N°58
PRIX : 24€ TTC
TRIMESTRIEL
FÉVRIER > AVRIL 2025

Global Security Mag

THE LOGICAL & PHYSICAL SECURITY MAGAZINE

L'IDENTITÉ ET L'ACCÈS NUMÉRIQUES EN CYBERSÉCURITÉ

INTERVIEWS

p. 17

Dr. Yosra Barbier
Regional Information Security Officer-Europe de l'Ouest Allianz Partners et Secrétaire du CEFCYS, Ph.D

p. 27

Loïc GUÉZO
Vice-Président du Clusif, Senior Director, Cybersecurity Strategy, Proofpoint

OFFERT PAR

FÉDÉRATION FRANÇAISE DE LA CYBERSÉCURITÉ
FFCYBER


LEVAS SAS
CYBER INFO
Vous souhaite une excellente année
2025
levas-cyberformations.com

EDITO

L'ART DE LA TRANSMISSION

Il semble essentiel de savoir transmettre…

Après avoir œuvré pour créer et pérenniser l'Identité du Magazine Global Security Mag (GS Mag) et de l'évènement GS Days (Les journées francophones de la Sécurité de l'Information et de la Cyber), après avoir brillamment accompli la mission essentielle de la diffusion de l'Information au sein de la communauté Cyber et Cybersécurité, Marc Jacob Brami a choisi de me transmettre la mission.

Afin que l'accès à l'Information continue à travers de multiples canaux, nous avons décidé de relancer le Magazine GS Mag en format papier et numérique, à l'occasion de la 15e édition des GS Days du 28 janvier 2025.

La diffusion du GS Mag en format papier et numérique, avait été interrompue en décembre 2021 (numéro 57). L'année s'était aussi terminée avec notamment une Conférence du CLUSIF (L'Association de référence de la Sécurité de l'Information), titrée, L'Identité numérique dans tous ses états. Alors, quoi de plus naturel que le thème principal de ce 58e numéro, soit *l'Identité et l'Accès Numériques en Cybersécurité*.

L'Identité numérique est un ensemble d'éléments qui permettent d'identifier les humains, les animaux, les plantes, les objets numériques, et de donner l'accès aux informations numériques après une possible et souhaitable étape d'authentification (vérification de l'identité).

- **L'Internet a transformé le monde et les interactions des êtres.**
- **La transformation numérique du monde s'accélère de plus en plus.**
- **L'Intelligence Artificielle est reconnue comme la nouvelle révolution numérique.**

Le Quantique ou l'Informatique Post-Quantique promettrait de bouleverser le monde numérique, notamment par la capacité illimitée de déchiffrer les données, ce qui pourrait sensiblement augmenter la fameuse surface d'attaque chère aux pirates informatiques.

Alors que faire, comment faire ? S'informer et se sensibiliser le plus souvent possible via Global Security Mag et les GS Days, semble être un des ingrédients pour rester en Vigilance, en Alerte, et en Veille…

THE ART OF TRANSMISSION

It seems essential to know how to pass on…

After having worked to create and perpetuate the identity of Global Security Mag (GS Mag) and the GS Days event (Les journées francophones de la Sécurité de l'Information et de la Cyber), and after having brilliantly accomplished the essential mission of disseminating information within the Cyber and Cybersecurity community, Marc Jacob Brami has decided to hand over the mission to me.

To ensure that access to Information continues through multiple channels, we have decided to relaunch GS Mag in both paper and digital formats, to coincide with the 15th edition of GS Days on January 28, 2025.

The distribution of GS Mag in paper and digital format was interrupted in December 2021 (issue 57). The year also ended with a conference organized by CLUSIF (L'Association de référence de la Sécurité de l'Information), entitled L'Identité numérique dans tous ses états.

So what could be more fitting than for the main theme of this 58th issue to be Digital *Identity and Access in Cybersecurity*.

Digital Identity is a set of elements that identify humans, animals, plants and digital objects, and give access to digital information after a possible and desirable authentication stage (identity verification).

- **The Internet has transformed the world and the way people interact with each other.**
- **The digital transformation of the world is accelerating.**
- **Artificial Intelligence is recognized as the new digital revolution.**

Quantum or Post-Quantic Computing promises to turn the digital world upside down, notably through the unlimited ability to decipher data, which could significantly increase the famous attack surface so dear to hackers.

So what can be done? Getting informed and raising awareness as often as possible, via Global Security Mag and GS Days, seems to be one of the ingredients for staying Vigilant, Alert and On the Lookout…

HS2
Hervé Schauer Sécurité

Formation cybersécurité technique

INTRODUCTION • RÉSEAUX
INFRASTRUCTURES • DÉFENSE

PROGRAMME

Introduction à la cybersécurité

ESSCYBER
Essentiels techniques de la cybersécurité
SECUCYBER
Fondamentaux techniques de la cybersécurité

Sécurité des réseaux et des infrastructures

SECUARCH
Sécurité des architectures
SECUWIFI
Sécurité et Red Team Wi-Fi moderne
SECUPKI
Infrastructures de clés publiques
SECUPKIWIN
Infrastructures de clés publiques Windows

Sécurité défensive

SECUWIN
Sécurisation des infrastructures Windows
SECULIN
Sécurité Linux
SELinux
Comprendre SELinux et savoir modifier la politique de sécurité
SECUWEB
Sécurité des serveurs et des applications Web
SECUINDUS
Cybersécurité des systèmes industriels
SECUOBJ
Sécurité des objets connectés
SECUMOBILE
Audit sécurité d'applications mobiles Android et iOS

+ 33 974 774 390

www.hs2.fr

formation@hs2.fr

SOMMAIRE

SUMMARY

N°58 FEVRIER>AVRIL 2025
globalsecuritymag.fr,
globalsecuritymag.com,
globalsecuritymag.de, gsdays.fr
ISSN : 1959 - 7061
Dépôt légal : à parution
Éditée par LEVAS SAS
RCS Paris 947 665 543
5 avenue des Gobelins 75005 Paris
Tél. : +33 7 89 65 15 70
e-mail : vj@globalsecuritymag.com

ABONNEMENT :
Version papier : 24 € TTC (TVA 20%)
Version PDF : 12 € TTC (TVA 20%)

RÉDACTION :
Directeur de la Publication
et Rédacteur en Chef :
Valentin Jangwa

CRÉATION, CONCEPTION ET RÉALISATION GRAPHIQUE
Marine Volpi

PUBLICITÉ :
LEVAS SAS
Présidente : Laurence Beuchard
levas-formations.com
comptabilite@levas-formations.com

COUVERTURE ET INTERIEUR :
ISTOCK

IMPRESSION :
Wagram Editions
8 rue Salvador Allende
95870 Bezons
Imprimé sur papier certifié PEFC

Certifié PEFC
Ce produit est issu de forêts gérées durablement et de sources contrôlées
PEFC
10-32-3010
www.pefc-france.org

COMITÉ SCIENTIFIQUE :
Pierre Bagot, Francis Bruckmann
Eric Doyen, Catherine Gabay,
François Guillot, Olivier Iteanu,
Dominique Jouniot,
Patrick Langrand, Yves Maquet,
Thierry Ramard, Hervé Schauer,
Michel Van Den Berghe,
Bruno Kerouanton, Loïc Guézo,
Marc Jacob Brami, Sylvie Lévy,
Yelena Jangwa-Nedelec,
Anne Guyot, Nicolas Liard et
Valentin Jangwa, In Memoriam,
notre regretté Zbigniew Kostur

Future of IT

19 JUIN 2025

AGORA CLUB

DSI et CIO

Paris · Lyon · Nantes · Bordeaux

AGORA CLUB

RSSI et CISO

IN CYBER FORUM 1-3 AVRIL 2025 LILLE GRAND PALAIS

Au-delà du *Zero Trust*, la confiance pour tous

europe.forum-incyber.com

ORGANISÉ PAR Forward

AVEC LE SOUTIEN DE Région Hauts-de-France MEL MÉTROPOLE

RETROUVEZ-NOUS SUR YouTube LinkedIn

> JANVIER <

- **14 janvier • Paris**
  Dîner du Cercle de la sécurité
  www.lecercle.biz
- **14 > 16 janvier • Dubaï (EAU)**
  Intersec
  www.intersecexpo.com
- **15 > 17 janvier • Osaka (Japon)**
  Japan IT Week
  www.japan-it-osaka.jp/en-gb.html
- **20 > 22 Janvier • Putrajaya, (Malaysia)**
  Asia International Security Summit & Expo 2025 (AISSE'25)
  aisse.my/
- **21 > 22 janvier • Dubaï**
  CS4CA MENA
  www.cs4ca.com
- **23 janvier - Paris**
  Panocrim du CLUSIF
  www.clusif.fr
  Matinale du CRIP
  www.crip-asso.fr/events
- **28 janvier**
  Paris 3e Espace Saint-Martin
  GS DaysJournées Francophones de la Sécurité de l'Information et de la Cyber • 15e édition
  Web : www.gsdays.fr
  Paris
  La nuit de l'AN2V
  www.an2v.org
- **28 > 29 janvier • Bangkok (Thailand)**
  Cybersec asia
  cybersec-asia.net/
- **29 janvier • Helsinki (Finlande)**
  e-crime & cybersecurity Nordics
  akjassociates.com/
- **29 > 30 janvier**
  Paris
  Cyber Show Paris
  www.cybershowparis.fr/
  Porte de Versailles - Paris
  Learning Technologies
  www.learningtechnologiesfrance.com

> FÉVRIER <

- **5 > 6 février**
  Paris-La-Défense
  IT Partners
  www.itpartners.fr
  Londres (UK)
  Cyber Security & Cloud Expo
  Lieu : Olympia
  www.cybersecuritycloudexpo.com/global/
- **5 > 7 février • Deauville**
  Rencontres AMRAE
  www.amrae.fr/les-rencontres-amrae
- **6 > 7 février • Paris**
  Université de l'AFCDP
  universite-des-dpo-2025.afcdp.net/page/c101-accueil/
- **9 > 12 février • Riyad (Arabie-Saoudite)**
  LEAP
  www.onegiantleap.com
- **10 > 11 février • Dubai, UAE**
  Gartner Security & Risk Management Summit
  www.gartner.com/en/conferences/emea/security-risk-management-uae
- **10 > 12 février •Denvers (USA)**
  Geo Week
  www.geo-week.com
  AEC Next Technology
  www.aecnext.com
  SPAR 3D
  www.spar3d.com/event
- **10 > 13 février • Riyad (Arabie-Saoudite)**
  LEAP
  www.onegiantleap.com
- **11 > 12 février • Deauville**
  Hactiv'Summit
  www.republikgroup-it.fr/hacktivsummit
- **Perth (Australie)**
  CS4CA ANZ
  www.cs4ca.com
- **11 > 13 février • Dubaï (UAE)**
  ISS World Middle East
  www.issworldtraining.com/iss_mea/index.htm
- **13 février • Luxembourg**
  Security Forum
- **17 > 20 février • Lisbonne (Portugal)**
  MAAWG
  www.m3aawg.org
- **18 > 19 février • Bern (Suisse)**
  Swiss Cyber Security Days
  swisscybersecuritydays.ch/
- **20 février • Londres (UK)**
  Technology Live !
  a3communicationspr.com/homepage/events/technology-live/
- **20 > 22 février • Porto (Portugal)**
  ICISSP
  www.icissp.org
- **24 > 25 février • Phoenix, AZ (USA)**
  Gartner CIO Leadership Forum
  www.gartner.com/en/conferences/na/cio-us-west
- **25 > 26 février • Munich (Allemagne)**
  Cyber Security for Critical Manufacturing
  europe.manusecevent.com/

> MARS <

- **3 > 4 mars • Sydney (Australie)**
  Gartner Security & Risk Management Summit
  www.gartner.com/en/conferences/apac/security-risk-management-australia
- **4 > 5 mars • Londres (UK)**
  e-crime & cybersecurity Congress
  akjassociates.com/
- **4 > 7 mars • Tokyo (Japon)**
  Security Show
  www.shopbiz.jp/en/ss
- **5 > 6 mars • Barcelone (Espagne)**
  Mobile World Congress
  www.mobileworldcongress.com
- **10 > 15 mars • Genève (Suisse)**
  Insomni'hack
  insomnihack.ch
- **11> 13 mars**
  Houston - Texas (USA)
  Critical Infrastructure Protection & Resilience North America
  www.ciprna-expo.com
  Lagos (Nigeria)
  Securex West Africa
  www.securexwestafrica.com
- **12 > 13 mars • Londres (UK)**
  Cloud Expo Europe & Data Centre World & Smart IOT
  www.cloudexpoeurope.com
- **13 mars • Paris**
  Matinale Cybersécurité du CRIP
  www.crip-asso.fr/events
- **18 > 20 mars**
  Cannes
  IT & CYBERSECURITY MEETINGS
  www.it-and-cybersecurity-meetings.com
  Hanovre (Allemagne)
  SecIT
  www.secit-heise.de
  Amsterdam (Pays-Bas)
  SGTech Week
  www.smartgrid-forums.com
- **19 > 20 mars • Porte de Versailles - Paris**
  Documation & Data Intelligence Forum
  www.documation.fr/
  Solutions Intranet & Collaboratif
  www.salon-intranet.com
- **19 > 22 mars • Brno (République Tchèque)**
  DFRWS EU
  dfrws.org/conferences/dfrws-eu-2025/
- **20 mars • Olso (Norvège)**
  Data Center Forum
  www.datacenter-forum.com/events/oslo/2025
- **21 mars • Online**
  Conférence AFCDP
  universite-des-dpo-2025.afcdp.net/page/c101-accueil/
- **24 > 25 mars • London (UK)**
  Gartner Identity & Access Management Summit
  www.gartner.com/en/conferences/emea/identity-access-management-uk
- **24 > 26 mars • Tel Aviv (Israël)**
  Cybertech Goblal Tel Aviv
  www.cybertechisrael.com/
- **25 > 26 mars • Houston, Texas (USA)**
  CS4CA USA
  www.cs4ca.com
- **26 > 28 mars • Sophia (Bulgarie)**
  Real World Crypto
  rwc.iacr.org/2025/
- **27 mars • Paris**
  Diner du Cercle de la sécurité
  www.lecercle.biz
- **31 mars > 4 avril • Hanovre (Allemagne)**
  HANNOVER MESSE
  www.hannovermesse.de/en

> AVRIL <

- **1er avril • Lille**
  CoRI&IN
  www.cecyf.fr
- **1er > 2 avril • Francfort (Allemagne)**
  DACHsec
  cyberseries.io/dachsec/
- **1er > 3 avril • Lille**
  Forum InCyber Europe ex FIC
  europe.forum-incyber.com/
  ID Forum
  id-forum.eu/
- **1er > 4 avril**
  Singapour
  Black Hat Training & Briefings Asia
  www.blackhat.com
  Las Vegas (USA)
  ISC West
  Web : www.iscwest.com
- **6>8 avril • Singapour**
  CS4CA APAC
  www.cs4ca.com
- **8 > 10 avril**
  Amsterdam (Pays-Bas)
  Commercial UAV Expo Europe
  www.expouav.com/europe
  Prague (République Tchèque
  Smart Systems Integration
  Web : www.smartsystemsintegration.com
- **9 avril • Stockholm (Suède)**
  e-crime & cybersecurity Nordics
  akjassociates.com/
- **10 > 11 avril • Barcelone (Espagne)**
  Third Party & Supply Chain Cyber Security Virtual Summit
  sccybersecurity.com/
- **15 avril • Istanbul (Turquie)**
  ENBANTEC Cyber Security
  www.enbantec.com
- **15 > 17 avril • Moscou (Russie)**
  Securika/MIPS
  www.securika-moscow.ru/Home
- **16 > 17 juin • Singapour**
  CS4CA APAC
  www.cs4ca.com
- **21 > 23 avril • Angers**
  BotConf
- **21 avril**
  Workshops
- **22 > 25 avril**
  Conférence
  www.botconf.eu
- **23 > 24 avril • Madrid (Spain)**
  Cyber Intelligence Europe
  intelligence-sec.com/events/cyber-intelligence-europe-2025/
- **23 > 25 avril • Tokyo (Japon)**
  Japan IT Week
  www.japan-it.jp/en
- **28 avril > 1er mai • San Francisco (USA)**
  RSA Conference
  www.rsaconference.com
- **28 avril > 2 mai • Sydney (Australie)**
  The Web Conference
  www2025.thewebconf.org/
- **29 avril • Helsinki (Finlande)**
  Data Center Forum
  www.datacenter-forum.com/events/helsinki/2025
- **29 > 30 avril • Oman (Muscat)**
  DTX Oman
  Lieu : Sheraton Oman Hotel
  www.dtxoman.com
- **30 avril • Vienne (Autriche)**
  e-crime & cybersecurity Austria
  akjassociates.com/
- **30 avril - 1er mai • Londres (UK)**
  Learning Technologies
  www.learningtechnologies.co.uk/

JULIETTE GIRAULT

Directrice communication du Clusif

INTELLIGENCE ÉCONOMIQUE ET SÉCURITÉ DE L'INFORMATION : DES LIENS À TISSER

LA GUERRE DE L'INFORMATION EST DÉSORMAIS UNE RÉALITÉ CONCRÈTE POUR NOMBRE D'ENTREPRISES, OU DEVRAIT L'ÊTRE. UNE PRISE DE CONSCIENCE SALUTAIRE QUAND, RÉSEAUX SOCIAUX À L'APPUI, LES SPHÈRES D'INFLUENCES SE DIVERSIFIENT, S'ÉLARGISSENT, SE DÉCONCENTRENT.

La cybersécurité a donc déjà l'intelligence économique (IE) dans son champ de vision, à tel point que le thème est régulièrement abordé par les professionnels. Citons par exemple la conférence du Clusir Normandie en 2022 ou celle du Clusif en 2024.

Plus largement, des pans entiers du vocabulaire de l'intelligence économique se retrouvent dans la prise de décision opérationnelle d'acteurs de tous les secteurs sociaux et économiques. Les crises récentes nous ont brutalement rappelé la relative fragilité de nos économies et dans une certaine mesure de nos institutions. Dans un jeu d'acteurs étatiques, économiques et cybercriminels en mouvement, les décisions doivent être précédées d'une documentation préalable des acteurs et des processus à l'œuvre. Des lignes de force.

EN PRATIQUE

La posture de l'intelligence économique a ceci de particulier qu'elle place le maniement de l'information au centre de son dispositif. En réception avec la veille, en émission avec l'influence. L'IE pense la décision comme inscrite dans un référentiel en mouvement. Elle est soumise bien sûr à des objectifs stratégiques mais aussi à la position des forces en présence à un moment.

