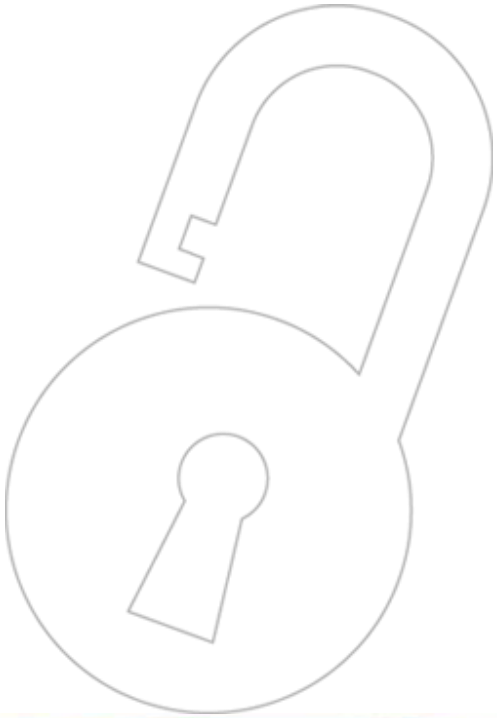


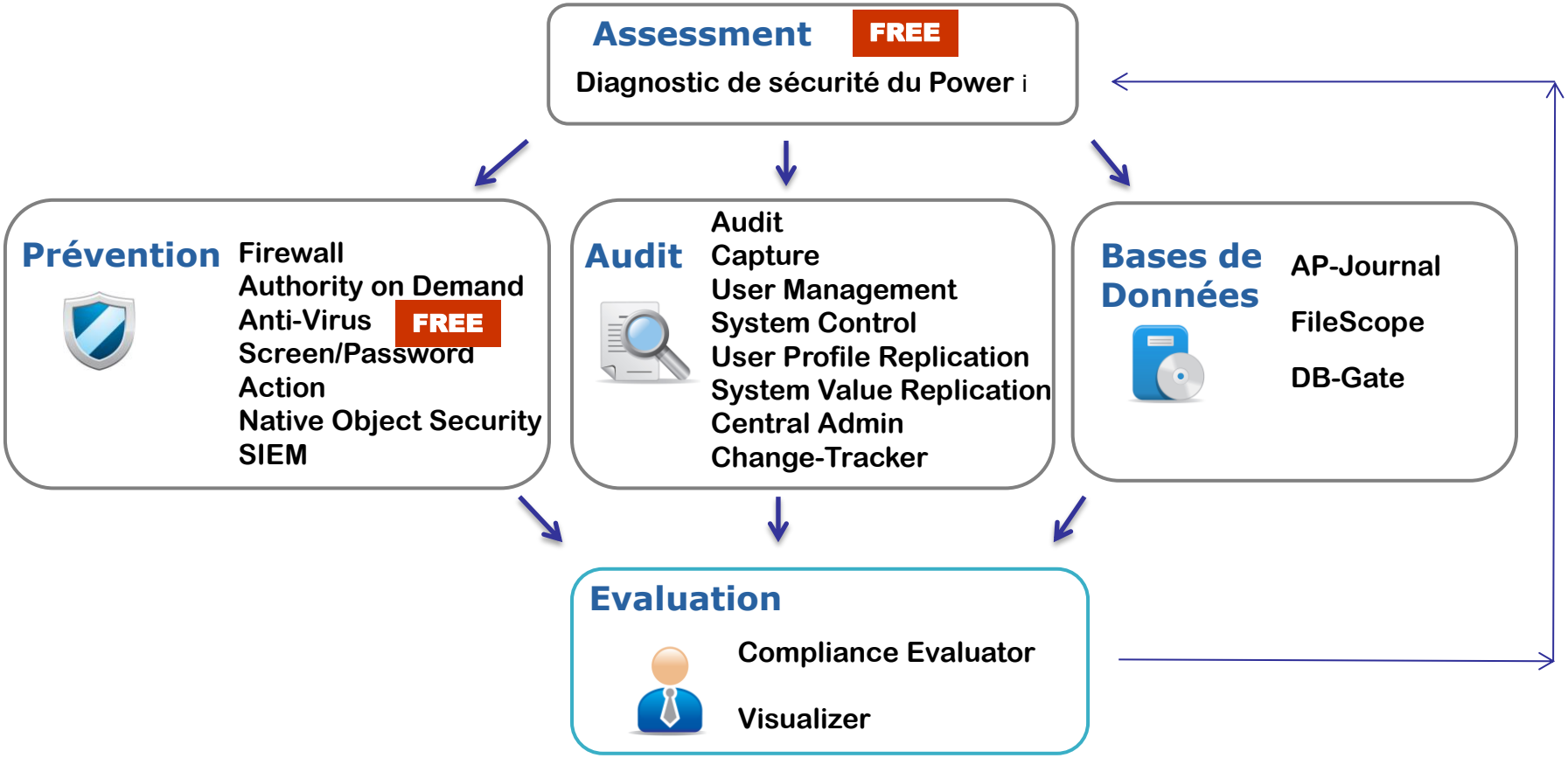
i Security – Bien plus qu'un Firewall pour IBM i

