Sécurité IBM i

Immersion dans 2 projets différents de remédiation

Guy Marmorat – Expert en Sécurité IBM i – Le 10 octobre 2024

iBelieve 2024
Présent et Futur de l'IBM i

ACMi CFD INNOVATION FRESCHE GAIA IBM itheis M81 precisely REMAIN resolution XCASE

2 projets différents de remédiation en termes de :

- complexité de l'environnement
- budget
- objectifs

Comment utiliser la Suite « Assure Security » pour atteindre ces objectifs ?

Sécurité IBM i - Projet de remédiation

Introduction

Entreprise	PME familiale leader sur le marché français - 4 milliards CA	Etablissement financier français et international (dans le top-20 Europe)
Infra	1 Prod, 1 backup, 1 test/dev	Chaque filiale est équipée d'au moins une partition de SIT (Test/Dev), UAT (Recette), Production, BackUp, parfois infocentre
Ressources IBM i	1 admin à temps partiel, assisté par un partenaire technologique	6 admins dont 4 seniors
Motivation du projet	Confrère ayant subi une attaque aux conséquences lourdes	Le durcissement de la sécurité est un projet prioritaire
Situation de départ	Page blanche - Difficulté d'apprécier le niveau de résistance en cas d'attaque similaire	Chaque filiale est à un niveau différent. De nombreux audits ont déjà été menés.
Objectif	Durcir la sécurité de façon urgente mais pérenne, tout en restant compatible avec les ressources et le budget	Sécurité optimale visée, implementée de façon incrémentale
Délai	18 mois	> 5 ans, avec jalons réguliers
Budget	< 100k	?

Sécurité IBM i - Projet de remédiation 1

Déroulement

Audit sécurité finesse 3/5 *(36 items de gravité élevée)*
Test de résistance finesse 3/5 *(91% des scenarios réussis)*

Test de résistance finesse 3/5 *(17% des scenarios réussis)*

Test de résistance finesse 3/5 *(3% des scenarios réussis)*

15 minutes par jour maximum (tâches assurées par le partenaire technologique)

Phase initiale	Phase remédiation 1	Phase fin de remédiation 1	Phase remédiation 2	Phase fin de remédiation 2	Statut	Tâches d'exploitation	Tâches Exploitation Ressources	Projets identifiés

Jour J — 6 mois — 7 mois — 9 mois — 13 mois — 15 mois

- Remédiation des failles de gravité haute et effort faible à moyen
- Contrôle d'accès via les points d'exit (granularité moyenne)

- Tuning en fonction du résultat du test de résistance
- Contrôle des déviations

Fin de projet

Contrôle automatisé des déviations, maintenance des règles de contrôle d'accès, revue de logs

Chiffrement des échanges

Sécurité IBM i - Projet de remédiation 2

Déroulement

Application du plan global de sécurité du groupe au monde IBM i

Audit trail complet, lisible, pertinent

Audit sécurité finesse 4/5
Test de résistance finesse 4/5
(3% des scenarios réussis)

1 admin dédié pour 50/75% de son temps

Phase initiale	Phase remédiation 1	Phase fin de remédiation 1	Phase remédiation 2	Phase fin de remédiation 2	Statut	Tâches d'exploitation	Tâches Exploitation Ressources	Projets identifiés
Jour J	6 mois	7 mois	24 mois	36 mois	> 4 ans			

- Contrôle des comptes à privilèges
- Contrôle d'accès via les points d'exit (granularité élevée)
- Rationalisation des pratiques liées aux échanges de données

- Intégration du monde IBM i au sein du SOC
- Remédiations
- Reporting évènements & déviations
- Déploiement & Consolidation
- CI/CD

Amélioration continue

Contrôle automatisé des déviations, maintenance des règles de contrôle d'accès, revue de logs

- MFA
- Durcissement protection données sensibles

Sécurité IBM i
Projet de remédiation 1

Phase de remédiation 1

Remédiation des failles de "Gravité Haute" et "Effort Faible à Moyen"
Contrôle d'Accès via les Points d'Exit (Granularité Moyenne)

Remédiation effectuée

(Gravité Elevée & Effort Accepté)

- Renforcement des mots de passe (expiration, complexité)
- QSECURITY passage de 30 à 40
- Possibilités restreintes
- Mots de passe par défaut
- Droits publics sur les profils
- Réduction des partages
- Application des PTFs
- Configuration DDM/DRDA durcie
- Profils de groupe comme marqueur de droits et/ou porteur de droits
- Durcissement config SSH

