



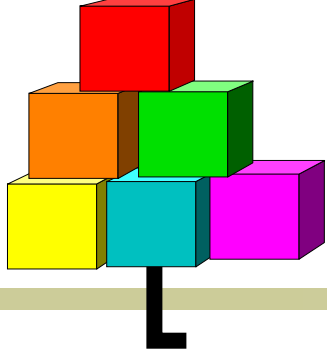
PRESENTATION



- L'objectif est d'être un acteur reconnu sur le marché :
 - du Conseil,
 - de l'Assistance à Maîtrise d'Ouvrage,
 - et une véritable référence dans le domaine de la Sécurité

- **ALYOTECH SECURITY** propose des interventions à forte valeur ajoutée dans la sécurité opérationnelle du Système d'Information, comme :
 - des missions de diagnostic et d'audit des processus de sécurité de l'entreprise en s'appuyant sur les normes de sécurité ISO 27002, COBIT et les processus IT, CMMI et ITIL.
 - la réalisation de tests sur les réseaux et systèmes d'exploitation,
 - la mise en œuvre de solutions opérationnelles pour remédier aux vulnérabilités en particulier par le durcissement des systèmes, la conception et le développement d'applications sécurisées.

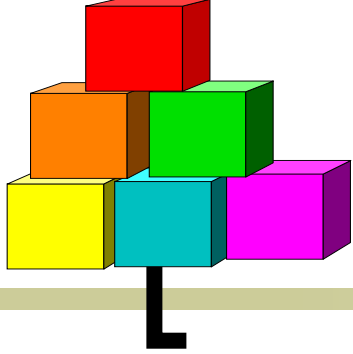
- *« Nous sommes convaincus que la sécurité est en train de devenir un enjeu de plus en plus stratégique pour les entreprises d'aujourd'hui compte tenu des phénomènes d'intrusion ou de piratage que l'on peut observer et nous entendons grâce à Alyotech Security nous positionner comme un acteur incontournable dans ce domaine »* a déclaré le management du **Groupe ALYOTECH**



Stratégie 1/2



- Pénétration du marché à travers l'audit & la formation,
- Politique grands comptes et sociétés implantées à l'internationale,
- Partenariats stratégiques avec des éditeurs de produits.



Stratégie 2/2



APPROCHE TECHNIQUE

APPROCHE JURIDIQUE

APPROCHE NORMES

Cœurs de métier

Infrastructures Informatiques Sécurisées

- ▶ Conseil / Expertise sécurité
- ▶ AMOA / AMOE sécurité
- ▶ Définition d'architectures sécurisées
- ▶ Expertise sécurité des systèmes d'information

Sécurité des Systèmes d'Information

- ▶ Conseil / Expertise
- ▶ AMOA / AMOE
- ▶ Audit / Analyse des risques / Tests d'intrusion et de Vulnérabilité
- ▶ Intégration de solutions
- ▶ Exploitation / Sécugérance...

Intelligence Economique

- ▶ Conception et pilotage de cellule de veille
- ▶ Analyse et cartographie de l'environnement concurrentiel
- ▶ Recherche d'informations stratégiques
- ▶ Stratégies d'influence

L'approche globale

- Veille technique
 - État de l'art et analyse des menaces et des vulnérabilités
 - Qualification de solutions
- Mesures aval
 - Urbanisation de la Sécurité du SI
 - Sécurisation physique (sites, accès, matériels)
 - Sécurisation logique (télécom, accès, réseaux, systèmes, applications...)
 - Continuité de l'activité
- Évaluation et diagnostic
 - Audits
 - Analyse de risques
 - Classification des actifs (physiques et logiques)
 - Tests d'intrusion
- Mesures amont
 - Schéma directeur sécurité
 - Politique de sécurité
 - Organisation de la sécurité
 - Normes de sécurité ISO 27002
 - Formation, sensibilisation

Une offre globale

respectant le cycle P.D.C.A(*) de la norme ISO 29002

Assistance Maîtrise d'Ouvrage

- Schéma directeur sécurité IT
- Définition politique sécurité : thématique / technique
- Évaluation des risques / Audit fonctionnel et technique
- Conception d'architectures sécurisées / Définition de cahier des charges



Intégration

- Assistance à Maîtrise d'Oeuvre
- Solutions techniques du marché
- Solutions techniques spécifiques
- Architecture Open source

