

CYBELIUS PRESS BOOK

[illegible]

Seclab et Cybelius annoncent un partenariat stratégique

Par [Marc Jacob](#), publié en février 2021

Seclab et Cybelius officialisent un partenariat technique et commercial. À travers cette annonce d'envergure, les deux partenaires souhaitent proposer une offre unique permettant de sécuriser efficacement les infrastructures des industriels.

Dans ce contexte, à travers cette offre commune et packagée qui associe les technologies CyfENCE de Cybelius et Sec-XN de Seclab, il sera possible de créer un espace de confiance sur les systèmes existants et de l'intégrer dans la politique de sécurité du client.

Concrètement, grâce à Seclab, Cybelius pourra améliorer les performances de son offre en ajoutant la rupture protocolaire, tout en gardant le principe d'une intégration de l'ensemble des mesures de sécurité. Ainsi, la société sera en mesure d'adresser le marché des systèmes extrêmement sensibles en ajoutant de la sécurité, de la connectivité, de l'exploitabilité et de la maintenabilité. Seclab de son côté pourra diffuser sa technologie au plus grand nombre et permettre à ses clients de cloisonner et protéger leurs réseaux. De ce fait, les scans et attaques réseau sont alors sans effet pour les clients et ils seront également protégés contre d'éventuelles fuites de données.

L'alliance entre Cybelius et Seclab offre donc une réponse concrète et opérationnelle à différents cas d'usage : sécurisation des liaisons critiques (mises à jour, téléconduite, administration, etc.), mise en œuvre d'un bastion interne pour les informations sensibles (filtrage utilisateurs, authentification) ou encore création d'une zone de protection pour les sauvegardes et les logs.

Cybersécurité IT/OT : Cybelius et Sesame IT invitent Gfi au bal, avec son SIEM

Les deux premiers ont récemment annoncé le développement conjoint d'une sonde réseau durcie capable de couvrir IT et OT. Gfi les rejoint et apporte son SIEM Keenaï composer une offre complète

Par Valéry Marchive. Publié le 8 juillet 2020

Jean-Michel Orosco, vice-président sénior de Naval Group en charge de la [cybersécurité](#), l'[expliquait lors d'un atelier](#) organisé lors de l'édition 2018 du Forum International de la Cybersécurité (FIC) : des groupes comme le sien ont besoin qu'on leur présente des solutions qui s'intègrent de manière cohérente avec leurs architectures, pas de produits isolés. Il semble avoir été entendu.

Ironie du calendrier, c'est lors de cette même édition 2018 du FIC que Cybelius et Gfi [annonçaient un partenariat](#). Dans le cadre de celui-ci, le premier apportait sa sonde de détection des attaques et des dérives des processus Cypres, ainsi que Cyfence, sa DMZ de sécurisation des échanges entre environnements IT et OT. De son côté, GFI Informatique avançait Keenaï, son système de gestion des informations et des événements de sécurité ([SIEM](#)) développé en interne sur la base de quatre solutions visant à détecter les attaques, identifier les menaces en temps réel, et réduire les risques.

Keenaï, proposé sous la forme d'un conteneur [Docker](#), s'appuie sur Logstash pour le parsing des journaux d'activité, et sur une grappe Elasticsearch pour leur stockage. Le moteur de corrélation et les outils de reporting [reposent en revanche sur des développements internes](#). Le moteur de corrélation peut mettre à profit des données contextuelles tierces, y compris externes. Il y a deux ans, Fabien Corrard, directeur cyberdéfense Keenaï chez Gfi, expliquait que l'entreprise travaillait à l'exploitation de l'[apprentissage machine](#), en combinant algorithmes supervisés et non supervisés.

Mais depuis, Cybelius a noué un partenariat avec Sesame IT, pour développer ensemble une sonde réseau durcie susceptible de couvrir aussi bien les domaines IT qu'OT – et donc le monde des systèmes industriels ([ICS/Scada](#)). Le socle matériel sera la sonde Jizô développée par Sesame IT et en cours de certification par l'Agence nationale pour la sécurité des systèmes d'information (Anssi).

Celle-ci est basée sur le système de détection d'intrusion ([IDS](#)) Suricata – à l'instar des deux sondes déjà qualifiées, Cybels Sensor de Thales, et les produits Gatewatcher. Les capacités analytiques – et notamment comportementales – développées pour Cypres par Cybelius, avec toute la connaissance protocolaire spécifique au monde des ICS/Scada que cela implique, vont être embarquées comme un traitement *ad hoc* sur Jizô.

Aujourd'hui, fermant la boucle, c'est Gfi qui se joint à la nouvelle aventure de Cyberlius et Sesame IT, en apportant Keenai. Dans un billet de blog, Dominique Mouillier, directeur des activités Cybersécurité chez Gfi, [explique](#) que « cette offre permettra de traiter toute la chaîne de détection depuis la sonde jusqu'au SIEM afin de réaliser le traitement des flux, l'analyse, la génération d'alertes, l'archivage et l'expertise détaillée sans jamais rompre le niveau de confiance ni perdre d'information ». Et de souligner au passage que « tous les composants de cette chaîne ont été durcis et suivent les référentiels de l'ANSSI, afin de pouvoir être déployés par les OIV [opérateurs d'importance vitale] et OSE [opérateurs de services essentiels] ».

