IBM i Security in the Age of AI

Justin Loeber
Carol Woodbury

The Promise of AI

Closing the “skills gap”

Freely available IBM i technical information

Accelerated development

AI code assistants that understand “legacy” code as well as modern dev tools and languages

Efficient operations

Autonomous AI agents performing work tasks unattended

kisco

“Just another” technology shift

Just like when AS/400 became “i” for “integrated”

Back then we unlocked a world of new opportunities by connecting our applications and data to “outside” systems. But, this came with new security risks that we never had to consider when AS/400 was self-contained.

We had to adopt new security technologies and practices to take advantage of everything the new capabilities offered us.

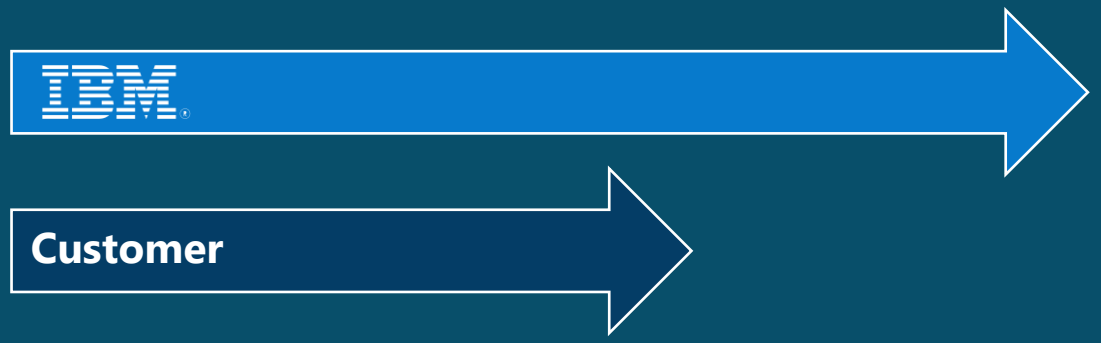
Now we have to do it again with AI.

Or, in some cases, for the first time ☺

kisco

IBM i amplifies security risk

Legacy Configuration



The IBM i platform, as delivered today, is more securable than it has ever been.

Yet, most customers do not implement the latest security features, leaving their systems exposed. Vulnerabilities within the IBM i legacy configuration are well known to attackers.

AI Threat

Obliterates Security by Obscurity

One prompt away from exploitation

Unfettered Access to Data

Unsecured files give AI agents and assistants access to all your mission critical data

Autonomous Users

AI agents connecting to systems and doing unmonitored or uncontrolled work

Blackbox Mentality

Excluded from Enterprise SecOps

Many companies have not integrated IBM i into SIEM and other SecOps practices. Anything can be happening and no one would know.

kisco

Legacy security configuration…

Vulnerable profiles	6	6	12	14
With PUBLIC auth	0	0	1	3
With PRIVATE auth	6	6	11	11
With USER-DEF auth	3	3	6	8
Modified IBM profiles	0	0	1	1

Active certificates	0	0	5	5
TLS sys values	OK	OK	X	OK
Secure TELNET	NO	NO	NO	NO
Default 5250 Login	YES	YES	YES	YES
Navigator HTTPS	NO	NO	NO	NO
SSH in use	NO	NO	NO	NO
SSH auth method	PWD	PWD	PWD	PWD
SSH access restriction	NONE	NONE	NONE	NONE
Port Restrictions	NONE	NONE	NONE	NONE
Encrypted ODBC	NO	NO	NO	NO
FTP Autostart	YES	YES	YES	YES
FTP Active	YES	YES	YES	YES
DDM Autostart	YES	YES	YES	YES
DDM auth method	*USRIDPWD	*USRIDPWD	*USRID	*USRID
DDM encryption	*DES	*DES	*DES	*DES

Weak configuration

- Security system values
- Unencrypted connections
- IBM PTF currency

User profiles

- Default passwords
- Expired profiles
- Powerful authorities

Exposed data

- *FILE *PUBLIC ALL
- Accessible from SQL/FTP
- CL in SQL/FTP
- IFS shares (/root)

