PROGRAMME DE FORMATION

# IA pour la supervision réseau et l'analyse des incidents

*Utilisez l'IA pour regrouper les événements, résumer les alertes et accélérer l'investigation tout en conservant des preuves techniques traçables.*

| DURÉE | NIVEAU | FORMAT | ORGANISATION |
|---|---|---|---|
| 2 jours | Intermédiaire | Présentiel ou à distance | Intra-entreprise |

## Finalité de la formation

Formation de deux jours à l'analyse assistée des journaux, métriques et alertes pour améliorer la supervision et le diagnostic des incidents réseau.

**Public concerné :** Administrateurs réseau, équipes NOC, support de niveau 2/3 et responsables infrastructure

**Prérequis :** Comprendre les principes de supervision, les journaux système et les protocoles réseau courants.

## Objectifs opérationnels

- Préparer des journaux et métriques pour une analyse assistée.
- Regrouper et classer des alertes liées à un même incident.
- Produire une chronologie technique et des hypothèses de cause.
- Construire un assistant utilisant les procédures internes.
- Générer un rapport d'incident étayé par les données disponibles.

## Compétences développées

- Normaliser des événements Syslog, Windows et pare-feu.
- Distinguer corrélation, anomalie et causalité.
- Évaluer la qualité d'une synthèse générée par un modèle.
- Mettre en place une boucle de validation opérateur.

# Programme détaillé

Le rythme alterne apports ciblés, démonstrations, manipulations guidées et mise en situation sur un environnement de laboratoire isolé.

## Jour 1 - Préparer et corréler les données de supervision

### Matin - Sources, formats et qualité des données

- Panorama : Syslog, événements Windows, journaux de pare-feu, SNMP et métriques.
- Horodatage, fuseaux, niveaux de sévérité et identifiants d'équipements.
- Nettoyage, normalisation, enrichissement et réduction du bruit.
- Séparation des données sensibles avant analyse par un modèle.

**Travaux pratiques :** Normaliser un jeu hétérogène de journaux et construire une chronologie commune.

### Après-midi - Classification et corrélation assistées

- Regroupement des alertes et détection des doublons.
- Classification par service, équipement, impact et priorité.
- Construction d'hypothèses et demande de preuves complémentaires.
- Limites des modèles face aux séries temporelles et aux événements incomplets.

**Travaux pratiques :** Corréler plusieurs alertes autour d'une perte de connectivité simulée.

## Jour 2 - Assistant de diagnostic et gestion d'incident

### Matin - Exploiter les procédures internes

- Préparation d'une base de procédures et principes de recherche documentaire.
- Découpage, métadonnées, droits d'accès et citations des sources.
- Conception d'un assistant guidant l'opérateur sans exécuter d'action dangereuse.
- Évaluation des réponses et traitement du cas « information insuffisante ».

**Travaux pratiques :** Construire une recherche documentaire sur un corpus de procédures réseau.

### Après-midi - Investigation et compte rendu

- Reconstitution de la séquence d'un incident.
- Plan de tests, qualification de l'impact et proposition de remédiation.
- Rédaction d'un rapport avec faits, hypothèses, décisions et actions.
- Indicateurs de qualité et intégration dans le processus d'exploitation.

**Travaux pratiques :** Analyser un incident complet et produire un rapport de remédiation sourcé.

## Projet ou atelier de synthèse

**Assistant de diagnostic capable d'analyser des journaux et de retrouver une procédure réseau pertinente.**

## Méthodes et moyens pédagogiques

- Apports techniques courts suivis d'une application immédiate.
- Démonstrations commentées et analyse collective des choix réalisés.
- Travaux pratiques individuels ou en binôme dans un laboratoire isolé.
- Supports numériques, fichiers d'exemple, modèles de procédures et corrigés.
- Adaptation possible aux technologies et contraintes de l'organisation après cadrage.

## Évaluation des acquis

- Questionnaire de positionnement en début de formation.
- Évaluation formative pendant les manipulations et corrections collectives.
- Mise en situation finale évaluée à l'aide de critères annoncés.
- Questionnaire de validation des connaissances et bilan individuel.
- Attestation de participation remise à l'issue de la formation.

## Environnement technique requis

- Poste avec navigateur et outils de manipulation de fichiers texte ou CSV.
- Jeu de journaux et corpus documentaire fournis par le formateur.
- Accès à un modèle d'IA autorisé ou à un environnement de démonstration.

## Accessibilité et adaptation

Le programme, le rythme et les modalités peuvent être adaptés aux besoins des participants et aux contraintes d'accessibilité identifiées lors du cadrage. Contactez Provence Cloud avant la session afin de préparer les aménagements nécessaires.

## Livrables remis aux participants

- Support de formation au format numérique.
- Fichiers, configurations ou scripts utilisés pendant les travaux pratiques.
- Fiches de contrôle et bonnes pratiques applicables en entreprise.
- Corrigé ou solution de référence du projet de synthèse.

## Contact

**Organisme :** Provence Cloud - ESN basée à Salon-de-Provence

**E-mail :** Contact@provencecloud.com

**Téléphone :** 06 64 47 14 64

**Modalités :** Formation intra-entreprise, en présentiel ou à distance, sur devis et après analyse du besoin.