21 octobre 2025 - PARIS

IDENTITY DAYS

Dernières tendances en Gestion des Identités et des Accès

Eric PÉRION
Partner Cyber, Canada & Amérique du Nord
onepoint.
Au-delà de l'évidence

IDENTITY DAYS

AGENDA DE LA CONFÉRENCE

Eric PÉRION

Partner Cyber
Canada & Amérique du Nord

onepoint.
Au-delà de l'évidence

Auparavant:

- **Accenture** en **Europe**, spécialiste IAM et stratégie cyber auprès de l'industrie A&D
- **Deloitte Canada**, responsable Conseil en Risques pour l'industrie de la Finance

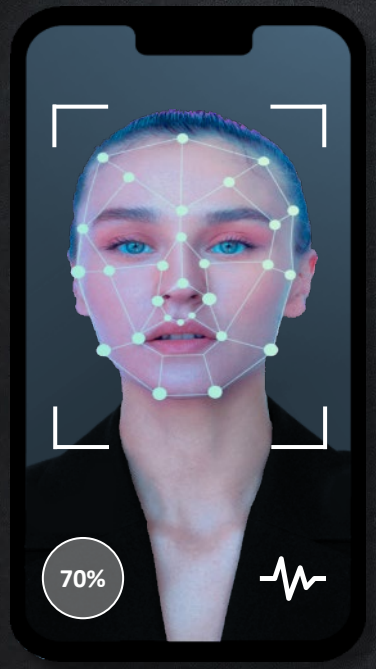
- **M**enaces émergeantes
- **P**réambule sur les tendances en matière de solutions
- **A**uthentification sans mot de passe
- **G**estion des accès basés sur le contexte (PBAC)
- **V**érification de l'identité & Identités décentralisées
- **G**estion de la menace sur les identités (ITDR)
- **A**uthentification basée sur le risque
- **G**estion des permissions dans les environnements Cloud (CIEM) et DevOps
- **C**onclusion – Zero Trust & l'Identity Fabric

IDENTITY DAYS

Menaces émergeantes

Menaces émergeantes en gestion des identités et des accès

Deepfakes



- **Accessible**, de **haute qualité** (ex: Gooey.AI, deepfakesweb.com)
- Protection difficile contre les **deepfakes vocaux** pour les centres d'appels

Considérer:

➔ **Détecter le caractère vivant**

➔ **Technologies de détection des deepfakes** (ex. Sensity)

Manipulation des prompts et des agents IA

- **Manipulations involontaire ou délibérée**
- **Agents mal autorisés** agissant par erreur sous le commandement de l'IA (ex: remise inexistante promise chez Air Canada)

Considérer:

➔ **Appliquer le principe Zero Trust et de moindre privilège pour les identités privilégiées utilisées par l'IA:**

- Authentifier les clients
- Authentifier l'IA auprès des systèmes privilégiés et auprès des tiers au nom des clients

IDENTITY DAYS

Préambule sur les tendances en matière de solutions

→ Qui a accès à quoi ?

→ Peut-on assurer l'authentification des utilisateurs de manière fiable ?

→ Peut-on s'assurer que les personnes ne puissent accéder que ce à quoi elles ont besoin d'accéder?

Cadre de capacités

de gestion des identités et accès

Utilisateurs
(employés, consultants, fournisseurs, partenaires, clients)

Postes de travail et mobiles, serveurs, composants réseaux

Applications, SaaS, Legacy

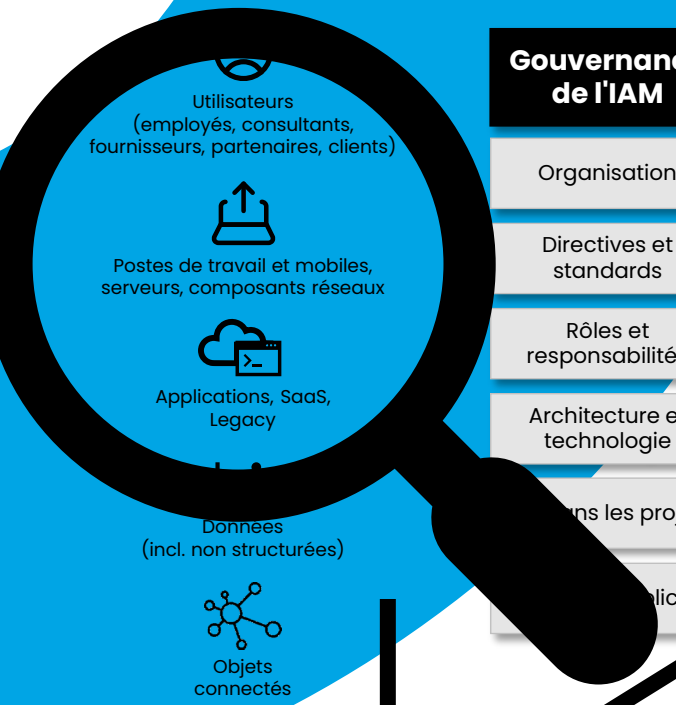
Données
(incl. non structurées)

Objets connectés

Gouvernance de l'IAM	Gestion des identités	Contrôle d'accès	Gestion des habilitations	Comptes à hauts privilèges	Risque et conformité	Tendances
Organisation	Cycle de vie des identités	Authentification	Ingénierie des profils de droit (RBAC,ABAC)	Gestion du cycle de vie des comptes à privilèges	Reporting, risques et conformité	Analytique des identités et intelligence
Directives et standards	Typologie des identités	Single Sign-On	Comptes non nominatifs	Voûte de mots de passe	Séparation des tâches	Gestion des accès infra Cloud (CIEM) & IAM pour DevOps
Rôles et responsabilités	Annuaire d'identités	Synchronisation des annuaires	Gestion des droits fins dans les systèmes	Administration des mots de passe	Certification des accès	Gestion des accès basés sur le contexte (PBAC)
Architecture et technologie	Gestion de l'unicité	Fédération des identités	Gestion centralisée et self-service	Intégration SSO	Contrôles préventifs	Gouvernances des accès aux APIs
IAM dans les projets	Demande d'accès	Libre-service de mots de passe	Référentiel des habilitations	Supervision de session	Risk scoring	IAM des "IoT"
Périmètre applicatif	Provisioning d'accès	Authentification forte (MFA)	Accès aux données non structurées		Gestion des exceptions	Gestion de la menace sur les identités (ITDR)
		Authentification basée sur le risque	Accès physiques			Identités décentralisées & Verify ID
		Authentification sans mot de passe				
		IAM Clientèle (CIAM)				

