L'IBM i face aux menaces actuelles et futures

Guy Marmorat
Expert en Sécurité sur IBM i
gmarmorat@resiliane.com

03 avril 2025

Sécurité IBM i

Où vous situez-vous ?

Pas vraiment conscient

- Non conscient des menaces et de leur impact
- Manque de sensibilisation
- Aucune évaluation des risques
- Manque de ressources

Conscient mais Statu quo

- Peur face à l'immensité de la tâche
- Peur du changement
- Peur des effets de bord
- Perte de la maitrise du SI
- Manque de transparence
- Maintenance du pré-carré
- Objectif unique: conforme à la règlementation

En cours de renforcement…

- Tout à fait conscient des risques
- Projet de renforcement de la Sécurité validé
- Audit IBM i en cours…

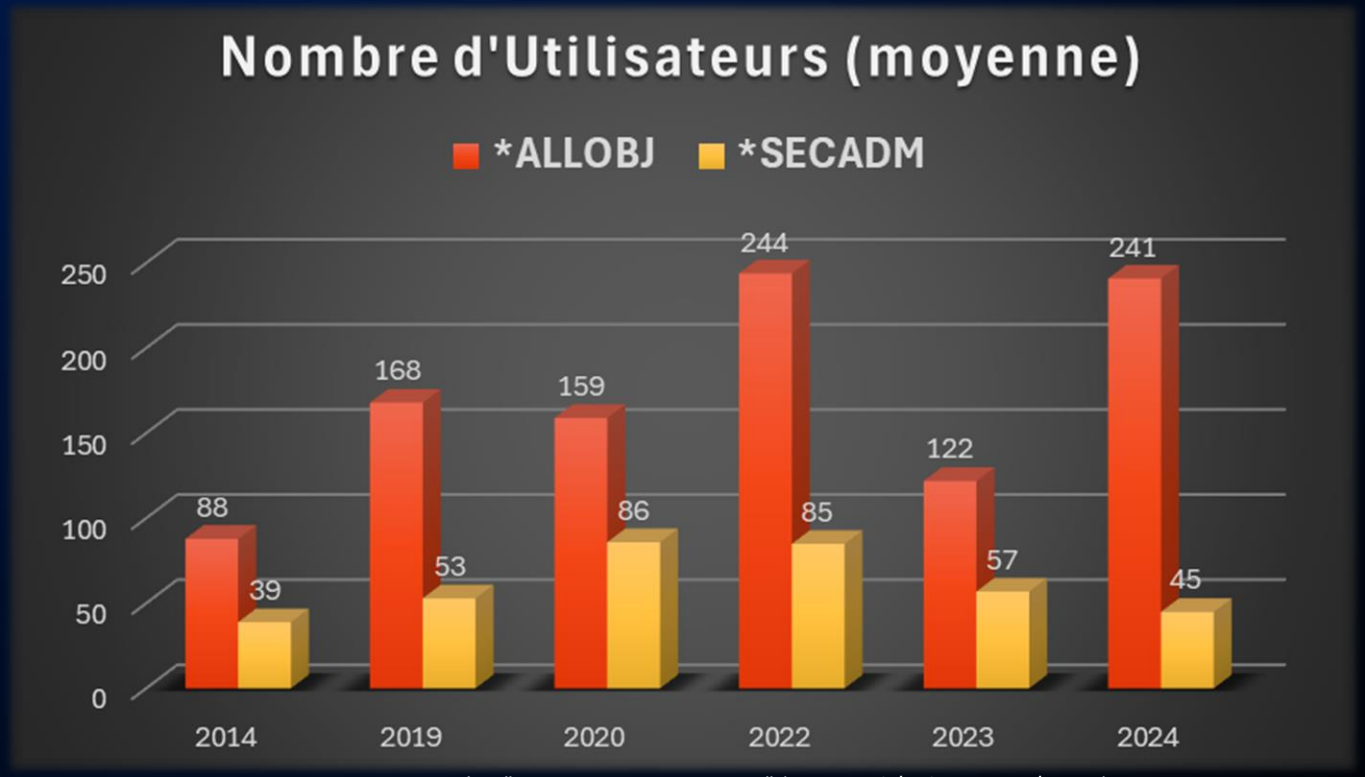
Mature

- Proactif
- Sensibilisation régulière des utilisateurs
- Audit IBM i effectué
- Remédiations en cours….
- Etablissement des règles de bonne pratique en cours d'amélioration

Sécurité IBM i

Evaluation de la situation

- Dette technique liée à la non-sécurité depuis le départ
- Sécurité ou simplement hygiène ?
- Recherche d'un coup de tampon « parapluie » plutôt que de travailler avec des experts reconnus
- Peu d'intérêt pour les stress-tests et tests de violation



Sources: enquêtes"State IBMiSecurity Survey" (Powertech/Help Systems/Fortra)

- Le mythe ***« IBM i sécurisé par nature » fait enfin partie du passé*** !! (« sécurisable » et non « sécurisé »)
- Cyber-Assurance : Les compagnies exigent de vraies mesures de sécurité (par ex: MFA dans certains cas)

Sécurité IBM i

DevSecOps

DevSecOps, abréviation de développement, sécurité et opérations, est une pratique de développement d'applications qui automatise l'intégration de la sécurité et des pratiques de sécurité à chaque phase du cycle de vie du développement logiciel, de la conception initiale à la livraison et au déploiement, en passant par l'intégration et les tests.

https://www.ibm.com/fr-fr/topics/devsecops

Un peu de terminologie :

- Terme DevOps apparu en 2007 (automatisation, monitoring)
- DevSecOps paragraphe ajouté à la page DevOps de Wikipedia
- Terme commence à apparaitre vers 2018
- DevSecOps (Development - Security - Operations)

La sécurité est une responsabilité partagée, intégrée du début à la fin. Cette notion est si importante qu'elle a donné naissance à l'expression DevSecOps pour souligner la nécessité d'intégrer la sécurité aux projets DevOps.

- Prise en compte de la sécurité dans le développement
- Industrialisation des vérifications de sécurité
- Tests de sécurité

Autre terme: DICP (Disponibilité, Intégrité, Confidentialité, Preuve)

Sécurité IBM i

Autres constats et tendances

- Après l'intrusion réussie : Exfiltration massive des données … ou … recherche des données sensibles et transfert discret, puis vente/échange sur le Dark Web
- Protection maximale & unique des réseaux … ou … approche multi-couches
- En cas d'APT (Advanced Persistant Threat) : détermination précise du point de restauration et recherche de TOUTES les connexions suspectes
- Scripts de connexion souvent trop faciles à découvrir
- Facile pour un admin de s'aménager discrètement des voies secrètes à utiliser

  plus tard au cas où….

- La phase d'identification des données sensibles est non démarrée ou largement incomplète
- Pourtant les données sensibles dites « structurées » peuvent être faciles à découvrir

Sécurité IBM i

IBM fait aussi sa révolution « DevSecOps » avec la 7.5

	Item		< 7.5	7.5
Initiale version	System Value QCRTAUT (default)		*CHANGE	*CHANGE
	Root (default)		*PUBLIC *RWX	*PUBLIC *RWX
	QPWDLVL (default)		0	3
	QSECURITY			not possible to go back to 20
	Function QIBM_NAV_ALL_FUNCTION (default)	Default *DENIED since 2022-05	*ALLOWED/*DENIED	*DENIED
	Command CRTUSRPRF (default)		PASSWORD(*USRPRF)	PASSWORD(*NONE)
	Command DSPLIB		shows all objects	only shows objects you have authority on
	New function QIBM_LIST_ALL_OBJS	DSPOBJD *NAME, QUSLOBJ, /QSYS.LIB/...		Default = *DENIED
	New function QIBM_LIST_ALL_OBJS_SQL	(IFS_)OBJECT_STATISTICS		Default = *DENIED
	displaying objects within '/home' directory		shows all objects	only shows objects you have authority on
	Authorities on DNS directories		*PUBLIC *USE	*PUBLIC *EXCLUDE
	Special authorities on DNS manipulations			many commands & APIs require special authorities
	Many objects in system libraries (default)		*PUBLIC *USE	*PUBLIC *EXCLUDE
	BRMS shipped database (default)		*PUBLIC *USE	*PUBLIC *EXCLUDE
	CRTJRN / JRNRCV		AUT(*LIBCRTAUT)	AUT(*EXCLUDE)
	Many objects related to PowerHA & Db2 Mirror		*PUBLIC *USE	*PUBLIC *EXCLUDE & special authority checking
Added afterwards	PTF SQL views			*USE required on WRKPTFGRP & DSPPTF
	IBM profile QRDARS*	Content Manager OnDemand		no longer used - removed
	IBM profile QMGTC	Management Central		no longer used - removed
	Qshell command db2mtool		password in clear-text	secured !
	DCM interface		heritage version	new interface http://system:2001/dcm
	QSYS2.USER_INFO & USER_INFO_BASIC	user_default_password		null for USER_INFO_BASIC

Liste non exhaustive

Encrypted downloads only for IBM Fix Central since 2023-02

Sécurité IBM i

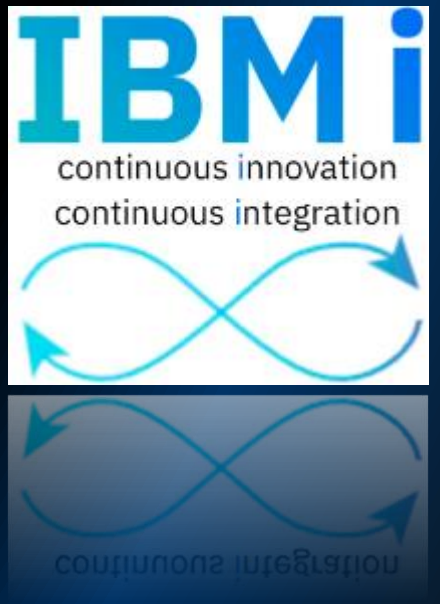
SYSTOOLS.SPECIAL_AUTHORITY_DATA_MART
SYSTOOLS.AUDIT_JOURNAL_NA() PS() VP()
QSYS2.AUDIT_JOURNAL_DATA_MART_INFO
avec DATA_MART_FILTER
SYSTOOLS.SEND_EMAIL()
(multiple email addresses & **attachments**)
SYSTOOLS.END_JOBS