Dans le domaine qui est le mien, celui de la communication, le professionnel se positionne à la croisée des chemins entre une organisation qui veut s'exprimer, exposer sa vision, proposer ses solutions, et un environnement où plusieurs langues se parlent, où de nombreux intérêts peuvent diverger, s'affronter, coopérer ou un peu de tout cela à la fois. Le communiquant qui veut appliquer les préceptes enseignés par l'IE écoute avant de parler. Il n'applique pas à l'aveugle les préceptes rutilants qui lui sont proposés, il lit le contexte et propose une voie qui ne vaut que si elle est informée. Il fait en sorte que son organisation parle d'une voix audible, intelligible, cohérente et qu'elle prenne toute sa place dans l'adversité d'où qu'elle vienne. Bref, l'information n'est pas du bruit, c'est un élément stratégique à part en entière. Et cela change tout.

CYBERSÉCURITÉ ET INTELLIGENCE ÉCONOMIQUE : QUELLES SYNERGIES ?

L'information trouve sa place assez naturellement dans la stratégie économique d'une entreprise, c'est en tout cas à souhaiter. Mais dans quelle mesure est-ce le cas dans d'autres disciplines comme la cybersécurité ? Quelles synergies peut-on dégager entre les équipes dédiées à l'intelligence économique et celles de la sécurité de l'information ? Ces disciplines ont-elles mutuellement des choses à s'apprendre ?

L'évolution récente des enjeux technologiques (IA, cryptomonnaies) et les rapports de force géopolitiques semblent accentuer les phénomènes cybercriminels à l'œuvre depuis plusieurs années. Lors de notre Panorama annuel de la cybercriminalité, les experts du Clusif se penchent notamment sur les aspects géopolitiques de la cybercriminalité. Une véritable clé de lecture des grands mouvements qui viennent impacter l'ensemble de notre tissu économique. Et je ne crois pas, à titre tout à fait personnel, que l'on puisse indéfiniment séparer le support de l'information de son contenu.

Quelles directions prendre, doit-on trouver des synergies ou à tout le moins amorcer un dialogue constructif, les professionnels des deux disciplines le diront. Mais gageons que la résilience collective passera par l'esprit d'échange et de progrès que nous avons toute capacité à produire. ■

Les crises récentes nous ont brutalement rappelé la relative fragilité de nos économies et dans une certaine mesure de nos institutions.

HS2
Hervé Schauer Sécurité

shutterstock

Formation Vie privée, Droit de la cybersécurité et Continuité d'activité

PROGRAMME

Vie privée et droit de la cybersécurité

RGPD :
RGPD/GDPR / Réglement Européen sur la Protection des Données personelles
DPO :
Formation DPO / Privacy Implementer
PIA :
PIA / ISO29134 / Appréciation des impacts sur la vie privée
SECUSANTE :
Protection des données de santé et vie privée
SECUDROIT :
Droit de la cybersécurité
SECUCLOUD :
Sécurité du cloud

Continuité d'activité

RPCA :
Formation RPCA
ISO22LA :
ISO22301 Lead Auditor
ISO22LI :
ISO22301 Lead Implementer

idcomm.fr

+33 974 774 390

www.hs2.fr

formations@hs2.fr

ÉRIC SINGER

Point du vue du RSSI Responsable Cursus Cybersécurité, ESIEE-IT

SELON VOUS,

QUELS SONT LES ENJEUX DU SUJET DE L'IDENTITÉ ET DE L'ACCÈS NUMÉRIQUES EN CYBERSÉCURITÉ

(employé.e.s ; consommateurs ; fournisseurs ; partenaires ; objets connectés ; etc.) ?

DANS UN MONDE DE PLUS EN PLUS CONNECTÉ ET OUVERT, LES INTERACTIONS AVEC DIVERS INTERLOCUTEURS TELS QUE LES EMPLOYÉS, CLIENTS, FOURNISSEURS ET SYSTÈMES AUTOMATISÉS SE MULTIPLIENT.

Le volume d'échanges par e-mail a considérablement augmenté depuis la pandémie de COVID-19. **En 2018, environ 280 milliards d'e-mails étaient échangés quotidiennement dans le monde.** Ce chiffre a atteint 347,3 milliards en 2023 et devrait dépasser 390 milliards en 2026.

Parallèlement, le nombre d'adresses e-mails a également augmenté, passant de 3,8 milliards en 2018 à une prévision de 4,7 milliards en 2026. Cette croissance est à mettre en perspective avec l'augmentation du nombre d'objets connectés (IoT), qui est passé de 7 milliards en 2018 à une estimation d'environ 30 milliards en 2026. Cet accroissement exponentiel de l'usage des identités numériques montre la systématisation des solutions digitales basées sur ces identités.

Cela représente une opportunité pour optimiser les processus métier et mieux connaître ses clients, mais cela comporte également des risques importants.

>>>

>>> POUR LES EMPLOYÉS

La gestion des identités des employés est prépondérante pour sécuriser l'accès aux applications et aux informations de l'entreprise. Elle garantit que chaque employé, selon ses droits et responsabilités, accède uniquement aux services et informations nécessaires à l'accomplissement de ses fonctions.

En appliquant le principe du moindre privilège et en adoptant un système de gestion des identités et des accès (IAM), les entreprises limitent l'accès des employés aux seules ressources indispensables à leurs fonctions. Cette approche réduit significativement la surface d'attaque en cas de compromission de comptes. De plus, sensibiliser les utilisateurs aux risques de phishing et mettre en place une authentification forte, telle que l'authentification à deux facteurs via un dispositif mobile, renforcent la sécurité des accès.

> Le volume d'échanges par e-mail a considérablement augmenté depuis la pandémie de COVID-19

POUR LES CONSOMMATEURS

Il est essentiel que les consommateurs ne soient plus les victimes directes des conséquences du vol de leurs données personnelles. Malgré les sanctions prévues par le RGPD, les violations massives de données clients restent trop fréquentes. Les récentes fuites de données touchant des acteurs majeurs de la distribution (Auchan, Free, SFR, Picard, Cultura, ...) soulignent l'urgence d'adopter des solutions de gestion d'identité et des accès clients (CIAM) pour prévenir ces types d'incidents et de préserver la confiance des consommateurs.

POUR LES FOURNISSEURS ET PARTENAIRES

Les attaques par la chaîne d'approvisionnement (supply chain attack) sont devenues une menace majeure pour la sécurité des entreprises. Les fournisseurs et partenaires sont desormais partie prenante de dans la chaîne de sécurité. Il est important de s'assurer que l'accès aux systèmes et aux données est sécurisé et que les partenaires adhèrent aux mêmes standards de sécurité que l'entreprise. Cela peut inclure des audits de sécurité réguliers, des accords de niveau de service (SLA) et l'implémentation de protocoles de communication sécurisés.

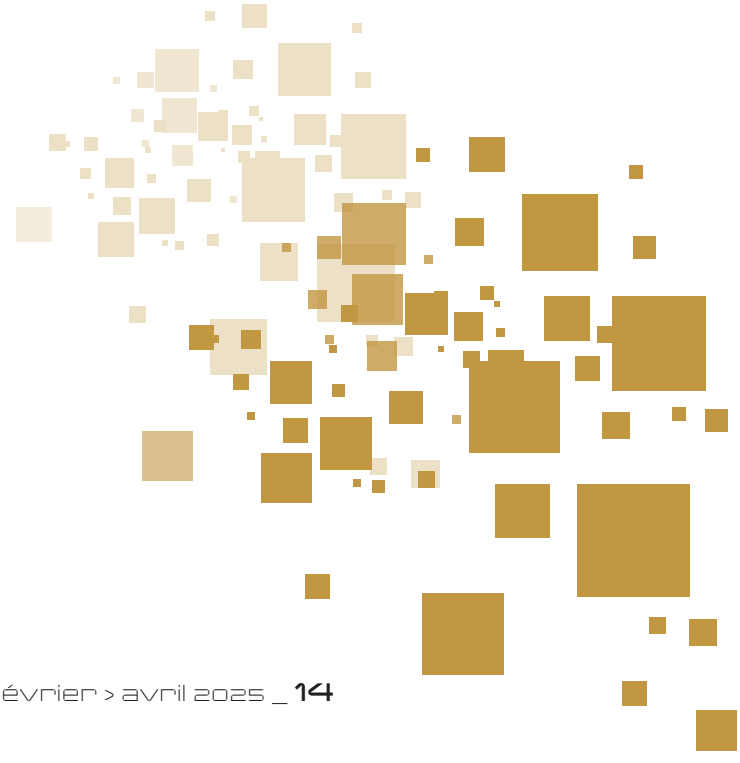
Les fournisseurs et les partenaires doivent être considérés comme des «tiers de confiance». Pour ce faire, il est indispensable d'établir des relations de confiance basées sur la transparence et la collaboration. Les fournisseurs et partenaires doivent être informés des politiques de sécurité de l'entreprise et être prêts à collaborer en cas d'incident de sécurité. La gestion des identités et des accès doit donc intégrer les partenaires externes, avec des rôles et permissions clairement définis.

POUR LES OBJETS CONNECTÉS (IOT)

Les objets connectés, ou Internet des Objets (IoT), posent un défi supplémentaire. Ces dispositifs permettent d'ajouter de « l' intelligence » et d'interconnecter, superviser et faire communiquer divers équipements dans les maisons, les voitures, ainsi que dans les infrastructures industrielles ou urbaines. Cependant, leur sécurité est parfois négligée, et bien qu'ils puissent fonctionner sur le long terme, leur protection n'est pas toujours garantie sur l'ensemble de leur cycle de vie.

Dans un écosystème « intelligent », pour se prémunir contre les cyberattaques, il est nécessaire de s'assurer que seuls des IoT autorisés et suffisamment sécurisés participent à son fonctionnement. Cela nécessite de sécuriser l'authentification des appareils, de maintenir leurs logiciels à jour avec les derniers correctifs de sécurité et de surveiller en continu les activités suspectes.

Les fabricants jouent un rôle important en intégrant dès la conception des fonctionnalités de sécurité pérennes et des mécanismes de gestion des identités pour leurs objets connectés. En parallèle, les entreprises doivent adopter des politiques de sécurité spécifiques aux appareils IoT afin de minimiser les risques de compromission et de garantir la résilience de leurs infrastructures. ■



REJOIGNEZ LE CESIN

CLUB DES EXPERTS DE LA SÉCURITÉ DE L'INFORMATION ET DU NUMÉRIQUE

COOPÉRATION - CONFIANCE - CONVIVIALITÉ

Un Club au service de ses membres

- # CONFÉRENCES
- # GROUPES DE TRAVAIL
- # ATELIERS
- # ENQUÊTES
- # FILS DE DISCUSSION
- # LIVRABLES
- # PARTAGE D'INFORMATION
- # SITE WEB
- # RÉSEAU SOCIAL
- # FORMATION
- # BOURSE D'EMPLOI
- # PARTENARIATS
- # ECHANGES AVEC LES POUVOIRS PUBLICS

CESIN

TOUS SECTEURS D'ACTIVITÉS GRANDES ENTREPRISES, ADMINISTRATIONS ET ENTREPRISES DE TAILLE INTERMÉDIAIRE

contact@cesin.fr - www.cesin.fr

FRANCK ROUXEL

Point du vue du CISO

SELON VOUS,

GESTION DE L'IDENTITÉ EN 2025

Franck Rouxel, expert en cybersécurité, cumule plus de 25 ans d'expérience dans le numérique. Ancien officier de l'armée de l'air, il a occupé des postes stratégiques de RSSI et de conseiller en sécurité. Son expertise dans la protection des systèmes critiques et sa vision holistique de la sécurité l'amènent aujourd'hui à explorer les dimensions organisationnelles et culturelles de la transformation numérique, essentielles à la résilience des entreprises.

DANS L'UNIVERS NUMÉRIQUE CONTEMPORAIN, L'IDENTITÉ S'IMPOSE COMME LA CLÉ DE VOÛTE DE TOUTE ORGANISATION MODERNE

Cette dimension, autrefois cantonnée à la simple gestion des accès, irrigue désormais l'ensemble des processus d'entreprise, transcendant le cadre traditionnel de la sécurité informatique. Face à l'accélération technologique et à la multiplication des menaces, les organisations doivent déployer des stratégies toujours plus sophistiquées pour protéger ce patrimoine immatériel.

Cette évolution transforme profondément le rôle du CISO (Chief Information Security Officer), et ce dans un contexte géopolitique particulièrement tendu. Les cyberconflits qui accompagnent désormais systématiquement les crises internationales nous font entrer de plain-pied dans ce que l'on pourrait appeler "le numérique de l'incertitude". Les tensions entre grandes puissances, la multiplication des acteurs malveillants étatiques et la militarisation croissante du cyberespace créent un environnement où la protection des identités numériques devient un enjeu de souveraineté. Dans ce contexte volatile, le CISO évolue vers un rôle d'acteur de l'antifragilité organisationnelle. Cette métamorphose ne répond plus seulement à des impératifs technologiques, mais aussi à une nécessité stratégique face à des menaces hybrides, où les frontières entre cybercriminalité classique et opérations d'État deviennent de plus en plus floues.

Au cœur de cette transformation, les solutions d'Identity and Access Management (IAM) et de Privileged Access Management (PAM) orchestrent une symphonie complexe d'interactions numériques. Ces outils, devenus indispensables, dépassent la simple gestion des authentifications pour embrasser l'ensemble du cycle de vie des identités numériques. Le Single Sign-On facilite l'expérience utilisateur tout en renforçant la sécurité, illustrant parfaitement l'alliance possible entre confort d'utilisation et protection des données.

La mise en œuvre de ces solutions s'inscrit dans une réflexion stratégique globale, où la gouvernance des identités devient un enjeu majeur. L'acteur de l'antifragilité

endosse alors un rôle de stratège et de facilitateur, créant des ponts entre les différentes composantes de l'organisation. Son expertise technique s'enrichit d'une vision business affûtée, permettant d'aligner les impératifs de sécurité avec les objectifs de croissance de l'entreprise.

Le cadre réglementaire, loin d'être une contrainte, devient un catalyseur d'innovation. RGPD, ISO 27001, directives REC, NIS2 : ces normes constituent autant d'opportunités pour repenser la gestion des identités numériques. En transformant ces exigences en avantages compétitifs, l'acteur de l'antifragilité renforce la confiance des parties prenantes et ouvre de nouvelles perspectives de développement.

L'ÉMERGENCE DE TECHNOLOGIES DISRUPTIVES ENRICHIT CONTINUELLEMENT LA PALETTE DES POSSIBLES

Identité décentralisée, biométrie avancée, intelligence artificielle : ces innovations redessinent les contours de la gestion identitaire. L'enjeu consiste désormais à intégrer ces avancées tout en préservant l'équilibre délicat entre innovation et sécurité, entre agilité et contrôle.

La multiplication des objets connectés complexifie encore davantage cette équation. Chaque nouveau dispositif IoT représente une identité supplémentaire à gérer, élargissant la surface d'attaque potentielle. Face à cette complexité croissante, l'approche antifragile révèle toute sa pertinence. Plutôt que de subir cette complexification, l'organisation apprend à en tirer parti, développant des mécanismes d'adaptation toujours plus sophistiqués.

Les cybermenaces évoluent également, gagnant en sophistication et en intensité géopolitique. Intelligence artificielle malveillante, deepfakes, attaques ciblées : l'arsenal des attaquants s'enrichit constamment, souvent alimenté par des moyens étatiques. Les récentes crises internationales ont démontré que les identités numériques constituent désormais des cibles privilégiées dans les stratégies de déstabilisation. Cette nouvelle donne exige une redéfinition permanente des stratégies de défense, où la protection des identités numériques joue un rôle central dans la préservation de la souveraineté numérique des organisations.

Le "numérique de l'incertitude" se caractérise par une imprévisibilité croissante des menaces et des ruptures technologiques. Les tensions géopolitiques peuvent désormais affecter en quelques heures la disponibilité de services cloud critiques, la fiabilité des chaînes d'approvisionnement technologiques, ou encore l'intégrité des infrastructures numériques.

Dans ce contexte, la gestion des identités des scénarios de crise jusqu'alors considérés probables : rupture d'accès aux services d'au internationaux, compromission massive d numériques, ou encore blackout des infras confiance. La réussite de cette transform largement sur l'évolution de la culture d'e sensibilisation et la formation continues des deviennent cruciales, transformant chaque l'organisation en acteur conscient de la sécurit Cette acculturation collective constitue le t où peut s'épanouir une véritable culture de l'an

L'AGILITÉ ORGANISATIONNE ÉMERGE COMME UNE COMP CLÉ DANS CE NOUVEAU PARADIGME

La capacité à adapter rapidement les proce évoluer les structures et à capitaliser sur d'expérience devient déterminante. En culti système ouvert et collaboratif, l'organisatio pratique et contribue tion collective des s sécurité.

> Les organisations doivent déployer des stratégies toujours plus sophistiquées

Cette approche holistiq tion des identités nume de nouvelles perspec promesses technologic éthiques, les organisa tracer leur voie avec d L'intégration de l'antifrag gouvernance transform en leviers de croissanc d'envisager l'avenir avec

À l'image des systèmes qui se renforcent face aux stress environne entreprises qui sauront cultiver leur antifra maintenant une gestion rigoureuse de le numériques seront les mieux armées po dans ce "numérique de l'incertitude". Cet marque l'émergence d'un nouveau parad protection des identités numériques devier ment un enjeu de sécurité, mais aussi de so de résilience face aux turbulences géopolitic

L'urgence de cette transformation n'a jama criante. Les crises récentes nous rappellent q numérique, loin d'être un espace virtuel déc réalités géopolitiques, en est devenu le mir même le champ de bataille principal. Dans c maîtrise des identités numériques s'impose compétence stratégique, garante de la pér l'autonomie des organisations dans un mon titude est devenue la seule constante. ■

CEFCYS
CErcle des Femmes de la CYberSécurité

Vous êtes expert(e), analyste, consultant(e), RSSI, étudiant(e), personne en reconversion ... Rejoignez la communauté du CEFCYS pour partager vos compétences, développer votre réseau et faire connaitre nos actions dans le monde de la cybersécurité : **contact@cefcys.fr**

Vous voulez soutenir nos actions et faire progresser la présence des femmes en cybersécurité... Rejoignez la communauté du CEFCYS pour partager vos expertises et formations à nos adhérentes, mettre en lumière vos talents féminins ... : **partenariat@cefcys.fr**

PUBLICATION DE LIVRES

Le tome 2 " **Je suis une femme, et je travaille dans la cybersécurité "** Portraits de 65 cyberwomen,
Le tome 3 est en projet pour 2025

JOBDATING

Organisé par le CEFCYS et Cyberjobs : conférences et entretiens avec des entreprises partenaires, mentorat de groupe .
Prochaine date : 7 mars 2025

EUROPEAN CYBER WOMAN DAY

Trophée européen de la femme Cyber

CYBER WOMEN DAY BY CEFCYS

PODCAST

Le CEFCYS a lancé son PODCAST "Les cyberstories racontées par des femmes". Retrouvez les épisodes sur Ausha https://podcast.ausha.co/les-cyberstories-racontees-par-les-femmes

SENSIBILISATION

Sensibilisation des jeunes aux métiers de la cyber ainsi qu'aux risques numériques dans les collèges lycées et écoles

COLLOQUES CEFCYS

Les colloques sont prévus en Octobre en marge du CyberMois. Le dernier avait pour thème : "Comment mieux sensibiliser aux risques cyber ?" au SENAT.

