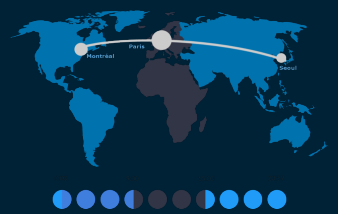
Focus sur le SOC Formind

SOC

- Intégration simple & rapide: moins de 3 mois avant le RUN
- Transparence, pas de souche propriétaire
- Amélioration continue au cœur de la relation client
- SOC 24/7



Éditeur référencé UGAP-SCC

EDR & NDR Managé	**Première brique d'un SOC.** **Mise en place de scénarios dédiés sur les endpoints et pilotage de la détection.**
XDR Plateforme	**Détection sur l'ensemble des assets sortant du modèle « corrélation de log » pour aller vers un orchestrateur d'alertes**
SOC Business (SIEM & DLP)	**Surveiller les actifs les plus critiques – Logs applicatifs** **Intégration de DLP pour lutter contre la fuite d'informations**
Cloud Managé	**Piloter la sécurité des environnements Cloud (Oracle, GCP, AWS,…)**
Industriel	**SOC OT : déployer la surveillance sur les actifs industriels pour garantir la production**

Partenaires technologiques

EDR	MS Defender, HarfangLab, CrowdStrike, SentinelOne
NDR	ExtraHop (Rise Above the Noise.), Darktrace, Custocy
SIEM	Azure Sentinel, elastic
Vuln.	Pentera, Armis, cyberwatch, hackuity
Autres	SECKIOT, pradeo

Focus sur les activités du VOC

Le VOC est un service dont les objectifs sont d'anticiper et de prévenir les cyberattaques grâce à un catalogue de service fournissant une vision éclairée de l'empreinte et du contexte numérique

VOC

- Comprendre les cybers menace et leurs modes opératoires.
- Avoir une carte d'identité de sa surface d'exposition et de son Shadow IT
- Détecter les attaques et enrichir les incidents pour réagir de façon plus pertinente

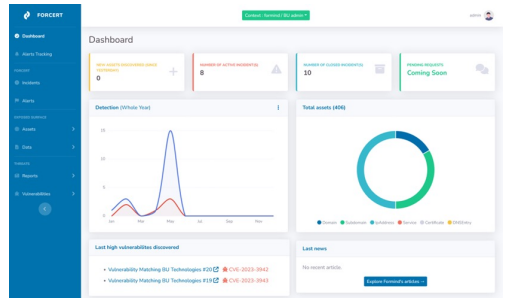
Veille	**Informer des vulnérabilités, des attaques et expliquer les tactiques, techniques et procédures. Analyser le contexte cyber d'une société sous un autre prisme : géographie, politique, secteur d'activité, …**
OSINT	**Analyser la surface d'exposition pour sécuriser les entreprises avant que les failles ne soient exploitées et aider à l'évaluation des risques liés aux tiers.**
CTI	**Identifier les infrastructures des attaquants, comprendre leurs évolutions et produire des rapports CTI**
ForCERT	**Mettre à disposition une plateforme centrale de gestion des services SOC-CERT Formind, des incidents et des activités de sécurité opérationnelles.**
Formation	**Formation sur les thématiques de Veille, d'OSINT et de découverte d'infrastructure CTI.**

Au cœur des contraintes normatives et régaliennes

ISO27001 — Programme CaRE — NIS2

LPM — TIBER EU/FR & TLPT — DORA

Un portail unifié



Focus sur les activités de la FIR

La **F**orce d'**I**ntervention **R**apide est une équipe d'experts en réponse à incidents mobilisable au besoin dont l'objectif est de contenir une cyber-attaque et de limiter l'impact business de nos clients

FIR

- Accompagne les équipes opérationnelles à monter en compétences.
- Contenir, éradiquer, remédier à un incident de cybersécurité.

