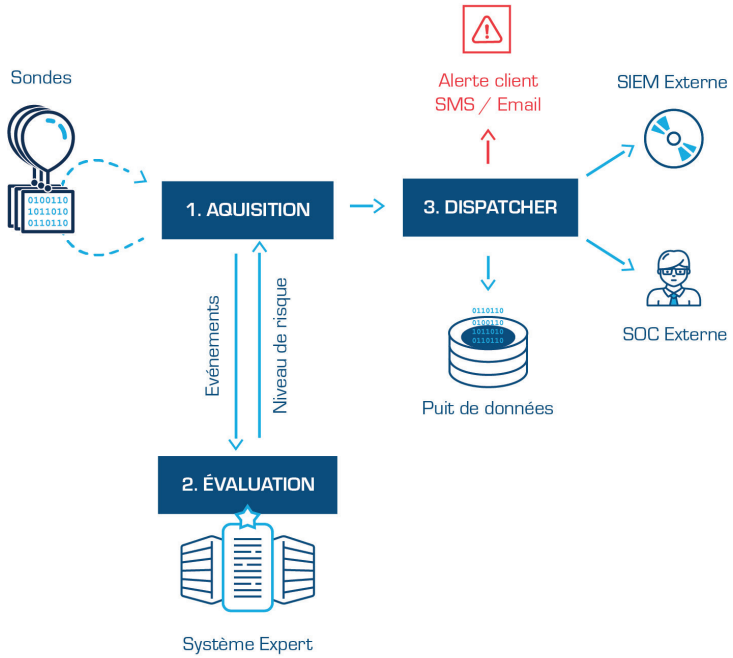
Sécurité et SiEM pour IBM i

STR-iCT : une application de sécurisation dédiée aux IBM i

Les IBM i (ex AS/400) sont des systèmes critiques qui gèrent souvent la majorité des activités d'une entreprise. Leur sécurisation est une des préoccupations majeures des DSI. Mais les outils standard de sécurisation du réseau ignorent ou au mieux méconnaissent ce système.

Fort de l'expérience de plusieurs dizaines d'années de sécurisation des IBM i, et l'audit de centaines de partitions, I.GAYTE.IT (prononcer à l'anglaise *i get it*) a créé le progiciel dédié à la sécurisation des IBM i.



- Ses sondes peuvent récupérer tous les évènements de l'IBM i que vous souhaitez.
- Un système expert unique évalue le niveau de risque de chacun de ces évènements en fonction de nombreux paramètres.
- Les données disponibles (adresse IP et port distants, profil utilisé, action effectuée, niveau de risque...) sont exportées vers un dispatcher chargé d'alerter si besoin et d'envoyer les données vers un puits de données, vers un SIEM, un SOC externe...

Sondes IBM i

- Journal d'audit
  - Violations, SST/DST, Connexions, Mot de passe, Supressions
- Exit point
  - IFS, SQL, FTP, ODBC/JBDC
- Détection d'Intrusions
- Divers
  - Audit, Legacy, Métriques

SiEM STR-iCT

- Système expert
  - Risque
- Alertes
  - Mail, SMS, Team, Slack

Traçabilité

- Reporting
  - Dashboards, Interface graphique
- Interrogation SQL
- Historisation des données

Sécurité externe

- SOC Externe
  - Syslog, API REST
- SIEM Externe
  - IBM QRADAR, Microdoft Sentinel, ELK, etc.

Les sondes : intercepter les évènements

Notre parfaite connaissance de l'IBM i et de ses mécanismes nous permet de récupérer une quantité importante d'évènements liés à la Sécurité et/ou à la traçabilité.

Plusieurs dizaines de sondes sont disponibles et configurables afin de collecter les données qui vous sont utiles.

LES SONDES

- Tentatives d'intrusions
- Mots de passe en erreur
- Tentative d'accès à un objet non autorisé
- Tentative de connexion NetServer
- Connexion en Kerberos (SSO)
- Utilisation d'un profil utilisateur inexistant/désactivé
- Suppression d'objets
- Gestion DST/SST
- Métriques
- Accès à l'IFS via NetServer
- Accès en FTP
- Audit Sécurité du système
- Suivi des modifications pour une colonne d'une table
- Gestion des valeurs système
- Gestion des profils utilisateur
- Accès SQL en ODBC/JDBC
- Et bien d'autres encore...

Système Expert de définition du risque

Chaque évènement est traité par notre Système Expert afin de déterminer le risque qu'il fait courir à l'IBM i et à la totalité du réseau. Il s'appuie sur l'expertise de I.GAYTE.IT en Sécurité des IBM i, sur l'expérience acquise en tentative d'intrusion de ces systèmes et sur les connaissances en cybersécurité.

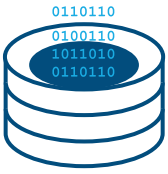
SiEM : STR-iCT for IBM i Event Manager : le SIEM dédié aux IBM i

STR-iCT peut être considéré comme un véritable SIEM (Security Information Event Manager) dédié à l'IBM i. Il collecte les données, en évalue le risque et déclenche les éventuelles alertes. Il peut fonctionner en autonome pour les entités qui ne disposent pas déjà d'un SIEM pour leur réseau.

Êtes-vous SiEM ou SIEM ?

