CAMPUS CYBER

BASF CONNECT

8 JANVIER 2025

BONNE ANNÉE 2025 !

AGENDA.

INTRODUCTION – ARNAUD TANGUY
TABLE RONDE
- -Genèse, gouvernance et axes stratégiques du collège basf
- -Focus régionalisation
- -Focus soutien et accompagnement des startups

PITCHS DES GROUPES DE TRAVAIL
- -Zero Trust
- -Sécurisation des APIs
- -Cryptographie post quantique
- -Evaluation des tierces parties en collaboration avec Board of Cyber
- -Sensibilisation
- -Sécurité Agile

MOT DE CLÔTURE
COCKTAIL

INTRODUCTION.

ARNAUD TANGUY

GROUP CSO D'AXA, SPONSOR DU COLLÈGE BASF, ET MEMBRE DU CONSEIL D'ADMINISTRATION DU CAMPUS CYBER

· GENÈSE, GOUVERNANCE ET AXES STRATÉGIQUES DU COLLÈGE BASF.

GIL DELILLE, CYBER SECURITY AND IT RISK SENIOR ADVISOR, CRÉDIT AGRICOLE

RIANTSOA BARBARESI, DIRECTRICE DE PROGRAMME, GROUPE BPCE

· GENÈSE, GOUVERNANCE ET AXES STRATÉGIQUES DU COLLÈGE BASF.

NOUS CONTACTER : communautes@campuscyber.fr

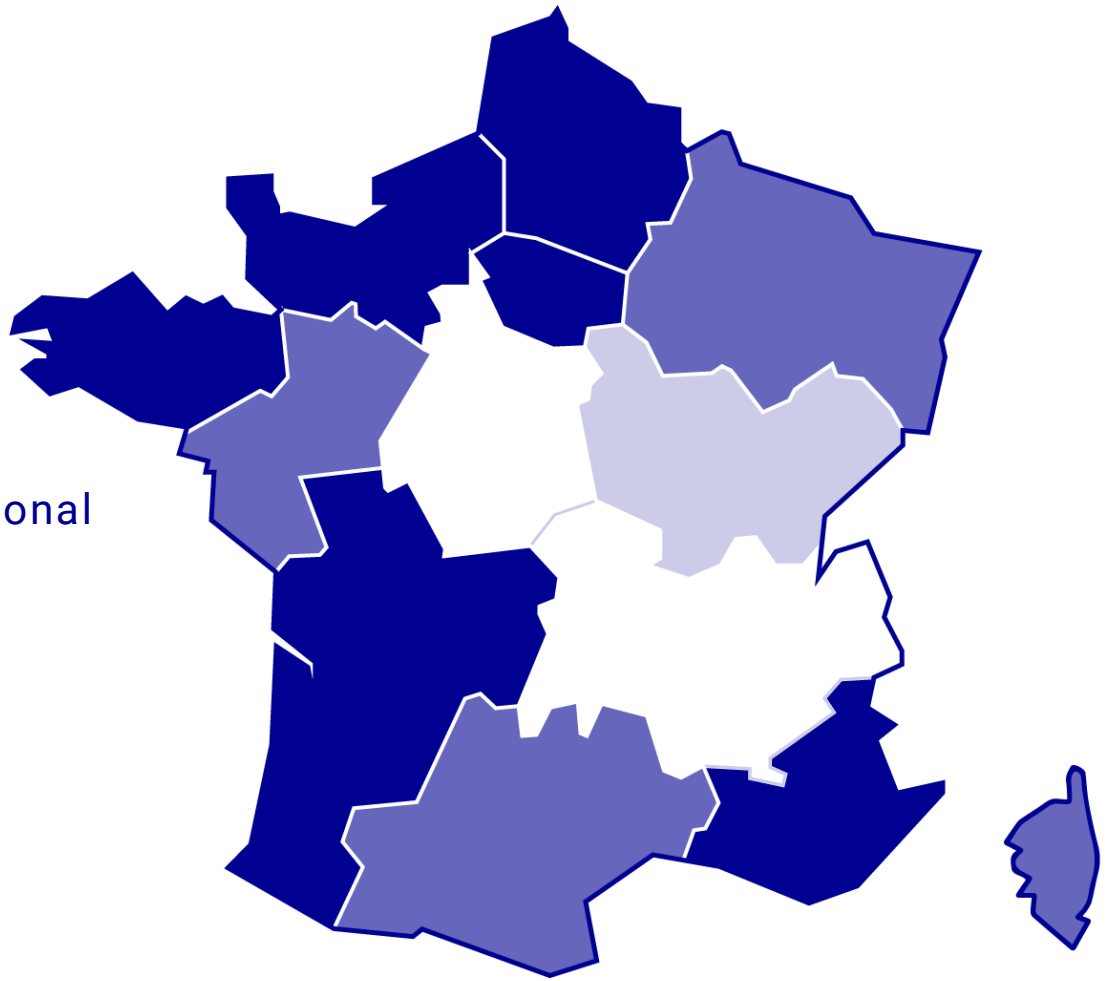
FOCUS « REGIONALISATION».

ANTHONY CHARREAU, RESPONSABLE DOMAINE CYBER DÉFENSE POUR EURO-INFORMATION ET SPONSOR DU COLLÈGE BASF

FAUSTINE SAUNIER, CHEFFE DE CABINET ET CHARGÉE DES PARTENARIATS, CAMPUS CYBER

BERTRAND LE PIOLOT, DIRECTEUR CYBERSÉCURITÉ GROUPE FDJ

RÉSEAU DES CAMPUS CYBER TERRITORIAUX.



Gouvernance : en cours de validation au niveau régional
CCT : /

Gouvernance : Membre du Campus Cyber National
CCT : pas de projet à date

Gouvernance : Membre du Campus Cyber National
CCT : projet en cours de préfiguration

Gouvernance : Membre du Campus Cyber National
CCT : Labellisé

+ **LEARNING EXPEDITION** CAMPUS CYBER HAUTS DE FRANCE.

· FOCUS « SOUTIEN ET ACCOMPAGNEMENT DES STARTUPS ».

GIL DELILLE, CYBER SECURITY AND IT RISK SENIOR ADVISOR, CRÉDIT AGRICOLE

BERTRAND LE PIOLOT, DIRECTEUR CYBERSÉCURITÉ GROUPE FDJ

EMILIE BONNEFOY, CO-FONDATRICE ET CEO, OPEN SEZAM

FRANÇOIS BADIN, RESPONSABLE DES PARTENARIATS, CYBERBOOSTER

CYRIL HAZIZA, DIRECTEUR SÉCURITÉ GROUPE KERING ET MEMBRE DE LA TASK FORCE STARTUPS

PITCH DES COMMUNAUTÉS.