Sesame IT, Cybelius et Gfi proposent une offre de détection et de protection

Par Marc Jacob. Publié en juillet 2020

Pour mieux parer aux attaques qui impactent les capacités industrielles au travers du SI Corporate (via l'ERP, la logistique, ou le MES), Sesame IT, Cybelius et Gfi ont décidé de joindre leurs forces afin de proposer une nouvelle offre intégrale de détection et de protection. Son but ? Unifier tous les éléments des attaques sur un même outil, avec un haut degré de précision, une investigation facilitée et des équipements durcis et souverains. Cette nouvelle initiative vient prolonger le partenariat existant entre Sesame IT et Cybelius.

Cette offre permettra de traiter toute la chaîne de détection depuis la sonde jusqu'au SIEM afin de réaliser le traitement des flux, l'analyse, la génération d'alertes, l'archivage et l'expertise détaillée sans jamais rompre le niveau de confiance ni perdre d'information.

L'interopérabilité fonctionnelle entre les produits, objet des travaux en cours et la capacité d'adaptation aux systèmes des clients permettront une intégration rapide du dispositif et l'accès immédiat à des résultats facilement exploitables. Cette chaîne complète permettra la gestion et une hiérarchisation automatisée d'un premier niveau de logs et d'alertes, afin d'optimiser les interventions humaines au sein des SOC's.

Le partenariat existant entre Sesame IT et Cybelius apporte une sonde durcie prête à traiter simultanément les environnements IT et industriels (OT), embarquant des méthodes de détection sur pattern et plusieurs suites d'algorithmes d'Intelligence Artificielle. Le SIEM Keenaï de Gfi permet d'exploiter toutes les informations qualifiées par ces dispositifs et réalise l'agrégation, la corrélation, et la visualisation graphique des alertes.

L'approche métier de Keenaï permet de présenter les attaques tant sur le SI Corporate que sur le SI Industriel. La représentation graphique intégrée de la cyber kill chain accélère leur compréhension et permet une réaction et une remédiation plus efficace et moins coûteuse en ressources opérationnelles. Tous les composants de cette chaîne ont été durcis et suivent les référentiels de l'ANSSI, afin de pouvoir être déployés par les OIV et OSE.

Cybelius : Les gestes barrières en cybersécurité

Par Les partenaires de Challenges le 03.06.2020

Lancée en 2017 pour répondre au besoin émergent en matière de cybersécurité, Cybelius protège les sites industriels des menaces informatiques. Entre innovation et pragmatisme, l'équipe d'ingénieurs en informatique industrielle et d'experts en cybersécurité, accompagnent les exploitants de A à Z dans le processus de mise en sécurité de leurs systèmes. La société, très ouverte sur l'Europe, est en train de devenir une référence dans son domaine.

Entretien avec Frédéric Planchon, fondateur et dirigeant de Cybelius.



Quels sont les enjeux en cybersécurité industrielle ?

La cybersécurité est une sécurité comme une autre. Elle est assez nouvelle et elle a ses particularités, mais ne doit pas être considérée comme exceptionnelle. Dans le domaine industriel, les enjeux sont énormes et les risques en forte augmentation, car la cybersécurité industrielle constitue un nouveau terrain d'exercice pour les hackers. Les enjeux concernent la disponibilité de l'outil de production, les aspects réglementaires, techniques, et touchent à la sécurité des personnes et des biens. Une attaque portée sur les sites Seveso peut s'avérer dangereuse, ou entraîner de lourdes pertes économiques pour les processus critiques, à la manière du malware NotPetya qui a causé des milliards d'euros de dégâts. N'importe quel site industriel ou infrastructure critique peut être concerné.

Challenge^s

Comment Cybelius répond à ces problématiques ?

On ne peut pas changer radicalement un système d'informatique industrielle : notre proposition est de mettre de la protection autour et au cœur du système. Le processus de mise en sécurité, sur lequel nous nous positionnons, repose sur des mesures organisationnelles et techniques.

Nous proposons dans un premier temps une évaluation détaillée de la situation : cette ce « point zéro » est essentiel pour déterminer les mesures adaptées au client. Nous effectuons ensuite la mise en sécurité, en établissant une sorte de muraille informatique autour du système industriel. Nous travaillons de façon à laisser aux exploitants la souplesse dont ils ont besoin pour poursuivre leurs activités.

Enfin, nous collaborons avec la direction des services d'informations du client pour surveiller ce qu'il se passe au sein du système, vérifier que les mesures fonctionnent bien et apporter tous les indicateurs, rapports et alertes pour prévenir les menaces. Nous obtenons les informations via la surveillance autour et à l'intérieur du système, au moyen d'une sonde. Nous utilisons des technologies de détection d'intrusion développées par Cybelius, innovantes et brevetées.

De quelle façon vous démarquez-vous ?

Nous prenons en main la problématique du client et nous l'accompagnons sur le long terme. Nos solutions sont toujours à la pointe car nous détenons à la fois une véritable expertise en informatique industrielle et nous nous informons continuellement sur les évolutions des menaces. Notre offre n'a pas d'équivalent : nous sommes à la fois prestataires de services, intégrateurs de solutions et éditeurs de produits en propre.

