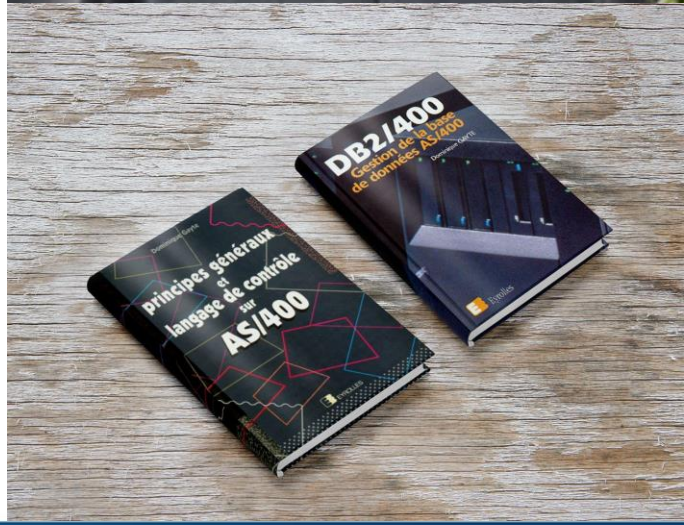
Dominique GAYTE
06 30 17 02 55
dominique@gayte.it - https://i.gayte.it

STR-iCT

Sécurisation avancée et traçabilité des IBM i

Dominique GAYTE

- Docteur ès sciences
- Intervenant « AS/400 » depuis 1990
- Expert
  - Sécurité
  - Développements complexes
- Auteur de plusieurs livres sur le sujet
- Formateur



Dominique GAYTE - suite

- Distingué par IBM comme IBM Champion
- Décerné aux experts reconnus par IBM

I.GAYTE.IT

- Expertise IBM i
- Focus sur la Sécurité
- Edition de logiciels

- Reconnu pour son Innovation et sa Recherche

Securit.i 2025

- Evènement Sécurité IBM i
  - https://i.gayte.it/category/securiti/
  - https://www.youtube.com/@igayteit
- Du mardi 16 septembre 2025 14H00
- Au mercredi 17 septembre 2025 17H00
- À Montpellier

Les enjeux de la Sécurité et de la traçabilité sur IBM i

IBM i et Sécurité

- Les IBM i ont souvent une Sécurité bâtie sur les principes des années 1990
  - À l'époque, peu ou pas de réseaux
  - Pas d'Internet
  - Pas de hackers, par de ransomware
- Mais ils sont souvent au cœur du système d'information de l'entreprise
  - 100 % du CA (ou de l'activité) passe généralement par ses applications
    - Comptabilité
    - Stocks
    - Gestion commerciale
    - Production
    - …
- Ils sont donc critiques et n'ont pas une configuration de leur Sécurité adaptée
- Ils sont souvent exclus ou méconnus des logiciels qui gèrent la Sécurité du réseau (SIEM)

La traçabilité

- Conservation d'un historique d'actions qui se sont produites
  - Au niveau des évènements
  - Sur les données
- Au cœur des normes
  - **NIS2**

Avec NIS2 les entreprises doivent s'organiser afin de pouvoir notifier un incident dans les 24 heures suivant sa détection et devront transmettre les preuves détaillées sous un mois aux autorités compétentes (l'ANSSI pour la France). Cela implique donc une forte capacité de traçabilité et de réactivité. Pour autant bon nombre d'organisations ne sont pas encore en mesure de produire les reportings exigés

La traçabilité

- Conservation d’un historique d’actions qui se sont produites
  - Au niveau des évènements
  - Sur les données
- Au cœur des normes
- **DORA** : impose une stratégie de résilience opérationnelle numérique

Les entités financières doivent définir et mettre en œuvre un processus de gestion des incidents TIC afin de détecter, de gérer et de notifier les incidents TIC.

