APPEL A PARTENAIRES POUR UN PROJET INNOVANT

2022

Personne à contacter

Louise POUPENEY
louise.poupeney@hydreos.fr

07 55 65 96 81

HYDREOS

Appel à partenaires pour un projet innovant

Qui sommes-nous ?

HYDREOS est le pôle qui fédère les acteurs de la filière de l'eau en Région Grand Est. Association au service de ses adhérents, HYDREOS met en relation les entreprises, les laboratoires de recherche, les organismes de formation et les acteurs du territoire, afin de favoriser le développement de projets innovants et ainsi d'accroître les performances du tissu économique local dans les métiers de l'eau.

Pourquoi un « Appel à partenaires » ?

L'objectif de cet appel est de porter à connaissance des collectivités les projets d'innovation en cours sur leur territoire dans le domaine de la gestion durable de l'eau**.**

En prenant part à un projet d'innovation**,** les collectivités s'impliquent dans sa mise en œuvre et en retirent des bénéfices multiples : apport d'informations stratégiques (techniques, réglementaires, etc.), amélioration des connaissances, expérimentation sur leur territoire, formation des agents, visibilité en tant que collectivité innovante, etc.

Ces projets peuvent concerner tous les domaines liés à l'eau : eau potable, assainissement, eaux pluviales, eaux industrielles, eau agricole, génie écologique, etc.

Pas de taille ou de ressources minimales, chaque projet est différent et la collectivité recherchée répond à des critères spécifiques au projet. Les petites collectivités sont souvent les bienvenues !

Devenez partenaire d'un projet d'innovation et faites de votre territoire un précurseur dans le domaine de l'eau !

Ci-dessous, vous trouverez :

- Le descriptif de l'innovation, ainsi que de l'entreprise ou du laboratoire qui la porte
- Les critères sur lesquels est recherché le partenaire (taille, localisation, réseau, etc.)

Vous êtes intéressés par le projet ? Vous avez des questions ? Vous souhaitez impliquer votre territoire dans l'innovation ? Contactez-nous !

Louise POUPENEY à l'adresse **louise.poupeney@hydreos.fr** **ou au 07 55 65 96 81**

Appel à partenaires pour un projet innovant

Description du projet

Thématique :

Gouvernance globale de la cybersécurité des technologies opérationnelles d'une infrastructure de l'eau, régie par une collectivité : Détection, protection, réponse en temps réel contre les cyber-attaques

Porteur :

CyVault, est une société d'ingénierie en Cyberdéfense implantée à Strasbourg et filiale d'un groupe canadien. L'entreprise est spécialisée dans la conception, le déploiement et la protection des infrastructures critiques, y compris des réseaux d'eau, en s'appuyant sur des modèles de cyber-défense avancés, testés et éprouvés.

Objectifs et descriptif rapide :

Les organismes publics liés au secteur de l'eau prennent progressivement conscience du besoin d'assurer la **cybersécurité de leurs infrastructures critiques**, de leurs données sensibles et de leurs environnements opérationnels.

Il s'agit d'un enjeu considérable dans la mesure où les systèmes opérationnels de l'industrie de l'eau présentent plus du double des vulnérabilités de celles du secteur de la santé.

En effet, **le secteur de l'eau est loin d'être épargné** comme l'a rappelé le cas d'une réserve d'eau en Floride en février 2021. Très médiatisée, cette cyber-attaque a démontré le manque de sécurisation des équipements de cette station de traitement de l'eau. Le cybercriminel avait exploité un logiciel d'accès à distance, trop peu sécurisé et avait modifié le paramétrage en hydroxyde de sodium utilisé pour réguler le pH de l'eau potable. Un agent de la station qui avait constaté une anomalie de manière inopportune, avait réussi à corriger la concentration, évitant un drame pour les populations de la ville. Aucune alerte n'avait fait réagir le personnel car aucune protection n'avait été installée au niveau TO.

Beaucoup moins médiatisés, les services d'assainissement des collectivités publiques françaises font également l'objet de nombreuses cyber-attaques, à l'instar de celui de la commune d'Oloron-Sainte-Marie fin 2021. Profitant d'une faille dans le système de gestion automatisée des pompes de relevage de la station d'épuration, un groupe de hackers identifié a posteriori appartenant à un Etat, avait réussi à s'introduire dans le système d'information et à demander une rançon avant de détruire des données.