Nouveautés 7.4 & 7.5

2024-07	TR10	TR4
2025-01	TR11	TR5

https://www.ibm.com/support/pages/ibm-i-75-tr5-enhancements

Column Name	System Column Name	Data Type	Description
AUTHORIZATION_NAME	USER_NAME	VARCHAR(10)	User profile name.
SPECIAL_AUTHORITY	SPCAUT	VARCHAR(9)	Special authority value.
AUTHORITY_SOURCE	AUTHSRC	VARCHAR(13)	Source of the special authority for this row. **GROUP PROFILE** The authority was obtained through the group profile in the GROUP_PROFILE_NAME column. **USER PROFILE** The authority is part of the user profile definition.
GROUP_PROFILE_NAME	GROUP_NAME	VARCHAR(10) Nullable	The group profile that provided the special authority for this row. Contains the null value if the special authority was obtained from the user profile.
STATUS	STATUS	VARCHAR(10)	The status of the user profile. ***DISABLED** The user profile is disabled; therefore, the user cannot sign on. ***ENABLED** The user profile is enabled; therefore, the user is able to sign on.
TEXT_DESCRIPTION	TEXT	VARCHAR(50) Nullable	The descriptive text for the user profile. Contains the null value if the user profile has no text description.
LAST_USED_DATE	LAST_USED	DATE Nullable	The date the user profile was used last. Contains the null value if the user profile has not been used.



Analyser, planifier (Audit de Sécurité)

Ne rien changer (Résistons à nos pulsions de la correction immédiate)

- Identifier les failles, vulnérabilités, trous de sécurité, défauts de configuration.
- Décrire la faille (si besoin, comment peut-elle être utilisée pour compromettre la sécurité, l'intégrité, la confidentialité)
- Lui affecter un niveau de risque

Proposer toutes les remédiations possibles

- Leur affecter un niveau d'effort estimé (incluant le risque de la remédiation elle-même)
- Lister les points de vigilance, anticiper tous les impacts possibles

Affecter une priorité, identifier les dépendances

Ne pas oublier : Garder toutes les évidences, y compris les valeurs ne nécessitant aucune correction.
Il se passe en général du temps entre la publication des résultats de l'audit et la remédiation !
Cela pourrait bouger…

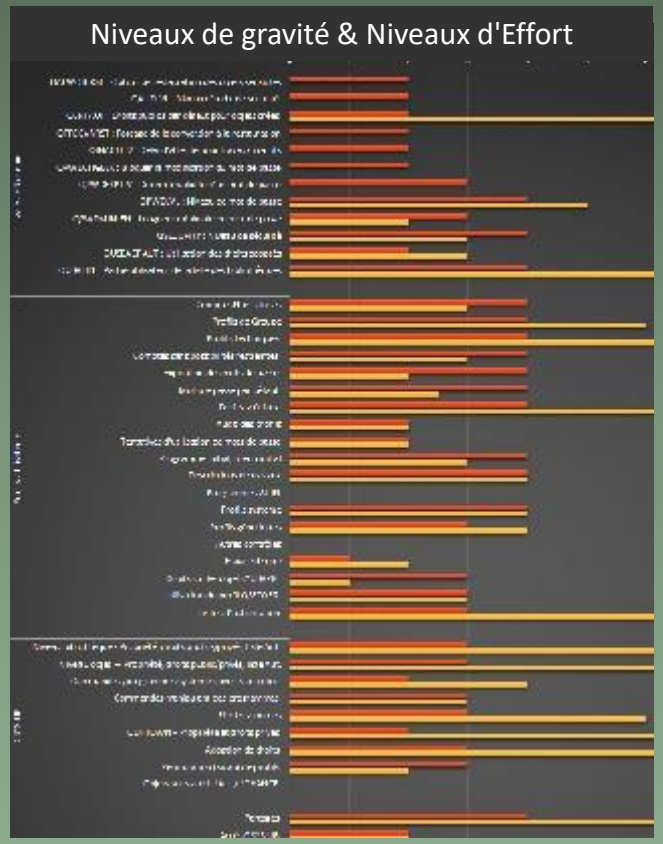
Analyser, planifier (Audit de Sécurité)

RAPPORT D'AUDIT DE SECURITE SUR IBM i

I. Revue des Valeurs Système
II. Revue des Profils utilisateurs
III. Système QSYS.LIB - Droits & Autres attributs des objets
IV. Système IFS - Droits & Autres attributs des objets
V. Autres données importantes
VI. Tests de violation d'accès

Confidentiel

PLAN DE REMEDIATION



Préparation de la remédiation

- Vérifier que la configuration est dans le même état
- Coder (Merci SQL !)
- Tester le processus complet de remédiation (bac à sable)
- Tester le processus complet de remédiation (recette)
- Effectuer des tests de non-regression

Mesurer les effets de la remédiation

- Vérifier les effets positifs directs (preuve, éducation, …)
- Identifier les effets négatifs directs
- Identifier les effets indésirables collatéraux

Envisager une éventuelle procédure de rollback

Mesures post-remédiation :

- Identifier les nouvelles déviations si elles devaient arriver
- Etre en capacité d'identifier des effets collatéraux plus insidieux
- Ne plus permettre à la faille de réapparaitre

Bien documenter l'ensemble

Remédier en Production

Vérifier que la configuration est dans le même état

Communiquer !

Lancer la procédure

- Choisir le bon moment en fonction des contraintes liées au type de remédiation. (IPL, changement dans d'autres serveurs & devices, changement dans des applications de gestion, etc…)
- Encore tester (Utilisateurs d'applications d'astreinte pour rejouer des transactions)
- Surveiller !

La remédiation peut être une action **impactante et risquée**.

Découper un gros sujet en parties autonomes, les plus petites possibles,

car **des solutions différentes** peuvent être apportées à chacune de ces parties.

Remédier en Production

Comment faire ?

Exemple : Suppression et/ou mitigation du droit spécial *ALLOBJ

- 1ère étape : Nettoyer les profils inutiles
- 2ème étape : Classifier les profils et leur affecter des groupes
- 3ème étape : Analyser le comportement des utilisateurs (authority collection, journaux, exit point) sur une période assez longue
- 4ème étape : Proposer les remédiations adaptées et/ou les contrôles supplémentaires

Ceci n'est qu'un exemple, à adapter à chaque situation et aux besoins de sécurité et de mise en conformité avec certaines règlementations.

Exemple :

Suppression et/ou mitigation du droit spécial *ALLOBJ
Comment s'y prendre ?

*ALLOBJ Supprimé

*ALLOBJ Sous surveillance

Categories d'utilisateurs	Ce qu'ils ont / n'ont pas le droit de faire sur les partitions de Production	Propositions de remédiation globale	Propositions de remédiation spécifique
Business application	Utilisent exclusivement des applications de gestion. De façon exceptionnelle et controlée, certains d'entre eux peuvent exporter/importer des données pour des besoins de gestion justifiés.	Affecter des profils groupe le plus possible (comme marqueur et porteur de droits) Contrôler les créations, modifications, restaurations de profils Contrôler les connexions Interdire les délégations d'utilisateurs (SBMJOB, APIs de swap) ou les justifier/contrôler	Authority collection et positionnement des droits Contrôle des imports/exports de données
Admin	Administrent le système et parfois aussi la base de données. Ne devraient pas lancer des processus de gestion. Ne devraient pas modifier ou voir les données.		Audit complet (joblog, journal système, journaux base de données, exit point, écrans) Autorisations à la demande de certaines commandes et/ou types d'accès
Support Exploitation	Suivent la bonne utilisation du système. Peuvent modifier des données dans certains cas et de façon controlée. Ne devraient pas lancer des processus de gestion.		Audit complet (joblog, journal système, journaux base de données, exit point, écrans) Emballage de certaines commandes utilisées régulièrement
R&D	Ont besoin de rechercher des contextes d'erreurs, parfois de debuguer. De façon exceptionnelle et controlée, ils peuvent restaurer des objets et corriger manuellement des données.		Elévation de droits à la demande et session auditée
Comptes de service	Sont utilisés pour des process automatiques qui requièrent une connexion à l'IBM i, tout en respectant des règles d'isolation. Ne devraient jamais être utilisés en dehors de ce cadre.		Contrôle des connexions inbound Contrôle des protocoles et fonctions utilisées Authority collection et positionnement des droits
Comptes batch	Sont utilisés pour des process automatiques qui ne requièrent aucune connexion à l'IBM i. Ne devraient jamais être utilisés en dehors de ce cadre.		Pas de mot de passe Pas de connexion Contrôle de la source (call stack, WRKJOBSCDE, ...) Authority collection et positionnement des droits
Profils propriétaires	Profils techniques dont le seul but est d'être propriétaires d'objets et éventuellement de participer à un mécanisme d'élévation de droits (adoption ou swap). Ne devraient jamais être utilisés en dehors de ce cadre.		Aucune connexion Aucune utilisation
Profils de groupe	Profils techniques dont le seul but est de regrouper des profils par rôle et donc de participer au mécanisme de sécurité des objets. Ne devraient jamais être utilisés en dehors de ce cadre.		Aucune connexion Aucune utilisation
Profils IBM réservés	Profils internes IBM. Ne devraient pas être modifiés et utilisés.		Aucune connexion Aucune utilisation autre que système
Consultants externes	Leur tâche varie en fonction de leur domaine de compétence. Leur activité doit être auditée.		Audit complet (joblog, journal système, journaux base de données, exit point, écrans) Elévation de droits à la demande et session auditée
QSECOFR	Dans la mesure du possible, réserver ce profil pour des tâches purement systèmes telles que l'application de PTF, des changements dans l'OS et le hardware. Son activité doit être auditée.		Audit complet (joblog, journal système, journaux base de données, exit point, écrans)

