



Dominique GAYTE

06 30 17 02 55

dominique@gayte.it - <https://i.gayte.it>

IBM i

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



Meet our 2024 IBM Champions

Jan Agopian	Thomas Barnham	Jerry Blumler	Marcus Dewitt	Mia Fontanetti	Charles Gaudio	Mike Jirwan	Mattias Kotzer	Michael Mackie	Joseph Morgan
Soren Algotz	Francis Baer	Heng Cai	Edouard Dorn	Elizabeth Dorn	Elizabeth Dorn	Sergio Inzalaco	Kouke Morimoto	Murali Mahalingappa	Kouke Morimoto
Abdullah Alshammari	Brandon Beeth	Rogelio Carrizo	Stephan Ertl	Jonathan Foghorn	Phillip Gaudio	Philip Gaudio	Charles Mathewyan	Prasanth Mahapatra	David Morris
Ashraf Alshammari	Samuel Beitel	Craig Cernigoi	Maximo Franco	Vincent Fougere	Suehan Guo	Carlotta Eiroa	Rafiq Mahato	Daniel Moseley	Theresa Moran
Abdelhakim Aouici	Gerd Becker	Miguel Carrone	Diego Heins	Sergey Fortner	Wesley James	Andres Koenig	Klaudia Komelkova	Dhanraj Mohaneshwari	Tyagi Mouri
Gaetan Aubertin	Francis Berger	John Carter	Danilo Ingianni	Swati Prasad	Gunawirya	Simon Lach	Liam O'Connell	Chaitanya Nayak	Andreas Mueller
Khaled Abu El Sed	Thomas Bellon	Lafayette Charnet	Geoffrey Dicker	Armed Fruehwagen	Maria Haeg	Bilal Jaber	Gregoire Koc	Emiel Madsion	Dinsh Hoava
Karl Adler	Maxime Benoit	Robert Chan	Sank Debroy	Radu Frereking	Justin Haim	Sunil Jaiswal	Ermek Kozmenov	Elmer Masberg Focad	Umesh Kumar
Yves Aelterre	Nicholas Benth	Robin Chinn	Felix Gehring	Mike Freudenberger	Sahil Anand Hobbs	Lukas Jais	Sandeep Koul	Briesh Manjani	Domonic Muehsch
Dimitrios Adjalt	Neil Bhat	Stewart Clark	Bhadrachandrasekara	BRUNO	Bhivada Mahalingam	Tim Jaiswal	Felix Krutz	Sanjay Manjaree	Parth Mahapatra
Andreas Adriaens	Carly Ben-Nun	Quinn Call	Harish Chandra	Max Fry	Dik Hanggarbin	Julian Jaiswal	Michael Krutz	Michael Krutz	Harsh Mahapatra
Kristian Kauf Aqvand	Harold Bernhardt	Alex DeLo	Srinivasan	Omnia Kari	Nikus Mahalingam	Armin Krawatz	David Madsion	Armin Krawatz	Craig Mullins
Hong Aqvand	David Bernhardt	Leo-Michael Demery	Randy Fire	Subhasis Khatkar	Subhasis Khatkar	Brent Krueger	John Janssen	John Janssen	Harsh Mahapatra
Ismael Ayoub	Yusuf Bernini	Paul Demery	Pavel Denisov	Thomas Khatkar	Thomas Khatkar	Wood Krause	Yusuf Bernini	Yusuf Bernini	Chris Murray
Yusuf Bernini	Robert Bernini	Subhas Chak	Paul Demery	Thomas Khatkar	Thomas Khatkar	Wood Krause	Yusuf Bernini	Yusuf Bernini	Chris Murray
Sam Mousal Aouadi	Yusuf Bernini	Subhas Chak	Paul Demery	Thomas Khatkar	Thomas Khatkar	Wood Krause	Yusuf Bernini	Yusuf Bernini	Chris Murray
Shoukat Ali	Yusuf Bernini	Subhas Chak	Paul Demery	Thomas Khatkar	Thomas Khatkar	Wood Krause	Yusuf Bernini	Yusuf Bernini	Chris Murray
Yusuf Bernini	Yusuf Bernini	Subhas Chak	Paul Demery	Thomas Khatkar	Thomas Khatkar	Wood Krause	Yusuf Bernini	Yusuf Bernini	Chris Murray
Yusuf Bernini	Yusuf Bernini	Subhas Chak	Paul Demery	Thomas Khatkar	Thomas Khatkar	Wood Krause	Yusuf Bernini	Yusuf Bernini	Chris Murray
Yusuf Bernini	Yusuf Bernini	Subhas Chak	Paul Demery	Thomas Khatkar	Thomas Khatkar	Wood Krause	Yusuf Bernini	Yusuf Bernini	Chris Murray
Yusuf Bernini	Yusuf Bernini	Subhas Chak	Paul Demery	Thomas Khatkar	Thomas Khatkar	Wood Krause	Yusuf Bernini	Yusuf Bernini	Chris Murray
Yusuf Bernini	Yusuf Bernini	Subhas Chak	Paul Demery	Thomas Khatkar	Thomas Khatkar	Wood Krause	Yusuf Bernini	Yusuf Bernini	Chris Murray
Yusuf Bernini	Yusuf Bernini	Subhas Chak	Paul Demery	Thomas Khatkar	Thomas Khatkar	Wood Krause	Yusuf Bernini	Yusuf Bernini	Chris Murray
Yusuf Bernini	Yusuf Bernini	Subhas Chak	Paul Demery	Thomas Khatkar	Thomas Khatkar	Wood Krause	Yusuf Bernini	Yusuf Bernini	Chris Murray
Yusuf Bernini	Yusuf Bernini	Subhas Chak	Paul Demery	Thomas Khatkar	Thomas Khatkar	Wood Krause	Yusuf Bernini	Yusuf Bernini	Chris Murray