Grandes tendances

de la gestion des identités et accès

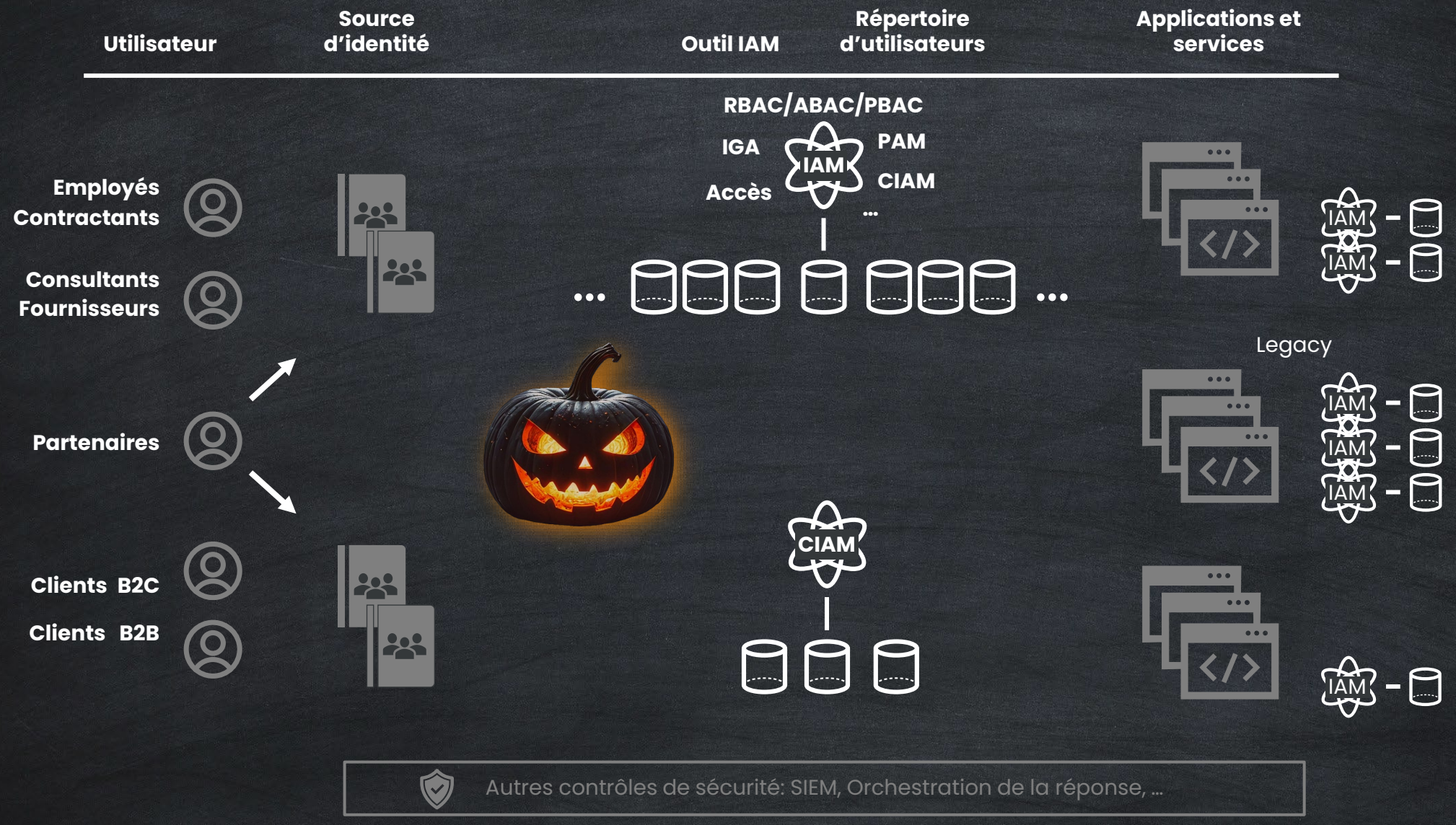


Gouvernance de l'IAM	Gestion des identités	Contrôle d'accès	Gestion des habilitations	Comptes à hauts privilèges	Risque et conformité	Tendances
Organisation	Cycle de vie des identités	Authentification	Ingénierie des profils de droit (RBAC,ABAC)	Gestion du cycle de vie des comptes à privilèges	Reporting, risques et conformité	Analytique des identités et intelligence
Directives et standards	Typologie des identités	ngle Sign-O	Comptes non nominatifs	Voûte de mots de passe	Séparation des tâches	Gestion des accès infra Cloud (CIEM) & IAM pour DevOps
Rôles et responsabilités	Annuaire d'identités	Synchronisation des annuaires	Gestion des droits fins dans les systèmes	Administration des mots de passe	Certification des accès	Gestion des accès basés sur le contexte (PBAC)
Architecture et technologie	Gestion de l'unicité	Fédération des identités	Gestion centralisée et self-service	Intégration SSO	Contrôle préventifs	Gouvernances des accès aux APIs
ns les projets	Demande d'accès	Libre-service de mots de passe	éférentiel des abilitations	Supervision de session	Risk scoring	IAM des "IoT"
licatif	Provisioning d'accès	Authentification forte (MFA)	Accès aux données non structurées		Gestion des exceptions	Gestion de la menace sur les identités (ITDR)
		Authentification basée sur le risque	Accès physiques			Identités décentralisées & Verify ID
		Authentification sans mot de passe				
		IAM Clientèle (CIAM)				

Zero Trust &
l'Identity Fabric

Transformation IAM désormais via des **solutions SaaS**,
y compris pour les grandes entreprises