Ce qui nous importe, c'est de toujours proportionner les mesures de sécurité aux enjeux. C'est pourquoi nous appliquons notre méthode APERO : Analyse Pour l'Evaluation des Risques Opérationnels. Nous cherchons à comprendre les risques et proposer les mesures de cybersécurité parfaitement adaptées, efficaces et à moindre coût. Tous nos clients sont très satisfaits de cette approche et nous avons la chance de compter parmi eux de gros industriels et de grands opérateurs, qui nous font confiance pour sécuriser leurs sites. Nous faisons déjà de l'export et nous revendiquons l'importance de s'ouvrir sur l'Europe : ses marchés sont actuellement plus matures que les marchés français. Cybelius est née grâce aux subventions du programme de recherche Horizon 2020, et nous ouvrons prochainement une filiale dans un pays européen.

Challenge^s

Comment Cybelius s'adapte en cette période de crise sanitaire ?

Nous avons rendu une grande partie de nos services accessibles à distance et nous minimisons les temps d'échange avec les clients. Ils sont importants pour comprendre et s'adapter aux systèmes mais notre équipe a suffisamment d'expérience pour aller à l'essentiel. Comme les mesures sanitaires prises contre l'expansion du virus, Cybelius applique des gestes barrières sur les systèmes informatiques. Notre priorité aujourd'hui est d'assurer le bon fonctionnement des sites industriels en limitant leurs dépenses. Nous sommes capables d'intervenir et sécuriser les systèmes rapidement, en quelques jours à quelques semaines.

Enfin, Cybelius a mis en place des formations à distance, qui vont de la sensibilisation à l'expertise, pour promouvoir l'hygiène informatique, car le facteur humain reste la plus grande force ou la plus grande faiblesse d'une protection.

<http://www.cybelius.fr/nos-solutions/crise-sanitaire-et-cybersecurite/>

<https://www.linkedin.com/company/cybelius-industrial-cyber-security>

0472418386



Vous avez dit "souveraineté économique" ? La preuve avec Sesame IT et Cybelius

SDBR News, 23 Juin 2020

[Sesame IT](#) et [Cybelius](#), deux start-up françaises expertes en cybersécurité dédiées à la détection d'attaques de réseau ont décidé de joindre leurs forces afin de développer une nouvelle sonde durcie.

Nous avons rencontré leurs dirigeants :

- Audrey Gayno-Amedro (CEO de Sesame IT)
- Frédéric Planchon (CEO de Cybelius)

AUDREY GAYNO-AMEDRO : CEO SESAME IT

SDBR News : Le Comcyber, l'Agence Innovation Défense et la DGA avaient lancé en 2019 le défi «deceptive Security*», visant à faire émerger une solution innovante et expérimentale pour faciliter l'analyse des cyber-attaques. Lors du FIC 2020, Sesame IT a été récompensée par un prix pour son démonstrateur Loki. Parlez-nous de Sesame IT...



Audrey Gayno-Amedro : Sesame IT a été créée en 2017 par Jérôme Gouy et moi. Nous avons tous deux une longue expérience dans l'Interception Légale de Télécommunications et une bonne expertise de la sécurité de l'IT et des Réseaux. Nous sommes rompus aux techniques d'analyse et d'extraction de données, dans les réseaux à très forts débits, et fortement sensibilisés aux conséquences des cyberattaques dirigées contre les opérateurs d'importance vitale (OIV). Nous avons donc entrepris de développer une solution de « haute fiabilité », une sonde durcie en profondeur, à la fois pour répondre aux besoins de la Loi de Programmation Militaire (LPM) mais aussi pour continuer de participer à la protection de la souveraineté de notre pays. Il a fallu 2 ans en Recherche et Développement pour créer cette nouvelle sonde « Jizô » qui est aujourd'hui en cours de qualification par l'ANSSI. Sesame IT est une start-up fondée pour développer un nouveau produit ciblé dès l'origine sur la détection d'attaques réseau. Nous sommes « Pure Player » en cybersécurité, ce qui nous différencie de beaucoup d'autres acteurs du marché.



SDBR News : En matière de sonde souveraine, nous avons suivi les aléas de la compétition, auprès de l'ANSSI, entre d'autres acteurs français. Pensez-vous que Sesame IT puisse être un outsider avec la sonde Jizô ?

Audrey Gayno-Amedro : Exactement, nous sommes un outsider ! Lorsque, courant 2018, nous avons demandé à l'ANSSI quelles étaient ses attentes en matière de sonde, nous sommes arrivés à la conclusion que les équipements sur lesquels nous travaillions pour faire de l'interception légale, avec des débits très importants et de la sécurité autour, étaient proches. Donc nous avons décidé de développer une sonde prenant en compte de façon native les exigences de l'ANSSI et non pas d'adapter un matériel existant à ses demandes... La start-up a débuté à deux personnes et compte aujourd'hui treize personnes qui ont travaillé sur la sonde adaptée aux réseaux IT en cours de qualification à l'ANSSI. Sans attendre la fin du processus de qualification de l'ANSSI, toujours un peu long, nous travaillons sur la phase II de notre projet qui est d'apporter ce protocole de sécurisation sur les réseaux industriels et IoT.

SDBR News : Avant d'aborder votre collaboration avec Cybelius et de parler des réseaux industriels, pouvez-vous me dire ce que la sonde de l'outsider Sesame IT a de plus ou de mieux que les autres sondes souveraines déjà identifiées ?