MASTERCLASS et WEBINAIRE

2 sujets par mois liés à la cyber sécurité. Les sujets traités sont d'actualité, proposés par nos partnaires

MENTORAT

Le CEFCYS propose 2 programmes de mentorat : format individuel et format groupé à destination des écoles pour des groupes d'étudiants.

Promouvoir les métiers de la cyber-sécurité auprès des femmes souhaitant accéder, se reconvertir ou partager leur expérience.

https://cefcys.fr/

contact@cefcys.fr

DR. YOSRA BARBIER

Regional Information Security Officer-Europe de l'Ouest Allianz Partners et Secrétaire du CEFCYS, Ph.D

SELON VOUS,

L'IDENTITÉ ET L'ACCÈS numériques en Cybersécurité

GS MAG : *Selon vous, quels sont les enjeux du sujet de l'Identité et de l'Accès numériques en Cybersécurité (employé.e.s ; consommateurs ; fournisseurs ; partenaires ; objets connectés ; etc.) ?*

YB : Au sein du Metavers (monde virtuel) dans lequel nous vivons aujourd'hui, le sujet de l'identité n'a jamais été aussi critique. Avec la croissance des attaques renforcées par l'intelligence artificielle, l'authenticité des comptes, images et vidéos n'a jamais été aussi complexes.

L'accès numérique en cybersécurité est aujourd'hui face à un grand défi : garantir l'authenticité des identités qui existent dans ce monde virtuel. Certes dans un contexte d'entreprises privées ou organismes publiques, nous nous outillons afin de garantir la conformité des accès et des droits numériques par rapport à la classification des données, ce que nous appelons les principes du besoin d'en connaître et du minimum privilège.

Cependant, cela nécessite une cartographie et un référentiel maintenu à jour des rôles et de leurs responsabilités.

GS MAG : *Quelles sont les stratégies et tactiques que vous avez appliquées, les solutions que vous avez mises en place ou que vous conseillez de mettre en place (MFA / Biométrie, IDaaS, Passwordless, contrôle d'accès, Zero Trust, PAM, API, etc.) ? Et pour quelles raisons ?*

YB : Dans un contexte où les services virtualisés sont très interconnectés aujourd'hui, les solutions PAM (Password and Access Management) ont fait leurs preuves surtout pour la sécurisation de l'identification et l'authentification entre applications (API, comptes de services) et entre les webservices. Ça semble simple en parlant d'interconnecter des services virtualisés. Mais cela peut être un casse-tête parfois lorsqu'on pense à durcir les IaC (Infrastructures as Code). Donc, oui les solutions PAMs sont devenues une configuration standard si on veut sécuriser nos environnements clouds et l'administration de nos actifs. Une autre technologie qui s'est marginalisée ces dernières décennies c'est le MFA (Multi-Factor Authentication). Bien que cela soit un moyen de renforcer l'authentification, il n'est plus aujourd'hui une mesure efficace afin de se prémunir du vol d'identité.

>>>

>>> Les attaques comme le hijacking de session ou l'interception des codes OTP via les attaques de SIM Swap ont bien montré la limite du MFA lorsque cela n'est pas bien durcit. C'est pour cela que le Zero trust est essentiel afin de réduire le risque d'exploitation de ces technologies. Rappelant que le Zero Trsut est un concept d'architecture dédié au renforcement de la sécurité d'accès aux ressources et aux services et non pas une technologie en soi*, Donc sa mise en place consiste à élaborer et à planifier toute une feuille de routes (roadmap) de sécurité répondant aux décisions de gestion de risques.

Ces mesures préventives se complètent généralement par des mesures de contrôles et de recertification d'habilitation et des accès ainsi que par des mesures de détection d'utilisation frauduleuses des identités numériques (exp. User Behaviour Analytics) sont nécessaires.

GS MAG : *Quelles évolutions voyez-vous dans ce domaine ? / Une adaptation constante face aux cybermenaces en évolution permanente ? Quid de l'IA et du Quantique ?*

Avec les évolutions des réglementations, de la technologie et des menaces, le sujet de l'identité et l'accès numérique reste central. Cela pousse à adopter des solutions d'authentification avancées comme la biométrie, les systèmes multi-facteurs et les architectures zéro confiance. La détection de fraude et de vol d'identités a déjà été amélioré avec l'intelligence artificielle qui permet une détection en temps réel de toute déviation du comportement légitime de l'utilisation de l'identité.

Une chose est sûre, il doit toujours y avoir une harmonie, une logique et surtout une adaptation au contexte lorsque nous déployons des solutions de sécurité. Avec l'arrivée de l'informatique quantique qui suscite des craintes quant à la vulnérabilité des systèmes actuels de cryptographie, nous allons vivre une accélération ainsi qu'une transition vers des algorithmes post-quantiques et des solutions comme la distribution quantique des clés (QKD).

De plus, des concepts émergents comme l'identité auto-souveraine (SSI), où l'utilisateur contrôle ses propres données via des technologies comme la blockchain, prennent de l'ampleur, tout comme les efforts pour une interopérabilité mondiale.

L'avenir de l'identité numérique repose sur une combinaison de résilience, innovation technologique et protection renforcée des données personnelles, face à des menaces en perpétuelle évolution. ■

garantir l'authenticité des identités qui existent dans ce monde virtuel.

VIDYA JUNGLEEA

Experte IAM et Cheffe de projet ILEX Inetum Software, Vice-Trésorière du CEFCYS

IDENTITY DAYS 2023 :
l'IAM au Cœur des Enjeux Cybersécurité

LORS DE MA CONFÉRENCE DU 24 OCTOBRE POUR LA 5E ÉDITION D'IDENTITY DAYS INTITULÉE "L'IAM : AU-DELÀ DES IDÉES REÇUES, LES CLÉS DE LA GESTION DES IDENTITÉS ET ACCÈS POUR UN PROJET RÉUSSI", J'AI ABORDÉ LES FONDEMENTS ESSENTIELS ET LES ENJEUX STRATÉGIQUES DE LA GESTION DES IDENTITÉS ET DES ACCÈS (IAM)

EN EFFET LES ENJEUX D'UN PROJET IAM SONT :

1_ Sécurité
Savoir qui accède à quoi, renforcer les mécanismes d'authentification (MFA, authentification adaptative), maîtriser l'ouverture et externalisation du SI,

2_ Améliorer l'expérience utilisateur
Faciliter l'accès avec une authentification unique par exemple, uniformiser et améliorer les parcours utilisateurs

3_ Optimiser le ROI
mutualiser les infrastructures d'authentification et d'autorisation et simplifier l'intégration des applications

4_ Standardisation
Répondre aux exigences réglementaires et accompagner la transformation numérique avec des solutions scalables et efficaces.

>>>

>>> Voici les points clés abordés :

IAM ET CYBERSÉCURITÉ

■ **État des Menaces :**

- 61 % des compromissions mondiales impliquent le vol d'identifiants d'après le rapport Verizon (2021,2022) et que 33 % des entreprises sondées rapportent des incidents d'usurpation d'identité (baromètre CESIN 2023).
- Le phishing reste une menace majeure, touchant 74 % des entreprises suivi de l'exploitation des failles (45 %), l'arnaque au président (41%) et tentatives malveillantes de connexions (33%).

■ **Approche Zero Trust :**

- En adoptant une approche Zero Trust, centrée sur les utilisateurs, les actifs et les ressources, IAM revêt un rôle stratégique pour maîtriser les identités et les habilitations afin de protéger le système d'information contre les dysfonctionnements liés au facteur humain, les utilisations frauduleuses, ainsi que la perte ou vol de données.

LES IDÉES REÇUES À COMBATTRE

■ **IAM c'est magique :**

- L'IAM ne se limite pas au déploiement d'une simple solution technique. il nécessite une harmonisation organisationnelle et une définition claire du périmètre projet. Cela nécessite de s'adapter aux contraintes internes, budgétaires et technologiques du marché.
- Un projet IAM mal cadré peut devenir une source de dysfonctionnements et entraîner une obsolescence rapide.

■ **IAM est complexe et coûteux :**

- Bien que transverse et potentiellement perturbateur, un projet IAM bien planifié est un investissement stratégique pour améliorer la sécurité et l'efficacité opérationnelle.

LES PIÈGES À ÉVITER

■ **Sous-estimer la cartographie des ressources :**

- Lors de la conférence, l'importance de recenser les identités, habilitations et référentiels dès le départ a été soulignée. Cela permet de déterminer les sources autoritaires et de centraliser les données critiques.

■ **Données non qualifiées :**

- Négliger le nettoyage préalable des données peut entraîner des incohérences majeures, comme les "comptes orphelins" d'utilisateurs partis.

■ **Personnalisation excessive des profils** :

- Trop de spécificités dans les habilitations peuvent rendre la plateforme coûteuse à maintenir et limiter sa scalabilité.

■ **Négliger la conduite du changement :**

- L'accent a été mis sur la nécessité d'accompagner les utilisateurs pour maximiser l'adoption de la plateforme et surmonter la résistance aux nouvelles habitudes.

LES BONNES PRATIQUES POUR UN PROJET IAM RÉUSSI

■ **Analyse Préliminaire :**

- Une analyse approfondie des besoins et des cas d'utilisation est cruciale pour choisir une solution adaptée et évolutive afin de maitriser les coûts et une planification à long terme.

■ **Implémentation progressive et Quick Win :**

- Une approche progressive et itérative, permettant de générer rapidement des résultats visibles tout en ajustant les étapes suivantes est recommandée. Il est crucial de prendre en compte l'existant et de choisir des solutions capables de s'interfacer avec des fournisseurs de contrôle d'accès, protéger les comptes à privilèges et interagir avec des standards du marché via APIs et web services. Pour déployer la stratégie IAM, il est essentiel de partir d'un socle commun capable d'intégrer toutes les composantes prévues.

■ **Confort Utilisateur :**

- Allier sécurité et ergonomie est essentiel. Une plateforme user-centric favorise une adoption rapide et réduit les erreurs humaines.

■ **Conduite du Changement :**

- La sensibilisation, la communication claire et l'implication des parties prenantes dès le départ sont des facteurs déterminants pour la réussite du projet. ■

mutualiser les infrastructures d'authentification et d'autorisation et simplifier l'intégration des applications

tealenium

```
sudo systemctl
start managed_infrastructure
--ProtectSystem=strict
```

Our People. Your Platform. Managed.
contact@tealenium.com

BENJAMIN LEROUX

Chief Marketing Officer, Advens
Membre du CA du Clusif et membre du CESIN
Former CISO

SELON VOUS,

L'IDENTITÉ ET L'ACCÈS numériques en Cybersécurité

GS MAG : *Selon vous, quels sont les enjeux du sujet de l'Identité et de l'Accès numériques en Cybersécurité (employé.e.s ; consommateurs ; fournisseurs ; partenaires ; objets connectés ; etc.) ?*

BL : La gestion des identités et des accès est un incontournable dans le domaine de la Cybersécurité. C'est même un des chantiers fondamentaux qu'il faut mettre en place, tant il regroupe de nombreuses problématiques (Qui a accès à quoi ? Avec quel niveau de sécurité ? Quelle robustesse pour contrôler ces accès ? etc.) et tant il couvre une part importante des périmètres à protéger (Tous les endpoints, tous les serveurs, toutes les applications, tous les métiers, etc.). C'est aussi un sujet réputé complexe, associé à des projets souvent complexes – et ce, probablement, pour les mêmes raisons !

Par rapport à tout cela, l'IAM nous semble être un bon révélateur du niveau de maturité d'une organisation. Les enjeux vont donc dépendre des enjeux Cyber de l'organisation.

- Votre organisation termine son « move-to-cloud » ? Vous allez devoir dompter les problématiques de sécurisation de l'AD dans le cloud puis vous attaquer à la rationalisation des accès aux différentes solutions SaaS utilisées par les métiers…
- Votre organisation déroule les premières étapes de son plan de sécurisation ? Vous devez vous assurer que le MFA est largement déployé et que les comptes font l'objet de revue régulière…
- Votre organisation a lancé un grand programme Industrie 4.0 ? Vous appliquez les principes de l'IAM à des assets industriels et des objets connectés…

L'IA pourra être utile pour enrichir les solutions de sécurité

GS MAG : *Quelles sont les stratégies et tactiques que vous avez appliquées, les solutions que vous avez mises en place ou que vous conseillez de mettre en place (MFA / Biométrie, IDaaS, Passwordless, contrôle d'accès, Zero Trust, PAM, API, etc.) ? Et pour quelles raisons ?*

BL : Face à tous ces cas de figure, il n'y a pas une seule stratégie… ni une seule solution miracle ! Mais on retrouve des points communs à toutes les situations que nous rencontrons chez nos clients.

Tout d'abord concernant la stratégie : un retour aux fondamentaux est bénéfique. Il faut se rappeler des objectifs visés par un projet IAM. Comme bien souvent, il s'agit de maitriser des risques. Il faut donc se concentrer sur les risques les plus critiques... ou les actions de remédiation les plus « rentables ». L'IAM est un domaine idéal pour illustrer cette approche : ne pas chercher à tout couvrir d'un seul mais y aller par étape, avec une priorité sur les risques forts et/ou des quick-wins pour montrer les avancées.

Pour les solutions et les dispositifs techniques, on retrouve par exemple :

- Le MFA pour l'accès aux suites bureautiques (Office 365, Google Workspace, etc.) et pour de plus en plus d'applications Métier
- Le PAM et les bastions pour renforcer la sécurité des comptes à privilèges mais aussi pour mieux gérer les accès des tiers (fournisseurs, mainteneurs, etc.).
- Le hardening / tiering de l'Active Directory pour protéger ce joyau qu'est l'AD dans un SI (à noter que c'est un sujet qui se décline désormais aussi bien au cloud qu'aux SI on prem)

Enfin, il faut noter que tous ces éléments doivent être intégrés de A à Z dans les démarches de sécurité. Il faut notamment veiller à prendre en compte la dimension « supervision » et intégrer les solutions concernées dans le plan de surveillance du SOC par exemple. De même, il faut intégrer, dans le plan de réponse à incident / plan de reconstruction, les capacités nécessaires à la reconstruction d'un AD en cas d'incident majeur.

GS MAG : *Quelles évolutions voyez-vous dans ce domaine ? / Une adaptation constante face aux cybermenaces en évolution permanente ? Quid de l'IA et du Quantique ?*

LG : Les évolutions sont en effet celles de la Cyber en général. Cependant nous souhaitons mettre en avant trois points d'attention.

Le premier concerne un « vieux classique » du sujet, à savoir le mot de passe. Les récentes évolutions du NIST ont montré qu'il faut changer de posture par rapport aux mots de passe (complexité, taille, fréquence de changement) : il est crucial de savoir se remettre en question… même s'il ne sera pas simple de modifier toutes les politiques de mots de passe disséminées au sein du SI !

Le second point concerne le cadre réglementaire. Tout le monde (ou presque) est au courant : l'année 2025 va être marquée par de nombreux textes de référence, tels que NIS 2, DORA ou encore le Cyber Resilience Act. Ces textes vont couvrir beaucoup de sujets de sécurité. L'identité et les accès seront concernés. Il sera donc crucial d'intégrer les exigences réglementaires dans la trajectoire IAM de votre organisation.

Enfin le dernier point porte sur l'IA - comment l'oublier ? L'IA pourra être utile pour enrichir les solutions de sécurité, par exemple dans la gestion courante de l'IAM comme la revue des accès ou la définition des rôles et des politiques d'accès.

Mais la question que nous souhaitons poser est la suivante : comment faire évoluer l'IAM face à la démocratisation des deep fakes et la difficulté à détecter des images, des voix et des vidéos plus vraies que nature ?...

La gestion des identités et des accès est un incontournable dans le domaine de la Cybersécurité

FRANCIS GRÉGOIRE

Deputy CEO, Memority

L'IA AU SERVICE DE L'IAM : QUELS BÉNÉFICES ?

Dans un contexte d'augmentation de la complexité des environnements et des services numériques, et pour faire face à des cybermenaces de plus en plus sophistiquées, l'usage de l'Intelligence Artificielle s'impose également au sein des solutions de gestion des identités et des accès (IAM). À la clé, des bénéfices d'enrichissement fonctionnel, une meilleure prise en compte des usages, une expérience utilisateur optimisée ou encore une simplification des projets de mise en œuvre. De nombreux acteurs de l'IAM, comme Memority, proposent désormais des fonctionnalités enrichies par l'IA.

VERS UNE DÉTECTION PROACTIVE DES MENACES

Les systèmes d'IAM génèrent et manipulent un nombre croissant de données, dont l'analyse par l'IA permet de détecter et de prévenir les risques liés aux identités. Ceci grâce à deux approches principales : l'analyse comportementale et la détection d'identités vulnérables. Dans le premier cas, il s'agit d'identifier des anomalies comportementales telles que des connexions inhabituelles et des comportements anormaux, qui permettent notamment d'adapter les scenarios d'authentification. Le second axe vise quant à lui à repérer les identités à risque, au regard d'identités comparables et ainsi d'initier automatiquement des actions correctives telles qu'une recertification.

Dans les deux cas, les bénéfices permettent d'améliorer la protection face aux fraudes et aux usurpations d'identités, tout en soutenant les équipes de sécurité.

VERS UNE PRISE EN COMPTE OPTIMISÉE DU CONTEXTE D'ACCÈS AUX APPLICATIONS

Depuis de nombreuses années, les équipes des systèmes d'information et de la sécurité travaillent sur l'application de politiques et de règles statiques qui présentent actuellement leurs limites dans un monde en pleine transformation digitale (accès distants, transformation applicative, transformation des organisations, etc.). Dans ce contexte, l'IA permet une gestion des accès augmentée grâce à l'analyse en temps réel du contexte de connexion (lieu, appareil, historique des connexions, etc.) pour apporter une réponse dynamique en fonction du niveau de risque mesuré. Cette approche prend en compte les paramètres propres à chaque accès en les enrichissant grâce à des sources externes.

Cette contextualisation renforce la sécurité, fluidifie les parcours utilisateurs, tout en s'adaptant constamment aux menaces.

VERS UNE ADMINISTRATION AMÉLIORÉE

Le constat est largement partagé : l'administration des rôles et des droits, et plus largement des identités, atteint un très fort niveau de complexité. Il en va de même pour la gestion des configurations et l'analyse des données à des fins de reporting. L'IA permet une automatisation et une industrialisation par la configuration et la gestion des modèles de droits. Le focus se portera désormais sur les usages, plus que sur la mise en place de règles, tout en simplifiant l'analyse et la création de rapports pour l'ensemble des parties prenantes (applications, métiers, sécurité, IT, conformité, etc.).

