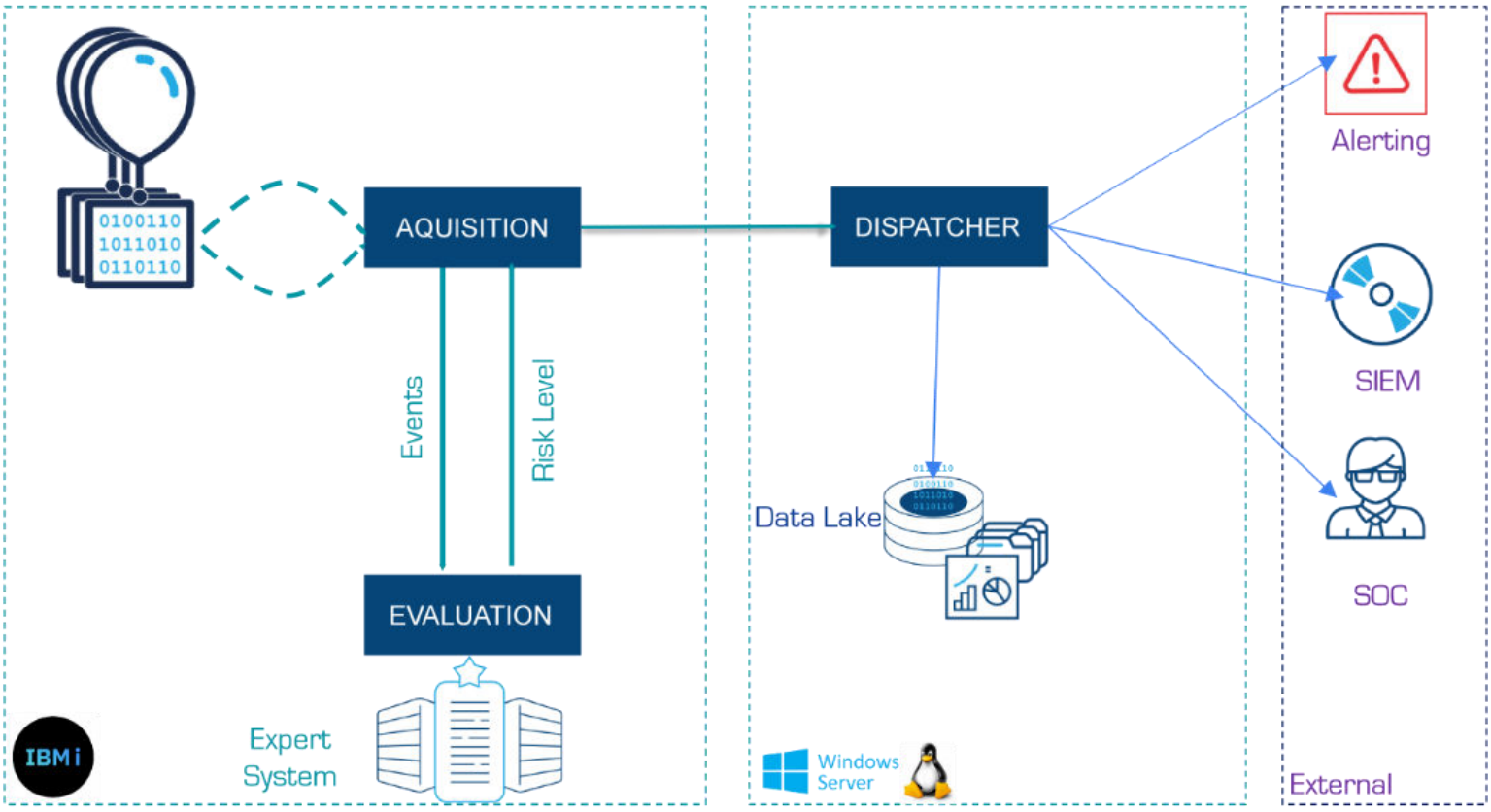
Security and SiEM for IBM i

STR-iCT : a security application dedicated to IBM i systems

IBM i (aka AS/400) are critical systems that often manage most of a company's activities. Their security is a major concern for IT departments. But the standard network security tools are unaware, or at best misunderstand, these systems.
With decades of experience securing IBM i systems, and the audit of hundreds of partitions, I.GAYTE.IT (pronounced "*I get it*") has created a program entirely dedicated to IBM i securing.