Audrey Gayno-Amedro : Il y a des différences majeures sur la structure du produit, même si les objectifs des différentes sondes sont les mêmes car ayant été toutes nourries aux exigences de l'ANSSI. Comme je vous le disais, nous avons pris en compte, dès le début de sa conception et dans l'architecture logicielle, le besoin de durcissement de la sonde au lieu d'essayer de durcir un produit du marché. C'est déjà ce qui explique notre rapidité à avoir pu présenter un produit opérationnel à l'ANSSI. En outre, la structure de notre produit est très efficace et tourne sur un seul serveur en « stand alone ». C'est un avantage pour l'utilisateur mais aussi au regard des contraintes de déploiement, car cela évite la surcharge de flux dans le réseau pour les renvoyer d'un équipement à un autre. Peut-être est-ce pour cela que l'ANSSI nous a fortement encouragés à développer la sonde « Jisô » ? Nous avons des POC qui tournent chez des prospects, mais nous attendons la qualification ANSSI pour débiter réellement sa commercialisation.



SDBR News : Que vient faire Cybelius dans un partenariat avec Sesame IT ?

FRÉDÉRIC PLANCHON : CEO CYBELIUS

Frédéric Planchon : Nous avons en effet une origine très différente, puisque nous travaillons depuis 2002 dans l'ingénierie industrielle et en 2010 nous avons rajouté la dimension cybersécurité à nos activités : Cybelius assure donc la sécurité d'installations et d'infrastructures industrielles, de l'évaluation, à la mise en sécurité ainsi que la surveillance en temps réel des systèmes industriels. Nous n'étions pas tournés vers la problématique d'une sonde souveraine mais nous avons reçu en 2015 une subvention européenne pour pouvoir développer une sonde de surveillance d'un système OT : vérifier le fonctionnement et le comportement du système industriel dans ses moindres détails et détecter les premiers signes des attaques avant que les dégâts ne soient occasionnés. Nous avons pu développer des algorithmes applicables aux SCADA, ce qui est une vraie attente des industriels. Notre maturité en matière de surveillance des réseaux industriels nous amène aujourd'hui à nous intéresser au marché régalien français. Le hasard du FIC 2020 nous a mis en contact avec les dirigeants de Sesame IT et nous avons estimé, les uns et les autres, que nos complémentarités pouvaient devenir un atout concurrentiel.

Audrey Gayno-Amedro : C'est en effet lors du FIC en janvier dernier que nous avons commencé à parler Frédéric et moi. Notre sonde est prête pour les réseaux IT mais il y a un vrai besoin pour les réseaux industriels, critiques ou non critiques. Frédéric et son équipe étant très pointus sur ces questions de réseaux OT, il nous a semblé comme une évidence que nous devions travailler avec des experts du monde industriel pour cette partie. Nous allons transposer pour l'OT des éléments que nous avons développés pour l'IT. Nous saurons à l'inverse embarquer tous les algorithmes d'intelligence artificielle développés par Cybelius dans notre sonde, l'amener à un niveau de sécurisation élevée et pouvoir ainsi présenter à l'ANSSI une sonde durcie IT – OT combinant détection sur pattern et analyse comportementale. C'est une aventure passionnante...

SDBR News : Aujourd'hui vous communiquez sur un protocole d'accord. Est-ce que ce protocole va déboucher sur une structure commune ?

Audrey Gayno-Amedro : Nous sommes deux sociétés d'ingénieurs, donc la première étape de notre travail en commun consiste à faire des tests et à construire une solution qui fonctionne très bien. Aujourd'hui, notre relation est donc très technique. Si nous communiquons, c'est que nous avons une conviction sur ce que nous allons faire. Ce partenariat répond à une forte demande des clients de type OIV (Opérateur d'Importance Vitale), c'est-à-dire des organisations privées ou publiques qui ont été identifiées par l'Etat comme ayant des activités indispensables pour le pays et qui attendent d'autres solutions que celles que le marché leur propose.





Frédéric Planchon : Nous sommes dans un microsysteme intéressant et, en toute immodestie, je pense que nous avons ensemble les capacités à créer techniquement un très beau produit, à la technologie très innovante, avec une complémentarité entre IT et OT, ce que personne ne fait au monde à notre connaissance, et une complémentarité sur l'analyse comportementale et sur la détection sur pattern, rarement intégrées sur le même outil. Entre ce que nous avons aujourd'hui qui est fonctionnel et la R&D amont qui est dans nos cartons, nous avons la capacité à pouvoir prendre une avance forte sur des pays leaders en cybersécurité. En matière de détection d'intrusion, le combat réside toujours entre l'épée et le bouclier. En cybersécurité, depuis des années, les acteurs suivent toujours les attaquants qui courent devant ! Aujourd'hui j'ai envie de dire « ça suffit », car nous avons un bouclier qui va être plus fort que l'épée, parce que notre technologie n'est pas suiveuse et que nous avons des technologies que les attaquants n'ont pas, donc nous pouvons être plus fort qu'eux. Cette solution de technologie 100% française sera commercialisée début 2021, auprès des grands clients français dès que l'ANSSI se sera prononcée. Ensuite, si les clients OIV nous suivent, il pourra y avoir une belle aventure industrielle à l'international également.

Audrey Gayno-Amedro : Nous sommes attachés à la valeur de ce qui est fait en France et, pendant la crise sanitaire, nous avons pu constater que tous les outils utilisés pour communiquer professionnellement pendant le confinement étaient finalement étrangers. Nous considérons qu'il y a quelque chose à faire pour ramener en France des creusets industriels, car nous avons de grandes capacités techniques. Donc nous sommes très motivés à participer à une ambition technologique et à une aventure patriote.

