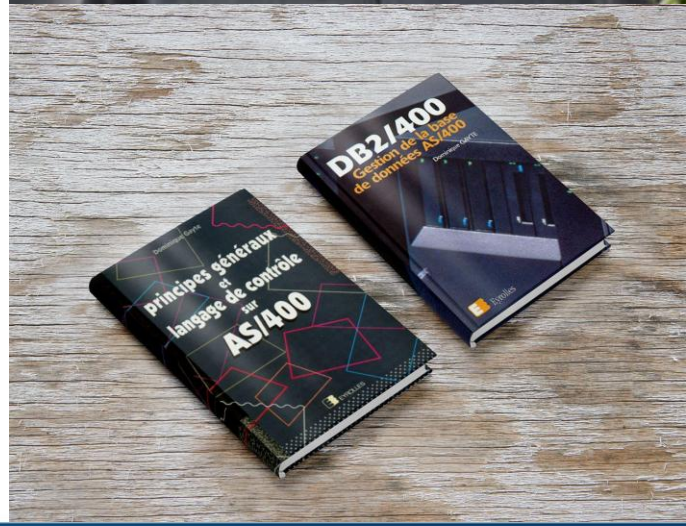
Dominique GAYTE
06 30 17 02 55
dominique@gayte.it - https://i.gayte.it

STR-iCT

Sécurisation avancée et traçabilité des IBM i

Dominique GAYTE

- Docteur ès sciences
- Intervenant « AS/400 » depuis 1990
- Formateur
- Expert Sécurité IBM i
  - Plus de 350 partitions IBM i auditées
  - Remédiations (sécurisation)
    - Base de données
    - Mots de passe
    - Cryptage de données
  - MFA (V7R6)
- Adore les développements complexes
- Auteur de plusieurs livres sur le sujet



Dominique GAYTE - suite

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

I.GAYTE.IT

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

- Reconnu pour son Innovation et sa Recherche

Securit.i 2026

- Evènement international Sécurité IBM i
  - https://i.gayte.it/evenement-securit-i-securite-ibm-i/
  - https://www.youtube.com/@igayteit
- Du mardi 09 septembre 2025 09H00
- Au mercredi 10 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 règlementations
  - NIS2
  - DORA
  - RGPD

Me Cathie-Rosalie Joly - Avocate

NIS2

Volet technique notamment avec le SOC/SIEM

- Security Operations Center
- Security Information and Event Management

1.Détection des cybermenaces

1. **SOC** : assure la surveillance continue des systèmes, la détection des comportements anormaux, et la réponse aux incidents.
2. **SIEM** : collecte, corrèle et analyse les logs pour identifier les menaces en temps réel.

2.Gestion des incidents

1. **SIEM** : permet de détecter les incidents via des alertes basées sur des corrélations d'événements.
2. **SOC** : coordonne la réponse aux incidents, l'analyse post-mortem et la communication avec l'ANSSI.

3.Évaluation et gestion des risques (classification et notification)

1. **SIEM** : fournit des données utiles pour l'analyse des risques (fréquence, gravité, typologie des incidents).
2. **SOC** : contribue à la cartographie des menaces et à classification.

Règlement DORA – Principaux éléments

1. **La gestion des risques informatiques** - gouvernance et organisation, détection, réponse et rétablissement

2. **La gestion, classification et notification des incidents liés à l'informatique** - processus de gestion des incidents liés à l'informatique, classification des incidents liés à l'informatique, notification des incidents majeurs liés à l'informatique, une centralisation des notifications d'incidents majeurs liés à l'informatique

3. **Des tests de résilience opérationnelle numérique** - exigences générales applicables à la réalisation de tests de résilience opérationnelle numérique, test des outils et systèmes informatiques, tests avancés d'outils, systèmes et processus informatiques sur la base de tests de pénétration fondés sur la menace

4. **La gestion des risques liés aux tiers prestataires de services informatiques** - principes clés pour une bonne gestion des risques liés aux tiers prestataires de services informatiques, principales dispositions contractuelles, cadre de supervision des tiers prestataires critiques de services informatiques, inspections sur place, supervision continue

5. **Des dispositifs de partage d'information** - un dispositif de partage d'informations et de renseignement sur les cybermenaces