Bien que la sûreté des personnes ait toujours primé sur la protection des systèmes opérationnels dans le secteur de l'eau, les deux sujets sont désormais indissociables. Un problème de cybersécurité au sein d'une collectivité peut vite engendrer un problème de sûreté/salubrité au niveau local voire national dans certains cas.

Appel à partenaires pour un projet innovant

Ces exemples montrent qu'une élévation de la cyber sécurité des installations de traitement d'eau est nécessaire et urgente, encore plus dans un climat politique et économique tendu.

L'objectif sera donc de concevoir, déployer et opérer une architecture de cyber défense, sur mesure, pour les installations de traitement d'eau de la collectivité. Cette protection de cyber sécurité sera capable de s'intégrer avec tous les éléments de la station.

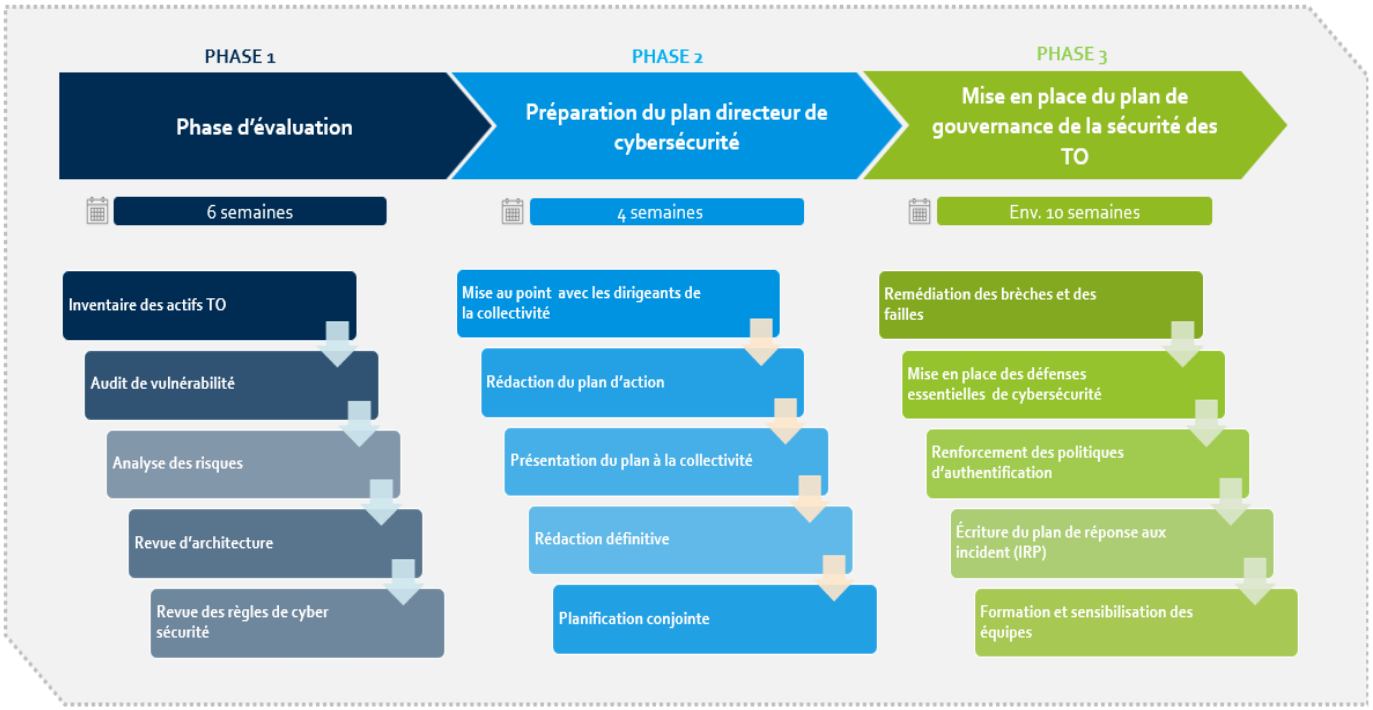
Notre solution basée sur la confiance zéro dans l'interconnexion entre le TI et le TO (Zero Trust Architecture) permettra une communication sécuritaire avec la zone TI. Le système de cyber protection sera interfacé avec un portail de posture et statut global cybersécurité temps réel pour fournir une visibilité à l'équipe TI de l'organisation.

