts vous transmettent un **rapport complet et détaillé avec une évaluation des risques Cyber par process / item,** accompagné de **recommandations afin de renforcer la sécurité** de votre système d'information.
Nos rapports concluent sur un niveau de risque : **Faible, Modéré, Elevé** ou **Critique**.

MOON TECH

Détail de nos missions d'évaluation

MISSIONS D'EVALUATION	FLASH	STANDARD	PREMIUM
Evaluation de l'exposition aux risques Cyber (Niveau 1) – En distanciel – 1 semaine ○ Rapport détaillé avec analyse des items suivants : Sécurité Physique ; Sécurité Logique ; Gestion du changement ; Exploitation ; Sauvegardes ; Secours IT ○ Listing des items traités avec des constats (risque – maturité) et des recommandations (recommandations – effort) ○ Rédaction d'une feuille de route (plan de remédiation) pour faciliter la prise de décision de la direction ○ Restitution du rapport auprès de la direction	✓	✓	✓
Evaluation de l'exposition aux risques Cyber (Niveau 2) – Sur place – 3 semaines à 1 mois ○ Offre d'évaluation de l'exposition aux risques Cyber (Niveau 1) ○ Rapport détaillé avec analyse des items suivants : La formation ; Le Système d'Information ; L'authentification ; La sécurisation des terminaux ; La sécurisation des réseaux ; Les administrateurs ; Le nomadisme ; La supervision ; L'analyse de risques ; Le RGPD ○ Analyse documentaire (Contrats prestataires informatiques ; Charte IT ; Assurance Cyber ; PRA/PCA ; Rapports de sauvegarde ; RGPD ; Etc.) ○ Analyse « physique » des salles Informatiques ○ Création/Mise à jour d'un schéma réseau simplifié ○ Création/Mise à jour d'une cartographie applicative ○ Tests sur boites mails de salariés de la société ○ Schéma d'estimation de la maturité de l'entreprise face aux risques		✓	✓
Analyse de l'environnement de production de la donnée financière (ITGC) + Analyse du logiciel comptable et de l'ERP (ITAC) – Sur place – 1 mois ○ Rapport détaillé avec analyse des items suivants ITGC : Sécurité Physique ; Sécurité Logique ; Gestion du changement ; Exploitation ; Sauvegardes ; Secours IT ○ Rapport détaillé avec analyse des items suivants ITAC : Données en entrée ; Traitement ; Données en sortie ; Intégrité des données ; Contrôle de gestion ; Composante applicative ; Analyse de l'interface comptable ○ Tests de conformité ○ Listing des items traités avec des constats (risque – maturité) et des recommandations (recommandations – effort) ○ Rédaction d'une feuille de route (plan de remédiation) pour faciliter la prise de décision de la direction ○ Restitution du rapport auprès de la direction			✓

Campagnes de phishing

A l'issue de la mission, nos experts vous font des **préconisations** sur les **outils** à mettre en place, les **formations** à prévoir et les **nouvelles campagnes de phishing** à programmer afin de **réduire les risques d'attaques au sein de votre entreprise.**

Réalisez une CAMPAGNE DE PHISHING adaptée à vos besoins.

Il suffit d'une seule personne réceptive à un mail frauduleux pour que l'entreprise soit mise en danger. Pour vous prémunir contre ces risques de cyberattaques, nous vous proposons de créer une campagne de phishing sur mesure afin de sensibiliser vos collaborateurs aux tentatives d'hameçonnage, avec plusieurs moyens de communication possibles : SMS, e-mail (pouvant intégrer une pièce jointe), QR code, livraison de clé USB, Wifi, IBAN.

Notre campagne de phishing se déroule en 3 étapes :

Modèles disponibles ou création d'un modèle personnalisé

Envoi de la campagne de phishing (via une solution 100% française)

Rapport détaillé faisant ressortir les failles humaines et technologiques

MOON TECH

Sensibilisation et formation des utilisateurs

L'humain est le premier rempart de protection des actifs de l'entreprise, il est aussi l'un des plus simple à faire progresser, par LA FORMATION ET L'ÉCHANGE.

C'est dans cette optique d'**écoute** et de **partage des bonnes pratiques** que nous vous proposons les « formations sécurité et hygiène informationnelle ».

Nos experts conçoivent un parcours de formation **adapté à vos besoins et à vos priorités**, afin de dispenser à vos salariés des **formations complètes sur les risques Cyber.**

Ces sessions de formations **sur-mesure** abordent des thématiques diverses telles que la gestion des mots de passe, la détection des attaques, l'importance de l'identité numérique ou la séparation des usages pro-perso.

Toutes nos formations se terminent par une **évaluation des acquis des participants**.

