Christophe Auberger, CTO Fortinet – *3 août 2022*

1. **Expert**
   - 25 ans dans la cybersécurité.
   - CTO chez Fortinet.
   - Auparavant, a monté un MSSP (Managed Security Service Provider) en France.
   - Expériences précédentes dans l'univers réseau, toujours avec un côté sécurité.
   - 20 ans qu'il travaille avec Nomios et ses pairs. Connait très bien le CEO de Nomios.
2. **Description de la chaîne de valeur**
   - **Constructeurs** : Palo Alto, F5, Fortinet – nombre d'acteurs limité. Ont des forces commerciales dont le rôle est de faire de l'évangélisation et convaincre le client final d'acheter leurs produits + soit de trouver un intégrateur, soit ils conseillent eux-mêmes un intégrateur. Pas de vente directe au client final.
   - **Distributeurs** : assimilés à des grossistes. Importent les équipements, font les démarches nécessaires (car en matière de cybersécurité, certains équipements sont considérés comme des armes, par ex. tout ce qui concerne la partie chiffrement).
   - Les distributeurs revendent les équipements à des **intégrateurs** comme **Nomios, Orange Cyber Défense, Axians**. Les distributeurs proposent aussi parfois des services financiers auprès des intégrateurs.
   - L'intégrateur vend les produits au client final, en y ajoutant son propre service de sécurité.
   - Des acteurs comme Orange Cyber Défense ou solution de Bouygues (ComOne ?) prennent surtout des projets globaux (de même que les multi global integrators comme Capgemini ou NTT).
   - L'intégrateur est relativement agnostique par rapport au constructeur, veut vendre la meilleure solution pour une problématique donnée.
   - **L'intégrateur se limite à deux constructeurs en général.**
   - Le client final achète de l'intégration ou des services.
   - Marché divisé en 3 :
   - **TPE** : pas adressées en direct par les constructeurs, des intégrateurs dédiés travaillent dessus, importance d'avoir une présence locale.
   - **ETI/milieu de marché** : (c.500-3000 postes à équiper). Une partie est adressée par les constructeurs, de plus en plus, via des forces commerciales (« territories ») (mais pas de vente directe).
   - **Grands comptes** : forces dédiées chez les constructeurs, voire même un commercial peut avoir un seul compte.
3. **Relations entre les constructeurs et intégrateurs**
   - Soit le client est à l'initiative de la demande (a déjà choisi son produit / sa technologie) et fait un appel d'offre pour trouver un intégrateur capable d'intégrer cette technologie, souvent parmi les intégrateurs avec lesquels il est déjà en partenariat.
   - Soit, le client a déjà un intégrateur (cas des grands comptes) et s'adresse directement à celui-ci, moins de formalisme qu'un appel d'offre.
   - **Partenariat intégrateur / constructeur** :
   - 2 conditions déterminant la catégorie de l'intégrateur chez le constructeur (silver, gold, platinum, etc): (1) **engagement sur un volume d'affaires sur un an**, (2) engagement de **formation** et de **certification** des équipes de l'intégrateur.
   - Chez Fortinet : 400-500 partenaires au total.
   - Catégorie auto-rise : niveau le plus bas, l'intégrateur a le droit de vendre les produits du constructeur, a des remises assez basses, mais en contrepartie, pas d'engagement de volume d'affaires ni de certification.
   - Niveau Platinium (le plus élevé) : 6 partenaires chez Fortinet dont Nomios, OCD, Bouygues, Axians, Interdata ? Nécessite plusieurs dizaines d'ingénieurs à haut niveau chez l'intégrateur.

- Ces catégories bougent ensuite assez peu car cela nécessite des investissements assez importants, pas tant financièrement qu'en termes de formation des équipes. Marché relativement stable.
- **Nomios est au plus haut niveau avec Fortinet et Palo** Alto, donc n'aurait pas d'intérêt à aller avec un 3ème fournisseur : cela coûte cher sans donner de volume d'affaires supplémentaire.

- L'intégrateur va vouloir diversifier ses partenariats dans le cas de produits disruptifs ou technologies nouvelles : un intégrateur peut être qualifié uniquement sur la gamme de produits disruptive du fournisseur.
- Sur des marchés matures comme le firewall (essentiellement du renouvellement), pas d'intérêt pour l'intégrateur d'avoir une multitude de technos différentes.