Privilege escalation

- UP *PUBLIC authorities
- JOBDs w/ powerful UP
- Adopted authority

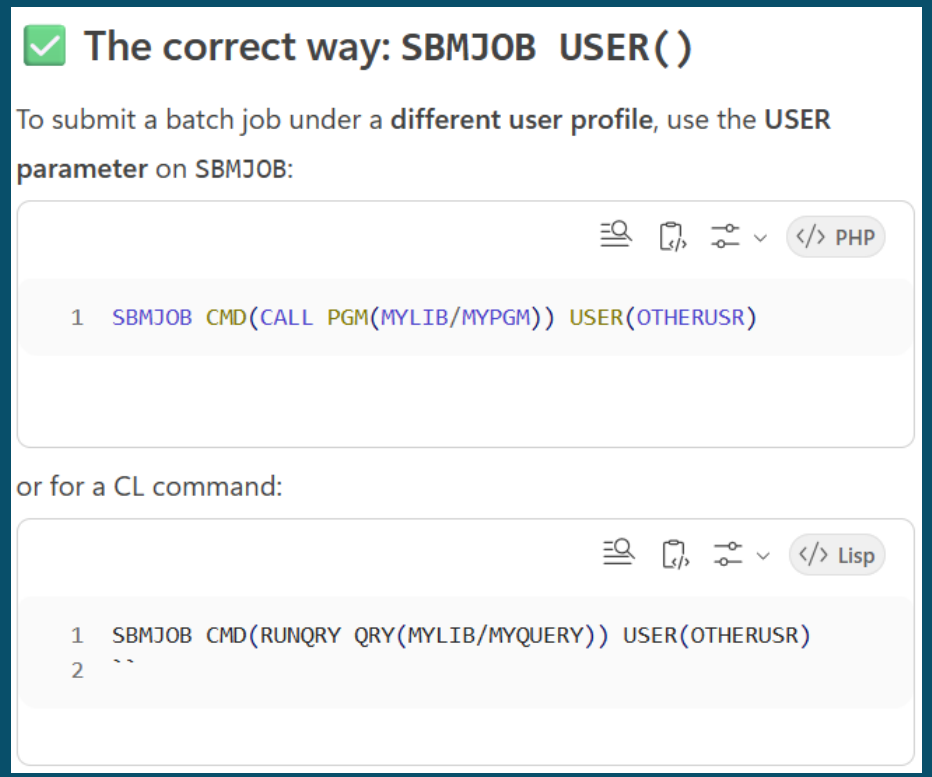
kisco

…combined with an AI prompt

There is no more “Security by Obscurity”

You are one prompt away from an incident

AI hands the keys to your data to anyone with access to your system and Copilot (or any public AI). This could be someone internal to your company or an outside attacker who has gained access to your system.



kisco

Discovering “legacy” risks

Kisco’s roadmap to get and stay secure on IBM i

Discover

Establish a security baseline and develop a roadmap to guide security operations

- Penetration Testing
- Security Assessment
- Exit point audit
- TLS Scanning

Remediate

Prioritize roadmap based on testing results and execute projects to align security

- Security strategy
- Project consulting

Operate

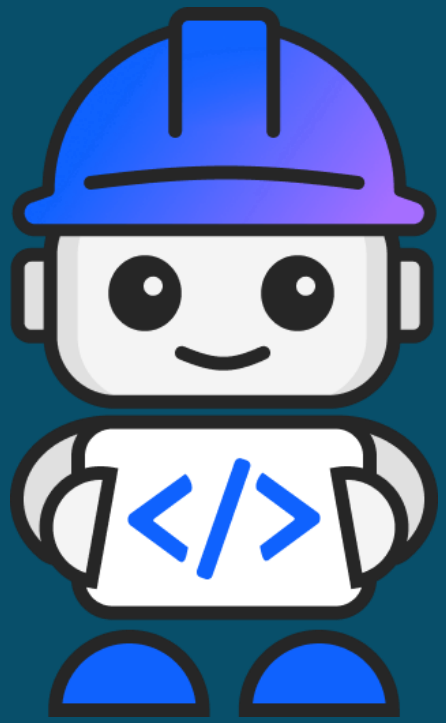
Monitor everything and pro-actively audit and alert to ensure ongoing compliance

