BRETAGNE SAILING VALLEY

Les Sailing Cafés #4

Cybersécurité & course au large

Jeudi 27 juin 2024
9h00 - 10h00

Webinaire en ligne

BRETAGNE DÉVELOPPEMENT INNOVATION

Région BRETAGNE

Panorama de la cybersécurité maritime

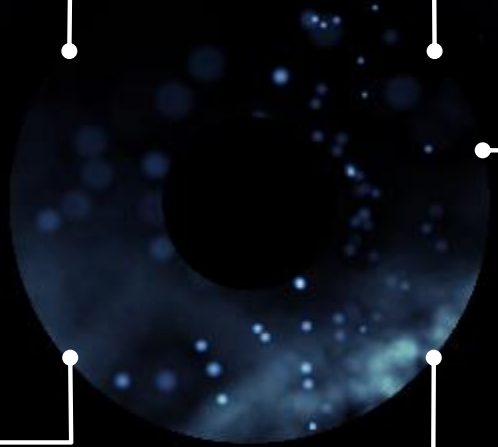

THREAT INTELLIGENCE
DRIVEN CYBERSECURITY

15 ans d'expérience

Différents clients :
Administration, CAC40,
SBF120, ETI & PME

3 Labels cyber

PASSI (RGS)
TF-CSIRT
ExpertCyber



Pure Player CYBERSÉCURITÉ

Paris, Rennes, Toulouse

5

Spécialités
Audit & Conseil
Threat Intelligence
SOC & CERT

+70 Consultants

10 langues maîtrisées
dont le russe, le chinois,
l'arabe, et l'ukrainien

CERT

Le OWN-CERT est composé de deux équipes : CTI & DFIR. L'équipe CTI effectue une veille continue de l'actualité des SSI, met en place des bulletins de sécurité contextualisés et
construit une cartographie des risques de chaque secteur en fonction des menaces et des acteurs. Nos équipes DFIR fournissent un soutien continu
à la demande ou sur site lorsque la gestion des incidents de sécurité, l'investigation numérique et l'analyse des codes malveillants sont nécessaires

SOC

Nous aidons nos clients à surveiller leurs systèmes d'informations. Nous avons choisi les dernières technologies au cœur de nos solutions SOC, EDR et XDR, afin d'offrir la meilleure détection et réaction. Parce que la souveraineté est au cœur de la cybersécurité, nous avons choisi une offre exclusivement française. Pour gagner en efficacité, nous avons fusionné nos équipes CERT et SOC et automatisé la plupart des activités traditionnelles de niveau 1 et 2.

AUDIT

Qualifiés PASSI RGS, nous aidons nos clients à identifier les vulnérabilités de leurs systèmes d'information par des tests d'intrusion, des revues de code, des audits d'architecture, des audits de configuration et proposons des recommandations pragmatiques pour les aider à corriger les vulnérabilités détectées. Nous réalisons également des audits de conformité afin d'identifier les points de non- conformité et d'accompagner le client en proposant des recommandations contextuelles et hiérarchisées.

CONSEIL

Nous aidons les entreprises à créer de la valeur et à atteindre leurs objectifs stratégiques de manière efficace en identifiant et en gérant les risques de sécurité des clients à tous les niveaux de l'architecture de l'entreprise. Sur la base de notre expérience, nous avons mis en place une méthodologie d'accompagnement spécifique adaptée aux problématiques de sécurité actuelles. Nous offrons à nos clients
un soutien et une assistance dans la mise en place ou l'amélioration de la sécurité de l'information (assistance CISO, Smart PMO, assistance technique, assistance DPO, etc.

NOTRE **SAVOIR-FAIRE**

ANTICIPATION

Analyse de l'exposition du SI

Évaluation de la menace d'intérêt & d'origine cyber

Diagnostic & maturité cyber

Audit PASSI

Test d'intrusion

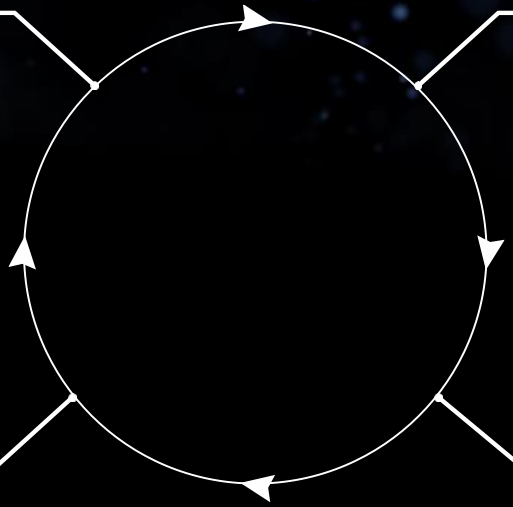
DÉTECTION

SOC managé MDR (XDR, EDR)