Remédiation non effectuée Risque assumé

(Gravité Elevée & Effort jugé trop Important)

- Partie utilisateur de la liste des bibliothèques
- Droits spéciaux des profils
- Droits sur les bibliothèques et objets
- Droits sur les objets de l'IFS
- Adoption de droits, permutation de profils

Implémentation de SAM

- Utilisation du modèle par défaut, augmenté de JobNotify
- Portée des règles limitée à la bibliothèque et aux répertoires de niveau 1/2/3
- 4 mois en mode simulation / réglage de la config SAM / formation
- Activation du mode bloquant pour les connexions
- Activation partielle du mode bloquant pour les transactions

	Situation testée	Résultat avec droits initiaux	Résultat avec droits usurpés	Remédiation
DB2	Découverte fichiers Db2 potentiellement sensibles	OK	OK	Exit points
	Accès en lecture aux fichiers db2 sensibles	OK	OK	Droits et/ou Exit points
	Téléchargement des fichiers db2 sensibles	OK	OK	Droits et/ou Exit points
	Accès en modification aux fichiers db2 sensibles	OK	OK	Droits et/ou Exit points
SPLF	Découverte fichiers spool potentiellement sensibles	OK	OK	Droits et/ou Exit points
	Accès en lecture aux fichiers spool sensibles	KO	OK	Droits sur OUTQ corrects
IFS	Découverte répertoires partagés	OK	OK	Droits et/ou Exit points
	Navigation dans les répertoires partagés sensibles	OK	OK	Droits et/ou Exit points
	Découverte fichiers stream dans répertoires partagés sensibles	OK	OK	Droits et/ou Exit points
	Accès en lecture aux fichiers stream sensibles	OK	OK	Droits et/ou Exit points
	Téléchargement des fichiers stream sensibles	OK	OK	Droits et/ou Exit points
	Upload de fichiers stream	OK	OK	Droits et/ou Exit points
Profils	Découverte de profils (72)	OK	OK	Exit points
	Découverte de profils en accès public (0)	KO	KO	Droits et/ou Exit points
	Connexion avec des profils avec mot de passe par défaut (12)	OK	OK	Remédiation & contrôle
	Connexion avec des profils puissants avec mot de passe par défaut (10)	**OK+**	OK	Remédiation & contrôle
	Usurpation de droits d'un profil puissant	**OK+**	OK	QSECURITY en 40 - sécurisation jobds
	Ajout *ALLOBJ à mon profil	**OK+**	OK	QSECURITY en 40 - sécurisation jobds
Appli	Programme initial adoptant des droits élevés	OK	OK	Droits
	Découvrir le mécanisme d'enrollement dans l'application	OK	OK	Droits et/ou Exit points
	S'enregistrer soi-même dans l'application	OK	OK	Droits et/ou Exit points
	Intercaler un programme de ligne de commande dans la chaine d'appel du programme initial	OK	OK	Droits et/ou Exit points
	Créer et compiler un programme CL	OK	OK	Droits et/ou Exit points
	Modifier un programme pour qu'il utilise l'adoption de droits	OK	OK	Droits et/ou Exit points
Scripts	Découverte de fichiers Db2 de connexion avec des IP et/ou users et/ou mots de passe	OK	OK	Changer méthodes de connexion
	Découverte de fichiers stream de connexion avec des IP et/ou users et/ou mots de passe	KO	KO	Changer méthodes de connexion
	Accès à d'autres serveurs avec les scripts de connexion découverts	KO	KO	
JOBSCDE	Découverte du planning des travaux	OK	OK	Droits et/ou Exit points
	Ajout d'entrée dans le planning	OK	OK	Droits et/ou Exit points
	Action sur entrée existante dans le planning	KO	OK	Droits et/ou Exit points
Divers	Partage root en lecture	KO	OK	Droits et/ou Exit points
	Partage root en lecture/modification	KO	OK	Droits et/ou Exit points
	Changer le paramètre AUTOSTART d'un protocole	KO	OK	Droits et/ou Exit points
	Permettre à des utilisateurs limités de taper certaines commandes	OK	OK	Droits et/ou Exit points

Contexte

Poste de travail non bridé (incluant ACS complet)

Profil sans droit spécial, sans groupe avec possibilités restreintes

OK Test de violation réussi
KO Test de violation échoué
OK+ Test de violation réussi qui permet en plus une élévation de droits et/ou une usurpation de profil

