



### *Notre approche:*

*MimetICS reproduit les environnements industriels réels et leurs flux OT, afin de relier la cybersécurité aux réalités du terrain*

Développée par Adamante, MimetICS est une solution de simulation OT cyber reproduisant fidèlement le comportement des systèmes industriels, réseaux et protocoles.

Elle permet de valider les cas d'usage de détection, de former les équipes, et de tester des scénarios d'attaque ou de réponse dans un environnement sûr, reproductible et contrôlé. MimetICS génère un trafic industriel authentique et réagit aux perturbations, permettant l'évaluation d'IDS, la qualification d'outils SOC OT et la sensibilisation des opérateurs.

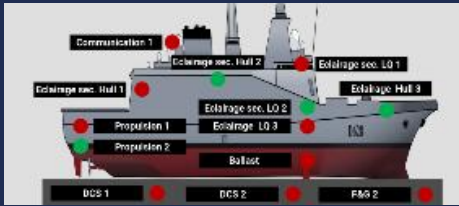
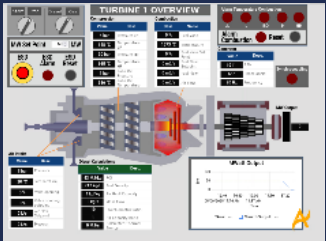
# MIMETICS

ADAMANTE  
CYBER

**SIMULATION OT RÉALISTE AU SERVICE DE LA  
CYBERSÉCURITÉ INDUSTRIELLE**

# MIMETICS

- ✧ **Simulation OT et comportement déterministe**
- ✧ **Reproductibilité totale des scénarios**
- ✧ **Intégration Hardware-in-the-Loop (PLC, routeurs, sondes)**
- ✧ **Compatible SOC OT, IDS, SIEM et plateformes CyberRange.**



- ✧ **Formation et sensibilisation**  
Exercices immersifs pour opérateurs, ingénieurs et SOC.
- ✧ **Tests de détection et IDS.**  
Validation de cas d'usage SOC OT dans un environnement réaliste.
- ✧ **Évaluation et benchmark de solutions.**  
Tests comparatifs et intégration d'outils de cybersécurité OT.
- ✧ **Scénarios d'attaque et trafic anormal.**  
Génération et observation de comportements OT dégradés.

# EXEMPLES DE PROJETS RÉALISÉS AVEC MIMETICS

Une plateforme commune, déclinée selon les besoins : détection SOC, formation, démonstration technique.



*TESTS SOC OT:* Valider les use-cases de détection et distinguer anomalies réelles / activité normale

- Validation de use-cases et d'alertes IDS dans un environnement OT simulé et déterministe.
- Connexion au SOC client, scénarios automatisés et collecte des résultats de détection.



*Démonstrateur de solutions OT:*  
*Démonstrateur de solutions OT.*

- Utilisation de la simulation pour présenter et tester leurs sondes et produits de cybersécurité industrielle.
- Reproduction de scénarios d'attaque et de détection sur des processus simulés.



*Partenariat CyberRange:* Fournir une base réaliste pour les entraînements et la démonstration client.

- Intégration de la simulation Adamante dans le CyberRange Airbus.
- Intégration dans leurs parcours de formation (LMS / mode gaming).



*Sensibilisation OT:* Sensibiliser opérateurs et managers aux risques.

- Environnement industriel simulé avec scénario d'attaque sur accès distant.
- Mise en situation d'opérateurs, ingénieurs et managers, analyse des réflexes face à l'incident.



*Partenariat & démonstration HIL:*  
*Démonstrateur de solutions OT.*

- Développement d'un démonstrateur mobile de simulation OT intégrant l'écosystème Weidmüller.
- Formations, salons et démonstrations conjointes en Hardware-in-the-Loop.