inwi cyberdéfense

la sécurité, notre métier

Catalogue des offres et services 2018

inwi BUSINESS

Pourquoi des offres de cybersécurité ?

Mon entreprise est-elle concernée ?

En 2018, les cyberattaques sont placées par le World Economic Forum au 3e rang des principaux risques auxquels les États, les institutions publiques ou privées font face. Le nombre des cyberattaques est multiplié par deux chaque année et le coût sur l'économie mondiale est estimé à 445 milliards de dollars ; aucun continent n'est épargné, car ces attaques viennent du Web.

Toutes les entreprises connectées au réseau internet ou échangeant des données au quotidien sont concernées. Les sites de e-commerce, les messageries, les serveurs informatiques, les employés, leurs comportements et habitudes, sont autant de vecteurs potentiels de cyberattaques.

Cyber-chiffres à retenir

752% de croissance des cyberattaques de type Ransomware en 2017

+400 millions de nouvelles variantes de logiciels malveillants enregistrées en 2017

8,4 milliards d'appareils IoT, vecteurs potentiels d'attaques sur la planète

91% de croissance des attaques par DDoS en 2017

64% des CIO en Afrique considèrent le "maintien de la sécurité" comme la priorité des défis commerciaux et informatiques (Source : IDC)

27,4% de croissance annuelle des coûts financiers engendrés par les cyberattaques en entreprise

X2 En cinq ans, le nombre d'infractions informatiques enregistrées par les entreprises a doublé

40% des professionnels marocains déclarent avoir déjà branché sur leur ordinateur des clés USB inconnues (source : Kaspersky 2017)

1 e-mail / 131 contient un malware (Source : Symantec)

33% des professionnels marocains affirment avoir déjà cliqué sur des pièces jointes sans en connaître la provenance (source : Kaspersky 2017)

83 981 attaques DDoS au Maroc (Source : Arbor 2017)

6 998 attaques DDoS par mois
230 attaques par jour
10 attaques DDoS par heure
(source : Arbor 2017)

Au Maroc, la réglementation évolue et un programme national est mis en place depuis 2016

95% des organismes utilisent internet.

La conformité aux réglementations est obligatoire sous l'impulsion de la DGSSI* (décret n°2-15-712 du 22 mars 2016).

Depuis 2016, une campagne nationale de lutte contre la cybercriminalité prévoit la sensibilisation, la formation et l'accompagnement à la protection contre les cyberattaques.

Le décret n° 2-11-508 a défini la nomenclature caractérisant les Organismes d'Infrastructures d'importance Vitale (OIV) qui concernent plus de 200 entreprises devant se conformer à la stratégie mise en place.

Établir une stratégie de défense est essentiel pour que l'entreprise puisse prévoir et se protéger des cyber-risques.

Le plus important n'est pas de se demander si vous serez attaqué un jour, mais comment y remédier et s'en protéger si cela venait à arriver

* DGSSI : Direction Générale de la Sécurité des Systèmes d'Information au Maroc.

inwi cyberdéfense, 1er catalogue d'offres de cybersécurité

Les menaces liées aux cyberattaques sont de plus en plus grandes, complexes et diversifiées. Leur caractère n'est pas hasardeux, mais vise à déranger une activité, à la neutraliser ou affecter l'image d'une entreprise.
Pour surveiller et sécuriser votre réseau informatique, vos plateformes et vos sites internet, **inwi Business** a mis en place **inwi cyberdéfense** un portefeuille d'offres dédié à la sécurité des entreprises. Mis en œuvre à partir de l'expertise **inwi Business** et des partenariats avec les leaders mondiaux des solutions de cybersécurité, notre catalogue adresse le besoin de toutes les entreprises.

ARBOR NETWORKS, paloalto, McAfee, RAPID7, Symantec

Nos 3 offres phares

SOC inwi Business

Business Protect

Managed Anti-DDoS

Pourquoi choisir inwi Business comme partenaire de votre sécurité informatique?

inwi Business est votre partenaire de choix pour adresser et vous protéger contre toutes les menaces du Web, les cyberattaques et les violations de données.

