Markess Blueprint®

SOC managé pour le mid-market

Édition 2023-2024

markess.
by exægis

Sommaire

Le Markess Blueprint®

Le **Markess Blueprint®** est le référentiel local d'aide au choix de solutions numériques des dirigeants français, qu'ils appartiennent à de grandes entreprises, des ETI, de PME et de collectivités.

Il offre aux décideurs une grille de lecture pertinente et objective permettant les comparaisons entre fournisseurs de solutions numériques.

Le Markess Blueprint s'appuie sur une double expertise locale, conjugaison de savoir-faire : celui d'Exaegis en matière d'audit et de notation de fournisseurs de solutions numériques, et celui de Markess en matière d'analyse de la demande et des évolutions des marchés numériques.

SOC managé pour le mid-market

Édition 2023-2024

Ce Markess Blueprint est consacré au SOC managé qui correspond aux services d'externalisation du centre opérationnel de sécurité ou SOC (Security Operations Center) assurés par des fournisseurs de services managés de sécurité ou MSSP (Managed Security Services Providers). Les résultats présentés se fondent sur une étude conduite durant l'année 2023 regroupant 21 sociétés dont les offres sont disponibles en France et adressant le mid-market.

Les critères d'appréciation ont été définis d'après l'expérience des analystes de Markess by Exaegis.

markess. by exaegis

Avant-propos

A mesure qu'elles numérisent leurs processus et qu'elles étendent leurs systèmes d'information, les organisations du mid-market du secteur privé (PME, ETI) et du secteur public (collectivités, établissements de santé, agences, etc.) font face à un nombre croissant de menaces de cybersécurité. Moins bien outillées que les grandes entreprises ou les administrations centrales, elles sont désormais des cibles privilégiées pour les hackeurs. Elles ont ainsi représenté près de 40 % des attaques par rançongiciel traitées ou rapportées à l'Agence nationale de la sécurité des systèmes d'information (ANSI) en 2022.

Dans ce contexte, les organisations ont de plus en plus recours à des prestataires de services externalisés de centre opérationnel de sécurité ou SOC managé (Security Operations Center) pour protéger leurs infrastructures numériques. Selon les estimations de Markess by Exaegis, le marché des services de SOC managé connaitra ainsi une croissance de plus de 15% en France en 2023.

Ces services tiers offrent une gamme complète de solutions de sécurité, de la surveillance en temps réel à la réponse aux incidents. Ils sont conçus pour aider les entreprises à renforcer leur posture de sécurité, à détecter et à répondre aux menaces, du moins en partie, en accompagnant un CERT (Computer Emergency Response Team) de manière proactive, tout en minimisant les coûts et les complexités liés à la gestion d'un SOC interne.

Les SOC managés sont particulièrement adaptés aux besoins des PME et ETI car ils leur proposent des solutions évolutives, flexibles et personnalisées, et leur permettent de choisir les services correspondant le mieux à leurs besoins.

Cette approche donne ainsi la possibilité aux entreprises et aux organisations publiques de tirer pleinement parti des avantages d'un SOC sans avoir à investir massivement dans des ressources internes.

Sur le plan de l'innovation, les prestataires de SOC managés profitent de plus en plus de l'automatisation et de l'intelligence artificielle (IA) pour améliorer leur efficacité. L'automatisation les aide à répondre aux incidents de manière plus rapide et cohérente, réduisant ainsi le temps d'arrêt et les pertes financières associées aux cyberattaques. L'IA, elle, permet d'analyser d'énormes volumes de données de sécurité en temps réel pour détecter plus rapidement les menaces potentielles.

Pour de nombreuses organisations, la conformité réglementaire est un moteur majeur d'adoption de services cyber, en particulier dans des secteurs réglementés comme la finance ou la santé. Les SOC managés peuvent les aider à se conformer aux exigences réglementaires de sécurité des données en fournissant des rapports et des audits détaillés sur leurs opérations de sécurité.

Face à cette demande croissante de sécurisation, de nombreuses offres de SOC managé ont vu le jour. Ce Markess Blueprint® les positionne selon leur empreinte sur le marché et leur adéquation aux besoins du mid-market.

Timothée Veiras
Research Analyst

markess. by exaegis

Définition du segment

SOC managé

Protection et prévention	Détection des menaces	Gestion des incidents & Réaction
• Gestion des vulnérabilités (veille, qualification, préconisation et suivi du déploiement des patchs) • Implication dans le processus de sensibilisation	• Collecte des évènements de sécurité et qualification des incidents (SIEM, EDR, XDR, NDR, SOAR) • Contrôle de sécurité (Scanneurs de vulnérabilités) • Veille & connaissance des menaces (veille sur le cybersquatting & défacement du site web, Threat Intelligence)	• Investigations et contribution à l'analyse • Participation à la réaction

Administration de la sécurité

- Système de détection d'intrusion (Sondes)
- Gestion des anti-virus (veille sécurité, surveillance et gestion)
- Prise en compte des alertes Data Loss Prevention

Profils utilisateurs

- Décideurs du numérique : DSI, RSSI, etc.
- Secteurs : défense, industrie, banque, assurance, secteur public, utilities, télécoms, distribution & commerce, etc.

markess. by exægis

Matrice de positionnement

SOC managé pour le mid-market

Édition 2023-2024

markess.
by exægis

Classification des fournisseurs

Leaders

Les **Leaders** sont les fournisseurs qui bénéficient à la fois d'une forte empreinte sur le marché (*market impact*) et d'une offre en forte adéquation avec les besoins des utilisateurs.