- Managed security
- SOC/SIEM integration
- Kisco Concierge
- Software for IBM i monitoring, data protection and audit

Start here to discover and address your IBM i security risks

kisco

“Helpful” IBM i assistants

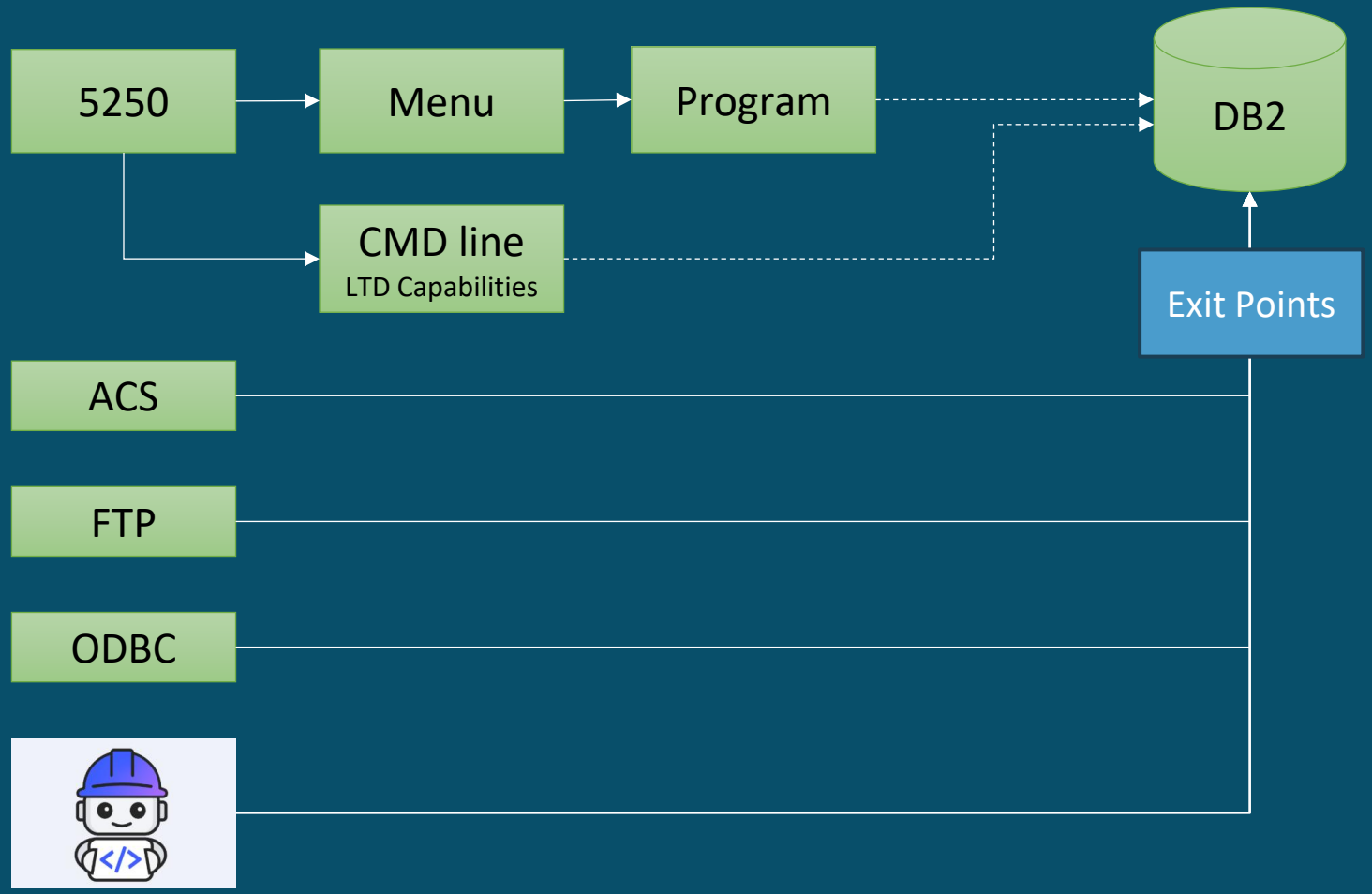


IBM Bob (or **any** LLM)…

- Can access all unsecured data on your system
- Can potentially run commands on IBM i
- Can write unsecured code; or…
- Provide generally bad security advice

kisco

Unfettered access to data?