+ **ZERO TRUST** - THIERRY LICCIARDELLO (BNPP), FANNY GIBEY (BNPP)

+ **SÉCURITÉ DES API** - VINCENT FELY (BPCE-SI)

+ **PQC** - VINCENT FELY (BPCE-SI)

+ **EVALUATION DES TIERCES PARTIES EN COLLABORATION AVEC BOARD OF CYBER** - MATHIEU PALANDRE (BANQUE DE FRANCE), GILLES FAVIER (BOARD OF CYBER)

+ **SENSIBILISATION** - ISABELLE DIDELOT (BNPP) ET JULIETTE FARCY (CAMPUS CYBER), LAURENT VERDIER (CYBERMALVEILLANCE.GOUV.FR)

+ **SÉCURITÉ AGILE** - BENJAMIN CHOBERT (BNPP)

ZERO TRUST.

THIERRY LICCIARDELLO (BNPP), FANNY GIBEY (BNPP)

ZERO TRUST.

History

Launched in 2022
As a “Groupe d’échange”
Very enthusiastic, ambitious approach

ZT **Communication Kit – mid 2022**

Attempt to build an GT beyond insurance / bank

ZT community launched **beginning of 2023**

12 entities

Community objectives

Because **ZT topic is wide and transversal** and could be enforced within different strategies, implementations, timelines, …
Working on common and cross members matters to create community key results is challenging

Increasing ZT maturity with a “**Self pace” approach** by **leveraging on members’ experience** and feedbacks

Collaborative and active spirit

Added value by helping members to gather data, needs, results, strategy, approach, use cases, …

Organization

Rules Agreement

Monthly meetings (face and remote)

“Capsule” Meeting rooms and Video Conf (by relying members’ solution)
BdF online storage tools for sharing documents

Agendas prepared collectively with rotating leadership

“kind” of Attendees
- “Core” members (~1/3)
- “Occasional” members (~1/3)
- “Never” (~1/3)

Topics

- Monthly ZT watch
- Maturity survey in Central banks
- REX from FS and pharmaceutical companies

- **Members’ REX**
  - ZT vision, strategy, programs and projects (ZT for Data, Use cases, …)
  - ZT implementations in the industrial sector
  - RFI/RFP on ZTNA solutions
  - IAM (current implementation, solutions, gaps/lacks, Usercube, …)
  - Architecture and exploratory studies (ZT inside Apps, Enterprise Browser, TLS/ECH)

- **Vendors overviews**
  - ZT vision and solutions (Broadcom, Palo Alto ,Netskope, Surf, …)

2025 expectations

Review members list
Increase participation of FS members
Extend community beyond FS

Continue with a rotating leadership

Move to CryptoBox for sharing documents

Non exhaustive topics to be shared :
- ZT between Applications
- ZT in Applications
- Feedbacks on solutions deployment/implementation
- …

ZERO TRUST.

- Learn and profit from **each members' valuable experience**
- **Increase and extend participation**
  - with Cyber campus **members in Financial Services**
  - with Cyber campus **members beyond Financial Services ?**
  - **Beyond Cyber campus** (regional cyber campuses, other International organizations, …) ?

Key takeaways

SECURISATION DES API.

VINCENT FELY (BPCE-SI)

SECURISATION DES API.

Pourquoi s'intéresser à la sécurité des API ?

- Pour répondre à la demande client. *+ de selfcare = + d'API ouvertes sur Internet*
- Pour sécuriser les échanges inter-SI et partenariats business. *API as a Product interne mais pas que*
- Parce que la réglementation imposera toujours + d'ouverture API. *DSP2, DSP3, FIDA*
- Parce que les incidents API sont de + en + fréquents. *Vecteur d'attaque le plus fréquent (Gartner)*
- Parce qu'avec l'IA les API sont de plus que jamais exposées. *Prompt injection direct / indirect*

Le GE Sécurisation des API

2023: Accélération de la tendance Open banking, Open finance → « Nous ne sommes pas seuls à faire des API (et donc de la Sécurité API ?) » → Bingo !

- 9 organisations réunies dans nos ateliers
- 1 atelier / mois (2h) avec thématique préparée à l'avance par 1 participant + veille sécurité API
- 2024 : Cadence des ateliers plus faible. Thème choisi à l'avance, mais plus de préparation préalable. Concentration sur la nature et le contenu du livrable à produire.

SECURISATION DES API.

Thématiques abordées lors des ateliers

Retex :

- Sensibilisation des dev aux failles critiques API
- Architecture d'une API Gateway
- Bonnes pratiques de dev sécurisé d'API

Discussions sur publications :

- Revue de l'évolution 2023 du Top 10 OWASP API

Echanges thématiques :

- Protection des API Anonymes
- Gouvernance de consommation des API externes / partenaires
- Gestion de l'IAM dans les API
- Gestion des incidents de sécurité API

Objectifs 2025

2. Fiabiliser le fonctionnement du GE

- Mise en place d'une gouvernance partagée
- Planning des échanges fixés à l'avance sur le Quarter

3. Mieux capitaliser sur les échanges du GE

- Mise à disposition d'un espace de stockage partagé
- Rédaction d'un livre blanc

Et le **#1** ? Toujours du fun et de la convivialité ! Il nous reste du boulot (voir slide suivante).

BRAINSTORM DE L'ATELIER #1 – MARS 2023.

CRYPTOGRAPHIE POST QUANTIQUE.

VINCENT FELY (BPCE-SI)

CRYPTOGRAPHIE POST QUANTIQUE.

SIGNATURE PROBANTE

CRYPTOGRAPHIE

CONFIDENTIALITÉ DES ÉCHANGES

SÉCURISATION DE LA BLOCKCHAIN

PROTECTION DES DOCUMENTS CONFIDENTIELS

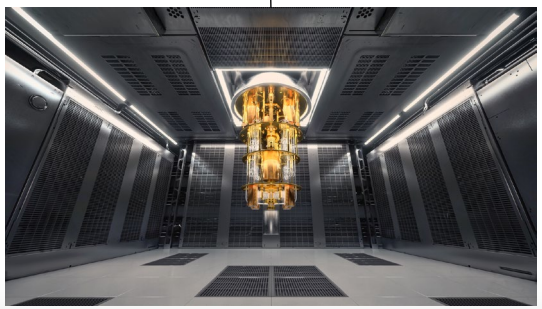
CRYPTOGRAPHIE POST QUANTIQUE.