Ils proposent des offres complètes et performantes (*market relevance*), et disposent d'un nombre important de références clients.

Leurs solutions sont préconisées pour les utilisateurs en recherche de solutions complètes, performantes et fortement présentes sur le marché.

Performers

Les **Performers** sont les fournisseurs fortement établis sur le marché local avec une large base de clients. Ils disposent également de moyens marketing, de partenariats importants et d'une bonne image (*market impact*).

Ils proposent des offres à forte notoriété et base installée sur un périmètre précis (*market relevance*).

Leurs offres sont particulièrement adaptées pour les utilisateurs souhaitant des solutions éprouvées et largement utilisées.

Visionnaires

Les **Visionnaires** sont les fournisseurs qui proposent des solutions particulièrement adaptées aux besoins des utilisateurs en termes d'étendue et de qualité de l'offre, d'innovation et d'adaptation au marché local (*market relevance*).

Leurs parts de marché restent limitées mais peuvent s'accroître à moyen terme (*market impact*).

Leurs solutions sont idéales pour les utilisateurs en recherche de solutions performantes et innovantes.

Outsiders

Les **Outsiders** sont les fournisseurs qui ont actuellement une présence limitée sur le marché (*market impact*) et sont positionnés sur un périmètre de solution restreint ou peu profond (*market relevance*).

Leurs offres sont adaptées pour les utilisateurs souhaitant répondre à des besoins spécifiques ou dont l'étendue voire la complexité sont limitées.

Axe vertical – Market Relevance

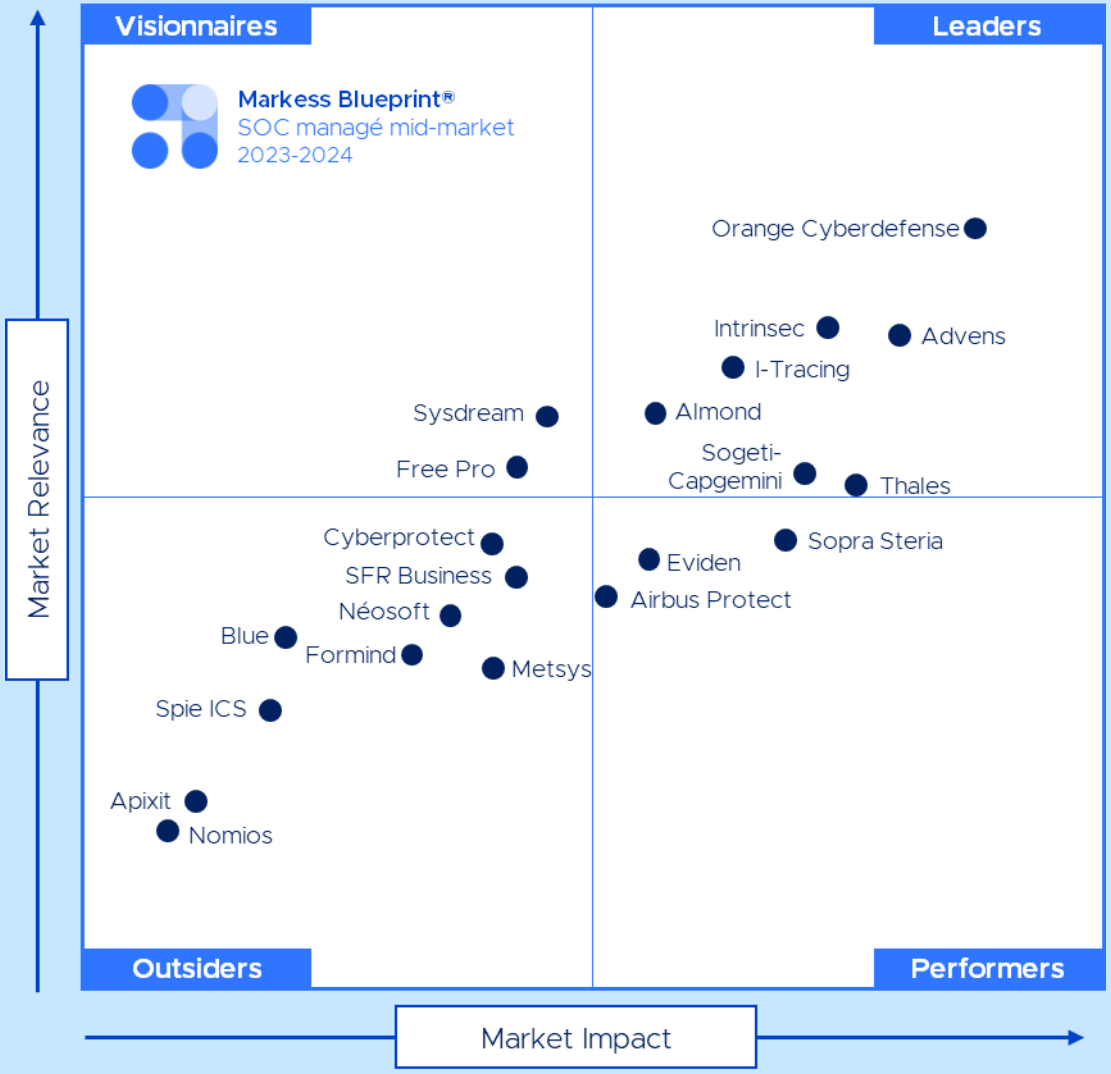
Critère d'évaluation	Indicateurs et informations pris en compte
Etendue de l'offre	
	Couverture fonctionnelle
	Couverture sectorielle
Qualité de l'offre	
	Compétences (technologiques, de sécurité, opérationnelles), expertises fonctionnelles et technique, capacités d'accompagnement conseil
	Ressources humaines disponibles
	Sécurité, continuité, stabilité
	Performances (taux de disponibilité, temps de déploiement, % de faux positifs, SLA….)
	Satisfaction produit et expérience utilisateur
Stratégie d'offre et innovation	
	Roadmap produit, évolution et adaptation à la demande
	Culture produit et R&D
Adaptation locale	
	Services support
	Localisation des infrastructures et données
	Conformité et sécurité