Nous déploierons notre plate-forme MXDR pour la **prise en charge automatique des attaques**, en installant des contrôles de sécurité sur toutes les zones ICS (Industrial Control System). Enfin, l'ensemble sera relié à notre **CyberSOC pour la gestion des attaques critiques et leurs remédiations** (Surveillance, Détection, Réponse aux Incidents). Ce dispositif permet donc de superviser en temps réel les biens critiques de l'infrastructure et détecter toute action pouvant compromettre leur sécurité.

Cette méthodologie innovante dite "Integrated Morphic Cyber Defense" (IMCD) apportera à l'organisation **une protection, une détection ainsi qu'une réponse en temps réel contre les cyberattaques** actuelles et émergentes qui visent les réseaux (IT/OT/xIoT).

C'est pourquoi nous voulons à travers cet appel à partenaire, accompagner une collectivité publique, en charge de la gestion de l'eau potable et/ou de la collecte du traitement des eaux usées, dans la mise en place d'un système de cyber protection temps réel afin de réduire les risques opérationnels, financiers, et surtout humains liés aux cyber-attaques. Ce projet permet de démontrer la nécessité d'impartitionner la cyberdéfense des installations vers des équipes chevronnés et aguerris aux cyber menaces, en leurs offrant notre **modèle de "Cyber Defense as a Service" (CDaaS)**.

Calendrier :



Appel à partenaires pour un projet innovant

Financement :

Le coût est estimé à 25 000 euros pour une période de 1 an pour une couverture de 25 machines (ICS). Le prix pourra être ajusté en fonction du nombre réel de machines.

Lorsqu'un partenaire sera identifié, une recherche de financements pourra être lancée par le biais de l'Agence de l'Eau concernée, ou d'Appels à Projets ciblés.

Critères

Type de partenaire :

Collectivité disposant d'infrastructure(s) et d'équipement(s) pour la gestion et la distribution de l'eau potable

Taille :

Collectivité de taille Intermédiaire.

Implication

Rôle prévu dans le projet :

Projet entièrement géré par les équipes de CyVault :

- ✓ Chef de projet
- ✓ Architecture expert ICS
- ✓ Cyber analystes

Ressources internes nécessaires (estimées) :

- ✓ Interlocuteur / relais technique au sein de la collectivité ainsi que les chefs de services concernés lors des réunions de pilotage.
- ✓ Schéma d'architecture TO

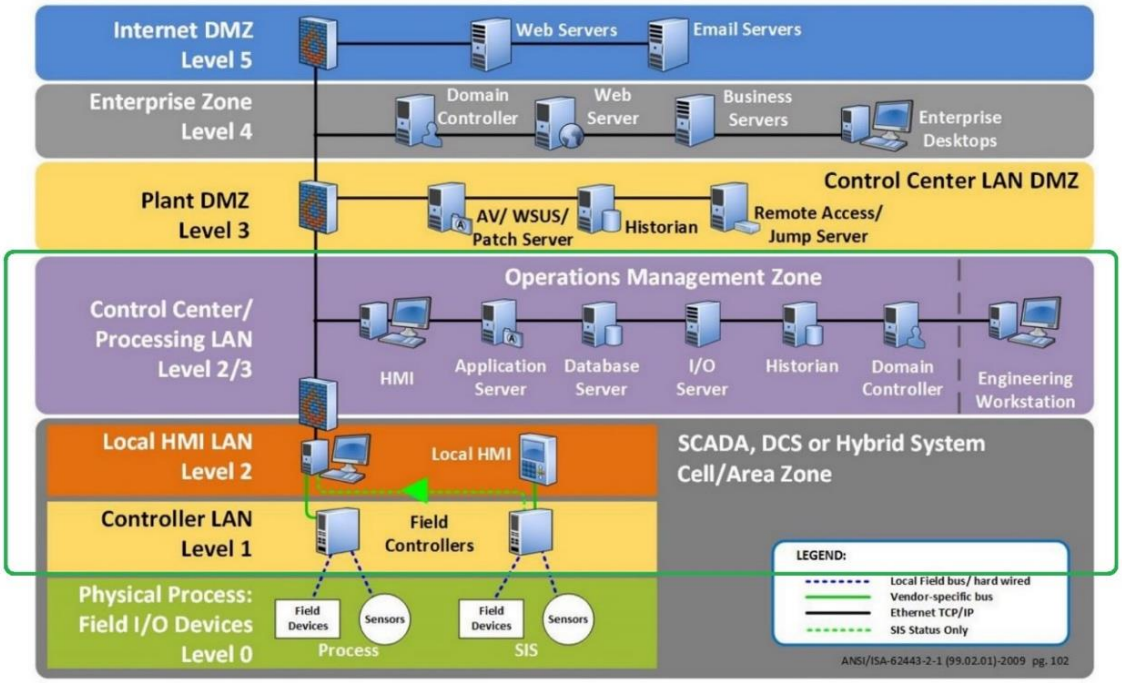
Appel à partenaires pour un projet innovant