SIGNATURE PROBANTE

CRYPTOGRAPHIE

CONFIDENTIALITÉ DES ÉCHANGES

SÉCURISATION DE LA BLOCKCHAIN



PROTECTION DES DOCUMENTS CONFIDENTIELS

CRYPTOGRAPHIE POST QUANTIQUE.

Cryptographie Quantique

Utiliser les propriétés de la physique quantique pour établir des protocoles de cryptographie.

Dépendance à des infrastructures qui restent entièrement à construire.

/

Cryptographie Post-Quantique

Résistant au quantique

Algorithmes basés sur des problèmes mathématiques que l'on considère comme résistant à un ordinateur quantique.

Permet d'entrevoir une transition douce sur nos matériels actuels.

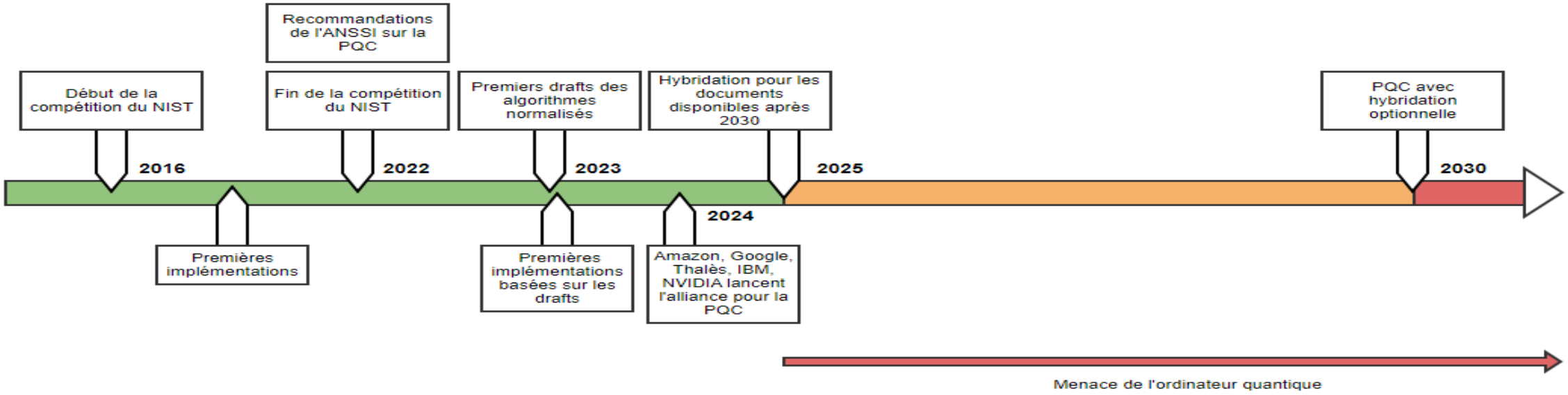
ECHANGE DE CLÉ

SIGNATURE

Old name	New name	Branch
Kyber	**ML-KEM** (FIPS 203) Module-lattice based Key-Encapsulation Mechanism Standard	Lattice-based
Dilithium	**ML-DSA** (FIPS 204) Module-lattice based Digital Signature Standard	Lattice-based
SPHINCS+	**SLH-DSA** (FIPS 205) Stateless Hash-Based Digital Signature Standard	Hash-based
Falcon	**FN-DSA** FFT over NTRU lattices Digital Signature Standard	Lattice-based

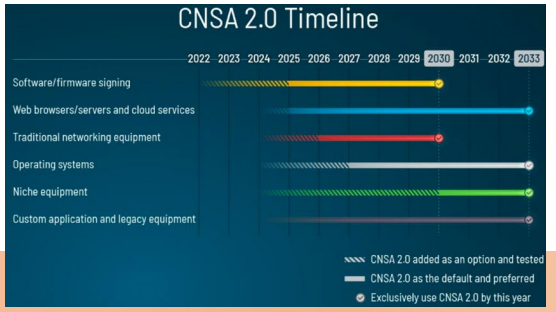
Standardisés en août 2024

CRYPTOGRAPHIE POST QUANTIQUE.



[Avis ANSSI sur la migration vers la cryptographie post quantique, 01/2024]

"Cryptographie Classique :
- Dépréciée en 2030
- Interdite en 2035"



[Timeline de la NSA pour finaliser la migration post quantique, 09/2022]

PQC : Bilan 2024 & Roadmap 2025.

Le GE PQC en quelques points :

- Démarrage en avril 2024
- 6 ateliers en 2024 dont une journée en octobre en présentiel à Paris dans les locaux de Campus Cyber
- Ambiance conviviale !

Objectif des ateliers du GE : Consolidation d'une base de connaissances & montée en compétences des acteurs.

- Par des discussions, partages entre participants, veille sur l'actualité PQC
- Par des rencontre avec des sociétés → PRADEO (en 2024) & IBM (planifiée en janvier 2025)

Objectif en 2025 : Faire le tour du niveau de maturité de nos fournisseurs sur la PQC en se répartissant l'effort & en publiant une synthèse partageable à tous les acteurs

EVALUATION DES TIERCES PARTIES EN COLLABORATION AVEC BOARD OF CYBER

MATHIEU PALANDRE (BANQUE DE FRANCE), GILLES FAVIER (BOARD OF CYBER)

TASK FORCE BASF ET BOARD OF CYBER : RISQUES CYBER LIÉS AUX TIERS.

Genèse

Combinaison de deux axes de travail du collège BASF :

- **GT Gestion du risque cyber fournisseurs et autres tiers**
- Enjeux communs à tous les membres du collège
- Difficultés à industrialiser le processus sans s'outiller
- Mutualisation utile mais complexe

- **Chantier "Start-up"**
- Renforcer les interactions entre le collège et les acteurs de la cyber
- Favoriser l'adéquation entre les initiatives des start-up et les besoins BASF

Opportunité et objectifs

Rencontre avec un acteur français de l'évaluation de la performance cyber

Identification de points de convergence entre les défis rencontrés par les entités BASF et les travaux réalisés par BoC

Réserves concernant les spécificités du secteur, notamment s'agissant des contraintes règlementaires

Proposition d'initier une task force traitant spécifiquement de l'outillage et de l'industrialisation du processus TPRM

Board of Cyber

Startup française TPCRM – Third Party Cyber Risk Management

Organisation

Cadre contraint : 4 ateliers, pour garantir un rythme et des résultats

Principaux constats :
- Notation automatisée, simple rapide et fiable
- Inventaire des fournisseurs
- Traiter les questionnaires de sécurité

Dans la diversité des contextes, émergent des convergences.