Une interface unique
pour toutes les solutions MSSP

Un service assuré en 24h/24 et 7j/7

Des partenariats stratégiques
avec les plus grands réseaux internationaux d'experts en sécurité

Un portefeuille sécurité complet
et adapté au besoin de toutes les entreprises

Des infrastructures de cybersécurité de dernière génération

Des solutions clé en main
et totalement gérées par inwi Business

SOC inwi Business

Et si nous mettions un SOC à votre disposition ? Découvrez notre offre phare

Le SOC inwi Business gère vos incidents et événements en s'assurant qu'ils soient correctement identifiés, analysés, communiqués, actionnés, défendus, enquêtés et signalés.
Notre équipe d'experts veille à votre sécurité en **24/7/365**.
Ce SOC composé d'experts en sécurité est **basé au Maroc**.

Opéré en partenariat avec Symantec

Comment fonctionne le SOC inwi Business ?

Lieu du niveau 1 : Casablanca
Fonctionnement du SOC : 24/7/365
Expertise : niveaux 1, 2 et 3
Log Management : solution en partenariat avec McAfee.
Plateforme de Vulnerability Management : solution en partenariat avec Rapid7

Les niveaux 2 et 3 sont assurés en partenariat avec **Symantec, leader du magic quadrant de Gartner depuis 13 ans et comptant plus de 1 000 professionnels de la cybersécurité certifiés !**

Catalogue de nos services SOC

	Log Management	**Collecter et conserver les logs**
S'adapter à vos besoins	**100%** Cloud	
	Choisissez le volume journalier des logs à collecter de **1 à 50 Go/jour**	
	Choisissez la durée de rétention des logs de **1 à 5 ans**	
	Monitoring	**Détecter, corréler et remonter les incidents**
Déploiement flexible	Utilisez votre propre **SIEM** ou celui de **inwi Business**	
Sur mesure	À partir de **500 EPS « Event per Second »** jusqu'à au-delà de **5 000 EPS**	
Vos SLA	Selon votre besoin de **8 h / 24 h, 5 j / 7** ou **24 h / 24, 7 j / 7 et 365 jours par an**	
Helpdesk	Experts de **inwi Business** et ses partenaires, disponibles par **le système de ticketing,** le courrier **électronique** et le **téléphone**	
	Incident Response	Intervenir, identifier la source, éradiquer la menace et dresser le plan d'action pour éviter toute récidive
Composez votre service	Une prestation à la demande sans abonnement, **facturée à l'heure**	
	Service Standard – 24 h pour intervention à distance **Service Premium** – 48 h pour intervention sur site	
Vous êtes victime d'une cyberattaque?	Nos experts identifient le type de menaces, sa source et son comportement, définissent un plan d'isolation, **éradiquent la menace** et ses sources d'échanges et **rétablissent le statut normal des services**	
Audit	**Table top exercice :** évaluer les outils, les processus et l'expertise que votre organisation utilise pour répondre aux cyberattaques, préparation à la gestion de crise, revue ou rédaction de SOPs (Standard Operating Procedures)	
	Intelligence Feeds	Offrir des flux d'intelligence afin de détecter, arrêter, prédire les menaces et renforcer les défenses
Enrichissez votre connaissance de la cyberdéfense	• Bulletins et flux de **vulnérabilité/menace** • **Résumé hebdomadaire** des renseignements • Bulletins sur les **menaces émergentes** • Live Intelligence Briefing sur **les menaces (webinar)**	
Modularité	En standard ou personnalisé pour votre **zone géographique** et votre **secteur d'activité** avec une **surveillance en temps réel** des points d'information pour identifier **pro-activement** les acteurs de la menace dont vous êtes la cible	

Vulnerability Management

Scanner, identifier et remédier aux vulnérabilités

	Vulnérabilités	**Express**	**Entreprise**
Déploiement flexible	Cloud	Cloud et sur site client	Cloud et sur site client
Scan interne / externe	Externe	Interne et externe	
Nombre d'adresses IP	**5**	**5**	**10**
Nombre d'appareils de scan	**-**	**2**	**5**
Nombre de comptes client	**1**	**1**	**3**
Appareils de scan additionnels	-	À la demande	À la demande
Adresses IP additionnelles	-	À la demande	À la demande
Rapport	✔	✔	✔
Rapport de conformité (PCI-DSS, ISO 27 001)	✔	✔	✔
Rapport personnalisé	-	✔	✔
Accès portail	-	✔	✔
Intégration d'actifs	Inclus, Max 5	Inclus, Max 5	Inclus, Max 10
Helpdesk	Inclus	Inclus	Inclus
Génération de plan de remédiation	Inclus	Inclus	Inclus
Session de restitution	-	-	Inclus

