Elastic Stack (Elasticsearch, Logstash, Kibana et Beats)

Lien : https://innov-systems.com/formation/elastic-stack-elasticsearch-logstash-kibana-et-beats

DURÉE	RÉFÉRENCE	CATÉGORIE
3 jours (21h)	**BSI76**	**Big Data - NoSQL**

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Appréhender les problématiques de recherche
- Découvrir Elasticsearch et les dernières nouveautés d'Elastic Stack
- Pouvoir mettre en oeuvre ElasticSearch
- Pouvoir mettre en oeuvre Logstash
- Pouvoir mettre en oeuvre Kibana
- Etre capable de sécuriser votre environnement
- Savoir Sauvegarder et restaurer vos données
- Surveiller et superviser votre architecture

POUR QUI ?

- Administrateurs
- Architectes
- Développeurs

Programme détaillé

1 / Introduction et vue d’ensemble

- Problématique de la recherche
- L’écosystème d’Elasticsearch
- Le rôle d’Elasticsearch, Logstash, Kibana et Beats
- L'offre d'Elastic Stack et cas d'usage dans les entreprises
- Principes et fonctionnement
- Exemples d’architectures
- Cas d’utilisations

2 / ElasticSearch : Indexation, Recherche et analyse de données

- Introduction à Elasticsearch
- Architecture et technologies : Comprendre Lucene, son coeur
- Concepts : Index, Document, Cluster, Noeud, Réplique
- Principes de l'API Rest
- L'indexation des données
- L'API d'indexation
- Configuration d'index
- Types de documents
- Rôle du mapping
- Index inversé
- Les différents types de champs, les champs prédéfinis
- Méta-données d'un index
- Analyse et extraction de texte
- Recherche
- L'API de recherche
- Types de requêtes

- Types de filtres
- Les suggestions
- Agrégations
- Recherche géolocalisée

3 / Logstash : Transformez et formatez vos données pour les utiliser depuis Elasticsearch

- Concepts : Input, Output, Filter(filtre), Codecs...
- Inputs : File, Redis, RabbitMQ...
- Les Filters : Grok, Date, Mutate...
- Les Outputs : File, Elasticsearch, Redis...
- Threading et haute-disponibilité

4 / Kibana : Visualisez les données d'Elasticsearch et Créez vos rapports

- Architecture Kibana, notions de plugins
- Types de recherches
- Visualisations prédéfinies
- Visualisations : Enregistrement, Définition et Styling
- L'éditeur de visualisation
- Le rôle du contrôleur

5 / Beats : Collectez, Parsez et envoyez simplement vos données

- Data Shippers et au monitoring temps réel
- Monitorez votre réseau grâce à PacketBeat
- Monitorez vos fichiers grâce à FileBeat
- Monitorez vos Windows event logs grâce à WinlogBeat
- Récupérer les métriques importantes de vos serveurs grâce à Metricbeat

6 / Scalabilité et clustering en Cluster

- Principe de fonctionnement d'une architecture HA de ELK
- La scalabilité des différents produits :
- Cluster Elasticsearch
- Instances logstash
- Kibana
- Monitoring et exploitation des architectures de production

7 / Administration, Surveillance et Déploiement

- Déploiement en production
- L'outil de monitoring Marvel
- Mesure de performance de l'indexation
- Changements dynamiques de configuration
- Politique de sauvegarde et restauration

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

22 au 24 Juil. 2026	Présentiel - Casablanca
16 au 18 Sep. 2026	Distanciel
11 au 13 Nov. 2026	Distanciel

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com