PROJET SMART REALISATION - SafeLink

PARTIE 2 : ANALYSE

1. GROUPE D'UTILISATEURS CIBLÉS

Persona 1 : Sophie Martin - Responsable IT PME

Caractéristiques :

- Âge : 35 ans
- Situation professionnelle : Responsable informatique dans une PME de 50 employés
- Formation : Ingénieur en informatique
- Centres d'intérêt : Cybersécurité, automatisation, domotique professionnelle
- Habitudes : Utilise quotidiennement des tableaux de bord de monitoring, applications de gestion de parc informatique

Objectif et enjeux quotidiens :

- Sécuriser le parc d'objets connectés de l'entreprise (caméras, capteurs, thermostats intelligents)
- Réduire les risques de cyberattaques via les objets connectés
- Maintenir la conformité RGPD et les normes de sécurité
- Optimiser les coûts de sécurité informatique

Problématiques de frustrations :

- Les solutions de cybersécurité IoT professionnelles sont trop coûteuses pour une PME
- Manque de visibilité sur ce que les objets connectés échangent réellement
- Difficulté à détecter les comportements anormaux des devices IoT
- Complexité des outils existants nécessitant des compétences avancées

Environnement d'utilisation :

- Ordinateur (bureau et portable)
- Connexion internet stable au bureau
- Accès distant occasionnel via VPN
- Environnement Windows/Linux

Solution actuelle (compensation) :

- Utilise des solutions de firewall classiques non adaptées à l'IoT
- Vérifications manuelles et sporadiques des logs réseau
- Segmentation réseau basique sans monitoring spécifique

Persona 2 : Marc Dubois - Passionné de domotique

Caractéristiques :

- Âge : 42 ans

- Situation professionnelle : Ingénieur télécommunications
- Familiale : Marié, 2 enfants
- Centres d'intérêt : Domotique, DIY électronique, sécurité informatique
- Habitudes : Installe lui-même des équipements connectés, suit les forums tech

❖ **Objectifs et enjeux quotidiens :**

- Protéger sa famille et son domicile équipé de nombreux objets connectés
- Garantir la confidentialité des données personnelles (caméras, assistants vocaux)
- Comprendre et contrôler les communications de ses devices
- Optimiser la surveillance de son réseau domotique

❖ **Problématiques de frustrations :**

- Inquiétude concernant les failles de sécurité des objets connectés chinois
- Manque de transparence des fabricants sur la gestion des données
- Absence d'outil accessible pour monitorer son réseau IoT domotique

❖ **Environnement d'utilisation :**

- Crainte de piratage et d'accès non autorisé à ses caméras/capteurs
- Smartphone/tablette principalement
- Réseau WiFi domestique personnalisable
- Préférence pour des solutions open-source ou personnalisables

❖ **Solution actuelle (compensation) :**

- Utilise des VLANs pour isoler les objets connectés
- Surveille occasionnellement les logs de son routeur
- Lit les forums pour identifier les vulnérabilités communes
- Bloque certains devices de communication avec l'extérieur

Persona 3 : Fatima Nkoto - Gestionnaire d'établissement scolaire

❖ **Caractéristiques** :

- Âge : 38 ans
- Situation professionnelle : Directrice adjointe d'un établissement scolaire
- Formation : Gestion administrative
- Centres d'intérêt : Innovation pédagogique, sécurité des élèves
- Habitudes : Utilise des outils digitaux simples et intuitifs

❖ **Objectif et enjeux quotidiens :**

- Assurer la sécurité physique de l'établissement (détecteurs de fumée, caméras)
- Gérer les systèmes de contrôle d'accès et de surveillance
- Respecter les réglementations sur la protection des données des mineurs
- Maintenir un budget limité pour l'infrastructure

❖ **Problématiques de frustrations :**

- Compétences techniques limitées en cybersécurité
- Besoin d'une interface simple et compréhensible
- Inquiétude sur les risques de piratage des systèmes de sécurité
- Difficulté à justifier des investissements en cybersécurité IoT

