



LA SOLUTION CAPSECUR

Solution SaaS éditée par Cap Atlantic Consulting

La
cybersécurité
opérationnelle



CONTEXTE, POSITIONNEMENT & SOLUTION

Constat

Les cyberattaques augmentent alors que les organisations restent insuffisamment préparées :

- Procédures de sauvegarde souvent incomplètes
- Plans de Sécurité de l'Information (PSI) peu formalisés
- Moins de 30 % des entreprises disposent d'un PCA
- Peu d'organisations testent régulièrement leur Plan de Reprise d'Activité
- Rares sont celles disposant d'un dispositif de gestion de crise structuré

Face à cette réalité, la cybersécurité ne peut plus être fragmentée ni uniquement réactive.

Notre réponse

CAPSECUR est un système agnostique et évolutif de sécurisation du Système d'Information, proposé sous forme d'abonnement, accessible à toutes tailles d'organisations.

L'objectif : atteindre un niveau de sécurité élevé et homogène, sans complexité excessive, de la TPE à la grande entreprise.

Une solution pensée pour les environnements critiques

- Technologies de l'Information (IT) & infrastructures classiques
- Systèmes industriels & Supervision, Contrôle et Acquisition de Données (SCADA)
- Systèmes embarqués & IoT
- Environnements multi-sites & sensibles

Une approche globale de la cybersécurité

CAPSECUR couvre l'ensemble du cycle de sécurité :

1. Sécurisation du système d'information
 - Application des meilleures pratiques de sécurité
 - Capitalisation continue des incidents et investigations
2. Stockage & archivage
 - Organisation et sécurisation des ressources de stockage
 - Mise en place de règles d'archivage adaptées aux obligations de conservation
3. Plan de Reprise d'Activité (PRA)
 - Identification des processus opérationnels critiques
 - Tests du PRA deux fois par an avec simulation de perte totale de données
4. Évolution continue
 - Veille et mises à jour mensuelles des logiciels intégrées à l'offre

Une plateforme unique

CAPSECUR centralise :

- Les audits et analyses de sécurité
- La surveillance en temps réel
- La détection et la réponse aux incidents
- Les rapports d'audit et de supervision

Le tout piloté depuis une plateforme unifiée.

SERVICES, MODULES & VALEUR AJOUTÉE

Détection & surveillance en temps réel – EDR (Détection et Réponse sur les Terminals) CAPSECUR

Après audit et validation de l'état de sécurité, CAPSECUR assure la protection continue des environnements critiques grâce à :

- Des agents déployés sur les équipements et automates
- Un serveur central intégrant :
 - Machine Learning
 - Référentiels de vulnérabilités
 - Intelligence artificielle adaptative selon les secteurs d'activité

Les référentiels utilisés reposent sur :

- Les bases CVE internationales (Vulnérabilités et Expositions Communes)
- Des référentiels d'alertes institutionnels
- La capitalisation des recherches et incidents clients CAPSECUR

Pentests & audits intégrés

CAPSECUR permet de réaliser des audits ponctuels ou réguliers :

- Tests d'infrastructure (routeurs, firewalls/Pare-feu, OS...)
- Tests applicatifs web
- Scans réseau Outil d'analyse des vulnérabilités (OpenVAS), Bloc de Messages Serveur (SMB), Shell Sécurisé (SSH), Protocole de Transfert de Fichiers (FTP), bases de donnée.
- Analyses de vulnérabilités et dénis de service

Le client peut auditer son SI (Système d'Information) à tout moment, avec traçabilité et autorisation formelle.

Module LAB – Entraînement & validation

CAPSECUR intègre un laboratoire cybersécurité structuré autour de 3 environnements :

- Plus de 250 outils d'audit et d'analyse
- Des dizaines d'applications volontairement vulnérables
- Des Systèmes d'Exploitation (OS) et services variés

Objectifs :

- Tester les capacités de détection et de défense
- Valider les mécanismes d'auto-apprentissage
- Former les équipes internes et clients sur des environnements réels

Module Reflex One – Capitalisation des compétences

Un module e-learning complète la plateforme pour :

- Renforcer la maîtrise des bonnes pratiques cybersécurité
- Mettre à disposition des contenus de formation en accès libre
- Capitaliser la connaissance sur la durée

Les rapports

CAPSECUR génère des rapports exploitables :

- Rapports d'audit
- Rapports de supervision en temps réel

En cas d'incident, ils servent :

- À l'analyse
- À la constitution de preuves
- Au dépôt de plainte si nécessaire

Notre valeur ajoutée

- Une offre de haute sécurité, simplifiée, packagée et accessible
- 18 ans d'expertise en cybersécurité des SI
- Protection comportementale (non statique)
- IA, Machine Learning (Apprentissage Automatique) et Big Data intégrés
- Capitalisation continue des attaques et vulnérabilités
- Approche complète : logiciel, expertise et infrastructure

Une offre packagée, simple et accessible

- Solution SaaS par abonnement
- Services intégrés à la plateforme
- Adaptée aux contraintes budgétaires et opérationnelles
- Évolutive selon vos besoins

CONTACTEZ-NOUS



5 Villa Houssay, 92200 Neuilly-sur-Seine



contact@cap-atlantic.com



+33 1 46 37 37 40



www.capsecur.eu | www.cap-atlantic.com



Solution référencée UGAP – Marché multi-éditeur SCC