markess. by exægis

Axe horizontal – Market Impact

Critère d'évaluation	Indicateurs et informations pris en compte
Performance commerciale	
	Chiffre d'affaires dans le segment
	Croissance, en regard du marché
	Références clients, nombre d'utilisateurs
Image	
	Notoriété
	Niveau de recommandation
	Satisfaction client globale
	Leadership d'opinion
	Image employeur
Go-to-market	
	Partenariats technologiques
	Partenariats commerciaux
	Capacités Marketing

Matrice de positionnement



L'avis de Markess

Pour répondre à la forte demande du mid-market en SOC managé, de plus en plus d'offres sont disponibles sur le marché. Trois profils de fournisseurs se distinguent :

- Les **ESN généralistes** qui ont des offres larges plutôt adaptées aux grandes ETI : Eviden (ex-Atos), SFR Business, Sogeti-Capgemini, Sopra Steria, Spie ICS, Thales.
- Les **pure players Cyber**, et les filiales dédiées, qui connaissent des fortes dynamiques : Advens, Airbus Protect (Airbus), Cyberprotect (Inherent), I-TRACING, Intrinsec (Neurones), Orange Cyberdefense (Orange), Sysdream (Hub One), Almond.
- Les **spécialistes du mid-market**, dont les opérateurs télécoms B2B qui se positionnent sur des offres combinées : Apixit, Blue, Formind, Free Pro, Metsys, Néosoft, Nomios.

L'intégration progressive de l'intelligence artificielle et l'automatisation dans les offres de SOC managé va accélérer la détection des menaces, améliorer la réactivité face aux incidents et alléger la charge de travail des analystes.

markess. by exaegis

Panorama des fournisseurs

Fournisseur	Advens	Airbus Protect	Almond	Apixit	Blue	Cyberprotect	Eviden	Formind	Free Pro	Intrinsec	I-Tracing	Metsys	Néosoft	Nomios	Orange Cyberdefense	SFR Business	Sogeti - Capgemini	Sopra Steria	Spie ICS	Sysdream	Thales	Moyenne
Classification	Leader	Performer	Leader	Outsider	Outsider	Outsider	Performer	Outsider	Visionnaire	Leader	Leader	Outsider	Outsider	Outsider	Leader	Outsider	Leader	Performer	Outsider	Visionnaire	Leader	
Market Relevance																						
Etendue de l'offre																						
Qualité de l'offre																						
Stratégie d'offre et innovation																						
Adaptation locale																						
Market Impact																						
Performance commerciale																						
Image																						
Go-to-Market																						

Faible — Fort

markess. by exaegis

Profils fournisseurs

SOC managé pour le mid-market

Édition 2023-2024

markess.
by exægis

Profil fournisseur

Advens

Présentation

Advens est **Leader** dans ce Markess Blueprint.

Créé en 2000 à Lille, Advens est un pure player de la cybersécurité spécialisé dans la Security-as-a-Service.

L'ESN est présente en France (Paris, Lille, Lyon, Aix-en-Provence, Toulouse, Bordeaux, Nantes et Rennes), au Québec (Montréal) et ambitionne de se développer en Europe. Elle compte plus de 450 employés.

Advens dispose d'une large offre de services composés d'un CISO Office, d'un CERT, d'un SOC, d'une expertise en stratégie de sécurité opérationnelle, offensive, d'intégration et de management des technologies de sécurité et de conformité.

Pour quelles organisations ? Advens adresse les grosses PME et les ETI, et propose des expertises en santé, secteur public et industrie 4.0.

Atouts

Advens dispose d'un service 24/7 Follow the sun (équipe au Canada et en Asie Pacifique) et d'une excellente couverture fonctionnelle avec des partenaires technologiques étrangers mais également français qui sont parmi les meilleurs du marché comme Gatewatcher, HarfangLab, SentinelOne, Microsoft, Vectra, Nozomi, Cortex et Corwdstrike. La société dispose de ses propres infrastructures de détection avec une plateforme SIEM développée entièrement en interne, ce qui réduit les coûts de licences et de facturation pour ses clients et renforce ses performances de détection. Les données collectées sont hébergées en France.

L'entreprise dispose d'un nombre important d'analystes qualifiés (N2 et N3) qui s'appuient sur le framework ATT&CK du MITRE et qui ont un niveau élevé de certification pour l'usage des technologies partenaires.

La certification PDIS est en cours de qualification.

Advens a une forte notoriété sur le marché du SOC managé avec plus de 150 clients tels que Malakoff Humanis, AG2R La Mondiale, L'Occitane, Andros, l'UGAP, CAIH, TF1, etc.. L'entreprise participe également à l'ensemble des évènements Cyber de références ainsi qu'à des webinaires et publie régulièrement sur le sujet.