Réponse à incident

Intervention en cas d'incident cyber avéré avec assistance à la réponse à incident et réalisation d'investigation numérique.

Sanity Check

Réalisation d'une analyse approfondie du système d'information à la recherche de comportement suspect ou d'une compromission.

Procédure

Mise en place de procédure de réponse à incident et de fiches réflexe à destination des équipes opérationnelles.

Exercice

Réalisation de simulation d'attaque et de crise cyber pour aider les équipes opérationnelles à appréhender un cyber incident.

Formation

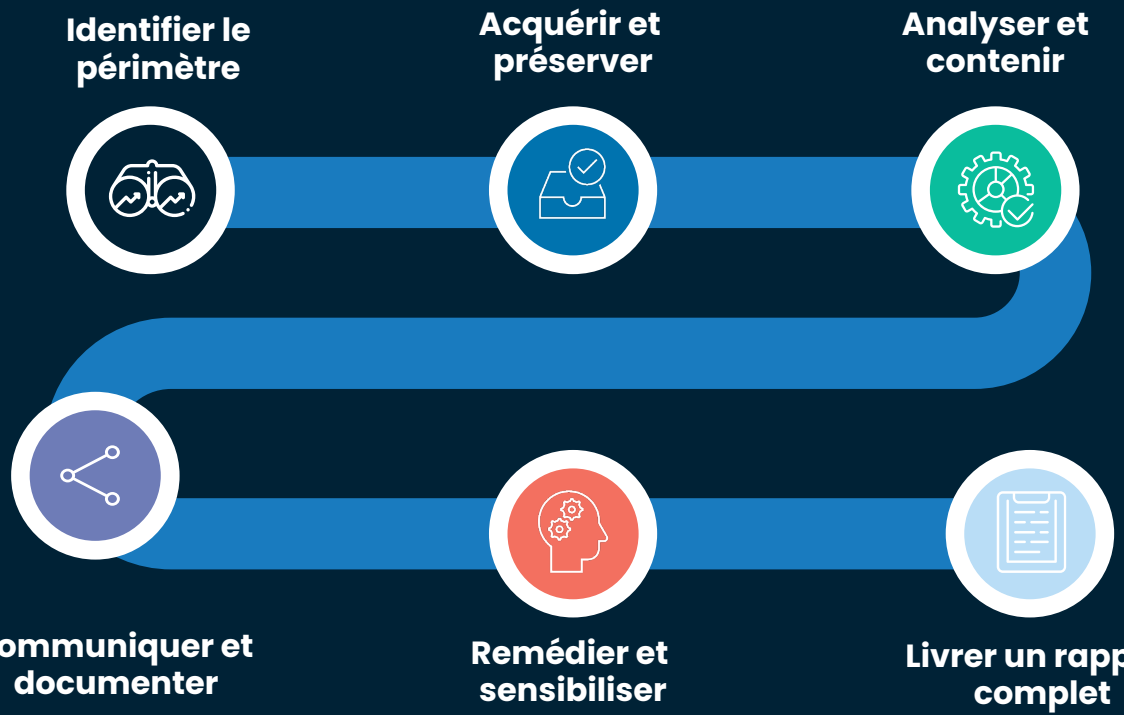
Formation sur les thématiques de détection, de réponse à incident et investigation numérique.

Les typologies d'incidents rencontrés

Une équipe pluridisciplinaire

Une équipe d'experts en réponse à incident mobilisable en 24/7

Déjà qualifié PASSI, Formind est officiellement en cours de qualification PRIS (Prestataire de Réponse à Incident de Sécurité) auprès de l'ANSSI et vise une qualification sur S2 2025.



3 niveaux de service

As a Rescue — Appelez-nous en cas d'incidents !

As a Service — Garantie prise en charge et intervention (4h max)

\+ Éditeur référencé UGAP-SCC

As a Service Premium — Astreinte 24/7

En cas d'incident de sécurité : fir@formind.fr – 01 81 89 30 02