Projet Tutoré Fiche Projet

SecureHub

BUT3 2024 – 2025

Nom de l’intervenant :

Michelle Bouvart

Florian Duchemin

Ganche Nolwenn

Khaled Maroua

Faurie Joris

Josselin Corby Ulysse

Description générale du projet

Le projet s'intitule SecureHub. Ce projet est à destination des entreprises souhaitant répondre aux exigences du NIS2. L'équipe regroupe Nolwenn et Joris, spécialistes du développement Frontend et Backend, Ulysse, expert en cybersécurité, et Maroua, responsable de la gestion de projet et commerciale. La date de démarrage est fixée en octobre 2024, avec une finalisation prévue pour juin 2025.

Contexte et objectifs

Les entreprises rencontrent des défis croissants dans la gestion de l'authentification multi-facteurs (2FA), en particulier dans les systèmes multi-applications où les solutions sont souvent non centralisées. Cette complexité entraîne des coûts élevés et une administration chronophage. Notre objectif est de concevoir une plateforme auto-hébergée, intégrant des solutions open-source, pour simplifier et centraliser la gestion du 2FA. Cela permettra de renforcer la sécurité des accès tout en optimisant la gestion administrative. Cette solution se distingue par son hébergement interne, permettant aux entreprises de stocker les accès 2FA sur leurs propres serveurs, garantissant ainsi un niveau élevé de confidentialité et de sécurité des données.

Parties prenantes et public visé

Les parties prenantes du projet incluent le commanditaire, qui définit les exigences et valide les livrables, ainsi que les entreprises souhaitant simplifier leur gestion du 2FA. Les utilisateurs de la solution, notamment les administrateurs systèmes, jouent un rôle clé dans la gestion et la configuration de la plateforme. Cette solution est particulièrement adaptée aux organisations des secteurs sensibles, comme la finance, la santé ou la défense, où la protection des données est cruciale. En centralisant et sécurisant les accès 2FA sur leurs propres serveurs, ces entreprises peuvent contrôler l'accès à leurs données, renforçant ainsi leur posture de cybersécurité.

Résumé du projet

Le projet comprend quatre phases principales : analyse des besoins, développement (frontend et backend), tests de sécurité et documentation finale. Les tâches clés incluent l'intégration de FreeOTP pour les codes TOTP (Time-based One-Time Password) et d'Authelia pour la gestion centralisée du 2FA. Les technologies et outils nécessaires incluent des plateformes open-source et des serveurs de tests internes. Les solutions sont susceptibles d'évoluer au cours de la mise en œuvre technique du projet.

Échéancier et phases du projet

Phase	Description	Échéance
Analyse des besoins	Collecte des besoins et rédaction de spécifications	Livrable 1 et 2
Prototype	Développement d'un premier prototype	Mi-janvier
Développement Backend/Frontend	Codage et intégration des API 2FA	Mars
Tests de sécurité	Exécution des tests de sécurité et validation des processus	Mai
Présentation finale	PoC (Proof of Concept) et démonstration au commanditaire	Juin

Livrables et critères de qualité

Livrable	Description	Critère de Qualité
Documentation technique	Instructions de configuration et utilisation	Clarté et exhaustivité

Rapport de sécurité	Analyse des résultats des tests et recommandations	Conformité avec les normes de sécurité
Présentation finale (PoC)	Démonstration de la solution en conditions réelles	Validation par le commanditaire

Contraintes et risques

Le projet devra respecter plusieurs contraintes, incluant la disponibilité de serveurs de test adaptés aux solutions open-source, ainsi que la conformité avec le RGPD pour la gestion des données d'authentification. Les principaux risques identifiés sont une possible incompatibilité avec certains systèmes d'entreprise et la complexité de déploiement multi-sites.

Déploiement et utilisation

L'application déployée doit être simple à installer et à configurer sur tout environnement Linux standard ou via Docker/LXC. Le processus de configuration doit être automatisé autant que possible, avec des paramètres par défaut sécurisés et une option de personnalisation via des fichiers de configuration ou des scripts. L'application doit offrir une interface graphique propre, intuitive et facile à utiliser. L'interface doit permettre une prise en main rapide, avec des fonctionnalités accessibles sans nécessiter de connaissances techniques avancées.

Utilité

La solution doit apporter une valeur ajoutée en matière de sécurité, en protégeant les systèmes contre les menaces externes et internes. Elle doit intégrer des mécanismes de chiffrement, de gestion des accès, et de journalisation des activités pour renforcer la protection des données. De plus, elle doit permettre une réponse rapide en cas d'incident de sécurité, tout en respectant les standards de conformité réglementaire.

Documentation complète

Une documentation claire et détaillée, incluant des étapes simples et des exemples de commandes pour l'installation, la configuration et la mise en place de la solution, est essentielle. Elle doit inclure des guides pour différents cas d'usage, avec des explications sur la configuration des paramètres.

Valeur et bénéfices

Ce projet permettra aux entreprises de réduire les coûts, de simplifier la gestion du 2FA et de renforcer la sécurité de leurs systèmes d'information. En répondant aux besoins des utilisateurs, cette solution apportera une valeur ajoutée en termes d'efficacité et de sécurité, tout en étant évolutive et adaptable à des environnements variés.

Procédure de gestion des modifications

Toute modification concernant les objectifs, le périmètre ou les ressources devra être validée par l'ensemble du groupe. Les changements devront inclure une révision de l'impact sur le planning, les ressources humaines et le budget.

Ressources et budget

Les ressources principales pour ce projet comprennent une équipe technique spécialisée, des serveurs de test virtuels (VM) et l'utilisation exclusive de solutions open-source. Les partenaires incluront des fournisseurs de solutions open-source comme DOCKER, Free OTP pour garantir la conformité et l'efficacité de la solution.