



PRÉSENTATION FORMIND

SERVICES MANAGÉS DE DÉTECTION & RÉPONSE AUX INCIDENTS DE SÉCURITÉ



Qui sommes-nous ?

CARTE D'IDENTITÉ

“ Notre conviction : la sécurité est un levier majeur de performance des entreprises ”



Une identité affirmée

- 🇫🇷 Société française et indépendante
- 🔗 Pure player du conseil et de l'intégration en cybersécurité
- 👥 300 clients issus de multiples secteurs d'activité

Un développement structuré



2010

Création de Formind



2017

Implantation à Rennes et Casablanca



2019

Qualification PASSI et implantation à Lyon



2022

Certification ISO 27001, outillage de nos offres

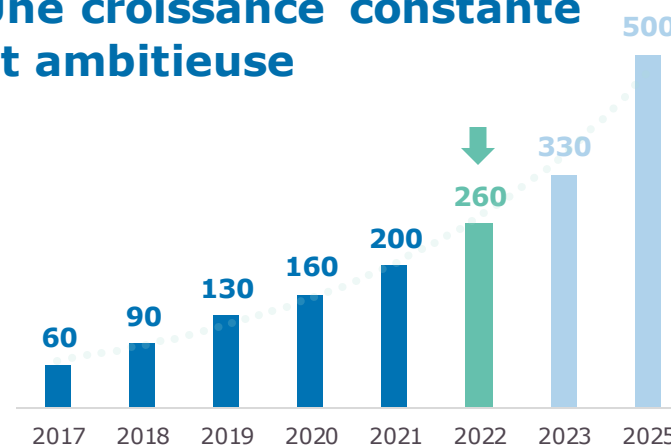


ACADEMY

2021

Implantation en Espagne et au Canada, Lancement de la Formind Academy

Une croissance constante et ambitieuse



Nos bureaux

9
VILLES

4
PAYS



Des valeurs fortes

Engagement
Bienveillance
Excellence
En mouvement

Ecoute

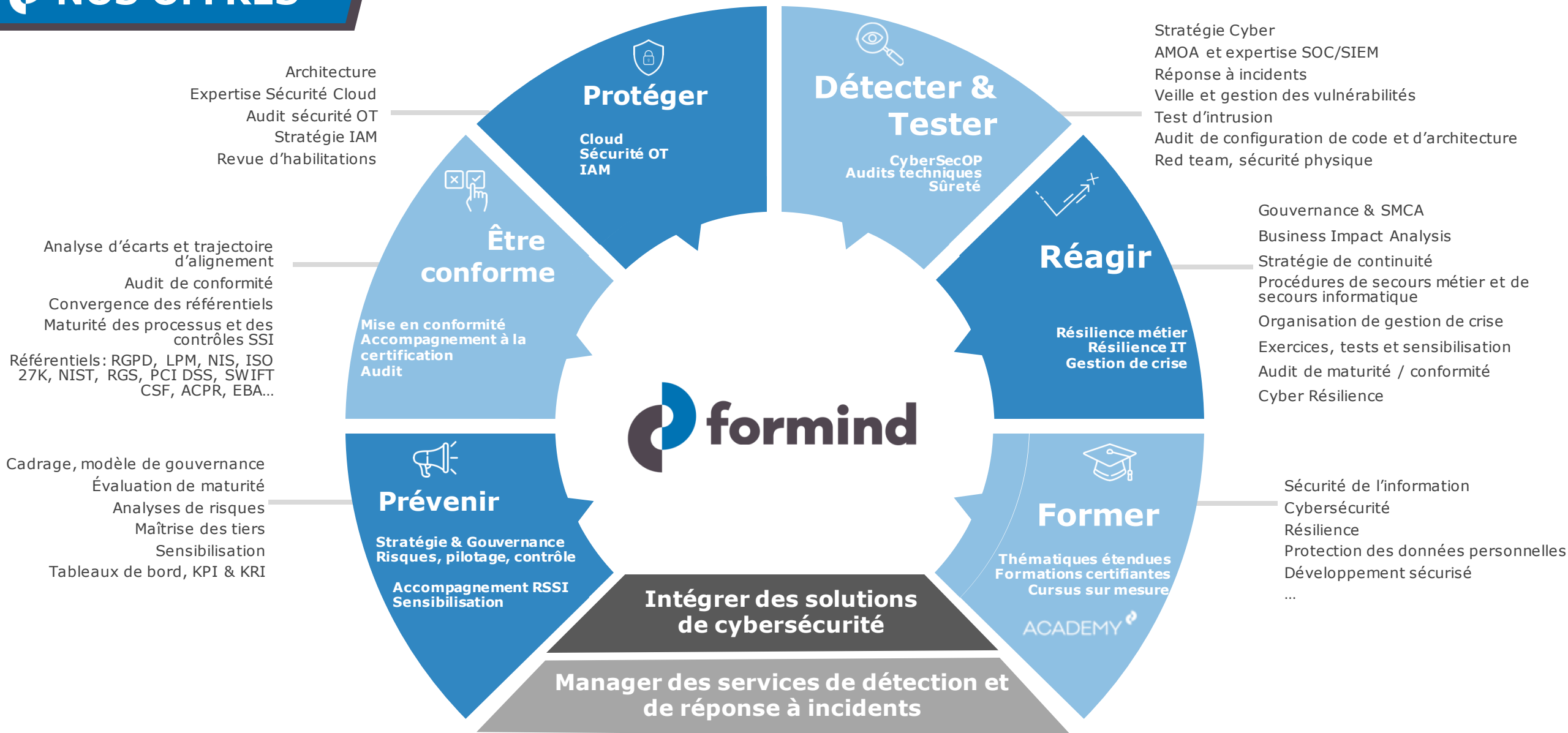


PÔLE D'EXCELLENCE
CYBER



Qualiopi
processus certifié





ILS NOUS FONT CONFIANCE !

