DAWAN

Plan de la formation

www.dawan.fr

Formation Surveiller et analyser ses journaux systèmes avec l'IA (Wazuh / SIEM / LLM)

Durée :	2 jours (14 heures)
Tarif inter-entreprises :	1 875,00 CHF HT (Présentiel) 1 500,00 CHF HT (Distanciel)
Public :	Administrateurs systèmes et réseaux - Analystes sécurité, équipes SOC / Blue Team - Responsables infrastructure souhaitant améliorer le traitement des alertes
Pré-requis :	Connaissances de base en administration systèmes (Linux ou Windows) - Notions sur les journaux systèmes, la supervision et la sécurité (logs, alertes, incidents) - Premières notions sur l'IA générative et les LLM appréciées mais non indispensables
Objectifs :	Comprendre comment l'IA peut aider à analyser des volumes importants de journaux systèmes et de sécurité - Savoir connecter un SIEM / Wazuh à un moteur IA pour qualifier et prioriser les alertes - Être capable de générer des synthèses, scénarios de remédiation et rapports à partir des logs
Modalités pédagogiques, techniques et d'encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l'Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat. • Un formateur expert.
Modalité d'évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.

Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	INT102823-F
Note de satisfaction des participants :	Pas de données disponibles
Contacts :	commercial@dawan.fr - 09 72 37 73 73
Modalités d'accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Rappels sur les journaux systèmes, la supervision et le rôle du SIEM

Typologie des journaux : système, application, réseau, sécurité
Centralisation des logs : syslog, agents, collecteurs, corrélation d'événements
Rôle d'un SIEM ou de Wazuh dans la détection d'incidents
Limites des approches classiques : bruit d'alerte, volumétrie, temps d'analyse
Atelier pratique : cartographier ses principales sources de logs et les scénarios d'exploitation associés

Principes et apports des LLM pour l'analyse de logs

Rappel sur les modèles de langage (LLM) et leurs capacités d'analyse textuelle
Cas d'usage typiques : classification, résumé, extraction d'éléments clés, génération d'hypothèses
Forces et limites de l'IA sur les journaux systèmes et de sécurité
Précautions : hallucinations, données sensibles, auditabilité des décisions
Atelier pratique : faire analyser quelques extraits de journaux "à la main" puis via un LLM et comparer les résultats

Connexion d'un SIEM / Wazuh à un moteur IA

Panorama des options : API cloud, modèles open source, Ollama, connecteurs existants
Architecture type : pipeline de logs vers un service d'analyse IA
Formats d'échange : JSON, champs clés, filtrage et anonymisation en amont
Stratégies d'échantillonnage : événements critiques, agrégation par type ou fenêtre de

temps
Atelier pratique : concevoir un flux d'export de journaux Wazuh vers un service IA (schéma et pseudo-code)

Concevoir des prompts et modèles de réponses adaptés à la sécurité

Écrire des prompts pour qualifier une alerte (gravité, impact, contexte probable)
Demander au modèle des scénarios de remédiation et des vérifications complémentaires
Standardiser les formats de réponse pour faciliter l'intégration (JSON, sections prévisibles)
Exemples de prompts pour la priorisation, le tri des faux positifs et la génération de rapports
Atelier pratique : créer une bibliothèque de prompts pour différents types d'événements de sécurité

Générer des synthèses, rapports et tableaux de bord assistés par l'IA

Transformer un flot brut de journaux en synthèse pour un administrateur ou un RSSI
Mettre en forme des rapports périodiques (journée, semaine, incident majeur)
Exploiter les sorties IA dans des tableaux de bord existants (SIEM, Grafana, outils internes)
Capitaliser sur les analyses pour améliorer les règles de détection
Atelier pratique : générer une synthèse d'incident et un mini compte rendu pour un comité sécurité

Aspects sécurité, confidentialité et gouvernance

Que peut-on envoyer ou non à un moteur IA selon la sensibilité des logs
Gestion de la journalisation, de la traçabilité et des responsabilités
Bonnes pratiques : anonymisation, environnements de test, charte d'usage de l'IA en sécurité
Préparer l'industrialisation : documentation, procédures, rôles et limites d'automatisation
Atelier pratique : définir un cadre d'usage de l'IA sur les journaux systèmes dans son organisation