Présentation avec Démos

iSecurity

RAZ-LEE
Experts @ Security and Compliance

La richesse fonctionnelle fait la différence



Qui sommes nous – à propos de RazLee

- Editeur de logiciels de sécurité de renom international
- Fondé en 1983, 100% axé sur IBM Power i
- 3 lignes de produits:
  - iSecurity Sécurité de **l'infrastructure informatique**
  - iSecurity Sécurité pour les **données utilisateurs**
  - Outils: Gestionnaire de fichiers, DB GATE-Accès Bases de données externes, Outils de Tuning, etc.
- Plus de 12.000 licences installées dans plus de 30 pays
- Réseau de distribution mondial
- IBM Advanced Business Partner
- Raz-Lee Security GmbH, Filiale directe en Europe depuis 2011 couvre également la clientèle de langue française

Nos clients

- Banques / Assurances
- Automobile
- Chimie / Pharmacie
- Production et commerce
- Services

Qui nous pose des problèmes ?

Près de 90% des problèmes de sécurité sur les systèmes IBM i proviennent du fait de collaborateurs internes

Et le reste ?

x% de collaborateurs externes

et

x% de „Hacker“

Pourquoi des problèmes, à cause de qui ?

Les inexpérimentés	**Font des essais - ne sont pas ralentis par la connaissance et ne se rendent compte de rien**
Les fanas	**Il leur faut du neuf…même au bureau on essaie d'installer des nouveautés**
Les égoïstes	**Connaissent les règles mais les transgressent pour leur propre intérêt**
Les saboteurs	**agissent avec l'intention délibérée de provoquer des dégâts**

Ce qui est grave, c'est que …

Nous

ne

remarquons

rien !

…ou du moins pas de suite

iSecurity

RAZ-LEE
Experts @ Security and Compliance

Pourquoi la transparence et le temps réel?

