Atelier d'Étude Solutions

Objectif du projet

Réaliser une étude comparative des principales solutions IAM du marché afin de recommander celles qui répondent le mieux aux besoins d'une entreprise fictive, selon des critères techniques, économiques et réglementaires.

Contexte

Vous êtes consultant en cybersécurité dans une entreprise fictive de 300 employés répartis sur trois sites (France, Espagne, Canada). L'entreprise gère des données sensibles (RH, clients, contrats, projets) et utilise plusieurs outils SaaS et on-premise : ERP, CRM, messagerie, VPN, dépôt de code, intranet, plateforme e-learning.

L'entreprise souhaite mettre en place une solution IAM centralisée pour :

- Gérer les identités et les accès des employés, prestataires et partenaires
- Automatiser le provisioning/déprovisioning
- Renforcer la sécurité (MFA, SSO, audit)
- Respecter les exigences RGPD

Livrables attendus

1. Étude comparative de 3 à 5 solutions IAM du marché (exemples : Okta, Microsoft Entra ID, Ping Identity, ForgeRock, OneLogin, IBM Security Verify, etc.)
2. Tableau comparatif selon des critères définis
3. Recommandation argumentée de la solution la plus adaptée à DataSecure

Etapes du projet :

- 1. Sélection des solutions IAM à comparer
- 2. Recherche documentaire (site officiel, études de cas, documentation technique)
- 3. Remplissage du tableau comparatif
- 4. Analyse des forces/faiblesses de chaque solution
- 5. Recommandation finale avec justification selon les besoins de l'entreprise

Sommaire :

1. IAM Sélectionné

1.2 CyberArk

CyberArk est une solution largement reconnue dans la gestion des accès privilégiés, ce qui la rend particulièrement adaptée aux environnements informatiques sensibles. Elle permet de renforcer la sécurité des identités en empêchant les accès non autorisés, qu'ils viennent de l'intérieur ou de l'extérieur. Grâce à ses fonctionnalités, les équipes informatiques peuvent définir des règles strictes sur la gestion des mots de passe, automatiser leur rotation et superviser les comptes à privilèges sur l'ensemble du parc informatique.

1.2 JumpCloud

JumpCloud mise sur une stratégie cloud native pour la gestion des identités et des accès (IAM), proposant des services d'annuaire, d'authentification unique (SSO) et de gestion d'appareils sur une plateforme unifiée. Destinée à un accès sûr partout, elle fonctionne avec les systèmes d'exploitation Windows, macOS et Linux. JumpCloud, en tant qu'annuaire ouvert, connecte les utilisateurs à leurs appareils, serveurs, applications et réseaux. En utilisant des outils tels que l'authentification multi-facteurs (MFA), l'accès sans mot de passe et les politiques contextuelles, elle assiste les organisations à renforcer leur sécurité tout en préservant la simplicité de l'expérience utilisateur.

1.3 Nuage IBM

IBM Cloud Identity offre une solution IAM conçue pour l'évolutivité, la conformité et l'intégration transparente aux environnements informatiques hybrides.

Elle prend en charge l'authentification unique (SSO), l'authentification multifacteur (MFA), l'accès adaptatif et la gouvernance des identités au sein de l'écosystème cloud de confiance d'IBM. S'appuyant sur des analyses pilotées par l'IA, elle aide les entreprises à gérer les risques et à garantir un accès sécurisé, tout en simplifiant l'intégration des utilisateurs et la gestion du cycle de vie.

1.4 Okta

Okta se positionne comme une plateforme d'identité cloud-native, spécialisée dans la sécurisation des accès pour les employés et les clients. Son activité principale consiste à fournir une authentification unique (SSO) transparente vers un très large éventail d'applications, qu'elles soient dans le cloud ou sur site.
Au-delà du SSO, ses compétences clés résident dans la fourniture d'une sécurité adaptative robuste grâce à l'authentification multifacteur (MFA) contextuelle, qui analyse le risque en temps réel pour ajuster les exigences de connexion.