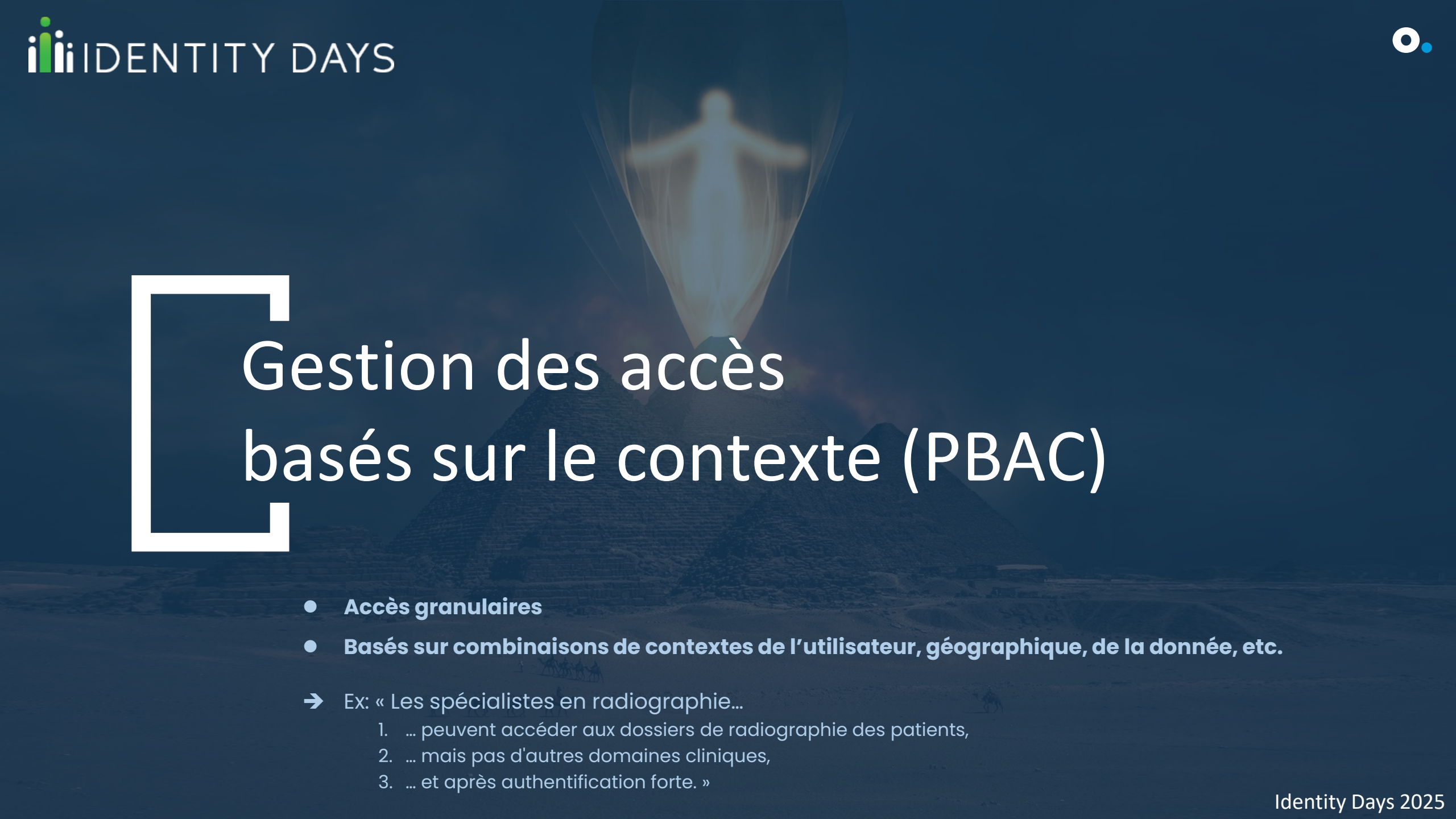
Environnement IT & IAM … complexe



Authentification sans mot de passe

- **Plus sûr**
- **Plus simple**

➔ Ex: Authentification FIDO, biométrie, NIP local, ...



Gestion des accès basés sur le contexte (PBAC)

- **Accès granulaires**
- **Basés sur combinaisons de contextes de l'utilisateur, géographique, de la donnée, etc.**

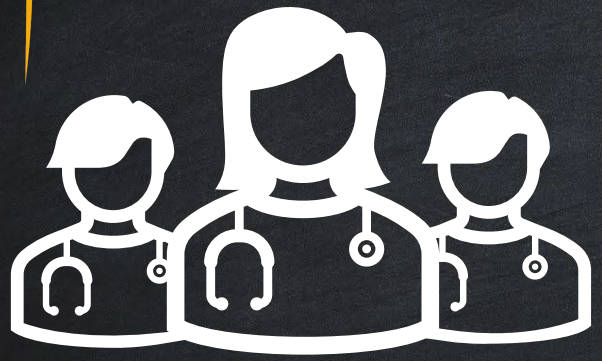
➔ Ex: « Les spécialistes en radiographie…

1. … peuvent accéder aux dossiers de radiographie des patients,
2. … mais pas d'autres domaines cliniques,
3. … et après authentification forte. »

Contrôle d'accès basé sur des politiques (PBAC)

Octroi des politiques

Politiques de contrôle d'accès (PBAC)



Docteurs

- Eve-Marie
- Sara
- Eric

➔ **Permettre ces actions**

✓ Rayon X : voir, éditer, imprimer, effacer

➔ **Pour ces personnes**

- Relation = "Médecin traitant"

  OU ID Personne = "101, 211, ou 591"