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 maîtrisés
- 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 maîtrise 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

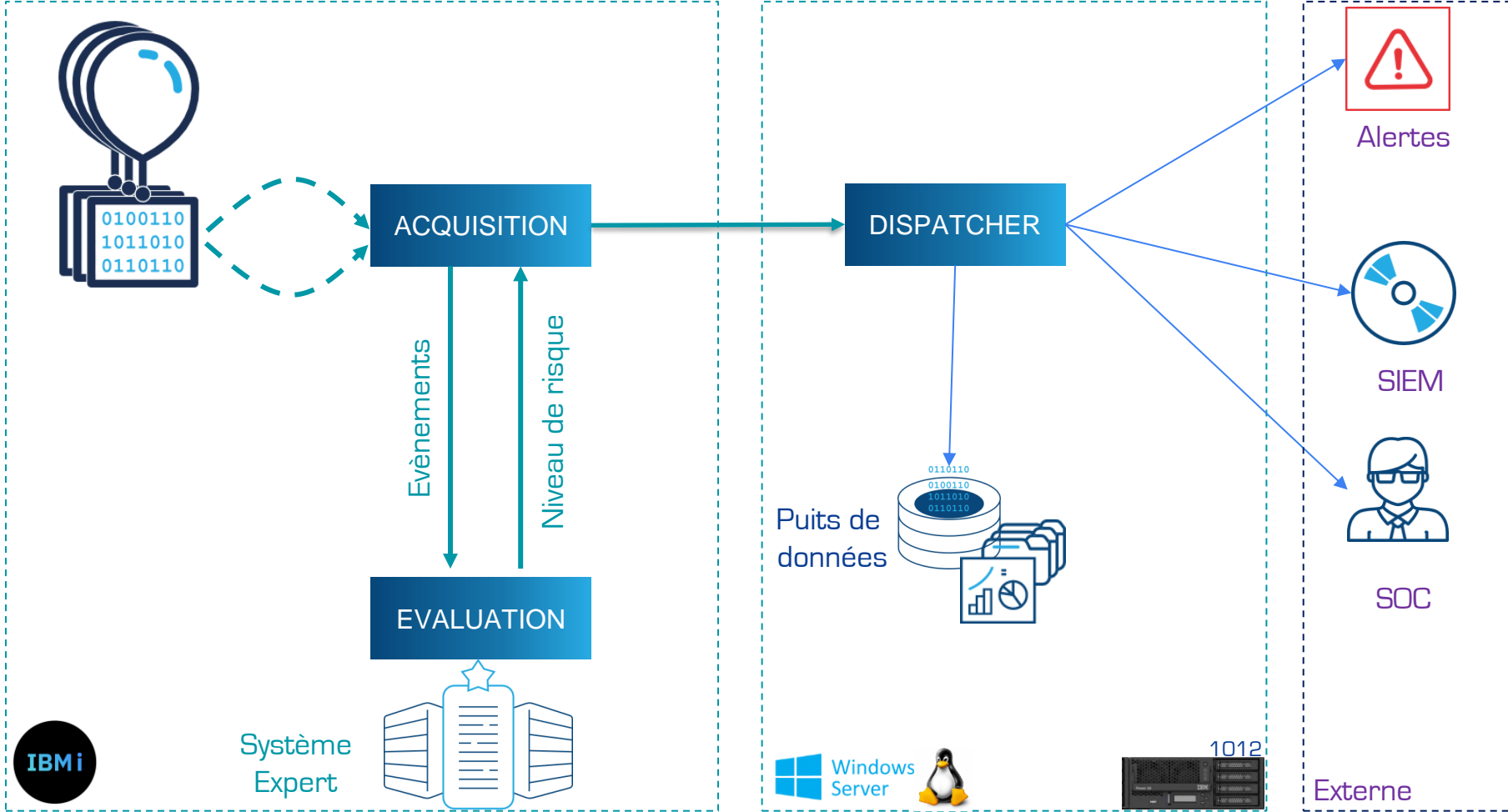
- L'IBM i est très bavard pour qui sait l'écouter
- Il produit (ou peut produire) une énorme quantité de données de traçabilité
- Mais
 - Pas toujours simple à retrouver
 - Pas toujours simple à lire (décrypter)
 - Pas toujours simple à configurer
- Rarement conservé de manière structurée
 - Quand on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