Banque et assurance



Energie



Mobilité



Retail



Industrie



Santé



Services



Télécoms



Construction



Médias et divertissement



Luxe



Public





Notre vision de la Sécurité Opérationnelle

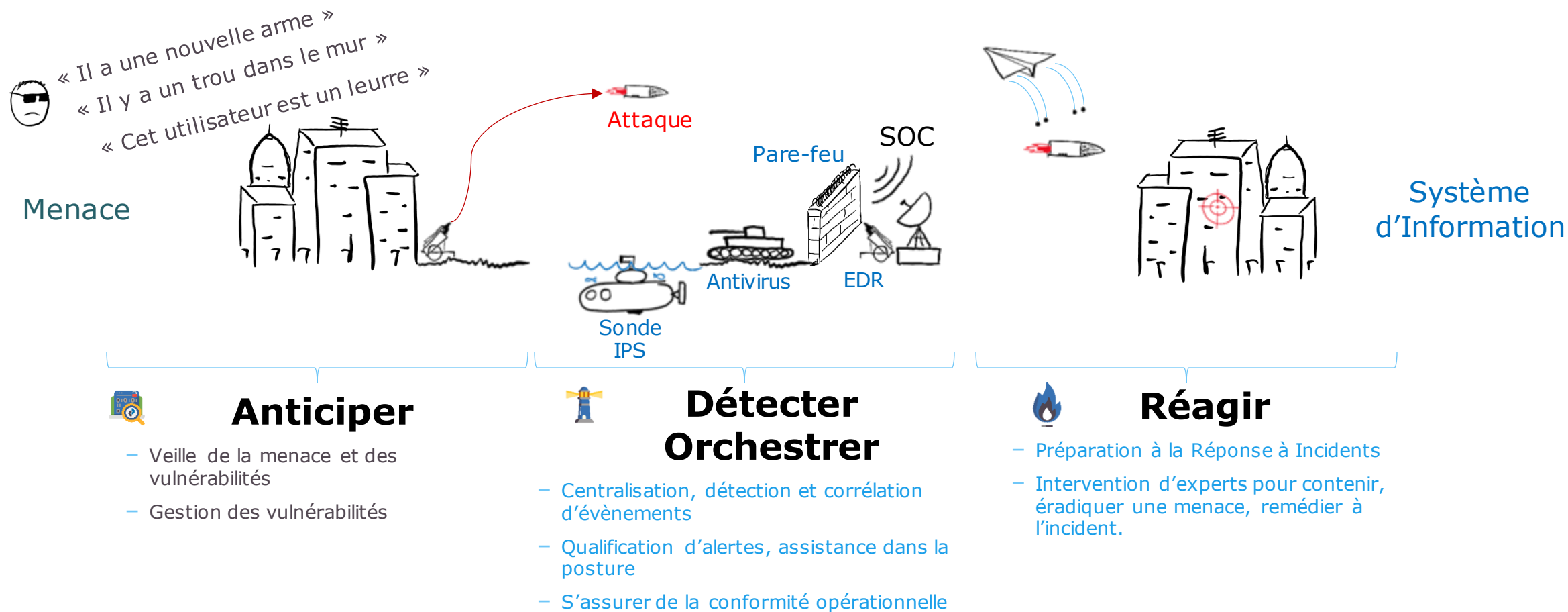


Notre vision de la gestion des incidents de sécurité

Notre offre : 3 piliers

Notre ambition

Être un **partenaire de confiance** dans la gestion des menaces et des incidents de cybersécurité, pour permettre à nos clients de se concentrer sur l'activité business





« **Véritable cockpit de la sécurité d'une entreprise, la cellule de détection alerte des intrusions avant que les dégâts ne soient irréversibles** »

Notre constat sur les solutions du marché

- La sécurité opérationnelle est souvent priorisée **a posteriori d'un incident** grave,
- Mettre en place une cellule de détection de zéro en interne est souvent **très complexe**
- Les prestataires gardent leur propriété intellectuelle **sans faire progresser** la maturité de leur client



Notre service et proposition de valeur



Une équipe de **50 experts** en détection et analyse d'événements de sécurité



Un **accompagnement du client de bout en bout**, pour le faire monter en maturité, fruit de notre ADN de conseil.



Un **service d'infogérance et de MCO** d'outils de détection qui restent propriété du client

PASSI

Prestataire d'audit PASSI

- Formind est **qualifié depuis Janvier 2019** par l'ANSSI
- Formind vise également la qualification **PASSI LPM**
- Différents types de prestations qualifiées:
 - Responsable d'audit
 - Audit de configuration
 - Audit de code
 - Audit d'architecture
 - Test d'intrusion



PRIS

Objectif de qualification 2024

- PRIS est la qualification de réponse à incidents de l'ANSSI, dont l'importance stratégique est soulignée dans votre expression de besoins.
- Formind a initié ses activités de réponse à incident (la **Force d'Intervention Rapide** ou FIR) en 2021 en suivant les directives de **PRISv1**.
- Types de prestations PRIS envisagées:
 - Investigation à large périmètre (ILP)
 - Investigation à périmètre restreint (IPR)
 - Recherche de Compromission (REC)

Formind travaille également en tant que partenaire de l'ANSSI pour des programmes tels que France Relance et Parcours Cyber.