Accès externes

- Lors de mes audits, je constate souvent que les comptes des services ne sont pas maitrisés
- Ce sont des profils utilisés par des applications clientes, à distance, qui accèdent à l'IBM i
  - ODBC, JDBC
  - FTP
  - Partage de fichiers (NetServer)
  - Web Services
- Souvent profil et mot de passe codés en clair !
  - Et souvent profil disposant de droits spéciaux (*ALLOBJ !)
- La maitrise de ces comptes de service est essentielle !
  - Quand est-ce qu'il y a des connexions externes ?
  - Pour quoi faire ?
  - Avec quel profil ?
  - Où est stocké le mot de passe (en clair) ?
  - Comment le modifier s'il est compromis
  - Comment renforcer le niveau de mot de passe (V7Rnext suppression des mots de passe en level 0 ou 1 !)
- Seule la traçabilité peut vous aider à y voir clair !

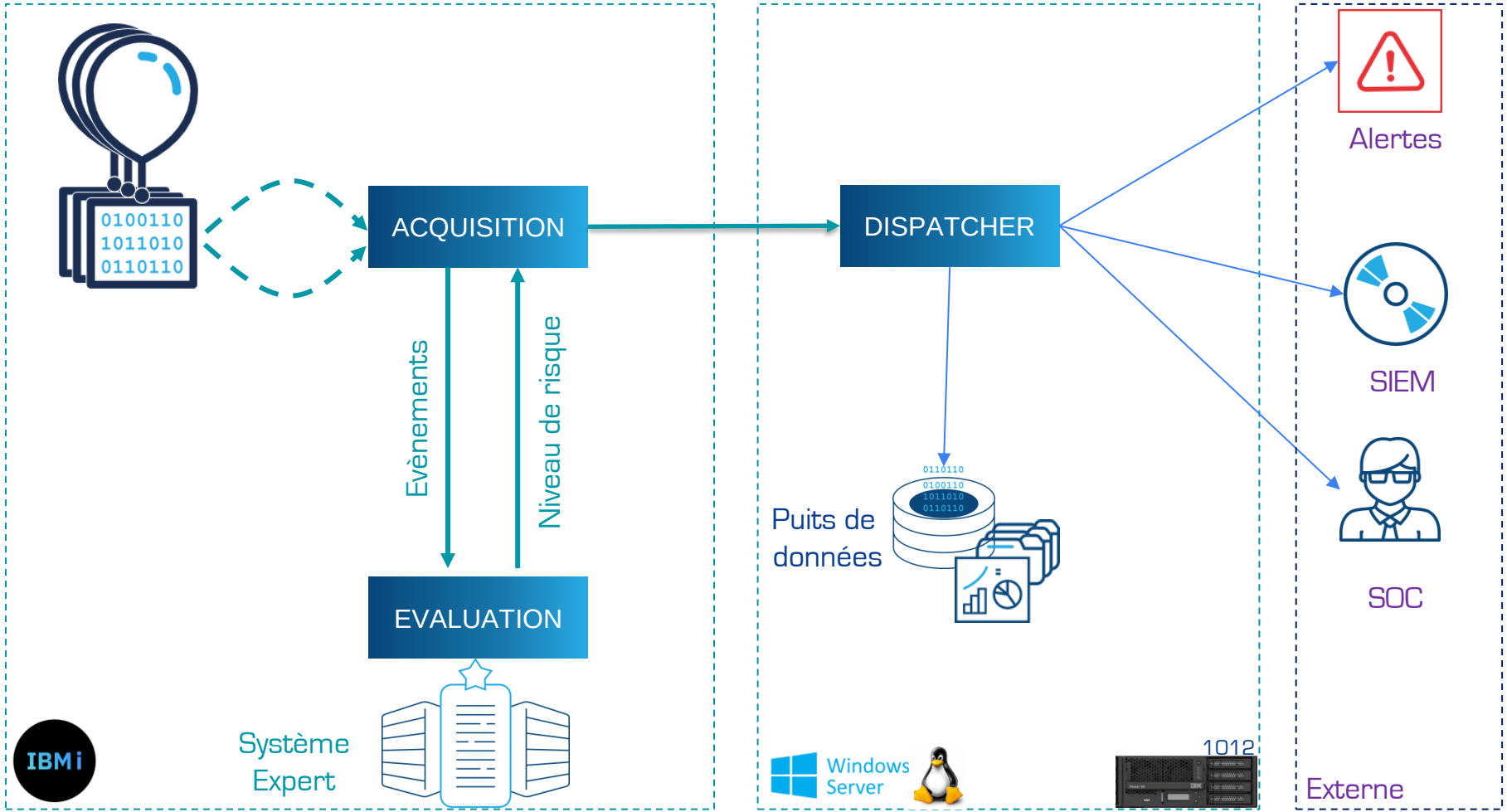
IBM i et traçabilité

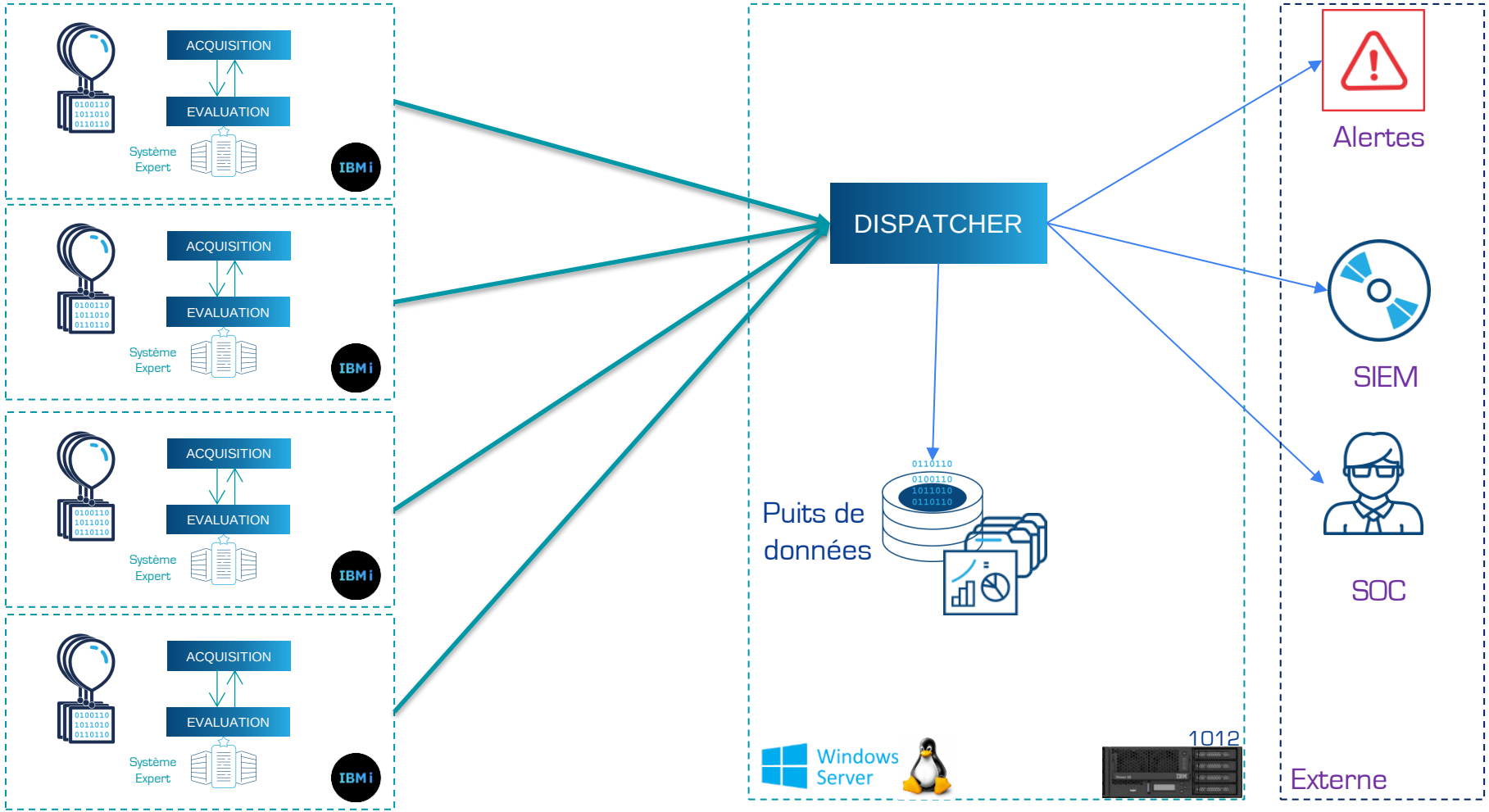
- L’IBM i est très bavard pour qui sait l’écouter
- Il produit (ou peut produire) une énorme quantité de données de traçabilité
- Mais
  - Pas toujours simple à retrouver
  - Pas toujours simple à lire (décrypter)
  - Pas toujours simple à configurer
- Rarement conservé de manière structurée
  - Quand on a besoin de l’information, elle n’est plus disponible
    - Récepteurs de journaux supprimés tous les jours, où même à la volée


