ATELIER DE COMPÉTENCES

4ème année INSA Centre Val de Loire
Spécialité Sécurité et Technologies Informatiques
Année 2023/2024

Nurdini BINTI MOHAMAD
Apprentie Analyste CSIRT

Tutrice académique
Sabine FRITTELLA

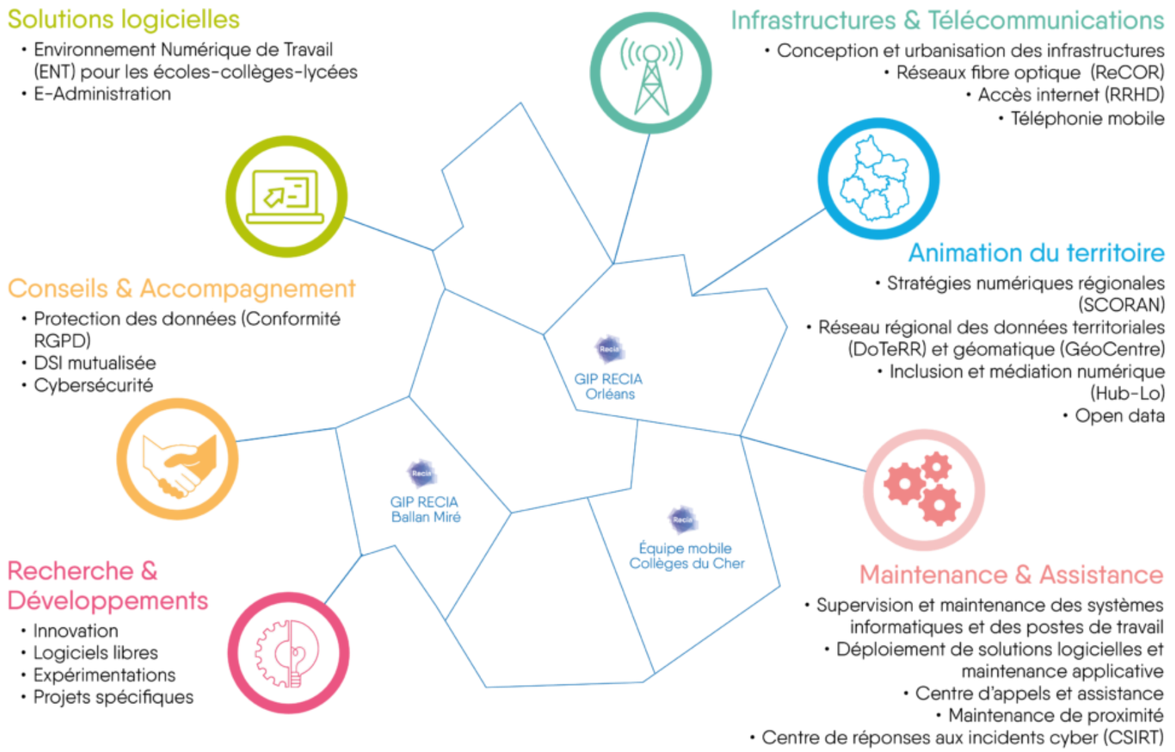
Maître d'apprentissage
Victor-Emmanuel de SA

SOMMAIRE

INSA
CENTRE VAL DE LOIRE

CONTEXTE

Présentation de l'entreprise



Activités et services du GIP RECIA

INSA CENTRE VAL DE LOIRE

CONTEXTE

Contexte du projet

Créé suite au programme d'incubation de l'**ANSSI** pour déployer des CSIRT régionaux.

CybeRéponse joue un rôle crucial dans l'assistance aux **collectivités**, aux **associations employeuses**, aux **PME/PMI** et aux **ETI** victimes d'attaques cyber.

Mission principale

Les services de CybeRéponse visent à promouvoir la **détection**, la **résolution** et la **prévention** des risques cyber auprès des acteurs régionaux.

