

SÉCURITÉ Sentinel

UNE COMPOSANTE DE L'OFFRE DE SÉCURITÉ NUMÉRIQUE

Réaliser une veille efficace pour mieux anticiper et réagir

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 :

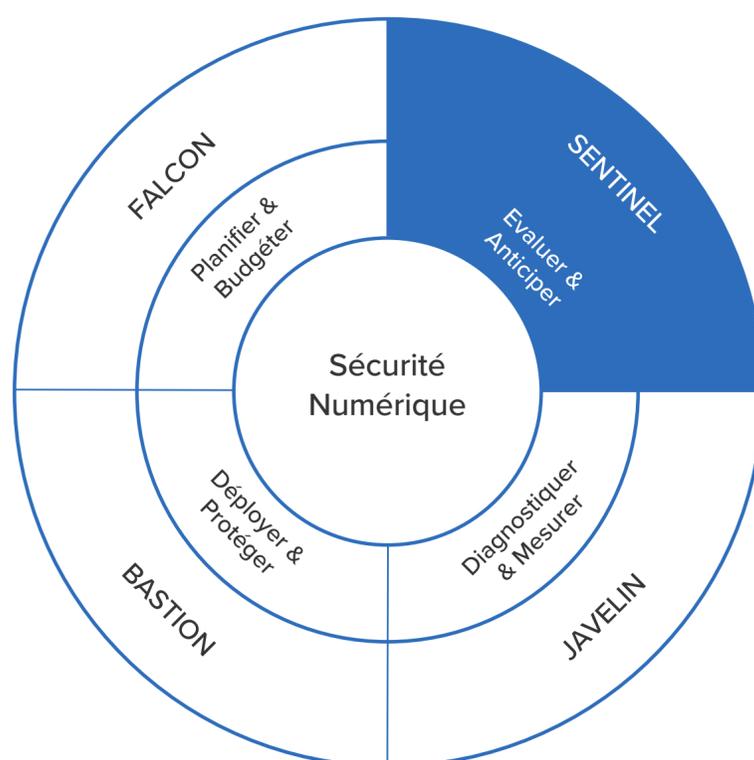
Falcon - Bastion - **Sentinel** - Javelin

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.

Puisqu'une protection totale est illusoire, la maîtrise du risque repose également sur la capacité à détecter et réagir vite face à un incident de sécurité.

Sentinel au travers de notre **SOC** et d'un SIEM assure à votre profit les tâches d'identification, de détection, de prévention, de réponse à incident en s'inscrivant dans les plus hauts **standards d'exigence de cybersécurité** tels que préconisés par l'ANSSI.





Soc

Un centre opérationnel de sécurité – SOC (Security Operations Center) – fournit des capacités centralisés et consolidées de prévention, de détection et de réponse aux incidents de cybersécurité. Nos spécialistes assurent la sécurité défensive au bénéfice des entreprises

Clientes: surveillance SSI, détection et analyse d'incidents de sécurité, investigations, reporting, amélioration continue, optimisations en matière de détection et veille SSI.



Veille

Le département Cyllene Cyber est chargé de la sécurité des Systèmes d'Information hébergés par Cyllene ou dans le Cloud. Afin d'entretenir la connaissance des menaces, Cyllene Cyber met en place les outils de surveillance, de contrôle et d'alerte adaptés.



Forensic

L'analyse forensique dans le domaine de la cybersécurité vise à comprendre les modalités d'une attaque par une analyse technique du Système d'Information. L'objectif de cette méthode d'investigation est de produire des preuves numériques de l'attaque cyber en vue d'une procédure judiciaire ou d'une action interne. Dès l'incident constaté, l'analyse forensique consiste à utiliser des outils et procédures spécifiques pour collecter les informations, analyser les données brutes et établir les conclusions.



Siem

Un SIEM (Gestion des informations et des événements de sécurité) désigne un ensemble de technologies de détection des cyber-menaces au sein d'un SOC. Ces technologies permettent l'analyse, la gestion et la corrélation de logs afin de mettre en exergue la potentialité de chaque menace. Le SIEM permet à nos experts une supervision poussée des systèmes surveillés, alliant expertise humaine et compétences en Machine Learning pour une cyber sécurité optimale.



Cyllene Lab

Le département Cyllene Cyber dispose d'un laboratoire permettant l'analyse de données et la réalisation de développements spécifiques et permettant de mener des tests en environnements réel, hors production.



Complémentarité des solutions

Sentinel est le complément naturel de notre offre Bastion qu'elle permet de faire évoluer dans la durée. Par l'actualisation de la connaissance des menaces, Sentinel nourrit également les offres Javelin dont elle permet de garantir la pertinence dans la durée.

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