STR-iCT
IBM i security and traceability

KHAN Nauman - nk@blue-channel.com
FACQ GUIRAUD Guilian – guilian@gayte.it

IBM i

KHAN Nauman

- Ex-IBMer (20 years' experience) & founder of Blue-Channel (Blue for Big Blue !) in 2008
- Operational marketing for IBM Business Partners (BPs) and Start-Ups, "only" with IBM

FACQ-GUIRAUD Guilian

- Systems and Networks Engineer
- SSO and security implementer for I.GAYTE.IT

About Us

I.GAYTE.IT research & develop innovative IBM i security and modernization software solutions

A few words from Mr Dominique GAYTE, I.GAYTE.IT's CEO & IBM Champion.
With over 35 years' experience in securing IBM i servers and implementing SSOs on hundreds of IBM i partitions all over the world, we wanted to converge our experience with extensive customer feedback to design unique & high added value software solutions for IBM i clients to protect their IBM i investments within an ever-increasing hostile IT environment.

I.GAYTE.IT in two words

Ease of SSO deployment for IBM i

Security and traceability for IBM i

Services

Security and traceability challenges on IBM i

IBM i and security

- IBM i’s often have security built on 1990s principles
  - At the time, little to no networks
  - No internet
  - No hackers nor ransomwares
- But often at the heart of a company’s information system
  - 100% of the activity generally goes through its applications
    - Accounting
    - Stocks
    - Business management
    - Production
    - …
- They are therefore critical and do not have a suitable security configuration
- They are often excluded or overlooked by network security softwares (SIEM)

Traceability

- Maintaining a history of actions that have occurred
  - For events
  - For data
- At the heart of new standards
  - NIS2
  - DORA
  - RGPD

Me Cathie-Rosalie Joly - Lawyer

NIS2

Technical aspect, particularly with SOC/SIEMs

- Security Operations Center
- Security Information and Event Management

1. **Cyber threat detection**
    1. **SOC** : ensures continuous monitoring of systems, detection of abnormal behavior, and incident response
    2. **SIEM** : collects, correlates, and analyzes logs to identify threats in real time
2. **Incident management**
    1. **SIEM** : enables incident detection through alerts based on event correlations
    2. **SOC** : coordinates incident response, post-mortem analysis, and communication with ANSSI
3. **Risk assessment and management (classification and notification)**
    1. **SIEM** : provides useful data for risk analysis (frequency, severity, types of incidents)
    2. **SOC** : contributes to threat mapping and classification

Règlement DORA – Key elements

1. **IT Risk Management** – governance and organization, detection, response, and recovery

2. **Management, classification, and notification of IT-related incidents** – IT incident management processes, classification of IT-related incidents, notification of major IT incidents, and centralization of notifications for major IT incidents

3. **Digital operational resilience testing –** general requirements applicable to conducting digital operational resilience tests, testing of IT tools and systems, advanced testing of IT tools, systems, and processes based on threat-led penetration testing

4. **Management of risks related to third-party IT service providers –** key principles for effective management of risks related to third-party IT service providers, main contractual provisions, supervisory framework for critical third-party IT service providers, on-site inspections, continuous monitoring

5. **Information-sharing arrangements –** a framework for sharing information and intelligence on cyber threats

	Events to be notified	Timeframe	Receiving authority	Penalty
NIS2	**"Significant"** incidents affecting the availability, integrity, authenticity, or confidentiality of networks/systems, causing: • Severe operational disruption or financial losses • Material, physical, or moral damage to third parties	• **Initial early warning** without undue delay and in any case within 24 hours after becoming aware of the incident • Notification within 72 hours after becoming aware of the significant incident • Then final report within 1 month	ANSSI in France	• Essential entities: €10,000,000 or at least 2% of total worldwide annual turnover • Important entities: €7,000,000 or at least 1.4% of total worldwide annual turnover
DORA	**Major ICT-related incidents** in the financial sector (banks, insurance companies, critical ICT service providers)	• **Initial early warning** without undue delay and in any case no later than 24 hours after becoming aware of the incident and within 4 hours after its classification • Then an intermediate report within 72 hours • A final report when the incident is resolved: 1 month	ACPR & AMF in France	• Competent authorities have all necessary supervisory, investigative, and sanctioning powers • Member States may impose criminal and administrative penalties • The penalty amount, calculated from the date indicated in the penalty decision, may be up to 1% of the average daily worldwide turnover of the critical ICT third-party provider
GDPR	**Personal data breach** posing a risk to the rights and freedoms of individuals	• Within **72 hours** after becoming aware (initial notification possible, followed by additional information)	CNIL and, if high risk, the affected individuals	• €10,000,000 or at least 2% of total worldwide annual turnover • €20,000,000 or at least 4% of total worldwide annual turnover