Business Protect

Qui a dit que les solutions de Next Generation Firewalls n'étaient réservées qu'aux grandes entreprises ? Découvrez notre offre en détail.

inwi Business protège tout votre réseau informatique depuis sa plateforme de sécurité centralisée.
Afin de vous garantir une sécurité optimale, nous mettons à votre disposition le meilleur de notre expertise, que ce soit en mode Cloud ou à partir de pare-feux informatiques (firewalls) installés chez vous et administrés par les experts de **inwi Business**.

Quelques exemples de menaces du quotidien

Les entreprises doivent affronter l'accroissement des risques et des menaces informatiques, dont les plus connues sont :

- Des cyberattaques
- Le cheval de Troie
- Les e-mails de spam ou accompagnés de virus
- La vulnérabilité de certains logiciels
- Des structures dépendantes d'internet
- Des infections par des logiciels espions (spywares)
- Des attaques d'applications
- Des vols de données
- Des technologies vieillissantes ou non mises à jour
- Ransomware et logiciels malveillants

inwi Business vous propose ce service en partenariat avec PaloAlto

paloalto NETWORKS®

Filtrage Web et applicatif
Examine le trafic internet et applicatif et fixe les règles de gestion et droits des utilisateurs

Anti-virus, anti-spyware et anti-spam
Décèle et détruit les virus informatiques et les logiciels espions, borne le volume des e-mails non sollicités

Réseau privé virtuel
Crée un lien direct entre des ordinateurs distants, en isolant le trafic à travers la mise en place d'un tunnel

Protection Zero Day
Détecte et protège contre les attaques inconnues

Pare-feu nouvelle génération
Mesure la prévention des applications et des paquets et respecte la politique de sécurité du réseau

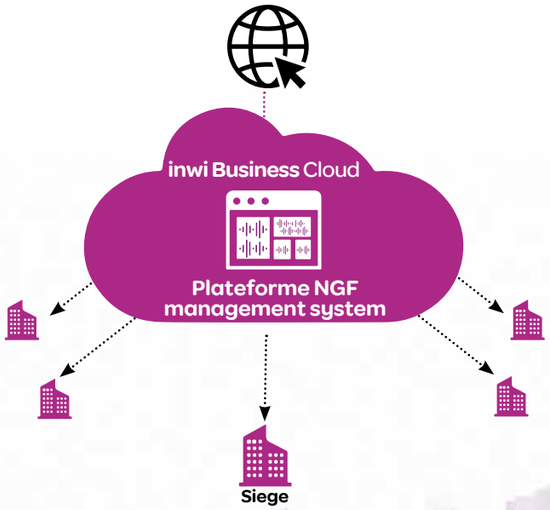
Repérage et prévention d'intrusion (IPS)
Détecte des activités suspectes ou anormales, et renvoie une analyse sur les tentatives réussies comme échouées des intrusions

Data Loss Protection (DLP)
Assimile, examine et protège l'information grâce à des analyses de contenu détaillé

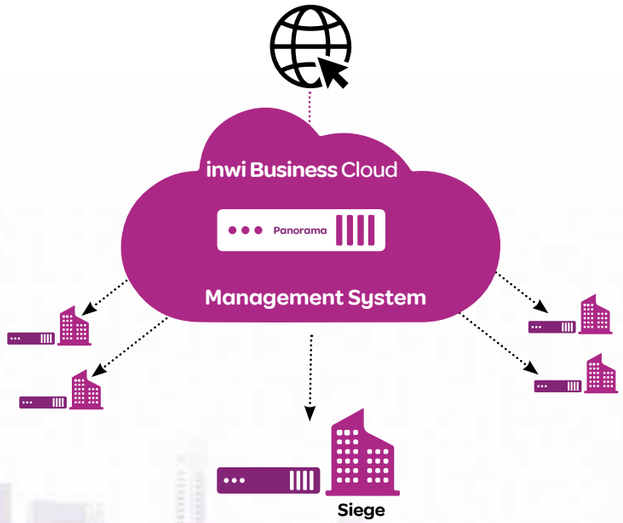
Vol d'identité
Protège contre le vol des identifiants d'utilisateurs légitimes pour accéder aux informations névralgiques d'une entreprise

Business Protect
Flexibilité de déploiement, offre disponible aussi bien en mode 100% Cloud que sur site client !