Formind en quelques mots

Notre écosystème de partenaires

Les partenariats permettent de justifier d'une expertise reconnue et éprouvée de solutions de protection et de détection avec les acteurs les plus influents du secteur cyber



L'équipe partenariat



Managers de partenariat

Points de contact privilégiés des éditeurs, ils assurent un lien étroit entre vous et votre solution



Experts Solution

Ils interviennent ponctuellement en support et apportent une forte valeur ajoutée sur des thématiques/outils précis



Intégrateurs

Ils effectuent les manipulations sur les outils et réalisent les tests et corrections



Analystes

En phase de RUN, ils opèrent vos solutions avec une expertise opérationnelle de l'outil et du métier SOC



Des best of breed locaux...



EDR



Vulnérabilité



Sondes



GRC



Bastion



Identités



IAM

retarus:

Résilience

Formind membre de
HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY



...aux leaders reconnus



8 certifiés



20 certifiés



5 certifiés



5 certifiés



2 certifiés



5 certifiés



3 certifiés



5 certifiés



10 certifiés



2 certifiés

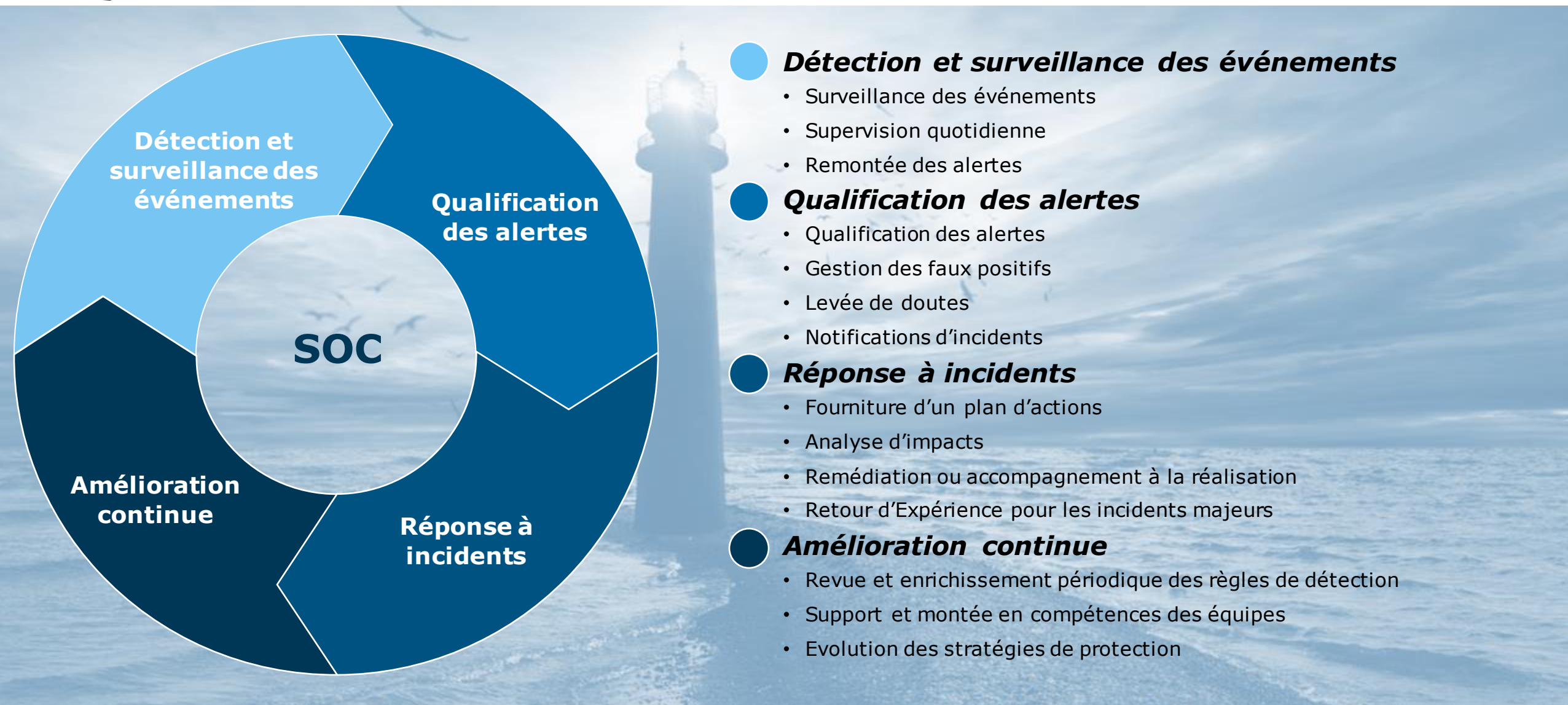


5 certifiés

NB: plusieurs consultants sont également en cours de certification et ne sont pas comptabilisés à ce stade



