Formation Machine Learning avec Elastic Stack

Objectifs de la formation Machine Learning Elastic Stack:

La pile Elastic Stack permet d'ingérer tout type de données dans un cluster Elastic search et de les analyser via les outils de visualisation proposés par Kibana. Depuis peu, Elastic propose également des fonctionnalités de Machine Learning permettant la détection d'anomalie et la prévision. Principalement utilisée pour la surveillance d'infrastructure et la sécurité, cette solution peut être appliquée à d'autres domaines.
Cette formation de 2 jours passe en revue les fonctionnalités de Machine Learning d'Elastic Stack et, au travers d'ateliers, elle démontre l'efficacité du machine learning appliqué à la surveillance d'infrastructures SI.

Au cours de cette formation Machine Learning Elastic Stack, vous apprendrez à :

- Installer Elastic Stack pour utiliser le machine learning
- Comprendre comment détecter des anomalies avec les fonctionnalités de Machine Learning d'Elastic Stack
- Appliquer la détection d'anomalie pour la surveillance et la sécurité des systèmes d'information
- Visualiser les résultats dans des tableaux de bord, des vues personnalisées, utiliser les alertes.

À qui s'adresse cette formation ?

Public :

Cette formation Machine Learning Elastic Stack s'adresse à toute personne souhaitant appliquer le machine learning à des problématiques de gestion d'infrastructure et de sécurité.

Pré-requis :

Une première expérience avec Elastic Stack est nécesaire pour cette formation sur la fonctionnalité Machine Learning.

Contenu du cours Machine Learning Elastic Stack

Introduction à Elastic Machine Learning

Big Data et Machine Learning
Machine Learning appliqué à l'IT
Historique de Elastic Machine Learning (Elastic ML)
Concepts : Jobs, Noeuds ML, Bucket, Alimentation en données
Index ELS utilisé, Détails d'un job, les différents types de jobs
Installation

Travaux Pratiques :

Installation d'Elastic Stack et mise en place des fonctionnalités Machine Learning

Détection de changement

Définition du taux d'occurrence normal, Les différentes fonctions de comptage
Définition de la rareté
Catégorisation des évènements

Travaux Pratiques :

Anomalie de décompte, détection de message rare dans des fichiers de logs

Analyse de cause

Importance et limitation des KPI

Segmentation et enrichissement des données

Scinder les analyses, détecter les influenceurs

Corrélation visuelle, Utilisation de l'explorateur d'anomalie

Travaux Pratiques :

Identification d'un process fautif dans des données fournies par packetbeat

Analyse de la sécurité

Indicateur de compromission

Volume et disparité des données, géométrie des attaques

Enrichissement avec logstash

Investigation et analyse

Travaux Pratiques :

Détection d'une exfiltration DNS

Gestion des alertes

Alertes automatiques, configuration

Création d'alerte manuelle

Travaux Pratiques :

Configuration des seuils d'une alerte

Kibana Dashboard et Canvas

Options de visualisation dans Kibana, Timelion

Données Machine Learning en TimeSeries, Timelion

Correlation HeatMap

Utilisation de Canvas et Slides

Travaux Pratiques :

Utilisation de Timelion, HeatMap, Canvas

Prévisions

Prévision temporelle ou valeur, incertitude

Forecast API

Série temporelle unique

Série temporelle multiple

Travaux Pratiques :

Mise en place d'alertes sur données prévisionnelles