Par exemple, un administrateur pourra à terme demander à l'IA d'attribuer à un nouvel employé les mêmes droits qu'un collaborateur existant, tout en excluant les droits inutilisés ou incompatibles. Par ce cas d'usage, on mesure aisément les bénéfices de l'IA en matière de productivité, tout en limitant les erreurs humaines.

VERS DES PROJETS PLUS RAPIDES ET PLUS RICHES FONCTIONNELLEMENT

Face à des projets IAM déjà complexes, il serait peu pertinent que le déploiement de l'IA apporte un lot de complexité supplémentaire ! Les ambitions précédemment évoquées s'en trouveraient décevantes et induiraient la frilosité des organisations à se lancer.

Mais là encore, l'IA est au rendez-vous, au travers des agents IA, qui prennent en charge la configuration des solutions IAM. L'apprentissage des typologies de configurations selon les cas d'usage permet de proposer des accélérateurs, aussi bien pour les configurations des solutions que pour la mise en place des connecteurs de provisioning et de fédération.

Ainsi, les administrateurs et les intégrateurs pourront se concentrer sur des tâches à forte valeur ajoutée, tout en livrant des projets plus rapidement et avec des fonctionnalités enrichies.

LE POINT DE VIGILANCE : TRAÇABILITÉ ET CONFORMITÉ DES SYSTÈMES D'IA

La dynamique de généralisation de l'IA semble aujourd'hui bien engagée et tend à se généraliser. Pour autant, il convient de rester très vigilants pour garantir la sécurité et la conformité. En effet, il est fondamental que les décisions prises par l'IA restent toujours traçables et explicables pour inspirer confiance et permettre une validation ou une revue humaine. De plus, les modèles doivent respecter les cadres réglementaires, tels que le RGPD ou l'AI Act, en s'appuyant sur des données fiables et cloisonnées. ■

CONCLUSION

Il est évident que l'IA marque une véritable révolution pour les solutions et les projets IAM en apportant une réponse aux défis actuels et futurs : détection proactive des menaces, gestion dynamique des accès, automatisation des tâches et accélération des projets.
À l'image de certains éditeurs du secteur, Memority emprunte la voie de l'IA, considérant cette dernière comme un véritable accélérateur au service de la transformation digitale des organisations et de leur protection contre les cyberattaques.

L'IA est une opportunité stratégique que nous saisissons pour enrichir encore la proposition de valeur portée par notre Identity Factory sur des problématiques stratégiques telles que la performance métier, l'expérience utilisateur, la sécurité et la mise en conformité.

ÉCHANGER ET AGIR ENSEMBLE POUR LA CONFIANCE DANS LE NUMÉRIQUE

Le Clusif est l'association de référence de la cybersécurité en France.
Reconnu d'utilité publique par l'Etat, sa mission consiste à favoriser les échanges d'idées et de retours d'expérience. Les membres du Clusif sont issus de tous les secteurs économiques.

REJOIGNEZ-NOUS !

Et contribuez à l'ensemble de nos activités :

Le Panorama de la cybercriminalité
Les conférences
Le podcast
Les publications
Les études sur les pratiques de sécurité
Les exercices de crise et les défis cyber étudiants
Nos nombreuses contributions auprès des métiers hors cyber, des pouvoirs publics

CLUSIF

LOÏC GUÉZO

Vice-Président du Clusif, Senior Director, Cybersecurity Strategy, Proofpoint

SELON VOUS,

L'IDENTITÉ ET L'ACCÈS NUMÉRIQUES EN CYBERSÉCURITÉ

GS MAG : *Selon vous, quels sont les enjeux du sujet de l'Identité et de l'Accès numériques en Cybersécurité (employé.e.s ; consommateurs ; fournisseurs ; partenaires ; objets connectés ; etc.) ?*

LG : Depuis de nombreuses années, les efforts faits autour de la protection, durcissement et maintien en condition opérationnelle et de sécurité des infrastructures auraient dû détourner ces sujets des gros titres des journaux.

Pourtant, les nombreuses brèches d'infrastructure désormais constatées selon le schéma de la publication d'une vulnérabilité d'un fournisseur majeur (comme par exemple ici https://www.lemagit.fr/actualites/366613950/Fortinet-passage-a-la-case-patch-pour-les-utilisateurs-de-FortiManager) ou d'une défaillance systémique d'un fournisseur en SaaS, comme ici Microsoft Teams et Outlook inaccessible, au niveau mondial le 25 novembre https://www.ouest-france.fr/high-tech/microsoft/microsoft-victime-dune-panne-mondiale-outlook-et-teams-touches-3f484462-ab1c-11ef-b615-96f9c0483433, sans oublier une mise à jour catastrophique de Crowdstrike en juillet 2024 ayant provoqué une panne géante https://www.courrierinternational.com/article/technologies-crowdstrike-s-excuse-devant-le-congres-americain-apres-la-panne-geante-de-l-ete_222610 nous rappellent la fragilité de notre monde interconnecté. >>>

une IA qui sait donner du sens aux mails reçus et alerter en cas de suspicion de tentative de fraude financière

>>> Toujours plus numérique, les enjeux autour du sujet de l'Identité et de l'Accès numériques sont désormais essentiels dans notre vie. Les pirates l'ont bien compris : aujourd'hui ils ne piratent plus les infrastructures mais se connectent au système d'information…

A ce titre, l'arrestation de 5 membres du gang Scattered Spider illustrent parfaitement cette mutation. Comme le documentait Le Monde le 21 novembre 2024 https://www.lemonde.fr/pixels/article/2024/11/21/cinq-membres-du-groupe-de-pirates-scattered-spider-arretes_6407020_4408996.html «Ils s'infiltraient en envoyant des messages d'hameçonnage (phishing) ou en usurpant l'identité d'employés au téléphone, toujours dans le but d'obtenir des identifiants permettant de mettre un premier pied dans le réseau…». CQFD

GS MAG : *Quelles sont les stratégies et tactiques que vous avez appliquées, les solutions que vous avez mises en place ou que vous conseillez de mettre en place (MFA / Biométrie, IDaaS, Passwordless, contrôle d'accès, Zero Trust, PAM, API, etc.) ? Et pour quelles raisons ?*

LG : L'Identité est clairement le nouveau périmètre de l'organisation. A ce titre, une Gouvernance complète doit être établie, outillée et suivie avec son cortège de revues de comptes à privilèges, mesures sécuritaires complémentaires quand la personne est « ciblée », accompagnement des profils à risques…

La première mesure technique recommandée est aujourd'hui la mise en place de MFA. Facilement mutualisable pour plusieurs accès, elle renforce considérablement la difficulté pour les attaquants. Attention à ne pas tomber dans l'ignorance de son contournement possible toutefois. Comme pour toute évolution, elle ne tiendra que quelque temps face aux innovations des attaquants voire à des défauts d'implémentation…

Arrêtons de dire que l'Humain est le maillon faible de la chaîne, renforçons le et soutenons le pour en faire le dernier rempart avisé, conscient des enjeux et meilleur collaborateur du RSSI et des équipes opérationnelles quand il reportera un mail suspicieux, prélude à une attaque ciblée…

GS MAG : *Quelles évolutions voyez-vous dans ce domaine ? Une adaptation constante face aux cybermenaces en évolution permanente ? Quid de l'IA et du Quantique ?*

LG : Buzzword de 2024, le potentiel de l'IA est encore devant nous. À court terme, on a pu constater une nouvelle vague de démocratisation rapide et une multiplication des possibilités offertes aux attaquants : génération de texte de mails en toutes langues, sans faute et aux formulations correctes, assistance à la génération de code automatique, voire dernièrement recherche (et identification) d'une 0-day. Dans le même temps, on annonce des capacités automatiques de traitement de données dans les SOC qui libèrent les analystes pour les « vrais » incidents, une IA qui sait donner du sens aux mails reçus et alerter en cas de suspicion de tentative de fraude financière par exemple, une nouvelle vague de capacité de reconnaissance visuelle (type OCR).
Rien de dramatique pour la cybersécurité, une nouvelle accélération !

Pour le quantique, là aussi un monde ancien transitionne avec les publications récentes de mesures de cryptographies post-quantiques (PQC), comme les préconisations de l'ANSSI du 25 novembre 2024 https://cyber.gouv.fr/actualites/lanssi-partage-deux-etudes-de-marche-sur-la-cryptographie-post-quantique-menees-aupres.

Pour mémoire, la PQC est un ensemble d'algorithmes cryptographiques classiques comprenant les établissements de clés et les signatures numériques mais assurant une sécurité conjecturée contre la menace quantique.

Elle représente pour l'ANSSI, et donc pour nous, la voie la plus prometteuse pour se prémunir contre la menace de l'apparition d'un ordinateur quantique.

L'ANSSI a d'ailleurs décidé d'accélérer son agenda initial de 2021, montrant indirectement l'accélération des recherches et applications concrètes.

Toutes les industries doivent inclure la menace quantique dans leur analyse de risque et désormais envisager l'inclusion de mesures de protection spécifiques…

Le buzzword de 2025 ? ■

PATRICK MARACHE

Associate Partner, Cybersecurity & IAM expert, Wavestone

SELON VOUS,

L'IDENTITÉ ET L'ACCÈS NUMÉRIQUES EN CYBERSÉCURITÉ

GS MAG : *Selon vous, quels sont les enjeux du sujet de l'Identité et de l'Accès numériques en Cybersécurité (employé.e.s ; consommateurs ; fournisseurs ; partenaires ; objets connectés ; etc.) ?*

PM : La gestion de l'identité et des accès numériques répond à des enjeux de trois grandes natures : contribuer à réduire le risk Cyber, anticiper et accompagner les initiatives métiers et améliorer l'expérience utilisateur.

Bien sûr, ces enjeux vont se combiner différemment suivant la population qui est couverte. Ainsi, à titre d'exemple, pour les consommateurs, l'IAM vise avant tout à simplifier la mise en relation, à fluidifier le parcours achat quel que soit le point d'accès, à fournir des données permettant de mieux analyser les habitudes pour favoriser l'acte d'achat ou encore à permettre au consommateur d'exercer ses droits liés notamment au RGPD. A contrario, pour les employés, les transformations sont portées par des objectifs d'amélioration de l'efficacité opérationnelle (créer rapidement et de manière automatisée les comptes des utilisateurs, modéliser et regrouper les droits d'accès afin limiter les sollicitations vers les managers…), la maîtrise des risques opérationnels et réglementaires associés aux habilitations accordées (principe du moindre privilège, campagnes régulières de revue des droits…), enfin des mécanismes modernes d'authentification forte (MFA) sont quasi systématiquement déployés, tant pour améliorer la sécurité que pour offrir un accès confortable aux utilisateurs, en particulier lors des mouvements vers toujours plus de Cloud.

GS MAG : *Quelles sont les stratégies et tactiques que vous avez appliquées, les solutions que vous avez mises en place ou que vous conseillez de mettre en place (MFA / Biométrie, IDaaS, Passwordless, contrôle d'accès, Zero Trust, PAM, API, etc.) ? Et pour quelles raisons ?*

PM : Les grandes entreprises s'appuient sur des plans de transformation pluriannuels pour repenser en profondeur leur gestion des Identités et des accès. Cette approche permet à la fois de définir une trajectoire globale vers une cible cohérente et d'identifier des « quick wins » à mettre en œuvre dans les premiers paliers. Ainsi, ce sont généralement les >>>

>>> thématiques autour de l'authentification (MFA), comptes à privilèges (PAM) et la création d'un référentiel unifié des identités qui sont traitées en premier. Sur cette fondation, il est ensuite possible de transformer plus profondément toute la chaîne d'accès en s'appuyant sur des technologies de type Passwordless, Conditionnal Acces Control ou encore ITDR et contribuer ainsi à faire pivoter le modèle de sécurité de nos clients vers des principes ZeroTrust.

En parallèle, il est souvent nécessaire de lancer des initiatives de « reprise en main » des habilitations qui, au fil des évolutions du SI et des réorganisations, souffrent d'un manque de maîtrise. A cette fin, les acteurs du secteur financier, précurseur en matière de cybersécurité, s'appuient majoritairement sur des équipes et des solutions dédiées et orientées « Identity Data Management ». Celles-ci sont construites autour d'un puit de données où sont déversées toutes les données d'identités et d'habilitations et d'un moteur « Analytics & Intelligence » permettant des analyses approfondies des habilitations sans impacter, dans un premier temps, la production.

Nous avons par ailleurs constaté un mouvement généralisé vers des fournisseurs de solutions « IAMaaS » pour l'ensemble des pans fonctionnels de l'IAM.

La prochaine étape sera certainement une approche orientée « plate-forme » regroupant un maximum de services IAM chez un même fournisseur ; toutefois elle ne se concrétise pas encore chez nos clients.

GS MAG : *Quelles évolutions voyez-vous dans ce domaine ? / Une adaptation constante face aux cybermenaces en évolution permanente ? Quid de l'IA et du Quantique ?*

PM : De nombreuses forces (cybermenaces, cadre réglementaire, évolutions SI, évolutions des organisations, évolutions des usages…) s'exercent sur l'IAM. C'est donc un domaine structurellement en forte (r)évolution. Pour les 5 prochaines années, nous identifions trois axes majeurs qui façonneront l'IAM

ÊTRE PLUS EFFICACE ET EFFICIENT

L'IAM est passé d'un sujet « d'experts », avec une visibilité faible dans l'entreprise et morcelée par thématique, à un sujet de premier plan évoqué en Comex a minima DSI. Cela oblige les équipes IAM à s'adapter à de nouvelles exigences d'efficacité, de « valorisation » des apports et des gains, de stratégie à long terme. Les évolutions viseront à mieux piloter l'efficacité de son IAM et la qualité de ses données

contribuer à réduire le risk Cyber, anticiper et accompagner les initiatives métiers et améliorer l'expérience utilisateur

d'identité, à s'engager sur des KPI « métiers » sur des processus de « bout-en-bout », à tirer bénéfice des innovations technologiques comme les wallet ou l'IA. Pour cette dernière, des cas d'usages ont déjà été identifiés par nos clients, avec cependant une limitation : pour les secteurs régulés, les préconisations formulées par l'IA devront être « justifiables » pour être mises en œuvre et éviter le « biais d'acceptation ou de confiance ».

Mais le prérequis majeur à ces évolutions réside dans la refonte de son Operating Model IAM et l'émergence de nouveaux rôles et responsabilité dont celui de « C-Identité-O ».

ANTICIPER LES RISQUES ET CONTRIBUER AUX NOUVEAUX MODÈLES DE SÉCURITÉ ZEROTRUST

De manière globale, les entreprises pivotent progressivement vers le modèle Zero Trust en redéfinissant leur modèle de sécurité des end-points, des zones réseaux, de l'authentification, des données suivants leur criticité… L'identité doit assurer son rôle de « liant fédérateur » entre les différentes évolutions et ainsi asseoir un modèle Zero Trust cohérent.

Etant plus visible, centrale et mutualisée, l'IAM voit son niveau de criticité augmenté tout comme son niveau d'exposition aux menaces externes (risques cyber, incertitudes géopolitiques pouvant conduire à devoir « couper » ou rendre autonomes certains pays pour n'en citer que deux). Ainsi, la résilience des services IAM devient un sujet de premier ordre.

ÊTRE PLUS AGILE POUR S'ADAPTER AUX CHANGEMENTS

Enfin, l'IAM ne sera pas la seule à subir des transformations profondes sur les années à venir : contraintes géopolitiques, acquisitions ou cessions, ouverture élargie du SI à ses partenaires, adoption de technologies de signature et de chiffrement « post-quantum », multicloud, remplacement progressif des systèmes legacy vers des solutions SaaS et en particulier suppression des Active Directory, passage à l'échelle de l'agile… sont autant de changements auxquels l'IAM devra s'adapter en permanence. Et pour ce faire, l'IAM se doit de devenir plus agile, plus ouverte, plus modulaire. ■

Une (cyber) sécurité qui s'adapte à vos défis (numériques)

Parlons de vos projets 2025

↘ Davidson.fr/cybersecurite

CYBERSÉCURITÉ
BY DAVIDSON

Entreprise B Certifiée

L'IDENTITÉ ET L'ACCÈS NUMÉRIQUES EN CYBERSÉCURITÉ

La gestion des identités et des accès (IAM) n'est plus simplement un sujet technique, elle est devenue un levier stratégique incontournable pour les organisations.

Avec plus de 15 ans dans la Cybersécurité, j'ai vu comment les menaces évoluent et comment la gestion des identités devient à la fois une réponse aux défis de cybersécurité et un facilitateur pour les utilisateurs.

> QUELS SONT, SELON VOUS, LES ENJEUX (ORGANISATIONNELS, TECHNIQUES, JURIDIQUES, GÉOPOLITIQUES, AUTRES) DU SUJET DE L'IDENTITÉ ET DE L'ACCÈS NUMÉRIQUES EN GÉNÉRAL ET EN CYBERSÉCURITÉ ?

Les enjeux sont multiples et interdépendants :

- **Organisationnels :**
  Aujourd'hui, il est vital de centraliser et de standardiser la gestion des identités pour des volumes croissants d'utilisateurs (employés, clients, partenaires).
  Mais il faut aussi penser à l'expérience utilisateur : simplifier la sécurité avec des solutions comme le Single Sign-On ou la biométrie tout en assurant une robustesse face aux menaces. Avec la généralisation du télétravail, maintenir cette rigueur est un défi permanent.
- **Techniques**
  Nous devons sans cesse innover pour garantir l'évolutivité des systèmes IAM, intégrer des outils comme la biométrie ou l'authentification sans mot de passe, et utiliser l'intelligence artificielle pour détecter les comportements inhabituels avant qu'ils ne deviennent des incidents.
- **Juridico-réglementaires**
  Les réglementations comme le RGPD et les lois sectorielles imposent une vigilance accrue sur la protection des données personnelles. La souveraineté des données ajoute une couche de complexité que nous ne pouvons pas ignorer.
- **Géopolitiques**
  Les identités numériques sont désormais des cibles dans les cybers conflits. Les entreprises doivent naviguer entre des solutions globales et des approches locales pour protéger leurs ressources stratégiques tout en restant interopérables.

> COMMENT CES ENJEUX INFLUENCENT- ILS VOS PRÉCONISATIONS ET SERVICES CHEZ DAVIDSON CONSULTING ?

Chez Davidson consulting, nous abordons chaque projet avec une vision stratégique et pragmatique, façonnée par le retour d'expérience de nos consultants Cybersécurité. Nous parvenons à combiner l'expertise technique et la compréhension des enjeux métiers de nos clients pour leur offrir des solutions adaptées.