Le SOC Formind





Services proposés : Détection des incidents de sécurité – le SOC

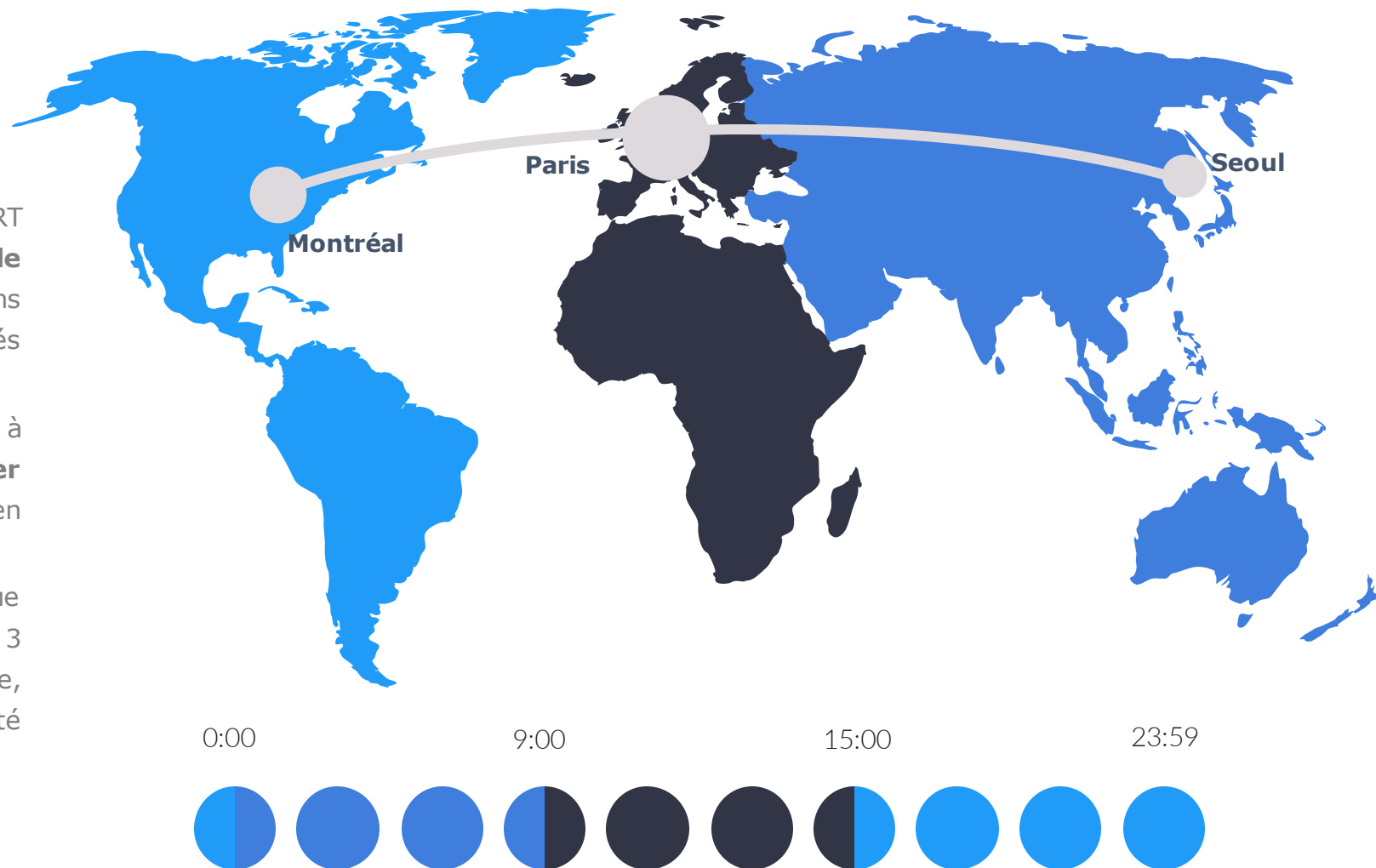
SOC and CERT : an international team

50 experts blue-team À votre service 24-7

Lancés en 2017, les services SOC et CERT sont composés de **passionnés de technologie** qui travaillent ensemble dans la gestion des incidents et des vulnérabilités et les réponses aux incidents.

Partout dans le monde, nous continuons à renforcer nos capacités en faisant **certifier** nos analystes (SANS, Microsoft...) et en augmentant nos activités de 80% en 2022.

C'est l'activité **Follow-the-Sun** : chaque fuseau horaire est régi par l'un de nos 3 bureaux ; à chaque heure de la journée, quelqu'un s'occupe de votre sécurité pendant la journée.





Notre vision de la gestion des incidents de sécurité
Construire un service centralisé

Notre ambition

Être un **partenaire de confiance** dans la gestion des menaces et des incidents de cybersécurité et valoriser vos produits afin de vous concentrer sur votre activité business



**Dispositif innovant,
résultats à l'état de
l'art**

Nos différenciants :

- ✓ **Intégration simple & rapide:** moins de 2 mois avant le RUN
- ✓ **Transparence.** Pas de savoir propriétaire
- ✓ **Amélioration continue** au cœur de la relation client

« XDR »



SIEM

- Mise en place de l'architecture de collecte
- Gestion du SIEM
- Amélioration continue