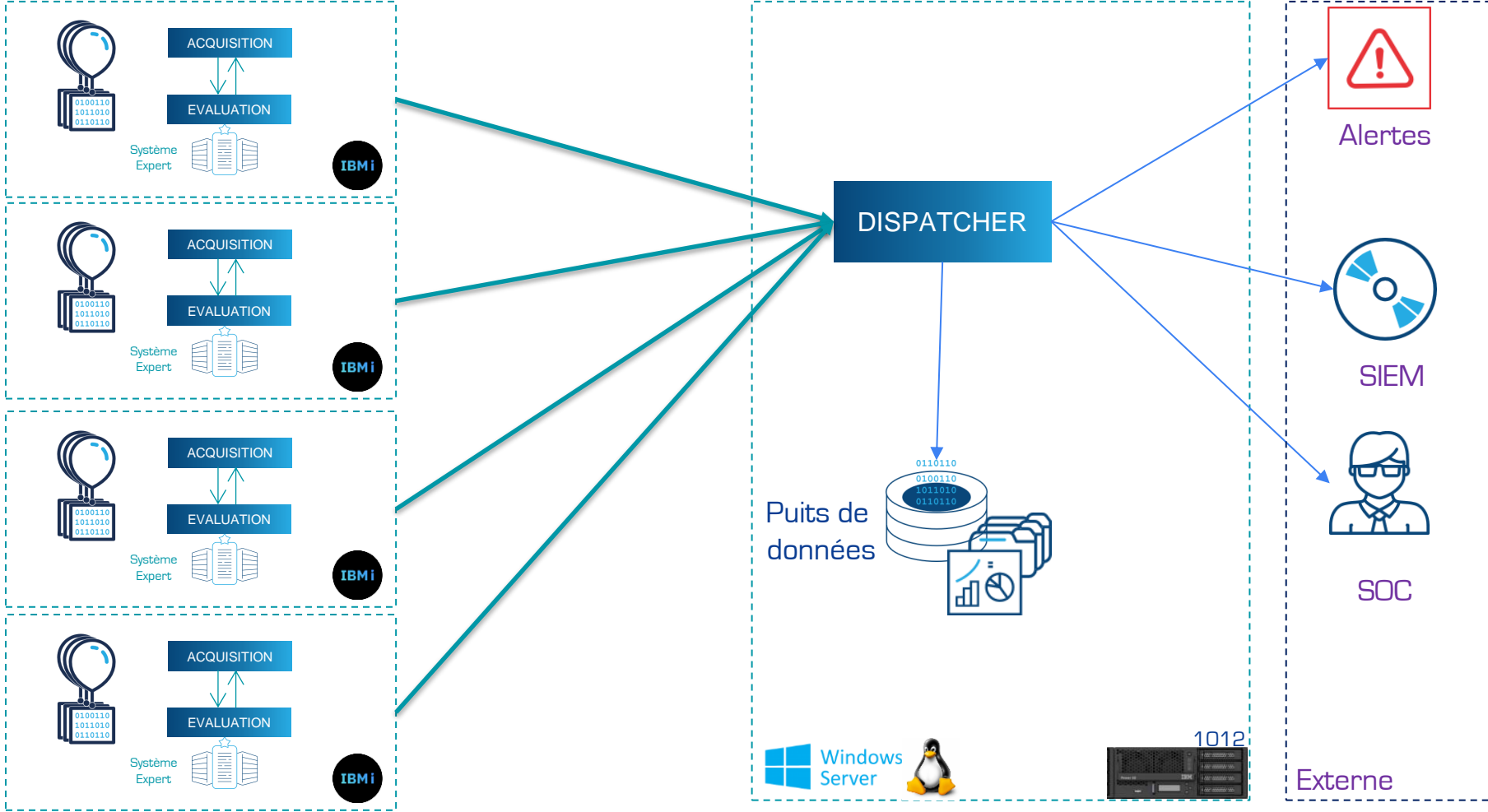


STR-iCT



- STR-iCT 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)





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