	Situation testée	Résultat avec droits initiaux	Résultat avec droits usurpés	Remédiation
DB2	Découverte fichiers Db2 potentiellement sensibles	KO	KO	Exit points
	Accès en lecture aux fichiers db2 sensibles	KO	KO	Exit points
	Téléchargement des fichiers db2 sensibles	KO	KO	Exit points
	Accès en modification aux fichiers db2 sensibles	KO	KO	Exit points
SPLF	Découverte fichiers spool potentiellement sensibles	KO	KO	Exit points
	Accès en lecture aux fichiers spool sensibles	KO	KO	Droits sur OUTQ corrects
IFS	Découverte répertoires partagés	KO	KO	Exit points
	Navigation dans les répertoires partagés sensibles	KO	KO	Exit points
	Découverte fichiers stream dans répertoires partagés sensibles	KO	KO	Exit points
	Accès en lecture aux fichiers stream sensibles	KO	KO	Exit points
	Téléchargement des fichiers stream sensibles	KO	KO	Exit points
	Upload de fichiers stream	KO	KO	Exit points
Profils	Découverte de profils (72)	KO	KO	Exit points
	Découverte de profils en accès public (0)	KO	KO	Droits et Exit points
	Connexion avec des profils avec mot de passe par défaut (12)	KO	KO	Remédiation & contrôle
	Connexion avec des profils puissants avec mot de passe par défaut (10)	KO	KO	Remédiation & contrôle
	Usurpation de droits d'un profil puissant	KO	KO	QSECURITY en 40 - sécurisation jobds
	Ajout *ALLOBJ à mon profil	KO	KO	QSECURITY en 40 - sécurisation jobds
Appli	Programme initial adoptant des droits élevés	KO	KO	Droits
	Découvrir le mécanisme d'enrollement dans l'application	KO	KO	Exit points
	S'enregistrer soi-même dans l'application	KO	KO	Exit points
	Intercaler un programme de ligne de commande dans la chaine d'appel du programme initial	OK	OK	Risque assumé
	Créer et compiler un programme CL	KO	KO	Droits
	Modifier un programme pour qu'il utilise l'adoption de droits	KO	KO	Droits
Scripts	Découverte de fichiers Db2 de connexion avec des IP et/ou users et/ou mots de passe	KO	KO	Exit points
	Découverte de fichiers stream de connexion avec des IP et/ou users et/ou mots de passe	KO	KO	Exit points
	Accès à d'autres serveurs avec les scripts de connexion découverts	KO	KO	
JOBSCDE	Découverte du planning des travaux	KO	KO	Exit points
	Ajout d'entrée dans le planning	KO	KO	Droits
	Action sur entrée existante dans le planning	KO	KO	Droits
Divers	Partage root en lecture	KO	KO	Droits
	Partage root en lecture/modification	KO	KO	Droits
	Changer le paramètre AUTOSTART d'un protocole	KO	KO	Droits
	Permettre à des utilisateurs limités de taper certaines commandes	KO	KO	Exit points

Contexte

Poste de travail non bridé (incluant ACS complet)

Profil sans droit spécial, sans groupe avec possibilités restreintes

OK Test de violation réussi
KO Test de violation échoué
OK+ Test de violation réussi qui permet en plus une élévation de droits et/ou une usurpation de profil

Sécurité IBM i
Projet de remédiation 2

Projet de Sécurité IBM i

- Débuté en 2019
- Planification
- POC & Décision sur l'outillage retenu
- Allocation budget
- Allocation ressources internes & externes
- Définition d’un standard interne de Sécurité IBM i
- Macro-objectifs

Macro-Objectifs

Technologies

Macro-Objectifs

	Exit Points	Elévation Droits	Journal	Service SQL	Autre Soft
Intégration du monde IBM i au sein du SOC	SAM ✓	EAM ✓	**MR** ✓ **SIEM** add-on		
Remédiations	SAM		MR ✓	✓	
Reporting évènements & déviations	**SAM**		**MR** ✓	✓	
Contrôle d'Accès	**SAM** ✓				
Contrôle des comptes à privilèges	SAM ✓	**EAM** ✓	✓	✓	
Déploiement & Consolidation				✓	**CDS** ✓
CI/CD	SAM				✓
Rationalisation des pratiques liées aux échanges de données		✓	✓	✓	✓
Renforcement de l'authentification (MFA)	SAM ✓				**MFA** ✓