La transparence est le premier pas vers la sécurité

La transparence est la base de la conformité

Seules les informations fournies en temps réel seront utiles

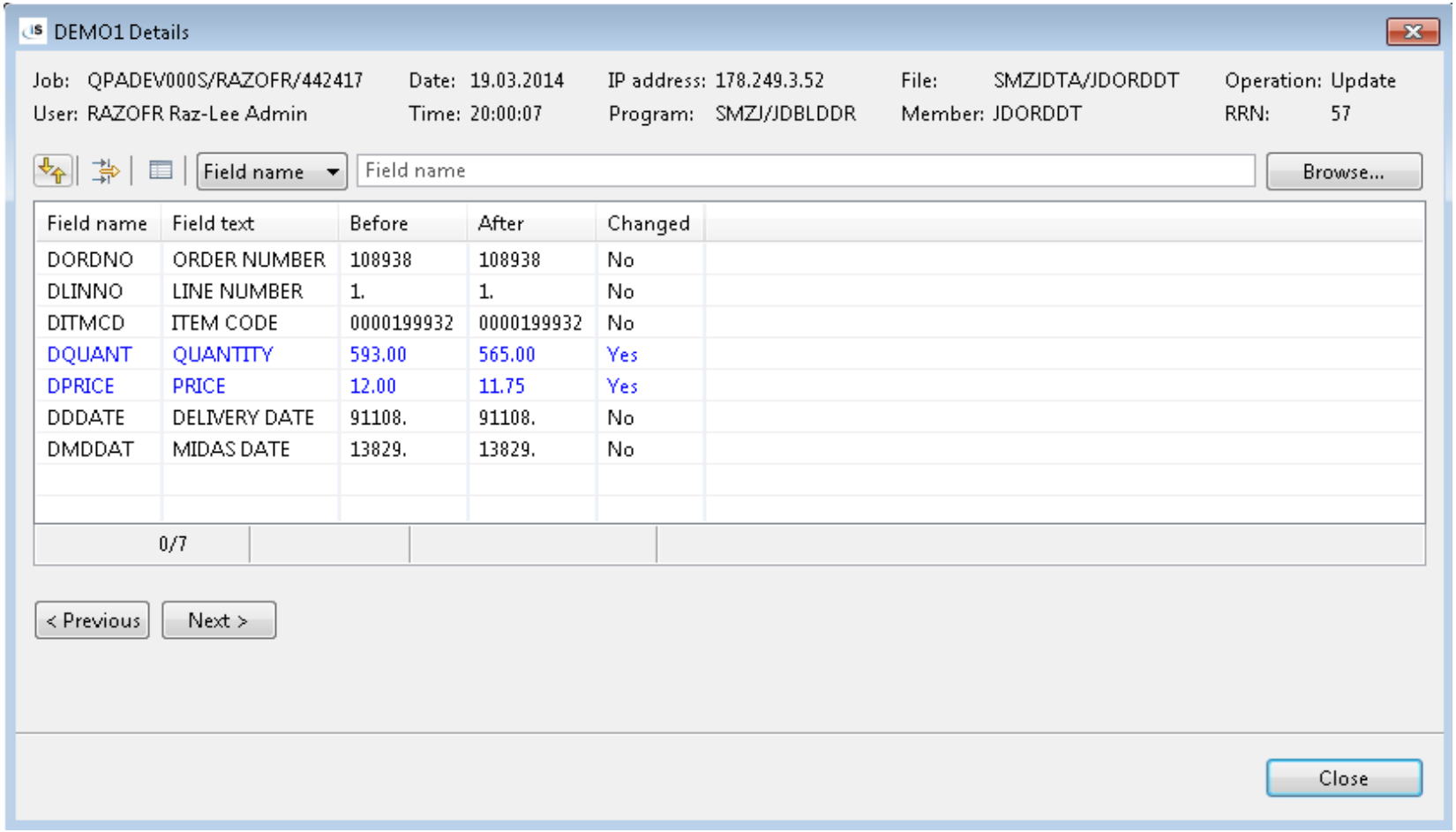
Exemple : accès SQL

- **Date:** 19.03.2014
- **Time:** 17:24:44
- **Result:** Rejected
- **Operation mode:** *FYI
- **Server:** Database Server - SQL access & Showcase
- **Decision level:** OBNTV=Object authority-Native
- **Message ID:** GRE6541
- **Text:** *SQL *FYI* Denied for RENGEL to SMZ1/DEMOPF *FILE. SQL: SELECT ITEMNO,SDESCR,VEND#,QTYOH,QTYOH,QTYOO,PRICE,PRCDAT,DESCR FROM SMZ1/DEMOPF FOR FETCH ONLY. Function READ_RCD. IP address 178.249.3.52. Interface CWBTF.EXE - IBM i Access-Datenübertragung (ver V7R1M0SI00). The examined security rule was for file SMZ1/DEMOPF user RENGEL operation READ.