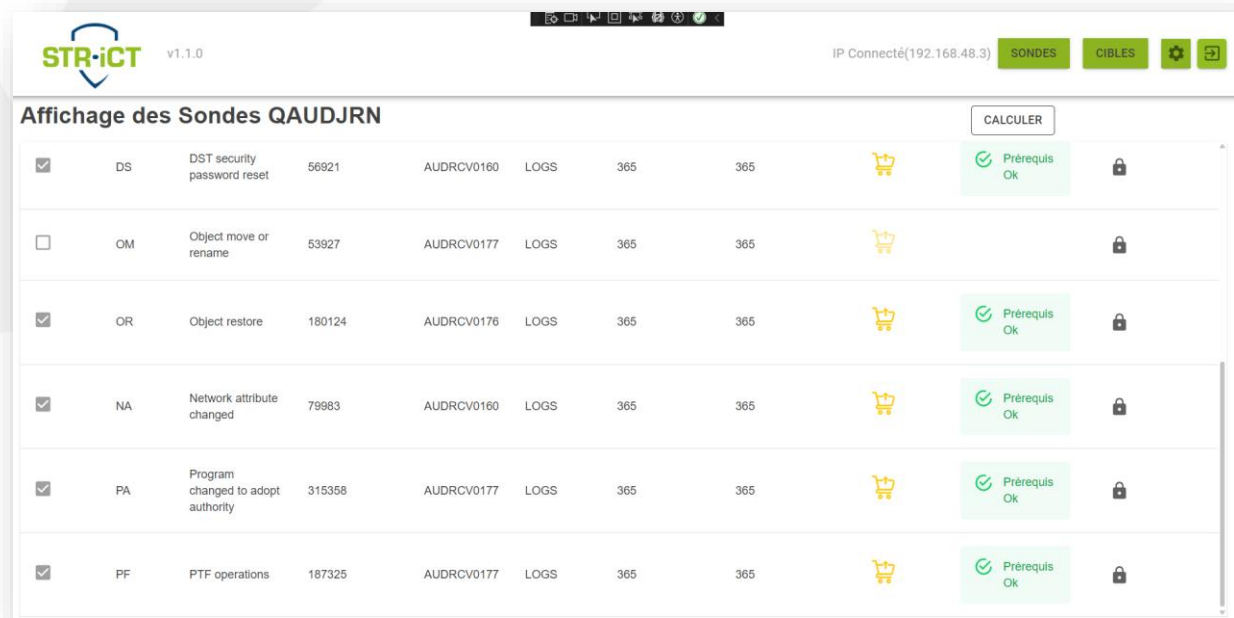
- Audit
 - Profils
 - Valeurs système
 - Bonnes pratiques
 - ...
- Intégration dans Assure Security (CILASOFT-Guy MARMORAT)