❖ **Environnement d'utilisation :**

- Ordinateur de bureau principal
- Tablette pour supervision mobile dans l'établissement
- Connexion internet variable selon les zones
- Besoin d'alertes en temps réel sur smartphone

❖ **Solution actuelle (compensation) :**

- Fait confiance aux systèmes installés sans monitoring actif
- Dépend d'un prestataire externe pour les problèmes
- Vérifications visuelles manuelles des équipements
- Absence de système de détection d'intrusion réseau

2. BÉNÉFICES DE LA SMART RÉALISATION (Méthode SMART)

- **Pour Sophie (Responsable IT PME)**

Spécifique : Réduire les incidents de sécurité liés aux objets connectés de 80% en détectant automatiquement les comportements anormaux (connexions suspectes, échanges de données inhabituels).

Mesurable :

- Nombre d'alertes de sécurité générées et traitées
- Temps de détection d'une anomalie : < 5 minutes
- Nombre d'objets connectés monitorés : 100% du parc IoT
- Taux de faux positifs : <10%

Atteignable : Grâce à l'interface centralisée MQTT et aux capteurs ESP32, le système peut surveiller en temps réel tous les objets connectés sur le réseau de l'entreprise.

Réaliste : Le prototype utilise des technologies éprouvées (ESP32, MQTT, Raspberry Pi) et accessible, adaptées au budget d'une PME (< 500€ pour le prototype complet).

Temporel :

- Mise en place du prototype : 3 mois
- Détection d'anomalies opérationnelle : 4 mois
- ROI attendu : 6 mois (réduction des coûts de gestion des incidents)

- **Pour Marc (Passionné domotique)**

Spécifique : Obtenir une visibilité complète sur 100% des communications de ses 25 objets connectés domotiques via un tableau de bord intuitif accessible depuis son smartphone.

Mesurable :

- Nombre de devices IoT monitorés en temps réel
- Temps d'identification d'un device compromis : < 10 minutes
- Fréquence de consultation du dashboard : quotidienne
- Satisfaction utilisateur : >8/10

Atteignable : L'interface web responsive développée sur Raspberry Pi permet un accès depuis n'importe quel appareil connecté au réseau local. Possibilité d'extension via VPN.

Réaliste : Le système (<200€ en matériel) et sa modularité permettent une adoption progressive et personnalisation selon les besoins spécifiques.

Temporel :

- Installation du système : 1 week-end
- Configuration des capteurs : 2 semaines
- Apprentissage et optimisation : 1 mois
- Automatisation complète : 2 mois

- **Pour Fatima (Gestionnaire établissement)**

Spécifique : Garantir un monitoring continu des 15 systèmes de sécurité IoT de l'établissement (détecteurs, caméras, contrôles d'accès) avec alertes automatiques en cas d'anomalie.

Mesurable :

- Disponibilité du système de monitoring : >99%
- Temps de réponse aux alertes critiques : <2 minutes
- Nombre d'incidents détectés proactivement : augmentation de 100%
- Formation du personnel : 100% en 1 mois

Atteignable : Interface simplifiée avec système d'alertes par notifications et codes couleurs intuitifs, ne nécessitant pas de compétences avancées.

Réaliste : Solution adaptée aux contraintes budgétaires des établissements publics, avec possibilité de déploiement progressif et maintenance simplifiée.

Temporel :

- Phase pilote : 2 mois
- Déploiement complet : 4 mois
- Formation complète du personnel : 1 mois
- Évaluation de l'efficacité : tous les 6 mois

3. ANALYSE DE LA CONCURRENCE

Solutions commerciales existantes

1. Cisco IoT Threat Defense

- Enterprise : Cisco Systems
- Description : Solution professionnelle de sécurité IoT pour entreprises
- Prix : 5.000€ - 50.000€ selon le nombre de devices
- Avantages :
    - Intégration avec l'écosystème Cisco
    - Support 24/7
    - Détection avancée par IA
- Inconvénients :
    - Coût prohibitif pour PME
    - Nécessite des pros sur site avec particuliers
    - Complexe, expertise technique pointue
- Utilisation : Grandes entreprises et infrastructures critiques