Avantages retirés :

Les avantages retirés sont multiples :

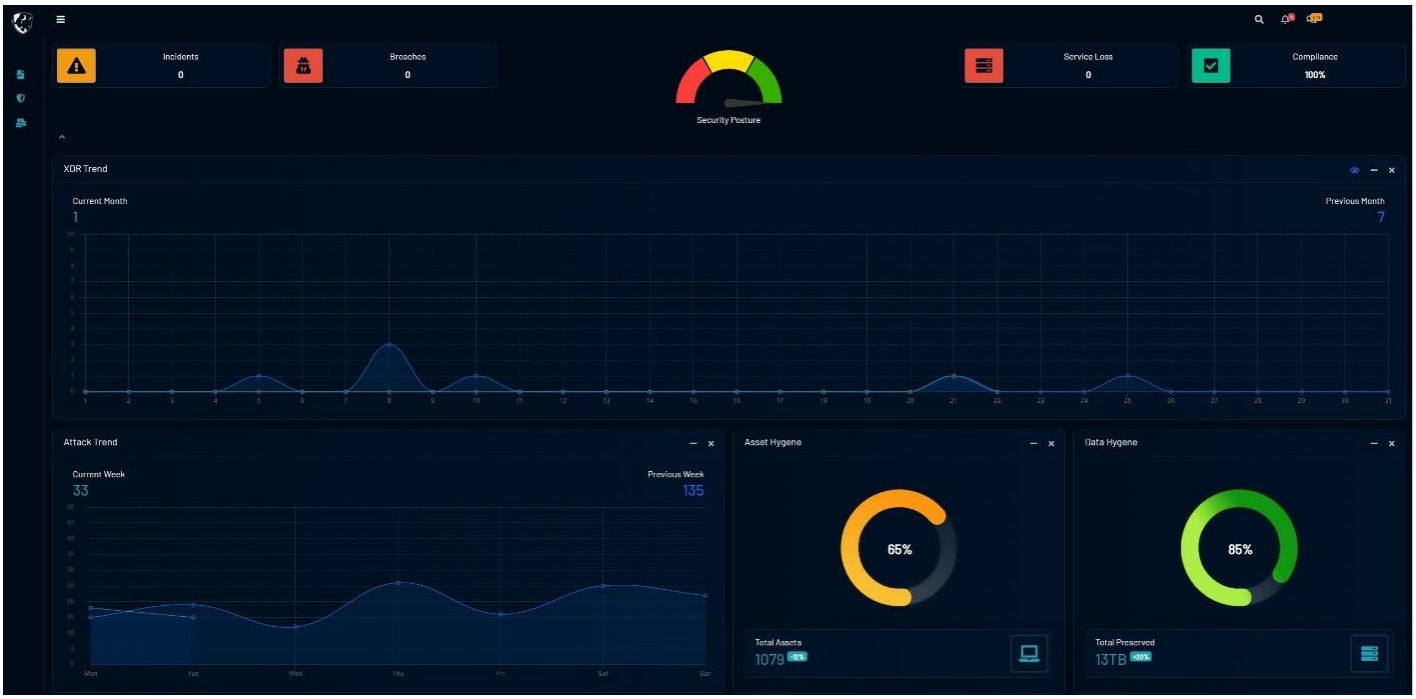
- ✓ Impartitionner la cyberdéfense et diminution des coûts d'exploitation
- ✓ Augmentation de la sécurité globale et minimisation du niveau de risque
- ✓ Assurer une continuité acceptable des services de distribution et/ou de traitement de l'eau
- ✓ Impact positif sur l'image de la collectivité
- ✓ Diminution des risques de sûreté (vies humaines)
- ✓ Service de support "4-Tier"
- ✓ Surveillance, détection, réponse aux incidents en temps réel
- ✓ Résilience accrue (ex : RPO - durée maximale de perte de données acceptée, RTO - durée maximale d'interruption admissible)