*ALLOBJ *ALLOBJ *ALLOBJ *ALLOBJ *ALLOBJ *ALLOBJ *ALLOBJ *ALLOBJ *ALLOBJ

Remédier en Production

- Pas d'idéologie, on n'écarte aucune méthode à priori (exit point, adoption, swap, RCAC, SIEM, MFA, …)
- Mais… l'achat d'un package de sécurité ne règle pas tous les cas par miracle
- Attention aussi aux outils gratuits d'analyse : souvent limités, orientés, et non contextualisés

  - Investir dans le maintien d'une partition de recette à l'image de la production (ROI)
  - Dire plutôt, « Environnement » de Recette d'ailleurs

  - Focus sur les failles à risque élevé, à effort faible à moyen
  - Paralléliser les tâches en fonction de l'effort estimé et des dépendances

Les applications externes

Première installation

Mise à jour

Correctif

Conserver systématiquement

l'audit trail complet

joblog

journaux

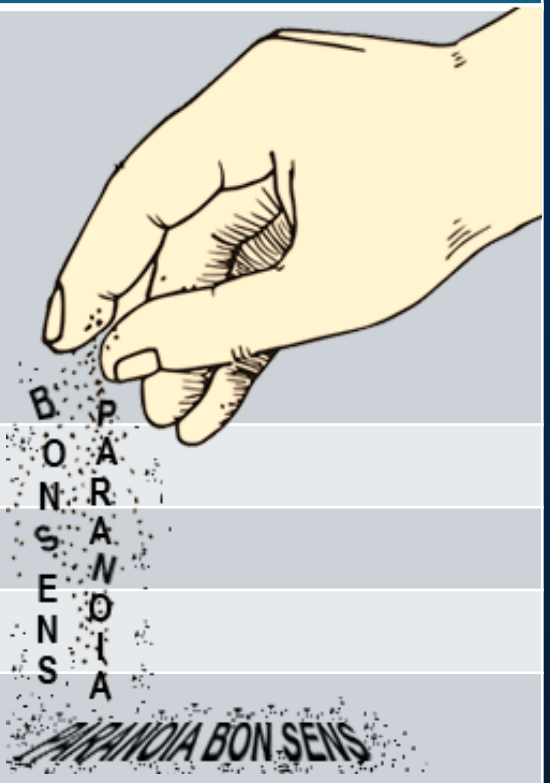
exit point

Les applications externes

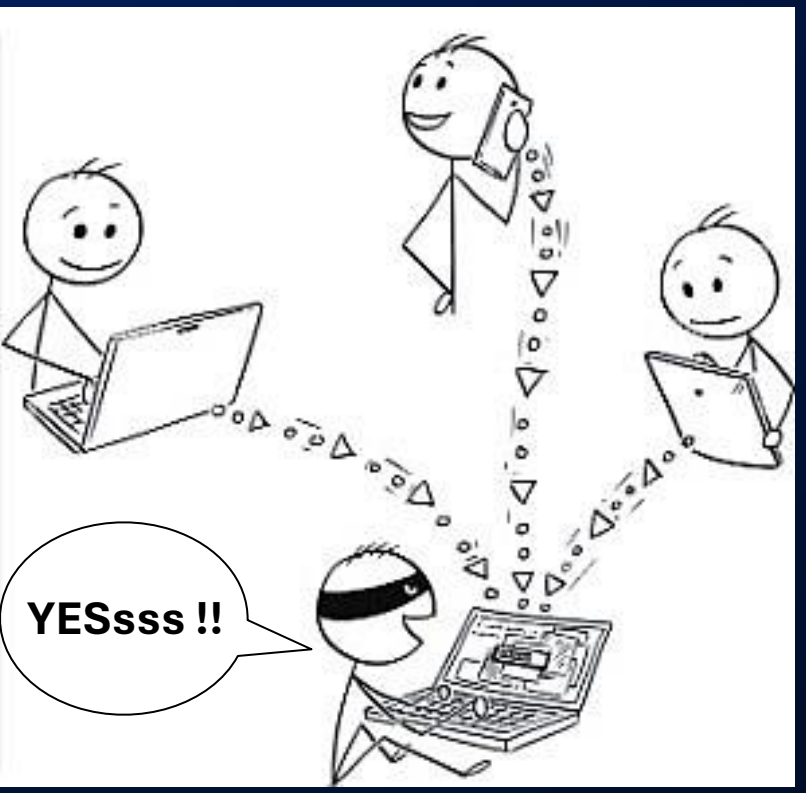
Exemple d'un questionnaire à adresser à l'éditeur	
Lister les nouveaux éléments : • les bibliothèques • les répertoires IFS • les objets restaurés dans d'autres bibliothèques existantes • les objets restaurés dans d'autres répertoires IFS existants • les profils avec leurs attributs • les listes d'autorisation • les sous-systèmes	.....
Décrire et justifier les modifications apportées au système : • programmes d'exit • function usage (ex : RCAC) • valeurs système • autres éléments (sous-systèmes existants, QAQQINI, TCP/IP, DDM, SST users IDs, etc…)	.....
Décrire le schéma général de la sécurité au niveau des bibliothèques, objets, IFS en détaillant : • les droits publics • les éventuels droits privés • la propriété • les listes d'autorisation • les exceptions	.....

Les applications externes

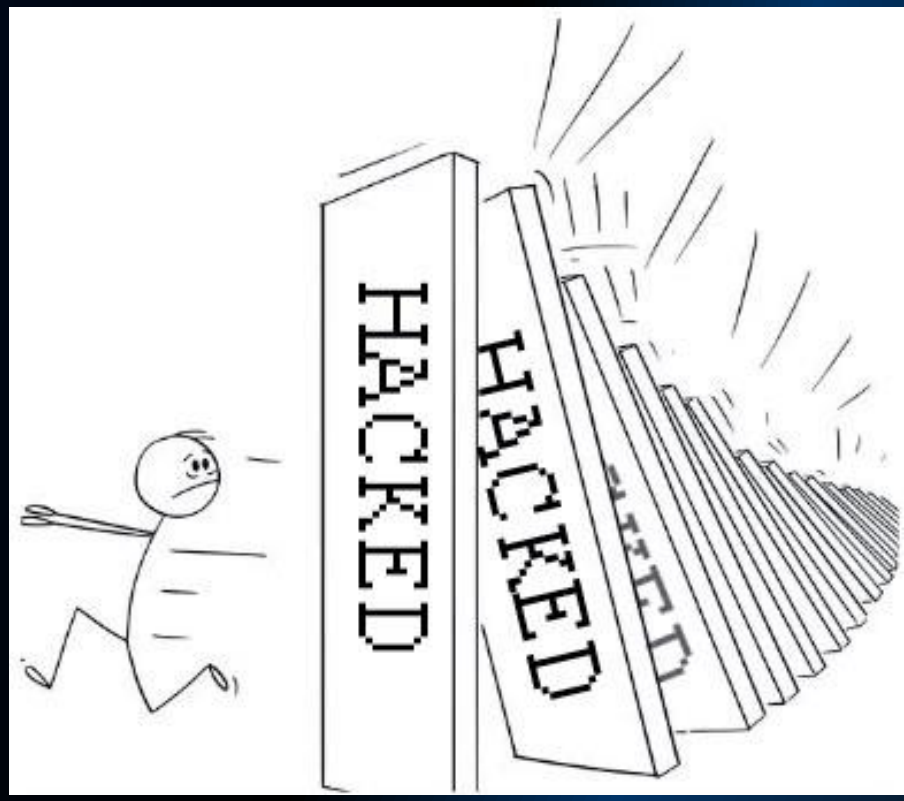
Exemple d'un questionnaire à adresser à l'éditeur (suite)	
Expliquer si les profils ont besoin de droits spéciaux et pourquoi Expliquer si des commandes sont en ALWLMTUSR(*YES) Expliquer si des programmes adoptant des droits élevés existent et confirmer que ces programmes n'ouvrent pas de ligne de commande Expliquer si des programmes utilisent les APIs de swap pour élever leurs droits et confirmer que ces programmes n'ouvrent pas de ligne de commande	.....
Décrire la gestion de la journalisation des données	.....
Décrire le principe d'enregistrement des utilisateurs finaux	.....
Donner les différentes valeurs des registres client si application ODBC, JDBC	.....
Justifier si l'installation patche des objets système qui apparaitraient en erreur avec CHKOBJITG	.....



Les applications externes



CONFIANCE OU PAS ?



Software Supply Chain Attacks

Une seule attaque est égale à :
De multiples sites infectés et/ou accessibles via des back doors, la propagation étant assurée par des canaux de confiance

Les applications externes

CONFIANCE OU PAS ?