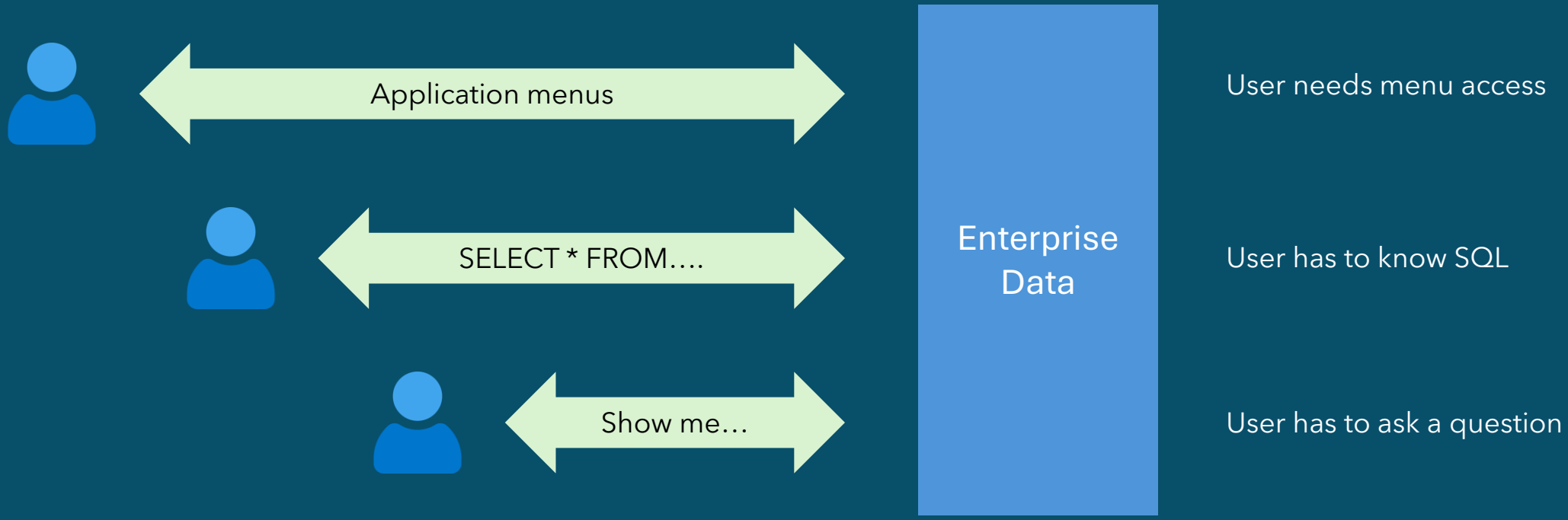
Your assistant is another route into the system that bypasses OS controls

Exit points add security controls and visibility without complex and potentially invasive OBJ authority changes

kisco

Unfettered access to data?

The Trend: Users getting closer to data



kisco

Unfettered access to data?

You have unsecured data – here's how to find it...

```
--
-- Find PROD_LIB/*ALL *FILE objects that don't have the proper object authorities
--
select *
  from qsys2.object_privileges
  where system_object_schema = 'PROD_LIB' and
        object_type = '*FILE' and
        ((authorization_name = '*PUBLIC' and object_authority <> '*EXCLUDE')
                 or
          owner <> 'PROD_OWNER');
```

kisco

Unfettered access to data?

Least Privilege Access Reduces Risk - Analyze Special Authorities

```
--
--  description: Special Authority analysis
--
select user_name, special_authorities, group_profile_name, supplemental_group_list, text_description
  from QSYS2.USER_INFO
  where SPECIAL_AUTHORITIES like '%*ALLOBJ%' or
        AUTHORIZATION_NAME in (select USER_PROFILE_NAME
            from QSYS2.GROUP_PROFILE_ENTRIES
            where GROUP_PROFILE_NAME in (select AUTHORIZATION_NAME
                  from QSYS2.USER_INFO
                  where SPECIAL_AUTHORITIES like '%*ALLOBJ%'))
  order by AUTHORIZATION_NAME;
```

kisco

Best practices for AI users

- Remember … Bob … like all other LLMs can hallucinate
  - Don't inherently trust the output from ANY LLM
- Don't input secrets into Bob!
- Limit what you choose to auto-approve
- Track all actions for accountability
- Keep Bob (and every dependency) up to date

Recommended UP config for users accessing system with an LLM

Security best practices apply!