➔ **Dans ce contexte**

- Mode d'urgence = faux
- Réseau = interne
- Niveau d'assurance MFA >=2

Auditeurs

➔ **Peuvent savoir**

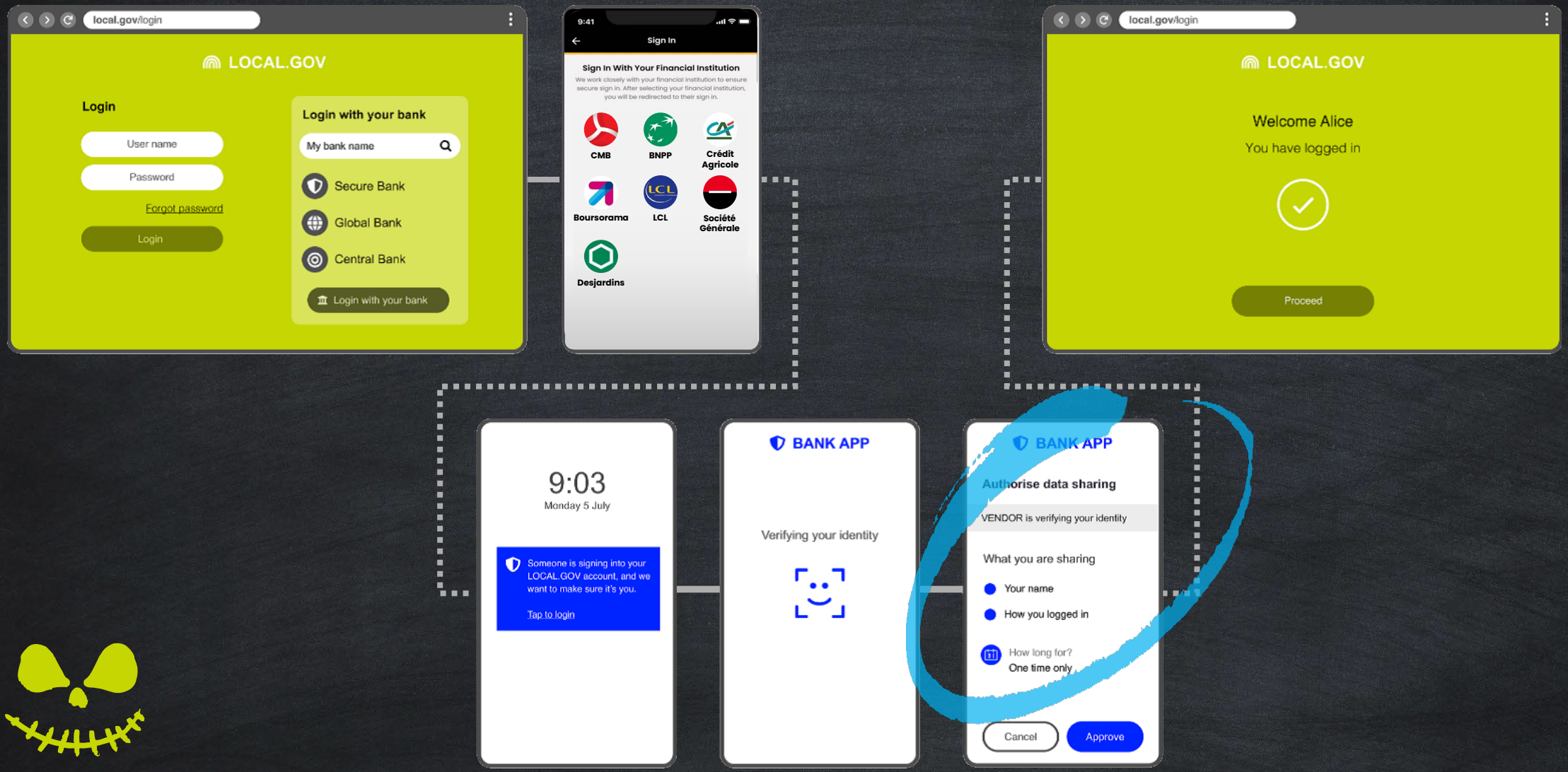
- QUI peut "voir", et
- QUI a approuvé l'octroi

IDENTITY DAYS

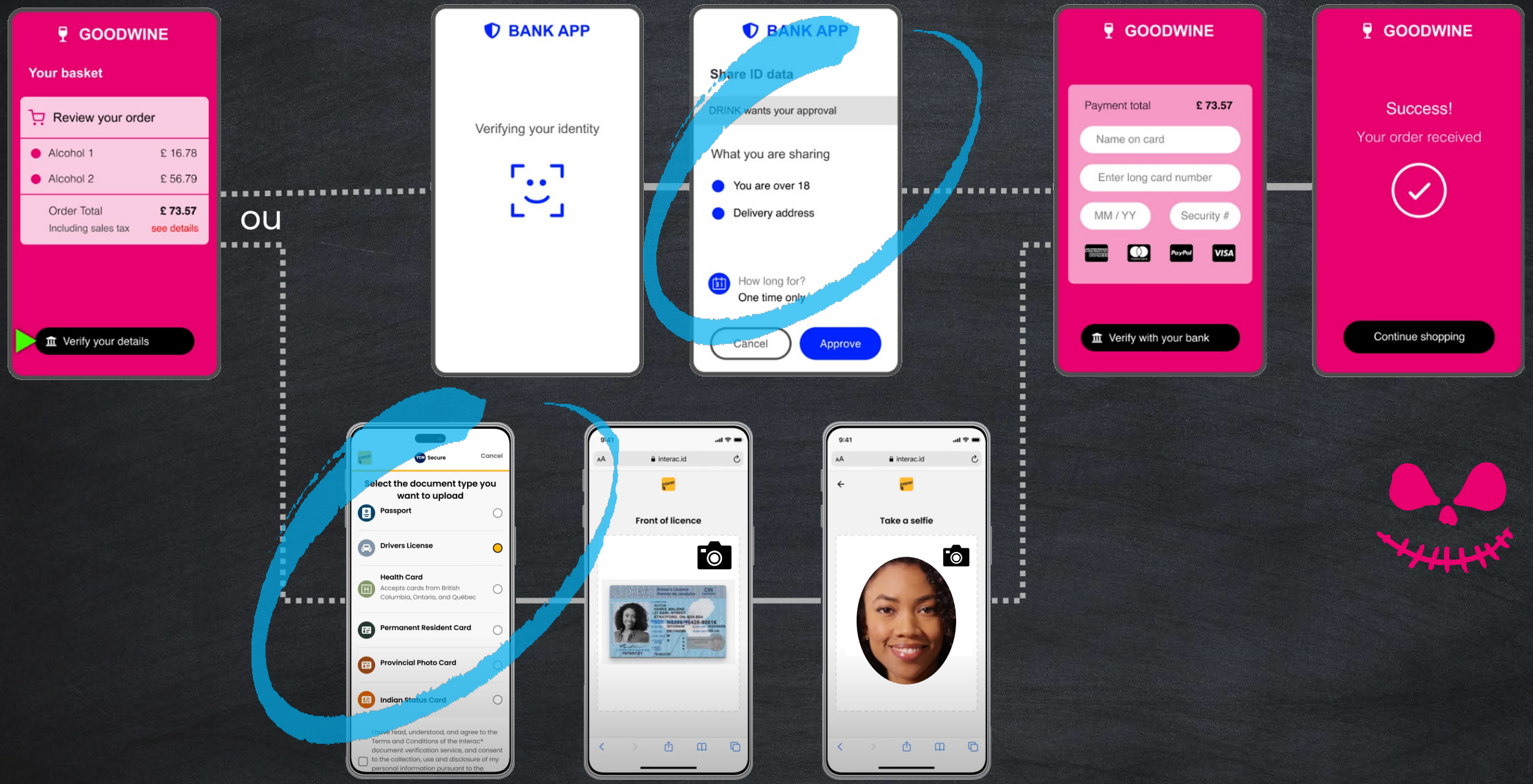
Vérification de l’identité & Identités décentralisées