A la suite de chaque parcours de formation, nos experts vous font un retour détaillé et échangent avec vous sur les **acquis** et les **points de vigilance,** et vous aiguillent sur les **thématiques à prioriser pour de futures formations**.

MOON TECH

Examen de conformité au RGPD

A l'issue de la mission, nos experts vous transmettent un **rapport détaillant le niveau de conformité au RGPD de l'entreprise, et des recommandations quant aux actions à mener avec les traitements à risque.**

Evaluez la conformité de vos traitements au RGPD.

Depuis la mise en application du RGPD, et afin de protéger la vie privée et les libertés individuelles, de nouvelles obligations sont à la charge des entreprises, administrations, collectivités, associations ou autres organismes.

Pour s'assurer de votre conformité, nous réalisons des examens de conformité au RGPD en 3 grandes étapes :

Prise de connaissance des activités de l'entreprise et de ses partenaires

Réalisation d'un audit à l'aide d'un logiciel éprouvé

Restitution des observations et recommandations

MOON TECH

Revue de la gouvernance des systèmes d'information

Réalisez une REVUE DE LA GOUVERNANCE DES SYSTÈMES D'INFORMATION.

La revue de la gouvernance permet de répondre aux questions que se pose la direction générale à propos du niveau de maîtrise de son Système d'Information (SI), et de fournir aux autres fonctions de l'entreprise ou de l'organisation une assurance raisonnable que leurs processus métiers sont bien soutenus par des Systèmes d'Information.

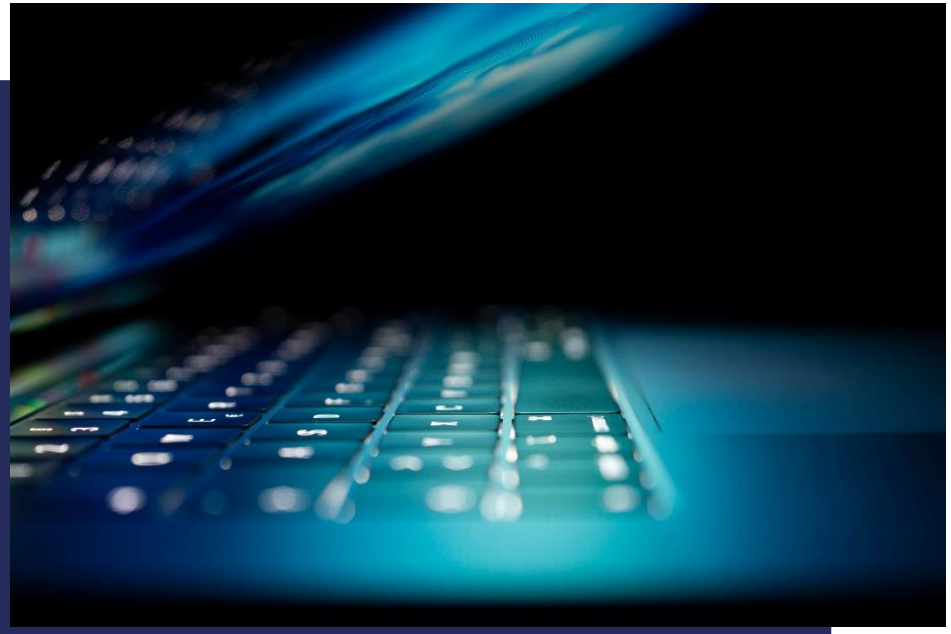
Nous réalisons ces contrôles en 3 grandes étapes :

Prise de connaissance du Système d'Information → **Analyse de documents, interviews et tests** → **Restitution des observations et recommandations**

A l'issue de la mission, nos experts vous transmettent un **rapport avec des recommandations quant aux actions à mener pour améliorer la qualité des processus de l'entreprise.**

MOON TECH

Examen des vulnérabilités



A l'issue de la mission, nos experts vous transmettent un **rapport détaillant les actions à mener en priorité pour corriger les potentielles failles de votre système serveurs et PC.**

Evaluez la sécurité de votre entreprise avec un EXAMEN DES VULNÉRABILITÉS.

Les examens des vulnérabilités permettent d'analyser les failles du système serveurs et PC, de tester la sécurité de votre système informatique et d'évaluer avec quelle facilité un pirate pourrait s'y introduire et y mener des actions illicites.

La mission se déroule en 3 grandes étapes :

1. Prise de connaissance du Système d'Information
2. Réalisation d'examens des vulnérabilités
3. Restitution des observations

MOON TECH

Tests d’intrusion physiques

Evaluez la sécurité de votre entreprise avec des TESTS D’INTRUSION PHYSIQUES

Les tests d’intrusion physiques permettent d’évaluer la facilité avec laquelle il est possible de s’introduire dans les locaux de votre structure et d’accéder aux équipements qui y sont connectés.