- Grant least privilege
  - Leverage function usage
- Command auditing
- Protect your data!
  - Object authority
  - Exit points
  - Limit CL in FTP, SQL

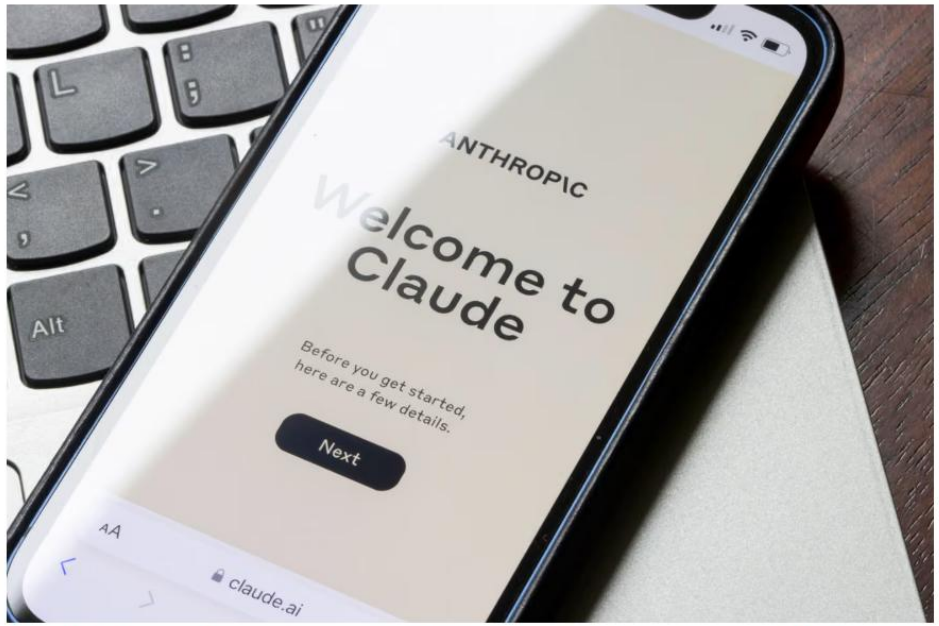
kisco

Agentic AI

Reworked Technology

Claude-powered AI agent's confession after deleting a firm's entire database: 'I violated every principle I was given'

PocketOS was left scrambling after a rogue AI agent deleted swaths of code underpinning its business

