

Stage CEOS IT

Cybersécurité & Développement Logiciel

Étudiant	Bryan Tillou
Établissement	BTS SIO — Option SLAM
Entreprise d'accueil	CEOS IT — ESN · Béthune (62)
Service	Sécurité & Maintenance Web
Période	Janvier – Février 2026 (6 semaines)
Tuteur	Équipe CEOS IT

Cybersécurité

WordPress

PHP / MySQL

JavaScript

Workflow Engine



1.	Présentation de l'entreprise CEOS IT	
2.	Contexte & Objectifs du stage	
3.	Mission 1 — Restauration site WordPress (Cyberattaque)	
4.	Mission 2 — Système de métriques Mobibat	
5.	Mission 3 — Triggers Workflow (Mails & Métriques)	
6.	Mission 4 — Planification type Crontab	
7.	Mission 6 — Configuration démo commerciale	
8.	Mission 7 — Généralisation du moteur Workflow	
9.	Mission 8 — Migration workflow archivage PDF	
10.	Compétences développées	
11.	Conclusion & Bilan	

1 Présentation de l'entreprise CEOS IT

Raison sociale	CEOS IT
Statut	ESN – Entreprise de Services du Numérique
Localisation	Béthune, Pas-de-Calais (62)
Domaines d'activité	Conseil SI · Cybersécurité · Infrastructure réseau & téléphonie · Édition logiciel métier · Gestion RH/comptable
Mission	Optimiser la performance, la sécurité et la fiabilité des écosystèmes numériques clients

CEOS IT accompagne ses clients dans leur **transformation digitale** en proposant une palette complète de services : conseil en systèmes d'information, cybersécurité, infrastructure réseau et téléphonie, édition de logiciels métier (dont **MOBIBAT**, solution dédiée au secteur du BTP), ainsi que des solutions de gestion comptable et RH.

2 Contexte & Objectifs du stage

Période	Janvier à Février 2026 — 6 semaines
Service	Équipe de sécurité et maintenance web
Objectif principal	Restauration d'un site WordPress de mairie victime d'une cyberattaque majeure, et développement de fonctionnalités dans le logiciel MOBIBAT

Objectifs pédagogiques

- Gérer une situation de crise cybersécurité en environnement réel
- Maîtriser les techniques d'analyse forensique et de décontamination
- Appliquer les bonnes pratiques de migration et mise à jour WordPress
- Développer autonomie, rigueur méthodologique et capacité d'adaptation
- Contribuer au développement d'un logiciel métier (MOBIBAT) en PHP/MySQL/JS

3

Mission 1 — Restauration WordPress (Cyberattaque)

Cette mission critique consistait à **restaurer un site WordPress de mairie gravement compromis** par une cyberattaque sophistiquée. Le site datant de 2015 (WordPress 3.x, PHP 5.4) contenait du code malveillant obfusqué massivement injecté dans l'ensemble de l'arborescence.

Phase	Titre	Description
	Audit forensique	Téléchargement via FileZilla, analyse VS Code (base64, XOR, désérialisation), SSH/PuTTY logs Apache, DBaver : comptes admins fantômes, crons malveillants.
Phase 2	Installation WP vierge	WordPress 6.5 / PHP 8.2 / MySQL 8.0. Connexion FortiClient VPN. Structure initiale documentée.
	Extraction & nettoyage	Export/inspection tables WordPress. Filtrage patterns malveillants. Récupération médias avec vérification MIME type.
Phase 4	Reconstruction UI	Refonte CSS navigation. Adaptation thème WP 6.5. Réintégration médias décontaminés. Redirections 301 SEO.
	Modernisation infra	WP 3.8 → 6.5, PHP 5.4 → 8.2. Suppression de 15 plugins obsolètes. Thème enfant personnalisé.
Phase 6	Migration hébergeur	Export SQL + SFTP. Configuration DNS (enregistrements A). SSL obligatoire. Mode maintenance (24–48h).
	Durcissement sécurité	Suppression comptes suspects. 2FA admins. Protection .htaccess anti-bruteforce. Sauvegardes auto 30 jours.
Phase 8	Tests & validation	Tests liens, formulaires, performances. Scan vulnérabilités. Présentation mairie. Recette acceptée.

