Cahier des Charges – Projet M2 Mastère Cybersécurité

Titre : Mise en place d'un SOC externalisé pour un réseau d'audioprothésistes

I. Contexte et objectifs du projet

Le client est un réseau de centres d'audioprothésistes répartis sur une trentaine de points de vente en France. Face à l'augmentation des menaces et au manque de ressources internes, la direction souhaite mettre en place un SOC externalisé. Ce projet vise à concevoir une plateforme de démonstration fonctionnelle, sécurisée, documentée et industrialisable.

Objectifs généraux :

- Déployer un SOC externalisé centralisant les événements de sécurité ;
- Créer un environnement de démonstration opérationnel ;
- Fournir un système industrialisable, intégrable dans un modèle d'infogérance.

II. Organisation de l'entreprise et besoins par brique SI

Brique SI	Description	Besoins de monitoring spécifiques
Postes de travail	Utilisés par les audioprothésistes	Auth. locales, exécutions suspectes, usage USB
Routeurs / Firewall	Équipements par centre	Flux réseau, accès non autorisés, config
Applications métiers	CRM, RDV, Dossiers patients	Logs applicatifs, erreurs, accès anormaux
Serveurs internes	Active Directory, fichiers	Accès partages, élévation de privilèges
Messagerie pro	Outlook, Zimbra, webmail	Phishing, spam, pièces jointes malveillantes

III. Fonctionnalités attendues du SOC

- Collecte multi-source (agents, syslog, API) ;
- SIEM open-source centralisé ;
- Règles de détection et alerting personnalisables ;
- Dashboards lisibles et segmentés ;
- Playbooks de réponse semi-automatisés ;

- Reporting simple et exportable ;
- Interface claire, accès web ;
- Reproductibilité et scalabilité de la solution.

IV. Interface utilisateur

L'interface sera web-based (UI des outils ou surcouche simple) et devra être :

- Accessible via navigateur ;
- Segmentée par rôles (supervision / analyste / admin) ;
- Lisible, ergonomique, documentée ;
- Optionnellement : CLI ou API exposée si automatisation prévue.

V. Intégration avec le SI existant

- Simulation d'un ou plusieurs sites clients (VMs ou conteneurs) ;
- Génération de logs réalistes (attaque/safe) ;
- Templates de déploiement client ;

VI. Répartition des rôles et tâches

Exemple de répartition des taches

- Étudiant 1 : Ingénieur SIEM – déploiement, collecte, intégration technique ;
- Étudiant 2 : Analyste SOC – détection, dashboards, playbooks de réponse ;
- Étudiant 3 : Coordinateur – supervision, démo, documentation complète.

Travail partagé : gestion de projet, documentation, sécurité, soutenances.

VII. Livrables attendus

- Analyse initiale ;
- Document Architecture Technique ;
- Démonstrateur opérationnel ;

- Dashboards & alertes configurés ;
- Playbooks / procédures ;
- Rapport technique complet ;
- Guide de déploiement & d’utilisation ;
- Vidéo de démonstration.