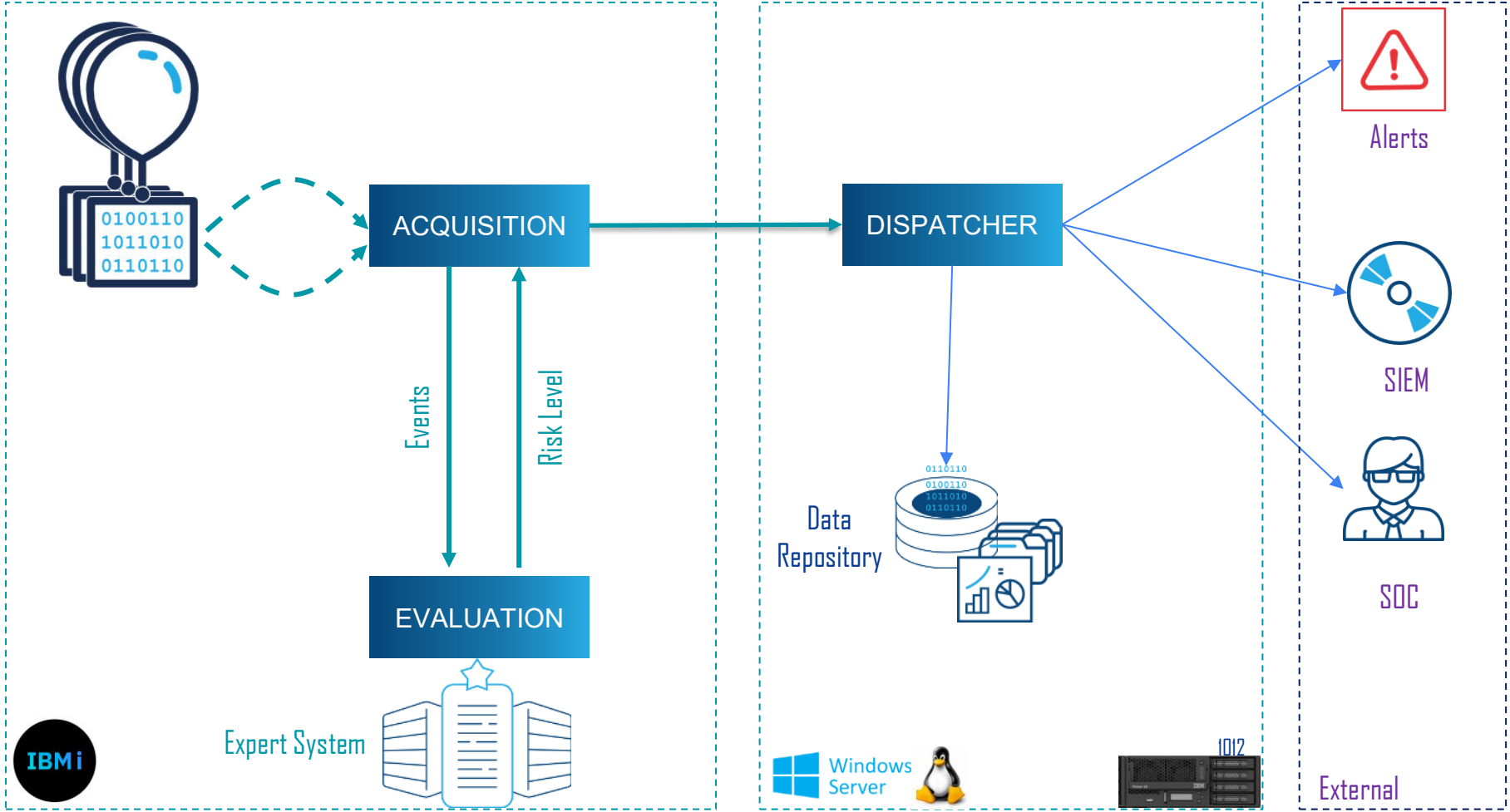
Control of service accounts

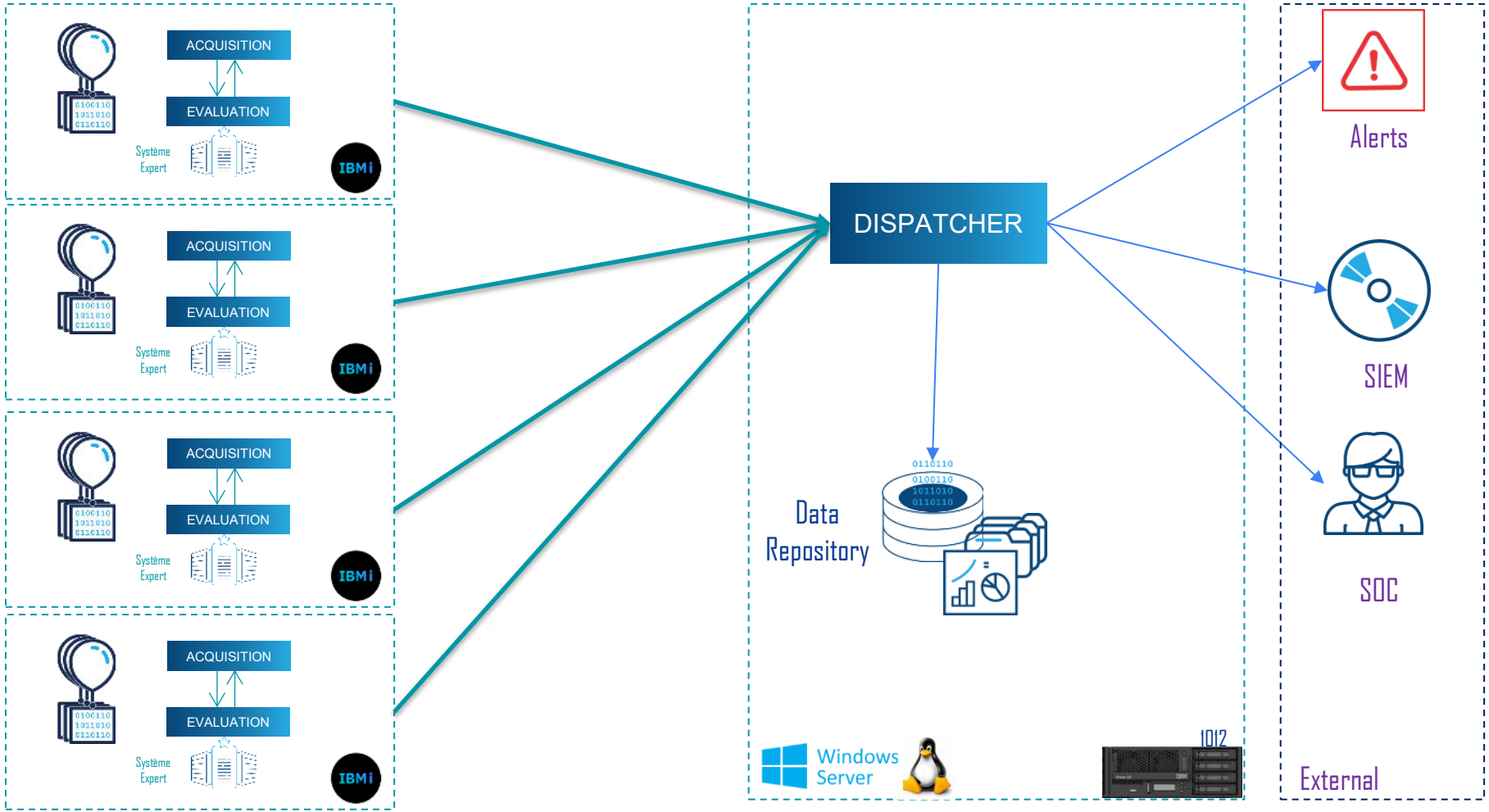
- During audits, we often observe that service accounts are not properly controlled.
- These are profiles used by client applications, remotely, to access the IBM i:
  - ODBC, JDBC
  - FTP
  - File Sharing (NetServer)
  - Web Services
- Profiles and passwords are often hard-coded in plain text!
  - And the profiles often have special privileges (*ALLOBJ!).
- Controlling these service accounts is essential!
  - When do external connections occur?
  - For what purpose?
  - With which profile?
  - Where is the password stored (in plain text)?
  - How can it be changed if it is compromised?
  - How can the password strength be improved (V7Rnext removal of level 0 or 1 passwords!)?
- Only traceability can help you see things clearly!

