



Catalogue de services Cybersécurité

2024-2025



Cybersécurité

La cybersécurité permet la mise en place de solutions pour protéger ses systèmes d'information, ses réseaux et ses données, contre les menaces et les attaques provenant de l'environnement numérique.

Sécuriser votre entreprise c'est protéger vos clients. Spécialisés en gestion informatique et composés d'experts, nous répondons à bon nombre de vos besoins.

C'est justement au sein des entreprises que les risques informatiques surviennent en général : quelle que soit leur taille, les données sont un capital précieux.

Cybersécurité



Nos Offres

Un audit informatique est une photo à l'instant T du niveau de sécurité global de votre système informatique. Il est possible d'auditer votre site web comme votre système d'information ou une application

PHISHING

Prestation permettant d'évaluer la capacité des employés à réagir face aux emails frauduleux. Sensibiliser les employés à la sécurité en ligne, renforcer les mesures de sécurité et réduire les risques de violations de données et d'attaque malveillantes.

PENTEST

Opération consistant à évaluer les vulnérabilités d'un système informatique en simulant une attaque, pour identifier les failles de sécurité et les points faibles qui pourraient être exploités par des attaquants malveillants.

ASSISTANCE À LA MISE EN CONFORMITÉ

Pour les entreprises, répondre à un PAS (plan d'assurance sécurité) imposé par un client implique souvent une mise à niveau de leurs pratiques, avec des audits réguliers et la fourniture de preuves de conformité.

AUDIT SÉCURITÉ

Offre permettant de faire le point sur le système d'information déjà en place au sein de l'entreprise afin de l'évaluer et d'en ressortir une liste de recommandation permettant d'en renforcer la sécurité.

SÉCURISATION M365

NIT accompagne les entreprises dans la mise en place et la sécurisation de leur environnement Microsoft 365 (M365), garantissant un déploiement efficace et protégé.

Phishing

NOS PRESTATIONS

Les attaques ont lieu lorsque votre système informatique présente des failles. Lors de cyberattaques, ces failles sont exploitées, permettant d'accéder à vos données sensibles ou de prendre le contrôle des systèmes.

Nous mettons en place une technique de fraude qui consiste à envoyer des courriels ou des messages frauduleux pour inciter les utilisateurs à divulguer des informations personnelles ou à cliquer sur des liens malveillants.

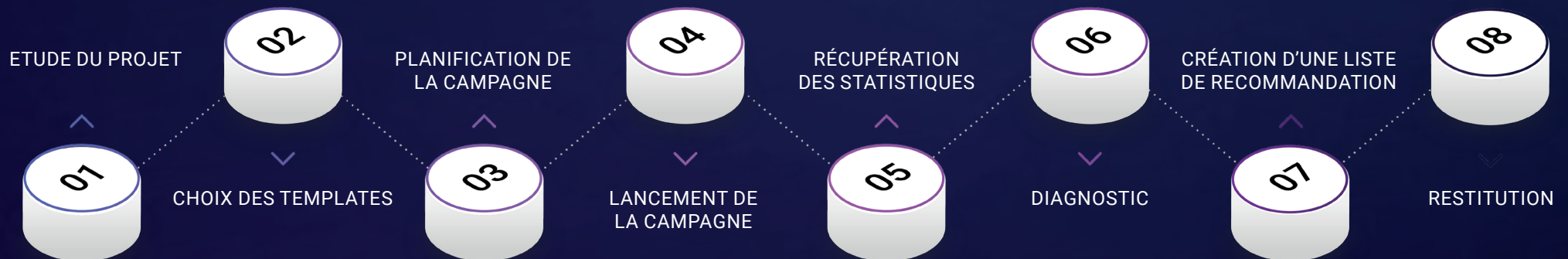
Toutes les solutions peuvent être hébergées sur nos infrastructures sécurisées.

1 TEMPLATE

3 TEMPLATES

5 TEMPLATES

DÉROULEMENT D'UNE CAMPAGNE DE PHISHING



Pentest

NOS PRESTATIONS

7 jours pour tous les types d'intrusion permettant d'analyser les agissements de l'interne à l'externe. Pour renforcer votre sécurité avec des simulations d'intrusion en conditions réelles.

BOITE BLANCHE

Tester la sécurité mise en place depuis le réseau interne de l'entreprise.