	Événements à notifier	Délai	Autorité destinataire	Sanction
NIS2	Incidents **« importants »** affectant la disponibilité, intégrité, authenticité ou confidentialité des réseaux/systèmes, causant : • Perturbation opérationnelle sévère ou pertes financières • Dommages matériels, physiques ou moraux à des tiers	• Alerte **initiale rapide** sans retard injustifié et en tout état de cause dans les 24 heures après avoir eu connaissance de l'incident • Notification dans les 72 heures après avoir eu connaissance de l'incident important, une notification d'incident • puis rapport final dans un délai d'1 mois	ANSSI en France	• Entités essentielles: 10 000 000 EUR ou à au moins 2 % du chiffre d'affaires annuel mondial • Entités importantes: 7 000 000 EUR ou à au moins 1,4 % du chiffre d'affaires annuel mondial
DORA	**Incidents majeurs liés aux TIC** dans le secteur financier (banques, assurances, prestataires TIC critiques)	• Alerte **initiale rapide** sans retard injustifié et en tout état de cause au plus tard dans les 24 heures après avoir eu connaissance de l'incident et dans les 4 heures après sa classification, • Puis un rapport intermédiaire 72 heures, • Un rapport final lorsque 'incident est terminé: 1 mois	ACPR & AMF en France	• Les autorités compétentes disposent de tous les pouvoirs de surveillance, d'enquête et de sanction nécessaires. • Les États membres peuvent imposer des sanctions pénales et des sanctions administratives • Le montant de l'astreinte, calculé à partir de la date indiquée dans la décision d'astreinte, est égal à 1 % au maximum du chiffre d'affaires quotidien moyen réalisé au niveau mondial par le prestataire tiers critique de services TIC
RGPD	**Violation de données personnelles** présentant un risque pour les droits et libertés des personnes	• **72 heures** après constatation (notification initiale possible, puis complément)	CNIL et si risque élevé, personnes concernées	• 10 000 000 EUR ou au moins 2 % du chiffre d'affaires annuel mondial • 20 000 000 EUR ou au moins 4 % du chiffre d'affaires annuel mondial