Cybelius et Sesame IT préparent leur sonde réseau durcie pour IT et OT

La première jeune pousse va apporter son expertise des systèmes industriels et des protocoles qui leurs sont spécifiques. La seconde va ainsi étendre le périmètre d'utilisation de sa sonde durcie Jizô, basée sur Suricata et en cours de qualification par l'Anssi.

Par Valéry Marchive. Publié le 18 juin 2020

Cybelius et Sesame IT viennent de nouer un partenariat pour développer ensemble une sonde réseau durcie susceptible de couvrir aussi bien les domaines IT qu'OT – et donc le monde des systèmes industriels (ICS/Scada). Dans un communiqué de presse, les deux jeunes françaises expliquent vouloir ainsi répondre « à une forte demande » des entreprises ayant été désignées opérateur d'importance vitale (OIV), et donc soumises à des exigences toutes spécifiques. La commercialisation de cette sonde est prévue pour le début 2021.

Sans surprise, le socle matériel sera la sonde Jizô développée par Sesame-IT et en cours de certification par l'Agence nationale pour la sécurité des systèmes d'informations (Anssi). Celle-ci est basée sur le système de détection d'intrusion (IDS) Suricata – à l'instar des deux sondes déjà qualifiées, Cybels Sensor de Thales, et les produits Gatewatcher. A l'automne dernier, Eric Leblond, fondateur de Stamus Network, et l'un des principaux développeurs de l'OISF, l'organisme porteur du développement de l'IDS, [nous expliquait à l'automne dernier](#) que cela ne relève pas vraiment du hasard : pour respecter le cahier des charges de l'Anssi au sujet des sondes souveraines, « la solution la plus simple pour y arriver était d'utiliser Suricata ».

De son côté, Cybelius va apporter son expertise des environnements industriels. La jeune pousse dispose d'ailleurs déjà d'une sonde réseau spécifique à ceux-ci, CyPres. Mais comme l'explique Frédéric Planchon, Pdg de Cybelius, elle est aujourd'hui principalement utilisée dans des phases d'évaluation, pour des audits des flux, des machines ou encore de la cartographie : la sonde est donc généralement déployée de manière très temporaire.

Les capacités analytiques – et notamment comportementales – développées pour Cypres, avec toute la connaissance protocolaire spécifique au monde des ICS/Scada que cela implique, vont être embarquées comme un traitement ad hoc sur Jizô. Pour mémoire, Vincent Nicaise, alors directeur marketing de Cybelius, nous expliquait, début 2018, [travailler avec Inria à l'adaptation d'algorithmes d'apprentissage automatique](#) pour ajouter justement la couche de détection de dérive comportementale.

Mais quel avenir Cybelius réserve-t-il désormais à CyPres ? Frédéric Planchon explique que cette sonde « a vocation à exister, notamment pour les besoins industriels ne nécessitant pas de produits qualifiés », auxquels il est donc possible de répondre avec une grille tarifaire plus légère. Et cela jusqu'à l'intégration de CyPres... sur CyFence, cette armoire pouvant embarquer différents services à la carte.

Cybelius et Sesame IT joignent leurs forces pour proposer une sonde durcie pour les réseaux critiques

Global Security Mag – juin 2020 par [Marc Jacob](#)

Cybelius et Sesame IT, deux start-up françaises dédiées à la cybersécurité ont signé un protocole d'accord ouvrant la voie à un développement commun pour un produit de type sonde durcie IT – OT. Cette nouvelle solution couvrira les domaines IT et OT, combinant détection sur pattern et analyse comportementale.

Sesame IT et Cybelius, deux start-up françaises expertes en cybersécurité dédiées à la détection d'attaques de réseau ont décidé de joindre leurs forces afin de développer une nouvelle sonde durcie. Ce nouveau produit servira de bouclier face à l'augmentation d'attaques informatiques toujours plus sophistiquées et permettra d'atténuer leur impact sur le fonctionnement des sociétés et d'augmenter notablement leur résilience. Il sera également le seul produit français à couvrir les domaines IT et OT en un seul produit unifié.

La sonde bénéficiera des qualités propres de la sonde durcie en profondeur Jizô de Sesame IT (comprenant des processus de hardening software avancés et en cours de qualification par l'ANSSI), et des algorithmes avancés d'IA avec analyse comportementale de Cybelius, adaptés aux protocoles industriels.

Ce partenariat répond à une forte demande des clients de type OIV (Opérateur d'Importance Vitale), c'est-à-dire des organisations privées ou publiques qui ont été identifiées par l'Etat comme ayant des activités indispensables pour le pays.

Cette solution de technologie 100% française sera commercialisée début 2021 en France et à l'international.

Cybersécurité industrielle : Gfi et Cybelius lancent une nouvelle solution

Global Security Mag - février 2020 par [Marc Jacob](#)

En pleine transformation digitale, le secteur industriel doit répondre aux nouveaux impératifs de cyberdéfense auxquels ses acteurs sont confrontés alors qu'ils restent encore démunis de moyens de protection. Pour y répondre, Gfi, acteur majeur des services et solutions numériques et spécialiste des enjeux de l'Industrie 4.0, et Cybelius, spécialiste de la cybersécurité industrielle, lancent le « CyFENCE & SIEM service ». Cette solution inédite sur le marché garantit aux directions des systèmes d'information une véritable vision sur leur activité afin de mieux piloter la sécurité de leurs installations.