- **Vérification intégrée de l’identité d’un utilisateur auprès d’un organisme tiers de confiance**

Vérification de l'identité, & identités décentralisées

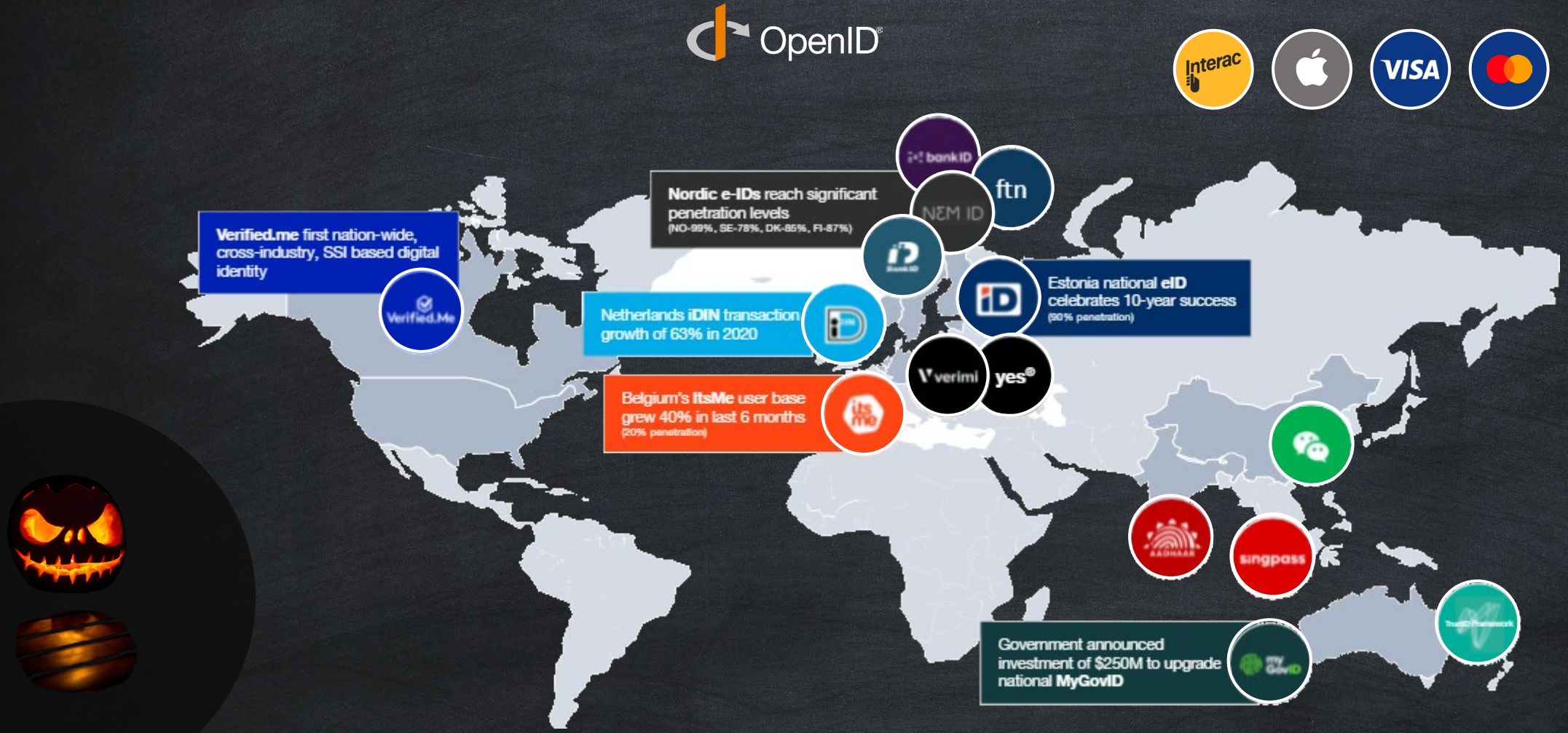


Vérification de l'identité, & identités décentralisées (suite)



Vérification de l'identité, & identités décentralisées (suite)

GAIN PoC – Global Assured Identity Network



IDENTITY DAYS

Gestion de la menace sur les identités (ITDR)