STR-iCT

STR-iCT

- STR-iCT est un logiciel dédié à la sécurisation et à la traçabilité des IBM i
- Il détecte les évènements qui sont en lien avec la Sécurité ou la traçabilité
- Un Système Expert unique évalue le risque de chacun de ces évènements
- Les données sont ensuite transmises à un dispatcher qui va déterminer les actions à réaliser, selon la configuration du client
    - Archivage dans un puits de données centralisant toutes les partitions (avec interface de consultation graphique)
    - Déclenchement d'alerte
    - Envoi éventuel vers un SIEM externe (Qradar, Sentinel, Splunk…)
    - Transmission à un SOC externe (Security Operation Center)


0100110
1011010
0110110
ACQUISITION
Evènements
Niveau de risque
EVALUATION
Système
Expert
IBMi
DISPATCHER
Puits de
données
0110110
0100110
1011010
0110110
Windows
Server
1012
Alertes
SIEM
SOC
Externe


ACQUISITION
EVALUATION
Système Expert
IBMi
ACQUISITION
EVALUATION
Système Expert
IBMi
ACQUISITION
EVALUATION
Système Expert
IBMi
ACQUISITION
EVALUATION
Système Expert
IBMi
DISPATCHER
Puits de données
Windows Server
1012
Alertes
SIEM
SOC
Externe

Sondes disponibles : journal d’audit

- Erreur de mot de passe
- Tentative de violation d’accès
- Suppression d’objets
- Connexion socket (port IP inexistant)
- Erreur de mot de passe NetServer
- Connexions SSO
- SST/DST : profils, actions
- Profils utilisateur
- Suppressions objets/IFS/DLO
- Gestion d’audit
- Gestion des valeurs système
- PTF
- Adoption de droits
- Gestion d’objets
- Restauration d’objets
- Attributs du réseau
- Commandes

Sondes disponibles : autres sondes

- Les tentatives d’intrusions détectées par l’IDS (système de détection d’intrusions)
  - Gestion des faux positifs
- Les points d’exit
  - Accès FTP
  - Les accès ODBC/JDBC
  - Les accès à l’IFS
- Traçabilité base de données (Legacy)
  - Modification des zones d’un fichier quelle qu’en soit l’origine
- Et bien d’autres encore…