SAM

EAM

MFA

MR

CDS

SIEM add-on

Projet de Sécurité IBM i

- Chaque action doit à minima contribuer à la mise en conformité avec les directives de sécurité du Groupe

  ✓ tout en recherchant le meilleur équilibre entre la granularité de la règle, sa lisibilité, sa maintenabilité, sa pertinence **dans le temps**

  ✓ et en créant des indicateurs **mesurant** l'efficacité, la non-régression, les déviations possibles, les éventuels effets de bord des actions entreprises

Prérequis

- Chaque profil est membre d'au moins un groupe, porteur de droits et/ou simplement marqueur
- Planification rigoureuse des PTFs, TR et upgrade de versions (PTFs HYPER appliquées rapidement). Incidents de sécurité traités en priorité
- Toute IP fixe est maintenue dans un référentiel avec des infos complémentaires telles que type d'équipement (device, serveur, …), catégorie (SIT, UAT, production, ...), descriptif, compte de service associé

Chronologie

Janv / Mars : Installation de base & formation
Fév / Juin : Reporting de base
Juin / Déc : Intégration SIEM

Janv 22 / Sept 23 :
Amélioration continue

Oct 20 / Oct 21 : Conception moteur du contrôle d'accès & tuning - temps long en mode apprentissage (intègre aussi l'adoption de la mesure par les utilisateurs)

Juin / Déc : Elévation de droits & Intégration au contrôle d'accès

Oct : Red Team - Script trouvé sur machine Linux mal sécurisée, décodage hash du mot de passe, accès sur une prod IBM i en 5250 avec un compte de service.

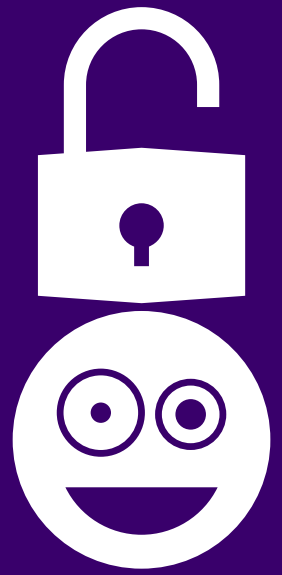
Depuis cette date, tous les autres tests d'intrusion ont été contenus et identifiés.

Août 22 / Août 23 :
Passage contrôle d'accès en mode bloquant

Projet de Sécurité

Changement de paradigme brutal depuis 2022

- Plusieurs vulnérabilités importantes découvertes depuis juin 2023 par Silent Signal et qui existent depuis toujours dans notre OS préféré…..
- Les éditeurs de logiciels sont de plus en plus la cible d’attaques. Quid de nos habitudes envers les tiers de confiance ?!!
- Les possibilités SQL et Open-source deviennent plus nombreuses et complexes
- Enfin, le contexte géopolitique se tend…



Technico : Exit Points

- Complète la Sécurité native
- Couche sollicitée en premier
- Besoin évident de sécurité contextuelle (object, function usage, exit point)
- Définition d'un accès en lecture ? Un SELECT associé à un download ACS n'est pas équivalent au même SELECT dans une application Java…. (exportation de données pour l'un)

Catégories de Points d'Exit en lien avec la Sécurité :

- ceux attachés à l'authentification (FTP Server, REXEC, ODBC, TCP Logon)
- ceux attachés aux transactions, commandes, fonctions, ... (FTP client, FTP Server, REXEC, ODBC, NetServer, Remote Commands, DDM)
- ceux attachés aux commandes (before, after)
- ceux attachés aux ouvertures de fichiers Db2 (valeur d'audit *CHANGE, *ALL) & IFS stmf (attributs *CRTRUNEXIT & *RUNEXIT)
- ceux attachés aux Sockets (communication de bas niveau - IP & Port)
- ceux attachés au moteur SQL (Query Governor, Query Supervisor)
- ceux plus exotiques (job_notify, virus scanning, profile, password, data queues, …)

Contrôle d’accès : les fondations

Listes blanches par typologie d'action ou d'objet touché :

- logon,
- Db2,
- IFS,
- remote commande,
- remote programme,
- data queue

Tout compte utilisateur est membre d'au moins un groupe (porteur de droits ou marqueur simple selon les cas)

Granularité des contrôles adaptée pour un pilotage dans la durée et une évolution aisée selon les nouveaux process et besoins de durcissement