- **Audits et stratégie**
  Nous réalisons des audits IAM complets pour identifier les vulnérabilités et définir des feuilles de route adaptées aux priorités des clients.
- **Solutions sur mesure**
  Nos consultants travaillent avec les solutions leaders du marché, mais nous veillons toujours à les adapter aux besoins réels de chaque organisation.
- **Formation et adoption**
  Une technologie seule ne suffit pas. Nous accompagnons les équipes internes pour assurer une adoption fluide et une maîtrise durable des outils.

> QUELLES SONT LES ÉVOLUTIONS PRÉVUES POUR VOS SERVICES FACE AUX NOUVELLES CYBERMENACES ? QUEL RÔLE JOUE L'IA ET QUEL SERA CELUI DU QUANTIQUE ?

- **Intégration de l'IA**
  L'intelligence artificielle est un axe clé de nos innovations. Elle nous permet de mieux détecter les menaces grâce à des analyses comportementales avancées (UEBA) et d'automatiser les processus critiques au sein des environnements SOC/CSIRT.
- **Anticipation du quantique**
  Nous savons que le calcul quantique redéfinira les règles de la cybersécurité. Nos équipes suivent avec attention ce sujet.

The document highlights the multifaceted challenges of Identity and Access Management (IAM) in cybersecurity, encompassing organizational, technical, legal, and geopolitical aspects.

Davidson consulting emphasizes the strategic importance of IAM, noting the need to centralize and standardize identity management while enhancing user experience and security.

Technically, the firm focuses on innovations like biometrics, password-less authentication, and AI for detecting unusual behavior. Legally, they address data protection regulations and sovereignty issues. Geopolitically, they navigate between global and local solutions to protect strategic resources.

Davidson consulting offers comprehensive IAM audits, customized solutions, and training to ensure smooth adoption of technologies. Looking ahead, they integrate AI for threat detection and automation, and prepare for the impact of quantum computing. Their Cyber Factory serves as an innovation lab for advanced attack simulations and security testing, positioning them at the forefront of cybersecurity trends and future challenges.

- **Cyber Factory**
  Nous avons développé un laboratoire d'innovation où nos consultants peuvent expérimenter des scénarios avancés de simulation d'attaques, tester des solutions de sécurité et se former.

Chez Davidson consulting, nous ne nous contentons pas de suivre les tendances. Nous nous efforçons d'être à l'avant-garde, en adaptant nos services pour protéger les organisations aujourd'hui et anticiper les défis de demain.

DAVIDSON CONSULTING

CONTACTS :
Jean-Michel LAFINE, Practice Leader Cyber
Web : www.davidson.fr
Courriel : jean-michel.lafine@davidson.fr

L'IDENTITÉ ET L'ACCÈS NUMÉRIQUES EN CYBERSÉCURITÉ

> SELON VOUS, QUELS SONT LES ENJEUX (ORGANISATIONNELS, TECHNIQUES, JURIDIQUES, GÉOPOLITIQUES, AUTRES) DU SUJET DE L'IDENTITÉ ET DE L'ACCÈS NUMÉRIQUES EN GÉNÉRAL ET EN CYBERSÉCURITÉ ?

Parmi les multiples défis liés à l'identité et aux accès numériques, Exabeam se concentre particulièrement sur la détection et la gestion des identités compromises, un enjeu crucial pour les organisations. Les attaques basées sur la compromission d'identifiants représentent une part importante des incidents de sécurité, et notre solution se distingue par sa capacité à y répondre efficacement grâce à l'intelligence artificielle (IA) et à l'analyse comportementale avancée (UEBA).

1_ Détection des comportements anormaux grâce à l'UEBA

Exabeam utilise l'User and Entity Behavior Analytics (UEBA) pour analyser en temps réel les comportements des utilisateurs et des entités (appareils, applications, etc.). En établissant une base de référence des comportements normaux, notre solution peut rapidement identifier des écarts significatifs. Par exemple, si un compte utilisateur légitime commence à accéder à des ressources sensibles à des heures inhabituelles ou depuis des localisations atypiques, cela déclenche une alerte pour investigation.

Cette approche comportementale permet de détecter des menaces que les règles de corrélations traditionnelles basées sur des scénarios bien identifiés ou des seuils ne pourraient pas repérer. Elle est particulièrement efficace contre les attaques sophistiquées, comme le phishing ou les mouvements latéraux dans un réseau, où les attaquants utilisent des identifiants valides pour rester sous le radar des solutions classiques.

2_ Machine learning pour une détection proactive

Notre solution intègre des modèles d'apprentissage automatique pour affiner en permanence la compréhension des comportements normaux et améliorer la précision des détections. Ces modèles analysent des millions d'événements, identifiant des schémas qui pourraient indiquer une compromission, sans nécessiter d'intervention manuelle constante. Cela réduit les faux positifs et améliore l'efficacité des analystes en leur permettant de se concentrer sur les véritables menaces.

Par exemple, Exabeam peut détecter des activités telles qu'une escalade des privilèges inhabituelle, des accès à des données généralement non consultées ou des connexions depuis des localisations légitimes mais jamais utilisées précédemment.

3_ Un Forensic centralisée et automatisée

Lorsqu'une activité suspecte est détectée, notre solution crée automatiquement une timeline intelligente qui regroupe tous les événements liés à une menace potentielle ou les actions effectuées d'une même personne. Cela permet aux équipes SOC d'avoir une vision complète, contextualisée par Exabeam et avec analyse de risque associé pour chaque action.

De plus, avec des fonctionnalités d'orchestration et d'automatisation, Exabeam peut initier des actions correctives telles que la désactivation automatique d'un compte compromis ou l'alerte d'une équipe spécifique.

En intégrant Exabeam, les entreprises gagnent en visibilité et en réactivité, tout en allégeant la charge de travail de leurs analystes et en améliorant la maturité globale de leur cybersécurité.

> QUELLES SONT LES ÉVOLUTIONS PRÉVUES DANS LES SOLUTIONS DE VOTRE ENTREPRISE ? UNE ADAPTATION CONSTANTE FACE AUX CYBERMENACES EN ÉVOLUTION PERMANENTE ? QUID DE L'IA ET DU QUANTIQUE ?

Chez Exabeam, l'adaptation continue aux cybermenaces est au cœur de notre stratégie d'innovation. Face à un paysage de menaces de plus en plus complexe et dynamique, nous renforçons constamment nos solutions en intégrant les dernières avancées technologiques, notamment en intelligence artificielle (IA), apprentissage automatique (Machine Learning) et intelligence générative (GenAI).

1_ Des modèles d'apprentissage en constante évolution

Exabeam utilise des modèles de Machine Learning qui apprennent en permanence les comportements normaux des utilisateurs et des entités. Ces modèles évoluent de manière individuelle pour chaque compte et chaque entité, en s'adaptant aux changements normaux dans le temps. Cela permet une détection plus fine des anomalies, même dans des environnements complexes où les habitudes des utilisateurs évoluent régulièrement. Grâce à cette capacité d'adaptation, nos solutions détectent non seulement les attaques traditionnelles, mais aussi les menaces avancées.

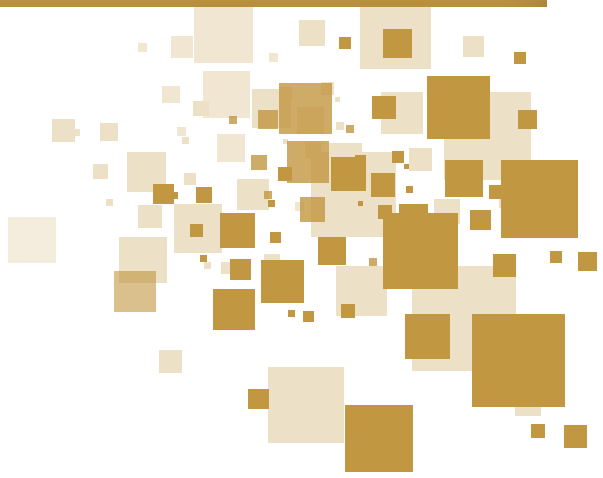
2_ GenAI : simplifier et automatiser le travail des analystes SOC

L'intégration de l'intelligence générative (GenAI) est une avancée majeure dans nos solutions. Nous l'utilisons pour automatiser et simplifier les tâches répétitives ou chronophages des analystes SOC.

The document explores the challenges of digital identity and access management in cybersecurity, highlighting the need to balance security with user experience, manage identities in hybrid environments, comply with regulations, detect compromised identities, and address geopolitical issues.

Exabeam focuses on detecting and managing compromised identities using AI and User and Entity Behavior Analytics (UEBA) to identify abnormal behavior and enhance threat detection.

Exabeam's solutions use machine learning for proactive detection and centralized forensics to provide contextualized risk analysis and automate corrective actions.
The company plans to continuously adapt to evolving cyber threats by integrating advancements in AI, machine learning, and generativeintelligence (GenAI) to improve detection accuracy and automate SOC analyst tasks. This approach aims to enhance visibility, reactivity, and overall cybersecurity maturity for organizations.



exabeam™

CONTACTS :
Matthieu POTIN, Regional Manager France
Courriel : Matthieu.potin@exabeam.com
+33 (0)6 08 01 57 37 • exabeam.com

L'IDENTITÉ ET L'ACCÈS NUMÉRIQUES EN CYBERSÉCURITÉ

> SELON VOUS, QUELS SONT LES ENJEUX (ORGANISATIONNELS, TECHNIQUES, JURIDIQUES, GÉOPOLITIQUES, AUTRES) DU SUJET DE L'IDENTITÉ ET DE L'ACCÈS NUMÉRIQUES EN GÉNÉRAL ET EN CYBERSÉCURITÉ ?

La gestion des identités et des accès s'impose comme un pilier stratégique pour assurer la sécurité, l'efficacité opérationnelle et la conformité réglementaire des entreprises. La complexification croissante des environnements hybrides (multiclouds, on-premises…) et la prolifération des identités – qu'il s'agisse de collaborateurs, prestataires, machines ou services – constituent un défi majeur pour les RSSI. L'impact des solutions de cybersécurité sur l'efficacité opérationnelle des équipes est aussi une priorité dans un contexte économique incertain où les entreprises doivent maintenir leur compétitivité et leur rentabilité. Les investissements en cybersécurité doivent être soutenus par des modèles économiques flexibles (souscription, pay-as-your-go…) afin de permettre aux organisations de piloter leurs stratégie cloud en choisissant le rythme de leur politique de migration SaaS et en maitrisant leur coût.

Enfin, avec les tensions géopolitiques croissantes, l'autonomie numérique et la protection des infrastructures critiques prennent une importance cruciale : il faut assurer la conformité aux exigences de protection des infrastructures et données locales (RGDP, NIS2, DORA…) - qui sont également une condition pour accéder à des couvertures d'assurance permettant de limiter les risques financiers liés aux cyber-attaques - tout en renforçant la résilience des entreprises face aux menaces externes.

> COMMENT CES ENJEUX SONT-ILS PRIS EN COMPTE PAR LES SOLUTIONS PROPOSÉES PAR VOTRE ENTREPRISE ?

WALLIX est un éditeur européen de solution de gestion des accès à privilège (PAM), reconnu comme un leader mondial sur son marché. En tant qu'acteur européen, nous comprenons pleinement les enjeux d'autonomie numérique de nos clients, et nous mettons également à profit notre expertise de sécurisation des identités et des accès, en répondant aux défis spécifiques des environnements OT et industriels. Cette double compétence, unique sur le marché, est régulièrement mise en avant par les cabinets d'analystes, qui considèrent WALLIX comme le seul acteur à intégrer ces deux dimensions dans sa stratégie.

Notre ambition au travers de nos solutions est de simplifier la cybersécurité des identités et des accès interne et externe (collaborateurs et prestataires), afin de mieux piloter son processus de mise en conformité tout en maitrisant l'efficacité des opérations.

Ce portefeuille est disponible On-Premises, en mode hybride ou via la plateforme SaaS WALLIX One, s'adaptant aux différents besoins des organisations qui veulent garder la maitrise de leur stratégie Cloud.

WALLIX One offre tous les bénéfices du SaaS et grâce à un modèle de sécurité « Zero Trust » s'assure que chaque demande d'accès d'une identité est vérifiée systématiquement, sans accorder une confiance implicite à un utilisateur ou entité. WALLIX One crée de manière transparente une première ligne de défense et diminue le risque de violation d'identité impliquant l'utilisation d'identifiants compromis toute en répondant au besoin d'accès rapide aux systèmes de l'entreprise.

Grâce à la simplicité d'utilisation et de mise en œuvre de nos solutions, associée à un TCO (Total Cost of Ownership) optimisé, nous aidons nos clients à renforcer leur efficacité opérationnelle.

L'automatisation des déploiements via l'Infrastructure-as-Code (IaC) permet également d'améliorer l'agilité des équipes techniques, de réduire les erreurs humaines et d'optimiser les ressources pour des opérations plus performantes.

Les solutions WALLIX emmènent donc rapidement nos clients vers une conformité aux réglementations en vigueur dans une maitrise toujours recherchée de simplicité et d'efficacité.

Avec WALLIX, nos clients évoluent librement dans un monde numérique plus sûr.

> QUELLES SONT LES ÉVOLUTIONS PRÉVUES DANS LES SOLUTIONS DE VOTRE ENTREPRISE ? UNE ADAPTATION CONSTANTE FACE AUX CYBERMENACES EN ÉVOLUTION PERMANENTE ? QUID DE L'IA ?

Nous allons proposer une console unifiée pour WALLIX One qui vise à améliorer l'expérience utilisateur (UX) et toujours à réduire le coût total de possession (TCO).

Nous permettrons d'opérer simplement et à distance l'ensemble des solutions de WALLIX, de centraliser et administrer les droits des utilisateurs sur toutes nos solutions tout en déployant et contrôlant la politique de sécurité des entreprises.

Cette console sera pour nos clients le cockpit idéal pour piloter une stratégie Zero-Trust, pour consolider ses tableaux de bords et audits afin de fournir rapidement des preuves de conformité.

Nous travaillons également sur l'analyse comportementale des utilisateurs avec de la détection pilotée par de l'intelligence artificielle. L'intégration d'analyses avancées et d'IA permet d'identifier les anomalies et de détecter les menaces potentielles de manière proactive.

The document discusses the critical role of identity and access management in cybersecurity, highlighting challenges such as hybrid environments, identity proliferation, and geopolitical tensions. WALLIX, a European leader in Privileged Access Management (PAM), addresses these issues by offering solutions that ensure digital autonomy, secure identities, and access, particularly in IoT and industrial settings. Their solutions, available on-premises, hybrid, or via SaaS, use a "Zero Trust" model to verify every access request, enhancing security and operational efficiency.

WALLIX plans to introduce a unified console for WALLIX One to improve user experience and reduce costs, and integrate AI for user behavioral analysis to detect anomalies proactively. Their flagship solutions include Workforce Access for secure and streamlined access, Privileged Access for managing critical IT assets, and Access Governance for overseeing identity authorizations and access certifications. These solutions help organizations comply with regulations, enhance operational efficiency, and navigate the digital world securely.advanced attack simulations and security testing, positioning them at the forefront of cybersecurity trends and future challenges.

CONTACTS :
Edwige Brossard, VP Communication
Julien Cassignol, Chief Product & Technology Officer
Courriel : info@wallix.com

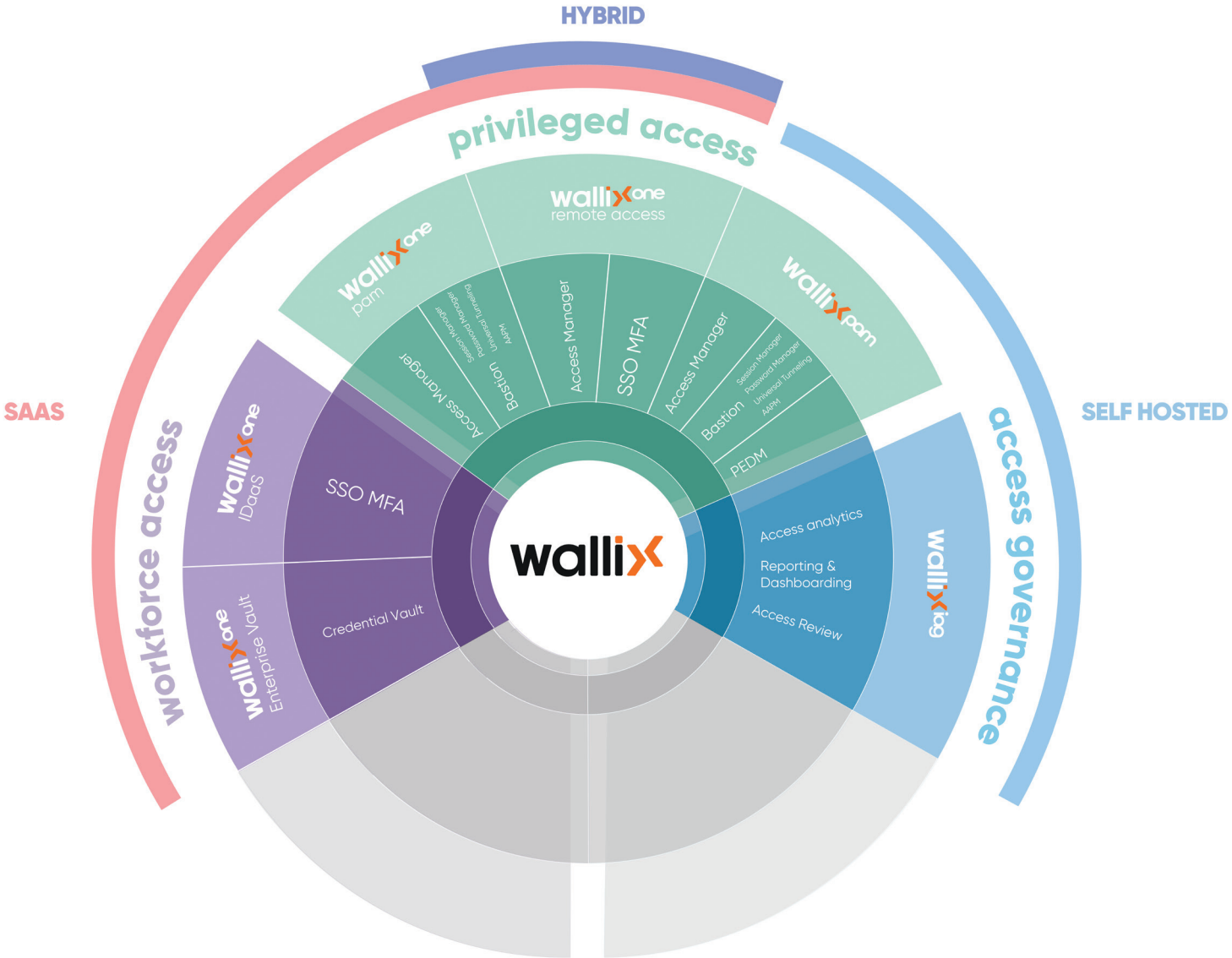
>>>

SOLUTIONS PHARES

>>> WORKFORCE ACCESS
Sécurisation transparente de tous les accès
WALLIX One IDaaS et WALLIX One Enterprise Vault améliorent la sécurité et l'expérience utilisateur en rationalisant l'accès avec SSO et MFA et en centralisant et cryptant les données d'identité sensibles pour un partage sécurisé.