Techniques d'obfuscation identifiées

Technique	Description
Encodage Base64	Code encodé pour ressembler à des données binaires inoffensives
Opérations XOR	Chiffrement du payload avec une clé secrète
Reconstruction dynamique	Noms de fonctions (eval, exec, system) reconstruits caractère par caractère
Injection dans images	Code PHP caché dans les métadonnées EXIF de fichiers JPG

Outils utilisés

Outil	Rôle
Visual Studio Code	Analyse du code malveillant, édition fichiers WordPress, débogage PHP
DBaver	Administration MySQL, export/import BDD, nettoyage tables infectées
FileZilla (FTP/SFTP)	Téléchargement fichiers contaminés, upload vers nouvel hébergeur
FortiClient VPN	Connexion sécurisée au réseau CEOS IT et serveurs clients

Outil	Rôle
PuTTY (SSH)	Accès serveurs Linux, permissions, analyse logs Apache
WordPress 6.5 / PHP 8.2 / MySQL 8.0	Stack modernisée pour la reconstruction du site

4 Mission 2 — Système de métriques Mobibat

Mise en place d'un **système de métriques** pour MOBIBAT : centraliser des statistiques métier (usage, erreurs, activité), les filtrer, les visualiser et fournir un indicateur synthétique sur le dashboard.

Comparatif des solutions envisagées

Solution	Évaluation	Décision
QuestDB	Très rapide mais limitations auth/config	✗ Écarté
Elasticsearch	Puissant mais licence SQL/JDBC payante	✗ Écarté
Autres moteurs	Config incompatible contraintes sécurité	✗ Écarté
MySQL z_metrics	Requêtes maîtrisées, flexible via JSON, existant	✓ Retenu

Architecture technique retenue

Modèle de données	Table z_metrics (InnoDB, utf8mb4) : metric_id, user_id, site_id, document_id, metric_date, metric_name, metric_category, metric_value (DECIMAL), metric_data (JSON), metric_flags.
Page back-office (/back/test)	Formulaire de filtres + tableau paginé. JS : loadMetrics(), populateRow(), renderMetricData(). Filtres synchronisés dans l'URL.
API MetricsController.php	get() avec WHERE dynamique et pagination, stats() pour métriques du jour (total, erreurs, %). Retour JSON structuré.
Dashboard front	Carte synthétique % erreurs du jour. Appel AJAX /api/metrics/stats. Redirection filtrée vers la page de métriques au clic.

Langages : PHP (backend) · SQL (filtres/pagination) · JavaScript (AJAX, URL params) · HTML/TPL (templates) · CSS (design glassmorphism).

5 Mission 3 — Triggers Workflow (Mails & Métriques)

Fiabilisation du moteur de workflow interne de MOBIBAT pour les absences : sélection automatique du bon mail, du bon template et des bons paramètres selon le type d'événement.

Trigger	Événement	Template mail
absence_add	Ajout d'une absence	mobibat_absence_add.tpl
absence_accept	Absence acceptée	mobibat_absence_accept.tpl
absence_reject	Absence refusée (avec motif)	mobibat_absence_reject.tpl
absence_prolong	Prolongation (ancienne date fin)	mobibat_absence_prolong.tpl

Résultats obtenus :

- Triggers fiables et cohérents — bon mail envoyé selon le type d'absence
- Paramètres dynamiques correctement injectés : {ABSENCE_DATE_START}, {ABSENCE_DATE_END}, {ABSENCE_OLD_DATE_END}
- Templates lisibles et homogènes — système extensible pour futurs triggers

6 Mission 4 — Planification type Crontab

Déploiement d'un **système de planification automatisé** inspiré du crontab Unix : lisible, configurable en base de données, extensible — capable d'exécuter des workflows à des moments précis.

Expression cron (6 champs)	Déclenchement
0 0 * * * *	Toutes les heures à hh:00:00
* /10 * /5 * * * *	Toutes les 10 secondes, toutes les 5 minutes
0 30 8 * * 1-5	À 08h30 les jours ouvrés (lundi–vendredi)

Fonctionnalités clés :

- Parsing et normalisation : NULL → *, */N (intervalle), valeur exacte
- Protection contre l'exécution infinie si tous les champs sont NULL
- Mode intervalle réel : X secondes après la dernière tâche (utile en métiers)
- Intégration dans la boucle d'exécution workflow + logs détaillés

7

Mission 6 — Configuration démo commerciale

Configuration d'une **démonstration commerciale complète** du logiciel CEOS IT : environnement crédible avec données fictives cohérentes, scénarios métier complets simulant une entreprise réelle du secteur BTP.

