

Devensys Cybersecurity est un **pure-player en cybersécurité**,
Projet lancé à Montpellier il y a **plus de 10 ans** par trois ingénieurs.

L'actionnariat est **100% français**, composé des fondateurs et de salariés.
Les équipes sont toutes basées en France, **zéro sous-traitance**.

Politique de **rémunération commerciale 100% au fixe**, 0% de variable.

Nos valeurs : **Expertise · Qualité · Ethique**



5 M€
CA 2021



35
Collaborateurs



22+
Experts certifiés



150
Clients actifs



+45%
Croissance/an



Une approche certifiante

Nos **nombreuses certifications** démontrent nos capacités à vous fournir des prestations réalisées selon les règles de l'art. Dans des domaines en perpétuelle évolution, nos équipes se forment en continu pour proposer un **service de haute qualité**.

- Equipe de direction experte en cyber
- Habilitation **secret** (défense, OTAN)
- **Formateurs** ISC² CISSP & EC-Council
- **DU Cybercriminalité**
- Ex-service de renseignements français
- Ex-force de l'ordre français
- Certifications ITIL



Ils font appel à nos services



LES OFFRES DE SERVICES

Consulting

Red Team & Pentest

Audit

Conseil

Analyse de risques

Sensibilisation utilisateurs

Formations

MCO

- Support et conseil illimités
- Maintenance préventive
- Maintenance évolutive
- Maintenance curative
- Rapports
- SLA

Starter-SOC

- Périmètre mono-solution
- Contrat MCO inclus
- SIEM/SOAR limité
- Détection des intrusions
- Intervention sur intrusion
- Equipe SOC Analyst

SOC 24/7 – SLA 30min

- Périmètre global
- SIEM/SOAR complet
- Détection des intrusions
- Corrélation et Enrichissement
- Intervention sur intrusion
- Equipe SOC Analyst
- Rapport personnalisés
- Support et conseil illimités
- CSIRT (Forensic)

Expertises

SECURE-NETWORK

Firewall, segmentation, VPN, NAC, SASE, WAF

SECURE-IDENTIY

Auth, SSO, MFA, passwordless, gestion MDP, PKI & HSM, Bastion d'admin

SECURE-COLLAB

Antispam, DMARC, CASB, chiffrement, classification

SECURE-ENDPOINT

EPP&EDR, Endpoint Privilege MDM, chiffrement

Première partie du Workshop Microsoft Sentinel

Prise de contact :

- Présentation des interlocuteurs
- Présentation de la démarche
- Les attentes
- Présentation de l'agenda

Récupération des informations essentielles au Workshop Microsoft Sentinel

Réunion de lancement :

- Les engagements de la procédure
- Les outils nécessaires
- Les attentes
- Les étapes

Définition du périmètre de déploiement : création d'un document de déploiement

Gestion du changement (si nécessaire) : le client doit suivre son processus de gestion des modifications et obtenir l'approbation des modifications de configuration conformément au périmètre défini.

Configuration :

- Configuration des licences d'évaluation
- Configuration des outils nécessaires

Finalisation de l'installation de Microsoft Sentinel

Phase de lancement

Intégration

Récupération des données (3 semaines) avec gestion des incidents par le SOC Devensys Cybersecurity

Deuxième partie du Workshop Microsoft Sentinel

Réunion de présentation des résultats :

- Présentation et discussions autour des résultats
- Les prochaines étapes

Besoins Client :

- Les solutions de sécurité Microsoft nécessaires
- Les budgets nécessaires

Démonstration des solutions de sécurité Microsoft

Les prochaines étapes de la sécurisation du SI Client

Décommissionnement :

- Effacer les logs récupérés
- Effacer les changements de configuration effectués
- Désactiver les licences d'évaluation
- Managed Detection and Response (MDR) transition

Journée de restitution

Décommissionnement