L'Identité, principal vecteur de la matrice du MITRE ATT&CK

La plupart des cyberattaques sont basées sur l'identité

Reconnaissance	Développement des Ressources	Accès Initial	Exécution	Persistance	Élévation de Privilège	Évasion de la Défense	Accès aux Identifiants	Découverte de Données	Déplacements Latéraux	Collecte	Commande et Contrôle (C2)	Exfiltration	Impact
• Hameçonnage • Sondage des services d'authentification • Collecte des identifiants de la victime	• Pirater les comptes des victimes • Établir des comptes sur les systèmes des victimes • Exploiter les relations de confiance	• Hameçonnage • Compromission de la chaîne d'approvisionnement • Utiliser des comptes valides	• Exécution initiée par l'utilisateur	• Édition de comptes • Création de comptes • Utilisation d'autres comptes valides • Modification des politiques d'authentification	• Abus des contrôles d'élévation de privilège • Création / édition de jetons d'accès • Modification des politiques et des confiances de domaine • Ajout / modification de la fédération • Ajout de contrôleurs de domaine malveillants • Subversion des contrôles de confiance	• Abus des contrôles d'élévation de privilège • Manipulation des jetons d'accès • Création / édition de jetons d'accès • Ajout / modification des permissions • Usurpation d'identité • Modification des politiques d'authentification • Ajout de contrôleurs de domaine malveillants • Dissimulation d'artefacts • Effacement des journaux	• Utilisation d'identifiants trouvés, piratés, contrefaits ou internes • Modification des politiques d'authentification • Extraction des identifiants des OS / applications • Interception de l'authentification multi-facteurs • Vol / contrefaçon de jetons, tickets, certificats et cookies • (Toutes les techniques impliquent l'identité)	• Comptes • Confiances de domaine • Ressources • Politiques de groupe • Politiques de mots de passe • Listes de membres de groupe • Permissions • Propriétaires de systèmes	• Hameçonnage interne • Exploitation de services à distance • Utilisation de matériel d'authentification alternatif (jetons SAML contrefaits)	• Utilisation de comptes récoltés ou créés lors de tactiques précédentes	• Utilisation de comptes récoltés ou créés lors de tactiques précédentes	• Utilisation de comptes récoltés ou créés lors de tactiques précédentes	• Suppression de compte • Déni de service (DoS) • Arrêt de services • Détournement de ressources • Dommages de divers types et coûts • Inhibition de la récupération

Détection & remédiation de la menace sur les Identités

Vulnérabilités

- Identités exposées
- Identités mal configurées
- Identités non gérées

Menaces

- Vol / prise de contrôle de compte
- Menaces internes / d'initiés
- Phishing et ingénierie sociale
- Utilisation abusive d'un accès privilégié

Surveillance & Détection de la menace

- **Tentatives** de connexion inhabituelles
- **Accès non autorisé** à des données sensibles
- **Robot** vs. Humain
- **Manière inhabituelle** de taper, rythme de pression des touches, façon de tenir ou main qui tient le téléphone, *swipe*
- **Adresse IP, lieu, heure, appareil, navigateur,** inhabituels ou suspects
- **Déplacement** entre 2 endroits à une vitesse impossible

Analyse & réaction automatique

Blocage ou autre action IAM

sur la tentative d'accès

Intégration et alerte aux autres capacités cyber

(SIEM, Pares-feux, IDS)

Authentification basée sur le risque

- **Authentification multi-facteurs « sur stéroïdes »**
- **Différents niveaux d'accès d'une personne, en fonction de son comportement et du niveau de risque évalué en temps réel et vs. historique**

➔ Ex: « Peut-être accès OK pour la 100ème fois depuis le même appareil et même endroit …
… MAIS a-t-on une vitesse ou taux d'erreur d'écriture très différent de d'habitude? Si OUI, demandons une authentification fort en plus! »

Authentification basée sur le risque (RBA)

Authentification | **Évaluation du score de risque** | **Ajustement de Méthode d'authentification**

Score de risque

- Faible
- Élevé

Critères

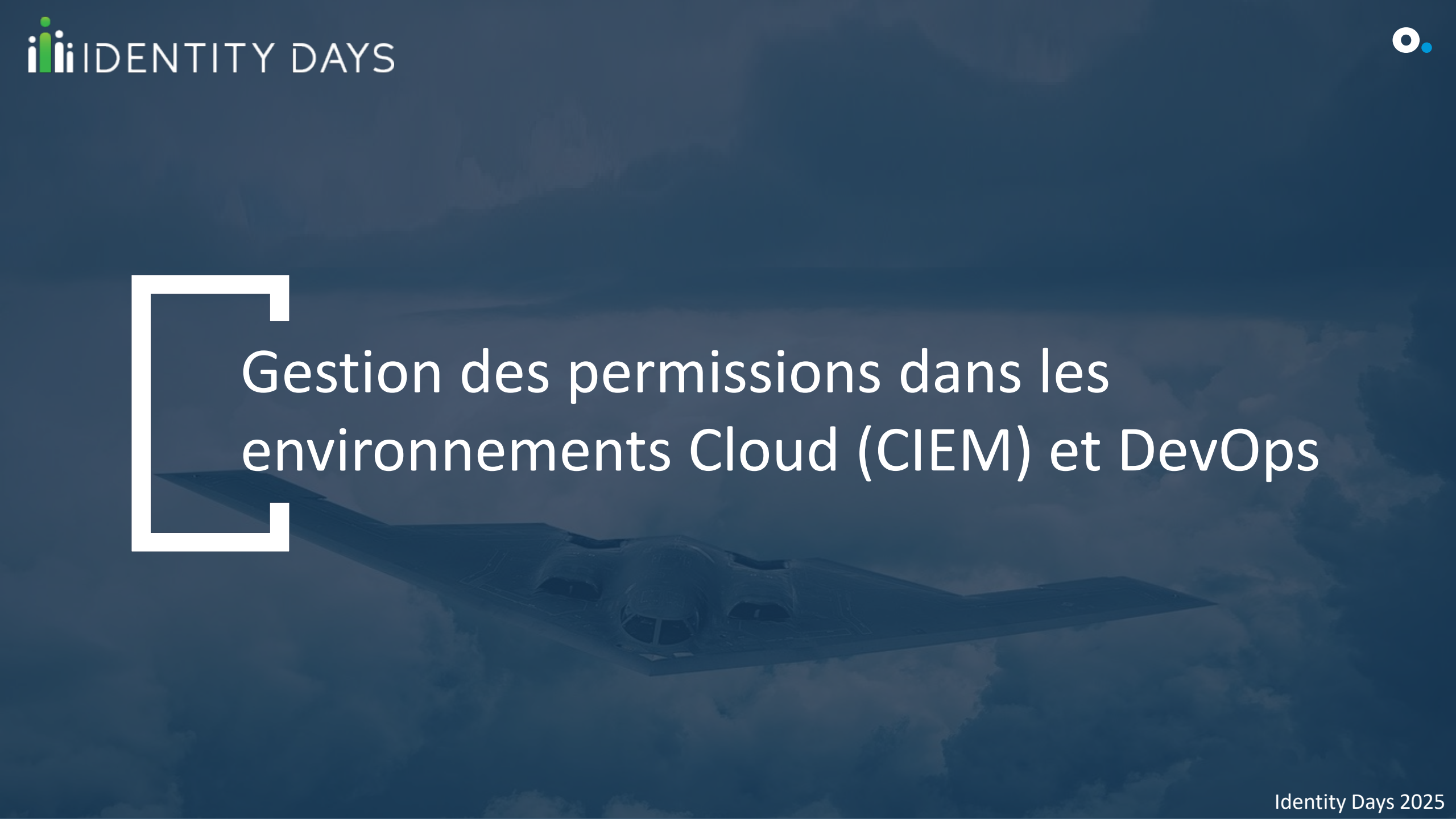
- ✓ **Sensibilité** des données, **criticité** de l'action
- ✓ **Manière** de taper, rythme de pression des touches, façon de tenir ou main qui tient le téléphone, *swipe*
- ✓ **Lieu, heure, appareil, navigateur, IP**
- ✓ **Déplacement** entre 2 endroits à une vitesse impossible
- ✓ **Historique** d'incidents, nb de tentatives
- ✓ **Détection de robot**