2. Documentation

2.1 CyberArk

CyberArk permet un accès sécurisé pour les identités humaines et machines, détecte et intègre automatiquement les comptes privilégiés et garantit que les comptes à haut risque sont régis par des contrôles stricts.
Voici une liste des principals caractéristique :

- Gestion des accès privilégiés.
- Gestion de l'identité numérique.
- Services d'annuaire.
- Authentification unique (SSO) et MFA adaptative.
- Analyse du comportement des utilisateurs.
- Application de la politique de mot de passe.

Étude de cas – CyberArk

Un groupe industriel international confronté à des risques internes a choisi CyberArk pour sécuriser ses comptes à privilèges. La mise en œuvre du coffre-fort numérique, de la rotation automatique des mots de passe et du monitoring des sessions à haut risque a permis de renforcer le contrôle des accès sensibles. Résultat : une meilleure traçabilité des actions critiques, une réduction significative des accès non autorisés et une conformité renforcée face aux exigences réglementaires (ISO 27001, RGPD).

2.2 JumpCloud

JumpCloud simplifie la création, la mise à jour et la révocation des accès utilisateurs depuis un seul et même endroit, tout en renforçant la protection grâce à l'authentification multifacteur (MFA), aux codes TOTP et aux politiques conditionnelles. Il aide les organisations à réduire le temps d'intégration et les erreurs en automatisant la gestion des accès.
Voici également une liste des principals caratéristique :

- Gestion du cycle de vie des identités.
- Connexion unifiée et sécurisée.
- Contrôles d'accès basés sur le contexte.
- Authentification sans mot de passe.
- Authentification multifacteur (MFA)
- Single Sign-On (SSO)

Étude de cas – JumpCloud

Une entreprise technologique de 200 employés, répartis sur plusieurs sites internationaux, a déployé **JumpCloud** pour centraliser la gestion des identités sans infrastructure locale. Grâce à la plateforme, les équipes IT ont automatisé le **cycle de vie des utilisateurs** (création, modification, suppression) et appliqué des politiques de sécurité unifiées sur les postes Windows, macOS et Linux. L'activation du **SSO et du MFA** sur les applications critiques a renforcé la sécurité, tout en simplifiant l'expérience utilisateur.

2.3 Okta

Le site officiel de Okta est disponible sur ce lien:
https://www.okta.com/

Le lien portant sur le Single Sign On Okta est trouvable ci-dessous:
https://www.okta.com/products/single-sign-on-workforce-identity/

La capacité à fournir un accès sécurisé et centralisé à de multiples applications via un seul ensemble d'identifiants est la fonctionnalité la plus connue d'Okta.
Au-delà du SSO, ses compétences clés résident dans la fourniture d'une sécurité adaptative robuste grâce à l'authentification multifacteur (MFA) contextuelle, qui analyse le risque en temps réel pour ajuster les exigences de connexion. Okta excelle également dans l'automatisation du cycle de vie des identités (provisioning et déprovisionnement), en s'intégrant directement avec les systèmes RH pour gérer les arrivées, les changements de rôle et les départs de manière centralisée et automatisée. Sa plateforme, conçue comme un annuaire universel, permet d'unifier les identités provenant de multiples sources (comme Active Directory, LDAP ou des applications RH) en un seul profil utilisateur, simplifiant ainsi considérablement l'administration et le contrôle des accès.

Documentation technique:

Okta Help Center (help.okta.com) : C'est le hub principal pour les administrateurs système et les équipes IT. Il contient toute la documentation produit. On y trouve des guides d'installation et de configuration détaillés pour chaque fonctionnalité, des notes de version, des articles de la base de connaissances pour le dépannage de problèmes courants et des guides sur les meilleures pratiques de sécurité.

Okta Developer Center (developer.okta.com) : Ce portail est entièrement dédié aux développeurs. C'est une ressource de premier ordre qui contient tout le nécessaire pour interagir avec les APIs d'Okta ou intégrer l'identité dans des applications personnalisées. Il inclut :

- Des guides de démarrage rapide pour des cas d'usage courants.
- Une documentation de référence complète pour les APIs REST, avec des exemples de requêtes et de réponses claires.
- Des SDKs pour les langages de programmation les plus populaires, ce qui accélère considérablement le développement.
- Des tutoriels approfondis sur l'implémentation des protocoles d'identité standards comme OAuth 2.0 et OpenID Connect.