Sondes en cours de développement

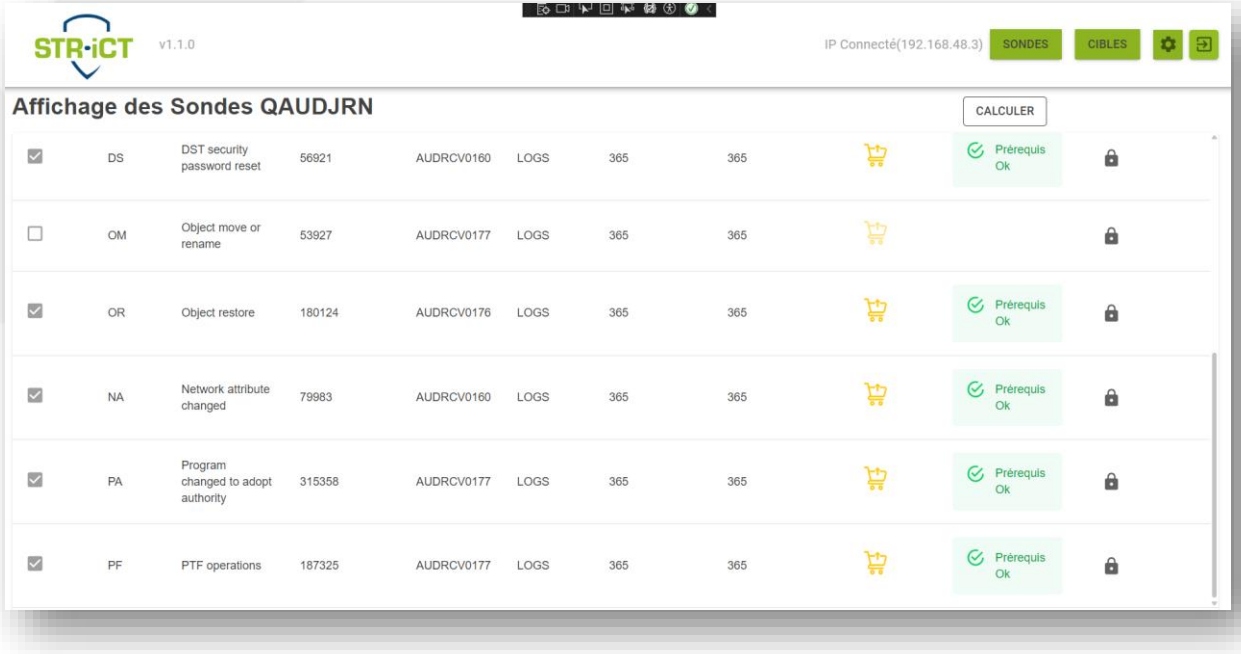
- Audit
  - Profils
  - Valeurs système
  - Bonnes pratiques
  - …
- Intégration dans Assure Security (CILASOFT-Guy MARMORAT)

Le Système Expert

- Objectif : détermination du risque induit par l'évènement
- Toute notre expérience
- Toutes les connaissances en cybersécurité
- Tous les mécanismes d'attaques identifiés par notre pot de miel sur Internet
  - Jusqu'à ~~30 000~~ ~~50 000~~ 100 000 attaques par jour
  - Une énorme base de connaissances