Authentification additionnelle

(ex: FIDO 2, ...)

IDENTITY DAYS

Gestion des permissions dans les environnements Cloud (CIEM) et DevOps

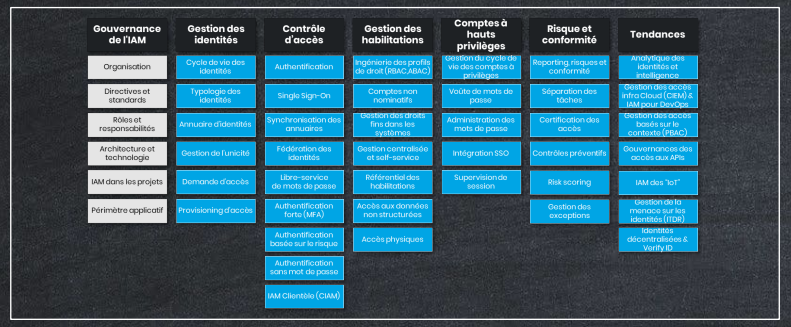


IDENTITY DAYS

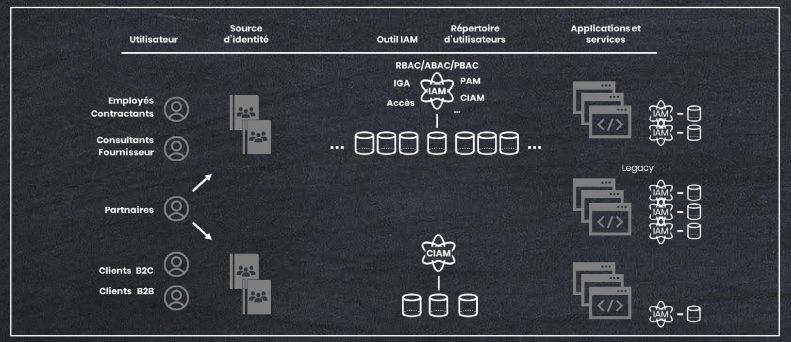
Zero Trust & l'Identity Fabric

Identity Fabric : Concept et objectifs

Cadre de capacités IAM

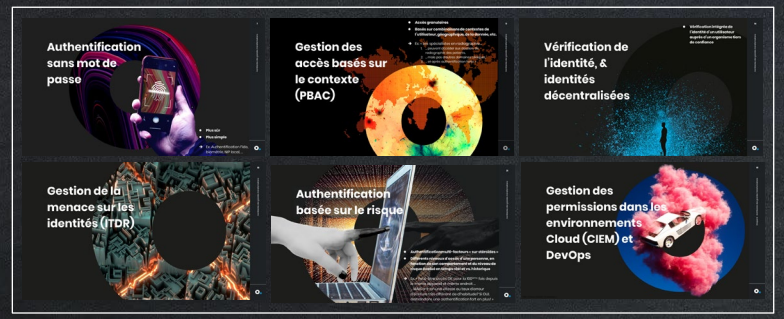


Environnement IT & IAM complexe



Nouvelles fonctions IAM

pour gérer les menaces en évolution



Identity Fabric

L'Identity Fabric a vocation à résoudre les problèmes de:

- **Complexité** (incl. Legacy)
- **Interopérabilité** (ex:
  - entre capacités IAM/cyber
  - avec environnement tiers)
- **Évolutivité**
- **Expérience fragmentée des utilisateurs**

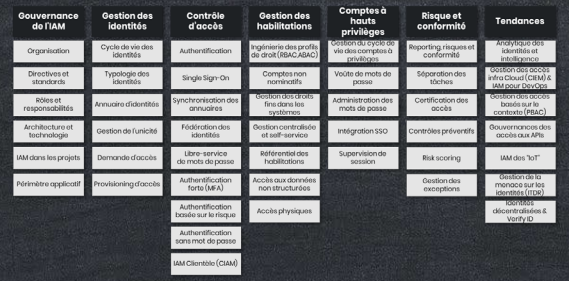
L'Identity Fabric, une évolution, pas une révolution

Utilisateurs

- **Employés, Contractants**
- **Fournisseurs, Consultants**
- **Partenaires**
- **Clients B2 C & B2B**
- **Postes de travail et mobiles, serveurs, composants réseaux Objets connectés**

Éléments clés d'une Identity Fabric

Capacités IAM fondamentales



+

- **Basée sur API** (crucial pour l'interopérabilité)
- **Orchestration Zero Trust**
  - Basée sur des signaux et événements internes et externes (SSE *)
  - Gestion des sessions en continu (CAEP *)
  - Identités centralisées & décentralisées
- **RBA & ITDR**
- **Intégration des applications Legacy** pour la gestion des accès (low code)
- **Synchronisation / consolidation des annuaires**
- **Gestion des accès env. Cloud (CIEM) et DevOps**