2. Firewall (Purple Gold)

- Enterprise : Firewall LLC
- Description : Boîtier de sécurité réseau pour foyers et petites entreprises
- Prix : 350€ - 600€ (achat unique)
- Avantages :
    - Facile à installer
    - Barrière intuitive
    - Protection générale
- Inconvénients :
    - Monitoring IoT limité
    - Pas de personnalisation avancée
    - Boîte noire (pas open-source)
    - Pas de capteurs environnementaux intégrés
- Utilisation : Foyers connectés, petits bureaux

3. Home Assistant + Add-ons sécurité

- Enterprise : (Open-source Nabu Casa pour support)
- Description : Plateforme domotique avec modules de sécurité
- Prix : Gratuit (open-source) + matériel (150-500€)
- Avantages :
    - Open-source et personnalisable
    - Large communauté
    - Intégrations multiples
- Inconvénients :
    - Configuration complexe
    - Précise sur la cybersécurité IoT
    - Nécessite compétences techniques
    - Monitoring réseau basique
- Utilisation : Passionnés tech, makers

4. Fing Desktop/Business

- Enterprise : Fing Limited
- Description : Outil de découverte et monitoring réseau
- Prix : Gratuit (version basique) / 36-156/mois (Premium) / Sur devis (business)
- Avantages :
    - Interface simple
    - Détection automatique des devices
    - Alertes de sécurité basiques
- Inconvénients :
    - Fonctionnalités limitées en version gratuite
    - Pas de capteurs physiques
    - Monitoring passif uniquement
    - Analyse de trafic superficielle
- Utilisation : Particuliers, PME

Analyse comparative : Positionnement de SafeLink

Critère	Solutions pro (Cisco)	Solutions grand public (Firewalla)	Open-source (Home Assistant)	SafeLink
Prix	5 000€+	350-600€	150-500€	< 200€
Complexité	Élevée	Faible	Moyenne	Moyenne
Personnalisation	Limitée	Très Limitée	Élevée	Élevée
Capteurs physiques	Non	Non	Oui (via intégrations)	Oui (intégrés)
Focus Cybersécurité IoT	Élevée	Moyen	Faible	Élevée
Open-source	Non	Non	Oui	Oui
Cible	Grandes entreprises	Foyers/PME	Makers	PME/Makers/Education

❖ **Problématiques identifiées chez la concurrence**

1. Cap de prix : Soit très cher (solutions pro), soit fonctionnalités limitées (solutions grand public)
2. Manque de transparence : Solutions propriétaires "boîte noire"
3. Absence de capteurs physiques : Monitoring purement réseau, sans détection environnementale
4. Complexité ou limitations : Soit trop complexe (HA), soit trop limité (Fing, Firewalla)
5. Pas de focus éducatif : Aucune solution adaptée à l'apprentissage de la cybersécurité IoT

Opportunité pour SafeLink : SafeLink se positionne sur un segment inexploité :

- Solution abordable (<200€) avec focus cybersécurité IoT
- Capteurs physiques intégrés (détection environnementale + réseau)

- Open-source éducatif (apprentissage, personnalisation)
- Cible PME, makers et établissements éducatifs
- Modulaire et évolutif selon les besoins

4. PÉRIMÈTRE

4.1 Exigences Fonctionnelles

Story Mapping: SafeLink

[Note: There is a small checkbox image here, likely representing a story map diagram, but no detailed map is provided in text.]