Points d'attention

Advens ne dispose pas encore de qualification ANSSI PDIS même si celle-ci est en cours.

L'opérateur adresse majoritairement le mid-market et les grands comptes français et semble moins adapté pour les petites PME.

markess. by exægis

Profil fournisseur

Blue

Présentation

Blue est **Outsider** dans ce Markess Blueprint.

Créé en 2005 à Rennes, Blue (ex-Bretagne Télécom) est un opérateur télécom avec une expertise dans la cybersécurité, le cloud, les réseaux, la communication unifiée et l'hébergement.

L'entreprise a un ancrage territorial fort dans le Grand Ouest et au niveau national. Elle compte plus de 170 employés et 2500 clients en France et un chiffre d'affaires de 41 millions d'euros en 2023.

Blue Cyber propose une offre de bout en bout, de la prévention à la remédiation, avec l'utilisation de solutions performantes comme Qradar d'IBM, CyberArk, SentinelOne et Cortex de Palo Alto.

Pour quelles organisations ? Blue adresse majoritairement les PME et les ETI. Son offre SOC est particulièrement adaptée aux PME ayant besoin de services personnalisables.

Atouts

Blue dispose d'un service de sécurité des systèmes d'informations complet (sécurité des données, du SI, des accès, du réseau) qui permet un bon accompagnement relatif aux besoins du client pour les PME, ETI. Ces offres se déclinent en 3 packs avec un « Micro SOC » basé sur des logiciels XDR, un « ZeroTrustSOC » avec un XDR, un bastion Blue Cyber et la mise en place d'un MFA (authentification multi facteur) et un « ZeroTrustSOC & Response » qui dispose d'un XDR, un MFA, un bastion, un SIEM et un SOAR.

Blue s'appuie sur des partenaires technologiques parmi les plus qualifiés du marché comme Qradar d'IBM, CyberArk, SentinelOne, Fortinet, Vmware, Purestorage ou Cortex de Palo Alto avec des certifications pour chacun d'eux ainsi que sur des analystes de N1, N2 et N3.

L'opérateur détient un datacenter hautement sécurisé à Châteaubourg en propre et un supplémentaire est prévu en 2024 à Nantes. Blue est certifié ISO27001, HDS (Hébergeurs de Données de Santé) et ambitionne d'être référencé SecNumCloud en 2024.

Points d'attention

L'offre SOC de Blue au-delà de son positionnement sur l'arc atlantique manque encore de notoriété et d'impact sur le marché national.

La capacité marketing de Blue sur le SOC est encore limitée. Il n'existe pas de blog technique et de communication sur les vulnérabilités par exemple mais l'entreprise créée du contenu vidéo sur le sujet.

L'opérateur ne dispose pas de qualifications ANSSI PDIS, néanmoins l'architecture de son SOC est basée sur cette qualification.

markess. by exægis

Profil fournisseur

Cyberprotect

Présentation

Cyberprotect est **Outsider** dans ce Markess Blueprint.

Créé en 2004 à Lyon, Cyberprotect a rejoint le groupe Inherent, anciennement Adista, en 2022. Inherent a comme objectif d'en faire un acteur majeur des services managés de cybersécurité.

Cyberprotect s'appuie sur ses solutions de collecte et de traitement d'évènements de sécurité (Blackhole), sa suite de services managés (Solar Belt) et son service de surveillance Lunar qui sont dévoués à son SOC CyberproVerse.

Pour quelles organisations ? Cyberprotect adresse majoritairement les PME et les ETI pour tous types de secteurs d'activité.

Atouts

Le SOC de Cyberprotect, CyberproVerse est au centre de tous les services proposés par l'entreprise qui investit et développe des solutions de surveillance, de collecte et de traitement des évènements. Par ailleurs, son SOC s'appuie sur des solutions open source comme GIT, CORTEX, Terraform ou TheHive. Sa R&D lui confère une excellente connaissance et optimisation de ses outils de détections comme le SIEM, EDR ou le NDR. L'opérateur offre une suite complète et complémentaire de services managés et dispose de bonnes compétences opérationnelles largement éprouvées. L'entreprise s'appuie sur les principales recommandations PDIS.

L'offre de Cyberprotect est parfaitement adaptée aux PME et aux ETI et bénéficie d'une expertise historique sur ce segment. Un accompagnement de bout en bout est offert aux utilisateurs constitués d'une équipe d'experts certifiés ITIL Foundation v3, chargé de traiter les demandes des clients.

Soutenue par le groupe Inherent, Cyberprotect devrait avoir un plus fort impact sur le marché dans les années à venir concernant la promotion de la marque employeur, la participation à des évènements et la visibilité sur le segment.

Points d'attention

Malgré de bonnes compétences, l'opérateur ne dispose pas de qualification ANSSI PDIS, et de peu de certification sur leurs partenaires technologiques. Son nombre de salariés sur le SOC est restreint en comparaison à d'autres fournisseurs plus matures qui bénéficient d'une traction financière et commerciale plus importante.

Profil fournisseur

Free Pro

Présentation

Free Pro est **Visionnaire** dans ce Markess Blueprint.

En 2021, le Groupe Iliad a fait l'acquisition de l'opérateur Jaguar Network, renommé Free Pro et devenu la filiale B2B du Groupe. En 2023, Iliad a également racheté ITrust, spécialiste français de la cybersécurité, dans le but de développer son offre de services managés et de solutions de sécurité. Free Pro compte environ 500 collaborateurs et 40 000 clients.