Configuration des sondes

- Toute la configuration est réalisée en graphique

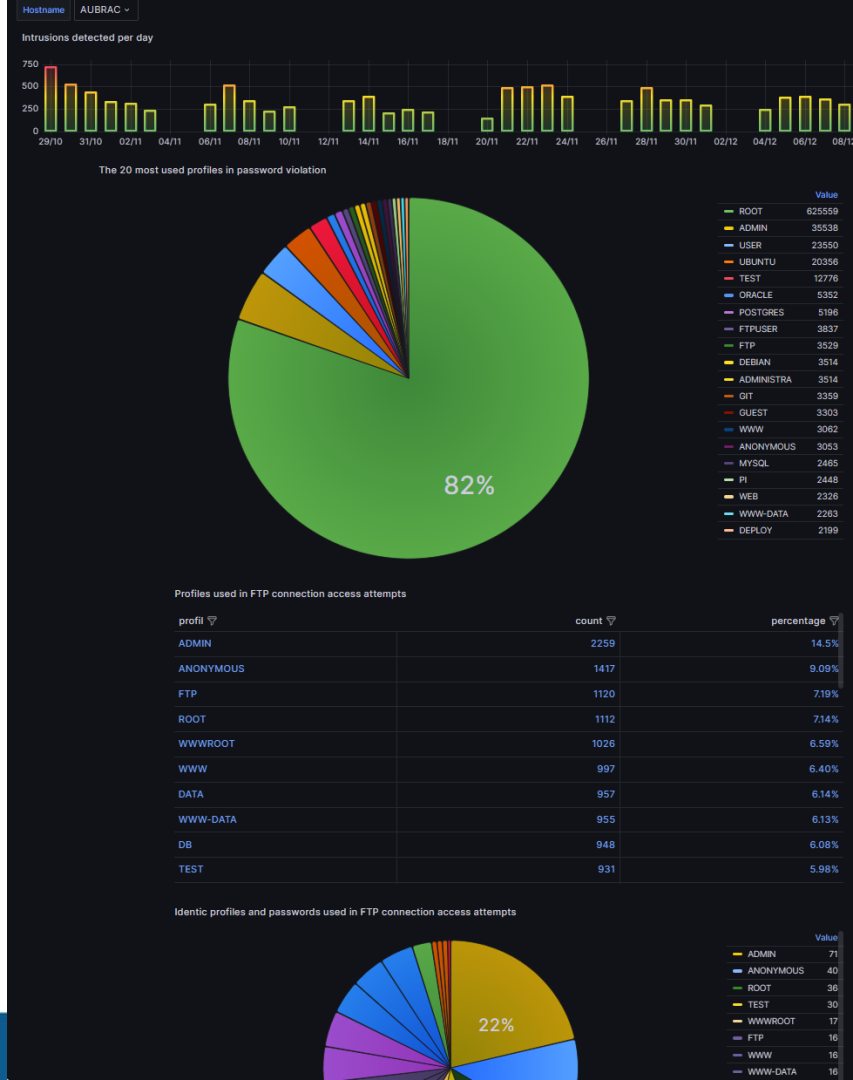


Le dispatcher

- Réceptionne les données (Web Service)
- En fonction de la configuration
  - Enregistre en local dans un puits de données (avec interface graphique de restitution)
  - Envoie vers un SIEM externe (Microsoft Sentinel, Elastic Search (ELK) , IBM Qradar, Splunk…) ou vers notre SiEM STR-iCT
  - En Web Services ou en SYSLOG
  - Déclenche des alertes

L’interface graphique du puits de données

- Basée sur Grafana
- Graphique avec possibilités d’interrogation en SQL
- Agrégation des données de plusieurs IBM i
- Facilement adaptable



Êtes-vous SiEM ou SIEM ?

- Security Information Event Manager
- Les SIEM gèrent la Sécurité de tout le réseau
  - Sauf IBM i en général !
- STR-iCT est un véritable SIEM à part entière dédié à l'IBM i
  - Acquisition des données, détermination du risque, alerte, reporting
- SiEM : STR-iCT for IBM i Event Manager
- Mais STR-iCT sait aussi communiquer avec les SIEM du marché

Licences

- Une licence par partition IBM i
  - Partition de backup intégrée à la partition principale
- Soit en mode licence perpétuelle
  - Maintenance annuelle obligatoire
- Soit en mode souscription (location annuelle)
  - Maintenance incluse
- Dépend du type IBM i (P05, P10…)

Merci

Dominique GAYTE
06 30 17 02 55
dominique@gayte.it - https://i.gayte.it

I.GAYTE.IT