

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS						SESSION 2025	
Tableau de synthèse des réalisations professionnelles							
NOM et prénom : Gheorghe-Tony LAMBERT-TATHY				N° candidat :			
Centre de formation : SUP'CHASSAGNES				Option :SISR		SESSION 2025	
Adresse URL du portfolio : tony.lamberttathy.com							
<div>Compétences mises en œuvre</div> <div>Réalisations professionnelles (intitulé et liste des documents et productions associés)</div>	Période (sous la forme du JJ/MM/AA au JJ/MM/AA)	B1.1-Gérer le patrimoine informatique	Répondre aux incidents et aux demandes d'assistance et d'évolution	Développer la présence en ligne de l'organisation	Travailler en mode projet	Mettre à disposition des utilisateurs un service informatique	Organiser son développement professionnel
		<ul style="list-style-type: none"><li>• B1.1.1- Recenser et identifier les ressources numériques</li><li>• Explorer des référentiels, normes et standards adoptés par le secteur</li><li>• Mettre en place et vérifier les niveaux d'habilitation associés à un service</li><li>• Vérifier les conditions de mise à jour d'un service informatique</li><li>• Gérer des sauvegardes</li><li>• Vérifier le respect des règles d'utilisation des ressources numériques</li></ul>	<ul style="list-style-type: none"><li>• Collecter, suivre et orienter des demandes</li><li>• Traiter des demandes concernant les services réseau et système, les applications</li><li>• Traiter des demandes concernant les applications</li></ul>	<ul style="list-style-type: none"><li>• Participer à la valorisation de l'image de l'organisation sur les médias numériques en utilisant les outils de réseaux sociaux et des enjeux économiques</li><li>• Réviser les services en ligne de l'organisation et mesurer leur impact</li><li>• Participer à l'évolution d'un site Web exploitant les données de l'organisation.</li></ul>	<ul style="list-style-type: none"><li>• Analyser les objectifs et les modalités d'organisation d'un projet</li><li>• Planifier les activités</li><li>• Evaluer les indicateurs de suivi d'un projet et analyser les écarts</li></ul>	<ul style="list-style-type: none"><li>• Réaliser les tests d'intégration et d'acceptation d'un service</li><li>• Accompagner les utilisateurs dans la mise en place d'un service</li></ul>	<ul style="list-style-type: none"><li>• Mettre en place son environnement d'apprentissage personnel</li><li>• Mettre en œuvre des outils et stratégies de veille informationnelle</li><li>• Développer son projet professionnel</li></ul>
Réalisation en cours de formation							
TP-AP-TD-Cours							
Portfolio	09/2024 au 14/04/2025						B1.6.4
TPs-GLPI	11/24 au 12/2024		B.1.2.1				
Veille technologique	09/2024 au 14/04/2025						B1.6.2
MOOC Cybersécurité et MOOC RGPD	12/2024 au 15/04/2024						B1.6.1
AP M@banque	23/01 au 01/04/2024	B1.1.3, B1.1.5, B1.1.6	B1.2.2			B1.5.2	
GSB	09/01/2024 au 24/01/2024			B1.3.1 B1.3.2 B1.3.3	B1.4.2	B1.5.2	
Projet RTL Industrie (infrastructure réseau + IA + HA + VPN)	10/2024 au 06/2025	B1.1.1, B1.1.4 , B1.1.5	B1.2.2		B1.4.1	B1.5.1 B1.5.2 B1.5.3	
AP InfoDev – Gestion de projet (Trello, méthode Kanban)	02/02 au 01/04/2024				B1.4.1 B1.4.2 B1.4.3		B1.6.4
Présentation et analyse technique de l'APT 41 : DOUBLE DRAGON	10/2024 au 11/2024	B1.1.6			B1.4.1 B1.4.2	B1.5.3	B1.6.2 B1.6.3
Réalisations en milieu professionnel en cours de première année							
Stage 1 ère année du 06/05/2024 au 07/06/2024							
Objectif du stage : Réalisation de tests d'intrusion sur les sites web de deux clients pour identifier les failles de sécurité, rédiger des rapports d'analyse, proposer des solutions, et vérifier leur efficacité après implémentation.							
Installation de l'environnement de travail – Kali Linux, configuration de VPN, mise en place des outils (ZAP, Burp Suite, WPScan, Nmap, etc.)		B1.1.1					B1.6.1
Définition du périmètre de test avec le tuteur – Approche boîte noire, choix des outils, identification des attentes clients			B1.2.1		B1.4.1		
Analyse préliminaire des cibles (reconnaissance passive) – Utilisation de TheHarvester, Wappalizer pour collecter des infos techniques		B1.1.1	B1.2.2			B1.5.1	
Scan de vulnérabilités WordPress avec WPScan – Identification de plugins vulnérables, versions obsolètes			B1.2.2			B1.5.1	
Tentatives de brute force sur comptes admin WordPress – Génération de wordlist ciblée, stratégie d'attaque personnalisée		B1.1.6				B1.5.1	
Scan réseau avec Nmap – Découverte de ports ouverts et services actifs		B1.1.1	B1.2.2				
Analyse des flux HTTP avec ZAP et Burp Suite – Interception de requêtes, test de vulnérabilités XSS et injections		B1.1.6				B1.5.1	
Recherche de fichiers cachés avec FFuF et DirBuster – Exploration de l'arborescence non indexée du site			B1.2.2			B1.5.1	
Élaboration d'une matrice de risques selon ISO 27005 – Evaluation des risques selon l'impact et la probabilité		B1.1.4			B1.4.3		
Rédaction de rapports techniques et synthèses hebdomadaires – Description des vulnérabilités, preuves, solutions proposées						B1.5.3	B1.6.3
Résolution de problèmes liés au filtrage IP – Contournement avec l'option Onion Over VPN de NordVPN					B1.4.3		B1.6.2
Propositions de solutions aux clients + plan d'action sécurité – Recommandations concrètes (mises à jour, protections supplémentaires, etc.)			B1.2.3			B1.5.3	
Réalisations en milieu professionnel en cours de deuxième année							
Stage 2 ème année du 06/01/2025 au 21/02/2025							
Partie 1 : Automatisation des posts LinkedIn / Facebook							
Analyse du besoin et rédaction du plan d'automatisation			B1.2.1		B1.4.1		