TP de Validation : Audit de Conformité ANSSI ReCyF v2.5

Analyse d'écarts réglementaires et mesures d'hygiène de sécurité

Nom de l'étudiant : _____
Date : _____

Module : Panorama global et mise en oeuvre des mesures
Score / Note de l'évaluateur : _____ / 20

1. Présentation du Cas d'Étude : HydroMéca Industrie

La société HydroMéca Industrie conçoit et produit des vannes et pompes hydrauliques destinées aux réseaux publics de distribution d'eau potable et de collecte d'eaux usées.
Caractéristiques de l'entité : 120 salariés, chiffre d'affaires annuel de 18 M€, implantée en France. Elle gère un réseau bureautique connecté et un réseau industriel SCADA isolé pilotant les automates d'assemblage de l'usine.

Question A : Identifiez le statut réglementaire de HydroMéca Industrie sous le régime NIS2 et justifiez votre réponse en précisant les seuils de taille (salariés et chiffre d'affaires) et le secteur d'activité :

☐ Non concernée ☐ Entité Importante (EI) ☐ Entité Essentielle (EE)

Justification de la classification :

2. Analyse de conformité et remédiation technique

Pour chacun des constats d'audit suivants identifiés dans l'usine d'HydroMéca, spécifiez l'objectif de sécurité obligatoire du ReCyF v2.5 violé, détaillez le risque cyber induit et rédigez la mesure corrective correspondante (MAC).

Constat 1 : Cartographie des services

« Le service informatique dispose d'une liste dynamique des adresses IP connectées au réseau bureautique. En revanche, il n'existe aucune documentation formalisant la liste des serveurs et composants réseau nécessaires au bon fonctionnement de la chaîne d'assemblage SCADA. »

Objectif ReCyF v2.5 concerné (Nom et Numéro) :

Justification par le risque (Pourquoi est-ce critique ?) :

Mesure Acceptable de Conformité (MAC) préconisée :

Constat 2 : Accès à distance des prestataires

« Les prestataires externes de maintenance SCADA se connectent à distance pour paramétrer les automates. L'accès s'effectue via un VPN sécurisé uniquement par un simple mot de passe partagé. De plus, plusieurs comptes appartiennent à des techniciens ayant quitté leur entreprise de maintenance depuis plusieurs mois. »

Objectif ReCyF v2.5 concerné (Nom et Numéro) :

Justification par le risque (Pourquoi est-ce critique ?) :

Mesure Acceptable de Conformité (MAC) préconisée :

Constat 3 : Stratégie de sauvegarde

« Les bases de données de suivi de production sont sauvegardées toutes les nuits sur un serveur NAS situé dans la baie informatique de l'usine. Le serveur de sauvegarde est directement connecté au domaine Active Directory principal bureautique pour simplifier la réplication. »

Objectif ReCyF v2.5 concerné (Nom et Numéro) :

Justification par le risque (Pourquoi est-ce critique ?) :

Mesure Acceptable de Conformité (MAC) préconisée :

Constat 4 : Gestion de crise cyber

« HydroMéca n'a pas de plan de gestion de crise formalisé. En cas d'attaque par ransomware bloquant l'usine, le plan de l'équipe informatique est d'utiliser le canal Teams interne pour s'organiser et d'informer le Directeur Général sur son téléphone fixe. »

Objectif ReCyF v2.5 concerné (Nom et Numéro) :

Justification par le risque (Pourquoi est-ce critique ?) :

Mesure Acceptable de Conformité (MAC) préconisée :

Constat 5 : Administration du réseau SCADA

« Le responsable automatisme utilise son ordinateur portable professionnel habituel pour se connecter au réseau SCADA industriel et modifier le code des machines. Cet ordinateur est aussi utilisé pour lire les e-mails de l'entreprise et naviguer sur le Web. »

Objectif ReCyF v2.5 concerné (Nom et Numéro) :

Justification par le risque (Pourquoi est-ce critique ?) :

Mesure Acceptable de Conformité (MAC) préconisée :