Activités Utilisateur

- Surveillance réseau IoT
  - Visualiser tous les devices connectés
  - Consulter l'état en temps réel
  - Voir l'historique des connexions
  - Identifier les devices non autorisés
- Détecter les anomalies
  - Recevoir des alertes en temps réel
  - Analyser les patterns de communication
  - Identifier les comportements suspects
  - Visualiser les tentatives d'intrusion
- Monitorer l'environnement
  - Consulter température/humidité
  - Détecter les mouvements (PIR)
  - Surveiller la qualité de l'air (MQ2/MQ7)
  - Détecter les variations de luminosité
- Gérer la sécurité
  - Configurer les règles d'alerte
  - Bloquer/autoriser des devices
  - Définir des zones de confiance
  - Exporter les logs de sécurité
- Administrer le système
  - Ajouter/supprimer des nœuds ESP32
  - Configurer les capteurs
  - Mettre à jour le firmware
  - Sauvegarder/restaurer la configuration

❖ **User Stories Prioritaires**

- Épic 1 : Monitoring Réseau

US1.1 - Visualisation des devices En tant qu'administrateur réseau, Je veux voir la liste de tous les objets connectés sur mon réseau Afin de connaître en temps réel l'état de mon parc IoT Priorité : HAUTE | Estimation : 5 points

US1.2 - Détection automatique En tant qu'utilisateur, Je veux être alerté automatiquement lorsqu'un nouvel appareil se connecte Afin de détecter les connexions non autorisées Priorité : HAUTE | Estimation : 8 points

US1.3 - Analyse de trafic En tant que responsable sécurité, Je veux visualiser le volume et la nature des échanges de données Afin d'identifier les communications anormales Priorité : MOYENNE | Estimation : 13 points

- Épic 2 : Détection d'Intrusion

US2.1 - Alertes comportementales En tant qu'utilisateur, Je veux recevoir une notification lorsqu'un device a un comportement suspect Afin de réagir rapidement à une potentielle intrusion Priorité : HAUTE | Estimation : 13 points

US2.2 - Détection physique En tant que gestionnaire de sécurité, Je veux être alerté en cas de mouvement détecté dans une zone sensible Afin de prévenir les intrusions physiques Priorité : MOYENNE | Estimation : 5 points

US2.3 - Corrélation Événements En tant qu'analyste sécurité, Je veux corréler les événements réseau et physiques Afin de détecter les patterns d'attaque complexes Priorité : BASSE | Estimation : 21 points

- Épic 3 : Monitoring Environnemental

US3.1 - Dashboard environnemental En tant qu'utilisateur, Je veux visualiser les données environnementales (température, humidité, gaz) Afin de surveiller les conditions de mes équipements Priorité : MOYENNE | Estimation : 8 points

US3.2 - Alertes environnementales En tant que responsable sécurité, Je veux être alerté en cas de détection de gaz dangereux ou de conditions anormales Afin de prévenir les risques d'incendie ou d'intoxication Priorité : HAUTE | Estimation : 3 points

- Épic 4 : Administration

US4.1 - Configuration des nœuds En tant qu'administrateur, Je veux ajouter et configurer de nouveaux nœuds ESP32 Afin de gérer mon réseau de surveillance Priorité : HAUTE | Estimation : 8 points

US4.2 - Gestion des règles En tant qu'utilisateur avancé, Je veux définir des règles personnalisées de détection Afin d'adapter le système à mes besoins spécifiques Priorité : MOYENNE | Estimation : 13 points

US4.3 - Export et reporting En tant que responsable conformité, Je veux exporter les logs et générer des rapports Afin de documenter les incidents et assurer la conformité Priorité : BASSE | Estimation : 8 points

4.2 Exigences Non Fonctionnelles

❖ **Sécurité**

- Authentification forte : Accès à l'interface web protégé par login/mot de passe (minimum 12 caractères, complexité requise)
- Chiffrement des communications : MQTT avec TLS 1.3, HTTPS pour l'interface web
- Isolation réseau : VLAN dédié pour les nœuds ESP32, séparation du réseau de production
- Logs sécurisés : Horodatage cryptographique, intégrité vérifiable
- Mises à jour sécurisées : OTA (Over-The-Air) avec signature numérique

❖ **Performance et Capacité**

- Latence : Détection d'anomalie < 5 secondes
- Throughput : Support de 50 devices simultanés minimum
- Stockage des données : Logs conservés 30 jours, agrégation 1 an
- Disponibilité : 99% uptime, avec downtime maximum 1h/mois
- Ressources : Fonctionnement sur Raspberry Pi 3B+ minimum (1 Go RAM)