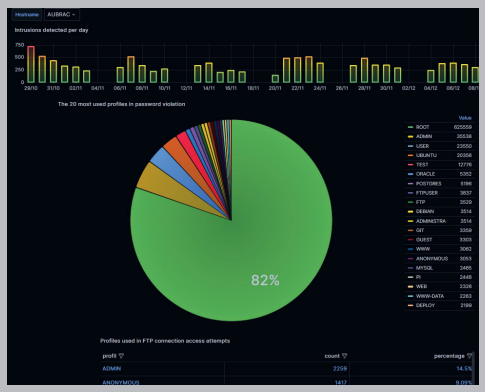
Ceux qui disposent déjà d'un SIEM pour gérer la Sécurité de tous les éléments du réseau savent que l'IBM i en est généralement exclu. STR-iCT peut leur transmettre les données afin d'avoir une gestion centralisée. STR-iCT est interfacé avec les principaux SIEM du marché, n'hésitez pas à nous contacter à ce sujet.

Avec STR-iCT, on peut décider du type des données transmises au SIEM. L'archivage des données (puit de données) peut être celui de STR-iCT afin de diminuer les frais liés au SIEM externe, souvent calculés en fonction du trafic géré. Dans ce cas, seules les informations critiques (à haut niveau de risque) sont communiquées au SIEM.



Le puit de données de STR-iCT : stockage des données et restitution graphique

Tous les évènements définis dans votre configuration (graphique) sont stockés dans notre puit de données et constituent une mine de renseignements. Il s'agit d'un endroit unique, doté d'une interface graphique, qui vous présente des tableaux de bord configurables et qui vous laisse utiliser un requêteur SQL pour répondre à vos moindres besoins. Cette interface très ergonomique, basée sur Grafana, est totalement configurable pour un grand confort d'utilisation.



Grafana

Traçabilité

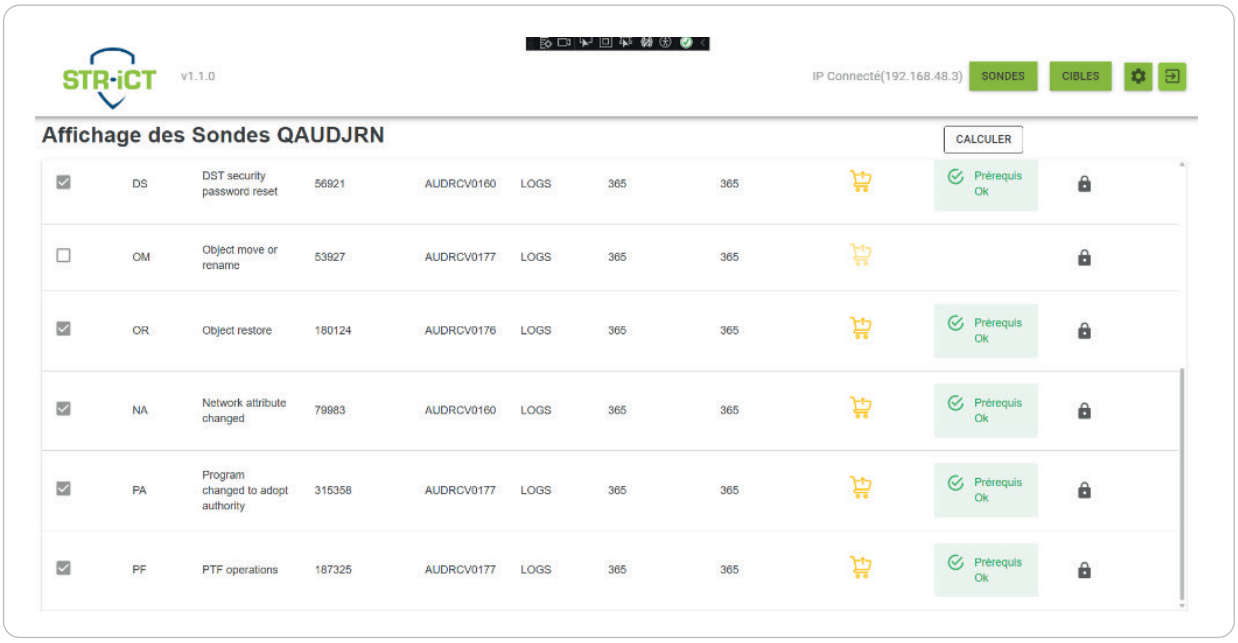
Seule la traçabilité vous permet de comprendre les évènements passés. Quelles ont été les tentatives de connexions à partir de telle adresse IP, qui a modifié le fichier des virements la semaine dernière, quelles sont les travaux lancés par un profil, qui a modifié les valeurs système ou les profils SST/DST... ?

Vous pouvez retrouver simplement ces informations dans l'interface graphique de notre puit de données.

La rétention des informations pour chaque type d'évènement est simplement configurable par notre interface graphique. Il est aussi possible de disposer d'une rétention de longue durée (données froide).

SOC externe

Certaines organisations utilisent des SOC externes (Security Operation Center) pour gérer la Sécurité du réseau. STR-iCT communique les données importantes à ces SOC afin qu'ils disposent de toutes les données issues de l'IBM i et nécessaires au bon déroulement de leur mission.



I.GAYTE.IT

FRANCE 2030

La Région Occitanie Pyrénées - Méditerranée

lozère LE DÉPARTEMENT

Pour plus d'informations

i.gayte.it/str-ict
str-ict@gayte.it

Vous êtes un partenaire IBM, un MSP hébergeant des IBM i ou un distributeur de SIEM, **nous avons un contrat de partenariat à forte valeur ajoutée pour vous** : i.gayte.it/ipp

I.GAYTE.IT est une marque de GAYTE.IT - Siège - 46, Le Villeret - 48170 ST JEAN LA FOUILLOUSE - FRANCE
Centre R&D – POLeN - 12 rue Albert Einstein - 48000 MENDE
Agence Montpellier - 32 chemin Notre Dame - 34160 BEAULIEU