Etude de cas:

Innovatech Solutions est une société de conseil en technologie en pleine croissance, comptant environ 500 employés.. Pour servir ses clients, l'entreprise s'appuie sur un écosystème d'applications cloud variées (Microsoft 365, Salesforce, Slack, AWS) ainsi que sur des outils sur site, notamment une base de données clients et un système ERP hérité.

Innovatech a choisi de déployer plusieurs produits de la suite Okta pour répondre à ses défis :

- Single Sign-On (SSO) : Pour offrir aux employés un portail unique et sécurisé leur donnant accès à toutes leurs applications avec un seul ensemble d'identifiants.
- Adaptive Multi-Factor Authentication (MFA) : Pour renforcer la sécurité des connexions en exigeant une deuxième forme de vérification, avec des politiques intelligentes qui n'ajoutent de la friction qu'en cas de connexion à risque (ex: depuis un nouvel appareil ou un pays inconnu).
- Lifecycle Management : Pour automatiser le cycle de vie des identités. En intégrant Okta à son système RH (Workday), la création, la mise à jour et la révocation des accès sont devenues entièrement automatisées, du premier au dernier jour de l'employé.

L'implémentation d'Okta a eu un impact transformationnel et mesurable pour Innovatech Solutions. En adoptant Okta, Innovatech Solutions a non seulement résolu ses défis immédiats en matière de sécurité et d'efficacité, mais a également mis en place une fondation d'identité solide et évolutive pour soutenir sa croissance future en toute sécurité.

2.4 Nuage IBM

Site Officiel :

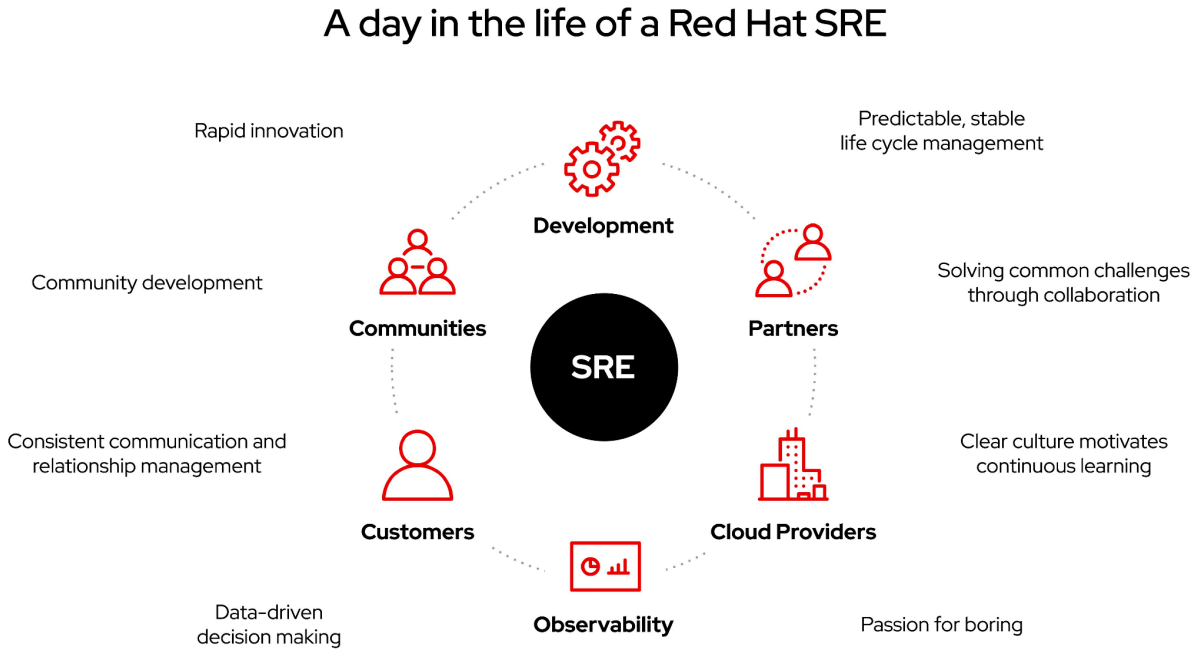
Le site informatique de **Nuage IBM** est trouvable cis-dessous :
https://cloud.ibm.com/docs/account?topic=account-iamoverview&utm=

Il sert de porte d'entrée principale pour comprendre et implémenter la gestion des identités et des accès (IAM) au sein de la plateforme IBM Cloud.