Investigation dark web (fuite de données)

Exercice Red Team

Brand monitoring



AMÉLIORATION

Assistance à la conformité & à la certification : ISO27001, ISO27701, RGPD, HDS, NIS2, II901

Gouvernance externalisée : RSSI, DPO

RÉACTION

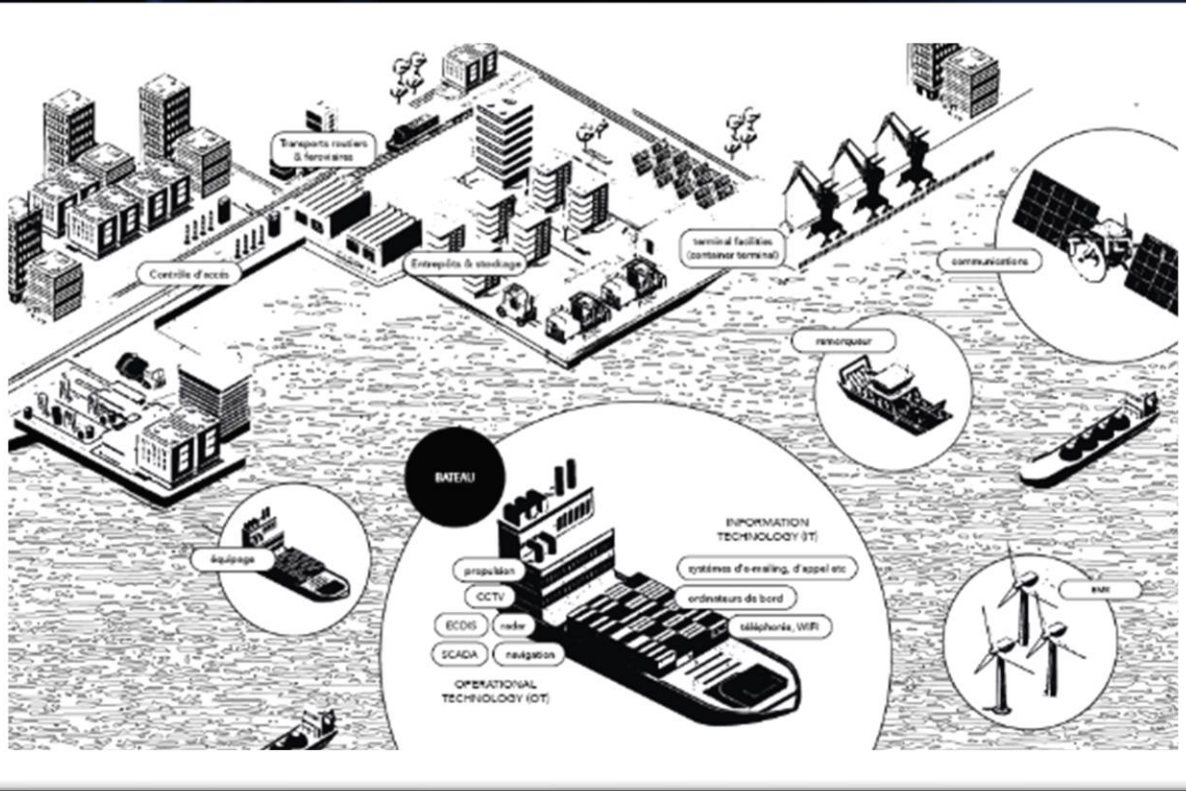
Traitement des incidents de sécurité

Forensic & Levée de doute

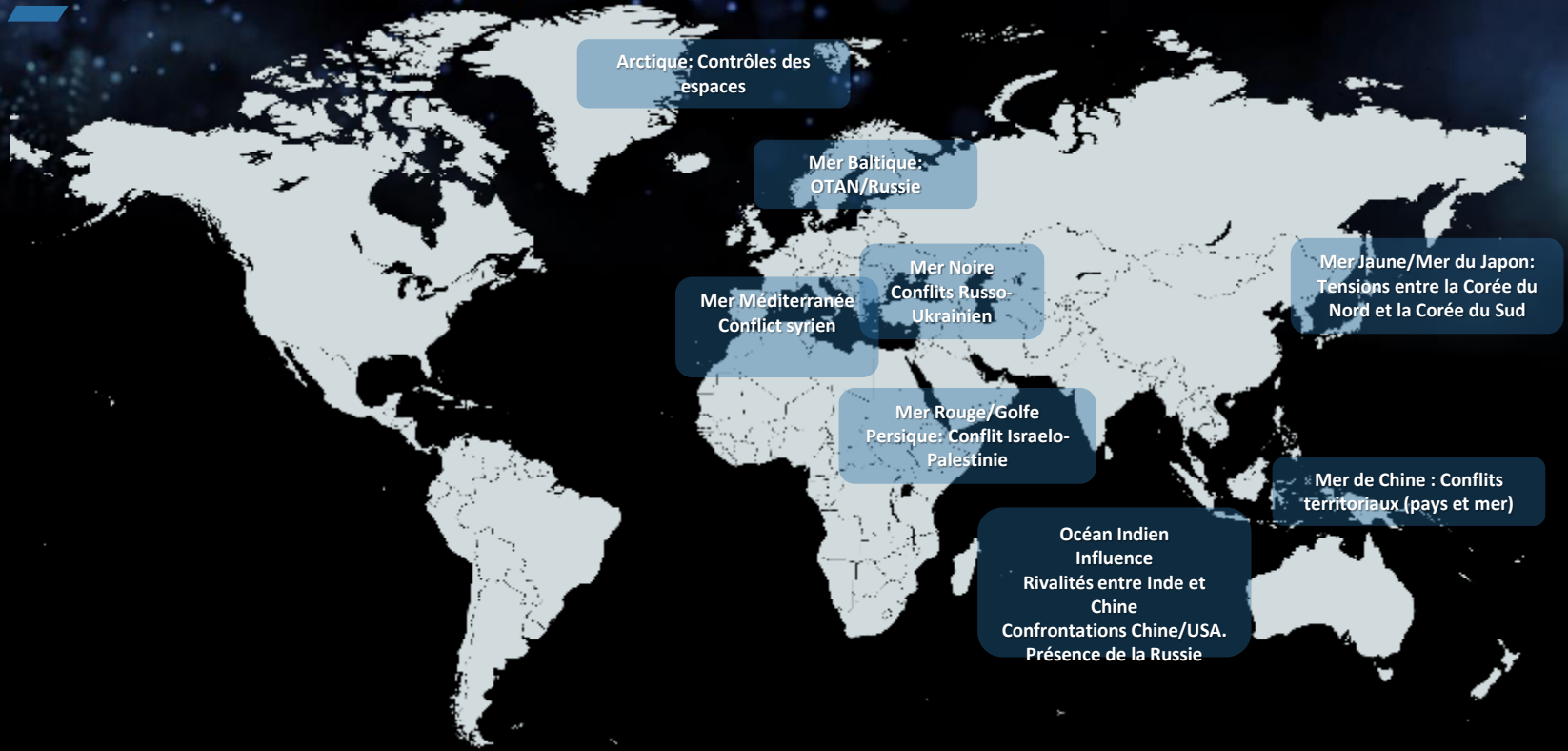
Gestion de crise

L'écosystème du domaine maritime

• Les **ports** : qu'ils soient de commerce, de pêche, multimodaux, d'importance locale, régionale, nationale ou internationale : avec leurhinterland [zone d'influence et d'attraction économique du port s'étendant dans les terres], ils irriguent l'économie de matières premières, de biens et de services indispensables au fonctionnement des économies ;
• Les **navires**, dans toute leur diversité :
navires à passagers, porte-conteneurs, méthaniers, pétroliers, navires de soutien, navires de recherche, navires câbliers
• Les **armateurs** ;
• Les installations **offshore** ;
• Les nombreuses **entreprises** du secteur maritime : sous-traitants, chantiers navals et réparation navale ;
• **L'industrie** navale ;
• La **plaisance** ;
• Le secteur de la **pêche, de l'aquaculture et des produits de la mer** ;
• Les acteurs du **transport**, de la **logistique**, de la manutention ;
• Sociétés de classification, assurances ;
• Les **services numériques** maritimes partagés ;
• Les **administrations publiques** maritimes ;
• Les **énergies marines renouvelables** (EMR) ;
• Les **écoles** et centres de recherche maritimes ;
• Les **infrastructures sous-marines** : câbles sous-marins, infrastructures
de distribution de pétrole et de gaz.