PRIVILEGED ACCESS
Contrôler les comptes à privilèges
WALLIX PAM et WALLIX Remote Access protègent les actifs informatiques critiques en gérant respectivement les comptes à privilèges, souvent cibles de brèches majeures, et en contrôlant l'accès à distance pour maintenir la sécurité tout en permettant une interaction transparente avec des fournisseurs tiers.

ACCESS GOVERNANCE
Examen des accès et contrôle des droits
WALLIX IAG améliore la gouvernance des accès en fournissant une cartographie complète des identités et de leurs autorisations respectives, en agissant comme une tour de contrôle pour superviser les campagnes de certification d'accès et en suivant les changements de personnel dans toutes les applications de l'entreprise.



11ème édition

UNIVERSITÉS D'ÉTÉ

CYBERSÉCURITÉ & CLOUD DE CONFIANCE

9.09.25 **STATION F - PARIS**

EVÉNEMENT ORGANISÉ PAR

HEXATRUST

CLOUD CONFIDENCE & CYBERSECURITY

L'ÉVÉNEMENT DE RENTRÉE DE LA FILIÈRE CYBER & CLOUD DE CONFIANCE

AVEC LE SOUTIEN DE

CAMPUS CYBER

CESIN

Global Security Mag
THE LOGICAL & PHYSICAL SECURITY MAGAZINE

IT for Business

Scannez le QR code pour vous inscrire à la 11e édition des UECC.

IDENTITÉ ET ACCÈS NUMÉRIQUES :

ENJEUX ET RÉPONSES TECHNOLOGIQUES POUR UNE CYBERSÉCURITÉ RENFORCÉE BASÉE SUR UNE OFFRE EUROPÉENNE

L'accélération de la transformation digitale des organisations induit le déploiement de mesures de cybersécurité de plus en plus robustes. Au cœur de ces évolutions, la gestion des identités et des accès (IAM) s'impose comme un axe de développement majeur dans la stratégie globale del'entreprise. Les solutions IAM doivent aujourd'hui être intégrées et capables de sécuriser toutes les typologies d'identités, en s'appuyant sur les besoins métiers, tout en garantissant une expérience fluide pour l'utilisateur.

> QUELS SONT LES ENJEUX ORGANISATIONNELS, TECHNIQUES, JURIDIQUES ET GÉOPOLITIQUES DE L'IDENTITÉ ET DE L'ACCÈS NUMÉRIQUES EN CYBERSÉCURITÉ ?

La protection du patrimoine applicatif et des données est devenue une priorité, encadrée par de nombreuses réglementations telles que le RGPD, NIS2 ou DORA. La gestion des identités et des accès (IAM) joue un rôle essentiel pour assurer la conformité à ces exigences. Ce besoin s'inscrit plus largement dans un contexte géopolitique où une maîtrise rigoureuse des accès au système d'information s'avère indispensable.

Dans ce contexte, les équipes IAM doivent élargir leur champ d'action au-delà de leur rôle traditionnel, souvent perçu comme purement « technique » ou centré sur la cybersécurité. Une collaboration étroite avec les métiers de l'entreprise devient essentielle. Cette (nouvelle) approche stratégique doit être soutenue et encouragée par la direction générale.

Sur le plan technique, rapprocher l'identité et l'accès à travers une plateforme unique permet une approche globalisée et couvrant toutes les typologies d'identités et tous les cas d'usage. Les bénéfices sont nombreux en termes de valeur et de rationalisation de l'architecture.

> COMMENT LA PLATEFORME SAAS MEMORITY RÉPOND-ELLE À CES ENJEUX ?

Memority est une plateforme IAM SaaS permettant de maîtriser la gestion des identités numériques, de protéger les accès aux applications et de renforcer les moyens d'authentification. Dotée d'une forte capacité de configuration, l'Identity Factory Memority permet de rationaliser et d'industrialiser les architectures IAM, en couvrant toutes les typologies d'identités (employés, clients, fournisseurs, partenaires, objets, etc.).

Cette approche Identity Factory 360° permet aux organisations de gérer leurs identités, de maîtriser les accès et de bénéficier d'une visibilité complète sur les usages des utilisateurs, permettant ainsi de détecter rapidement les anomalies et de réagir efficacement aux menaces grâce aux différentes fonctionnalités de l'IAM : IGA, CIAM, SSO, fédération et MFA.

Memority répond à trois enjeux stratégiques majeurs au cœur de la transformation digitale des entreprises :

- L'industrialisation des processus d'identité au service de la performance métier : déploiement plus rapide et sécurisé dans le cadre de la création de nouveaux services à destination des clients, partenaires et fournisseurs.
- Une expérience utilisateur fluidifiée qui ne s'impose plus comme un frein aux usages : accès simplifié vers les applications, self-service intuitif pour la gestion des accès et des moyens d'authentification, etc.
- Le renforcement et l'industrialisation de la sécurité et la conformité, grâce à des circuits de validation (demandes et contrôles d'accès) maîtrisés et adaptés aux profils métiers de l'entreprise.

> QUELLES ÉVOLUTIONS POUR MEMORITY FACE AUX CYBERMENACES ? QUID DE L'IA ?

L'IA nous permettra de prendre en compte l'ensemble des données de la plateforme tout en les enrichissant avec des sources externes telles qu'une CTI pour améliorer les décisions de notre moteur d'authentification, dynamiser la gestion des droits applicatifs ou identifier les droits à risque. Nous avons de nombreux chantiers sur ce sujet et annoncerons prochainement des nouveautés !

The document discusses the importance of Identity and Access Management (IAM) in the context of digital transformation and cybersecurity. As organizations accelerate their digital initiatives, robust cybersecurity measures, including IAM, become crucial. IAM solutions must secure various identities while ensuring a seamless user experience and compliance with regulations like RGPD, NIS2, and DORA.

The Memority SaaS platform addresses these challenges by offering a unified approach to managing digital identities and protecting access to applications. It supports different identity types (employees, customers, suppliers, etc.) and provides functionalities like IGA, CIAM, SSO, federation, and MFA. Memority aims to industrialize identity processes, enhance user experience, and strengthen security and compliance.

Looking ahead, Memority plans to integrate AI to improve authentication decisions, manage application rights, and identify risks. The platform's unified strategy offers an innovative, industrial, and French solution for orchestrating digital identities and controlling access, positioning IAM as a strategic pillar of security and IT within enterprises.

CONCLUSION

Face à l'accélération de la transformation digitale des organisations, à la nécessité de fluidifier les parcours utilisateurs et aux cybermenaces, la gestion des identités et des accès doit être considérée comme un pilier stratégique sécurité, IT et d'entreprise.

La stratégie unifiée proposée par Memority à travers son Identity Factory apporte une réponse industrielle, innovante et française permettant d'orchestrer l'ensemble des identités numériques et de maîtriser leurs accès.

SOLUTIONS PHARES

MY-Identity :
gestion du cycle de vie de l'ensemble des identités (IGA)

MY-Access :
authentification de vos utilisateurs (SSO / Fédération)

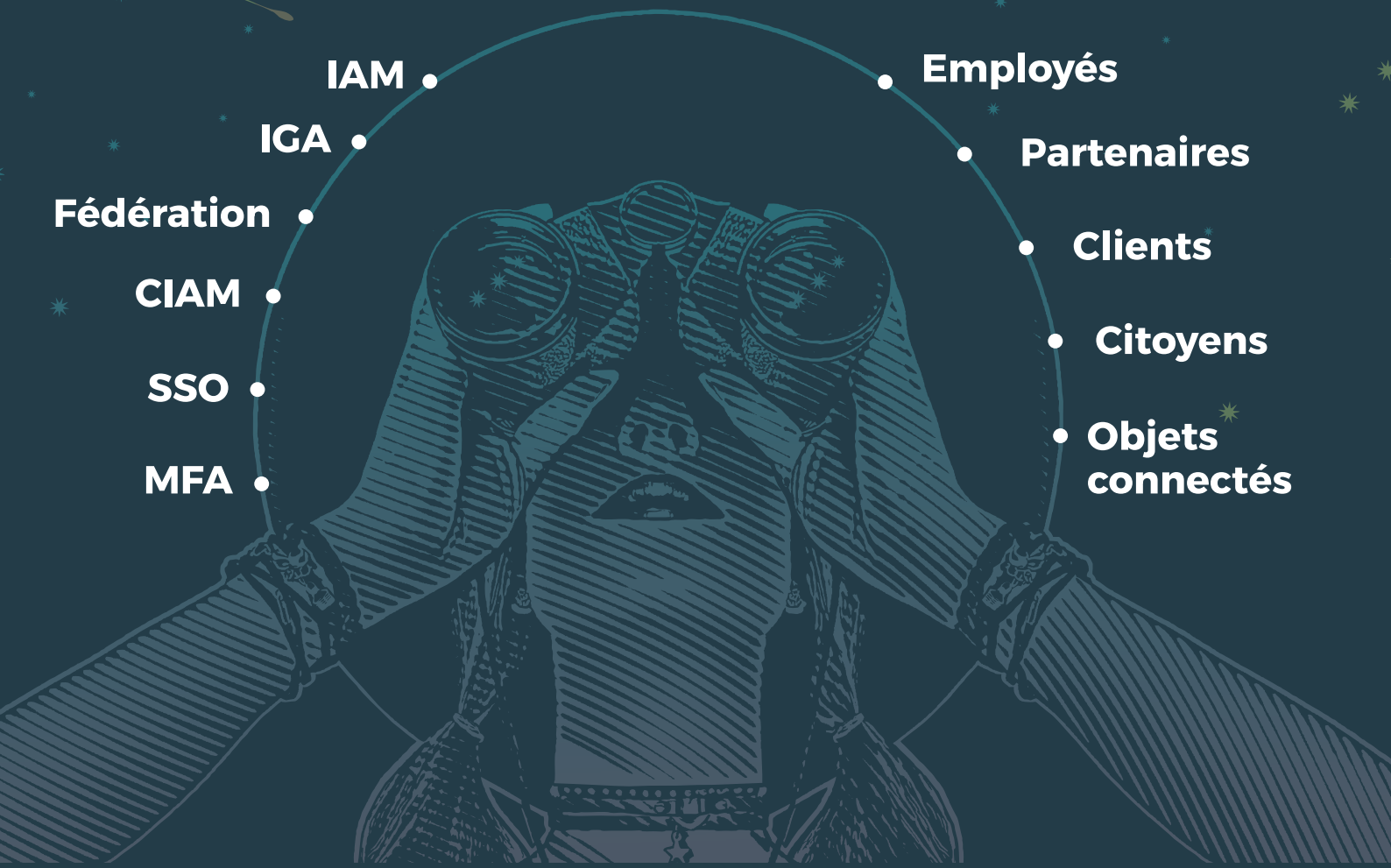
MY-Keys :
gestion des seconds facteurs d'authentification (MFA)

memority

CONTACTS :
Alexis de Calan, VP Sales & Marketing
Courriel : contact@memority.com
Web : www.memority.eu

memority

L'IDaaS européen qui accélère votre business



www.memority.eu

20 | 21 | 22
MAI 2025
MONACO

READY FOR IT!

Le grand saut des ETI
sera au cœur des réflexions
de cette 6ème édition

Rejoignez la communauté & rendez-vous du 20 au 22 mai à Monaco

pour l'événement incontournable des acteurs engagés
dans la transition et la sécurité numériques.

Vous avez des projets d'investissement en cours ou à venir ?

Pour vous inscrire, scannez ce QR code !

Les inscriptions sont ouvertes et soumises à validation

Suivez-nous ! ready-for-it.com | Ready For IT | RFIT_event

COMEXPOSIUM ONE TO ONE

NICOLAS
LIARD

Senior Sales Engineer Exabeam
Hacker Ethique
Membre du Clusif

GESTION DES IDENTITÉS ET DES ACCÈS :

UNE STRATÉGIE ZERO TRUST AU CŒUR DE LA SÉCURITÉ DE LA SUPPLY CHAIN ÉTENDUE À L'INTELLIGENCE ARTIFICIELLE GÉNÉRATIVE.

La gestion des identités et des accès (IAM, pour Identity and Access Management) est devenue un pilier stratégique dans la cybersécurité moderne, où les attaques se multiplient et les environnements informatiques deviennent plus complexes.

Dans un contexte marqué par l'adoption croissante de l'architecture Zero Trust, qui repose sur le principe de « ne jamais faire confiance, toujours vérifier », il est crucial de comprendre l'interaction entre IAM et les principes Zero Trust pour protéger efficacement les chaînes d'approvisionnement numériques.

Avec des capacités de génération de contenu dynamique, d'analyse contextuelle en temps réel et d'automatisation des tâches, l'IA générative transforme les modes de traitement et de gestion des données, mais elle crée aussi de nouvelles menaces et risques en matière de sécurité.

En effet, les vulnérabilités de la supply chain ont été exploitées par des cyberattaques notoires, révélant la nécessité d'une approche holistique de sécurité.

IMPORTANCE D'UNE STRATÉGIE IAM

La gestion des identités et des accès, ou IAM, consiste à établir des règles pour contrôler et surveiller l'accès aux systèmes, aux applications, et aux données sensibles d'une organisation. Une stratégie IAM bien conçue répond à plusieurs impératifs : sécuriser l'accès aux ressources critiques, prévenir les intrusions, respecter les réglementations de conformité, et limiter les menaces internes. Cependant, dans un environnement IT en constante évolution, marquée par la complexité des infrastructures cloud, l'essor du télétravail et la multiplication des utilisateurs externes (fournisseurs, partenaires, clients), les RSSI doivent faire face à des défis multiples pour assurer une gestion des accès efficace et sécurisée.

LES MENACES RELATIVES AUX IDENTITÉS ET AUX ACCÈS

L'augmentation des menaces liées aux identités et aux accès représente un changement de paradigme. Ces menaces se concentrent sur l'exploitation des identifiants et des privilèges pour accéder aux ressources de l'organisation de manière furtive. Parmi les principales menaces liées aux identités et aux accès, on retrouve fréquemment le Vol des informations d'identifications : Le phishing, le « credential stuffing », et d'autres techniques permettent aux attaquants de voler des informations d'identification et de s'introduire dans le réseau sans être détectés mais aussi l'élévation des privilèges qui permet aux attaquants à partir d'un accès initial d'augmenter leurs privilèges pour accéder à des données sensibles ou compromettre des systèmes critiques. Une fois dans le réseau, les attaquants utilisent des techniques de mouvement latéral pour accéder à d'autres systèmes, en exploitant souvent des faiblesses dans la gestion des accès. Des comptes inactifs, la plupart du temps oubliés, peuvent être exploités par les attaquants pour accéder aux ressources sans attirer l'attention. Si l'authentification multi-facteurs renforce la sécurité, elle peut aussi être contournée par des techniques avancées, comme les attaques par interception ou l'exploitation de failles dans les processus d'authentification.

Ces menaces requièrent donc une surveillance constante et une capacité de réponse rapide, et nécessitent une approche adaptée pour détecter les activités suspectes relatives aux identités et aux accès qui sont malheureusement la plupart du temps invisibles pour les organisations.

LES ORGANISATIONS DOIVENT FAIRE FACE À PLUSIEURS DÉFIS SPÉCIFIQUES LORSQU'IL S'AGIT DE DÉTECTER DES MENACES LIÉES AUX IDENTITÉS ET AUX ACCÈS

La gestion des identités et des accès génère un volume considérable de logs d'événements, couvrant les tentatives de connexion, les accès aux ressources, les changements de privilèges, et les activités anormales. Le tri et l'analyse de ces vastes ensembles de données pour identifier les schémas suspects, peut vite devenir une tâche herculéenne, notamment dans les environnements hybrides où les utilisateurs accèdent aux ressources depuis divers points géographiques et plateformes.

Les menaces internes, souvent issues de l'abus d'accès privilégié par des employés ou des sous-traitants, sont parmi les plus difficiles à détecter. Ces menaces peuvent émaner d'employés mécontents, mais aussi de comptes compromis ou mal configurés. En effet, les mouvements d'un utilisateur légitime peuvent souvent ressembler à ceux d'un utilisateur malveillant. Cette ambiguïté dans l'analyse des comportements rend la détection des activités suspectes complexe.

Les outils de sécurité traditionnels, souvent centrés sur la détection des menaces réseau et des logiciels malveillants, sont parfois mal adaptés pour surveiller les activités relatives aux identités et aux accès. Avec l'adoption croissante des environnements multicloud et hybrides, les identités des utilisateurs, qu'il s'agisse de collaborateurs ou de partenaires, se retrouvent réparties sur plusieurs plateformes.

Ce morcellement rend difficile la création d'une vue unifiée des identités et des accès. Cette complexité d'intégration et de gestion des identités multiplie les points de vulnérabilité et complique la surveillance et la corrélation des événements de sécurité.

Les cybermenaces évoluent rapidement et les centres de sécurités opérationnels (SOC) peinent souvent à disposer d'analystes ayant les compétences nécessaires pour identifier les menaces sophistiquées et comprendre les vulnérabilités liées aux identités et aux accès. La formation continue et l'acquisition de compétences spécifiques à la gestion des identités deviennent donc une priorité pour renforcer les capacités de détection.

>>>

>>> NOUVEAUX ENJEUX ET RISQUES SPÉCIFIQUES LIÉS À L'INTELLIGENCE ARTIFICIELLE GÉNÉRATIVE

L'intégration de l'Intelligence Artificielle générative pose des enjeux uniques en matière de gestion des identités et des accès (IAM), surtout lorsqu'elle implique des services externes. Avec des capacités de génération de contenu dynamique, d'analyse contextuelle en temps réel et d'automatisation des tâches, l'IA générative transforme les modes de traitement et de gestion des données, mais elle crée aussi de nouvelles menaces et risques en matière de sécurité.

Les solutions d'IA générative, pour fonctionner efficacement, requièrent souvent l'accès à de vastes ensembles de données, y compris des informations personnelles ou sensibles. Par exemple, des modèles génératifs peuvent être utilisés pour créer des réponses dynamiques basées sur l'historique des interactions utilisateurs ou des données de contexte opérationnel. Cependant, cette exigence d'accès aux données élargit considérablement la surface d'exposition des données,

Les modèles génératifs eux-mêmes, qu'ils soient internes ou fournis par des services externes, nécessitent une gestion rigoureuse des privilèges d'accès. Ces modèles sont la plupart du temps accessibles via des API, qui sont susceptibles d'être appelées par plusieurs services, qu'ils soient internes ou externes. Cela expose les entreprises à des risques accrus de compromission.