IBM met en avant la conformité aux normes internationales (RGPD, HIPAA, ISO 27001, SOC 2) et l'intégration fluide avec des milliers d'applications grâce à des connecteurs prédéfinis. L'approche d'IBM repose également sur l'analyse des comportements utilisateurs alimentée par l'IA, permettant de détecter les anomalies et d'adapter les politiques d'accès en temps réel.

Etudes de cas :

IBM met en avant plusieurs cas d'utilisation concrets de son offre IAM. Par exemple, une grande banque internationale a déployé **IBM Cloud Identity** pour automatiser la gestion des droits d'accès dans un environnement multi-sites et hybride. Grâce aux modèles IAM d'entreprise proposés par IBM, l'équipe SRE (Site Reliability Engineering) a pu rationaliser la gestion des comptes et réduire significativement les erreurs liées au provisionnement manuel.



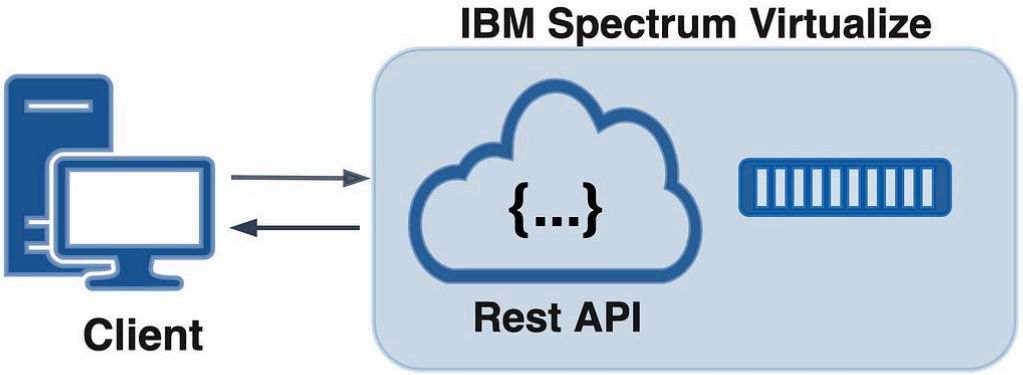
Par ailleurs, IBM utilise sa propre solution en interne à très grande échelle, avec plus de **27 millions d'utilisateurs gérés via IBM Security Verify**. Ces retours d'expérience démontrent la capacité de la solution à s'adapter aussi bien à des environnements complexes qu'à des organisations internationales devant répondre à des exigences strictes de conformité et de sécurité.

Documentation technique :

La documentation technique d'IBM Cloud Identity fournit des informations détaillées sur toutes les fonctionnalités et outils disponibles pour gérer les identités et les accès dans IBM Cloud. Elle décrit en profondeur la manière de créer et gérer les utilisateurs, les groupes d'accès, les identifiants de service et les profils de confiance, et explique comment ces éléments interagissent pour garantir un contrôle d'accès précis et sécurisé.

Elle détaille également les politiques d'accès et les contrôles basés sur les rôles (RBAC), permettant aux administrateurs de définir des règles spécifiques pour chaque utilisateur, groupe ou ressource. Les bonnes pratiques de sécurité sont également abordées, comme la limitation des sessions actives, la gestion des tokens d'accès et le suivi des comptes orphelins, afin de minimiser les risques liés aux accès non autorisés.

La documentation fournit des guides pour l'utilisation des différents outils et interfaces : la console IBM Cloud pour l'administration graphique, la CLI IBM Cloud pour automatiser les tâches et les API REST pour intégrer la gestion des identités dans des applications tierces ou des environnements hybrides.



Ces API permettent, par exemple, de gérer les identités, les clés API, les profils de confiance et les politiques d'accès de manière programmatique, offrant ainsi une grande flexibilité aux équipes IT.