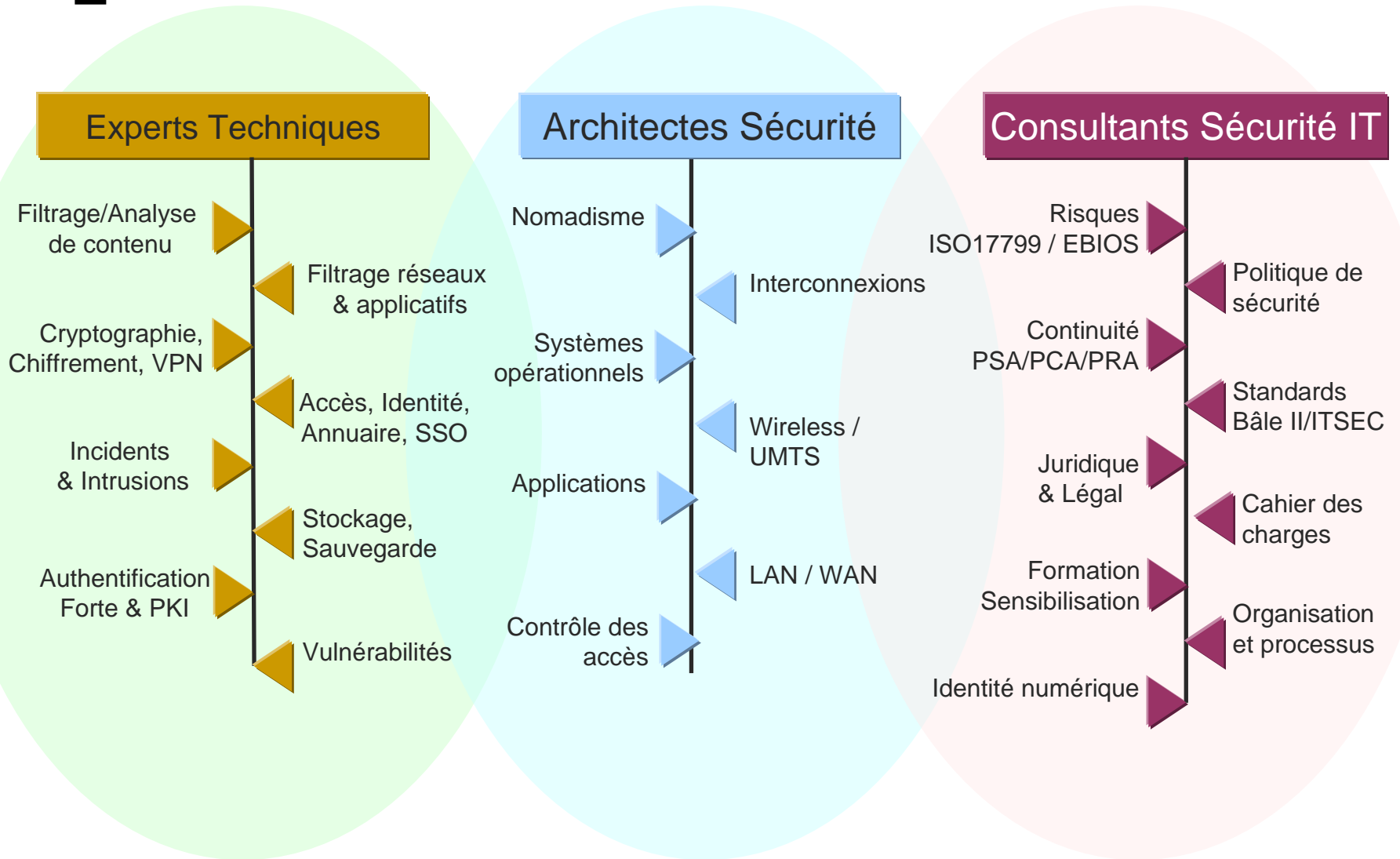


Management

- Supervision et exploitation de la sécurité IT
- Administration de la sécurité IT
- Offre globale de sécurgérance externe / interne

(*) P.D.C.A : Plan Do Check Act

Des compétences globales ...





Compétences 1/2



- **Audit Sécurité,**
- **Vérification et validation des systèmes informatisés**
tests d'intrusion, expertise des systèmes sous l'angle de la sécurité.
- **Aide aux choix de solutions et d'architectures de sécurité,**
- **Réalisation, intégration, mise en oeuvre et accompagnement de solutions,**

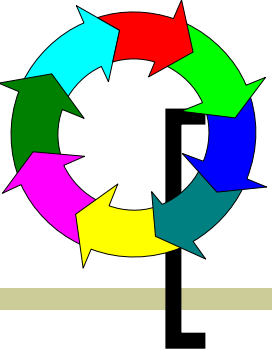


Compétences 2/2

- Méthodologie sécurité,
- Aspects techniques/juridiques/Normes
- Architecture et réseaux,
- Intranet et internet,
- Systèmes d'information,
- Vulnérabilités des systèmes,
- Détections et tests d'intrusion,
- Formation et transfert de savoir-faire.

Tests d'intrusion : déroulement

- Recueil d'informations
 - repérage des systèmes à attaquer,
 - identification des services fournis et logiciels correspondants.
- Recherche de vulnérabilités
 - identification de failles connues,
 - recherche de failles nouvelles.
- Exploitation des vulnérabilités et intrusion
- Occupation des systèmes compromis
 - installation de backdoors, rootkits, etc.
 - poursuite des attaques.



MISE EN PLACE D'ARCHITECTURES SECURISEES

- Élaboration des spécifications,
- Conduite de projet et déploiement,
- Domaines :
 - sécurité des accès physiques et logiques (authentification forte, cloisonnement,...),
 - sécurité des échanges (VPN, chiffrement,...),
 - sécurité des systèmes et réseaux (serveurs, postes de travail, sauvegarde, lutte antivirale, cloisonnement,...),
 - sécurité des middlewares et des applications

Des références globales ...

- Casip Cojasor
- CASVP (Mairie de Paris)
- Institut Français du Pétrole
- Groupe Lucien Barrière
- Groupe Louvre Hôtel
- Louis Dreyfus
- ORANGE
- Oudot & Associés
- PARCS ENCHERES
- Prédica
- Saint Gobain...

Nos Coordonnées



 104, Boulevard Auguste Blanqui 75013 PARIS

 : 01 55 43 09 41

 : 01 55 43 09 21

contact@alyotechsecurity.fr