L'Industrie 4.0 est une nouvelle génération d'usines connectées, robotisées et intelligentes, animées par l'émergence de nouvelles technologies. Pour autant, cette révolution qui transforme le paysage industriel ouvre également la voie à de nouveaux risques, les cyberattaques en premier lieu. Les pirates ciblent désormais jusqu'aux automates et contrôleurs de sécurité et menacent l'appareil de production. Les conséquences sont souvent considérables. Récemment des cyberattaques ont obligé des industriels à arrêter leur production. Et l'Union Européenne a par ailleurs adopté le Cybersecurity Act en juin dernier, considéré comme essentiel pour renforcer la sécurité du marché numérique européen.

Fruit d'un partenariat engagé en janvier 2019 entre deux entreprises françaises, cette nouvelle solution porte sur le développement d'une offre globale IT et OT, dans le domaine de la cybersécurité. Une utilisation simple, facteur de gains réels pour les industriels. Reposant sur un système de mise en oeuvre rapide, environ 20 jours par site, « CyFENCE & SIEM service » propose une dizaine de fonctions de sécurité pour les industriels quelle que soit leur dimension.

Communiqué de presse & livres blancs



Seclab et Cybelius annoncent un partenariat stratégique

Lyon, mardi 16 février 2021 – Seclab, le spécialiste de la protection des infrastructures critiques et stratégiques, et Cybelius, l'un des leaders de la cybersécurité industrielle 4.0, officialisent un partenariat technique et commercial. À travers cette annonce d'envergure, les deux partenaires souhaitent proposer une offre unique permettant de sécuriser efficacement les infrastructures des industriels.

Dans ce contexte, à travers cette offre commune et packagée qui associe les technologies CyFENCE de [Cybelius](#) et Sec-XN de [Seclab](#), il sera possible de créer un espace de confiance sur les systèmes existants et de l'intégrer dans la politique de sécurité du client.

Concrètement, grâce à Seclab, Cybelius pourra améliorer les performances de son offre en ajoutant la rupture protocolaire, tout en gardant le principe d'une intégration de l'ensemble des mesures de sécurité. Ainsi, la société sera en mesure d'adresser le marché des systèmes extrêmement sensibles en ajoutant de la sécurité, de la connectivité, de l'exploitabilité et de la maintenabilité. Seclab de son côté pourra diffuser sa technologie au plus grand nombre et permettre à ses clients de cloisonner et protéger leurs réseaux. De ce fait, les scans et attaques réseau sont alors sans effet pour les clients et ils seront également protégés contre d'éventuelles fuites de données.

L'alliance entre Cybelius et Seclab offre donc une réponse concrète et opérationnelle à différents cas d'usage : sécurisation des liaisons critiques (mises à jour, téléconduite, administration, etc.), mise en œuvre d'un bastion interne pour les informations sensibles (filtrage utilisateurs, authentification) ou encore création d'une zone de protection pour les sauvegardes et les logs.

Xavier FACELINA, CEO de Seclab « Cette alliance stratégique avec Cybelius va nous permettre d'élever encore plus le niveau de sécurité des industriels qui sont de plus en plus exposés au risque cyber. La complémentarité de nos offres nous permettra d'apporter une réponse technique et commerciale commune à nos clients qui pourront ainsi s'appuyer sur des solutions de confiance 100 % françaises pour sécuriser leurs opérations et ne pas être impactés dans leur production par exemple. »

Frédéric PLANCHON, Président de Cybelius : "J'ai fondé Cybelius en 2017 avec la vision d'un écosystème au fait des particularités de l'industrie, plus encore que sur nos technologies innovantes. Ce partenariat en est une belle concrétisation. Et l'intégration de Sec-XN dans CyFENCE montre déjà une première réalisation exemplaire, qui n'a pas d'équivalent sur le marché."



À propos de SECLAB :

SECLAB a été fondé en 2011 pour fournir une solution à une entreprise locale de production d'énergie nucléaire qui n'avait pas pu trouver de produit pour améliorer sa technologie de sécurité actuelle afin de répondre aux nouvelles exigences du gouvernement. Avec leur aide et leurs conseils sur les exigences, SECLAB a développé le "Secure Xchange Network", qui est maintenant un élément clé de leur technologie "Electronic AirGap". Depuis, SECLAB fourni des solutions à des entreprises du monde entier et dans différents secteurs d'activité.

À propos de CYBELIUS :

Fondée par des experts en informatique industrielle et en cybersécurité, Cybelius assure la sécurité des installations et infrastructures industrielles. De l'évaluation, à la mise en sécurité ainsi que la surveillance en temps réel des systèmes industriels, les solutions Cybelius couvrent tout le processus de la cybersécurité, avec une offre produits et services en phase avec les forts besoins du marché.

Contact Presse :

Franck TUPINIER

TEL : 06 74 68 37 93

Cybelius et Sesame IT joignent leurs forces pour proposer une sonde durcie pour les réseaux critiques

Ce nouveau produit disposera de fonctionnalités de détection avancées pour l'IT et l'OT.