3. Tableau comparatif

Critère	CyberArk	JumpCloud	Nuage IBM	Okta
Sécurité	Fort accent sur la sécurisation des accès privilégiés (PAM, coffre de comptes à haut privilège, rotation, sessions sécurisées)	Bonne sécurité pour les accès "utilisateurs", MFA, authentification conditionnelle intégrée	MFA adaptatif, gestion des rôles, audit complet, détection d'anomalies (ThreatInsight)	MFA adaptatif, gestion des rôles, audit complet, détection d'anomalies (ThreatInsight).
Intégration	Intégration avec AD, LDAP,	Fortes intégrations cloud, OS	Vaste catalogue de plus de 7000	Vaste catalogue de plus de 7000

	systèmes legacy, environnements hybrides, outils de sécurité, API	multiples (Windows, macOS, Linux), annuaires, applications SaaS	intégrations SaaS et on-premise, API robustes	intégrations SaaS et on-premise, API robustes
Gestion des identités	Gère les comptes privilégiés, les comptes de service ; moins orienté “identités standard”	Gère les utilisateurs, le cycle de vie (provisioning / désactivation)	Gestion centralisée via Universal Directory	Provisioning/déprovisionnement automatisé (Lifecycle Management), gestion centralisée via Universal Directory.
Expérience Utilisateur	Interface parfois perçue comme complexe (notamment pour la configuration)	Interface plutôt intuitive, facile à utiliser (parmi les retours utilisateurs)	Interface utilisateur claire, SSO transparent, accessible multi-appareils	SSO transparent, interface utilisateur intuitive, accessibilité multi-appareils via l'application Okta Verify.
Administration	Administration puissante mais nécessitant souvent des compétences spécialisées	Administration assez centralisée, simplicité de gestion	Console d'administration centralisée, délégation de tâches, rapports détaillés	Console d'administration centralisée et facile à utiliser, délégation de tâches, rapports détaillés.
Coût	Coût élevé, notamment pour PAM et les modules avancés, coût de mise en œuvre et support élevé	Modèle par utilisateur, coût compétitif pour les besoins standard	Tarification modulaire par utilisateur/mois, plusieurs licences souvent nécessaires	Modèle de tarification modulaire par utilisateur/mois, nécessitant souvent plusieurs licences pour une solution complète.
Conformité	Bon support pour les audits, traçabilité, contrôle des sessions privilégiées	Support raisonnable pour les exigences réglementaires selon modules	Aide à la conformité RGPD, certifications ISO 27001, SOC 2, FedRAMP	Aide à la conformité RGPD, certifications ISO 27001, SOC 2, FedRAMP.
Scalabilité	Scalabilité	Bonne	Plateforme	Plateforme

	possible mais peut nécessiter une architecture robuste	scalabilité cloud-native, support de croissance	hautement évolutive, adaptée à toutes tailles d'entreprises	hautement évolutive, conçue pour s'adapter à la croissance des entreprises de toutes tailles.
Gestion des tiers	Peut gérer les comptes de tiers avec des accès privilégiés (via PAM)	Possibilités de donner des accès temporaires ou conditionnels aux tiers	Gestion des accès pour partenaires et prestataires via portails B2B dédiés	Gestion des accès pour les partenaires et les prestataires via des portails B2B dédiés.
Support & documentation	Bonne documentation, mais retours d'utilisateurs sur la complexité et les temps de support	Support bien noté, documentation claire, communauté	Documentation complète, communauté active, support technique réactif structuré en niveaux	Documentation complète, communauté active, support technique réactif et structuré en niveaux.

4. Analyse des forces/faiblesse

4.1 CyberArk

Voici un Pros / Cons pour la solution de CyberArk

Pros :

- Accès fluide aux applications.
- Fonctionne bien avec l'infrastructure existante.

Cons :

- La documentation pourrait être plus complète.
- Les fonctionnalités de reporting sont assez basiques.