MFT (Managed File Transfer)

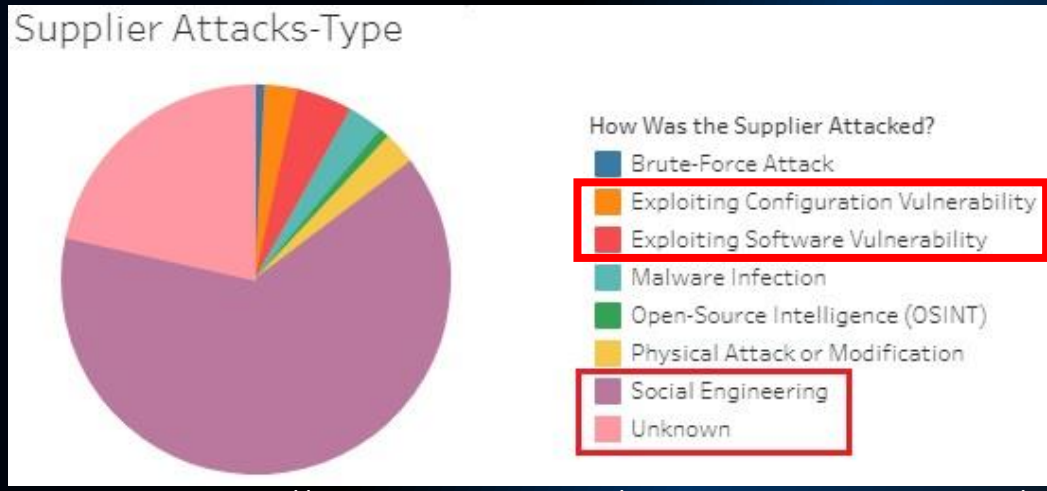
Cleo	9.8	2024-12
Cleo	9.8	2024-10
CrushFTP	not available	2024-12
CrushFTP	10.0	2024-04
CrushFTP	9.8	2023-11
Globalscape	7.5	2023-06
GoAnywhere MFT	not available	2024-12
GoAnywhere MFT	9.8	2024-01
GoAnywhere MFT	7.2	2023-02
IBM Sterling	9.1	2025-01
IBM Sterling	7.5	2024-11
IBM Sterling	9.8	2024-08
IBM Sterling	7.5	2024-08
MoveIT	9.8	2024-06
MoveIT	9.1	2024-06
MoveIT	7.5	2024-05
MoveIT	7.1	2024-01
MoveIT	7.2	2023-11
MoveIT	8.8	2023-09
MoveIT	9.1	2023-07
MoveIT	9.8	2023-06
WS_FTP Server	8.1	2024-08
WS_FTP Server	8.8	2023-11
WS_FTP Server	9.6	2023-09
Titan MFT	9.1	2023-10

Vulnérabilités avec score > 7.0
nvd.nist.gov/vuln | cve.org | ibm.com/support/pages

SIEM et autres produits de Sécurité

		HIGH (7.x)	CRITICAL (9.x)
SolarWinds	2025		1
	2024	27	7
	2023	22	3
IBM QRadar	2024	3	
	2023	10	
ArcSight	2024	2	1
	2023	1	1
Splunk	2025	2	
	2024	13	
	2023	16	1
Elastic	2024	2	
	2023	15	1
Graylog	2024	1	
	2021	2	2

- Compte de service à privilèges très élevés
- Exfiltration difficilement détectable dans la signature du run
- Application considérée comme critique pour le business



Source : https://www.comparitech.com/software-supply-chain-attacks/

Et l'Operating System IBM i

CONFIANCE OU PAS ?

CVE ID	Date	CVSS Ba	title	PTF 7.3	PTF 7.4	PTF 7.5
CVE-2024-55898	22/02/2025	8.5	IBM i could allow a user with the capability to compile or restore a program to gain elevated privileges due to an unqualified library call. A malicious actor could cause user-controlled code to run with administrator privilege	SJ03652	SJ03651	SJ03650
CVE-2024-38473	08/12/2024	8.1	IBM HTTP Server (powered by Apache) for IBM i is vulnerable to a remote attacker obtaining sensitive information, bypassing security restrictions, and a server-side request forgery due to multiple vulnerabilities	SJ02216	SJ02234	SJ02352
CVE-2024-38474	01/10/2024	8.2	IBM HTTP Server (powered by Apache) for IBM i is vulnerable to a remote attacker causing a denial of service, executing arbitrary code, and mapping URLs to filesystem locations due to multiple vulnerabilities	SJ01752	SJ01739	SJ01738
CVE-2024-1737	13/09/2024	7.5	ISC BIND on IBM i is vulnerable to a remote attacker causing a denial of service due to multiple vulnerabilities	SJ01570	SJ01569	SJ01540
CVE-2024-6387	28/08/2024	8.1	OpenSSH for IBM i is vulnerable to an attacker executing arbitrary code due to a signal handler race condition			SJ01687
CVE-2024-38330	03/07/2024	7.0	IBM Managed System Services for i and IBM System Management for i are vulnerable to a local user gaining elevated privilege due to unqualified library calls	SJ01174	SJ01170	
CVE-2024-27316	25/06/2024	7.5	IBM HTTP Server (powered by Apache) for IBM i is vulnerable to a denial of service attack using HTTP/2 protocol	SJ01169	SJ01168	SJ01169
CVE-2024-31890	20/06/2024	7.8	IBM i is vulnerable to a local privilege escalation due to a flaw in IBM TCP/IP Connectivity Utilities for i	SJ00680	SJ00679	SJ00681
CVE-2024-27275	20/06/2024	7.4	IBM i is vulnerable to a privilege escalation due to the ability to configure a physical file trigger in Db2 for IBM i	SJ00297	SF99704 - 28	SF99950 - 7
CVE-2024-27264	21/05/2024	7.4	IBM i is vulnerable to a local privilege escalation due to an unqualified library call in IBM Performance Tools for i	SJ00163	SJ00164	SJ00164
CVE-2024-31879	17/05/2024	7.5	IBM i is vulnerable to a denial of service of network ports due to deserialization of untrusted data in Management Central	SJ00629	SJ00619	
CVE-2024-25050	27/04/2024	8.4	IBM Rational Development Studio for i is vulnerable to a local privilege escalation due to an unqualified library call in compiler infrastructure	SI86096	SI86136	SI86179
CVE-2021-23450	24/04/2024	9.8	IBM Administration Runtime Expert for i is vulnerable to attacker executing arbitrary code on the system due to Dojo	SJ00250	SJ00250	SJ00250
CVE-2024-20952	27/03/2024	7.4	IBM Java SDK and IBM Java Runtime for IBM i are vulnerable to confidentiality impacts and a timing-based side-channel attack due to multiple vulnerabilities.	SF99725 - 32	SF99665 - 22	SF99955 - 9
CVE-2023-51385	23/02/2024	9.8	OpenSSH for IBM i is vulnerable to an attacker executing arbitrary commands due to improper validation	SI85948	SI85948	SI85935
CVE-2023-43064	10/02/2024	7.0	IBM Facsimile Support for i is vulnerable to a local user gaining elevated privileges due to an unqualified library call	SI85663	SI85663	SI85663
CVE-2017-15708	03/01/2024	9.8	IBM Db2 Web Query for i is vulnerable to a remote attacker bypassing security restrictions or executing arbitrary code, to a local authenticated attacker obtaining sensitive information, or to denial of service		SF99672 - 03	SF99673 - 03
CVE-2023-44487	14/12/2023	7.5	IBM WebSphere Application Server Liberty for IBM i is vulnerable to denial of service due to a flaw in handling multiplexed streams	SI85403	SI85402	SI85401
CVE-2023-42006	29/11/2023	8.4	IBM Administration Runtime Expert for i is vulnerable to an attacker obtaining sensitive information due to CVE-2023-42006	SI84843	SI84843	SI84843

Nombre de CVE		HIGH (7.x)	CRITICAL (9.x)
IBM i	2020	13	0
	2021	9	5
	2022	22	4
	2023	25	2
	2024	24	4
	>28/03/2025	1	0

Et l'Operating System IBM i

CONFIANCE OU PAS ?