Nous réalisons ces tests d’intrusion physiques en 3 grandes étapes :

- Prise de connaissance de la sécurité des locaux
- Réalisation des tests d’intrusion physiques
- Restitution des observations

A l’issue de la mission, nos experts vous transmettent un **rapport détaillant les actions à mener en priorité pour corriger les potentielles failles de sécurité de vos locaux.**

MOON TECH

Social Engineering

A l'issue de cette mission, nos experts vous remettent un rapport complet sur les diverses analyses effectuées lors de cette campagne et vous livrent leurs **recommandations sur les actions à mener afin de réduire le risque informatique qui pèse sur votre structure**.

Vos salariés sont-ils bien protégés ?

Sont-ils assez vigilants ?

Notre mission social engineering a pour objectif d'évaluer les connaissances de vos salariés en matière de sécurité informatique afin de pouvoir, par la suite, leur proposer un parcours de formation sur-mesure et adapté à leurs besoins.

Notre intervention se découpera en plusieurs actions, avec entre autres :

- Des tests pour évaluer la sensibilisation de vos salariés aux risques cyber (transmission de mots de passe à des personnes non habilitées…),
- Des tentatives de prise en main à distance des postes des utilisateurs.

MOON TECH

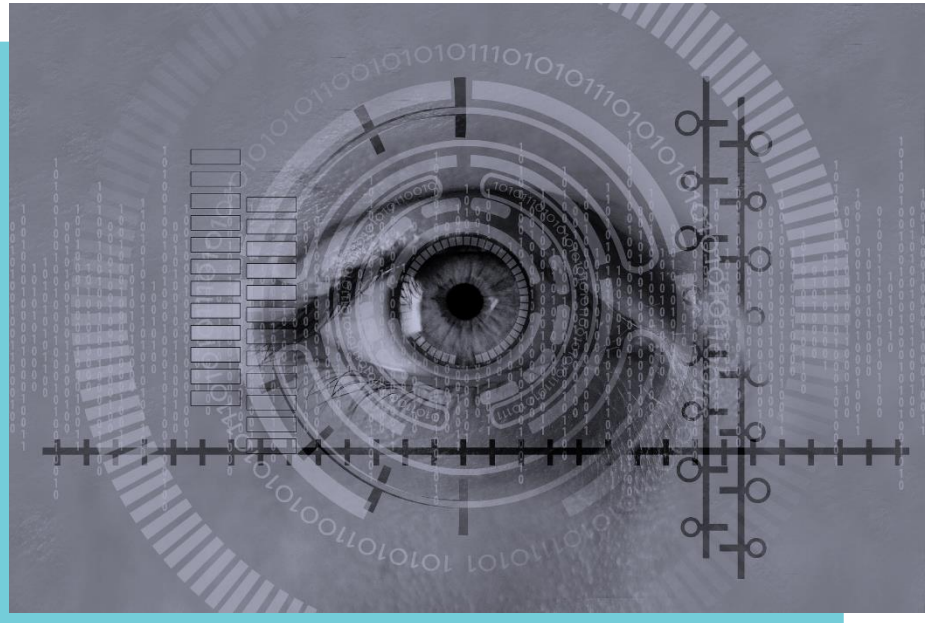
Revue des ITGC et ITAC

Une évaluation financière fiable exige des contrôles ITGC et ITAC de qualité.

Les contrôles généraux informatiques et les contrôles applicatifs sont essentiels dans le cadre des travaux de vérification des comptes, la sécurité informatique impactant directement la fiabilité et l'exhaustivité des données financières.

Nous réalisons ces contrôles en 4 grandes étapes :

1. Analyser l'environnement informatique et des dispositifs de contrôle internes
2. Réalisation d'une revue des contrôles généraux informatiques
3. Réalisation d'une revue des contrôles applicatifs
4. Restitution des observations et recommandations.



A l'issue de la mission, nos experts vous transmettent un **rapport avec des recommandations visant à améliorer l'hygiène informationnelle de l'entreprise.**

MOON TECH

Protection de vos données

Moontech vous propose le TankR, une Appliance de Cyber Sauvegarde Ultra Sécurisée qui respecte l'ensemble des préconisations de l'ANSSI, vous permettant de sauvegarder les paramétrages de vos systèmes d'information et de redémarrer ces derniers en cas d'attaque ou de perte de données.

Piratage à distance quasi-impossible

Conçu pour isoler physiquement les sauvegardes de tout réseau, le TankR protège les données stockées contre les cyber-attaques mais également contre les sinistres accidentels et majeurs.