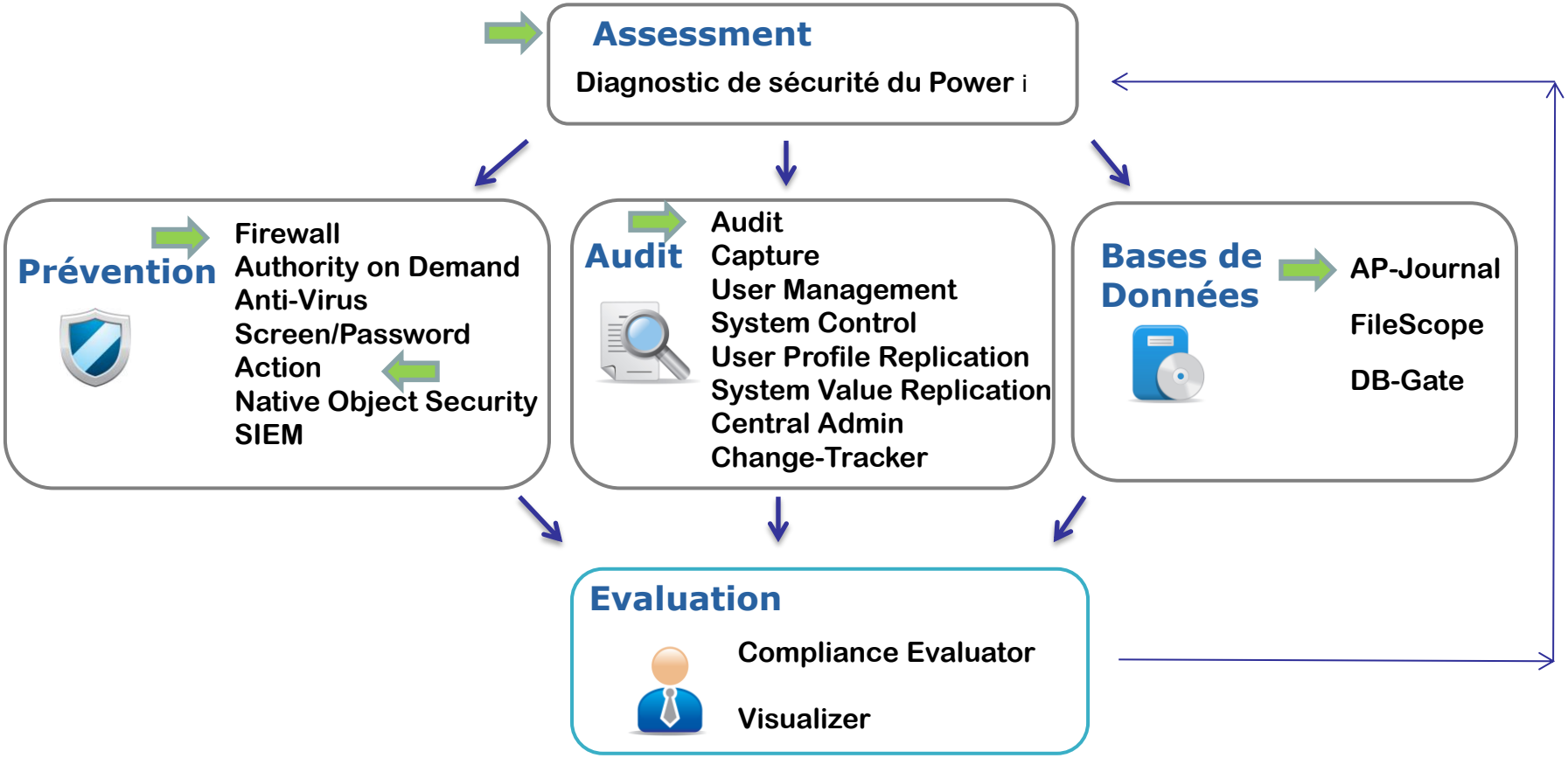
Exemple : modification de valeur système

- **Date:** 19.03.2014
- **Time:** 08:02:01
- **User:** RENGEL1
- **Type/Sub type:** SV/A
- **Type text:** A system value was changed.
- **Program:** RE_AUD
- **Job:** 442119/RENGEL1/RE_AUD
- **Message ID:** MSV0100
- **Text:** *SECURITY User RENGEL1; System value QALWOBJRST changed to *ALL from *ALWPTF. Job 442119/RENGEL1/RE_AUD.

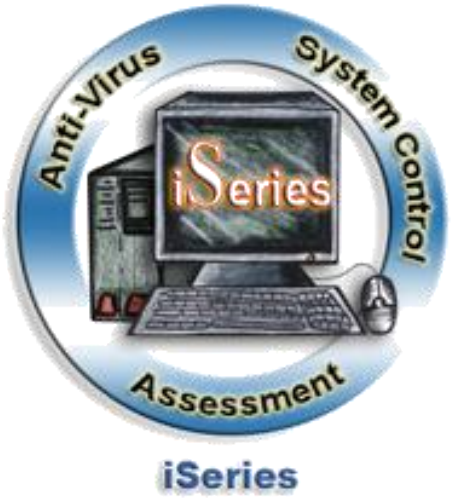
Modification dans une base de données



Priorités pour aujourd'hui



Module : Assessment



- **Analyse gratuite et complète de l'état de sécurité de vos Power i**
- **Edition instantanée d'un compte rendu détaillé sous forme d'un document HTML, sans installer de programme sur votre Power i**
- **Information sur vos risques et recommandations**
- **Aperçu graphique de l'état de sécurité de votre Power i**
- **Documentation des améliorations apportées par les mesures de correction.**