Free Pro propose deux offres Cyber XPR, l'une à destination des PME et PMI et l'autre à destination des ETI et des grands groupes.

Pour quelles organisations ?

L'offre de SOC est particulièrement adaptée aux TPE et PME ayant besoin de services clé-en-main, souverains et à un tarif accessible.

Atouts

L'opérateur dispose d'une offre SOC complète qui s'appuie sur la solution souveraine développée par ITrust avec un SIEM basé sur 3 moteurs de détection et la corrélation des données (UEBA/SOAR, Threat Hunting, Threat Intelligence). L'offre inclut également un scan de vulnérabilité, un EDR (XDR) et un service managé pour assurer la gestion des solutions.

L'entreprise dispose d'un important budget R&D et travaille avec des laboratoires de recherches français comme l'IRIT (Institut de Recherche en Informatique de Toulouse), le LAAS (Laboratoire d'Analyse et d'Architecture des Systèmes du CNRS) ou le LIPN (Laboratoire d'Informatique de Paris-Nord).

Les outils proposés sont labélisés ISO9001, PASSI RGS, Label CNIL et France Cybersecurity.

Les bureaux (le SOC) sont à Paris et Toulouse pour assurer un service de surveillance 24x7 en continu (protection contre une attaque/sinistre/coupure sur l'un ou l'autre des sites).

Le SIEM et les données sont hébergés dans les Data Centers Free Pro.

Points d'attention

L'opérateur ne dispose pas de qualification ANSSI PDIS.

L'offre Cyber XPR est packagée et n'offre pas un niveau de personnalisation aussi élevé que celles de certains opérateurs positionnés dans ce Blueprint. Toutefois, cette structure d'offre lui permet de proposer des tarifs attractifs à des organisations qui ne sont pas en capacités d'investir massivement dans la sécurisation de leur SI.

Lancée en 2023, l'offre a encore besoin de se faire connaitre et de gagner en maturité.

markess by exaegis

Profil fournisseur

Intrinsec

Présentation

Intrinsec est **Leader** dans ce Markess Blueprint.

Fondé en 1995 en Ile-de-France, Intrinsec est une ESN spécialisée dans le domaine de la cybersécurité. L'entreprise a rejoint le groupe Neurones en 1999 et affichait une croissance de près de 20% en 2022.

Elle compte 200 collaborateurs qui couvrent de nombreux domaines dans la cybersécurité comme l'audit de sécurité, les tests d'intrusions, le conseil et les services managés de sécurité (créés en 2011) avec la veille SSI, la gestion des vulnérabilités, la Threat Intelligence, le SOC et le CERT.

Pour quelles organisations ? Intrinsec adresse tous les types d'organisations, de la PME à la grande entreprise. Le fournisseur compte des références clients dans tous les secteurs.

Atouts

Intrinsec a une offre éprouvée et reconnue sur le segment du SOC managé. L'entreprise collabore avec de nombreux partenaires et éditeurs comme Splunk, Crowdstrike, Sentinel One ou Sekoia qui figurent parmi les meilleurs éditeurs du marché sur leurs solutions respectives (SIEM, SOAR, EDR, XDR etc.).

Les équipes sont composées d'analystes à haut niveau de certification et de formation (ITIL V4, ISO 27001 LA, ISO ISO 27005, Splunk Fundamentals 1, 2 et 3, Crowdstrike FHT 105, FHT 109). Intrinsec investit fortement en R&D pour développer son offre et ses outils (SIEM, EDR, XDR).

Intrinsec est multi-qualifiée par l'ANSSI : PASSI LPM et RGS pour ses activités d'audit et de test d'intrusion, et PRIS pour ses activités de réponse à incidents. Elle est également membre du CESIN et du Campus Cyber, participe à de nombreux événements (webinaires et conférences au CESIN, évènements éditeurs) et organise le Club clients Intrinsec Cyber Threat Intelligence.

L'ESN adresse les PME, les ETI et les grandes organisations avec des offres différenciées en fonction des besoins et avec une approche personnalisée de son offre dans la conception, le déploiement et les services fournis.

Points d'attention

L'offre ne dispose pas de la certification ANSSI PDIS (Prestataires de Détection d'Incidents de Sécurité).

La notoriété et la visibilité de l'ESN reste inférieure à celle des gros acteurs généralistes du marché.

markess. by exægis

Profil fournisseur

I-Tracing

Présentation

I-TRACING est **Leader** dans ce Markess Blueprint.

I-TRACING est un pure player des services de cybersécurité fondé à Paris en 2005. Le fournisseur compte 550 salariés pour un chiffre d'affaires supérieur à 90 millions d'euros en 2022 et une forte croissance de l'ordre de 30%.

L'entreprise est basée à Paris et dispose d'une présence à Londres, Hong-Kong et Montréal.

L'entreprise propose des services d'audit, de conseil et d'ingénierie de solutions, de formation et des services de sécurité managés.

Pour quelles organisations ? I-TRACING adresse majoritairement les ETI et grandes organisations, avec notamment une forte proportion d'acteurs du luxe, retail, grande distribution, banques, d'assureurs et opérateurs télécoms.