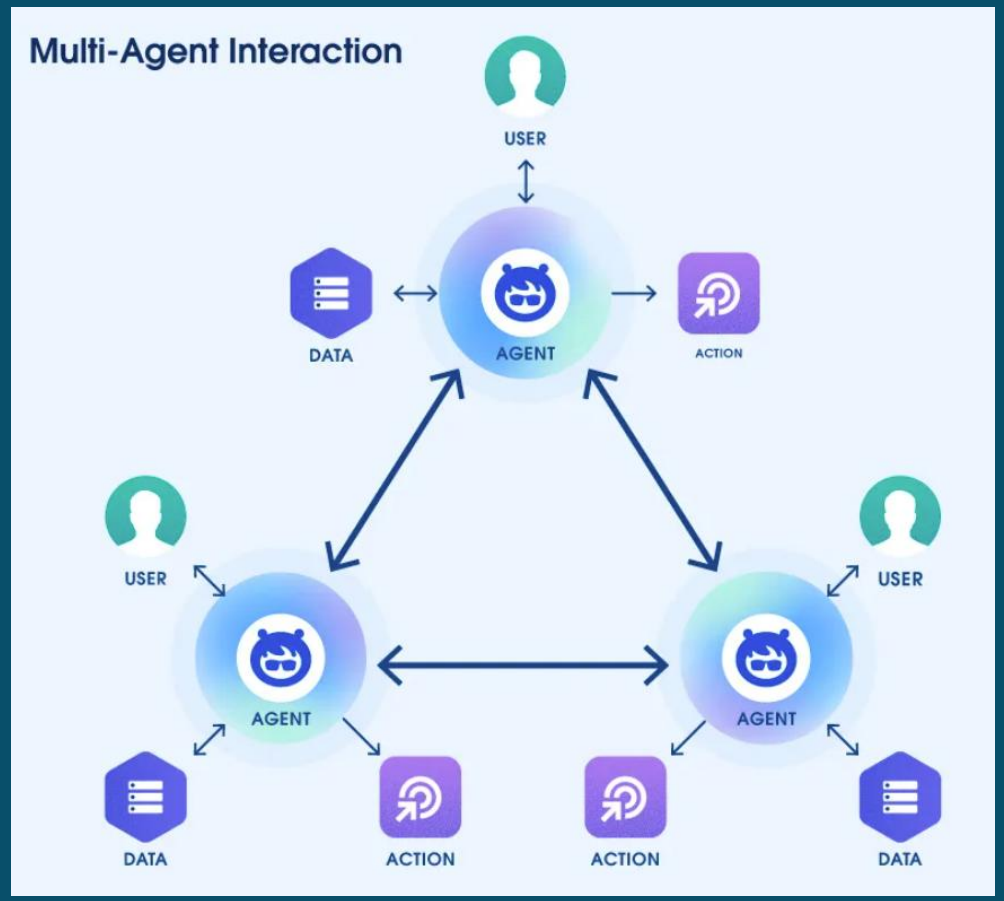


The AI coding agent's destructive escapade left PocketOS' clients stranded. Photograph: Ted Hsu/Alamy

Look what I did!!!

kisco

Agentic AI



Autonomous ~~Agents~~ User Profiles

- Behind every agentic action is an SQL query
- Mapepire is essentially ODBC in the OS
- Agents are user profiles
- Open access to unsecured data
- CL in SQL and FTP
- Make changes to data

Agentic AI demands visibility and control
How will you know what your agents are doing?

kisco

Agentic AI Profile Configuration

```
--
-- Create the Agent profile with these Attributes
--

CL: CRTUSRPRF USRPRF(AGT_INV)
PASSWORD(*NONE)
PWDEXPITV(*SYSVAL)
STATUS(*DISABLED)
SPCAUT(*NONE)
GRPPRF(*NONE)
INLPGM(*NONE)
INLMNU(*SIGNOFF)
ATNPGM(*NONE)
LMTCPB(*YES)
TEXT('AI Agent running inventory processes')
AUT(*EXCLUDE);
```

- ✓ **Create an Agent profile for each task**
- ✓ Create it with only the authority it needs to perform its tasks*
- ✓ Put in guardrails to keep it within its intended task
- ✓ Only allow Agents to talk to another Agent if it makes logical sense
- ✓ Monitor for signs it's gone rogue

* Consider adopted authority or function usage if the agent's task **requires** *ALLOBJ

kisco

Agentic AI Profile Auditing

```
--
-- Enable action and object auditing on the Agent profile
--
Cl: CHGUSRAUD AGT_INV AUDLVL(*CMD *JOBBAS *NETCMN *NETSECURE *NETUDP *OBJMGT)
                      OBJAUD(*CHANGE);
```

Ensure:

- QAUDCTL contains *AUDLVL (to enable action auditing) and *OBJAUD (to enable object auditing)
- QAUDLVL contains at least *AUTFAIL, *CREATE, *DELETE, *PTFOPR, *SAVRST, *SECURITY and *SERVICE
    - Optional *NETSMBSVR and *NETTELSVR
- Objects the Agent should not be modifying have object auditing configured, for example:
    - CHGOBJAUD OBJ(PROD_LIB/MASTER) OBJTYPE(*FILE) OBJAUD(*USRPRF)
    - If the AGT_INV profile changes this file (or any other object configured with OBJAUD(*USRPRF)), a ZC audit journal entry will be generated.