Et depuis ?

Innover

- Adapter notre roadmap
- Exploiter des modèles d'IA dans les questionnaires

Next Steps ?

Simplifier, automatiser

Leader européen TPCRM

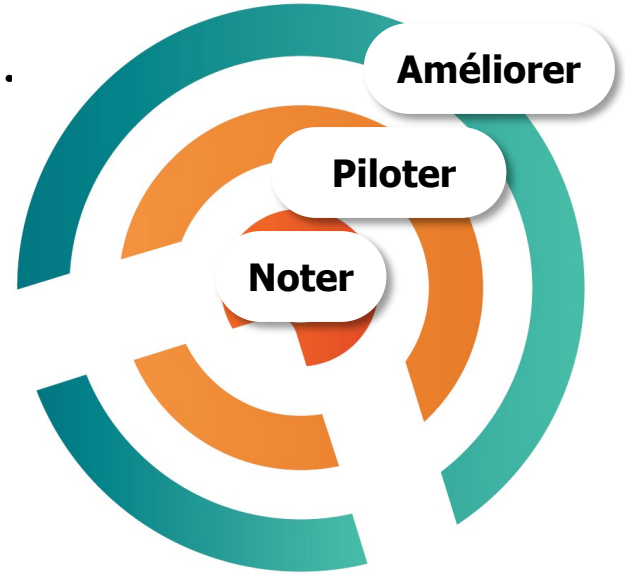
TPCRM

Beyond Rating.

Notation en continu ou due dil

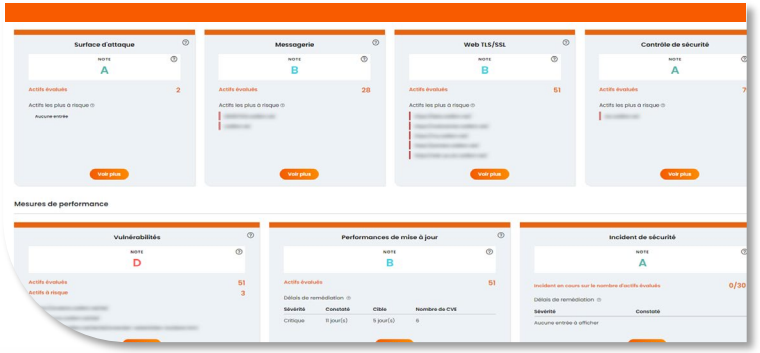
Notation non intrusive

Notation 100% automatisée



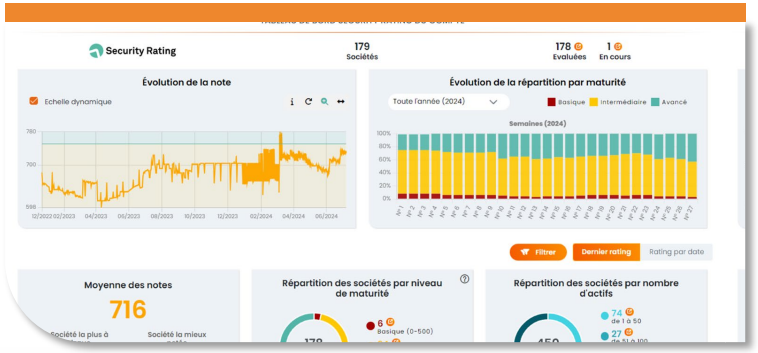
Noter

« Noter votre maturité cyber et celle de votre écosystème »



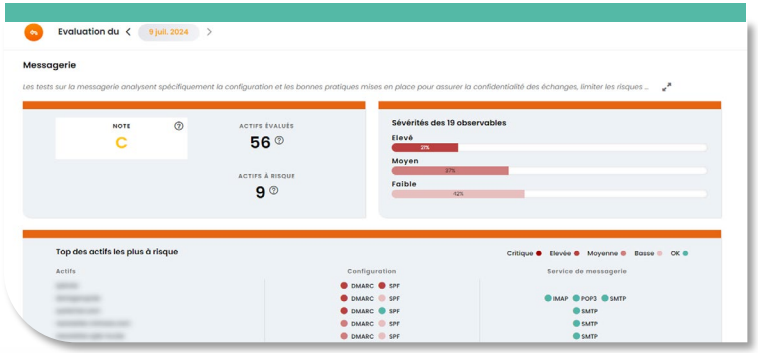
Piloter

« Créer un écosystème de confiance »



Améliorer

« Améliorer votre performance et celle de votre écosystème »



TASK FORCE BASF ET BOARD OF CYBER : RISQUES CYBER LIÉS AUX TIERS.

Genèse

Combinaison de deux axes de travail du collège BASF :

- **GT Gestion du risque cyber fournisseurs et autres tiers**
- Enjeux communs à tous les membres du collège
- Difficultés à industrialiser le processus sans s'outiller
- Mutualisation utile mais complexe

- **Chantier "Start-up"**
- Renforcer les interactions entre le collège et les acteurs de la cyber
- Favoriser l'adéquation entre les initiatives des start-up et les besoins BASF

Opportunité et objectifs

Rencontre avec un leader français de l'évaluation de la performance cyber

Présentation des solutions et chantiers de BoC

Identification de points de convergence entre les défis rencontrés par les entités BASF et les travaux réalisés par BoC

Réserves concernant les spécificités du secteur, notamment s'agissant des contraintes règlementaires

Proposition d'initier une task force traitant spécifiquement de l'outillage et de l'industrialisation du processus TPRM

Board of Cyber

Startup française TPCRM – Third Party Cyber Risk Management

Organisation

Cadre contraint : 4 ateliers, pour garantir un rythme et des résultats

Principaux constats :
- Notation automatisée, simple rapide et fiable
- Inventaire des fournisseurs
- Traiter les questionnaires de sécurité

Dans la diversité des contextes, émergent des convergences.

Et depuis ?

Innover

- Adapter notre roadmap
- Exploiter des modèles d'IA dans les questionnaires

Next Steps ?

Simplifier, automatiser

Leader européen TPCRM

TASK FORCE BASF ET BOARD OF CYBER : RISQUES CYBER LIÉS AUX TIERS.