Paris, mercredi 17 juin 2020 - Cybelius et Sesame IT, deux start-up françaises dédiées à la cybersécurité ont signé un protocole d'accord ouvrant la voie à un développement commun pour un produit de type sonde durcie IT – OT. Cette nouvelle solution couvrira les domaines IT et OT, combinant détection sur pattern et analyse comportementale.

[Sesame IT](#) et [Cybelius](#), deux start-up françaises expertes en cybersécurité dédiées à la détection d'attaques de réseau ont décidé de joindre leurs forces afin de développer une nouvelle sonde durcie. Ce nouveau produit servira de bouclier face à l'augmentation d'attaques informatiques toujours plus sophistiquées et permettra d'atténuer leur impact sur le fonctionnement des sociétés et d'augmenter notablement leur résilience. Il sera également le seul produit français à couvrir les domaines IT et OT en un seul produit unifié.

La sonde bénéficiera des qualités propres de la [sonde durcie en profondeur Jizô](#) de Sesame IT (comprenant des processus de hardening software avancés et en cours de qualification par l'ANSSI), et des algorithmes avancés d'IA avec analyse comportementale de Cybelius, adaptés aux protocoles industriels.

Ce partenariat répond à une forte demande des clients de type OIV (Opérateur d'Importance Vitale), c'est-à-dire des organisations privées ou publiques qui ont été identifiées par l'Etat comme ayant des activités indispensables pour le pays.

Cette solution de technologie 100% française sera commercialisée début 2021 en France et à l'international.

Audrey Gayno-Amédéo, CEO SESAME IT, commente : « Nous avons toujours pensé que pour mettre au point le meilleur outil répondant à la demande des réseaux industriels, il fallait joindre nos forces et nos expériences à celles d'une expertise de l'informatique industrielle. L'association avec Cybelius a été une évidence. Les performances de notre sonde Jizo vont s'exprimer pleinement en OT grâce à leur maîtrise reconnue des réseaux industriels et les algorithmes très performants qu'ils ont mis au point. »

Frédéric Planchon, CEO de CYBELIUS ajoute : « La fragilité actuelle de l'informatique industrielle en fait LE secteur important, voire vital, de la cybersécurité. Le rapprochement IT et OT est la seule voie d'avenir, mais les particularités du monde industriel restent un enjeu fort. Nous avons toujours pensé que cette dualité serait à la fois technologique et commerciale. Le partenariat avec SESAME IT est particulièrement adapté pour CYBELIUS, car notre connaissance et notre culture du monde industriel ne suffisent pas pour devenir numéro 1. La combinaison de nos technologies pourrait nous permettre de devenir une référence mondiale. »

À propos de SESAME IT :

La société a été fondée en 2017 par Audrey Gayno-Amedro et Jérôme Gouy, deux experts sécurité et réseaux, ayant une longue expérience dans l'Interception Légale de Télécommunications. Rompus aux techniques d'analyse et d'extraction de données dans les réseaux à très forts débits, et fortement sensibilisés aux conséquences des cyber-attaques dirigées contre les OIV, ils ont entrepris de développer une solution 'haute fiabilité', à la fois pour répondre aux besoins de la Loi de Programmation Militaire, mais aussi pour continuer de participer à la protection de la souveraineté de notre pays. Pure Player Cyber-sécurité, Sesame IT est dédiée à la détection d'attaques réseau.

À propos de CYBELIUS :

Fondée par des experts en informatique industrielle et en cybersécurité, Cybelius assure la sécurité des installations et infrastructures industrielles. De l'évaluation, à la mise en sécurité ainsi que la surveillance en temps réel des systèmes industriels, les solutions Cybelius couvrent tout le processus de la cybersécurité, avec une offre produits et services en phase avec les forts besoins du marché.

Contact Presse :

Sylvia Guirand

sylvia.guirand@gmail.com









































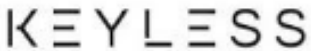





















06 20 86 78 00

Nos livres blancs à télécharger :

- [Changement d'approches sur les données en cybersécurité industrielle](#), Février 2020
- [L'humain dans la cybersécurité industrielle](#), Mars 2020