Contrôle d’accès : les fondations

Logon Inbound & Outbound	Compte de service : Profil - IP(s) - Protocole Autre compte : Groupe Profil - IP(s) ou Range – Protocole	NB : NetServer n'a malheureusement pas de point d'exit dédié au logon

DB2	profil/groupe profil - type accès (lecture/modification) - protocole - bibliothèque - fichier (rarement à ce niveau)
IFS	profil/groupe profil - type accès (lecture/modification) - protocole - chemin (rarement au niveau du fichier)
Rmt PGM	profil/groupe profil - protocole - bibliothèque - programme
Rmt CMD	profil/groupe profil - protocole - bibliothèque - commande - paramètres
Fonctions	profil/groupe profil - protocole - fonction
SQL	profil/groupe profil - protocole - partie de la phrase SQL
Commands	profil/groupe profil - travail - IP - Stack (bibliothèque & programme)
Data Queue	profil/groupe profil - type accès (lecture/modification) - bibliothèque - objet *DTAQ

Contrôle d’accès : les plus+

- Les applications SQL clientes doivent montrer pattes blanches !
- Contrôle renforcé via les registres clients

- Contrôle des commandes lançant du SQL + Contrôle contextuel des phrases SQL

- Commandes sensibles bloquées sauf avec élévation de droit + ticket valide
  - Exemples: CHGSYSVAL, ADDLNK, EDTF, UPDDTA, STRSST, …

- Maintenance d'une piste d'audit des utilisateurs supprimés
- Forcer certains utilisateurs à fermer la session avec l’option LOG(*LIST)

- Construction de la log :
  - transactions rejetées
  - transactions acceptées dans des contextes particuliers :
    - profils puissants
    - recherche de chaîne de caractère potentiellement sensible dans la string
    - autres critères (IP, stack, debug temporaire, etc…)

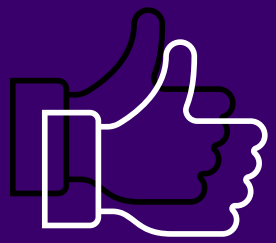
Contrôle d’accès : les plus+

- TELNET vs Travail interactif….
- Point d'exit JOB_NOTIFY avec capacité de blocage d'ouverture de session
- Etanchéité des environnements (PROD-PROD, UAT-UAT, SIT-SIT)
- Contrôle renforcé pour les passerelles entre environnements différents

- Contrôle des valeurs de paramètres sensibles sur des commandes telles que : SBMJOB, ADDLNK, EDTF, ADDJOBSCDE, CHGJOBSCDE, …

- Fin du contournement de l'outil de DevOps : Blocage des commandes qualifiées CPYSRCF, RMVM, RNMM, STRRLU, STRSDA, STRSEU
- Blocage des modifications de source pour les bibliothèques et répertoires non référencés en DevOps

- Ajustement dynamique de priorités et de l’activation du multi-processing en fonction de critères tels que le current user, le job, l'IP



Contrôle d’accès : les plus+

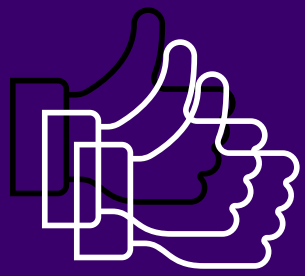
- Console surveillant toutes les partitions de façon globalisée avec auto-refresh