+ DÉMONSTRATION DE LA CAPACITÉ DES PME / STARTUP À PARLER AU GE

+ MEILLEURE COMPRÉHENSION DES ATTENTES / LIMITES

+ REMONTER LES BESOINS SPÉCIFIQUES AU SECTEUR BASF

+ IDENTIFIER LES POINTS DES CONVERGENCE

En Bref

AWARENESS / SENSIBILISATION.

ISABELLE DIDELOT (BNPP) ET JULIETTE FARCY (CAMPUS CYBER),
LAURENT VERDIER (CYBERMALVEILLANCE.GOUV.FR)

AWARENESS.

- Rassemble les organisations du Collège Banques Assurances
- Depuis le 30 juin 2022
- Ambition : partager, sans préparation, nos expériences sur des thématiques planifiées et communiquées à l'avance.
- 2022-2023 : organisateur BNP Paribas
- 2024 : organisateur La Banque Postale
- **Investissement : 1 h / mois**
- **Les règles :**
  - Partage actif de tous les participants sur les thématiques, du moment qu'on se connecte à l'échange
  - Être transparent en cas de changement de situation / disponibilité / intérêt des personnes membres de ce groupe…
- **Qu'est-ce qu'on y gagne ?**
  - Benchmark et partage d'idées, de pratiques…
  - Renforcement de l'écosystème Cyber Banques et Assurances

« SE RÉUNIR EST UN DÉBUT, RESTER ENSEMBLE EST UN PROGRÈS, TRAVAILLER ENSEMBLE EST UN SUCCÈS »

HENRY FORD

SENSIBILISATION.

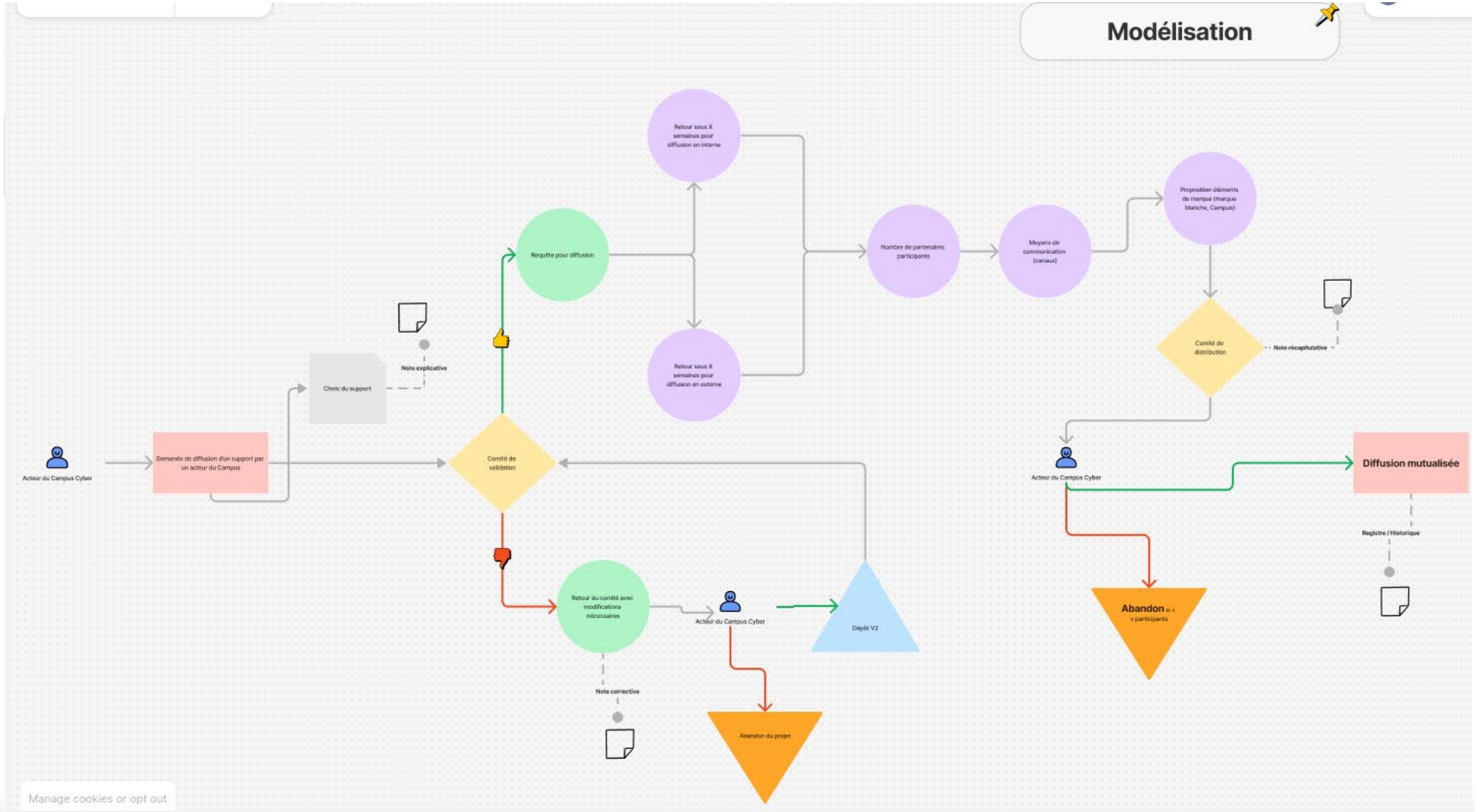
- Rassemble des **organisations de tous les secteurs**
- Rassemblés grâce au Campus Cyber
- Du **05 Juillet 2022 au 31 décembre 2023**
- Ambition : créer une campagne de sensibilisation commune, adressée au même moment
- **Une impulsion commune : Campus, Cybermalveillance.gouv.fr, BNP Paribas**
- Temps : > 1 jour / mois + les rencontres
- Synergie de moyens (création de supports de communication, infographie, etc.)
- Les règles :
  - Être transparent si changement de situation / disponibilité…
  - Attention, le GT n'est pas un lieu d'activité commerciale (ex. démarchage)

- Qu'est-ce qu'on y gagne ?
  - Mieux connaître et participer au renforcement de l'écosystème Cyber en France
  - Participer à des actions visibles du « grand public » et TPE/PME
- **Outputs : Définition de 2 cibles prioritaires :**
  - « Actifs digitaux »
  - -> PCCA et Campagne Fraud Fight Club
  - Les TPE/PME
  - -> Kit des recommandations essentielles