Annexes



Zone couverte par notre protection, détection et réponse aux incidents

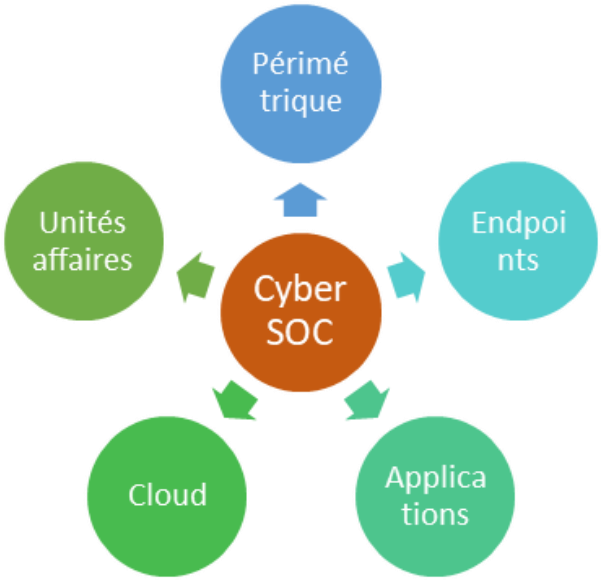
Appel à partenaires pour un projet innovant



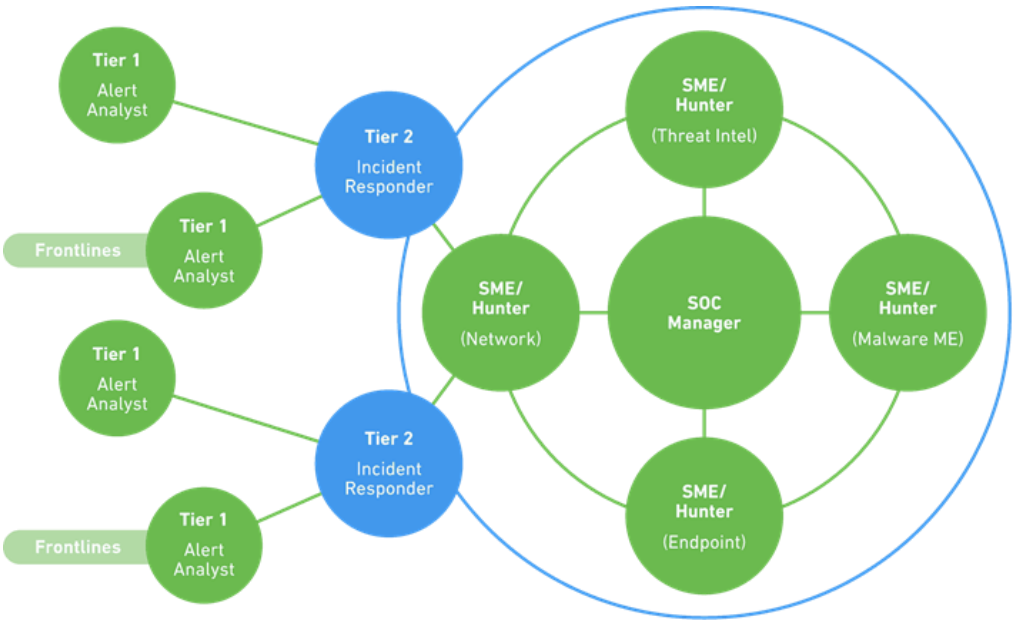
Exemple d'un tableau de monitoring temps réel

Photo de notre CyberSOC (Security Operations Center)

Appel à partenaires pour un projet innovant



Environnement technologique couvert par notre CyberSOC



Service de Support 4 Tiers :

***Niveau 1** – Opérateurs qui relèvent les alertes quotidiennes et font un premier diagnostic*
***Niveau 2** - Analystes sécurité qui réalisent une analyse détaillée et répondent aux incidents*
***Niveau 3** – Expert sécurité / Chasseur de menaces sollicités pour les incidents critiques*
***Niveau 4** – Directeur du SOC*