❖ **Compatibilité**

- Protocoles : MQTT, HTTP/HTTPS, CoAP (future extension)
- Capteurs : Support DHT22, PIR, MQ2, MQ7, phototransistors
- Navigateurs : Chrome, Firefox, Safari, Edge (versions récentes)
- Systèmes : Interface responsive (desktop, tablette, smartphone)
- Standards : Conforme IEEE 802.11 (WiFi), MQTT 3.1.1

❖ **Fiabilité et Disponibilité**

- Redondance capteurs : DHT22 x2 pour tolérance aux pannes
- Monitoring : Régémarrage automatique des ESP32 en cas de freeze
- Alimentation : Batteries Li-ion pour fonctionnement sur batterie (24h minimum)
- Recovery : Sauvegarde automatique configuration toutes les 6h
- Failover : Stockage local sur ESP32 en cas de perte connexion broker

❖ **Évolutivité**

- Architecture modulaire : Ajout de nœuds sans reconfiguration globale
- Scalabilité : Support GPIO pour distribution multi-niveaux capteurs
- API : REST API pour intégration avec systèmes tiers
- Plugins : Système de plugins pour nouvelles fonctionnalités

❖ **Maintenabilité**

- Code open-source : Documentation complète, GitHub
- Mise à jour OTA : Firmware ESP32 et Raspberry Pi updatable à distance
- Logs détaillés : Niveaux DEBUG, INFO, WARNING, ERROR
- Monitoring système : Métriques CPU, RAM, réseaux visibles dans l'interface
- Configuration centralisée : Fichiers de config YAML/JSON éditables

❖ **Utilisabilité**

- Interface intuitive : Courbe d'apprentissage < 30 minutes
- Dashboard temps réel : Rafraîchissement automatique toutes 5 secondes
- Visualisations : Graphiques interactifs, codes couleurs (vert/orange/rouge)
- Accessibilité : WCAG 2.1 niveau AA, support lecteurs d'écran
- Multilingue : Français et Anglais (autres langues extensibles)
- Mobile-first : Interface tactile optimisée pour smartphones

5. RESSOURCES NÉCESSAIRES

5.1 Ressources Humaines

Équipe de Développement (4 personnes)

Développeur IoT / Firmware (1 personne - 40% temps)

- Gestion des capteurs et GPIO
- Optimisation énergétique
- Programmation ESP32 C++/Arduino
- Configuration MQTT et protocoles IoT

Développeur Backend (1 personne - 30% temps)

- Serveur MQTT (Mosquitto)
- Base de données (InfluxDB/PostgreSQL)
- API REST/WebSocket
- Logique de détection d'anomalies
- Compétences : Python/Node.js, MQTT, SQL/NoSQL, Docker

Développeur Frontend / UX (1 personne - 30% temps)

- Dashboard temps réel
- Visualisations de données (charts, graphs)
- Design UX/UI
- Compétences : React/Vue.js, HTML/CSS, D3.js/Chart.js, UI/UX

Spécialiste Cybersécurité / DevOps (1 personne - 20% temps)

- Architecture sécurisée (TLS, authentification)
- Tests d'intrusion et vulnérabilités
- Configuration réseau (VLANs, firewall)
- CI/CD et déploiement
- Compétences : Sécurité réseau, Kali Linux, Docker, Git/GitHub Actions

5.2 Ressources Matérielles

Prototype (déjà identifié dans la demande)

- ESP32 x4

- Raspberry Pi 3B+ (avec carte microSD 32 Go)
- Capteurs : DHT22 x2, PIR x2, MQ2, MQ7, Phototransistor x2
- Breadboards x4
- Batteries Li-Ion 18650 + TP4056 x4
- LEDs x10
- Câbles de connexion
- Box WiFi
- Coût estimé : ~150-200€