« LE CHEMIN EST CLAIR, MAIS LES VOYAGEURS SONT NOMBREUX ET LEURS PAS DISCORDANTS »

PROVERBE CHINOIS

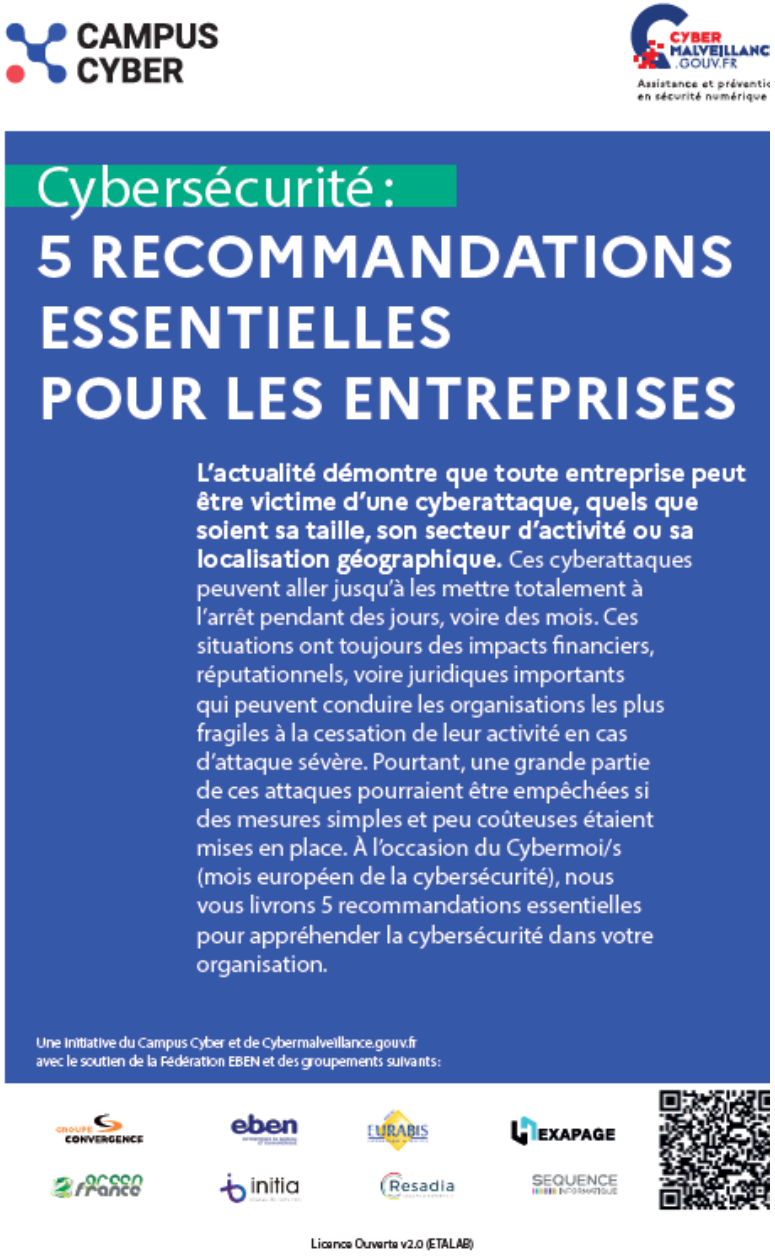
LE PLAN DE COMMUNICATION CYBER AUGMENTÉ.

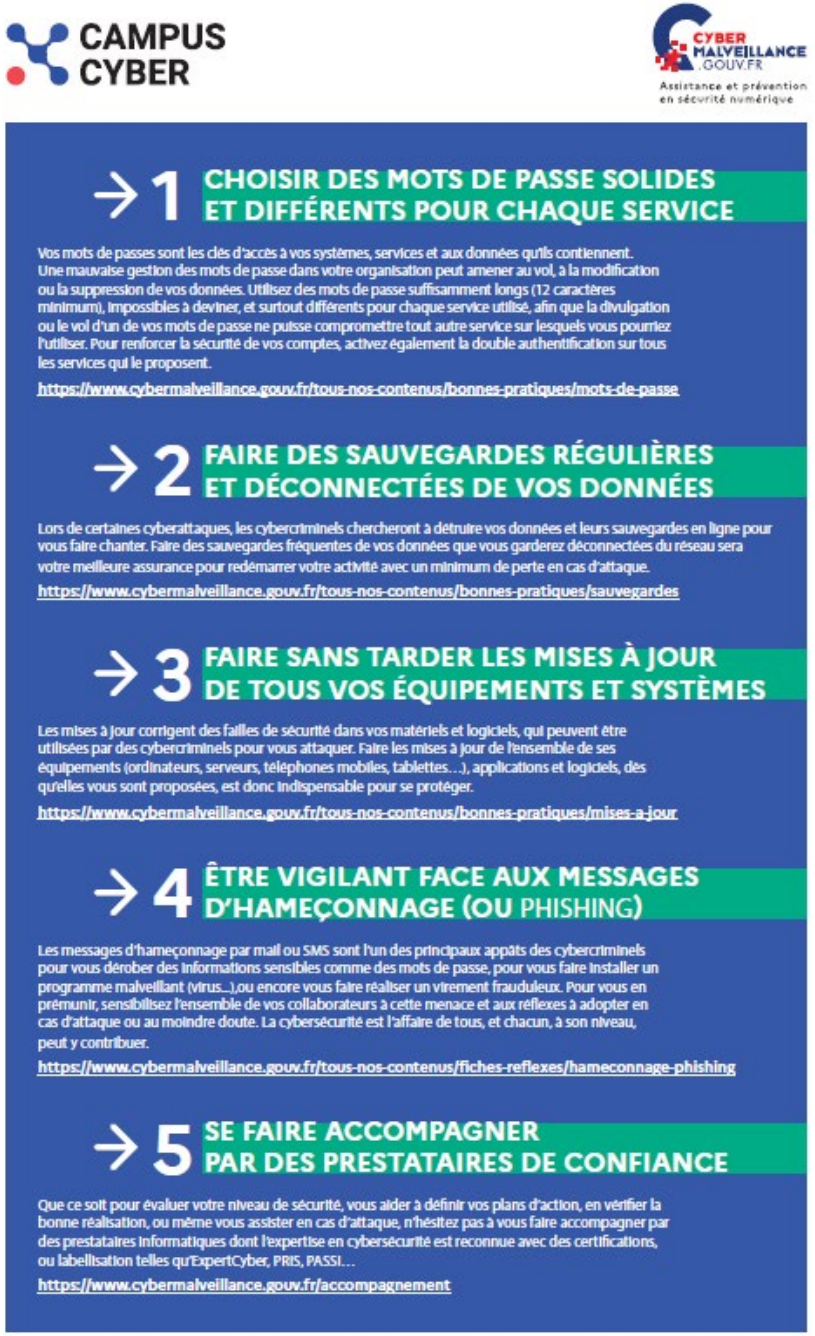


CAMPAGNE FRAUD FIGHT CLUB

- Production de Master Card avec contribution des membres du Campus
- Diffusion par les membres du Campus

COMMUNICATION COMMUNE À L'INTENTION TPE/PME.





