

Thales lance la plateforme française de renseignements sur la menace cyber pour une plus grande autonomie et une résilience renforcée avec 10 autres acteurs français

- Le 5 avril 2023, Thales a annoncé le lancement du projet collaboratif, Socle Commun du Renseignement cyber et de la Détection, rassemblant 11 acteurs français spécialistes en cybersécurité. L'objectif de ce projet est de créer d'ici 3 ans une plateforme unique pour les entreprises et administrations publiques, leur donnant accès aux services de renseignements d'intérêt cyber.
- Dans le cadre de la [stratégie nationale cyber](#) du plan d'investissement France 2030, l'Etat a annoncé la nécessité d'accompagner le développement de la filière française de cybersécurité. Sollicités pour proposer des technologies innovantes, essentielles à la garantie de la souveraineté de la France, des industriels français, spécialisés en cybersécurité, se sont rassemblés pour contribuer au projet Socle Commun du Renseignement cyber et de la Détection. Ce projet a été retenu dans le cadre de l'appel à projet lancé par Bpifrance. Ce projet a été financé par l'Etat dans le cadre de France 2030.
- Piloté par Thales, le projet Socle Commun du Renseignement cyber et de la Détection regroupe des acteurs issus des secteurs public et privé : ATOS (ligne d'activités Eviden), Filigran, Geotrend, Glimps, Harfanglab, KOR Labs Cybersecurity, Sekoia, Snowpack ainsi que l'Institut Mines-Télécom SudParis et INP Grenoble. S'il a pour objectif de s'adresser à des organisations françaises, ce dispositif permettra d'instaurer les fondements d'une offre de services centralisée dotée d'un Centre d'Analyse de la Situation Cyber Nationale, ayant pour vocation de répondre à terme aux enjeux de souveraineté européenne.



Alors que les systèmes d'information des organisations sont de plus en plus complexes et les cyberattaques de plus en plus sophistiquées, la société dans son ensemble doit généraliser la mise en place d'outils contribuant à sa cyber résilience à l'image des préconisations récentes de la BCE qui mettra au point des stress tests cyber dédiés aux institutions bancaires d'ici un an¹. La mise en place d'une base nationale unique de renseignements cyber adossée à un centre d'analyse technique permettra, en amont, de fournir un panorama mutualisé de la

¹ Interview with Verslo žinios (europa.eu) : « *We need banks to be prepared. That's why for next year we are launching a thematic stress test on cyber resilience, which will try to test how banks are able to respond to and recover from a successful cyberattack. It's a new exercise, and we will devote quite a significant amount of time and resources to it, to have a better understanding of where the banks' strengths and weaknesses are. We plan to have the results by around the middle of next year.* »

menace pour mieux l'anticiper, la détecter et partager de l'information entre acteurs au sein d'une même communauté d'intérêt.

« Thales porte l'ambition d'accélérer la montée en maturité des capacités de renseignements cyber françaises pour renforcer la sécurité collective aux côtés de ses homologues spécialistes en cybersécurité. En fédérant un écosystème, ce projet fera bénéficier ses utilisateurs d'une plateforme considérablement enrichie, il contribuera à l'autonomie stratégique de la France dans ce domaine, » précise, **Pierre-Yves Jolivet, VP Cyber Solutions, Thales.**

Un point unique de mutualisation du renseignement cyber en France

Sous l'impulsion de Thales qui coordonnera les capacités et expertises de 10 acteurs spécialisés en cybersécurité, le projet Socle Commun du Renseignement cyber et de la Détection, fournira un éventail de services qu'aucun autre Etat n'a encore pu rassembler en un seul dispositif : une base nationale qui mutualisera les données et les valorisera au sein d'un cloud de confiance, un service d'analyse permettant de comprendre la menace à l'instant T, une analyse automatique de la tendance et des projections sur la base de modèles bénéficiant des technologies avancées d'intelligence artificielle.