Apparition de Cybelius sur des radars en cybersécurité

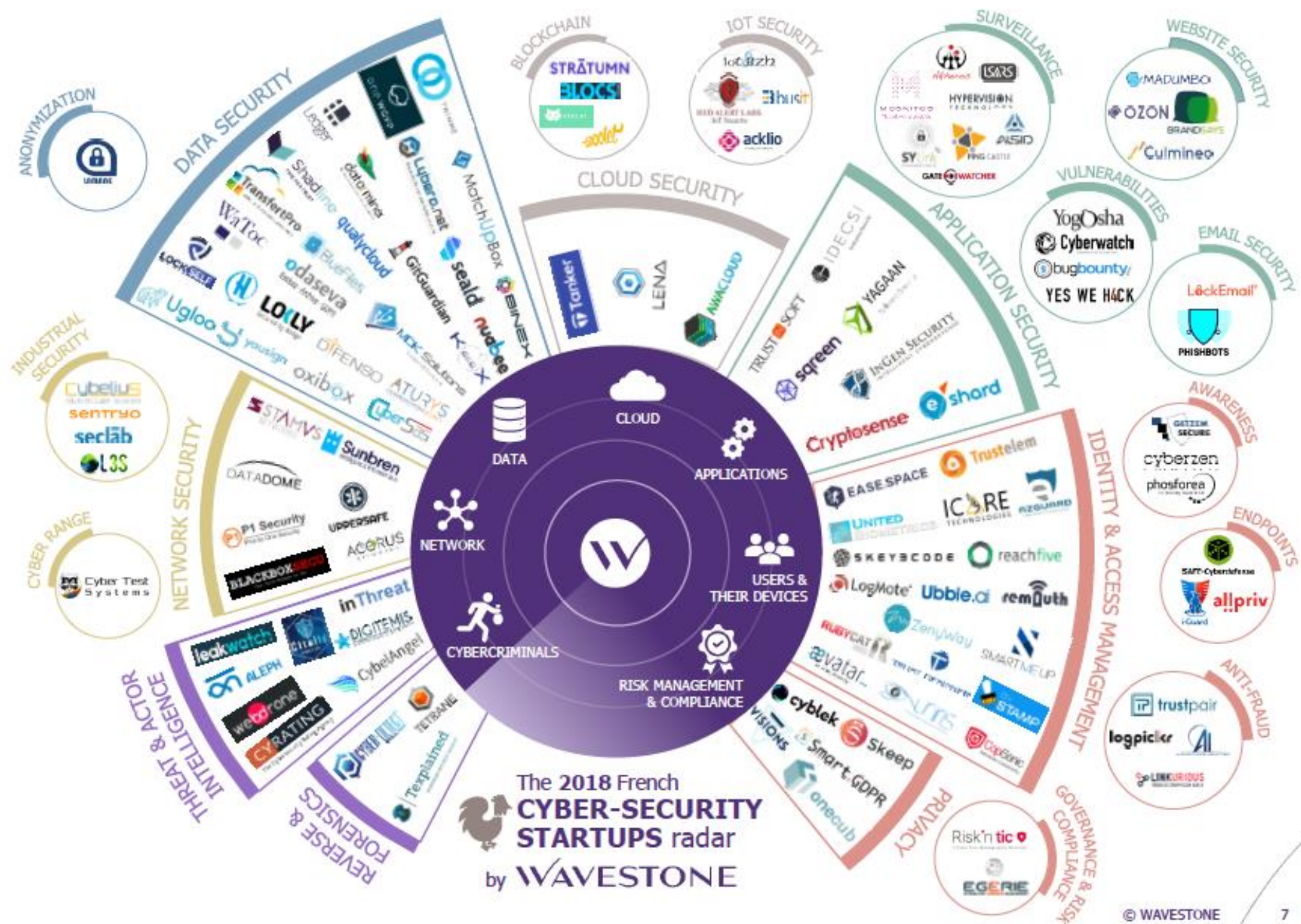
Cybelius apparaît dans la Watchlist du Cybersecurity Scale-up Mapping V2.0 de 2020 par European Champions Alliance, dans la catégorie « Service ».

EUROPEAN CYBERSECURITY MAPPING: WATCHLIST		
Satisfied with this mapping? Write to welcome@european-champions.com		
Application Security	Service	Data Protection
 XignSys  NOVALYS  YES WE HACK  PROVE & RUN  cryptosense  YogOsha  Watcha  OGO	 ALEPH  BEWARE CYBERLABS  Arkhineo  Cybelius Industrial Cyber Solutions	 comcrypto  Search Guard  LOLLY  WaToo  Shadline  EGERIE  seald
Cloud Security	<p>Powered by</p>  European Champions Alliance <p>In collaboration with</p>  VECTORPILOT	Cryptography
 EGERIE  Shadline  Outpost24  cloud		 Watcha  seald  SECURE-iC  cryptosense
IoT, Embedded & Industrial Systems		Security Engineering & Endpoint/Mobile Security
 acklio  TRUSTED OBJECTS  EUSTAMP		 AXBX  SECURE-iC  i-Guard
Identity & Access Management	Security Operation	Threat Management
 XignSys  intelliCard solutions ag  NEOWAVE  unikname CARE  IDEE  KEYLESS  NEXIS	 Cyberwatch  EVINA	 FRAUDBUSTER  EGERIE  ALEPH  ENGINSIGHT  webdrone  CONNECTLINE  OZON  TENZIR  i-Guard  KUB  EVINA  SERINUS  BEWARE CYBERLABS  XNETSOLUTIONS  MainDefense  6cure
	Stenography & Watermarking	Email Security
	 WaToo	 comcrypto

Cybelius apparaît dans le radar des startups cybersécurité françaises 2020 de Wavestone, dans la catégorie « Network Security ».



Cybelius apparaît dans le radar des startups cybersécurité françaises 2018 de Wavestone, dans la catégorie « Industrial Security ».



Publications LinkedIn

- [« Les 5 fonctions nécessaires pour sécuriser un système OT »](#)
- [« La sonde de détection d'intrusion CyPRES face aux attaques mondiales »](#)
- [« Cybelius dans la chaîne de valeur »](#)
- [« Vos systèmes industriels peuvent-ils contrer la Cyber Kill Chain ? »](#)
- [« Vulnérabilités détectées en 2020 sur l'environnement OT par Cybelius »](#)
- Vidéo sur la solution NP-View utilisée par Cybelius : [logiciel d'audit pour les systèmes industriels](#)
- Présentation des [solutions Cybelius](#)
- Présentation de la [sonde CyPRES à l'Institut de Recherche Technologique System X](#)
- Présentation de la solution [CyFENCE & SIEM Services](#)



Cybbelivus

Industrial Cyber Solutions