4.2 JumpCloud

Voici un Pros / Cons pour la solution de JumpCloud

Pros :

- Réduit le temps d'intégration et de départ.
- Combine SSO, LDAP, Radius, MFA et les politiques de périphérique dans une seule plateforme

Cons :

- Les groupes d'utilisateurs imbriqués ne sont pas pris en charge.
- Les fonctionnalités SSO pourraient être plus avancées.
- L'installation et la configuration peuvent être complexes au début.
-

4.3 Okta

Pros :

- Facilité d'intégration et écosystème : Le plus grand catalogue d'intégrations du marché, ce qui simplifie grandement le déploiement dans un environnement
- Expérience utilisateur et administration : Reconnu pour sa simplicité d'utilisation, tant pour les utilisateurs finaux que pour les administrateurs.
- Fiabilité et maturité : En tant que leader du marché, la plateforme est éprouvée, stable et bénéficie d'une haute disponibilité.

Cons :

- Coût modulaire : Le coût peut augmenter rapidement car les fonctionnalités essentielles (Lifecycle Management, Advanced MFA) sont souvent des modules payants séparés.
- Focus sur l'identité applicative : Moins outillé nativement pour la gestion fine des appareils ou la sécurité des serveurs locaux par rapport à d'autres solutions (e.g JumpCloud).
- Dépendance et "vendor lock-in" : Une fois l'entreprise profondément intégrée à l'écosystème Okta (Universal Directory, Workflows), il devient techniquement complexe et coûteux de migrer vers un autre fournisseur.

4.4 Nuage IBM

Concernant les avantages et inconvénient de cette IAM.

Avantages:

- Intégration fluide avec automatisation.
- Analyses solides et surveillance du comportement des utilisateurs.

Inconvénients:

- Idéal pour les entreprises déjà familiarisées avec les outils IBM.
- Peut être trop complexe pour les petites organisations.

5. Recommandation Finale

Nous avons opté comme solution finale Okta !

Et voici pourquoi.

Tout d'abord une des notions très importante, l'aspect d'une bonne sécurité robuste et d'une sécurité qui se voit polyvalente/adaptative. Okta fournit un meilleur MFA contextuelle car il y a une analyse de risque en temps réel et une gestion centralisée des accès via un puissat SSO (Single-Sign-On) ce qui réduit drastiquement la surface d'attaque. Il s'intègre simplement à certaines politiques de sécurité avancées comme le RBAC, Zero Trust, etc.

Okta possède une intégration vraiment très intéressante, cette solution se voit en sa possession environ 7000 applications intégrées (SaaS et on-premise). Il possède également beaucoup d'outils natif comme l'ERP, CRM, VPN, messagerie, un dépôt de code, e-learning. Okta se voit compatible avec beaucoup d'LDAP et est compatible avec l'Active Directory.

Pour la partie du cycle de vie des identités, Okta est capable de trouver les orphelins beaucoup plus facilement dans des arborescences complexes et détermine son facteur de risque ainsi que détecter les erreurs humaines. L'interface se voit très intuitive pour des Administrateurs, possède un système d'alerte et est fourni avec un bon accès depuis une tablette ou un smartphone par exemple.

Les consoles sont simples à utiliser avec une possibilité d'évolutions (ajout de plugin possible).

Okta possède un ajout majeur, Okta possède les certifications suivantes : RGPD, ISO 27001, SOC 2, HIPAA, FedRAMP.
Un suivi d'activité complet, avec une bonne traçabilité et un reporting d'accès.

Pourquoi pas les autres ?

CyberArk	Très puissant sur le PAM (comptes privilégiés) mais trop orienté admin/serveurs. Interface complexe, surdimensionnée pour des utilisateurs standards. Idéal en complément d'un IAM général comme Okta, mais pas seul.
JumpCloud	Bon pour les environnements cloud hybrides et la gestion d'appareils, mais manque de maturité sur certains aspects comme le SSO avancé et les groupes imbriqués. Peut convenir à des PME très techniques, moins à une structure de 300 personnes multisite.
IBM Cloud Identity	Très riche et fiable, mais complexe à déployer et administrer, surtout si vous n'avez pas déjà une stack IBM. Plutôt destiné à des grandes entreprises très IT-centric avec des ressources internes conséquentes.

Dans ce contexte Okta est LA solution vers laquelle nous souhaitons nous tourner.