- Sur site / depuis un accès VPN sur une session utilisateur classique
- Création d'un utilisateur pour l'opération
- Définition des créneaux horaires (par défaut 8h-20h)
- Définition du périmètre d'action
- Rédaction et envoi d'une lettre de mission (mandat) à signer avant le début du test d'intrusion.
- Rapport
- Document technique répertoriant les failles exploitées et les correctifs à mener

BOITE GRISE

Tester la sécurité mise en place depuis le réseau interne de l'entreprise avec des accès limités.

- Sur site / depuis un accès VPN
- Définition des créneaux horaires (par défaut 8h-20h)
- Définition du périmètre d'action
- Rédaction et envoi d'une lettre de mission (mandat) à signer avant le début du test d'intrusion.
- Rapport
- Document technique répertoriant les failles exploitées et les correctifs à mener

BOITE NOIRE

Tester la sécurité mise en place sans accès au réseau interne de l'entreprise.

- Définition des créneaux horaires (par défaut 8h-20h)
- Définition du périmètre d'action et des limites/autorisations à affecter au test d'intrusion
- Rédaction et envoi d'une lettre de mission (mandat) à signer avant le début du test d'intrusion.
- Rapport
- Document technique répertoriant les failles exploitées et les correctifs à mener

Assistance À LA MISE EN CONFORMITÉ

NIT accompagne les entreprises dans leur mise en conformité avec les exigences de sécurité dictées par les plans d'assurance ou les contrats de sécurité imposés par leurs clients.

Pour les entreprises, répondre à un PAS (plan d'assurance sécurité) imposé par un client implique souvent une mise à niveau de leurs pratiques, avec des audits réguliers et la fourniture de preuves de conformité.



NIT propose une expertise complète pour évaluer les écarts entre les exigences demandées et l'état actuel des dispositifs de sécurité.

Grâce à des audits, des recommandations ciblées et des solutions adaptées, NIT aide ses clients à aligner leurs pratiques sur les standards requis, tout en garantissant la mise en place de mesures correctives efficaces.

NIT permet aux entreprises de répondre rapidement aux attentes de leurs partenaires, tout en renforçant leur propre résilience face aux menaces.

Audit

NOS PRESTATIONS

Afin d'optimiser au mieux toutes les ressources de votre parc informatique, nos techniciens réalisent un audit complet de votre système d'information. Notre structure propose alors une veille technique, une assistance de tous les instants ainsi qu'un service d'audit et de conseils personnalisés pour chaque client. À destination des PME et des grandes entreprises, NIT, spécialisée audit informatique Lyon, répond à tous vos besoins et se montre disponible pour vous fournir une prestation de qualité tout en appréciant la discrétion de nos équipes.

Architecture réseau

Parc informatique

Infrastructure serveur

Système de sauvegarde

Logiciels clients

Sécurité de l'ensemble du SI

liste non exhaustive des actions menées

Inventaire du parc informatique (l'ensemble des équipements propriétaire et locataire)

Schéma réseau

Emplacement du matériel réseau et du serveur

Scan du réseau

Segmentation du réseau

Analyse du serveur (système)

Inventaire des logiciels utilisés

Connexion sur un poste client

Analyse du plan de sauvegarde

Analyse des systèmes d'impression

Analyse du système de vidéo/caméras

SÉCURITÉ / INFRASTRUCTURE

5 jours

Présence de 2 experts sur les cinq journées.
(Expert cybersécurité et expert infrastructure et réseau)

Etude sur
site client

01

Rédaction
(2 jours)

02

Restitution
et remise du
livrable

03

Sécurisation

ENVIRONNEMENT M365

NIT accompagne les entreprises dans la mise en place et la sécurisation de leur environnement Microsoft 365 (M365), garantissant un déploiement efficace et protégé.

NOTRE SOLUTION

- Intervention à travers un audit de votre environnement Microsoft 365
- Vous permettre de connaître votre niveau de sécurité
- Accompagnement dans l'optimisation de cette dernière
- Livrable : rapport détaillé

Revoir les
paramétrages

01

Entretiens
organisationnels

02

Recommandations

03



Régie **Assistance technique**

Vous recherchez un expert en cybersécurité ?

NIT mobilise pour vous la personne idéale pour intervenir dans votre entreprise.

Nous proposons un mode d'intervention en régie pour répondre à vos besoins, en vous permettant d'intégrer une expertise précise à votre équipe.

Cet expert intervient pour une durée prédéfinie, variable en fonction de vos exigences, sur une fréquence adaptable à votre besoin, sur un projet ou sur le quotidien en tant que ressource supplémentaire.



NIT
INFORMATIQUE
TECHNOLOGY

www.novances-it.com