Aucune installation nécessaire, la protection est la gestion centralisée est assurée par la plateforme NGF* de **inwi Business**



Des équipements sont installés dans les sites du client et la gestion centralisée est assurée depuis le Cloud **inwi Business**



* Next Generation Firewall

Nos 3 packs

	Engagement 12 mois	Engagement 24 mois	Engagement 36 mois
	Business Protect CleanPipe	**Business Protect Virtual**	**Business Protect Dedicated**
Déploiement flexible	Cloud	Cloud	Sur site client
À votre mesure	Des profils à la carte	Par paliers de débit et du nombre d'utilisateurs	
Next Generation FIrewall	✔	✔	✔
Protection ZeroDay	✔	✔	✔
Détection/Protection d'intrusion (IPS)	✔	✔	✔
Contrôle applicatif	✔	✔	✔
Filtrage web	✔	✔	✔
Anti-virus Anti-Spam Anti-Spyware	✔	✔	✔
Rapport	✔	✔	✔
Filtrage de fichier		✔	✔
VPN SSL et IPSec		✔	✔
DNS Sinkhole		✔	✔
Politique personnaliée		✔	✔
Protection vol d'identité			✔
Data Leak Prevention (DLP)		**Option**	**Option**

Managed Anti-DDoS

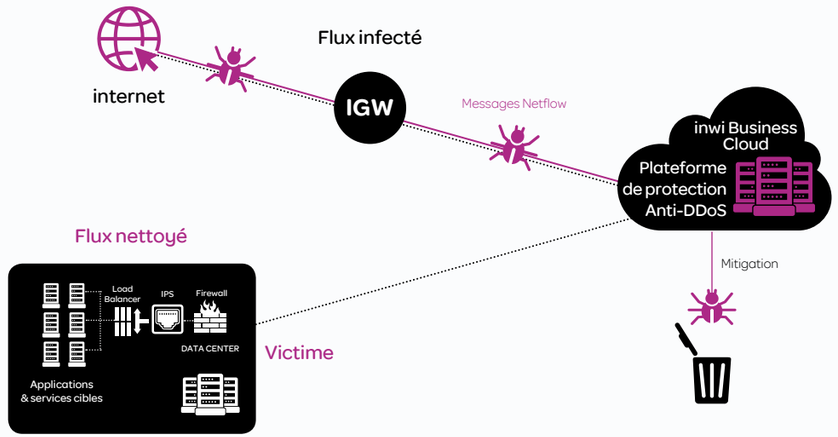
Ne laissez pas des inconnus ou des robots saturer vos serveurs !

Les attaques DDoS ou par déni de service ont pour objectif de saturer vos serveurs pour les rendre inopérants.

Les impacts d'une attaque DDoS sur l'activité d'une entreprise sont divers et ont pour conséquence :

- **des coûts directs :** perte de revenus et d'occupation des ressources (liée à l'inactivité pendant l'attaque), possibles pénalités liées à l'indisponibilité d'un service vis-à-vis des clients;
- **des coûts indirects :** comme la perte de productivité et la perte d'image;
- **des coûts de perte d'opportunités :** comme la désaffection des clients et les opportunités commerciales manquées.

Comment se passe une attaque DDoS et comment y remédions-nous ?