Conflits géopolitiques



Zoom

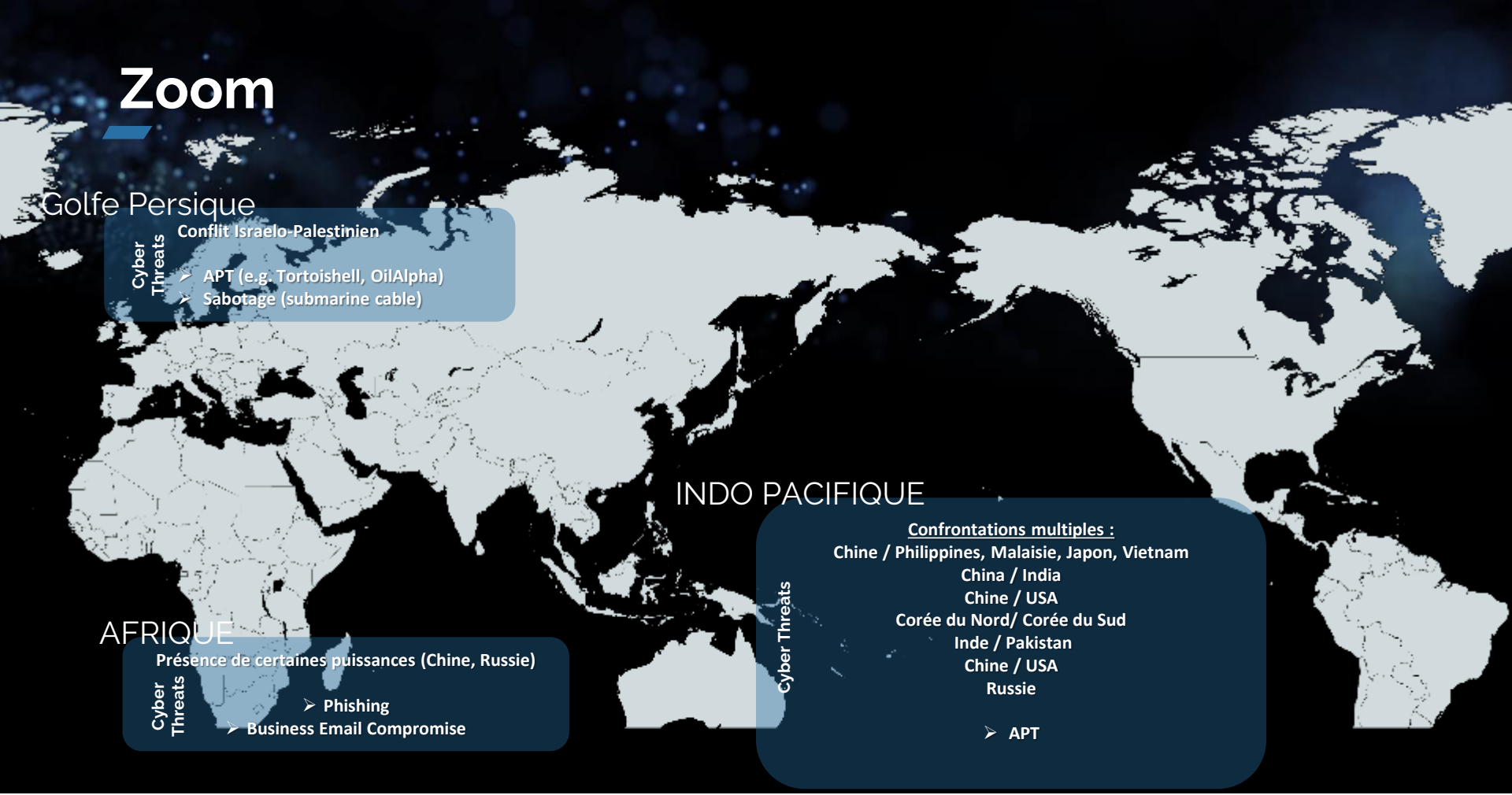
Europe

Cyber Threats

Conflit Russo-Ukrainien

- ➔ DDoS
- ➔ Ransomware
- ➔ APT
- ➔ GNSS Decoying and jamming

Zoom



Golfe Persique

Conflit Israelo-Palestinien

Cyber Threats

- APT (e.g. Tortoishell, OilAlpha)
- Sabotage (submarine cable)

AFRIQUE

Présence de certaines puissances (Chine, Russie)

