SÉCURITÉ

Falcon

UNE COMPOSANTE DE L'OFFRE DE SÉCURITÉ NUMÉRIQUE

La maîtrise de votre risque numérique à 360°

Pour répondre au besoin croissant de **sécurité numérique**, Cyllene déploie son offre de **CyberSécurité** dans une démarche globalisante selon quatre volets complémentaires, cohérents et opérationnels :

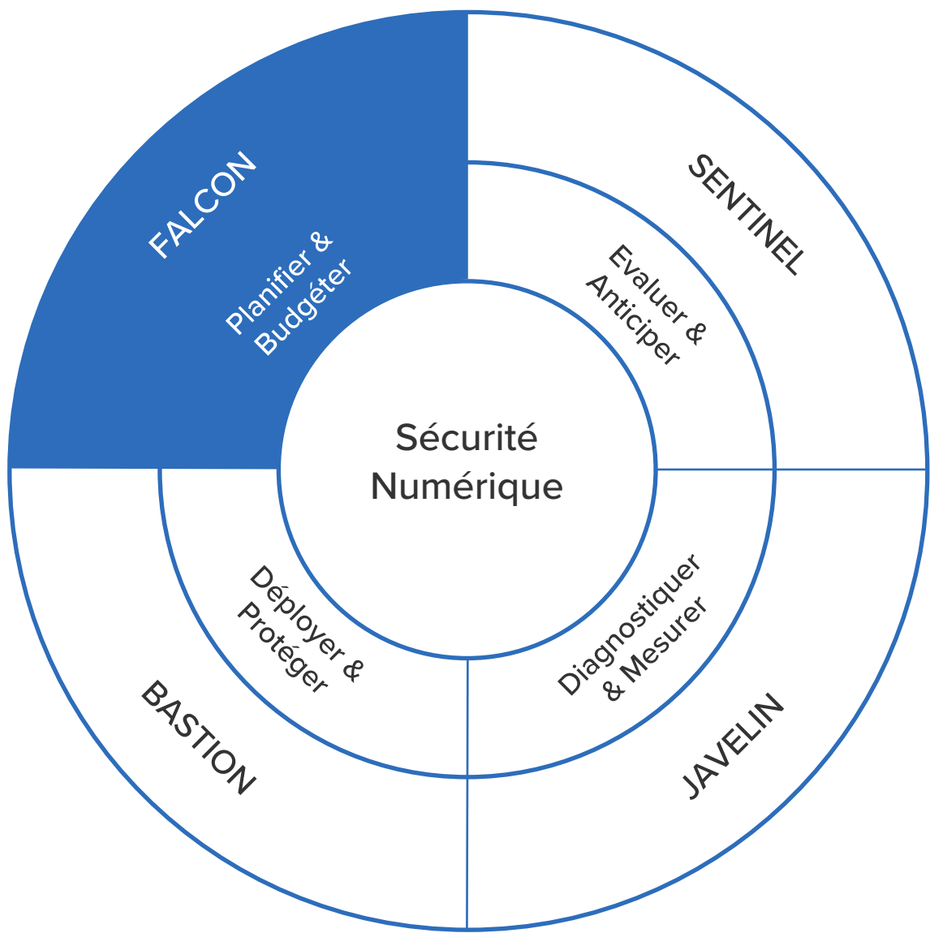
Falcon - Bastion - Sentinel - Javelin

La création de Valeur de l'Entreprise repose chaque jour d'avantage sur la maîtrise du numérique. Croissance exponentielle des volumes, nouveaux services web, travail nomade, valorisation stratégique des données grâce à l'IA et la blockchain, forte dynamique de l'écosystème IoT et complexité des interconnexions des SI sont autant d'enjeux et de facteurs d'opportunité ou de risque pour l'Entreprise.

L'offre de Sécurité Numérique est la réponse de Cyllene aux attentes des dirigeants pour planifier et organiser (**Falcon**), déployer et protéger (**Bastion**), diagnostiquer et mesurer (**Javelin**), évaluer et anticiper (**Sentinel**) tout en satisfaisant aux obligations réglementaires et aux exigences juridiques et assurantielles ; elle complète la démarche « **Security By Design** » déjà en vigueur au sein de toutes les autres offres du Groupe.

Dans une approche de **«Security Decision Making As-a-Service»**, Falcon propose un accompagnement dans le cadre d'une relation long terme avec des **experts** en cybersécurité, expérimentés, outillés et familiers des besoins et problématiques, au titre de leurs nombreuses missions pour diverses entreprises.

Falcon permet d'étendre le champ de vision du décideur sur l'ensemble de sa **Sécurité Numérique,** afin de structurer une politique de **cybersécurité.**



Analyse des risques

Identification des besoins organisationnels concernant les exigences en maintien de sécurité de l’information.
Réalisée via la méthode EBIOS conçue par l’ANSSI, l’analyse de risques est la composante essentielle à la mise en place d’un système de management de la sécurité de l’information.

Schéma directeur

Constitution d’un plan ou d’un programme de cybersécurité efficace à partir des composantes : enjeux, menaces, organisation , mesures de sécurité.
Les diverses études de cadrage et les plans de recommandation de solutions alimentent le schéma directeur qui doit être décliné sur les plans budgétaires et calendaires.

Plan de traitement

En fonction des risques retenus et des objectifs de sécurité de l’organisation, le traitement des risques va déboucher sur un plan et des recommandations de mesures détaillées, organisationnelles et techniques, ainsi que sur des préconisations de feuille de route opérationnelle pour leur mise en oeuvre.

Résilience

La réponse et la gestion des situations de crise sur incidents de sécurité sont réalisées à travers un programme d’accompagnement contextualisé comportant l’adaptation aux enjeux, la prise en compte des menaces et scénarios, la communication en mode crise; un cycle pluriannuel d’exercices, et l’élaboration et la mise à jour de fiches « Réflexes ».

Dashboard et kpi

La mise en oeuvre des mesures du plan de traitement doit s’accompagner de la mise en place et du maintien opérationnel d’indicateurs de performance destinés à en assurer le contrôle. La définition de KPI pertinents, adaptés au contexte de l’organisation et la constitution d’un tableau de bord orienté « métier » et «opérationnel» sont nécessaires.

Complémentarité des solutions

L’offre Falcon s’appuie autant que nécessaire sur Bastion qui vise à la mise en place d’une sécurité robuste et intégrée, sur Sentinel afin de disposer d’un temps de réaction optimal face aux menaces grâce à une veille permanente avancée et sur Javelin pour une évaluation des vulnérabilités et des surfaces d’attaque.

Envie d’aller plus loin ?

Un de **nos experts** sera ravi d’échanger avec vous pour mieux **comprendre votre besoin.**

Contact : contact@groupe-cyllene.com