CVE_ID	PUBLISHED_DATE	SCORE	PTF_V7R5	PTF Loaded Status	CREATED	APPLIED	DAYS_TO_PATCH	DESCRIPTION	PTF Product ID
CVE-2024-55898	2025-02-22	8.5	SJ03650	-	-	-	-	IBM i could allow a user with the capability to compile or restore a program to gain eleva...	-
CVE-2024-38473	2024-12-08	8.1	SJ02352	SUPERSEDED-SJ02602	-	2025-02-12	66	IBM HTTP Server (powered by Apache) for IBM i is vulnerable to a remote attacker obtaining...	577ODG1
CVE-2024-38474	2024-10-01	8.2	SJ01738	SUPERSEDED-SJ02602	-	2025-02-12	134	IBM HTTP Server (powered by Apache) for IBM i is vulnerable to a remote attacker causing a...	577ODG1
CVE-2024-1737	2024-09-13	7.5	SJ01540	-	-	-	-	ISC BIND on IBM i is vulnerable to a remote attacker causing a denial of service due to mu...	-
CVE-2024-6387	2024-08-28	8.1	SJ01687	APPLIED	2024-08-22	2025-02-12	174	OpenSSH for IBM i is vulnerable to an attacker executing arbitrary code due to a signal ha...	5733SC1
CVE-2024-27316	2024-06-25	7.5	SJ01169	APPLIED	2024-06-21	2024-10-29	130	IBM HTTP Server (powered by Apache) for IBM i is vulnerable to a denial of service attack ...	577ODG1
CVE-2024-31890	2024-06-20	7.8	SJ00681	APPLIED	2024-06-20	2024-10-29	131	IBM i is vulnerable to a local privilege escalation due to a flaw in IBM TCP/IP Connectivi...	577OTC1
CVE-2024-27264	2024-05-21	7.4	SJ00164	APPLIED	2024-05-18	2024-10-29	164	IBM i is vulnerable to a local privilege escalation due to an unqualified library call in ...	577OPT1
CVE-2024-25050	2024-04-27	8.4	SI86179	APPLIED	2024-03-08	2024-10-29	235	IBM Rational Development Studio for i is vulnerable to a local privilege escalation due to...	577OWDS
CVE-2021-23450	2024-04-24	9.8	SJ00250	SUPERSEDED-SJ00857	-	2024-10-29	188	IBM Administration Runtime Expert for i is vulnerable to attacker executing arbitrary code...	5733ARE
CVE-2023-51385	2024-02-23	9.8	SI85935	SUPERSEDED-SI86102	-	2024-05-03	70	OpenSSH for IBM i is vulnerable to an attacker executing arbitrary commands due to imprope...	5733SC1
CVE-2023-43064	2024-02-10	7.0	SI85663	-	-	-	-	IBM Facsimile Support for i is vulnerable to a local user gaining elevated privileges due ...	-
CVE-2023-42006	2023-11-29	8.4	SI84843	SUPERSEDED-SJ00055	-	2024-05-03	156	IBM Administration Runtime Expert for i is vulnerable to an attacker obtaining sensitive i...	5733ARE
CVE-2023-40685	2023-10-27	7.4	SI84794	PERMANENTLY APPLIED	2023-10-20	2023-11-04	15	IBM i is vulnerable to a local privilege escalation due to flaws in Management Central	577OSS1
CVE-2023-3341	2023-10-20	7.5	SI84740	-	-	-	-	ISC BIND on IBM i is vulnerable to denial of service due to a stack exhaustion flaw	-
CVE-2023-2650	2023-10-10	7.5	SI84812	PERMANENTLY APPLIED	2023-10-06	2023-11-04	29	OpenSSL and OpenSSH for IBM i are vulnerable to arbitrary code execution, denial of servic...	5733SC1
CVE-2023-38408	2023-10-10	8.1	SI84812	PERMANENTLY APPLIED	2023-10-06	2023-11-04	29	OpenSSL and OpenSSH for IBM i are vulnerable to arbitrary code execution, denial of servic...	5733SC1
CVE-2023-40375	2023-10-03	7.4	SI84247	PERMANENTLY APPLIED	2023-09-22	2023-11-04	43	IBM i is vulnerable to a local privilege escalation	577OSS1
CVE-2023-38408	2023-09-07	8.1	SI84812	PERMANENTLY APPLIED	2023-10-06	2023-11-04	29	OpenSSL and OpenSSH for IBM i are vulnerable to arbitrary code execution, denial of servic...	5733SC1
CVE-2023-2650	2023-09-07	7.5	SI84812	PERMANENTLY APPLIED	2023-10-06	2023-11-04	29	OpenSSL and OpenSSH for IBM i are vulnerable to arbitrary code execution, denial of	
CVE-2023-30990	2023-07-14	8.6	SI83472	PERMANENTLY APPLIED	2023-06-14	2023-08-06	53	IBM i is vulnerable to an attacker executing CL commands due to an exploita	
CVE-2023-0286	2023-05-09	8.2	SI83245	PERMANENTLY APPLIED	2023-04-14	2023-08-06	114	OpenSSL for IBM i is vulnerable to denial of service attacks and the ability	
CVE-2022-4450	2023-05-09	7.5	SI83245	PERMANENTLY APPLIED	2023-04-14	2023-08-06	114	OpenSSL for IBM i is vulnerable to denial of service attacks and the ability	
CVE-2022-4304	2023-05-09	7.5	SI83245	PERMANENTLY APPLIED	2023-04-14	2023-08-06	114	OpenSSL for IBM i is vulnerable to denial of service attacks and the ability	

A VOUS DE PATCHER RAPIDEMENT

CVE_ID	PUBLISHED_DATE	SCORE	PTF_V7R5	GROUP_INSTALLED	PTF_GROUP_STATUS	PTF_GROUP_DESCRIPTION	DESCRIPTION
CVE-2024-27275	2024-06-20	7.4	SF99950 - 7	SF99950 - 6	INSTALLED	DB2 FOR IBM I	IBM i is vulnerable to a privilege escalation due ...ysic...
CVE-2024-20952	2024-03-27	7.4	SF99955 - 9	SF99955 - 9	INSTALLED	JAVA	IBM Java SDK and IBM Java Runtime for IBM i are vu...ity impacts ...
CVE-2017-15708	2024-01-03	9.8	SF99673 - 3	SF99673 - 3	INSTALLED	DB2 WEB QUERY FOR I V2.4.0	IBM Db2 Web Query for i is vulnerable to a remote at...passing security restrict...
CVE-2022-40609	2023-08-25	8.1	SF99955 - 6	SF99955 - 9	INSTALLED	JAVA	IBM Java SDK and IBM Java Runtime for IBM i are vulnerable to arbitrary code execution...

PATH_NAME	OBJECT_TYPE	CREATE_TIMESTAMP	DATA_CHANGE_TIMESTAMP	OBJECT_CHANGE_TIMESTAMP	LAST_USED_TIMESTAMP
/[redacted]/LIB/log4j-1.2.5.jar	*STMF	2002-11-21 14:33:08	2011-03-17 05:23:28	2014-06-08 02:06:12	2014-06-08 00:00:00
/[redacted]/lib/log4j-1.2.5.jar	*STMF	2004-08-31 14:11:43	2011-03-16 19:58:08	2014-06-08 02:12:14	2016-03-05 00:00:00
/[redacted]/lib/log4j-1.2.5.jar	*STMF	2011-05-26 13:55:33	2011-05-26 13:55:33	2016-03-06 10:49:47	2023-01-27 00:00:00

Log4j : Détection des fichiers suspects dans l'IFS avec date < 2021-12

*LIBL & SQL Path et la Sécurité

CVE ID	Date	CVSS Base score	title
CVE-2024-55	22/02/2025	8.5	IBM i could allow a user with the capability to compile or restore a program to gain elevated privileges due to an **unqualified** library call. A malicious actor could cause user-controlled code to run with administrator privilege
CVE-2024-38	03/07/2024	7.0	IBM Managed System Services for i and IBM System Management for i are vulnerable to a local user gaining elevated privilege due to **unqualified** library calls
CVE-2024-27	21/05/2024	7.4	IBM i is vulnerable to a local privilege escalation due to an **unqualified** library call in IBM Performance Tools for i
CVE-2024-25	27/04/2024	8.4	IBM Rational Development Studio for i is vulnerable to a local privilege escalation due to an **unqualified** library call in compiler infrastructure
CVE-2023-43	10/02/2024	7.0	IBM Facsimile Support for i is vulnerable to a local user gaining elevated privileges due to an **unqualified** library call

Adopted authority risks and recommendations

You should use adopted authorities with care to prevent possible security risks.

Allowing a program to run using adopted authority is an intentional release of control. You permit the user to have authority to objects, and possibly special authority, which the user will not normally have.

Adopted authority provides an important tool for meeting diverse authority requirements, but it should be used with care:

- Make sure that programs that adopt authority and call other programs perform library qualified calls. Do not use the library list (*LIBL) on the call.

Library security and library lists

Attention A user who is authorized to the commands to work with library lists can potentially run a different version of a program.

ADDLIBLE	*CMD	Add Library List Entry	*USE
CHGLIBL	*CMD	Change Library List	*USE
CHGSYSLIBL	*CMD	Change System Library List	*EXCLUDE
EDTLIBL	*CMD	Edit Library List	*USE
RMVLIBLE	*CMD	Remove Library List Entry	*USE
CHGCURLIB	*CMD	Change Current Library	*USE
SBMJOB	*CMD	Submit Job	*USE
SETASPGRP	*CMD	Set ASP Group	*USE
QLICHGLL	*PGM	Change Library List	*USE
QSYSLIBL	*SYSVAL	System part of the library list	
QUSRLIBL	*SYSVAL	User part of the library list	
	*JOBD		
SET PATH			
...			

Security risks of library lists

This topic gives specific examples of the possible security exposures of library lists and how to avoid them.

Library lists represent a potential security exposure. If a user is able to change the sequence of libraries on the library list, or add additional libraries to the list, the user might be able to perform functions that break your security requirements.

Recommendations for system portion of library list

This topic provides the recommendations for the system portion of the library list.

The system portion of the library list is intended for IBM-supplied libraries. Application libraries that are carefully controlled can also be placed in the system portion of the The system portion of the library list represents the greatest security exposure, because the libraries in this part of the list are searched first.

Source : IBM i 7.5 Security Reference

Messages « France-Travail »

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

France Travail

Accédez à tous vos services candidats

Bonjour,

A la suite d'une cyberattaque dont France Travail et Cap emploi ont été victimes, des données personnelles de demandeurs d'emploi ont été extraites et sont donc susceptibles d'être divulguées et exploitées de manière illégale.

Vos nom, prénom, identifiants France Travail, numéro de sécurité sociale, date de naissance, adresses électronique et postale, sont concernés par ce vol. **Votre mot de passe France Travail et vos coordonnées bancaires ne sont en revanche pas concernés.** Il n'existe pas de risque concernant votre indemnisation.

Nous vous recommandons néanmoins la plus grande vigilance quant aux risques d'hameçonnage (mails ou appels frauduleux qui permettraient de vous leurrer pour vous inciter à communiquer des données financières ou personnelles) ou de tentatives d'usurpation d'identité et vous invitons à retrouver tous les conseils et informations sur le site https://www.cybermalveillance.gouv.fr

Autopsie du cas « France-Travail »

Cyberattaque France Travail : la CGT dénonce « des niveaux de sécurité insuffisants »

…
Dans le détail, la CGT-DSI de France Travail relève que « lors du projet de connexion du partenaire Cap Emploi en 2022 »,
le risque qui s'est matérialisé avec la récente cyberattaque avait bien été identifié et qu'il avait été alors préconisé de « renforcer l'authentification […] avec un deuxième facteur d'authentification (2FA), conformément aux exigences de l'Anssi ».
Las, lit-on, « il n'a jamais été mis en place ». En fait, selon le syndicat,
« il aura fallu une attaque d'ampleur jamais vue pour la mettre en place pour les salariés de Cap Emploi en seulement 1 ou 2 semaines ! ».