Mitigation intelligente et automatique

Nos 3 packs

	Managed Anti-DDoS Emergency	Managed Anti-DDoS Standard	Managed Anti-DDoS Premium
Mode de déploiement	Cloud	Cloud	Cloud et sur site client
Nombre de mitigations	Par intervention	Illimité	Illimité
Détection attaques volumétriques	Inclus	Inclus	Inclus
Détection attaques protocolaires	Inclus	Inclus	Inclus
Détection attaques applicatives		À la demande	Inclus
Mitigation attaques	À la demande	Inclus	Inclus
Mitigation applicative		À la demande	Inclus
Déclenchement de la mitigation	Suite confirmation client	5 à 20 min après détection	Permanent
Disponibilité		99,8%	+ GTR 4h
Rapport	Fin de mitigation	Mensuel	Mensuel
Alerte e-mail		Inclus	Inclus
Portail client		Inclus	Inclus
Trafic entrant	Inclus	Inclus	Inclus
Trafic sortant			Inclus

inwi Business vous propose ce service en partenariat avec Arbor Networks

ARBOR NETWORKS

Vous souhaitez comprendre le jargon de la cyber sécurité en 1 minute ? Voici notre cyber glossaire

• **SOC :** ou Security Operating Center, est un centre de contrôle opérationnel de la supervision d'un réseau de sécurité informatique qui permet de détecter des cybermenaces, des attaques ou des virus informatiques.

• **MSSP :** ou Managed Security Service Provider, désigne les services de sécurité informatique offerts aux entreprises en mode Cloud par **inwi Business**.

• **Anti-DDoS :** ou Anti-Distributed Denial of Service, désigne un système permettant de se prémunir des attaques provenant de l'internet et caractérisé par une tentative de déni de service.

• **Vulnerability Management :** désigne le service de scan des vulnérabilités qui vise à identifier les vulnérabilités liées à une organisation selon sa couverture des risques et à fournir une liste de recommandations priorisées pour y remédier.

• **Monitoring :** désigne la mise en place et gestion du SIEM afin de détecter, corréler et remonter les incidents à partir de plusieurs sources de données (log, réseau, netflow), s'interfacer avec plusieurs plateformes (analytics, intelligence) afin d'enrichir la gestion des menaces.

• **Threat Intelligence :** désigne un service d'intelligence qui permet d'enrichir le service de monitoring et de gestion des incidents du SOC. Il offre des flux d'intelligence émanant de plusieurs sources afin de détecter et arrêter les cyberattaques, prédire les menaces, renforcer de manière proactive les mécanismes de défense.

• **Incidence Response :** désigne l'intervention des équipes en amont, lors de l'apparition de l'incident ou d'un post-incident afin d'identifier la source, éradiquer la menace et dresser le plan d'action pour éviter toute récidive. La réponse aux incidents peut se faire à travers une intervention à distance, ou à travers une intervention sur le site de l'entreprise.

• **SIEM :** ou Security Information & Event Management, désigne le système permettant la collecte, l'agrégation et la corrélation des événements du système d'information.

• **CERT :** ou Computer Emergency Response Team, désigne un centre d'alerte et de réaction aux attaques informatiques, destiné aux entreprises ou aux administrations, mais dont les informations sont généralement accessibles à tous.

• **EPS :** ou Event Per Second, est un terme utilisé dans la gestion informatique pour définir le nombre d'événements ou de processus qui se déroulent à un moment donné sur n'importe quel système informatique.

• **Firewall :** (ou pare-feu) est un outil informatique (matériel et/ou logiciel) conçu pour protéger les données d'un réseau (protection d'un ordinateur personnel relié à Internet par exemple, ou protection d'un réseau d'entreprise).

• **OWASP :** Open Web Application Security Project est une communauté en ligne travaillant sur la sécurité des applications Web.

• **CVE :** ou Common Vulnerabilities and Exposures, est un dictionnaire des informations publiques relatives aux vulnérabilités de sécurité. Le dictionnaire est maintenu par l'organisme MITRE, soutenu par le département de la Sécurité intérieure des États-Unis.

• **CWE :** ou Common Weakness Enumeration, est une liste des vulnérabilités que l'on peut rencontrer dans les logiciels. Cette liste est maintenue par l'organisme MITRE, le projet étant soutenu par la National Cyber Security Division et le département de la Sécurité intérieure des États-Unis.

Une question sur nos offres et services ?

Appelez-nous au 05 29 10 10 10, contactez votre responsable de compte habituel,
ou adressez-nous un mail sur :
servicecommercial.entreprises@inwi.ma

inwi
BUSINESS