IBM i and traceability

- The IBM i is very talkative if you know how to listen to it
- It produces (or can produce) a massive amount of traceability data
- But
  - Not always simple to find
  - Not always simple to read (decrypt)
  - Not always simple to configure
- Rarely kept in a structured manner
  - It can take a lot of disk space
  - Information is not available when we need it
    - Log receivers deleted every day, or on the fly


STR-iCT


0100110
1011010
0110110
ACQUISITION
DISPATCHER
Alerts
SIEM
SOC
External
Events
Risk Level
Data
Repository
EVALUATION
Expert System
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
Data Repository
Windows Server
Alerts
SIEM
SOC
External

STR-iCT

- STR-iCT is a dedicated software to secure IBM i’s
- Detects events that are related to security and traceability
- A unique Expert System assesses the risk of each of these events
- Data is sent to a dispatcher that determines the actions to be carried out, according to the customer’s configuration
  - Archiving in a data repository, centralizing all the IBM i partitions (with a graphical consultation interface)
  - Alert trigger
  - Send to an external SIEM (Qradar, Sentinel…)
  - Transmit to a SOC (Security Operation Center)

Available probes : audit log journal

- Password error
- Access violation attempt
- Object deletion
- Socket connection (non existing IP port)
- Netserver password error
- SSO connections
- SST/DST : profiles, actions
- User profiles
- IFS/DLO object deletion
- Audit management
- System values management
- PTF
- Rights adoption
- Object management
- Object restoration
- Network attributes
- Commands

Available probes : other probes

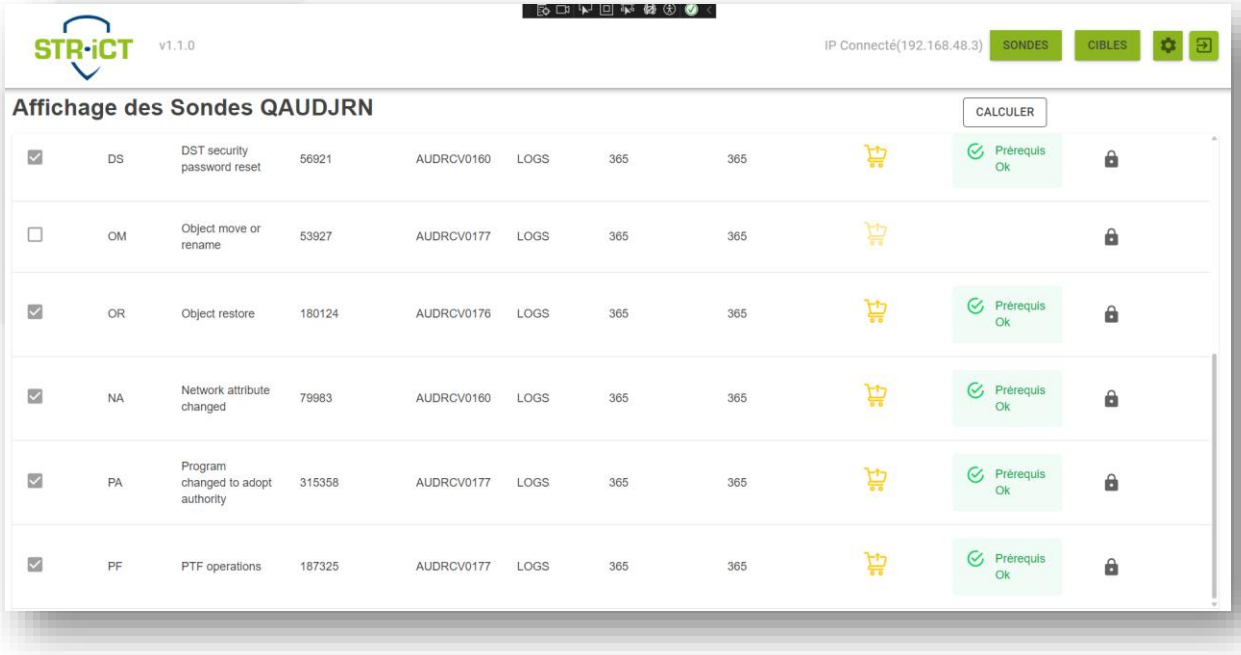
- Intrusion attempts detected by the IDS (Intrusion Detection System)
  - False positives management
- Exit points
  - FTP access
  - ODBC/JDBC access
  - IFS access
- Database traceability (Legacy)
  - Modification of areas of a file regardless of its origin
- Audit
  - Profiles
  - System values
  - Best practices
  - …
- Assure Security integration (PRECISELY ex CILASOFT)