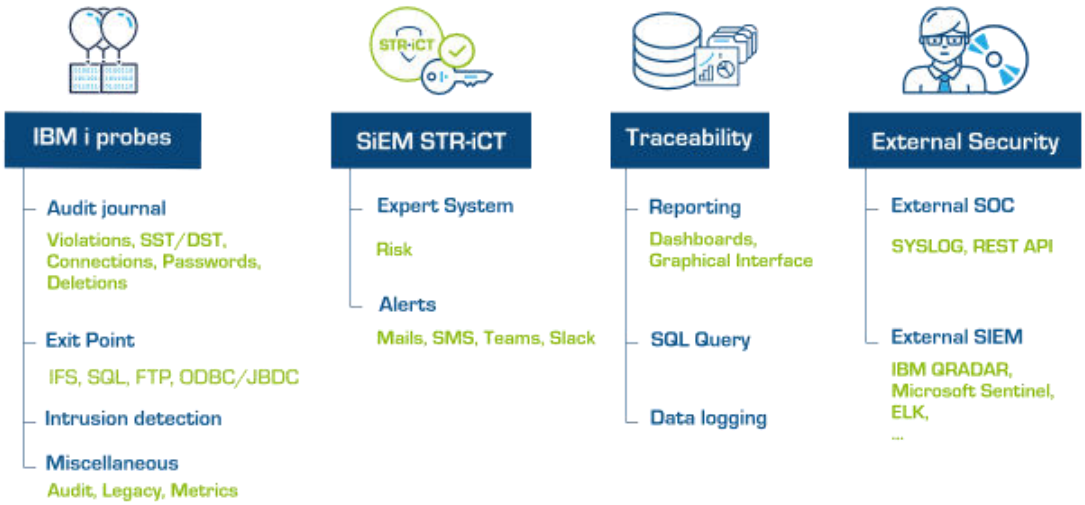


DATA STREAM

Probes can recover all the selected events triggered on the IBM i system.

A unique expert system evaluates the risk of each event depending on a multitude of parameters.

The available data (IP addresses and distant ports, used profile, action performed, risk level...) are exported to a dispatcher that is responsible for alerting, if necessary, and sending this data to a data lake, a SIEM, an external SOC...



The probes: intercept events

Our perfect knowledge of the IBM i system and its mechanisms allows us to recover a significant quantity of events linked to security and/or traceability.
Several dozen probes are available and configurable to collect data that will be useful to you.

PROBES

- Attempted intrusion
- Wrong passwords
- Attempted access to an unauthorized object
- Attempted connection to NetServer
- Kerberos connection (SSO)
- Attempt to connect to a nonexistent or deactivated user
- Object deletion
- DST/SST management
- Metrics
- Access to IFS via NetServer
- FTP access
- System security audit
- Track changes for a column in a table
- System values management
- User profile management
- SQL access in ODBC/JDBC
- And many more...

Risk Defining Expert system

Each event is processed by our Expert System to determine the risk that it puts the IBM i through and to the entire network. It relies on I.GAYTE.IT's expertise in terms on IBM i security, on the acquired experience in intrusion attempts on these systems, and on general cyber security knowledge.

SiEM: STR-iCT for IBM i Event Manager: The dedicated SIEM for IBM i's

STR-iCT can be considered like a real SIEM (Security Information Event Manager) dedicated to IBM i systems. It collects data, evaluates the risk and eventually triggers alerts. It can operate autonomously for the companies that do not have their own SIEM on their network.

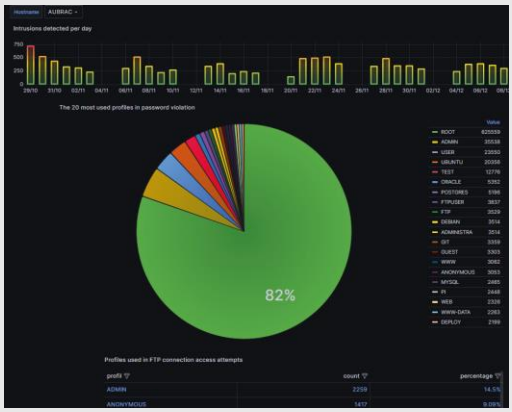
Are you SiEM or SIEM?