INSA
CENTRE VAL DE LOIRE

CONTEXTE

Contexte du projet

Équipe

N1 : le premier point de contact

N2 : la gestion des incidents et la mise en relation avec les prestataires de la région

Équipe

20 prestataires de la région : compétences spécifiques

Développeuse interne : analyse approfondie des incidents, développer des outils personnalisés

INSA
CENTRE VAL DE LOIRE

MISSIONS RÉALISÉES

1. Gestion et optimisation des outils de gestion des appels

OBJECTIFS

- Rechercher une solution plus performante pour améliorer notre efficacité opérationnel
- Identifier les limitations de l'outil existant - ODOO
- Optimiser les outils de gestion des appels au sein du CSIRT

INSA
CENTRE VAL DE LOIRE

MISSIONS RÉALISÉES

1. Gestion et optimisation des outils de gestion des appels

Étape 1 : Analyse approfondie de l'outil ODOO

Étape 2 : Recherches et évaluation de nouvelles solutions - TheHive et Zammad

Étape 3 : Développement de fonctionnalités spécifiques pour optimiser la gestion des déclarations d'appels - **la création de formulaires adaptatifs**, **la mise en place de la génération automatisée de dossier d'incident**

COMMENT ?

odoo

Zammad

INSA
CENTRE VAL DE LOIRE

MISSIONS RÉALISÉES

1. Gestion et optimisation des outils de gestion des appels

RÉSULTAT

- Simplification de la saisie des déclarations d'appels grâce aux formulaires adaptatifs.
- La génération automatisée de dossier d’incident standardisés.
- La mise en pré-production en juillet.

INSA
CENTRE VAL DE LOIRE

MISSIONS RÉALISÉES

1. Gestion et optimisation des outils de gestion des appels

	Compétences mobilisées
Analyse Niveau 3	analyse approfondie des besoins de l'entreprise en identifiant les lacunes dans l'outil CRM actuel.
Adhésion Niveau 2	Communication efficace avec les équipes internes pour obtenir leur soutien dans les décisions critiques.
Mise en œuvre opérationnelle Niveau 3	Configuration d'un serveur dédié pour la génération automatisée de fichiers PDF à partir des tickets d'incident.
Traitement de l'info Niveau 3	Développement de documents détaillés, y compris des manuels d'utilisation complets pour Zammad
Corrections Niveau 3	Amélioration du formulaire de saisie des déclarations d'appels pour optimiser la réactivité et la flexibilité.

INSA
CENTRE VAL DE LOIRE

MISSIONS RÉALISÉES

2. Optimisation de la base de données

OBJECTIFS

- améliorer la qualité et la précision des informations utilisées quotidiennement
- Aligner les données avec les besoins opérationnels
- Établir un processus de maintenance des données

INSA
CENTRE VAL DE LOIRE

MISSIONS RÉALISÉES

2. Optimisation de la base de données

COMMENT ?

Données SIRENE et BANATIC

INSA CENTRE VAL DE LOIRE

MISSIONS RÉALISÉES

2. Optimisation de la base de données

DIFFICULTÉS

- Diversité des sources de données et des formats, nécessitant une approche méthodique.
- Défis techniques pour assurer l'exactitude des données et l'intégration fluide dans Zammad.

RÉSULTATS

- En cours de développement.
- Mettre en rélation partenariats stratégiques avec des acteurs clés comme Dev'UP pour aligner nos données avec les leurs.

INSA
CENTRE VAL DE LOIRE

MISSIONS RÉALISÉES

2. Optimisation de la base de données

Compétences mobilisées

Corrections Niveau 3	Utilisation de scripts Python pour automatiser le processus de correction.
Contrôle Niveau 3	Réalisation d'audits pour garantir la précision des informations.
Gestions des risques - Niveau 2	Identification des risques liés à la qualité des données.
Mise en Œuvre Opérationnelle Niveau 3	Automatisation de l'injection de données dans Zammad et l'utilisation d'API et d'outils d'automatisation comme n8n.

INSA CENTRE VAL DE LOIRE

MISSIONS RÉALISÉES

3. Participation active aux réunions avec les prestataires et événements de cybersécurité

OBJECTIFS

- Rester informé des développements et des défis en cybersécurité.
- Approfondir mes connaissances et échanger avec des pairs et experts.
- Améliorer la compréhension des besoins et attentes des prestataires.