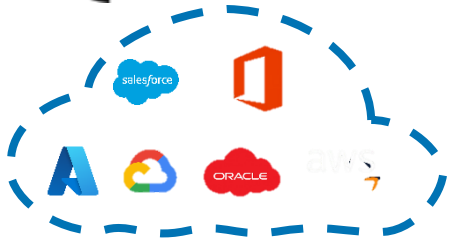
MDR et Vuln

- Intégration des composants (MDE, MDO, MDI, Vuln mgmt)
- Hunting & remédiation

**Centre de détection géré par nos experts cybersécurité
pour vous alerter en temps réel 24/7**



Construire un service managé avec FORMIND



*Infonuagique : Office365,
AWS/Azure/GCP, Salesforce...*



*Infrastructure : réseaux/pare-feux,
commutateurs, web, mandataires...*



*Donnée métier critique : ERP,
PLM, CRM, CMAO...*



*Annuaire & Messagerie : AD,
Exchange...*



Serveurs Windows, Linux...



Postes utilisateurs, PC, Mac...

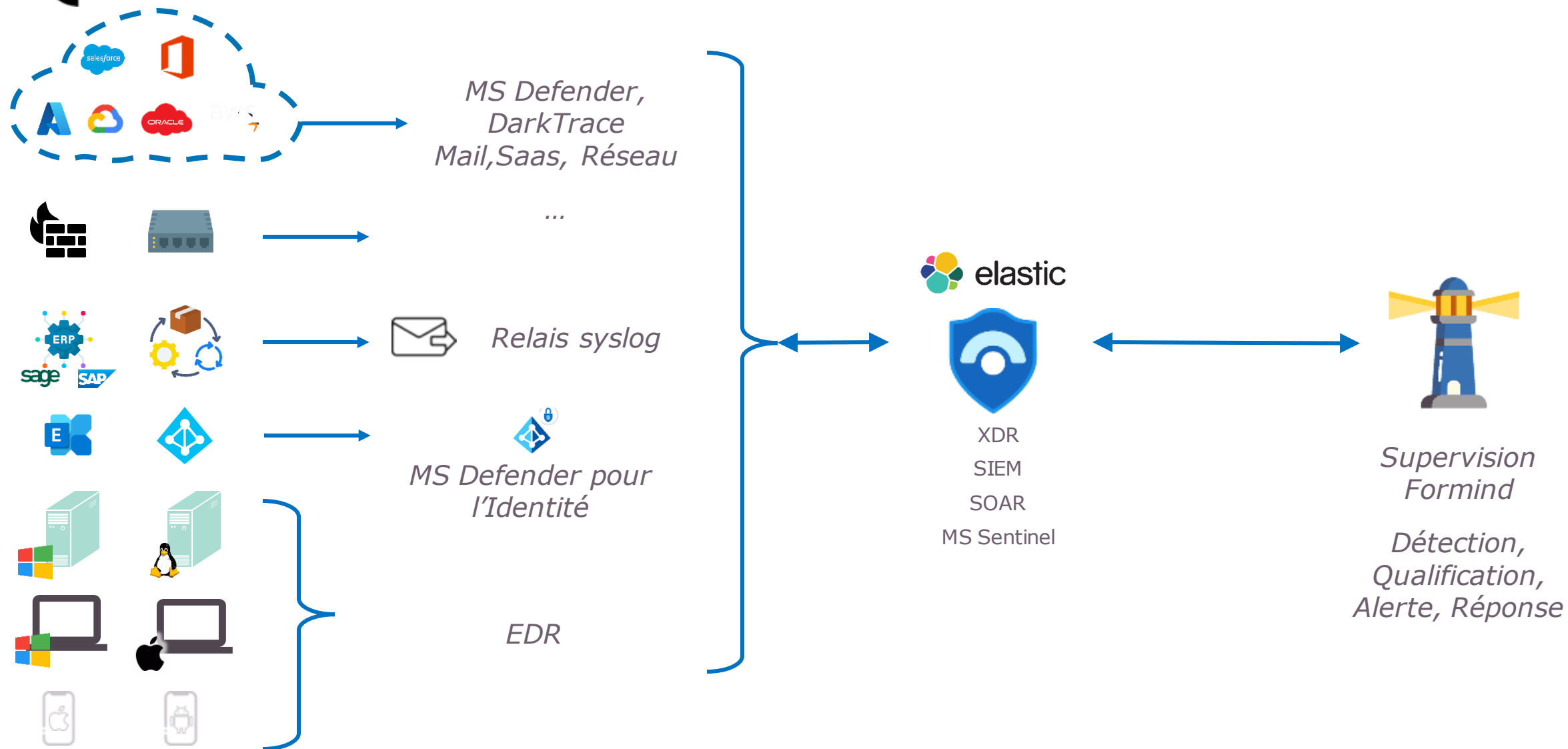


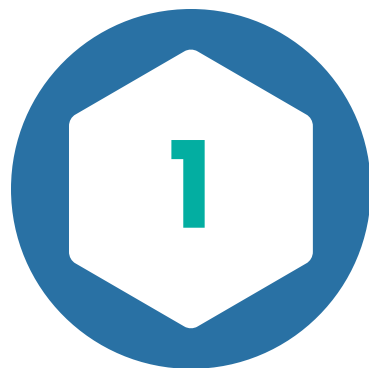
Ordiphones : iOS, Android

**Votre système d'information
est un ensemble de
technologies riches
d'informations de sécurité
devant être orchestrées...**