Those who already have their own SIEM to manage the security of all the elements on their network know that IBM i's are generally excluded. STR-iCT can transmit the data from the IBM i to their existing SIEM to have centralized management. STR-iCT is capable to communicate with the main SIEMs on the market, do not hesitate to contact us about this.

With STR-iCT we can decide what type of data we want to send to the SIEM. Data archiving (data sink) can be that of STR-iCT in order to reduce costs to the external SIEM, often calculated in terms of managed traffic. In that case, only the critical information (that has a high level of risk) are sent to the SIEM.

STR-iCTs data lake: data storage and graphic restitution

All the elements defined in your (graphical) configuration are stored in a data sink and constitutes a data mine of gold. It is a unique place, equipped with a graphical interface that shows you editable dashboards and lets you use a SQL query tool to meet your every need. This very ergonomic user interface, based on Grafana, can be entirely edited for a great comfort of use.



Traceability

Only data traceability allows you to understand passed events. What connection attempts were made, from which IP address, who modified las weeks money transfer file, what process was launched by which profile, who modified system values or the SST/DST profiles...?

You can simply retrieve this information in the graphical user interface of our data sink.

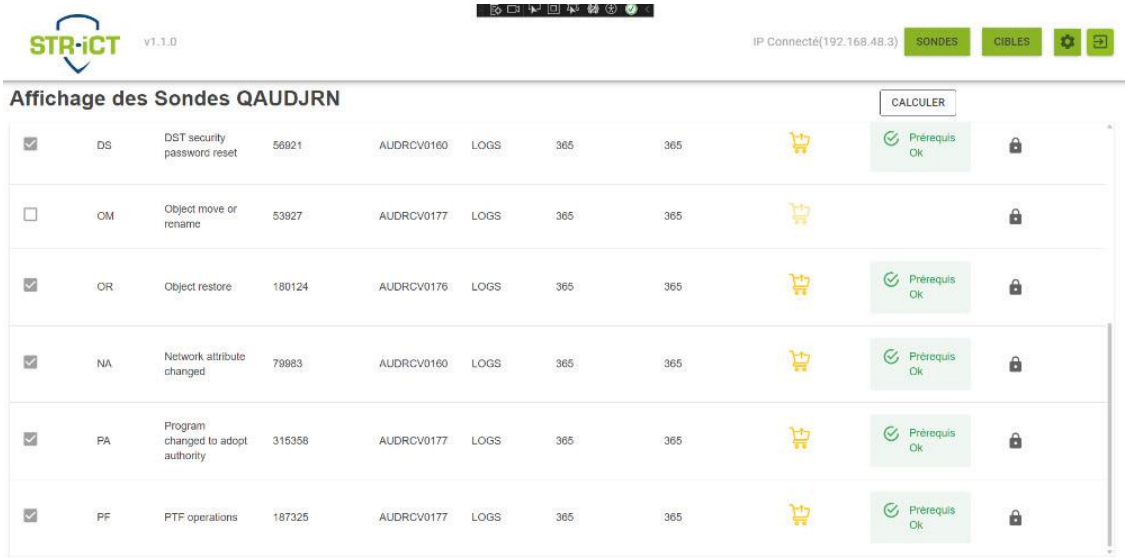
Data retention for every type of event is easily configurable in our graphical interface. It is also possible to configure a long-term data retention policy (cold data).

External SOC

Some organizations use external SOCs (Security Operation Center) to manage network security. STR-iCT communicates important information to these SOCs so they have all the data from the IBM I that is necessary to the proper functioning of their mission.

Graphical Interface

Data configuration and analysis are carried out via graphical user interfaces.



Our Services

We assist you in securing your IBM i, in the deployment of STR-iCT and in-service support.

Fell free to contact us, or our authorized partners, for any service related to IBM i Security.

STR-iCT made by I.GAYTE.IT
IBM i Security Software & Services

FRANCE 2030

La Région Occitanie Pyrénées · Méditerranée

lozère LE DÉPARTEMENT

For more information
i.gayte.it/str-ict
str-ict@gayte.it

You are an IBM partner, an MSP hosting IBM i or a SIEM distributor,
we have a partnership contract at high added value for you: i.gayte.it/ipp