Programme de cours
Observabilité avec la Suite Elastic (ELK) : Logs, Métriques et Alerting

Durée :	3 jours soit 21 heures	Référence :	IF-ELK

Public visé :

- Administrateurs systèmes, Ingénieurs DevOps, SRE, Responsables de l'exploitation.

Pré-requis :

- Notions d'administration Linux, bases du protocole HTTP et curiosité sur le monitoring.

Objectifs pédagogiques :

- Mettre en œuvre l'architecture complète de la stack ELK.
- Collecter des logs et des métriques via Elastic Agent et les Beats.
- Transformer et enrichir les données brutes (Logstash & Ingest Pipelines).
- Construire des tableaux de bord d'exploitation avancés sous Kibana.
- Configurer un système d'alerting pour la supervision proactive.

Compétences acquises à l'issue de la formation :

- Mettre en œuvre l'architecture complète de la stack ELK.
- Collecter des logs et des métriques via Elastic Agent et les Beats.
- Transformer et enrichir les données brutes (Logstash & Ingest Pipelines).
- Construire des tableaux de bord d'exploitation avancés sous Kibana.
- Configurer un système d'alerting pour la supervision proactive.

Modalités pédagogiques :

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises ou intra-entreprises sur mesure.
La formation est animée par un(e) formateur(trice) durant toute la durée de la session et présentant une suite de modules théoriques clôturés par des ateliers pratiques validant l'acquisition des connaissances. Les ateliers peuvent être accompagnés de Quizz.
L'animateur(trice) présente la partie théorique à l'aide de support de présentation, d'animation réalisée sur un environnement de démonstration.
En présentiel comme en téléprésentiel, l'animateur(trice) accompagne les participants durant la réalisation des ateliers.

Moyens et supports pédagogiques :

Cadre présentiel
Salles de formation équipées et accessibles aux personnes à mobilité réduite.
- Un poste de travail par participant
- Un support de cours numérique ou papier (au choix)
- Un bloc-notes + stylo
- Vidéoprojection sur tableau blanc
- Connexion Internet
- Accès extranet pour partage de documents et émargement électronique

Cadre téléprésentiel
Session dispensée via notre solution iClassroom s'appuyant sur Microsoft Teams.
- Un compte Office 365 par participant
- Un poste virtuel par participant
- Un support numérique (PDF ou Web)
- Accès extranet pour partage de documents et émargement électronique

Informations sur l'accessibilité :

Description / Contenu

Module 1 : Introduction à l'Observabilité Moderne

- Les 3 piliers : Logs, Métriques, Traces.
- Présentation de la stack : Elasticsearch, Kibana, Logstash, Beats/Agent.

Module 2 : Collecte de données (La source)

- Déploiement des Beats (Filebeat, Metricbeat, Heartbeat).
- Nouveauté : Utilisation de Fleet et de l'Elastic Agent pour une gestion centralisée.
- Monitoring de services (Nginx, Docker, Bases de données).

Module 3 : Traitement et Transformation (Ingestion)

- Filtres Logstash (Grok, Mutate, Date).
- Utilisation des Ingest Pipelines (plus légers que Logstash).
- Normalisation avec l'Elastic Common Schema (ECS).

Module 4 : Visualisation avec Kibana

- Exploration de données (Discover) et création de vues.
- Utilisation de Lens et TSVB pour les séries temporelles.
- Création de Dashboards de santé système.

Module 5 : Alerting et Maintenance

- Création de règles d'alerte (seuils CPU, erreurs de logs).
- Connecteurs de notification (Email, Slack, Webhooks).
- Surveillance de l'état de santé de la stack ELK elle-même.