INSA
CENTRE VAL DE LOIRE

MISSIONS RÉALISÉES

3. Participation active aux réunions avec les prestataires et événements de cybersécurité

RÉALISATIONS

- Participations active aux réunions avec nos prestataires, qui ont lieu tous les deux mois.
  - Présentation des statistiques de notre centre de réponse aux incident cyber.
- Participation à des événements clés – Assises de la Cybersécurité et les Ateliers de Protection des Données

RÉSULTATS

- Echanger des connaissances et des bonnes pratiques.
- Sensibilisation accrue aux enjeux et meilleures pratiques de cybersécurité
- Enrichissement des connaissances et adaptation aux évolutions du secteur.

INSA
CENTRE VAL DE LOIRE

MISSIONS RÉALISÉES

3. Participation active aux réunions avec les prestataires et événements de cybersécurité

Compétences mobilisées

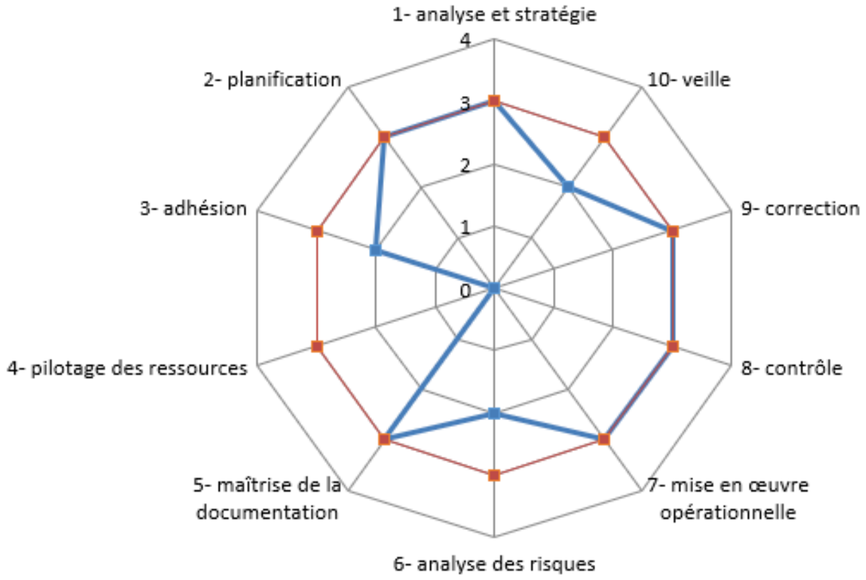
Adhésion Niveau 2	La présentation claire et concise des statistiques et des résultats obtenus à partir de nos activités
Veille Niveau 2	Participation régulière à des ateliers de protection des données et aux assises de la cybersécurité.

INSA CENTRE VAL DE LOIRE

BILAN

La montée en compétences

niveau	apprenti	attendu
1- analyse et stratégie	3	3
2- planification	3	3
3- adhésion	2	3
4- pilotage des ressources	0	3
5- maîtrise de la documentation	3	3
6- analyse des risques	2	3
7- mise en œuvre opérationnelle	3	3
8- contrôle	3	3
9- correction	3	3
10- veille	2	3



Martice croisée activité/compétences

INSA CENTRE VAL DE LOIRE

BILAN

Perspectives Futures : Prochains Projets et Compétences à Valider

LA MISE EN PLACE DE NOUVEL OUTIL ZAMMAD

JOURNALISATION DES ÉVÉNEMENTS DU SYSTÈME D'INFORMATION

- Adhésion - Niveau 3
- Pilotage des Ressources - Niveau 3
- Maîtrise de la Documentation - Niveau 3
- Analyse des Risques - Niveau 3
- Veille - Niveau 3

INSA
CENTRE VAL DE LOIRE

MERCI !

cybeRéponse
CENTRE-VAL DE LOIRE

Avez-vous des questions ?

INSA
CENTRE VAL DE LOIRE