iSecurity

RAZ-LEE
Experts @ Security and Compliance

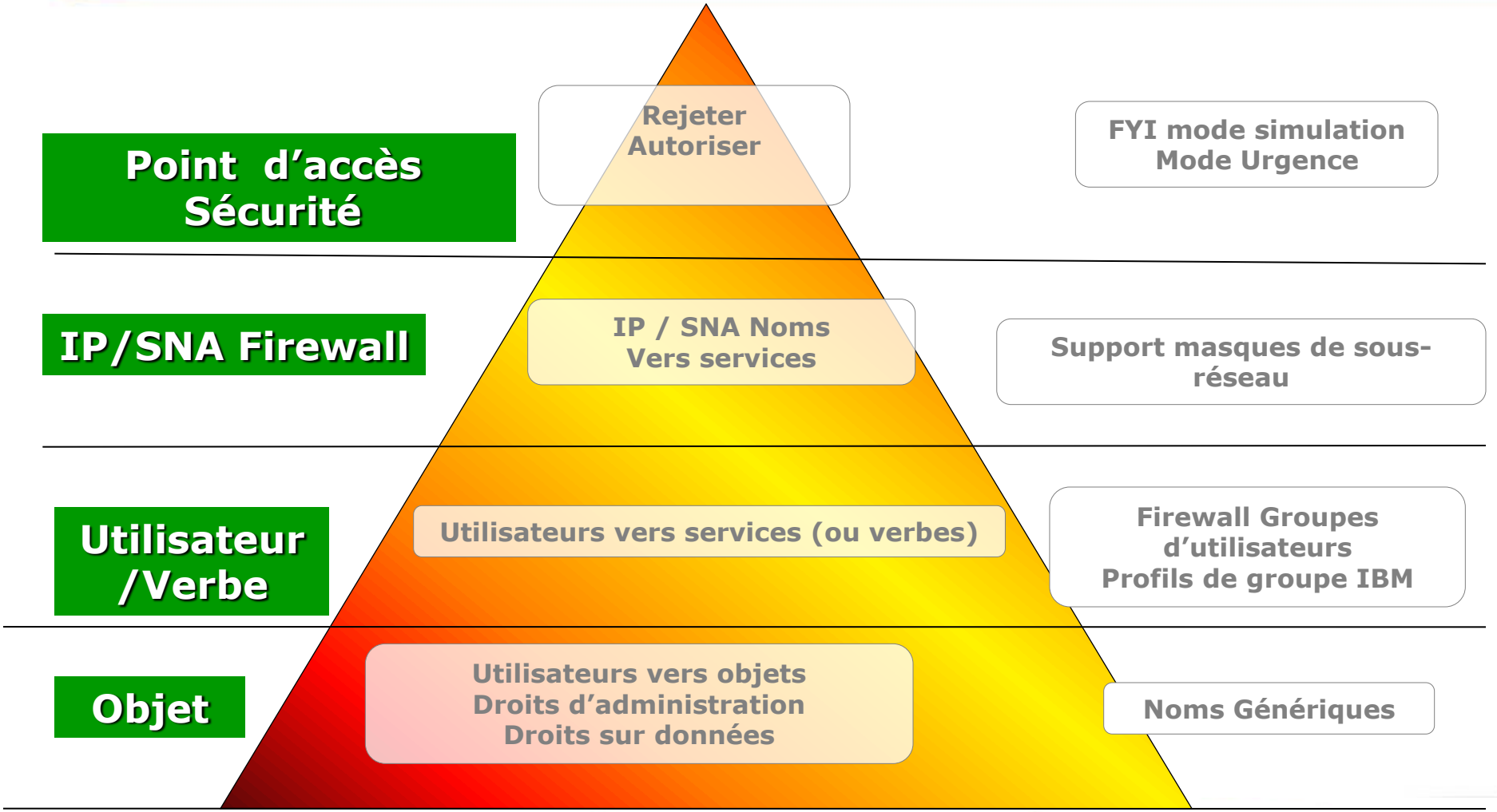
Module : Firewall

- Protège des accès à partir de l'extérieur du Power i
- Couvre 100% des points d'accès critiques (y compris ODBC, Telnet, FTP, Remote Command, SSH, DBOPEN, etc.)
- Protection au niveau Serveur, Adresses, Utilisateurs jusqu'au niveau de l'objet – extrêmement efficace même dans de vastes environnements avec des règles de protection complexes
- Gestion de groupes par utilisateurs, applications, sites ou encore en fonction de plages horaires
- Protection des connexions IP entrantes et sortantes

iSecurity

RAZ-LEE
Experts @ Security and Compliance

Module : Firewall



iSecurity

RAZ-LEE
Experts @ Security and Compliance

Module : Audit

- **Affiche toutes les activités en cours sur Power i dans un format facilement lisible et initie en temps réel les actions à entreprendre pour faire face aux problèmes de sécurité potentiels.**
- **Dispose d'un générateur de rapports puissant avec plus de 200 rapports prédéfinis.**
- **Possibilité d'afficher divers types d'audits à partir de requêtes simples**
- **Un assistant permet de définir rapidement des requêtes sans programmation**

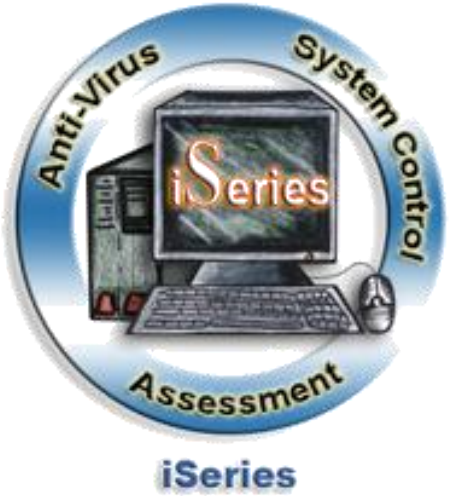
Module : Action

- Système très performant de Détection d'Intrusions (IDS) : déclenche des alertes et lance automatiquement les fonctions de trigger
- Constitue une réponse interactive aux alertes provenant des modules Firewall, Audit, AP-Journal et Screen
- Messages d'alerte par mail, message i/OS, SMS ou Pager
- Générateur d'instructions CL pour définir les fonctions de réaction.
- Intégration à SIEM-pour lancer automatiquement des alertes via Syslog ou SNMP (par exemple vers Arcsight, IBM Tivoli, RSA envision, OP OpenView, …)

Module : AP-Journal