Construire un service managé avec FORMIND





Cadrage Design

- Définition de la stratégie de détection (règles et criticité des assets)
- Mise en place de la gouvernance projet
- Première itération des documents (procédures de déploiement) et architecture
- Identification des modes de communication et processus de gestion des incidents



BUILD

- Intégration des agents & modules, installation des sondes et forwarder
- Mise en place des transferts de logs vers le SOC FMD
- Ajout des règles de réponse automatique



Recette

- VABF (Simulation d'attaque, test fonctionnel de règles, bascules)
- VSR (1 mois)

T0+2 mois



RUN

- Gestion des incidents : levée de doute, qualification, alerting, plan d'actions
- Amélioration continue : [Points toutes les semaines de 30 min.](#)
- Comité de pilotage



Force d'Intervention Rapide



En cas d'incident cyber :
Force d'Intervention Rapide
01 81 89 30 02 /
fir@formind.fr



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 attaque SSI et de limiter l'impact business de nos clients



De l'identification du périmètre impacté à la mise en place des solutions de remédiation, des profils d'experts à disposition :





Force d'Intervention Rapide

Déroulement type



- Mise en place des **actions d'endiguement**
- **Eradication des persistances**
- Identification des **actions pour le retour à la normale**

- **Identification** du périmètre
- **Acquisition** des données
- **Analyse des données**
- **Partage des résultats d'investigation**

Prise en compte du contexte : capacités de réaction, processus de crise, éléments métier...



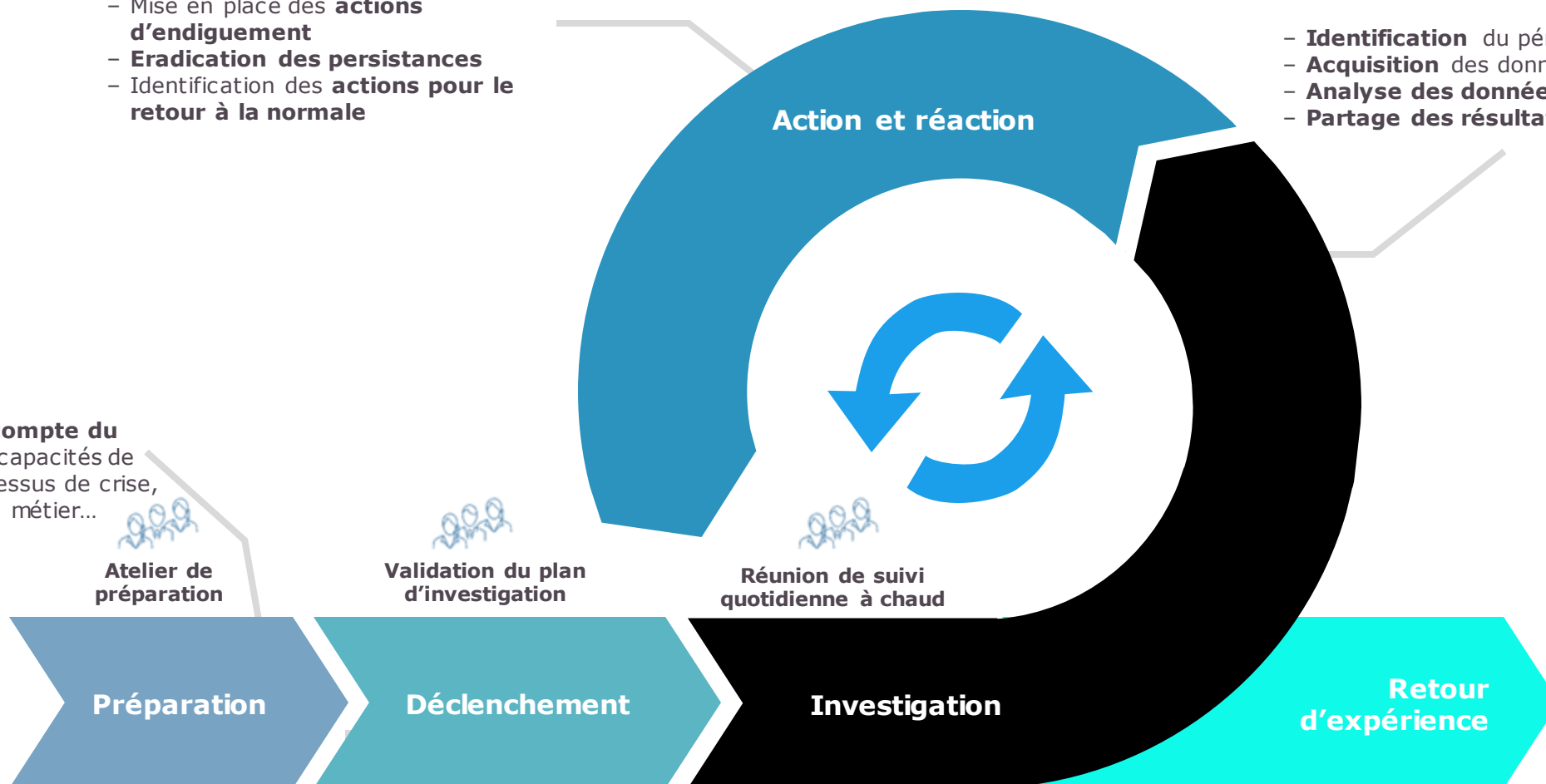
Atelier de préparation



Validation du plan d'investigation



Réunion de suivi quotidienne à chaud



Client direct
SOC Formind

- **Qualification** de l'incident
- **Définition** de l'équipe et estimation du temps d'intervention
- **Lancement** des premières actions d'endiguement

- **Présentation** du rapport d'incident
- **Retour d'expérience**
- Identification des **actions d'amélioration**



CERT – cellule de veille



Présentation du service de Threat Intelligence

Un arsenal de renseignement technique...