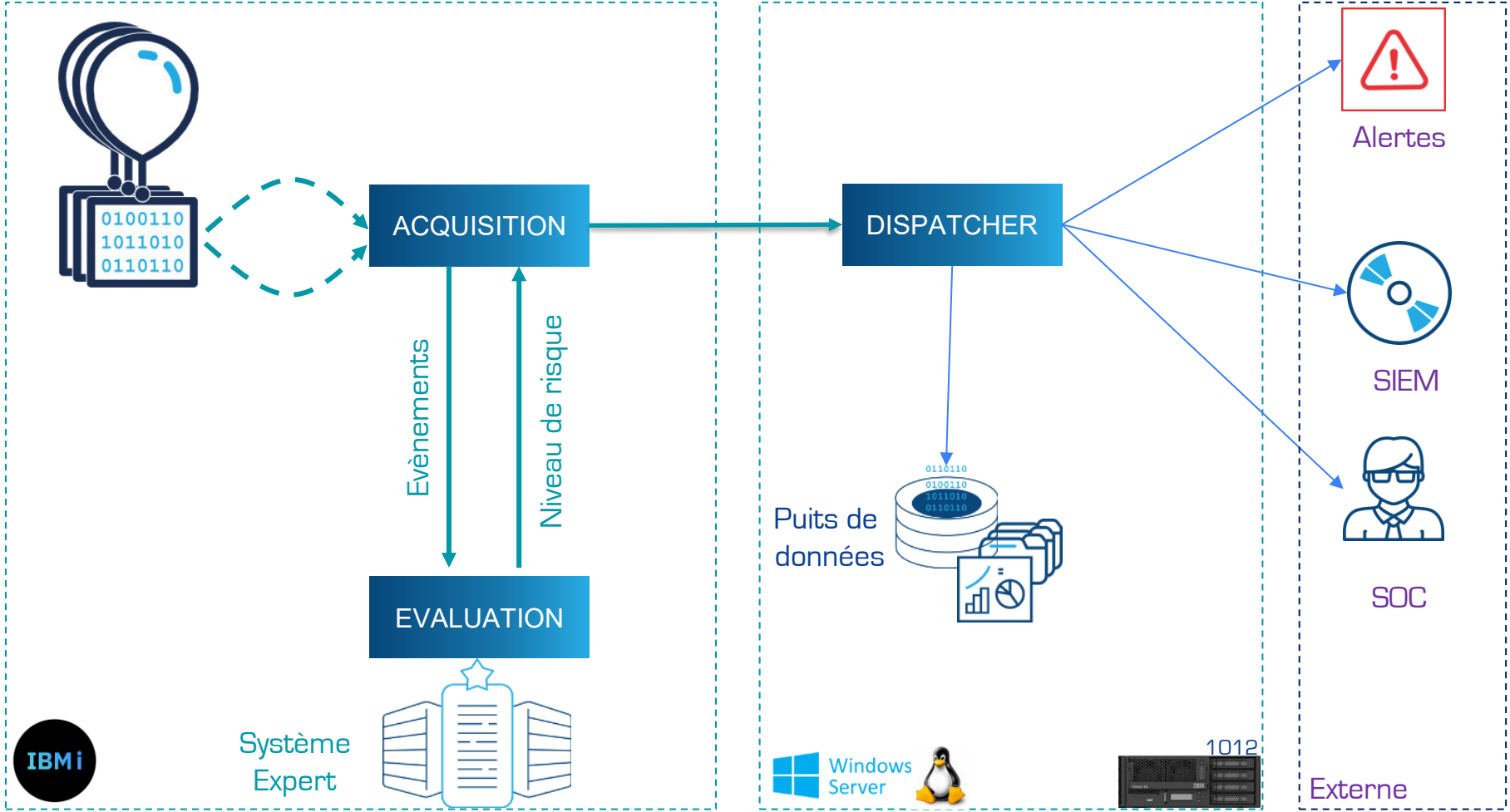
Maitrise des comptes de service

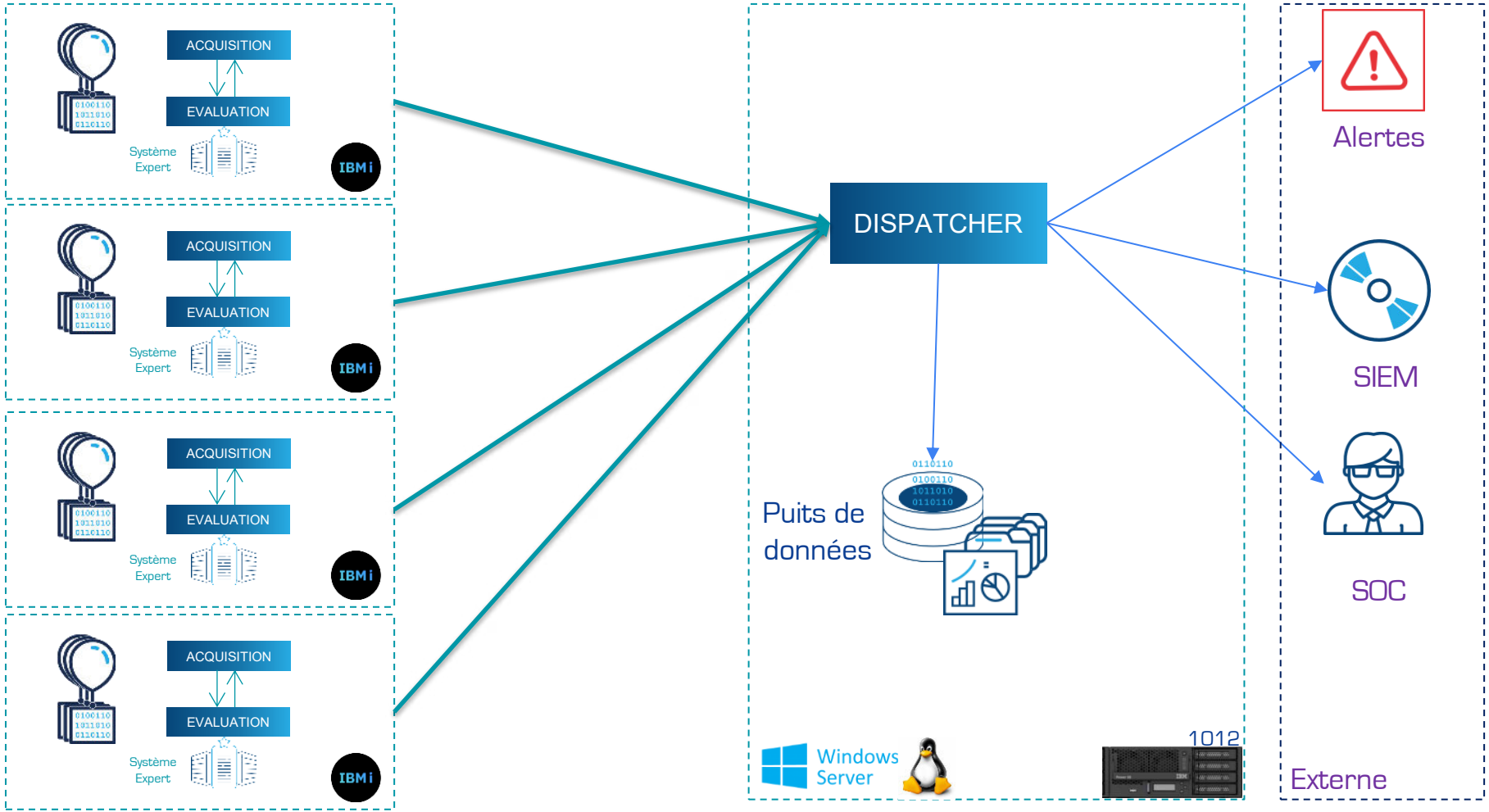
- Lors de mes audits, je constate souvent que les comptes des services ne sont pas maitrisés
  - Indispensable pour faire évoluer le niveau de mot de passe
- Ce sont des profils utilisés par des applications clientes, à distance, qui accèdent à l'IBM i
  - ODBC, JDBC
  - FTP
  - Partage de fichiers (NetServer)
  - 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