En outre, selon la CGT-DSI, « les salariés de Cap Emploi ont des autorisations d'accès non restreintes ».
Et les prestataires travaillant pour la DSI, sur site ou à distance,
« disposent des droits à l'identique des internes, que ce soit dans l'environnement de qualification ou de production du SI ».

Dès lors, le syndicat demande le déploiement de l'authentification à facteurs multiples
« pour tous les partenaires et salariés qui se connectent sur notre SI », et l'application « stricte du principe de moindre privilège ».
…
Ainsi, pouvait-on lire dans le communiqué de presse,

« potentiellement, les données personnelles de 43 millions de personnes » sont susceptibles d'avoir été « exfiltrées »,
sur la base de deux comptes d'agents Cap Emploi détournés : ils jouissaient manifestement de droits d'accès très étendus.
…

https://www.lemagit.fr/actualites/366580413/Cyberattaque-France-Travail-la-CGT-denonce-des-niveaux-de-securite-insuffisants

Nos données personnelles sur le Darkweb

+ 10 000

Janvier 2023 : La **CAF**
Données personnelles de **+10 000 allocataires** disponibles sur le site d'un prestataire privé pendant presque 2 ans.

10 Millions

Août 2023 :
Prestataire **Pôle Emploi MAJOREL**
Vol des données personnelles
10 millions d'usagers
Mise en vente sur le Darknet
Noms, Prénoms,
N° de Sécurité sociale
Statut du demandeur d'emploi

Vulnérabilité dans MOVEit chargée de numériser les documents transmis par les demandeurs d'emploi

20 Millions

Février 2024 :
Viademis & Almerys,
84 mutuelles touchées
20 millions d'assurés
Usurpation ID d'un professionnel de santé (ID & mot de passe + accès aux plateformes de Tiers Payants)
Identités,
N° de SS
Cartes vitales

43 Millions

Mars 2024 :
France Travail (ex-Pôle Emploi)
43 millions de personnes

+ Entre janvier 2022 et juin 2023:
187 incidents ont été signalés par des collectivités territoriales à l'ANSSI,
soit une moyenne de 10 par mois.

- Interconnexion avec les prestataires
  - **droits d'accès trop étendus**

Rappel - Plusieurs alertes :

- **Juin 2021 :**
  - **Importantes extractions de données par un agent en dehors des heures de travail**
  - **plusieurs dizaines de milliers de demandeurs d'emploi concernés**
- **En 2022, rapport d'audit montrant un indice maximal de 4**
- **En 2023 : 11,4 millions d'utilisateurs de Pôle Emploi dans les mains de plusieurs pirates**
- **La DSI a été alertée à plusieurs reprises :**
  - **Identification à 2 facteurs, conformément aux exigences de l'ANSSI, n'a jamais été mise en place.**
  - **Application « stricte du principe de moindre privilège »**

- **Juin 2021 :**
  - Extractions massives de données par un agent en dehors des heures de travail
  - Données transmises à une Agence d'Intérim
  - Plusieurs dizaines de milliers de demandeurs d'emploi concernés
  - Vente de données sur le Web

- **2022**
  - Rapport du Service Informatique de France Travail alerte d'un risque d'attaque (analyse de risque identifie une faille)
  - Application « stricte du principe de moindre privilège »
  - Audit ANSSI effectuée => Rapport positif sur la Sécurité informatique ;-)

- **2023**
  - 10 millions d'identités volées chez le prestataire MAJOREL
  - Mise en vente sur le Darknet (Noms, Prénoms, N° de Sécurité sociale, Statut du demandeur d'emploi)
  - Données non anonymisées stockées dans une BASE DE TEST

- **6 février 2024 – Attaque en 2 Temps !**
  - Entrée discrète sur la BD via Cap emploi
  - Hackers => Appel Support de France Travail pour renouveler le Mot de Passe d'un ID usurpé
    - VOLUMETRIE faible pour ne pas se faire voir => Phase de Test
    - Mise au point du SYSTEME DE REQUETAGE

- **Du 6 février au 5 mars 2024, les hackers ont eu accès au système** (selon le Parquet de Paris)

- **29 février 2024**
  - Transfert massif de fichiers (intégralité potentielle de la base de données)

43 millions de personnes

Nettoyage des ID !!
(20 ans dans les fichiers)

Manipulation de TROP de données !

Droits d'accès trop étendus !

Double Authentification
Non mise en place

Shadow IT

Auteur(s) & Méthode(s)
non encore identifiés

https://www.radiofrance.fr/franceinter/podcasts/secrets-d-info/secrets-d-info-du-samedi-25-mai-2024-3179825

Les applications externes

CONFIANCE OU PAS ?

Les éditeurs se sentent concernés depuis peu….
Le renforcement des tests de sécurité s'améliore,
mais la tâche est immense….

Nouveau comportement à adopter :

- Challenger les éditeurs
- Monitorer les activités d'installation, mise à jour, application de correctifs
- Tendre vers le Zero-Trust

Hacking History and News affecting the IBM i Security perception

Big chock Incredulity	09/08/2015	DEF CON	Live session	"Hack the legacy! IBM i (aka AS/400) revealed"
	02/09/2015	ITJungle	Article	Did IBM i Just Get Hacked at DEF CON?
	16/09/2015	ITJungle	Article	Hacker Defends DEF CON Talk on IBM i Vulns
Scary/ Mutilple layers of defense	16/03/2016	ITJungle	Article	Verizon Outlines Disturbing AS/400 Breach At Water District
Starting to work on it	25/01/2017	ITJungle	Article	What Was Discussed At the Big LUG Meeting
Apps: trusted or not trusted?	27/01/2021	ITJungle	Article	SolarWinds Hack Raises Concern for IBM i Shops
Zero-day - Score = 10	15/12/2021	ITJungle	Article	Critical Log4j Vulnerability Hits Everything, Including the IBM i Server
Software Supply Chain Attack	03/10/2022	ITJungle	Article	Software Supply Chain Attacks Are A Growing Threat
Zero-day on MFT	15/02/2023	ITJungle	Article	Zero-Day Vulnerability in Fortra's GoAnywhere MFT Being Actively Exploited
IBM i vulns	23/08/2023	ITJungle	Article	A Hacker's Dozen: 11 New Security Vulns Reported in IBM i
Library List	02/09/2024	TROOPERS24	Live session	"IBM i for Wintel Hackers" by Silent Signal
Privilege escalation	16/09/2024	ITJungle	Article	**Ethical Hackers Discuss Penetration Work On IBM i**

"So one thing to know about this library list issue is that we've already discovered like literally hundreds of these," Varga-Perke said. "So this is not an exception. It seems to be the rule. IBM is cleaning up the place right now, as you can see in their advisories. But yeah, it's a really rich attack surface. And as you can see, it's like basic logic bugs. You can find it if you have access to such a system really easily using basically strings."

Having exit programs in place is a definite plus, Varga-Perke said, particularly as they present "custom defenses that the attackers cannot prepare for." IBM i shops could also get more information about how hackers are targeting IBM i by implementing honey pots, or canaries, that attract hacker and then track their movements.

Règles d'or du Contrôle d'Accès via les Points d'Exit

Que faire avec un programme d'exit ?

- Rejeter certaines connexions et/ou transactions
- Loguer les tentatives rejetées
- Loguer certaines connexions et/ou transactions au caractère sensible (user admin, table critique, IP non recensée, call stack non applicatif, etc…)
- Déclencher des actions (envoi dans une SIEM, alerte, remédiation automatique, challenge MFA, interagir avec un SOAR, etc…)

Le programme d'exit est appelé avant le « Authority-Checking Process ».

Règles d'or du Contrôle d'Accès via les Points d'Exit

Choisir le bon compromis pour la protection des profils de service

A la connexion :

- Très contraignant (contrôle a minima sur le trio user-IP-protocole)
- Intransigeance sur les connexions « manuelles » avec des comptes de service

A la transaction :

- Définir la granularité de la règle (en fonction des ressources pour suivre les remontées, de la criticité des données, …).
- Le vocabulaire peut être vaste : l'utilisateur et ses attributs, le protocole et la fonction, le fichier DB2, son membre et sa bibliothèque, le chemin IFS, le contexte (date/heure, job, call stack, IP, registre), l'iASP, le détail de l'instruction (phrase SQL complète, commande complète, programme avec les paramètres, …)
- Mode forteresse ou Zero-trust
- Isolation : inbound/outbound (prod avec prod, recette avec recette, dev avec dev)
- Listes blanches, noires ou combinaison ?