SÉCURITÉ AGILE.

BENJAMIN CHOBERT (BNPP)

SÉCURITÉ AGILE.

ETA: Early-Q2 2025

"Face à l'adoption croissante des méthodologie Agile visant à réduire le Time-To-Market, la Sécurité dans les développements doit répondre à de nouveaux impératifs de célérité."

+ **Stream 1: Gouvernance**
  Avancement: 95%
  5 contributeurs actifs

  Contenu du livrable:
  - Secure SDLC, processus, comitologie, …
  - Gestion des vulnérabilités en développement
  - Threat modeling

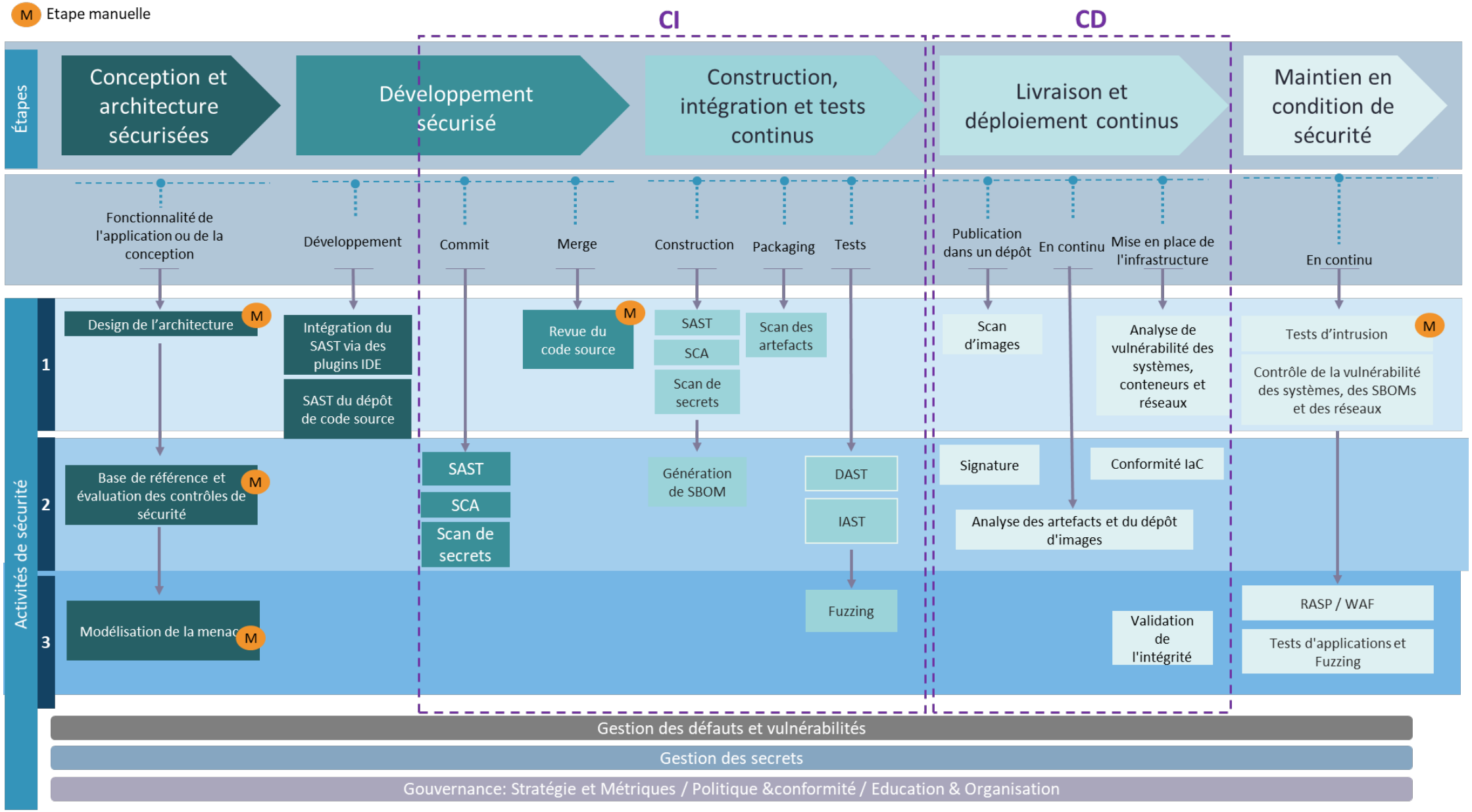
+ **Stream 2: Security Champions & SME**
  Avancement: 85%
  5 contributeurs actifs

  Contenu du livrable:
  - TOM Security Champions & SME
  - Programme de formation Security Champions