Les +

- Décliné de 1 à 70 To
- Surveillance à distance
- Attaque de surface régulière sur nom de domaine
- Livraison
- Installation
- Hotline
- Rapport mensuel

Cyber-sécurité / cyber-sauvegarde / cyber-résilience

- Systèmes innovants qui rendent **invisibles** vos données sur les réseaux et les **protègent** de toutes attaques et risques majeurs
- Permet de redémarrer votre entreprise suite à une **attaque** de **malwares** et de **ransomwares** ou simplement suite à une **défaillance de disques durs** ou **une fausse manipulation**
- **Réduction importante des effets** d'un sinistre informatique, qu'il soit criminel, matériel ou accidentel
- Données rendues **immutables** et **incorruptibles** faces au ransomware et cryptovirus de nouvelle génération

Protection des risques physiques majeurs

Protection explosion | Protection d'eau | Protection contre le feu | Projection contre le vol | Protection électromagnétique | Protection Cage faraday | Suppression Radio, wifi, GPS, 3G

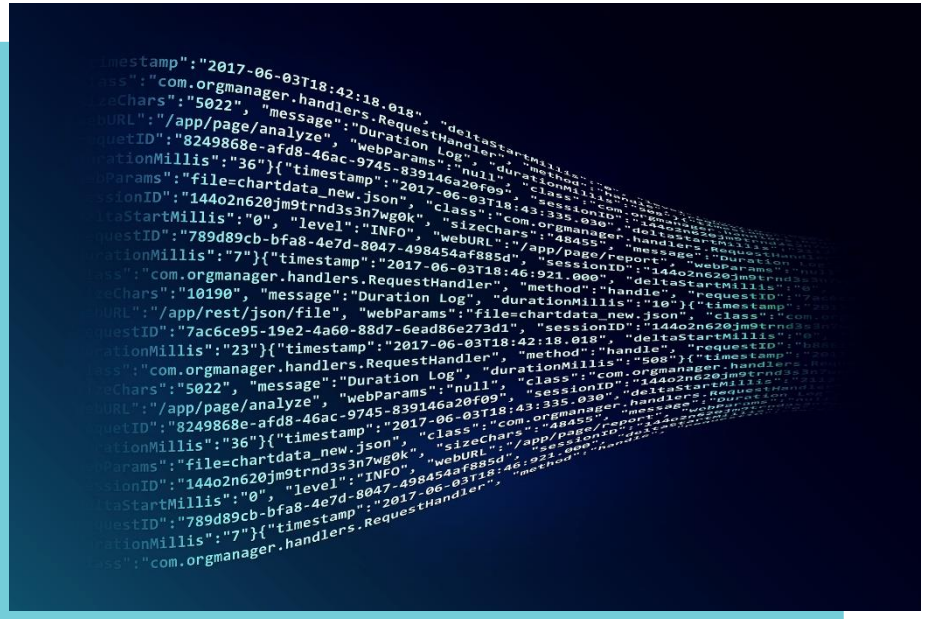
Récupération de données

Ne laissez plus vos données s'évaporer, utilisez une solution de RÉCUPÉRATION DES DONNÉES.

Les disques durs d'ordinateurs, et notamment ceux de vos collaborateurs nomades, peuvent facilement s'abimer avec le temps. Si aucune sauvegarde n'est réalisée, à la première panne, toutes vos données seront perdues.

Nos techniciens partenaires spécialisés dans la remontée de ces données dites « disparues » interviennent alors pour récupérer vos données, selon le processus suivant :

- Diagnostic quant à la faisabilité de l'opération
- Extraction des données sur support neuf
- Restitution des données au client



Rédaction d'un cahier des charges

Vous avez acté les orientations à donner à votre SI pour renforcer sa sécurité, mais comment allez-vous RÉDIGER UN CAHIER DES CHARGES afin de définir le bon partenaire pour les mettre en place ?

A la suite de notre mission d'évaluation de l'exposition aux risques cyber, nous vous aidons à **rédiger un cahier des charges qui englobe les observations détaillées par nos experts dans le plan de remédiation**, puis **nous** vous accompagnons par la suite dans la consultation et le choix des prestataires informatiques.

La mission se découpe en 3 phases :

Phase 1
Suite à une évaluation, définition du **périmètre d'intervention** et **rédaction du cahier des charges**

Phase 2
Interrogation des prestataires

Phase 3
Restitution des observations

Les observations vous seront remises sous forme de rapport à la fin de mission, afin que vous puissiez choisir sereinement et avec le niveau d'informations nécessaire, le prestataire informatique avec lequel vous souhaitez collaborer.

Contact

MOON TECH

CONSEIL ET SÉCURITÉ INFORMATIQUE

75 rue de la Villette 69003 Lyon

04 51 08 79 77

contact@moontech.fr

www.moontech.fr