- Aide à automatiser l'administration des modifications de la base à travers la documentation et des rapports d'exceptions dans le journal de base de données
- Analyse ad hoc des modifications dans les fichiers de base de données avec options de filtrage
- Regroupement des fichiers liés dans des applications avec des options de filtrage
- Stockage à long terme et suivi de processus avec Business Analyse
- Notifications et actions automatiques selon filtres

Autres modules



- **Visualizer**
  - **Outil de Business Intelligence sur PC pour analyse rapide sous forme graphique de la base d'informations d'iSecurity**
  - **Regroupe les informations des modules Firewall, Journal, et Audit avec analyse en profondeur (DrillDown) jusqu'au niveau objet**
- **Capture**
  - **Enregistrement des sessions 5250 pour la documentation ou pour tracer des processus à la demande**
  - **Définition simple des règles d'enregistrement des diverses sessions**
  - **Recherche rapide grâce à un moteur de recherche puissant (recherche full text)**
- **Authority on Demand**
  - **Attribution de droits fondé sur des règles d'autorisations selon besoins avec saisie de code PIN**
  - **Enregistrement complet des activités à travers Audit et Capture**

iSecurity

RAZ-LEE
Experts @ Security and Compliance

Autres modules

- **Anti-Virus**
  - **Détection en temps réel des virus avec mise à jour quotidienne des signatures de virus depuis Clam AV**
  - **Analyse des objets IFS et objets i/OS suspects**
- **Compliance Evaluator**
  - **Définition des règles de conformité propres à l'entreprise avec définition de requêtes pour l'évaluation de l'état de conformité**
  - **Présentation Excel de paramètres de sécurité avec évaluation de l'ensemble du système**
- **Replication**
  - **Réplication de profils utilisateurs ou valeurs systèmes selon filtres pour des systèmes ou partitions multiples**