Cyber Threats

- Phishing
- Business Email Compromise

INDO PACIFIQUE

Confrontations multiples :

Chine / Philippines, Malaisie, Japon, Vietnam
China / India
Chine / USA
Corée du Nord/ Corée du Sud
Inde / Pakistan
Chine / USA
Russie

Cyber Threats

- APT

612

incidents de sécurité durant l'année 2023

Source: M-CERT

Les grandes tendances

MENACES

HACKTIVISTE

CYBERCRIMELLE

ETATIQUE (ADVANCED PERSISTANT THREAT)

TOP VICTIMES

PORT

DEFENSE

ADMINISTRATION

INDRUSTRIE

TRANSPORT & LOGISTIQUE

Zoom sur les vecteurs initiaux d'attaques

- LES CAMPAGNES DE PHISHING ET DE SPEAR-PHISHING

Des phishing taillés sur mesure (usurpation du jargon maritime…)

- L'EXPLOITATION DE VULNERABILITES

MOVEit, CITRIX, Outlook

- LES CAS DES CLES USB

Les supports USB restent des vecteurs potentiels de propagation de codes malveillants au sein du secteur maritime (SI déconnecté, Risque Supply Chain..)

- L'ACHAT D'ACCES EN LIGNE

Le cas des initial access brokers


OWN
PARIS _ RENNES _ TOULOUSE
+33 (0) 805 690 234
contact@own.security
WWW.OWN.SECURITY