4. **Remises**

- Un certain niveau de partenariat permet d'avoir un niveau de remise par défaut : entre 3-5% de remise supplémentaire d'un niveau à l'autre. Par exemple -55% de remise pour le niveau Platinium.
- Sur des projets importants ou structurants, si l'intégrateur a fait du travail en amont, connait le projet chez le client et a positionné le constructeur : cela tombe dans la catégorie **Prime**, 2 points de plus de remise.
- Dans le cas d'appels d'offre pour un client public : chacun dans la chaîne de valeur va faire un effort en termes de marge pour gagner le projet.

5. **Rôle des distributeurs**

- L'intégrateur achète au distributeur (grossiste). Ingram Micro, Exclusive Networks, Westcon.
- Relation constructeur/distributeur : les constructeurs ont des liens avec des distributeurs paneuropéens pour négocier des volumes d'achat, notamment dans le contexte actuel de tensions sur les équipements (objectif de limiter les délais d'approvisionnement).
- L'interlocuteur privilégié des constructeurs est l'intégrateur. **Le constructeur a une double force commerciale : directe (cible le client final) / « channel » (cible les intégrateurs).**

6. **Critères de sélection d'un intégrateur par un constructeur**

- **Compétence sur la solution**, notamment pour des solutions relativement récentes et un peu disruptives.
- **Le choix exprimé par le client final** : certains sont très attaché à certains intégrateurs et ne veulent pas travailler avec d'autres.
- La catégorie du **partenariat** : l'intégrateur est-il **prime** ou pas (a-t-il travaillé le projet en amont) ?
- La plupart des clients finaux travaillent déjà avec 2-3 intégrateurs donc le constructeur ne va pas imposer un 4ème intégrateur.

7. **Nomios**

- Partenaire de valeur.
- Très haut niveau de **technicité** à la fois au niveau commercial et technique. Important pour le constructeur.
- Gens **fiables**.
- Ont l'avantage de la **souplesse**, pas forcément le cas des gros comme Orange Cyberdefense ou l'intégrateur SFR. Volonté de traiter les projets de manière **efficace**.
- Un défaut, en train de se résorber : manque de capacité à aller traiter des **projets en dehors du territoire français**. Le rachat d'Infradata leur permet d'adresser des projets sur des périmètres plus importants. Mais ils n'ont pas le même niveau de capacité qu'Orange Cyberdéfense qui peut capitaliser sur la présence d'Orange, présent partout, parlent « d'usines à déploiement », y compris dans des pays compliqués (douanes/droits) comme le Brésil ou l'Inde.

8. **Tendances de marché**

- On constate un changement dans la manière dont les clients consomment la sécurité : avant, les clients achetaient de l'intégration.
- Désormais, en raison de la grosse pénurie de compétences cyber et du côté plus confortable : le client consomme le cyber sous forme de **services**. Plus confortable pour le RSSI car s'il achète du service managé, c'est le fournisseur porte l'engagement de service et pas lui.

- Aujourd'hui, le marché consiste encore beaucoup d'intégration, mais les courbes (avec les services managés) devraient se croiser d'ici 2-3 ans (estimation).
- **Les intégrateurs doivent se transformer pour aller vers la fourniture de services managés et doivent se positionner des offres plutôt sur mesure**. Peuvent profiter en cela d'un trou de marché :
  - La plupart des opérateurs (Orange Business Services, SFR, Bouygues Tel, NTT) ont déjà des services managés de sécurité, mais plutôt pour les **PME/TPE** car l'offre est très packagée, le service est consommé d'une certaine façon et pas une autre. Or, les grands groupes veulent pouvoir sélectionner parmi des offres. Les intégrateurs commencent à proposer cela, par ex. Nomios ou Pixit.
  - Certains acteurs type Atos, EADS, NTT proposent aussi des services managés de sécurité à des très grands groupes, très surmesure, mais on est plus proche de l'infogérance/du soft managé et le **coût est élevé**.
  - Donc il y a une vraie opportunité de marché pour les intégrateurs pour adresser ce segment avec des offres sur mesure, car ils ont les compétences, connaissent les clients et ont la souplesse pour le faire, alors qu'Atos etc. ont des coûts de structure trop importants, ne savent pas répondre à cela. Avoir un EDR managé chez un client avec 5-8k postes de travail n'est pas dans leur cible, leur coût serait hors marché.
- Ce shift vers les services amène les constructeurs à adapter leurs offres pour faire des **solutions multi-tenants** : l'intégrateur achète la solution et peut s'en servir avec plusieurs clients finaux, en étanchéité. Capacité de virtualiser des environnements sur des pare-feu.
- Impact **Covid** : n'a pas vraiment changé le business model mais a créé des opportunités. La cybersécurité a été l'un des rares marchés boostés par la crise sanitaire. Changement des mentalités.
  - « Work from anywhere » : capacité à pouvoir accéder aux apps de l'entreprise qui se trouvent partout, avec des équipements pas forcément maitrisés par l'entreprise.
  - A boosté la notion de **zero trust** : on valide à la fois l'identité numérique (partie fortement accélérée par cette crise) + l'équipement à partir duquel la personne se connecte. Modulation des accès.
- **Nomios est en ligne avec ses pairs sur ces tendances de marché-là**, sujets comme l'EDR, solutions d'authentification multi-facteur, ESSE (capacité à pouvoir connecter n'importe qui à n'importe quelle ressource sans déployer d'infrastructure lourde).