Atouts

I-TRACING a une excellente couverture fonctionnelle et dispose de nombreux partenariats technologiques comme Elastic Chronicle, Microsoft, Palo Alto, Sekoia, Splunk sur le SIEM ; SentinelOne, Crowdstrike sur l'EDR ; ou bien Vectra et Darktrace sur le NDR. Son SOC « Follow-The-Sun », qui s'appuie sur ses filiales de Montréal, Hong Kong et Paris, est en cours de qualification ANSSI PDIS et est composé uniquement d'analyste de niveau N2 et N3 avec un haut niveau de certification.

L'entreprise a un solide portefeuille clients et plus d'un plus de 120 clients sont utilisatrices de l'offre SOC dont une soixantaine en services managés.

I-TRACING est partenaire fondateur du CESIN, membre du Campus Cyber, labelisé Label France Cybersecurity et organise l'évènement We Share SOC dédié à leurs clients SOC, qui regroupe 70 interlocuteurs au travers d'un programme annuel constitués d'ateliers, de partage de retours d'expérience et de 2 évènements. Le fournisseur est présent sur de nombreux évènements en cybersécurité comme le FIC, les Assises ou IT & Cyber Meeting.

Points d'attention

I-TRACING adresse essentiellement les ETI et les grands groupes, son offre ne s'applique pas aux PME.

Le fournisseur ne dispose pas encore de la qualification PDIS, qui est toutefois en cours d'évaluation tout comme la qualification PAMS.

Malgré une notoriété importante, ce pure player a un go-to-market moins étoffé en comparaison avec d'autres acteurs positionnés en tant que leaders sur ce Blueprint.

Profil fournisseur

Orange Cyberdefense

Présentation

Orange Cyberdefense est **Leader** dans ce Markess Blueprint.

Crée en 2014, Orange Cyberdefense regroupe les activités Cyber du groupe Orange et compte plus de 3000 employés dans le monde.

Orange Cyberdefense décline son offre de SOC managé à travers trois offres : Micro-SOC (un service packagé et clé en main) Xtended-SOC (un service packagé mais qui prend en compte les spécificités des entreprises), Cyber-SOC (un service à la carte et personnalisé).

Orange Cyberdefense propose des offres ciblées pour les secteurs Administrations et collectivités, Industrie, Etablissements de santé et Services Financiers.

Pour quelles organisations ? Orange Cyberdefense adresse à la fois les grandes entreprises, les ETI et les PME.

Atouts

Orange Cyberdefense propose trois offres différenciées en fonction de la taille, des finances et du niveau de sécurité de chaque entreprise avec le Micro-SOC (EDR/XDR, Email et Cloud, SHIELD/réseaux) qui d'adresse plutôt au TPE et PME, avec l'Xtended-SOC (autour de technologies XDR) à destination des PME et ETI, et le Cyber-SOC pour les grandes entreprises et OIV (Opérateurs d'Importance Vitale). Cet éventail de propositions lui confère une position de leader sur le segment du SOC managé de la PME à la grande entreprise.

Ses offres sont qualifiées PASSI LPM/RGS, PDIS et PRIS par l'ANSSI ce qui contribue au savoir-faire d'Orange Cyberdéfense sur le sujet et les équipes SOC sont systématiquement certifiées sur au moins un éditeur partenaire (plus de 1000 certifications). Par ailleurs, Orange Cyberdefense investit massivement dans sa R&D avec plus de 250 chercheurs en cybersécurité.

L'entreprise a un fort impact sur le marché puisqu'elle participe à près de 20 groupes de travail spécialisés par secteur d'activité. De plus, plus de 80 publications et articles ont été produits par Orange Cyberdefense dans le cadre de conférences en cybersécurité en 2022. L'organisation dispose de nombreux partenariats institutionnels (Campus Cyber, ministère des Armées, etc.) et académiques (EGE, CentraleSupélec, etc.).

Points d'attention

Pas de points d'attention particuliers.

markess. by exægis

Profil fournisseur

Sysdream

Présentation

Sysdream est **Visionnaire** dans ce Markess Blueprint.

Créé en 2001 par Aéroports de Paris sous le nom d'ADP Télécom, Hub One compte aujourd'hui 5000 clients, 700 collaborateurs et a généré un chiffre d'affaires de 162 millions d'euros en 2022. L'opérateur s'est renforcé dans le domaine de la cybersécurité avec les acquisitions de Sysdream (2018), devenu sa filiale experte du sujet, puis d'Oikialog et d'Oveliane (2020). Sysdream affichait une croissance de plus de 30% en 2022. Sysdream est également éditeur de logiciels et propose des services d'audit, de formation, des services managés de SOC et de CERT ainsi que des services de sécurisation des SI et de GRC.

Pour quelles organisations ?

Dans le domaine de la cybersécurité Sysdream adresse principalement les ETI et grands groupes.

Atouts

Sysdream dispose d'un SOC souverain qualifiée PDIS qui garantit un haut niveau de sécurité. L'entreprise s'appuie sur un EDR souverain (HarfangLab), une plateforme Sekoia ou une solution développée en interne, suite au rachat d'Ovéliane, et compatible avec les principaux SIEM du marché, qui permet un suivi en termes de conformité.

Le budget R&D et les investissements faits dans le SOC de l'entité sont importants. Plusieurs millions ont ainsi été investis dans une démarche de construction et qualification réalisée sur 3 ans. Sysdream dispose d'un laboratoire de recherche et de développement en sécurité informatique éprouvé. Grace à son appartenance au groupe ADP, le fournisseur héberge ses infrastructures en France dans ses propres datacenters de Roissy et Orly, qui sont localisés dans des zones aéroportuaires sécurisées.