  ou …
- Sonde sur la log

  ➔ Réactivité en mode bloquant impérative

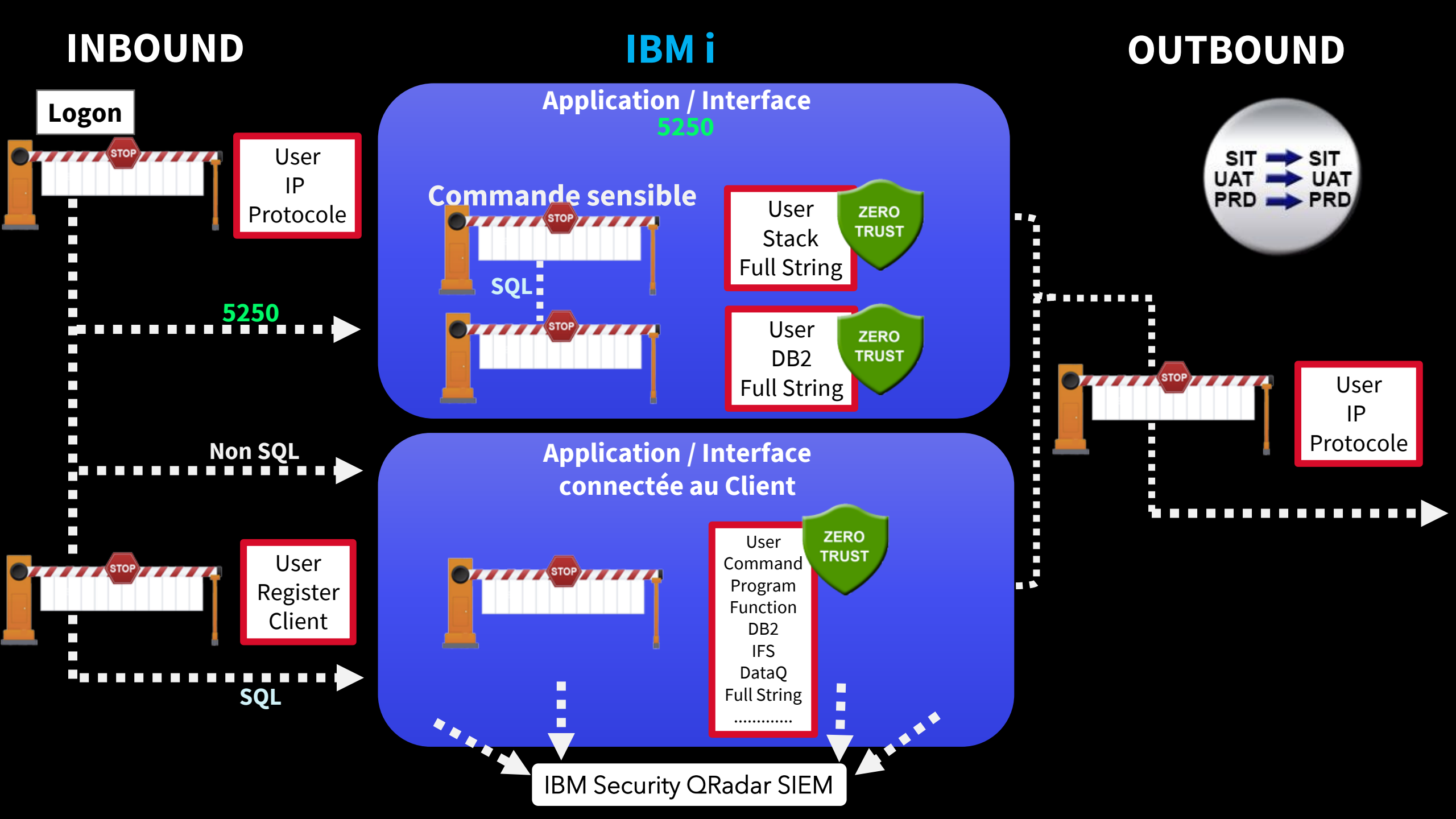
- Modèle de configuration maintenu sur une machine de référence
- Chaque règle est taguée sur une combinaison de 2 valeurs
  - Type partition: SIT, UAT, PROD, Infocentre, backup - Prod, non Prod - toutes
  - Filiale et/ou core banking : pays1, pays2, pays3, …. - soft1, soft2, soft3, ….- tous pays, tous soft
- Facilité de déploiement, confiance, lisibilité

Return On Investment



Elévation de Droits

- Contrôle des utilisateurs à privilèges
- Réduction de leurs droits permanents
- Elévation de droits à la demande et contrôlée par un numéro de ticket (ticket valide, attribué à l'utilisateur et la partition, avec option plage de dates)
- En fin de session élevée : envoi de la piste d'audit dans le ticket (joblog enrichie des SQL, commandes, écrans)


INBOUND
IBM i
OUTBOUND
Logon
User
IP
Protocole
5250
Non SQL
SQL
User
Register
Client
Application / Interface
5250
Commande sensible
SQL
User
Stack
Full String
User
DB2
Full String
ZERO TRUST
Application / Interface
connectée au Client
User
Command
Program
Function
DB2
IFS
DataQ
Full String
.....
SIT → SIT
UAT → UAT
PRD → PRD
User
IP
Protocole
IBM Security QRadar SIEM

Guy Marmorat – Expert en Sécurité IBM i – Le 10 octobre 2024