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


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 encore…

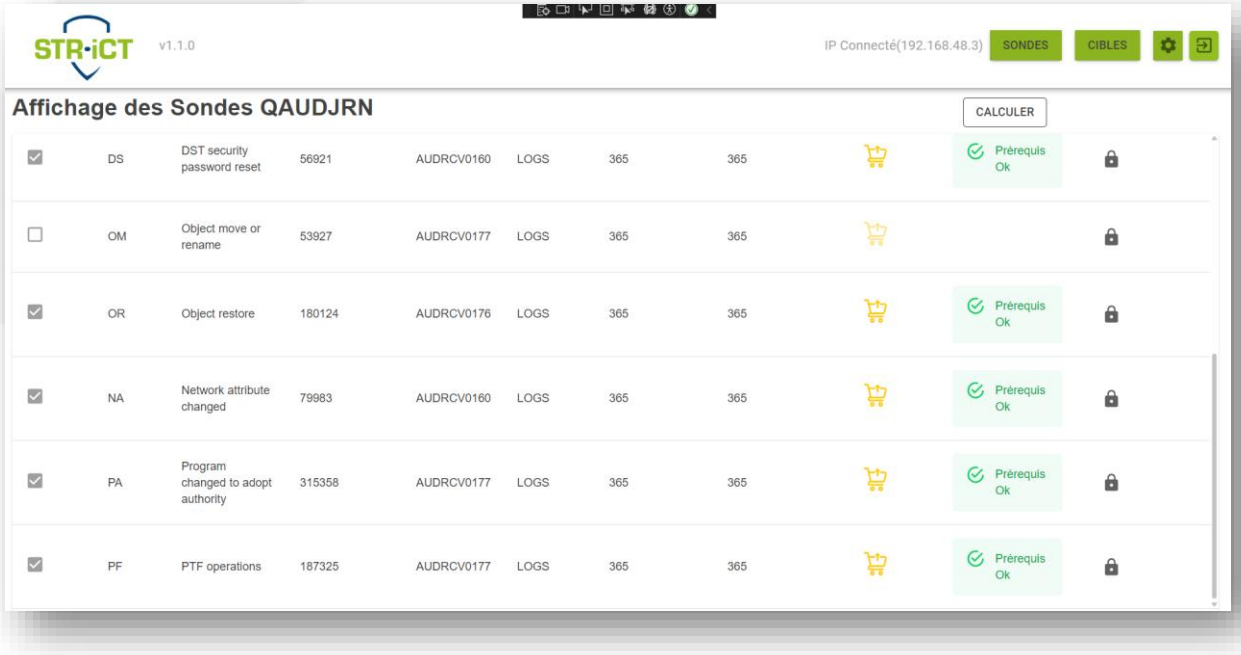
- Audit
  - Profils
  - Valeurs système
  - Bonnes pratiques
  - …
- Intégration dans Assure Security (Precisely - CILASOFT-Guy MARMORAT)