Module	Contenu configuré
ModulRH	Gestion des salariés, absences, suivi administratif RH
Mobibat Amiante	Chantiers réglementaires amiante, traçabilité et conformité
Mobibat Compagnon	Interface terrain, pointage salariés, suivi en temps réel

Impact stratégique : une démo cohérente et réaliste améliore la compréhension des prospects, renforce la crédibilité de la solution et facilite la transformation commerciale.

8

Mission 7 — Généralisation du moteur Workflow

Extension du moteur de workflow (modèle absences) à de **nouveaux modules métier** en conservant l'architecture validée : déclenchement par trigger, création de tâches, exécution automatique et envoi de mail.

Workflow	Trigger	Chaîne d'exécution
Pointages	ticking_validate	Trigger → workflow_tasks → données métier → remplacement variables → envoi mail
Notes de service	service_note_send	Tâche → données métier → liste destinataires → remplacement variables → envoi mail

Chaîne validée de bout en bout : front → API → création tâche → exécution workflow → envoi mail. Vérification statuts (à faire → en cours → terminé) et paramètres transmis.

9

Mission 8 — Migration workflow archivage PDF

Migration de l'archivage automatique des documents vers le pipeline moderne **workflow_tasks**, en conservant la compatibilité legacy et en améliorant le diagnostic.

Modification	Détail technique
Alignement workflow_tasks	Tâches archive dans workflow_tasks (date_start, date_end, flags, parameters). Intégration type archive dans la boucle principale.
Nouveau chemin PDF	/data/files/{CUSTOMER_NAME}/archives/tmp/{site_id}-{date}.pdf — organisation améliorée.
Lecture API robuste	Lecture prioritaire via /api/workflow/read + fallback vers workflow_site_tasks (legacy).
Correction SQL JSON	Requêtes JSON_EXTRACT corrigées — suppression erreur Invalid JSON path expression.

10 Compétences développées

Compétences techniques

Analyse forensique	Identification de code malveillant, reconstruction du scénario d'attaque
Administration WordPress	Migration de version, gestion BDD, architecture plugin/thème
Cybersécurité	Durcissement serveur, gestion des droits, protocoles ANSSI
Développement web	PHP, CSS/Flexbox, débogage, optimisation de performance
Administration système	SSH, permissions Linux, configuration serveur web (Apache)
Logiciel métier	PHP back-end, MySQL, JavaScript, moteur workflow asynchrone

Compétences méthodologiques

Gestion de crise	Priorisation des urgences, décisions rapides sous pression
Rigueur méthodologique	Protocoles de nettoyage, traçabilité des actions
Documentation technique	Procédures de restauration, guides d'exploitation
Communication client	Explication vulgarisée de problèmes complexes à la mairie

Compétences comportementales

Autonomie	Gestion complète du projet de A à Z sans supervision constante
Patience	Inspection manuelle de milliers de fichiers PHP infectés
Adaptabilité	Reconstruction complète en l'absence de backup exploitable
Esprit critique	Détection de patterns suspects et analyse forensique

11 Conclusion & Bilan

Une expérience professionnelle intense

Ce stage au sein de CEOS IT m'a confronté dès le premier jour à une situation réelle de cyberattaque sur une infrastructure publique. J'ai dû mobiliser rapidement l'ensemble de mes connaissances techniques tout en développant de nouvelles compétences sur le terrain.

Maîtrise complète de la chaîne d'intervention

La mission de restauration WordPress m'a permis de couvrir l'ensemble du cycle : analyse forensique, décontamination, migration, développement web et sécurité système — une expérience rarement accessible en formation initiale.

Vision globale du logiciel métier

Le développement de fonctionnalités dans MOBIBAT (métriques, workflow, crontab, archivage PDF) m'a apporté une vision complète du cycle de vie d'un logiciel : architecture, implémentation, tests, intégration et maintenance.

Orientation professionnelle confirmée

Cette expérience conforte mon orientation vers les métiers de la **cybersécurité** et de l'**administration système sécurisée**. Elle a renforcé des compétences transversales essentielles : autonomie, rigueur, communication et gestion de la pression.

Je tiens à remercier chaleureusement l'équipe CEOS IT pour leur confiance, leur accompagnement et leur disponibilité tout au long de ce stage.

Bryan Tillou
Étudiant BTS SIO
Mars 2026

CEOS IT
Entreprise d'accueil
Béthune (62)