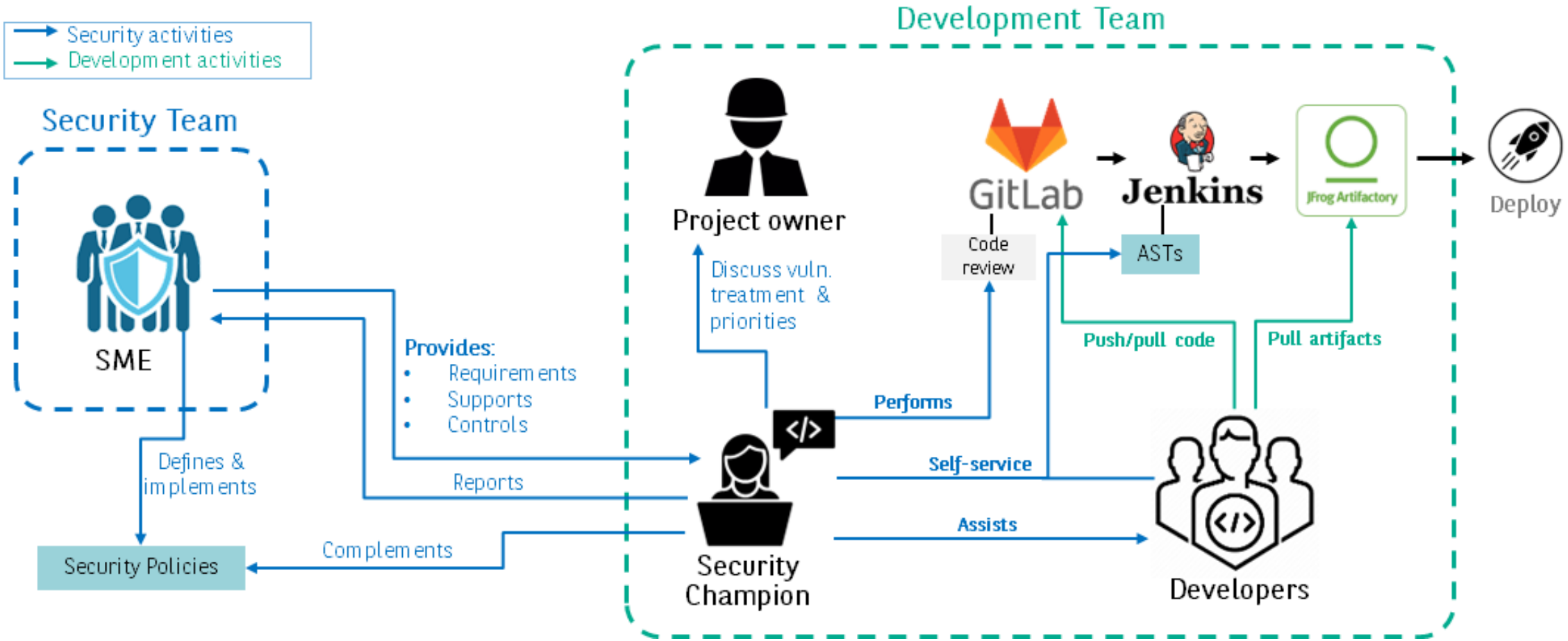
+ **Stream 3: Technologies**
  Avancement: 85%
  5 contributeurs actifs

  Contenu du livrable:
  - Etat du marché
  - Stratégie de monté en maturité technologique

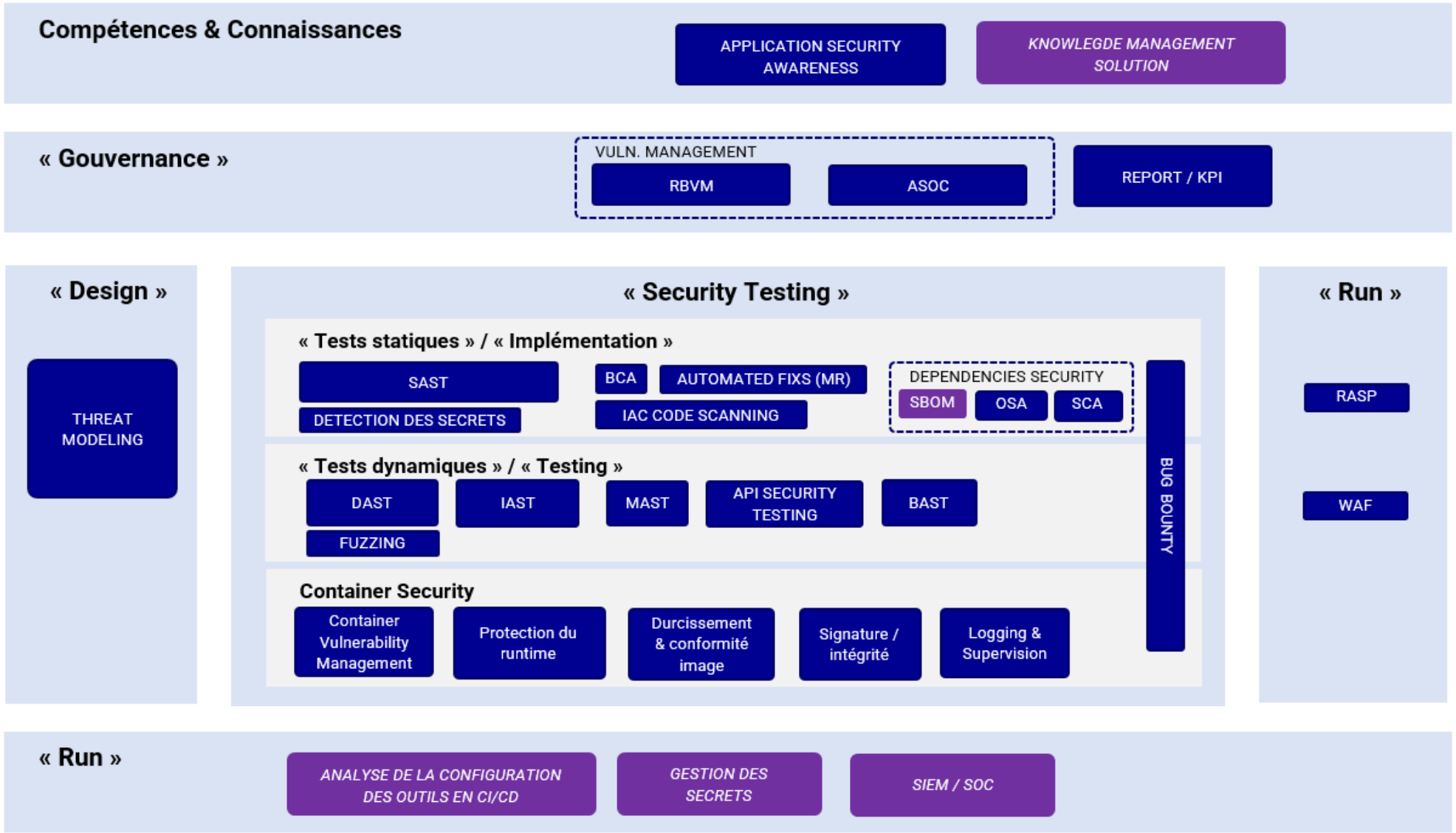
+ STREAM 1: GOUVERNANCE



STREAM 2: SECURITY CHAMPIONS & SME



STREAM 3: TECHNOLOGIES



MERCI !

TÉLÉCHARGER LES SLIDES :

→ https://wiki.campuscyber.fr/BASF_CONNECT

CAMPUS
CYBER