Règles d'or du Contrôle d'Accès via les Points d'Exit

Contexte d'analyse déjà complexe et ça continue!
Merci IBM ! (SQL & Open-source)
Volume de transactions plutôt en augmentation

- Instructions SQL complexes (jointures, fonction scalaire qcmdexc, alias, noms longs/courts, tables non qualifiées, troncatures des buffers, …)
- Renforcer certaines connexions (MFA, registres client, …)
- PASE & QSH

Critères de choix d'un package de sécurité

- Tests de résistance
- Attention au STRDBMON *ALL/*ALL/*ALL – utilisez les filtres !
- Impact CPU
- Orientation « data_centric » (DB2 & IFS)

Protection des commandes via les points d'exit

Protocol	Syntax
5250	***dspsysval qdate***
FTP Server	Quote Rcmd ***dspsysval qdate***
REXEC	**RUNRMTCMD CMD(*'dspsysval qdate '*)** RMTLOCNAME(system *IP) RMTUSER(user) RMTPWD( )
FTP Client	**Syscmd *dspsysval qdate***
IBM i Access for Windows	**Rmtcmd //system *dspsysval qdate***
ODBC / DRDA ACS Run SQL Script …	**Call qsys2.qcmdexc (‘*dspsysval qdate* ')**
	cl:*dspsysval qdate*
	select qcmdexc('*dspsysval qdate* ') as cmdtorun from sysibm.sysdummy1
DDM	**SBMRMTCMD CMD('*dspsysval qdate* ')** DDMFILE(library/DDMfile)
SSH	**db2 "call qsys2.qcmdexc (*'dspsysval qdate '*)"**
	system "*'dspsysval qdate '*"

Différentes méthodes pour exécuter une commande

Protection des commandes via les points d'exit

User profile : LMTCPB(*YES) & Command : ALWLMTUSR(*NO)

Protocol	Syntax	Exit Point
5250	***dspsysval qdate***	QIBM_QCA_RTV_COMMAND
FTP Server	Quote Rcmd ***dspsysval qdate***	QIBM_QTMF_SERVER_REQ
REXEC	RUNRMTCMD CMD('***dspsysval qdate*** ') RMTLOCNAME(system *IP) RMTUSER(user) RMTPWD( )	QIBM_QTMX_SERVER_REQ
FTP Client	Syscmd ***dspsysval qdate***	QIBM_QTMF_CLIENT_REQ
IBM i Access for Windows	Rmtcmd //system ***dspsysval qdate***	QIBM_QZRC_RMT
ODBC / DRDA ACS Run SQL Script …	Call qsys2.qcmdexc ('***dspsysval qdate*** ')	QIBM_QZDA_SQL2
	cl:***dspsysval qdate***	QIBM_QZDA_SQL2
	select qcmdexc('***dspsysval qdate*** ') as cmdtorun from sysibm.sysdummy1	QIBM_QZDA_SQL2
DDM	SBMRMTCMD CMD('***dspsysval qdate*** ') DDMFILE(library/DDMfile)	CHGNETA DDMACC( )
SSH	db2 "call qsys2.qcmdexc (***'dspsysval qdate'***)"	Database Monitor
	system "***'dspsysval qdate'***"	

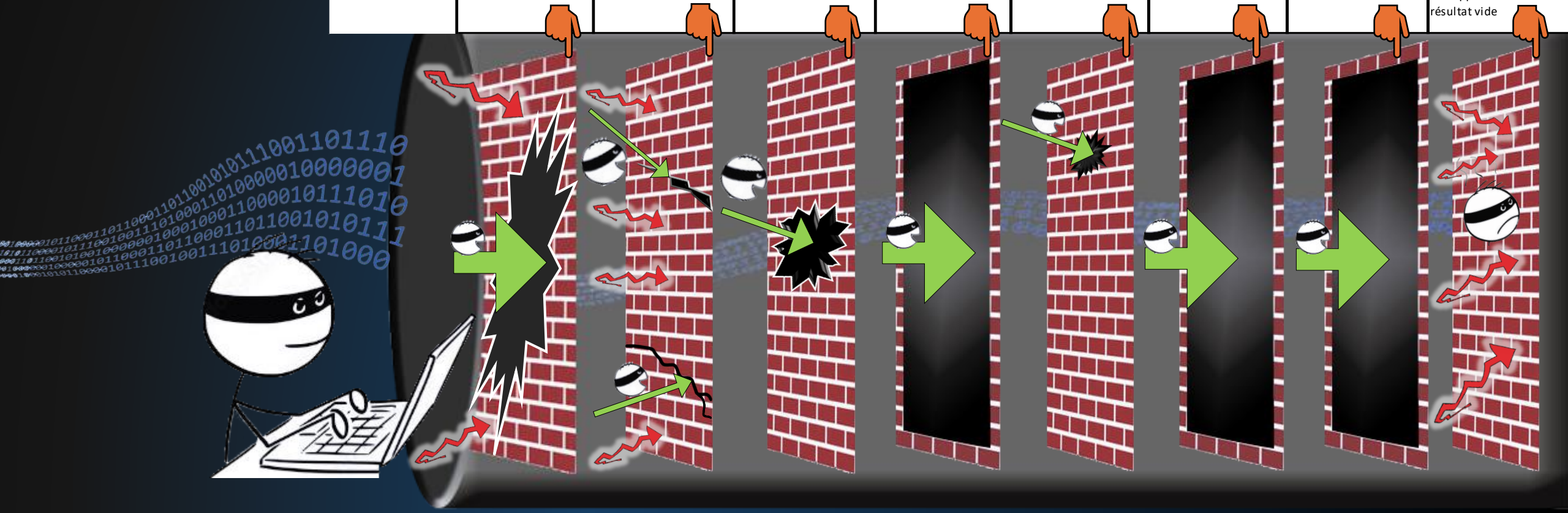
Paramètre LMTCPB respecté

Paramètre LMTCPB ignoré

L'efficacité de la sécurité par couches indépendantes

Exemple:
Tentative d'exfiltration de données sensibles

NIVEAU	Poste de travail	Poste de travail	Partition IBM i	Partition IBM i	Partition IBM i	Partition IBM i	Partition IBM i	Partition IBM i
Mesure de protection	droits admin interdits	déploiement software packagé selon role	droits publics *EXCLUDE sur les données; droits *CHANGE via le groupe applicatif	function usage	exit point SQL & FTP (connexion & détail)	exit point SQL (registres client)	exit point sur tables ultra-sensibles	RCAC
Statut de la mesure	en place	en place	en place	non activé car redondant avec les points d'exit	en place en mode bloquant	non activé car non supporté par le programme d'exit	non activé car programme d'exit non disponible ou non performant	en place
Méthode(s) de violation	phishing ou utilisateur malhonnête	FTP & DBeaver accessibles	SQL, FTP	SQL, FTP	FTP bloqué, SQL accessible	SQL accessible	SQL accessible	SQL accessible, mais pas de données restituées
Explications	prise de contrôle du poste via un proxy site web et installation d'un exécutable; récupération ID et mot de passe de connexion aux serveurs	ce poste appartenait à un utilisateur ayant un role différent; le poste n'a pas été nettoyé correctement avant redéploiement	le profil utilisé étant membre du groupe applicatif, son accès à la donnée est légitime	function usage non activé	les membres du groupe applicatif sont légitimes à utiliser une application Java manipulant les données IBM i dont la table sensible ciblée	pas de contrôle en place sur le client utilisé.	pas de contrôle supplémentaire sur la table sensible ciblée	permission SQL sur les fichiers sensibles avec analyse des critères d'environnement de travail via une fonction SQL: la lecture d'une table sensible en dehors de l'application donne un résultat vide



Renforcement de l'authentification : Mots de passe

Fonctions	Valeurs Système	Valeurs Profil	Bénéfices
Valeur Système pour le niveau de sécurité	QSECURITY (~~10, 20, 30~~, 40, 50)		Utilisateur requis ; Mot de passe requis
Valeurs Système pour les tentatives de connexion	QMAXSGNACN & QMAXSIGN	MAXSIGN(nn)	Protège contre les mots de passe devinés et les attaques par force brute
Valeur Système pour le niveau du mot de passe	QPWDLVL (~~0,1,2~~,3,4)		Renforce les mots de passe (longueur, types de caractères, chiffrement)
Valeurs Système pour la gestion des mots de passe	QPWDRULES, QPWDVLDPGM		Renforce les mots de passe (composition)
Single Sign-On & EIM		LCLPWDMGT(*NO) PASSWORD(*NONE)	Rationnalise la gestion des mots de passe
Valeur Système pour Secure sockets layer protocols	QSSLPCL (~~SSLV2, SSLV3, TLSV1.0, TLSV1.1~~, TLSV1.2, TLSV1.3)		Encrypte les transactions

Renforcement de l'authentification

Ensuite ?

2 pistes différentes:

- Continuer la complexification du mot de passe (risque de ne plus s'en souvenir ou utilisation coffre-fort de mots de passe)
- Utiliser une PassPhrase (mémorisable) et ajouter un second facteur (Passcode, Push Notification sur Smartphone, …)

Ne vous faites pas voler votre mot de passe :

- Chiffrer les mots de passe (QPWDLVL = 3 ou 4)
- Chiffrer les transactions (TLSV1.2, TLSV1.3)
- Contrôler drastiquement la récupération du mot de passe encodé pour prévenir le craquage offline (API QSYRUPWD)

Renforcement de l'authentification

Ensuite ?

Longueur de votre mot de passe	Que des chiffres	Alphabet mixte majuscule et minuscule	Alphabet mixte majuscule et minuscule, chiffres mixtes	Alphabet mixte majuscule et minuscule, chiffres mixtes, symboles
3	Immédiatement	Immédiatement	Immédiatement	Immédiatement
4	Immédiatement	Immédiatement	Immédiatement	Immédiatement
5	Immédiatement	Immédiatement	3 secs	10 secs
6	Immédiatement	8 secs	3 minutes	13 minutes
7	Immédiatement	5 minutes	3 heures	17 heures
8	Immédiatement	3 heures	10 jours	57 jours
9	4 secs	4 jours	153 jours	12 ans
10	40 secs	169 jours	1 an	928 ans
11	6 minutes	16 ans	106 ans	71 K ans
12	1 heure	600 ans	6 K ans	5 milliards d'années
13	11 heures	21 K ans	108 K ans	423 milliards d'années
14	4 jours	778 K ans	25 milliards d'années	5 Bn ans
15	46 jours	28 millions d'années	1 milliard d'années	2 Tn ans
16	1 année	1 milliard d'années	97 Bn ans	193 Tn ans
17	12 années	36 milliards d'années	6 Tn ans	14 Qd ans
18	126 ans	1 Tn années	374 Tn années	1 Qt année

Caler correctement vos valeurs système et attributs de profil :

- Sysval QPWDRULES *DGTMINn (longueur mini)
- Sysval QPWDLVL (longueur mini)
- Sysval QPWDRULES (types de caractères & +++)
- Sysval QPWDEXPITV (expiration)

  Attribut PWDEXPITV()

Revolution in Password's World ???!!!