Applications & services cibles

Internes

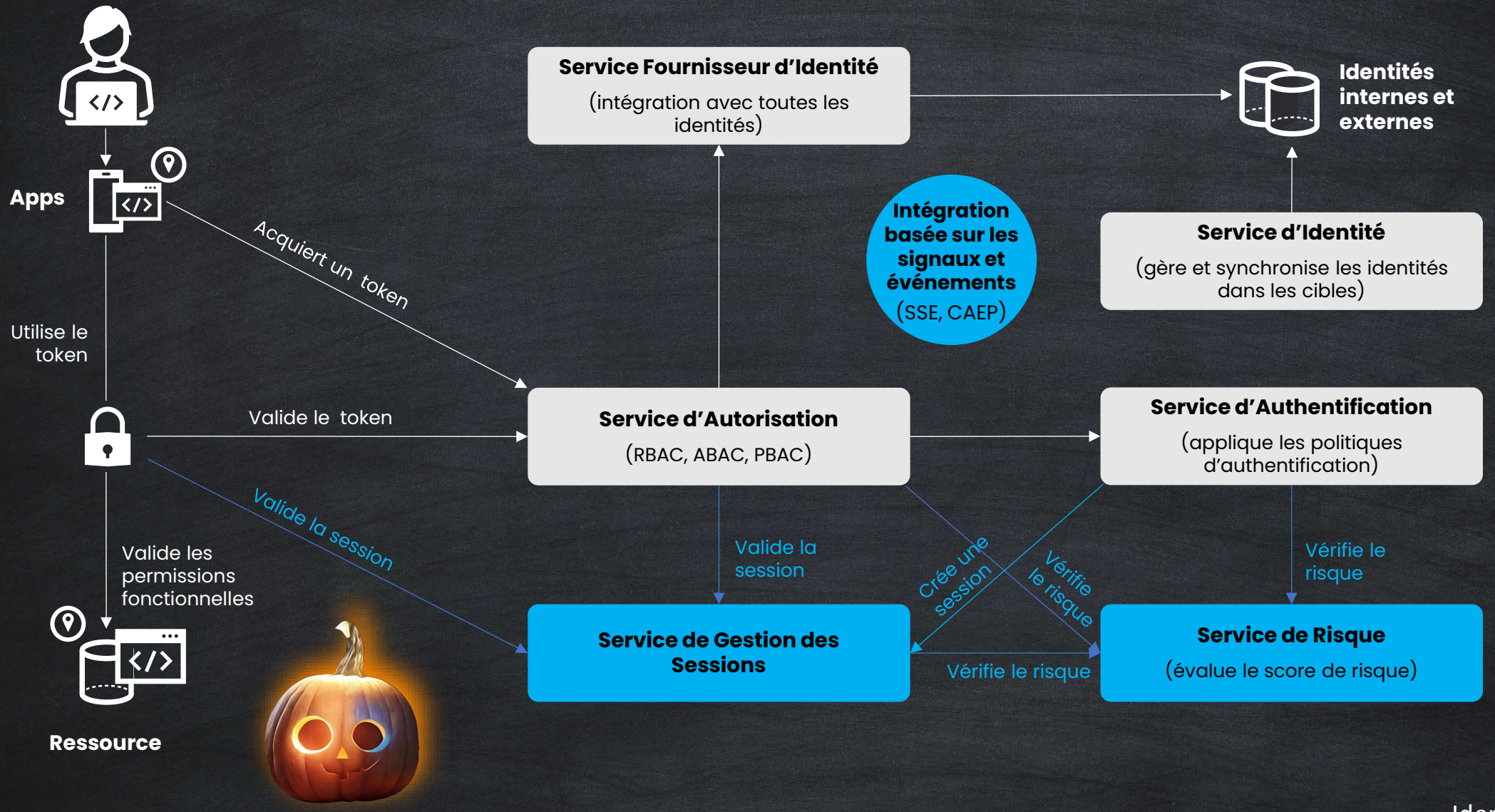
- Apps fédérées
- Web apps non fédérées
- Apps Legacy

Externes

- Cloud Public
- Cloud Privé
- Apps de partenaires avec fédération
- Apps de partenaires sans fédération

OpenID (*) https://openid.net/wg/sharedsignals/

Illustration d'une architecture Zero Trust



IDENTITY DAYS

Eric PÉRION

onepoint.
Au-delà de l'évidence

Merci !

IDENTITY DAYS

Sources

1. “The Top Trends Shaping Identity And Access Management In 2025” (Forrester, 2025), https://reprint.forrester.com/reports/the-top-trends-shaping-identity-and-access-management-in-2025-663a8ede/index.html
2. “What is the Identity Fabric?” (IBM, 2024), https://www.youtube.com/watch?v=uN5rr4n1fI0
3. “Definition: Identity Fabric” (Gartner, 2023) https://www.gartner.com/en/documents/4903431
4. “Identity Fabrics: Delivering IAM for the Digital Business” (KuppingerCole, 2021), https://www.youtube.com/watch?v=37p6G9WNmNk
5. “Evolving Identity and Access Management for the Digital Era” (KuppingerCole & Broadcom, 2023), https://www.kuppingercole.com/watch/evolving-iam-for-digital-era
6. GAIN PoC WhitePaper (Fondation OpenID, 2021), https://gainforum.org/GAINWhitePaper.pdf
7. Interac Verified (Interac), https://www.interac.ca/en/business/our-solutions/interac-verified/
8. Identity threat detection and response (IBM, 2024), https://docs.verify.ibm.com/verify/docs/use-cases-itdr
9. "Qu'est-ce que l'ITDR (Identity Threat Detection & Response) ?" (Proofpoint), https://www.proofpoint.com/fr/threat-reference/identity-threat-detection-and-response-itdr
10. "What is Identity Threat Detection and Response (ITDR)?” (StrongDM, 2024), https://www.strongdm.com/what-is/identity-threat-detection-response-itdr
11. “The Future of Identity Security: PAM+CIEM+ITDR” (KuppingerCole & BeyondTrust, 2023), https://www.kuppingercole.com/watch/identity-security-pam-ciem-itdr

21 octobre 2025 - PARIS

@IdentityDays
#identitydays2025