DAWAN

Plan de la formation

www.dawan.fr

Formation Sécurité Avancée Open Source : SSO (Authentik), Secrets et Coffres

Durée :	5 jours (35 heures)
Tarifs inter-entreprise :	3 875,00 € HT (standard) 3 100,00 € HT (remisé)
Public :	Administrateurs systèmes, DevOps, SRE, architectes sécurité ayant déjà des bases Linux, réseaux, Docker ou Kubernetes
Pré-requis :	Bonnes notions de TLS, reverse proxy, DNS, LDAP/AD, conteneurs, notions d'OIDC/SAML
Objectifs :	Déployer un SSO d'entreprise avec Authentik et fédération d'identités - Sécuriser et distribuer les secrets applicatifs avec HashiCorp Vault en haute disponibilité- Mettre en place des coffres forts numériques pour comptes privilégiés et secrets d'équipe - Industrialiser l'intégration SSO/Secrets dans CI/CD, VMs, conteneurs et Kubernetes, avec audit et rotation automatique
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.
Modalités 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 :	CYB102004-F
Note de satisfaction des participants:	4,70 / 5
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

Jour 1 — Déployer et fédérer un SSO avec Authentik

Positionner les standards d'authentification moderne : OIDC, OAuth2, SAML, tokens, scopes, claims
Installer Authentik en Docker Compose et découvrir Providers, Applications, Policies, Users, Groups
Configurer l'annuaire : intégration LDAP/AD, mappers d'attributs, synchronisation
Configurer les flux : OIDC (Authorization Code + PKCE), SAML SSO, proxies intégrés
Personnaliser l'expérience : pages de login, branding, gestion du consentement
Atelier fil rouge : protéger le Back-office de l'app avec Authentik et OIDC, mapping des rôles fonctionnels

Jour 2 — Renforcer Authentik en production

Sécuriser l'instance : TLS, reverse proxy NGINX/Traefik, gestion des secrets, 2FA/MFA
Gouverner les accès : Policies (IP, heures, groupes), RBAC avancé, delegation
Intégrer les IdP externes : Azure AD, Google Workspace, annuaires externes
Automatiser l'administration : API d'Authentik, scripts, backups, mises à jour
Monter en disponibilité : clustering, persistance Postgres, monitoring avec Prometheus
Auditer et tracer : logs, événements, intégration Wazuh/OpenSearch, alertes sur anomalies
Atelier fil rouge : basculer le Front et l'API sur OIDC avec Authentik, activer MFA adaptatif

Jour 3 — Gérer les secrets avec HashiCorp Vault

Comprendre les concepts : init/unseal, storage backend, auth methods, secret engines, policies

Installer Vault en mode dev puis HA intégré (Raft), activer l'audit device et les logs
Sélectionner les méthodes d'authent : AppRole, Kubernetes, LDAP, JWT, Token
Exploiter les moteurs de secrets : KV v2 pour config, Transit pour chiffrement/déchiffrement, Database pour secrets dynamiques, PKI pour certificats courts
Écrire des policies least-privilege et mettre en place l'auto-rotation des secrets dynamiques
Atelier fil rouge : extraire les secrets de l'app vers Vault KV, chiffrer des données avec Transit, générer des comptes DB éphémères

Jour 4 — Intégrer SSO et secrets dans l'infra et le CI/CD

Sécuriser les reverse proxies : NGINX auth_request + oauth2-proxy, Traefik ForwardAuth, intégration Authentik Proxy Provider
Intégrer dans les pipelines : accès temporaires à Vault depuis GitLab/Gitea Actions, masquage de variables, rotation post-déploiement
Gérer les secrets sur Kubernetes : auth k8s de Vault, CSI/Agent Injector, External Secrets Operator, bonnes pratiques de namespaces et RBAC
Protéger les accès SSH et machines : certificats SSH signés par Vault, récupération ponctuelle d'identifiants privilégiés
Comparer Ansible Vault, Mozilla SOPS/age et Vault pour IaC et inventaires
Atelier fil rouge : déployer l'app sur k3s avec Authentik (SSO via oauth2-proxy) et secrets rendus par External Secrets Operator

Jour 5 — Coffres forts numériques, PAM open source et conformité

Choisir un coffre d'équipe : Bitwarden (self-host), Passbolt et bonnes pratiques de partage et délégation
Mettre en place une gestion des comptes privilégiés légère : stratégies d'accès "break-glass", justification, journalisation et rotation via Vault
Sécuriser les fichiers et sauvegardes : Borg/Restic, SOPS/age, chiffrement côté client, clés de récupération
Tracer et répondre aux incidents : tableaux de bord d'authent, détection de comportements anormaux, playbooks de révocation de tokens et rotation massive de secrets
Aligner conformité et durabilité : politique d'expiration des secrets, revues périodiques d'accès, sauvegardes et tests de restauration, matrice RACI et preuves d'audit
Atelier fil rouge : déployer un coffre d'équipe, migrer les secrets restants, documenter le runbook d'incident et les preuves d'audit

Livrables et évaluations

Livrables : dépôts Git des ateliers, exports de configuration Authentik, scripts d’initialisation Vault, manifests Kubernetes et playbooks CI fournis
Évaluation continue : quiz courts en fin de module, validation par la mise en œuvre complète du fil rouge, revue de sécurité finale avec checklist d’audit
Attendus en sortie : plateforme SSO Authentik opérationnelle, Vault HA avec politiques et moteurs clés, reverse proxy OIDC en place, intégration CI/CD ou Kubernetes, coffre d’équipe en production pilote