SÉCURITÉ

Javelin

UNE COMPOSANTE DE L'OFFRE DE SÉCURITÉ NUMÉRIQUE

Evaluer ses vulnérabilités et sa surface d'attaque

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 :

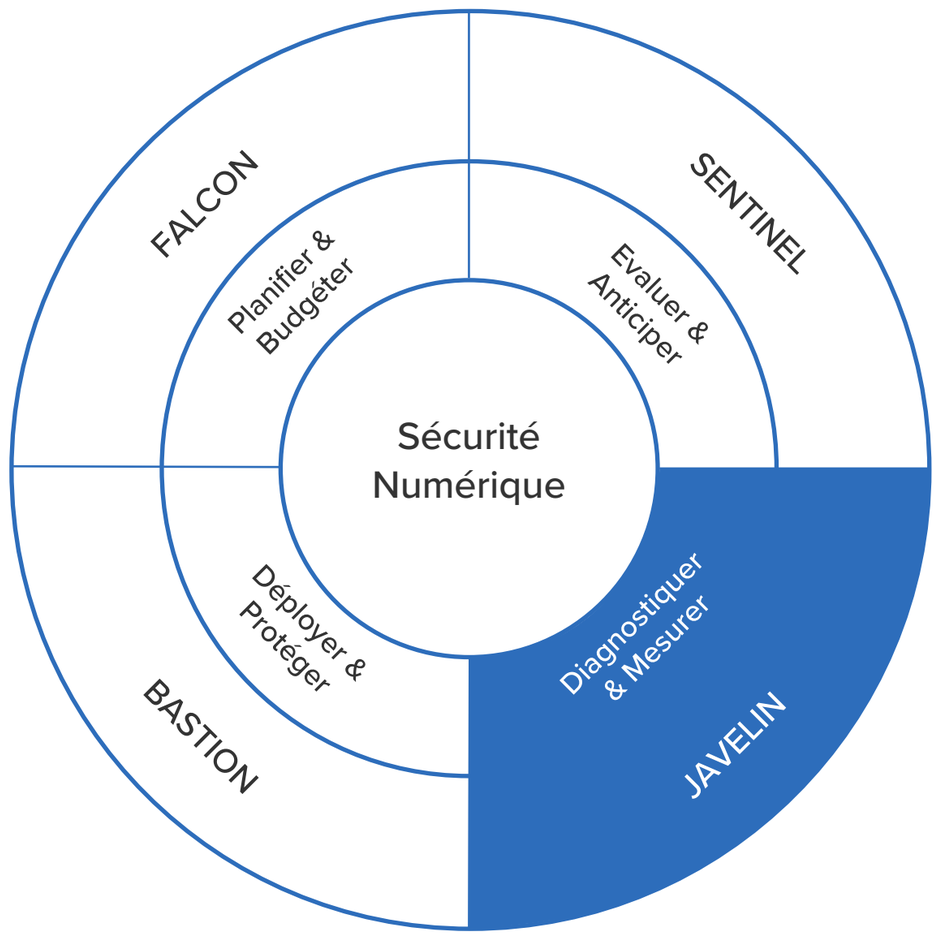
Falcon - Bastion - Sentinel - **Javelin**

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.

Javelin s'inscrit dans la démarche globale de maîtrise du risque de **cybersécurité** traduite sous la forme des offres Bastion et Sentinel.

On procédera principalement à des **audits** en amont (en appui d'une démarche de type Falcon afin de disposer d'un **diagnostic** initial fiable), ou en aval de la mise en place d'un dispositif afin d'évaluer les vulnérabilités résiduelles.



Pen Test

Réalisation de tests d’intrusion depuis l'intérieur ou l'extérieur du système d'informations audité afin d'y découvrir des vulnérabilités et de vérifier leur exploitabilité et leur impacts. L'auditeur se place alors comme attaquant potentiel en conditions réelles. Le Pen Test complète et améliore l’efficacité d'autres missions d'audit, ou démontre la faisabilité de l’exploitation des failles et vulnérabilités découvertes à des fins de sensibilisation.

Audit Organisationnel & Physique

L'audit porte sur la documentation sécurité et s'assure de :

- La conformité avec les besoins sécurité et les normes en vigueur
- L' adéquation aux mesures techniques mises en place
- La mise en pratique et la maintenance efficace

L’audit de sécurité physique se focalisera sur la sûreté des bâtiments, salles informatiques ou bureaux: contrôles d’accès, intrusion, vidéosurveillance…

Ingénierie Sociale/Phishing

Exploitation de vulnérabilités humaines ou liées à l'organisation de l'entité afin d'accéder à des informations confidentielles ou à certains actifs. La réalisation de tests d’ingénierie sociale via la mise en situation réelle, permet d’identifier les actions de sensibilisation à effectuer en priorité ainsi que les populations à cibler ou de vérifier l’efficacité d’une campagne.

Audit d'Architecture

Vérification de la conformité des pratiques de sécurité relatives au choix, au positionnement et à la mise en oeuvre des dispositifs matériels et logiciels déployés dans un système d’information, à l’état de l’art et aux exigences et règles internes de l’audité. L’audit peut être étendu aux interconnexions avec des réseaux tiers.

Audit de Configuration

Vérification de la mise en oeuvre de pratiques de sécurité conformes à l’état de l’art et aux exigences et règles internes de l’audité sur la configuration des dispositifs matériels et logiciels déployés dans un système d’information.

Red Team

Les tests d'intrusion Red Team évaluent les avoirs critiques d'une entreprise en mettant à l'épreuve ses différents moyens de protection, qu'ils soient physiques, humains, organisationnels et informatiques. Cette prestation se déroule en différentes phases et sur plusieurs semaines afin d’atteindre les objectifs désignés par la Direction.

Audit de systèmes industriels

Évaluation du niveau de sécurité d’un système industriel et des dispositifs de contrôle associés : audit d’architecture, un audit de la configuration des éléments composant l’architecture et audit organisationnel et physique.

Audit de Codes Source

Analyse de tout ou partie du code source ou des conditions de compilation d’une application afin d'y découvrir des vulnérabilités, dues à la programmation ou à des erreurs de logique et pouvant impacter la sécurité.

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