Renseignement sur la menace (CTI)

- Indicateurs de compromission (IOC)
- Indicateurs d'attaque (IOA)
- Renseignement sur les menaces actuelles

Renseignement sur l'exposition (OSINT)

- Données fuitées (*leaks*)
- E-Réputation
- Données sensibles exposées

Renseignement sur la surface exposée (VOC)

- Veille sur les dernières vulnérabilités contextualisées
- Scan de la surface exposée
- Suivi des remédiations



Portail ForCERT
unifié

...couplé à une proximité humaine



Le pilote du service (SDM)

Interlocuteur privilégié, il est garant du service rendu, connaît votre contexte et propose des améliorations du service sous forme de Comités mensuels



Les analystes CTI

Ils qualifient les découvertes des outils et ajustent les outils et la plateforme pour ne valider que les éléments qui vous sont pertinents



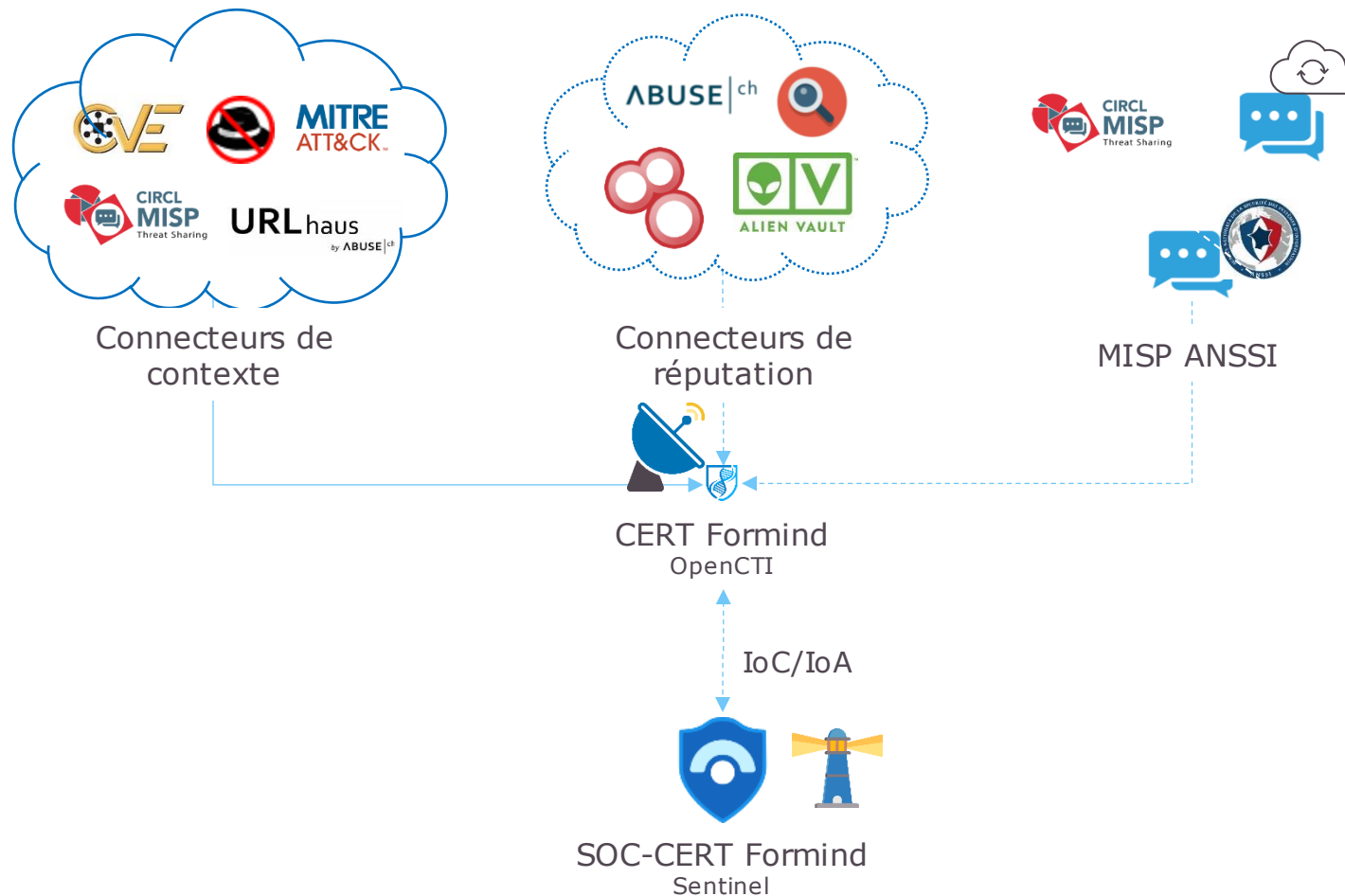
Les auditeurs techniques

Rompus aux facettes techniques du renseignement en source ouverte (OSINT), ils ajoutent de nouvelles méthodes de reconnaissance et les actifs vulnérables exposés



Vous!