Équipement de développement

- Ordinateurs de développement x4 (déjà possédés par l'équipe)
- Multimètre, oscilloscope (laboratoire)
- Switch réseau géré pour tests VLAN
- Routeur WiFi dédié aux tests

Infrastructure logicielle

- GitHub (gratuit pour open-source)
- Serveur de test/staging (petit hébergé sur Raspberry Pi supplémentaire)
- Outils de développement (VS Code, Arduino IDE, PlatformIO - gratuits)

5.3 Ressources de Connaissance et Formation

Documentation technique nécessaire :

- Datasheets ESP32, capteurs
- Protocoles MQTT, TLS
- Bonnes pratiques cybersécurité IoT (OWASP IoT Top 10)

Formation complémentaire si nécessaire :

- Sécurité des systèmes embarqués (2 jours)
- Analyse de trafic réseau avec Wireshark (1 jour)

5.4 Budget Estimatif

Catégorie	Coût	Remarques
Matériel prototype	200€	Fournir par le laboratoire
Équipement développement (tests)	6-50€	Déjà disponible
Hébergement cloud (tests)	8-50€	Option VPS pour tests distants
Formation	0-500€	Si formations nécessaires
Divers (câbles, composants)	50€	Marge imprévus
TOTAL	250-800€	Selon besoins formation

6. PERSPECTIVES À LONG TERME

6.1 Évolutions Techniques Post-Prototype

Phase 1 : Consolidation (6-12 mois)

- Amélioration de l'IA de détection
  - Implémentation d'algorithmes de machine learning (anomaly detection, clustering)
  - Apprentissage des patterns normaux pour réduction des faux positifs
  - Détection comportementale avancée (analyse temporelle, corrélations)
- Extension des capteurs
  - Support de nouveaux types de capteurs (vibration, son, qualité eau/air)
  - Intégration de caméras avec détection par vision (OpenCV)
  - Capteurs biométriques pour contrôle d'accès
- Optimisation énergétique
  - Mode deep sleep pour ESP32
  - Alimentation solaire pour autonomie
  - Panneaux solaires pour autonomie
  - Durée de vie batterie : 7 jours

Phase 2 : Industrialisation (12-24 mois)

- Scalabilité
  - Architecture distribuée multi-sites
  - Support de 500+ devices simultanés
  - Cloud hybrid (local + cloud pour analytics)
- Conformité et Certifications
  - Certification CE pour commercialisation Europe
  - Conformité RGPD renforcée
  - Standards industriels (IEC 62443 pour cybersécurité industrielle)
- Intégrations tierces
  - API publique pour intégrations (Zapier, IFTTT)
  - Connexions pour SIEM (Splunk, ELK)
  - Intégration avec plateformes domotiques (Home Assistant, Jeedom)

Phase 3 : Écosystème (24+ mois)

- Marketplace de plugins
  - Communauté de développeurs
  - Plugins certifiés et non-certifiés
  - Modèle économique freemium
- Services managés
  - SafeLink-as-a-Service (SaaS)
  - Monitoring 24/7 par équipe SOC
  - Support premium et SLA
- Développements premium
  - Versions pro/enterprise
  - SafeLink Pro : Version entreprise avec support
  - SafeLink EDU : Version éducative avec ressources pédagogiques

6.2 Marchés et Segments Ciblés

Marché Primaire (0-2 ans)

- PME (10-250 employés) : secteurs tertiaire, santé, retail
- Makers et passionnés tech : communauté DIY, FabLabs
- Établissements éducatifs : lycées techniques, universités, centres de formation

Objectif : 200 installations, 50 k€ CA

Marché Secondaire (2-5 ans)

- Collectivités locales : mairies, bibliothèques, équipements publics
- Industriel léger : ateliers, petites usines, entrepôts
- Santé : cabinets médicaux, EHPAD, petites cliniques

Objectif : 1000 installations, 300 k€ CA

Marché Tertiaire (5+ ans)

- Grands comptes (via partenariats)
- Secteur agricole connecté (AgriTech)