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

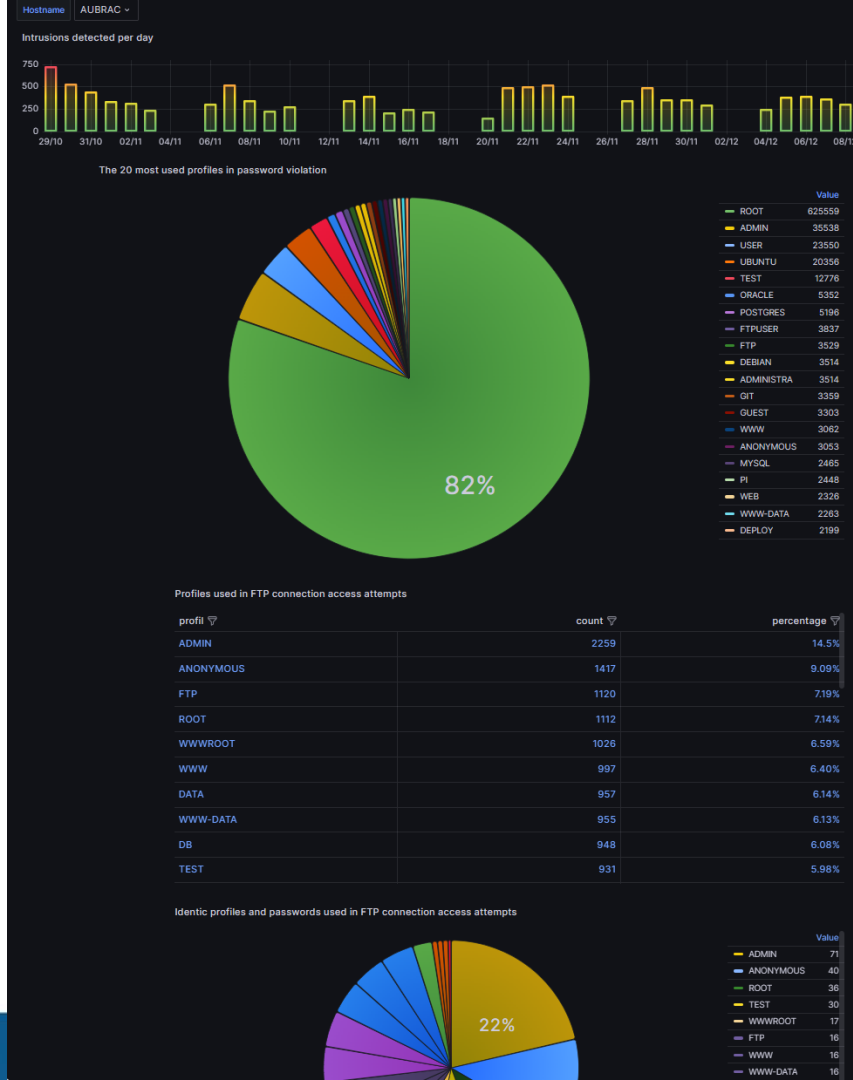
- Réceptionne les données (Web Service)
- En fonction de la configuration
  - Enregistre en local dans un puits de données (avec interface graphique de restitution)
  - Envoie vers un SIEM externe (Microsoft Sentinel, Elastic Search (ELK) , IBM Qradar, Splunk…) ou vers notre SiEM STR-iCT
  - En Web Services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

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
  - Pour s'intégrer au SIEM du réseau, s'il existe

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



Merci

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

I.GAYTE.IT