Version 4 issued on August 2024 of the NIST 800-63 document which contains Password Guidelines

PASSWORD COMPOSITION

Minimum length = 8 (better 15)

Maximum length = 64

Password complexity = no more complexity requirements

PASSWORD MANAGEMENT

No more automatic expiration, to be changed for a good reason only

New password different from previous ones

Password not trivial nor breached

Recommendation / Obligation

The Best Solution is:

Memorizable Passphrase + MFA

- Overly stringent password requirements are often **counterproductive**
- Password complexity and length requirements do not help defend against keystroke logging, **phishing and social engineering attacks**
- Security postures should not be weakened by simply removing password complexity and associated rules **without implementing the additional new system controls.**
- Requirement for users to regularly change their passwords, which originated **decades ago**, is outdated. Back then, people often used easily guessed names and dictionary words as passwords.
- When such strong passwords are in use, forcing users to change them every few months can **weaken security**. The additional burden leads users to create simpler, easier-to-remember passwords.
- When passwords are sufficiently long, the **character-type requirements add no real security benefit**. In fact, such rules can push users to choose weaker passwords.
- Strongly not recommended to **not use SMS** messages in Multifactor Authentication.

SIEM

Définition

SIEM - Security Information & Event Management

Rôle et Valeur Ajoutée :

- Corrélation des évènements IBM i avec le monde extérieur
- Externalisation et consolidation des logs
- Ségrégation des process
- Conformité avec certaines règlementations
- Contextualisation des activités et détection des incidents potentiels
- Analyse & Investigation (Forensic)

SIEM — Schéma général de la connexion & Terminologie

Exemple: Exportation de postes PW du journal QSYS/QAUDJRN en utilisant DISPLAY_JOURNAL & l'option generate_syslog => 'RFC3164' ou 'RFC5424'

Header RFC5424 (Newer)

Event message in CEF format

Formats
CEF :ArcSight
LEEF: Qradar
Raw

IBM i

```
<37>MAY  2 11:45:53 AMIE75 CEF:0|IBM|IBM i|7.5|QSYS-QAUDJRN|T-PW|Low|
reason=Invalid password msg=User ROWTON password not valid
deviceExternalId=QPADEV0004 suser=QSYS sproc=148719/QSYS/QINTER shost=AMIE75 src=10.20.30.40 spt=57712

<37>MAY  2 11:46:20 AMIE75 CEF:0|IBM|IBM i|7.5|QSYS-QAUDJRN|T-PW|Low|
reason=Invalid password msg=User GM password not valid
deviceExternalId=QPADEV0006 suser=QSYS sproc=152369/QSYS/QINTER shost=AMIE75 src=10.20.30.40 spt=58529

<37>1 2024-05-02T11:46:26.345632+01:00 AMIE75.RIT.LOCAL - - - - CEF:0|IBM|IBM i|7.5|QSYS-QAUDJRN|T-PW|Low|
reason=Invalid password msg=User GMXXX name not valid
deviceExternalId=QPADEV0006 suser=QSYS sproc=152369/QSYS/QINTER shost=AMIE75 src=10.20.30.40 spt=58529
```

An event = A payload

Header RFC3164 (Older)

Push via Syslog UDP/TCP/TCP TLS

Pull via LFP (.csv) FTP/SFTP/SNMP

API Cloud

SIEM

Agent de connexion sur l'IBM i

L'agent sur l'IBM i devra :

- Établir la connexion, la sécuriser si non UDP
- Gérer la boucle de l'itération choisie
- Construire le message
- Enrichir le message (ex: indicateur compte à privilèges)
- Catégoriser le message
- Tester périodiquement la connexion SIEM (si UDP)

Les sources IBM i sont :

- Le journal système **QAUDJRN**
- Les journaux database
- Les journaux propriétaires (user entries)
- **QHST**, MSGQs, JOBLOG, WATCH, …
- D'autres logs (exit point, Database Monitor, elevation, MFA, encryption, …)

Note: QAUDJRN et QHST supportent la sortie Syslog en standard

Les questions :

- Protocole UDP ou pas?
- Itération la plus proche du temps réel?
- Garantie du traitement de tous les évènements
- Filtrage : faible, moyen, précis ?? (incidence sur la tarification en EPS ou Gb/day)
- La construction du message doit optimiser son ingestion dans le SIEM (parser – DSM pour QRadar, etc…)
- Synchronisation des évènements entrants en tenant compte du retard d'ingestion et du fuseau horaire

SIEM

Nombre de tentatives depuis
cette IP dans un laps de temps donné ?

```
reason=Invalid password msg=User GMXXX name not valid
deviceExternalId=OPADEV0006 suser=QSYS sproc=152369/QSYS/QINTER
shost=AMIE75 src=10.20.30.40 spt=58529
```

Quel user connecté sur cette device ?

```
reason=Object move or rename msg=Object renamed fileType=*STMF
fname=erppgmx.savf oldFileName=erppgm.savf
filePath=/home/gm/erppgmx.savf oldFilePath=/home/gm/erppgm.savf
suser=QUSER sproc=153004/QUSER/QZLSFILET shost=AMIE75 src=10.242.2.3 spt=55515
```

Possible attaque en cours
Activité intense et inhabituelle via NetServer

En action

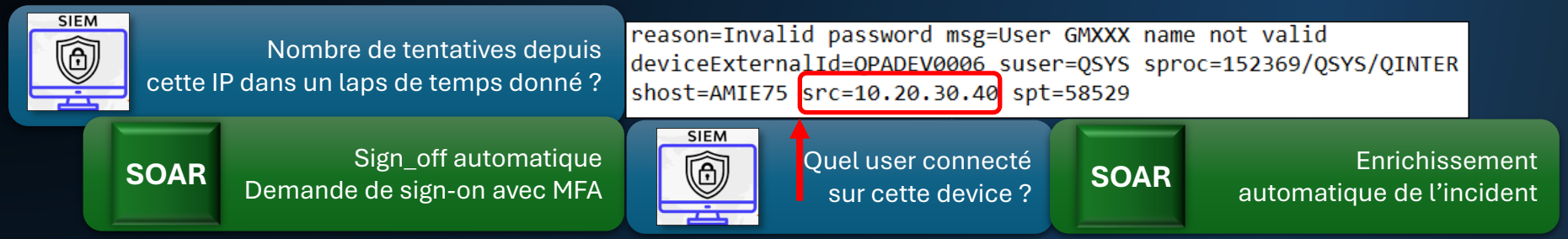
La SIEM aide dans les situations suivantes :

- Attaque de Déni de Service (DoS)
- Attaque de diversion (cacher ses traces dans le « brouhaha »)
- Attaque lente et sophistiquée (APT) – difficile à détecter.

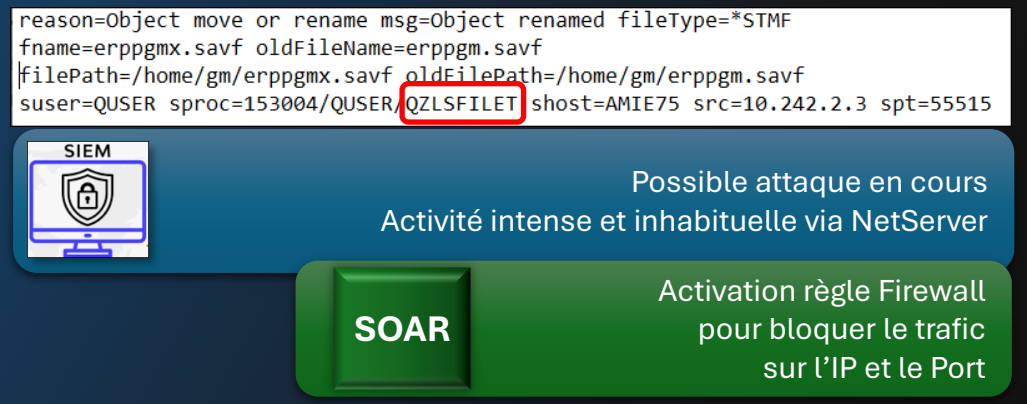
- Corrélation de base : dictionnaire d'IPs de mauvaise réputation – contournement via du IP spoofing
- Corrélation comportementale (UEBA - User and Entity Behavior Analytics) : utilise le Machine Learning pour déterminer les profils d'activités. Pourra donc identifier un delta même faible dans son comportement.
- Référentiel de comportement par rôle/département possible aussi.

SIEM

Prolongement vers le SOAR (Security Orchestration Automation and Response)



- **SIEM** détecte et crée un incident.
- **SOAR** prend le relai dans le traitement de l'incident, en mode manuel ou automatique.
- Lancement de routines (playbooks) associées aux incidents
- Exemples:
  - enrichissement automatique
  - remédiation semi-automatique
  - challenge avec MFA



Monde idéal :

- L'agent IBM i reçoit du **SOAR** une demande de remédiation via un programme d'exit

Merci
de votre attention !

Pour toute question :
Guy Marmorat (gmarmorat@resiliane.com)