The Expert System

- Objective: set the risk index induced by the event
- All our **experience**
- All our **cybersecurity knowledge**
- All cyber-attack mechanisms identified by our **honeypot** on the internet
  - Up to ~~30 000~~ ~~50 000~~ **100 000 attacks in one day**
  - A huge knowledge base of operating methods

DEMO - Probes configuration

- All the configuration is done graphically

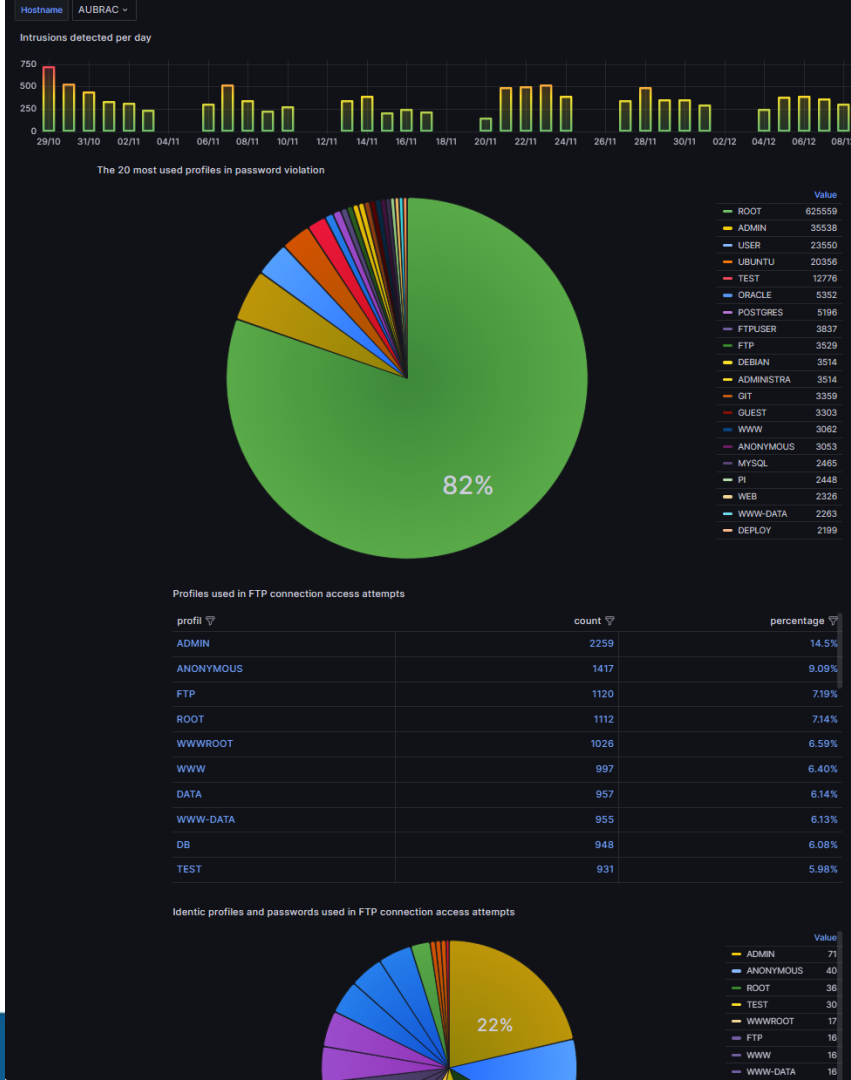


The dispatcher

- Receives data (Web Service)
- Depending on the configuration
  - Saves locally in a data repository (with a restitution graphical interface)
  - Sends to an external SIEM (Microsoft Sentinel, Elastic Search (ELK), IBM Qradar, SPLUNK…)
  - By Web Service or by Syslog
  - Generates alerts

DEMO - The data repository's graphical interface

- Based on Grafana
- Graphical, but with SQL queries possibilities
- Mutliple IBM i data agregation
- Easily adaptable



Are you SiEM or SIEM ?

- Security Information Event Manager
- SIEMs manage the security of entire network
  - But generaly not the IBM i !
- STR-iCT is a real SIEM in itself, dedicated to IBM i machines
  - Data acquisition, risk determination, alert, reporting
- SiEM : STR-iCT for IBM i Event Manager
- But STR-iCT also knows how to communicate with the other SIEMs on the market

Merci /
Thank you

FACQ GUIRAUD Guilian
guilian@gayte.it

KHAN Nauman
nk@blue-channel.com

https://i.gayte.it