La cybersécurité dans un bateau de course

La gestion de la data au sein de TRR

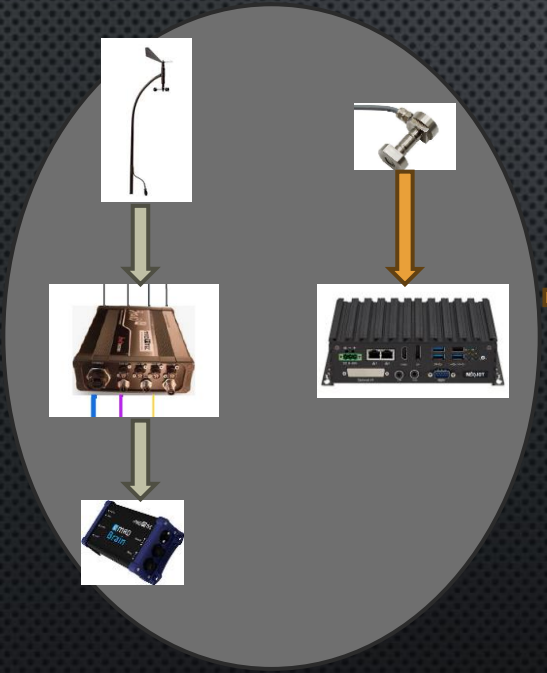
Présentation de TRR

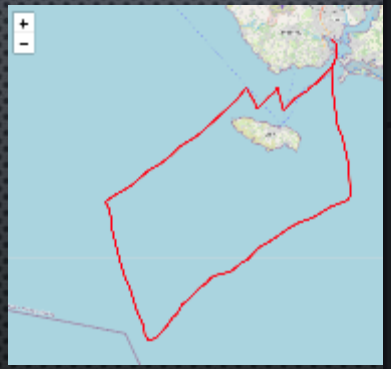
2 Skippers – 2 IMOCAS

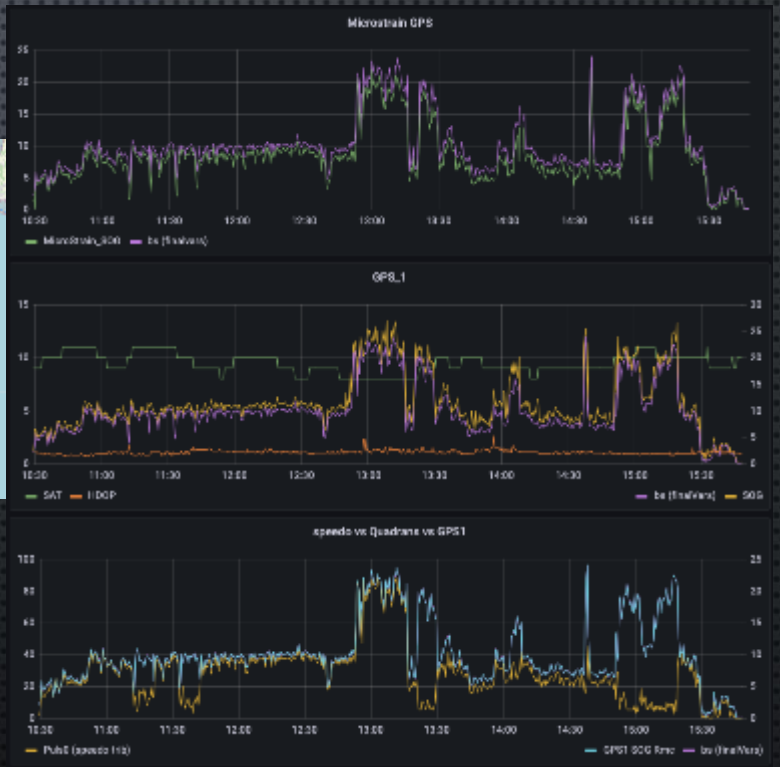
Thomas Ruyant & Sam Goodchild

L’infrastructure autour de la data

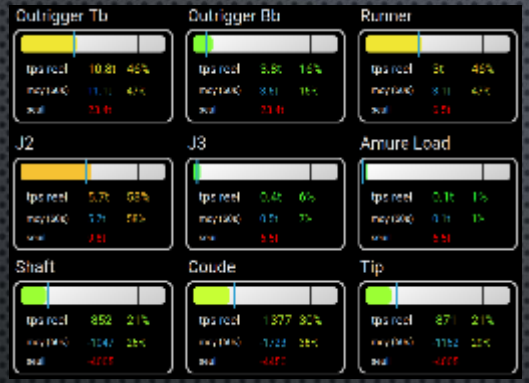
250+ capteurs, 50+ hertz
12500+ points de mesure par seconde







La data au service de la fiabilité

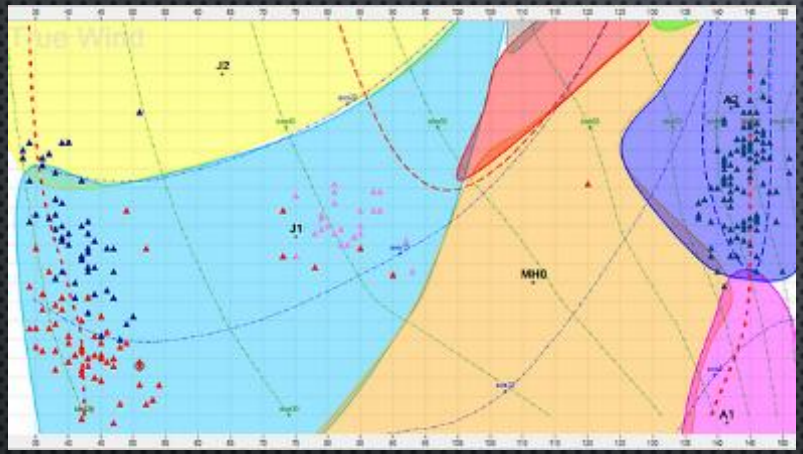


Sécurité gréément

Sécurité structurelle coque

Sécurité réseau

La data au service de la performance



Optimisation utilisation des voiles

Optimisation du pilote automatique

TWA	14	16	18	20
80	J2 (17.1)	J2 (20.2)	J2 (21.5)	J3 (22.6) J2 (22.5)
90	J2 (18.7) J0 (18.5)	J2 (22.2)	J2 (23.4)	J3 (24.4)
100	J0 (20.3)	J2 (24.3)	J2 (25.4)	J2 (26.1)
110	J0 (22.2)	Frac (25.9)	J2 (27.2)	J2 (27.5)

Optimisation vitesse bateau

Les bonnes pratiques

Recruter / se former

Prix initial : 3 000 € HT
Prix facturé à l'entreprise après réduction et aides européennes : 1 500 € HT

Le programme d'accompagnement pour la cyber-résilience des territoires et des entreprises.

PME/PMI ETI, collectivités et établissements du secteur public, le Pôle vous accompagne pour accélérer votre montée en maturité Cyber.

Premier volet

Un cyberdiagnostic pour l'amélioration de la résilience des entreprises

Questions ?

BRETAGNE SAILING VALLEY

👉 sailingvalley.bzh

BRETAGNE DÉVELOPPEMENT INNOVATION

Région BRETAGNE

Jérémie Jourdin
jeremie.jourdin@advens.fr

Alexis Aveline
alexis.aveline@tr-racing.fr

Marion Lachiver
marion.lachiver@own.security

Jack Noel
jack.noel@univ-ubs.fr