Les services d'IA générative peuvent également être utilisés à des fins d'ingénierie sociale automatisée si un accès non autorisé est obtenu, par exemple en générant des réponses ou en imitant des comportements humains pour compromettre la sécurité des comptes. La capacité de l'IA générative à imiter le langage humain augmente les risques d'usurpation d'identité et d'attaques sophistiquées visant à tromper les utilisateurs ou autres systèmes d'authentification.

En cas de compromission d'un service externe, les modèles génératifs pourraient être utilisés de manière abusive, ou les jetons d'accès aux services pourraient être volés, donnant accès à des fonctions critiques ou à des données sensibles. Par ailleurs, le fait de s'appuyer sur des services externes pose des problèmes de visibilité : les entreprises n'ont souvent qu'un contrôle limité sur les processus internes de sécurité des fournisseurs d'IA, ce qui peut entraver la conformité et accroître les risques de fuite de données.

L'APPROCHE ZERO TRUST, UN NOUVEAU PARADIGME DE SÉCURITÉ

L'approche Zero Trust remet en question le modèle de sécurité périmétrique traditionnel, qui suppose que tout ce qui est à l'intérieur du réseau est sûr, tandis que tout ce qui est extérieur ne l'est pas. Avec le Zero Trust, chaque entité – qu'il s'agisse d'un utilisateur, d'un appareil ou d'une application – est soumise à une vérification systématique, et l'accès aux ressources n'est jamais accordé par défaut.

Le modèle Zero Trust repose sur plusieurs principes :

1_ **Vérification explicite :** Authentification continue des utilisateurs et des appareils, même pour les sessions internes.
2_ **Moindre privilège :** Limiter l'accès aux ressources uniquement aux droits strictement nécessaires.
3_ **Micro-segmentation :** Découper le réseau en segments plus petits, limitant ainsi les possibilités de déplacement latéral en cas de compromission.

Les solutions Zero Trust offrent une protection accrue contre les attaques de la supply chain, où les tiers peuvent devenir des vecteurs d'attaque. La gestion des identités et des accès dans un modèle Zero Trust est une réponse stratégique pour sécuriser la supply chain.

MISE EN ŒUVRE DE L'IAM ZERO TRUST POUR LA SUPPLY CHAIN

Bien que le concept de Zero Trust soit relativement simple, sa mise en œuvre dans le cadre de la supply chain peut être complexe.

La première étape consiste à identifier les acteurs qui interagissent avec les systèmes de l'entreprise et à évaluer les risques associés. Une cartographie des relations et des dépendances est essentielle pour comprendre où des contrôles d'accès doivent être renforcés. Dans un modèle Zero Trust, chaque fournisseur ou partenaire est traité comme une entité à risque. Les accès sont accordés de manière conditionnelle et temporaire, et sont surveillés en temps réel. L'application stricte du principe de moindre privilège dans la supply chain est essentielle. Par exemple, une autorisation pour un fournisseur peut être limitée à un ensemble précis de données ou de systèmes, avec une révision périodique des droits accordés. L'implémentation de cette approche réduit la probabilité qu'un acteur externe puisse accéder à des informations sensibles en dehors de son périmètre de responsabilité.

Avec le Zero Trust, chaque entité – qu'il s'agisse d'un utilisateur, d'un appareil ou d'une application – est soumise à une vérification systématique, et l'accès aux ressources n'est jamais accordé par défaut

L'authentification adaptative, qui ajuste les contrôles en fonction du contexte de connexion, renforce cette vérification continue. Un utilisateur se connectant depuis un appareil non reconnu ou un pays étranger pourrait être amené à fournir une authentification supplémentaire. L'authentification multi-facteurs est un élément fondamental du Zero Trust. En exigeant une authentification forte pour chaque accès, les entreprises peuvent réduire considérablement le risque de compromission de compte.

Les attaques évoluent rapidement, et il est indispensable que les systèmes IAM soient en mesure de détecter et de répondre à des anomalies de manière proactive. L'intégration d'outils de détection des menaces basés sur l'IA peut renforcer les capacités de réponse. L'analyse comportementale basés sur des modèles d'IA prédictifs permet d'identifier des activités anormales, telles que des connexions inhabituelles ou des tentatives répétées d'élévation de privilèges, qui pourrait indiquer un compte compromis détecter des comportements anormaux, comme des tentatives d'accès répétées depuis des localisations inhabituelles ou des demandes d'accès à des ressources non autorisées. Dans une chaine d'approvisionnement complexe, où des milliers de connexions sont établies chaque jour, l'analyse comportementale permet de répondre en temps réel à des incidents potentiels avant qu'ils ne se transforment en brèches de sécurité. L'un des plus grands défis pour les équipes de cybersécurité est de réagir rapidement aux incidents et de maintenir une vue d'ensemble des événements liés aux identités et aux accès. Les solutions de SIEM (Security Information & Event Management) augmentées et SOAR (Security Orchestration Automation & Response) permettent d'automatiser la réponse aux incdients de sécurité.

La sécurisation de la supply chain dépend également de la collaboration avec les partenaires et les fournisseurs. Il est donc crucial de s'assurer que chaque acteur de la chaîne comprend et applique les principes de sécurité établis, notamment en matière d'authentification et de gestion des identités.

ÉTENDRE L'IAM ZERO TRUST À INTELLIGENCE ARTIFICIELLE GÉNÉRATIVE

L'authentification Zero Trust doit être appliquée à chaque interaction avec les services d'IA générative, qu'ils soient internes ou externes. En adoptant une approche Zero Trust, chaque microservice doit prouver son identité et être authentifié pour chaque appel API, réduisant ainsi la dépendance excessive à la confiance implicite entre les services. Les politiques d'accès peuvent être configurées de manière à ce que seuls certains microservices spécifiques aient des permissions pour interagir avec des modèles génératifs, en fonction de leur besoin exact. Le Zero Trust peut être renforcé par l'utilisation de jetons d'authentification de courte durée, qui limitent le risque de compromission d'accès prolongé. De plus, des audits de jetons doivent être effectués en temps réel pour garantir que seules les entités approuvées accèdent aux modèles génératifs.

Les contrôles d'accès basés sur des rôles (RBAC) et le principe du moindre privilège sont cruciaux pour limiter l'accès aux modèles d'IA générative. Cette approche limite les risques d'abus des privilèges et réduit la surface d'attaque en cas de compromission d'un service externe. La mise en œuvre du moindre privilège peut également inclure l'utilisation de mécanismes de segmentation

>>>

>>> réseau et de conteneurs pour séparer les différents microservices et services d'IA générative, limitant ainsi la propagation des menaces.

La surveillance des comportements d'accès aux modèles IA est essentielle pour détecter les utilisations suspectes ou anormales. L'UEBA (User & Entity Behavior Analytics) permet d'identifier des comportements inhabituels, tels que des accès excessifs, des tentatives de récupération massive de données, ou des interactions répétées depuis des services externes en dehors des plages normales d'utilisation.

Pour minimiser les risques de compromission, les jetons d'accès utilisés pour interagir avec les services d'IA générative doivent être gérés selon des protocoles rigoureux. Des jetons de courte durée et leur rotation fréquente limitent le risque d'utilisation prolongée en cas de compromission. Les audits de sécurité réguliers permettent de vérifier que tous les accès aux services IA, surtout ceux fournis par des tiers, respectent les politiques de sécurité et de conformité.

Enfin, les entreprises doivent établir des accords de niveau de service (SLA) et des normes de sécurité avec les fournisseurs de services d'IA générative pour garantir une protection adéquate des données. Ces normes doivent inclure des clauses spécifiques sur la confidentialité des données, la rétention des informations, et la sécurité des infrastructures des fournisseurs.

Les entreprises peuvent également envisager des audits ou certifications externes des services d'IA pour s'assurer que les pratiques de sécurité et de gestion des accès des fournisseurs sont conformes aux standards requis. ■

Il est crucial de comprendre l'interaction entre IAM et les principes Zero Trust pour protéger efficacement les chaînes d'approvisionnement numériques.

CONCLUSION

Dans le contexte actuel de cybermenaces sophistiquées et de chaînes d'approvisionnement interdépendantes, la gestion des identités et des accès associés au modèle Zero Trust se révèle être un outil essentiel pour protéger l'écosystème de l'entreprise.
En mettant en place des politiques d'accès rigoureuses et des vérifications constantes, les entreprises peuvent limiter l'impact des vulnérabilités liées à leurs partenaires et sous-traitants. Une approche IAM Zero Trust permet non seulement de réduire les risques de compromission mais également de renforcer la résilience globale de la supply chain face aux attaques.

Les solutions d'IA générative présentent des avantages notables en matière d'innovation, mais ajoutent des complexités et des risques uniques en matière de gestion des identités et des accès. Les entreprises doivent adopter une stratégie de sécurité axée sur le Zero Trust, des contrôles d'accès basés sur le contexte, et des solutions avancées de surveillance pour protéger efficacement les modèles et les données.

À l'heure où les cyberattaques deviennent de plus en plus ciblées et avancées, IAM et Zero Trust offrent aux entreprises une méthode proactive et stratégique pour protéger leur supply chain.

Édition Lextenso

AMÉLIE KÖCKE

Édition Lextenso

MYRIAM QUÉMÉNER

LIVRE CYBER : HACKER « ÉTHIQUE » ET CYBERSÉCURITÉ / OPPORTUNITÉS ET DÉFIS

■■ GS MAG : *Quel est le contexte et Quels sont les enjeux de votre livre ?*

■■ MQ/AK : Ce livre a comme point de départ une belle rencontre avec Amélie Köcke qui m'a demandé de diriger son mémoire sur le régime juridique des hackers éthiques ; j'ai trouvé le sujet pertinent et original ; on devait faire un article ensemble puis Les éditions Lextenso on proposer que nous fassions un ouvrage. À l'heure où les cyberattaques explosent, il nous est paru intéressant de présenter ces lanceurs d'alerte de cybersécurité encore méconnus qui à la fois fascinent et inquiètent tant la frontière entre hackers black hats et white hats peut être parfois tenue.

■■ GS MAG : *En quoi votre livre peut-il aider les RSSI (Responsables de la Sécurité des Systèmes d'Information) et CISOs (Chief Security Officers) ?*

■■ PM :

Les RSSI et les CISOs ont besoin de connaître tous les acteurs qui contribuent à renforcer la cybersécurité dans un écosystème de plus en plus fragilisé où les cybercriminels s'en donne à cœur joie et ce d'autant que nous sommes désormais dans un contexte de crise économique et géopolitique troublé. Cet ouvrage a pour objectif de mieux appréhender les cadres juridiques nécessaires pour faire intervenir des hackers, comme par exemple les contrats ou les bug bounty afin de sécuriser à la fois les entreprises qui y ont recours et les hackers éthiques eux- même.

■■ GS MAG : *Quels sont vos messages pour nos lectrices et lecteurs ?*

■■ PM :

Le message de cet ouvrage est de définir en fait une doctrine de cybersécurité pour le recours aux hackers éthiques. En effet, certaines plateformes de bug Bounty ont conscience que les hackers éthiques ne sont pas assez connus et peuvent faire peur aux entreprises et c'est la raison pour laquelle que les termes de chercheur ou de « hunter » sont encore davantage employés que celui de hacker éthique qui est désormais un vétitable métier de cybersécurité, à la condition de démontrer à la fois compétences et déontologie. ■

GOUVERNEMENT
Liberté
Égalité
Fraternité

17 CYBER
Mon assistance en ligne

Un service proposé par

POLICE NATIONALE
Gendarmerie nationale
CYBER MALVEILLANCE .GOUV.FR

JADE
LE VAN

Principal Sales Engineer, Snowflake

SELON VOUS,

L'IDENTITÉ ET L'ACCÈS NUMÉRIQUES EN CYBERSÉCURITÉ

GS MAG : *Quels sont les enjeux des concepts Datalake / Lakehouse ?*

JLV : Premièrement, un data lake est conçu pour stocker de gros volumes de données brutes dans leur format natif, qu'elles soient structurées, semi-structurées ou non structurées. L'entreprise centralise toutes ces données dans le data lake avant de décider quels besoins ces données vont venir servir. Du fait de la variété des formats récupérés, le data lake est souvent le terrain de jeu des data engineers, qui doivent reprendre la donnée pour la transformer et la rendre consommable dans d'autres outils, ainsi que des data scientists, qui utilisent ces données brutes pour entraîner et alimenter leurs modèles.

Un lakehouse, quant à lui, est à la croisée des mondes entre la centralisation de toutes les données de l'entreprise, quel que soit leur format, et la capacité de faire de l'analytique à grande échelle sur de la donnée structurée.

Il existe deux approches principales pour répondre aux besoins de performance analytique tout en gérant des données moins structurées :

- Adopter une plateforme de données performante et flexible qui permet de traiter efficacement tous types de données, qu'elles soient structurées ou non.
- Utiliser des formats de table ouverts comme Apache Iceberg, Delta Lake ou Apache Hudi, qui ajoutent des métadonnées aux fichiers qui composent une table. Ces métadonnées donnent des indications sur le contenu de chaque colonne et accélèrent ainsi les requêtes analytiques.

GS MAG : *En quoi les concepts Datalake / Lakehouse concernent les RSSI / CISOs ?*

JLV : Dans un data lake, de nombreux utilisateurs tels que les data engineers, les data scientists ou encore les data analysts accèdent à des données pour différents cas d'usage. Il est essentiel de s'assurer que chacun n'ait accès qu'aux données du périmètre sur lequel il travaille, et que ces accès soient logués et auditables en cas de soupçon d'accès frauduleux. Des mécanismes d'alertes en temps réel doivent donc être mis en place pour détecter les comportements inhabituels, comme l'extraction massive de données.

La gestion de la gouvernance et de la conformité est complexe en raison de la diversité des données et des réglementations applicables, comme par exemple la réglementation DORA pour les entités opérant en lien avec les marchés financiers.

>>>

>>> Pour donner un exemple concret de cas d'usage incluant des enjeux de sécurité, notre client Siemens Energy, leader mondial des technologies de l'énergie, a mis au point un chatbot d'IA pour questionner et résumer rapidement plus d'un demi-million de pages de documents de R&D internes. Ce projet a permis à l'entreprise d'aider ses équipes de recherche et développement à trouver plus rapidement les informations et accélérer les délais de commercialisation de nouvelles offres.

Siemens Energy a conçu ce chatbot sur des données présentes dans son Data Lake en utilisant les services d'IA Générative packagés de Snowflake. C'est parce que les services utilisés tournent dans le périmètre de sécurité de leur compte Snowflake que les équipes R&D ont pu avancer si vite sur ce projet d'envergure.

GS MAG : *Comment vos solutions interviennent-elles dans ces domaines Datalake / Lakehouse ?*

JLV : Depuis sa création, Snowflake vise à réduire les silos techniques et fonctionnels des entreprises en permettant de stocker et traiter de très gros volumes de données structurées, semi-structurées et non structurées avec une gouvernance et une sécurité optimales.

Pour répondre aux besoins des entreprises souhaitant gérer leurs données dans un environnement ouvert et interopérable, chez Snowflake nous intégrons pleinement le format open source Apache Iceberg. Cette approche permet aux utilisateurs de tirer parti de l'écosystème open source, tout en bénéficiant de la gouvernance, de la simplicité d'administration et de la performance propres à Snowflake.

Pour faciliter la mise en œuvre de l'interopérabilité, nous proposons aussi un catalogue ouvert basé sur le projet Apache Polaris. Il permet à différents moteurs de calcul d'accéder à la donnée stockée au format ouvert Apache Iceberg en appliquant une gouvernance unifiée pour tous les moteurs.

En résumé, Snowflake permet de construire un socle de données gouverné et sécurisé pour activer l'ensemble des données de l'entreprise, en respectant les choix d'architectures propres à chaque organisation. ■

Des mécanismes d'alertes en temps réel doivent donc être mis en place pour détecter les comportements inhabituels, comme l'extraction massive de données

CHRISTOPHE MENANT

Director, Cyber Security offering & Innovation lead, Capgemini France

SELON VOUS,

L'IDENTITÉ ET L'ACCÈS NUMÉRIQUES EN CYBERSÉCURITÉ

GS MAG : *Quels sont les enjeux des concepts Datalake / Lakehouse ?*

CMC : Les enjeux de cybersécurité liés aux Datalakes et Lakehouses -et auparavant aux Data Warehouses- sont nombreux et touchent à tous les aspects de la sécurité. Ces concepts s'articulent autour de l'exploitation de données, qu'elles soient structurées ou non, à des fins de business intelligence, de machine learning et plus récemment d'intelligence artificielle générative. La sécurité à appliquer varie selon la nature des données stockées, qu'elles soient sensibles, confidentielles ou soumises à des réglementations spécifiques. Elle dépend également de la finalité des traitements, notamment de l'usage des résultats et de leur impact potentiel. Tous les domaines de la sécurité sont concernés et nécessitent une approche adaptée, allant de la gestion des risques à des mesures de protection spécifiques selon les particularités de chaque usage.

GS MAG : *En quoi les concepts Datalake / Lakehouse concernent les RSSI / CISOs ?*

CMC : Les Datalakes et Lakehouses sont conçus pour stocker des données et les traiter dans le cadre d'activités métiers. Selon la nature des données, il est impératif de les sécuriser afin de prévenir toute « exposition », qu'il s'agisse d'exfiltration, de fuite ou de manipulation pouvant altérer les traitements effectués. Une telle exposition peut entraîner des risques majeurs pour l'organisation, comme des sanctions réglementaires liées au RGPD en cas de fuite de données personnelles ou des menaces d'espionnage industriel visant des informations confidentielles, des projets de recherche ou d'autres données stratégiques. À cela s'ajoutent des menaces comme les attaques de type ransomware, qui peuvent gravement perturber les activités. Ces risques peuvent avoir des répercussions multiples sur l'organisation, allant de pénalités réglementaires à une atteinte à l'image de marque, une perte de parts de marché, et dans les cas les plus critiques, la destruction ou l'indisponibilité des données et des infrastructures Lakehouses. Ces situations engendrent des coûts importants, notamment ceux liés à la restauration, à la remise en service et à la perte de productivité. Une gestion rigoureuse de la sécurité des Datalakes et Lakehouses est donc indispensable pour minimiser ces risques et protéger les actifs stratégiques des organisations.