Le Module: Compliance Evaluator

Thursday, April 16, 2009 — Report Filter: T..... Summary (NonBlanks).... Exceptions

iSecurity Compliance Evaluator

Sample Counts and Values Reports

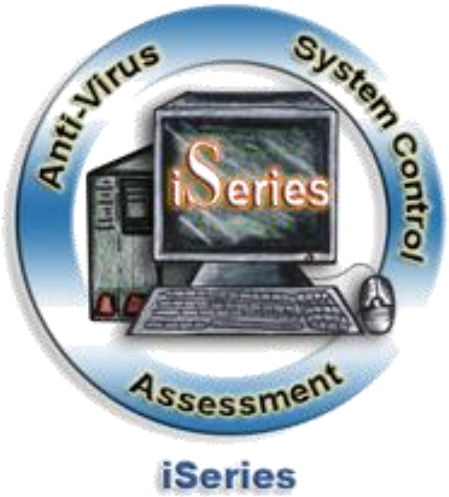
System:	S44K1246	S720
Compliance Rating:	75%	57%

Item	Topic	Name	Relative Importance	Current Value	Optimal Value	Rank for Topic	Current Value	Optimal Value	Rank for Topic
Network Activity			19%			74%			76%
CRTUP - Create User Profile				0	0-5		0	0-5	
FTPLOG - FTP Server Logon (*)				2	0-50		37	0-50	
FILSRV - File Server (*)				35	0-25		14	0-25	
RMTSRV - Remote				35	0-25		143	0-100	
User Profile Attributes			40%			97%			60%
User Profiles with *ALLOBJ				93	0-100		116	0-100	
Users with no password				17	0-15		70	0-70	
Powerful Users				88	0-100		107	0-100	
All System Values Information			29%			49%			48%
Previous end of system indicator	*SYSCTL	QABNORMSW		0	1		0	0	
Accounting level	*MSG	QACGLVL		*JOB *PRINT...	*NONE		0	0	
Initial number of active jobs	*ALC	QACTJOB		45			20		
Additional number of active jobs	*ALC	QADLACTJ		30			10		
Spooling ctl block additional	*ALC	QADLSPLA		2048			2048		
Additional number of total jobs	*ALC	QADLTOTJ		50			10		
Allow object restore option	*SEC	QALWOBJRS		*ALL	*ALL		*ALL	*ALL	

iSecurity

RAZ-LEE
Experts @ Security and Compliance

Autres modules



- **Native Object Security**
  - **Restauration des droits des objets dans les bibliothèques**
- **System Control**
  - **Contrôle l'environnement du Power i : utilisation CPU capacité disques, jobs, file d'attente de messages avec exécutions d'actions correspondantes**
- **User Management**
  - **Gestion d'utilisateurs avec activation/désactivation d'utilisateurs**
- **Password**
  - **Intègre et complète la gestion des mots de passe utilisateurs prévue dans l' i/OS**
- **Screen**
  - **Economiseur d'écrans pour sessions interactives avec gestion souple de critères comme des dates et horaires d'utilisation, interruption/arrêt de travaux…**

Autres produits

- **FileScope**
  - **Editeur de base de données Unicode multifonction (gestion de vues, jointures, éditeur unitaire, modifications en série, conversion de données, fonction undo)**
- **iBi Visualizer**
  - **Vue graphique de vos données avec Drill-down simple et rapide**
- **DB-Gate**
  - **Accès natif sur des bases de données externes (incl. Excel)**
  - **Support de STRSQL et embedded SQL**
  - **Integre l'autentification et la journalisation**
- **Change Tracker**
  - **Détection de changements en temps réel, suivi des modifications avec générateur de rapport et planificateur intégré**

Nous vous remercions pour votre attention !

Raz-Lee Security GmbH
Schulstr. 32
D 96472 Rödental

En France :
11 Rue André Malraux
67170 BRUMATH
Tél : 03 88 51 92 71
andre.meyer@razlee.com
www.razlee.fr

iSecurity

RAZ-LEE
Experts @ Security and Compliance