Une autonomie stratégique renforcée dans le domaine cyber

Ce projet fera bénéficier ses utilisateurs de nombreux avantages en terme de compétitivité, de réduction du coût de traitement des attaques et de renseignement cyber ; il apportera plus de confiance au quotidien dans l'utilisation des systèmes d'information et contribuera à une plus grande souveraineté en ayant recours à des solutions tricolores, ouvrant la voie à des standards reconnus en Europe ou à l'international.

Grâce aux données collectées issues de la participation des membres et de la communauté d'utilisateurs du Socle Commun du Renseignement cyber et de la Détection, ce projet permet la création d'un Centre de d'Analyse de la Situation Cyber Nationale. A terme, l'Europe pourra bénéficier d'une autonomie à l'échelle de l'Union dans la production et l'exploitation des données de renseignements cyber et d'une capacité de détection et d'échanges d'informations entre pays, entre secteurs d'activités ou entre entreprises. Ce projet ambitieux facilitera la promotion d'entreprises européennes émergentes et de leaders européens.

Un traitement de la donnée par communauté d'intérêt

Dans un contexte de guerre de l'information, les centres de cybersécurité opérationnels et les CERT (Computer Emergency Response Team) collectent une grande masse de données non enrichies et non contextualisées, et sont de plus en plus confrontés au phénomène d'intoxication de la donnée. Son traitement et son analyse sont devenus des compétences extrêmement recherchées par les entreprises de toute taille.

Selon une analyse de l'ANSSI publiée en mars 2023, le nombre d'intrusions avérées dans des systèmes d'information signalées à l'Agence a augmenté de 37% entre 2020 et 2021. Les PME,

ETI et collectivités sont les premières ciblées.² Bénéficiaire d'un centre de collecte et d'analyse des données unique, à l'information partagée au sein d'une même communauté d'intérêts telle que le spatial, le naval, l'aviation ou tout autre secteur d'activité, répondra à des besoins grandissants émanant d'acteurs jusqu'à présent peu outillés.

Ils participent au projet Socle Commun du Renseignement cyber et de la Détection :

ATOS (ligne d'activités Eviden)

Filigran

Geotrend

Glimps

Harfanglab

Institut Mines-Télécom SudParis

INP Grenoble.

KORLabs Cybersecurity

Sekoia

Snowpack

Thales

Assistez à la conférence du FIC le 6 avril 14h30-15h30 : [FIC EUROPE – Du 5 au 7 avril 2023 – Lille Grand Palais \(forum-fic.com\)](#)

Towards a strategic autonomy of cyber intelligence?

- *Alexis Caurette, VP Strategy and Marketing BL CDS*
- *Ivan Fontarensky, Cyber Threat Intelligence Expert*

A propos de Thales

Thales (Euronext Paris : HO) est un leader mondial des hautes technologies spécialisé dans trois secteurs d'activité : Défense & Sécurité, Aéronautique & Spatial, et Identité & Sécurité numériques. Il développe des produits et solutions qui contribuent à un monde plus sûr, plus respectueux de l'environnement et plus inclusif.

Le Groupe investit près de 4 milliards d'euros par an en Recherche & Développement, notamment dans des domaines clés de l'innovation tels que le quantique, l'Edge computing, la 6G et la cybersécurité.

Thales compte 77 000 collaborateurs répartis dans 68 pays. En 2022, le Groupe a réalisé un chiffre d'affaires de 17,6 milliards d'euros.

² [ANSSI - Panorama de la menace informatique 2022](#)



CONTACT PRESSE

Relations médias Thales

Marion Bonnet

+33 (0)6 60 38 48 92

marion.bonnet@thalesgroup.com

[Consultez le communiqué de presse et le rapport : 2022-2023 Un an de cyber conflit de l'Ukraine à l'Europe](#)

[Page d'accueil | Thales Group](#)

[Solutions de cybersécurité | Thales Group](#)