GS MAG : *Comment vos solutions interviennent-elles dans ces domaines Datalake / Lakehouse ?*

CMC : Capgemini traite les questions de sécurité dans ces domaines en adoptant une approche complète et structurée. En tenant compte de l'architecture, elle commence par une analyse des risques permettant de définir la nature des données et des cas d'usage liés au traitement des informations, le niveau de sécurité nécessaire et les priorités à mettre en place. Nous accompagnons également nos clients dans la mise en œuvre des exigences de sécurité identifiées, en couvrant de multiples domaines. Une fois ces mesures en place, nous prenons en charge l'exploitation des solutions de sécurité associées, tout en garantissant leur maintien en conditions opérationnelles. Enfin, Capgemini propose des services de surveillance continue pour sécuriser les environnements Datalake et Lakehouse, ainsi que des services de réponse et de traitement des incidents de sécurité disponibles 24 heures sur 24 et 7 jours sur 7. ■

OLIVIER ITEANU

Avocat et chargé d'enseignement à l'Université Paris I Sorbonne

AVAIT-ON BESOIN DE LA DIRECTIVE NIS2?

La Directive NIS2 du 14 Décembre 2022 sera sans nul doute l'évènement de cette année 2025 qui s'engage. Ce texte annonce dans son titre, son programme : « Directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union Européenne ». De prime abord, ce programme est tout à fait louable.
Mais avait-on besoin d'un tel texte de surcroît complexe, composé de 144 considérants, de 46 articles et de 3 annexes, pour un tel objectif ? Plus encore, avait-on besoin d'un texte communautaire de plus ? D'autant que cette Directive prend place aux côtés de deux autres textes communautaires à même date du 14 Décembre 2022 : il s'agit du Règlement DORA et de la Directive sur la résilience des entités critiques.

UNE DIRECTIVE TRÈS AMBITIEUSE

La Directive NIS2 est avant tout un texte de Loi très ambitieux pour le secteur de la cybersécurité. Il s'applique très clairement aux entreprises et crée à cet effet, deux nouveaux « acteurs juridiques », nommés « entités essentielles » et « entités importantes » soumises à la Directive. Les entreprises devront dès lors s'auto-qualifier dans un premier temps comme étant l'une l'autre de ces entités ou aucune des deux. Dans le dernier cas, elles ne seront pas contraintes d'appliquer NIS2. Pour déterminer si elles rejoignent l'une ou l'autre de ces trois catégories, la Directive donne aux entreprises 4 critères cumulatifs à remplir. Si l'un de ces critères manque, l'entreprise n'est donc pas concernée directement par le texte et les obligations qu'il contient. Les deux premiers critères sont d'ordre géographique. On peut les résumer en une proposition : les entreprises concernées sont celles qui sont établies dans l'Union européenne et qui fournissent des services au sein de l'Union. Le critère 3 est un critère d'activité. Pour être entité essentielle, il convient de développer une activité dans l'un des 18 secteurs d'activité listés à l'Annexe 1. Pour être entité importante, il faut figurer dans l'un des 7 secteurs d'activités énoncés à l'annexe 2. Enfin, le critère 4 est d'ordre quantitatif. L'entité doit occuper au moins 50 salariés ou réaliser un chiffre d'affaires annuel de plus de 10 millions d'euros ou son bilan comptable annuel s'élève à 43 millions d'euros

ou plus. Le texte précise cependant que les autorités conserveront la faculté de désigner telle entreprise, par exemple une Très Petite Entreprise qui ne remplit pas le critère 4, comme entité soumise à la Loi, en raison de son activité et de la fourniture particulière de tels produits ou de tels services, qui justifie qu'elle soit régulée par l'autorité de contrôle instituée par NIS2. Sur le plan du fond, il sera exigé de ces entités de prendre « les mesures techniques opérationnelles et organisationnelles appropriées et proportionnées » (article 21) pour gérer les risques qui menacent la sécurité. Les connaisseurs du RGPD y retrouveront quelques éléments de langage de ce règlement et de son article 32. Devant la généralité des termes, le rôle de l'ANSSI sera essentiel car seule cette autorité pourra caractériser en pratique de tels termes généraux. Pour cela, on peut penser qu'elle se réfèrera aux certifications les plus connues et répandues y compris son propre référentiel SecNum Cloud au moyen duquel l'ANSSI qualifie des fournisseurs de cloud computing. Enfin, pour être complet, la Directive NIS2 prévoit des sanctions administratives, amendes de 7 ou 10 millions euros et 1,4 ou 2% du chiffre d'affaires annuel mondial et total selon que l'on est qualifié d'entité essentielle ou importante ;

LA DIRECTIVE NIS2 EST-ELLE UNE CONTRAINTE DE PLUS OU UN ATOUT ?

La question posée en titre de notre article, est-elle une contrainte ou un atout ? Du point de vue de la société européenne, la Directive NIS2 est nécessaire. Les cyberattaques sont quotidiennes, ransomware en tête, et avec elles, les fuites de données souvent à caractère personnel. Quant aux fraudes à base d'usurpation d'identité numérique par faux sites web, fausses pages Facebook, le spoofing soit l'usurpation d'une adresse IP, le spam etc. qui servent de support à toutes sortes d'escroqueries, de faux ordres de virement ou d'arnaque au Président, ces délits sont désormais en nombre supérieurs au vol de véhicules ou cambriolages de domicile. Face cette explosion de délits, désormais l'apanage d'organisations internationales puissantes avec de fortes assises financières, le système policier et judiciaire se trouve en difficulté. La faute en est à une insuffisante coopération internationale policière et judiciaire, qui rend cette partie de gendarmes et de voleurs difficile pour le gendarme. La solution la plus immédiate et la plus efficace, consistait dès lors à faire ce que les fondateurs d'internet n'ont pas déployé, la mise en place de mesures techniques, organisationnelles et fonctionnelles imposées à l'écosystème pour faire barrage à cette cyberdélinquance dévastatrice pour nos sociétés. Le problème bien sûr, est d'abord philosophique car il s'agit au final de responsabiliser la victime si elle ne respecte pas ces mesures ou si elle ne notifie par l'incident ou la violation de données personnelles en temps utile, à l'autorité en charge du contrôle de ces mesures. Cependant, il n'y a sans doute pas le choix dans l'immédiat et il revient aux autorités de contrôle d'appliquer avec doigté et raison, les sanctions qui leur sont attribuées, se rappelant qu'elle sont d'abord « gendarme de la mise en conformité » et qu'à la différence d'un Tribunal, l'esprit des textes est qu'elles doivent rechercher avant tout la mise en conformité et que c'est seulement si l'entité refuse cette mise en conformité et ou ne l'applique pas de bonne foi, que la sanction devrait tomber.

Du point de vue des entreprises, la question atout ou contrainte, paraît plus mitigée. L'ANSSI et la plupart des observateurs évaluent à 15.000 le nombre d'entités qui seront concernées par NIS2 en France. Indirectement, ce sera sans doute beaucoup plus car, comme on l'a constaté avec le RGPD, les grandes entreprises, a priori donc les entités essentielles et importantes, vont imposer par le contrat à leurs partenaires et sous-traitants de toutes tailles, les obligations que la Loi leur impose. En effet, une question qui n'est pas traitée par la Directive NIS2 va tout changer, celle des responsabilités juridiques. Si une entité est négligente dans les mesures de sécurité informatique mises en place, au point de causer des préjudices à des tiers, elle peut se voir sanctionner administrativement par l'autorité en charge de sanctionner le défaut de conformité à NIS2. Mais cette sanction pourrait être ensuite le point de départ à des actions en responsabilité de la part de tiers ayant subi un préjudice, car la faute sera alors établie par la décision de sanction du contrevenant, par l'ANSSI. De la sorte, plus encore que pour le RGPD, les grandes entreprises vont sans doute imposer de manière plus tatillonne et par la voie du contrat, à leurs partenaires et sous-traitants, le respect de NIS2. Se conformer à NIS2 deviendra alors un critère de choix pour la grande entreprise. Mise en conformité que les entreprises européennes auront plus de facilité à mettre en œuvre que des concurrents extra-européens come les chinois ou les américains étant de surcroît rappelé qu'une action en responsabilité pourrait nécessiter d'appeler en garantie le partenaire ou sous-traitant. Si celui-ci est loin et non justiciable des juges européens, la grande entreprise se retrouvera seule face à ses responsabilités. Alors peut-être, NIS2 pourrait tout à la fois rimer avec plus de sécurité, mais aussi un peu plus souveraineté numérique et dès lors. On peut toujours espérer. ■

[1]Directive (UE) 2022/2555 du 14 Décembre 2022. Aux termes de son article 41, cette directive devait être transposée dans les Lois des Etats membres avant le 18 Octobre 2024. À l'heure où sont écrites ces lignes, peu d'Etats ont transposé le texte. En France, la situation politique et ses soubresauts, ont retardé le travail du Parlement. On peut cependant escompter que cette transposition interviendra courant 2025.

[2] Règlement (EU) 2022/2544 Digital Operational Resilience Act, une sorte de lex specialis de la Directive NIS2, c'est-à-dire une loi spéciale pour le seul secteur financier

[3] Directive (UE) 2022/2557

[4] En France, sans aucun doute, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

GOUVERNEMENT
Liberté
Égalité
Fraternité

17 CYBER
Mon assistance en ligne

Un service proposé par

POLICE NATIONALE
Gendarmerie nationale
CYBER MALVEILLANCE .GOUV.FR

QUIZ

L'IDENTITÉ ET L'ACCÈS NUMÉRIQUES EN CYBERSÉCURITÉ

1_ QU'EST-CE QUE L'AUTHENTIFICATION MULTIFACTORIELLE (MFA) ?

- ☐ **a)** Un système de sauvegarde de données
- ☐ **b)** Une méthode de vérification de l'identité utilisant deux ou plusieurs facteurs d'authentification
- ☐ **c)** Un logiciel antivirus
- ☐ **d)** Un protocole de chiffrement de données

2_ QUEL EST LE PRINCIPAL AVANTAGE DE L'UTILISATION DE L'AUTHENTIFICATION BIOMÉTRIQUE ?

- ☐ **a)** Elle est plus facile à pirater
- ☐ **b)** Elle offre une sécurité accrue grâce à l'utilisation de caractéristiques physiques uniques
- ☐ **c)** Elle est moins coûteuse à mettre en place
- ☐ **d)** Elle ne nécessite pas de connexion Internet

3_ QU'EST-CE QU'UN CERTIFICAT NUMÉRIQUE ?

- ☐ **a)** Un document papier signé électroniquement
- ☐ **b)** Un fichier électronique qui lie une clé publique à une identité
- ☐ **c)** Un logiciel de gestion de mots de passe
- ☐ **d)** Un dispositif de stockage de données

4_ QUEL EST LE RÔLE D'UN GESTIONNAIRE D'IDENTITÉS (IDENTITY MANAGER) DANS UNE ORGANISATION ?

- ☐ **a)** Gérer les sauvegardes de données
- ☐ **b)** Centraliser et gérer les informations d'identité des utilisateurs
- ☐ **c)** Développer des applications web
- ☐ **d)** Surveiller le trafic réseau

5_ QU'EST-CE QUE LE SINGLE SIGN-ON (SSO) ?

- ☐ **a)** Un système de sauvegarde de données
- ☐ **b)** Une méthode permettant à un utilisateur d'accéder à plusieurs applications avec un seul ensemble d'identifiants
- ☐ **c)** Un protocole de chiffrement de données
- ☐ **d)** Un logiciel de gestion de projets

RÉPONSES P.60

SELON CHAT.MISTRAL.AI

L'IDENTITÉ ET L'ACCÈS NUMÉRIQUES :

DÉFIS ET SOLUTIONS POUR LA SAUVEGARDE, LE STOCKAGE, L'ARCHIVAGE ET LA RESTAURATION DES DONNÉES

Dans un monde de plus en plus numérique, la gestion de l'identité et de l'accès (IAM) est devenue une composante essentielle de la cybersécurité.

Les Responsables de la sécurité informatique doivent non seulement protéger les données sensibles, mais aussi garantir que les bonnes personnes ont accès aux bonnes informations au bon moment.

Cet article explore les défis et les solutions liés à la sauvegarde, au stockage, à l'archivage et à la restauration des données dans le contexte de l'identité et de l'accès numériques.

LA GESTION DE L'IDENTITÉ ET DE L'ACCÈS (IAM)

La gestion de l'identité et de l'accès (IAM) est un ensemble de processus, de politiques et de technologies qui permettent de gérer les identités numériques et de contrôler l'accès aux ressources informatiques. Les systèmes IAM authentifient les utilisateurs et autorisent ou refusent l'accès aux données et aux applications en fonction de leurs rôles et de leurs permissions.

DÉFIS DE LA SAUVEGARDE DES DONNÉES

La sauvegarde des données est cruciale pour assurer la continuité des opérations en cas de perte de données. Cependant, dans un environnement IAM, la sauvegarde des données présente plusieurs défis :

1_ **Complexité des Permissions :** Les systèmes IAM gèrent des permissions complexes et dynamiques. Sauvegarder ces permissions de manière cohérente et restaurer les accès en cas de besoin est un défi majeur.

2_ **Volume de Données :** Les entreprises génèrent des volumes massifs de données. Sauvegarder ces données de manière efficace et sécurisée nécessite des solutions robustes et évolutives.

3_ **Sécurité des Sauvegardes :** Les sauvegardes doivent être protégées contre les accès non autorisés et les cyberattaques. Les responsables de la sécurité doivent s'assurer que les sauvegardes sont chiffrées et stockées dans des environnements sécurisés.

SOLUTIONS POUR LA SAUVEGARDE DES DONNÉES

1_ **Automatisation des Sauvegardes :** Utiliser des solutions automatisées pour sauvegarder régulièrement les données et les permissions IAM.

2_ **Chiffrement des Sauvegardes :** Chiffrer les sauvegardes pour protéger les données sensibles contre les accès non autorisés.

3_ **Stockage Redondant :** Utiliser des solutions de stockage redondant pour garantir la disponibilité des sauvegardes en cas de panne matérielle ou de cyberattaque.

DÉFIS DU STOCKAGE DES DONNÉES

Le stockage des données dans un environnement IAM présente également plusieurs défis :

1_ **Gestion des Accès :** Assurer que seules les personnes autorisées ont accès aux données stockées.

2_ **Conformité Réglementaire :** Respecter les réglementations en matière de protection des données, telles que le RGPD.

3_ **Évolutivité :** Adapter les solutions de stockage aux besoins croissants en termes de volume de données.

SOLUTIONS POUR LE STOCKAGE DES DONNÉES

1_ **Contrôle d'Accès Basé sur les Rôles (RBAC) :** Implémenter des politiques RBAC pour gérer les accès aux données stockées.

2_ **Audit et Surveillance :** Mettre en place des mécanismes d'audit et de surveillance pour détecter les accès non autorisés et les comportements suspects.

3_ **Stockage Hybride :** Utiliser des solutions de stockage hybride combinant le stockage sur site et dans le cloud pour répondre aux besoins d'évolutivité et de conformité.

DÉFIS DE L'ARCHIVAGE DES DONNÉES

L'archivage des données est essentiel pour la conservation à long terme des informations critiques.

Cependant, il présente plusieurs défis :

1_ **Durée de Conservation :** Déterminer la durée de conservation des données en fonction des exigences légales et opérationnelles.

2_ **Accessibilité :** Assurer que les données archivées restent accessibles en cas de besoin.

3_ **Intégrité des Données :** Garantir l'intégrité des données archivées sur de longues périodes.

SOLUTIONS POUR L'ARCHIVAGE DES DONNÉES

1_ **Politiques de Rétention :** Définir des politiques de rétention claires pour gérer la durée de conservation des données.

2_ **Solutions d'Archivage Sécurisées :** Utiliser des solutions d'archivage sécurisées pour protéger les données contre les accès non autorisés et les altérations.

3_ **Vérification Régulière :** Effectuer des vérifications régulières pour s'assurer de l'intégrité des données archivées.

DÉFIS DE LA RESTAURATION DES DONNÉES

La restauration des données est cruciale en cas de perte de données ou de cyberattaque. Cependant, elle présente plusieurs défis :

1_ **Rapidité de Restauration :** Restaurer les données rapidement pour minimiser l'impact sur les opérations.

2_ **Cohérence des Données :** Assurer la cohérence des données restaurées avec les permissions et les configurations IAM.

3_ **Sécurité de la Restauration :** Protéger le processus de restauration contre les accès non autorisés et les cyberattaques.

SOLUTIONS POUR LA RESTAURATION DES DONNÉES

1_ **Plans de Restauration :** Élaborer des plans de restauration détaillés pour restaurer rapidement les données en cas de besoin.

2_ **Tests Réguliers :** Effectuer des tests réguliers de restauration pour s'assurer de la cohérence et de la rapidité du processus.

3_ **Sécurisation du Processus :** Sécuriser le processus de restauration en utilisant des mécanismes de chiffrement et de contrôle d'accès.

CONCLUSION

La gestion de l'identité et de l'accès numériques est essentielle pour protéger les données sensibles et garantir la sécurité des environnements informatiques. Les défis liés à la sauvegarde, au stockage, à l'archivage et à la restauration des données dans un contexte IAM peuvent être surmontés grâce à des solutions robustes et sécurisées. Les responsables de la sécurité informatique doivent adopter une approche proactive pour protéger les données et assurer la continuité des opérations.
En intégrant des technologies avancées et en mettant en place des politiques de sécurité rigoureuses, les entreprises peuvent renforcer leur posture de cybersécurité et faire face aux menaces croissantes dans le monde numérique.

RÉPONSES DU QUIZ

1_ b) Une méthode de vérification de l'identité utilisant deux ou plusieurs facteurs d'authentification

2_b) Elle offre une sécurité accrue grâce à l'utilisation de caractéristiques physiques uniques

3_b) Un fichier électronique qui lie une clé publique à une identité**

4_b) Centraliser et gérer les informations d'identité des utilisateurs**

5_b) Une méthode permettant à un utilisateur d'accéder à plusieurs applications avec un seul ensemble d'identifiants**

SCALITY | storage software
RELIABLE, SECURE, SUSTAINABLE

Face au chaos des ransomwares

Adoptez une stratégie cyber-résiliente pour protéger votre entreprise

SCALITY
CORE5

1 Solution

5 Niveaux de cyber-résilience

www.artesca.scality.com/fr/#core

PRIVILEGED ACCESS / WORKFORCE ACCESS / ACCESS GOVERNANCE

wallix

Évoluez librement dans un monde numérique plus sûr

Libres et maîtres de vos systèmes, avec WALLIX vous opérez dans des environnements numériques et industriels où la sécurité ne freine pas vos activités. WALLIX sécurise les identités et accès afin de protéger vos actifs critiques face aux cybermenaces et de fluidifier vos interactions avec vos fournisseurs et vos clients. Leader Européen de la gestion des comptes à privilèges, WALLIX simplifie la mise en œuvre de la conformité et améliore l'efficacité opérationnelle des entreprises.

Avec WALLIX, vous bâtissez un monde numérique plus sûr pour innover, collaborer et grandir sans compromis.

www.wallix.com