En apportant votre connaissance interne (mots-clés, premiers noms de domaine...), vous démarrez le service et consultez les résultats sous forme de rapports et *via* le portail

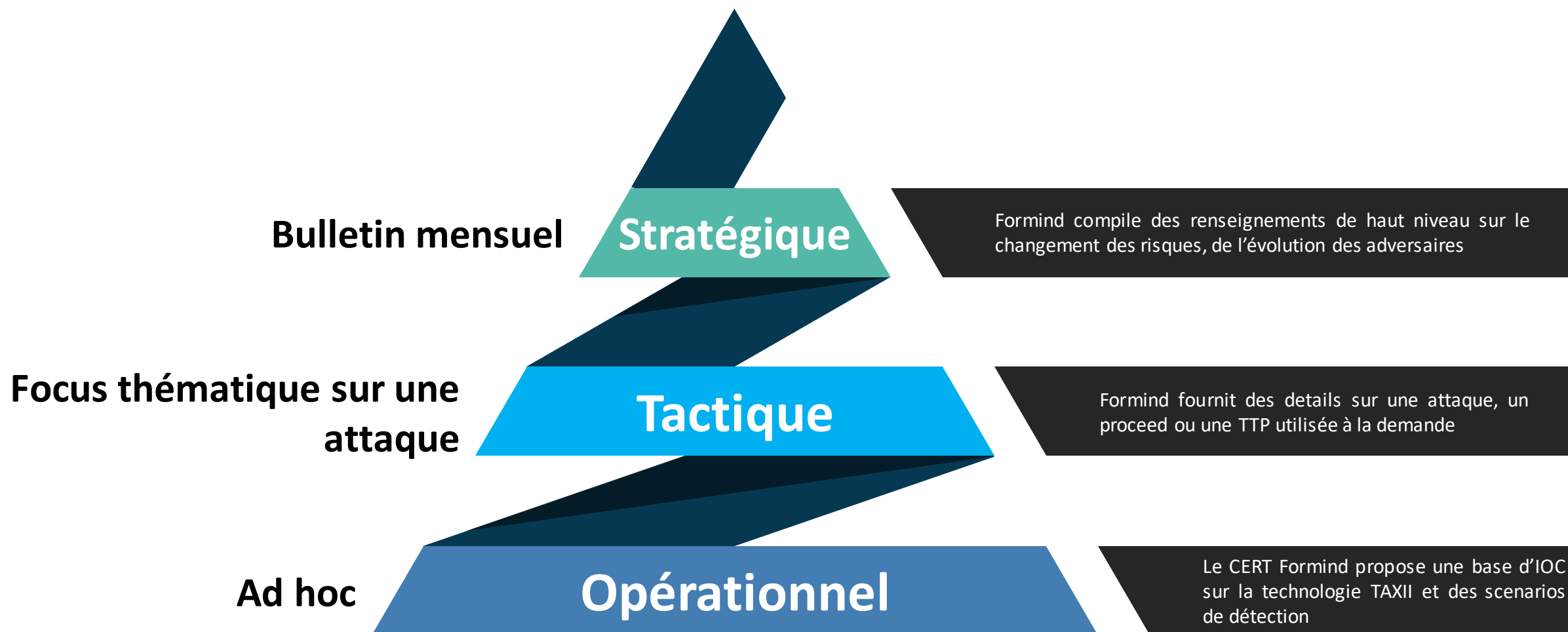


Les 3 missions de la CTI Formind

- **Veille cyber** sur l'évolution de la **menace** contextualisée à votre secteur d'activité
- **Enrichissement des alertes** remontées par le SOC
- **Utilisation des IOC** pour faire du Threat Hunting chez les clients

Une **grande variété de sources** provenant de l'externe et de notre CERT (SOC et FIR) impliquant une grande richesse, qualité et fiabilité en nos IOC/IOA

Des **résultats tangibles** : 5% des alertes du SOC Formind proviennent de la Cyber Threat Intelligence



Services

- Noms de domaine
- Sous-domaines
- Adresses Ip
- Technologies

Sites web

- Documents publics
- Offres d'emploi
- Contacts
- Adresses mail
- Pages administration

Réseaux sociaux

- Mots clés
- Réseaux d'attaquants
- Évènements liés aux prestataires

GitHub, Pastebin ...

- Code en ligne
- Clés API
- Mots de passe

Search Illicit Services, HaveIBeenPwned

- Adresses mail
- Mots de passe
- N° Téléphone
- Adresses
- Noms Prénoms

Darkweb

- Groupes ransomware
- Dernières attaques
- Fuites de données





Modèle de coût

BUILD

- Intégration solution : proportionnelle à la complexité réseau
- BUILD service (comitologie, gestion d'incidents, ...) et technique

→ **Coût forfaitaire**

RUN

- Gestion des alertes et incidents de sécurité
- Amélioration continue et changements de service inclus

→ **Cout fixe (comitologie) et cout à l'incident vrai positif**

Option

- Force d'intervention rapide

→ **Abonnement et coût à l'intervention**

Nous avons également défini des niveaux d'engagements (traitement des tickets, traitement des demandes/changements,...) et un catalogue des changements propre au service



Merci

 formind  @formind

www.soc-cert.formind.fr
www.formind.fr

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