En termes d'impact de marché, Sysdream organise une fois par an l'évènement Hack In Paris qui est connu des experts du domaine de la cybersécurité.

Points d'attention

Sysdream est dynamique mais manque encore de maturité concernant son go-to-market et sa performance commerciale.

Le fournisseur se concentre sur le haut du marché et adresse assez peu les PME, pour lesquelles il reste moins adapté.

Profil fournisseur

Thales

Présentation

Thales est **Leader** dans ce Markess Blueprint.

Thales compte près de 4000 salariés spécialisés dans les systèmes d'information critiques et la cybersécurité.

Le Groupe a acquis plusieurs acteurs de la cybersécurité (5 en 2022-2023) pour en faire l'un des acteurs mondiaux de la cybersécurité.

Son offre SOC se destine majoritairement à l'industrie, la finance, l'aérospatiale, l'aéronautique, au transport terrestre, à la défense et aux organisations du secteur public.

Pour quelles organisations ? Thales adresse les grandes entreprises et administrations centrales, ainsi que les ETI.

Atouts

Thales est multi-qualifié par l'ANSSI, PDIS, PASSI LPM/RGS, PRIS et certifié par un grand nombre d'éditeurs parmi lesquels on retrouve des leaders étrangers comme Palo Alto ou SentinelOne mais également français comme HarflangLab ou Gatewatcher.

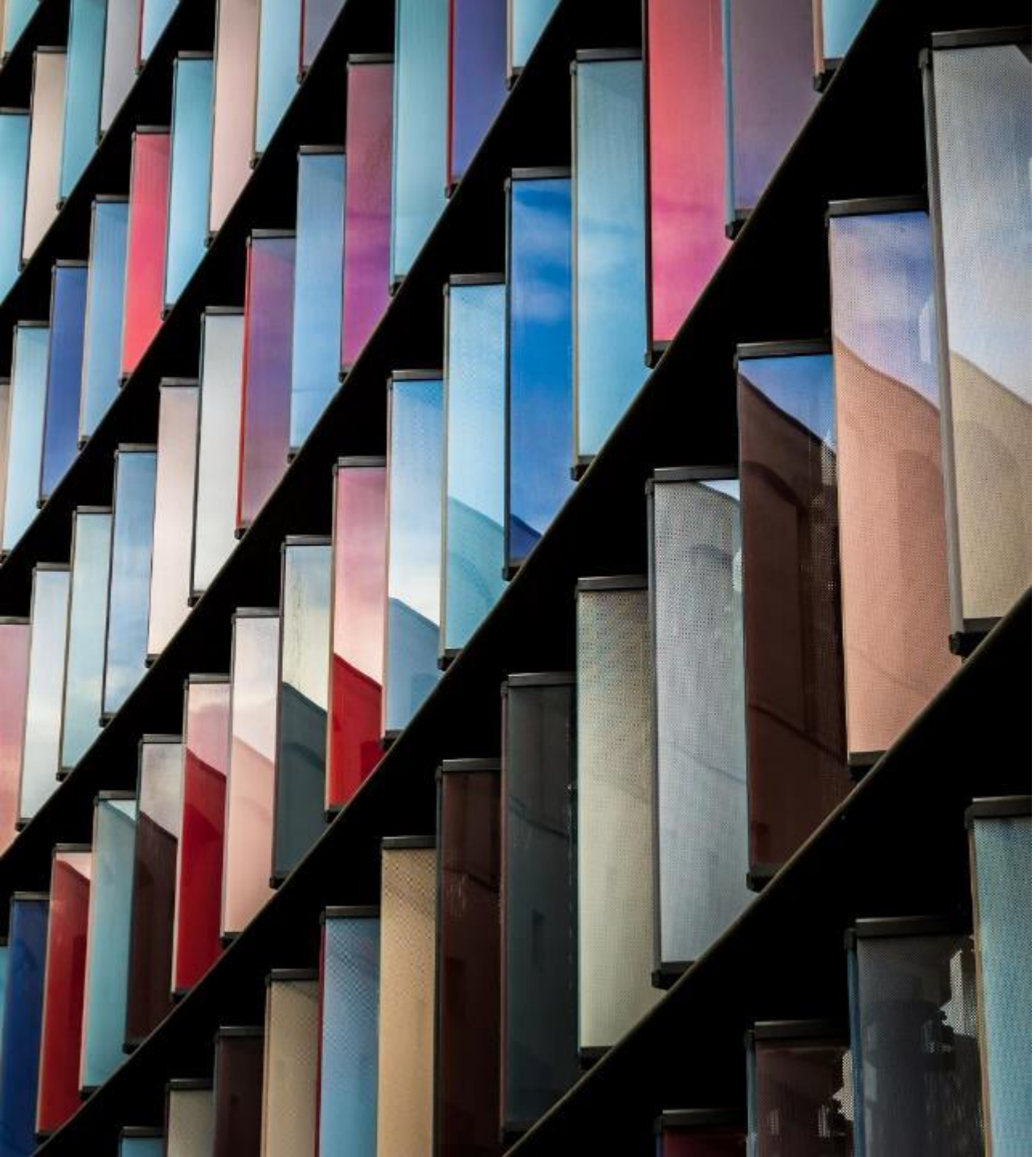
Thales développe également des solutions reconnues par l'ANSSI telles que la sonde de détection Cybels Sensor. Le fournisseur investit fortement en R&D pour développer et faire fonctionner l'ensemble de ses outils. Le fournisseur dispose d'un nombre important d'analystes dont une majorité de niveau 2 et de niveau 3.