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



STR-ICT v1.1.0 IP Connecté(192.168.48.3) **SONDES** CIBLES

Affichage des Sondes QAUDJRN CALCULER

<input checked="" type="checkbox"/>	DS	DST security password reset	56921	AUDRCV0160	LOGS	365	365		Prérequis OK	
<input type="checkbox"/>	OM	Object move or rename	53927	AUDRCV0177	LOGS	365	365			
<input checked="" type="checkbox"/>	OR	Object restore	180124	AUDRCV0176	LOGS	365	365		Prérequis OK	
<input checked="" type="checkbox"/>	NA	Network attribute changed	79983	AUDRCV0160	LOGS	365	365		Prérequis OK	
<input checked="" type="checkbox"/>	PA	Program changed to adopt authority	315358	AUDRCV0177	LOGS	365	365		Prérequis OK	
<input checked="" type="checkbox"/>	PF	PTF operations	187325	AUDRCV0177	LOGS	365	365		Prérequis OK	

Le dispatcher

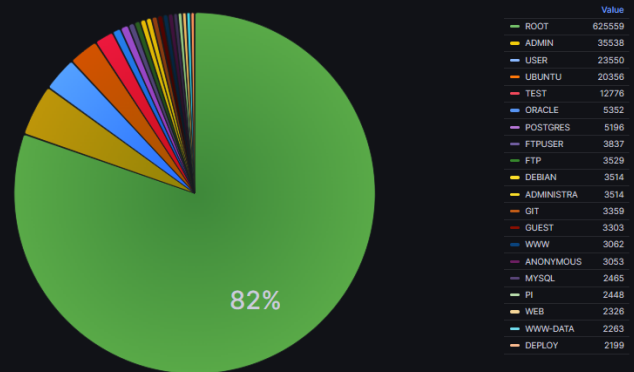
- Réceptionne les données (Web Service)
- En fonction de la configuration
 - Enregistre en local dans un puits de données (avec interface graphique de restitution)
 - Envoie vers un SIEM externe (Microsoft Sentinel, Elastic Search (ELK) , IBM Qradar, Splunk...) ou vers notre SiEM STR-iCT
 - En Web Services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



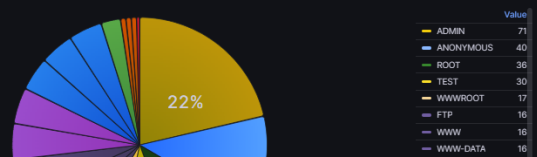
The 20 most used profiles in password violation



Profiles used in FTP connection access attempts

profil	count	percentage
ADMIN	2259	14.5%
ANONYMOUS	1417	9.09%
FTP	1120	7.19%
ROOT	1112	7.14%
WWWROOT	1026	6.59%
WWW	997	6.40%
DATA	957	6.14%
WWW-DATA	955	6.13%
DB	948	6.08%
TEST	931	5.98%

Identific profiles and passwords used in FTP connection access attempts



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>