9. <u>Pénurie de talents</u>

- C'est avant tout un problème d'**attractivité de la filière** cybersécurité, même dans les écoles d'ingénieur assez techniques. Les étudiants croient qu'ils ne vont faire que du codage, ce qui n'est pas le cas.
- Aussi bien chez les intégrateurs que les constructeurs, l'alternance pourrait beaucoup aider. Les intégrateurs [français] ont plus de facilité à le faire car ancrés dans le tissu national, les sociétés américaines comme la sienne chez Fortinet ont plus de mal à mettre les budgets en face.
- Également manque cruel de profils féminins.
- Pour autant, ne constate **pas de baisse des compétences** aujourd'hui, le niveau de compétence est bon chez les intégrateurs. Les constructeurs n'ont pas baissé leur niveau de certification dans cet environnement. Le problème est plutôt sur l'acquisition de nouveaux talents. Constructeur : s'interdit d'aller recruter chez les intégrateurs, qui ont déjà du mal à recruter.
- Des constructeurs comme Fortinet, Palo Alto, F5 arrivent encore à recruter facilement. **Nomios a bonne presse également**. SFR a eu beaucoup de difficultés car problèmes d'image (plans sociaux fréquents).
- Pour autant cela pourrait ralentir la croissance à terme.
- Ce contexte a créé une **inflation forte sur les salaires**. Cela n'a pas forcément été un problème chez les acteurs qui sont uniquement intégrateur cyber, des acteurs comme Atos sont plus impactés.
- Augmentation des coûts de structure (salaires) + augmentation du coût des composants : tous les constructeurs cyber ont fait plusieurs **augmentations de prix** sur l'année. Une partie a été absorbée par la marge chez beaucoup de constructeurs, mais pas non plus 30-40%.
- Ils ont été amenés à renégocier des contrats avec certains clients, qui comprennent.

10. Contractualisation

- Assez rarement avec les clients finaux sauf si un contrat cadre a été signé.
- Les constructeurs s'engagent sinon sur un niveau de remise car trop risqué de s'engager sur un prix de cession, ce qui varie ensuite est le prix public des équipements ou solutions.
- Le taux de remise change si le partenaire change de catégorie, sinon ne change pas.

11. Critères que recherche un intégrateur chez un constructeur

- Une certaine **image** car l'intégrateur veut servir un client qui veut un certain produit. Importance de l'attractivité de la solution pour le client.
- De la **facilité de déploiement**, sinon on risque de dépasser les jours prévus au départ pour le déploiement (car le client est au forfait).
- La **marge** que l'intégrateur se fait sur le produit (niveau de remise consenti).
- **Aspects de maintenance** : coûts de maintenance, mécanismes de réassurance proposés par le constructeur. Les intégrateurs ont leur propre offre de maintenance mais peuvent se réassurer chez le constructeur.
  - Nomios achète ainsi des équipements et prend une maintenance basique de la part du constructeur : c'est donc lui en tant qu'intégrateur qui porte les services de maintenance, permet de générer une marge supplémentaire.
  - Coûts de maintenance : 20% du prix du produit dans la sécurité, vs. 5% sur la partie réseau.
  - A noter que des constructeurs qui sont entre sécurité et réseau comme Cisco ou HP ont donc des coûts de maintenance plus bas. Cela peut poser problème pour les constructeurs cyber (concurrence prix sur les coûts de maintenance).
- Sinon les prix des constructeurs sont sur des ordres de grandeur similaires, pas de constructeur beaucoup plus bas que les autres.