Thales a un fort impact sur le marché français en étant membre d'organisations comme FIRST, TF-CSIRT, CESIN, R2GS, ECSO, ou CLUSIF, et en intervenant sur l'ensemble des salons importants du marché (FIC, Assises de la cybersécurité).

En termes de politique environnementale, Thales a reçu la note A- du Carbon Disclosure Project, confirmant sa place parmi les entreprises les plus transparentes et efficaces dans la lutte contre le changement climatique.

Points d'attention

Ciblant principalement les grandes organisations, l'offre SOC de Thales peut être surdimensionnée pour certaines organisations du mid-market et leurs contraintes budgétaires, notamment les PME.



Méthodologie

Markess Blueprint®

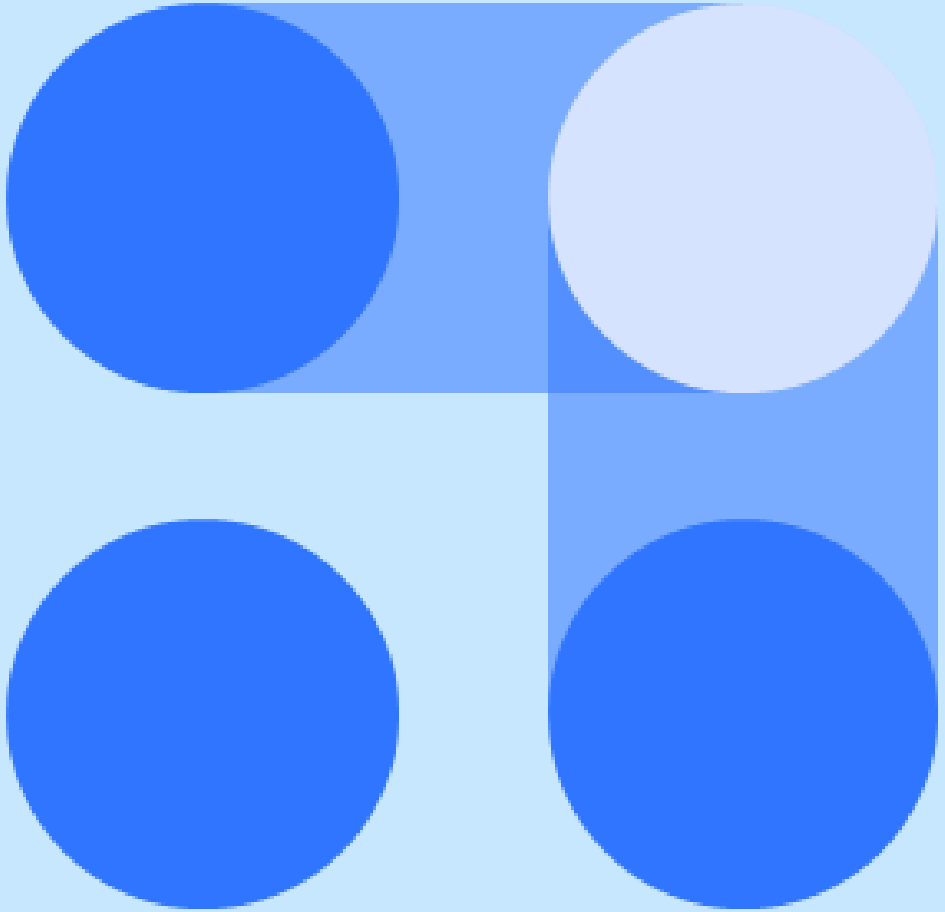
Édition 2023-2024

markess.
by exægis

Méthodologie

Le **Markess Blueprint**® est basé sur une méthodologie éprouvée et un processus rigoureux pour favoriser une lecture fiable et objective :

1. Sélection d'une typologie de solutions utilisée par les entreprises et les collectivités,
2. Sélection par Markess by Exaegis des offres et des fournisseurs candidats au Blueprint,
3. Pour chaque fournisseur, envoi d'une confirmation de son intégration au Markess Blueprint,
4. Déploiement du dispositif Markess by Exaegis : mise à disposition d'espaces privés et sécurisés de collecte des informations et de la documentation, démonstration des solutions, échanges,
5. Analyse des données collectées et confrontation aux bases d'informations internes à Markess by Exaegis, au regard de l'analyste expert du segment d'offre analysé,
6. Agrégation des résultats et présentation des résultats préliminaires à chaque candidat pour éventuels ajustements,
7. Publication et diffusion auprès des utilisateurs.



markess. by exægis

À propos de Markess by Exaegis

Fondée en 1997, Markess by Exaegis est la société d'études et de conseil de référence sur le numérique en France. Le socle de recherche continue, associé aux études et au conseil sur mesure, permet aux dirigeants des entreprises et organisations publiques comme des fournisseurs de solutions d'obtenir les informations, l'accompagnement et les outils indispensables dont ils ont besoin pour saisir les grands défis, les enjeux de leur transformation digitale et atteindre leurs objectifs.

Depuis 2018, la société fait partie du groupe Exægis, l'agence de notation référente du secteur du numérique.

Informations

www.markess.com

Markess by Exaegis
11 rue de Lourmel
75015 Paris
01 56 77 17 77

markess. by exægis

markess.
by exægis