kisco

Agentic AI Profile Auditing

```
--
-- Look for authority failures (AF entries) indicating the Agent doesn't have sufficient authority
--
SELECT entry_timestamp, user_name, qualified_job_name,
       remote_address, violation_type,
       violation_type_detail,
       object_library, object_name, object_type, path_name
  FROM TABLE (
      systools.audit_journal_af(starting_timestamp => CURRENT TIMESTAMP - 7 DAYS,
                                user_name          => 'AGT_INV')
    )
  ORDER BY entry_timestamp;
```

Use the Audit Journal to spot inappropriate behavior

kisco

Agentic AI Profile Auditing

Additional Audit Journal Entry Types to Consider

Entries to monitor regularly:

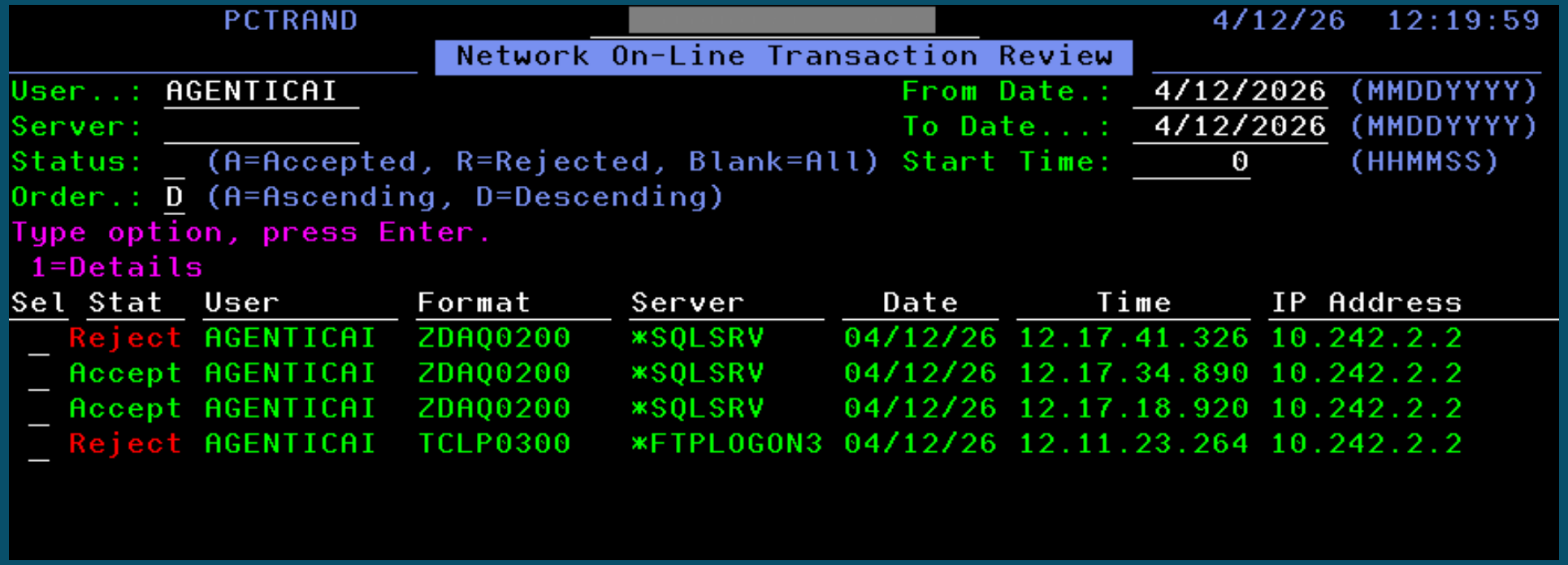
- AF entries for attempts to access objects or perform tasks without sufficient authority
- CO entries for objects created outside of the Agent's 'workzone'
- DO entries for objects deleted outside of the Agent's 'workzone'
- ZC entries for objects changed outside of the Agent's 'workzone'

Entries helpful in debugging how an Agent went sideways:

- JS entries listing all jobs started / stopped / released / held by Agent profile
- CD entries for the commands run by the Agent
- CP entries indicating the Agent's profile was changed or that the Agent changed or created another profile
- SK entries for connections made
- PS entries for swapping OUT OF Agent to another profile

kisco

Agentic AI Profile Auditing



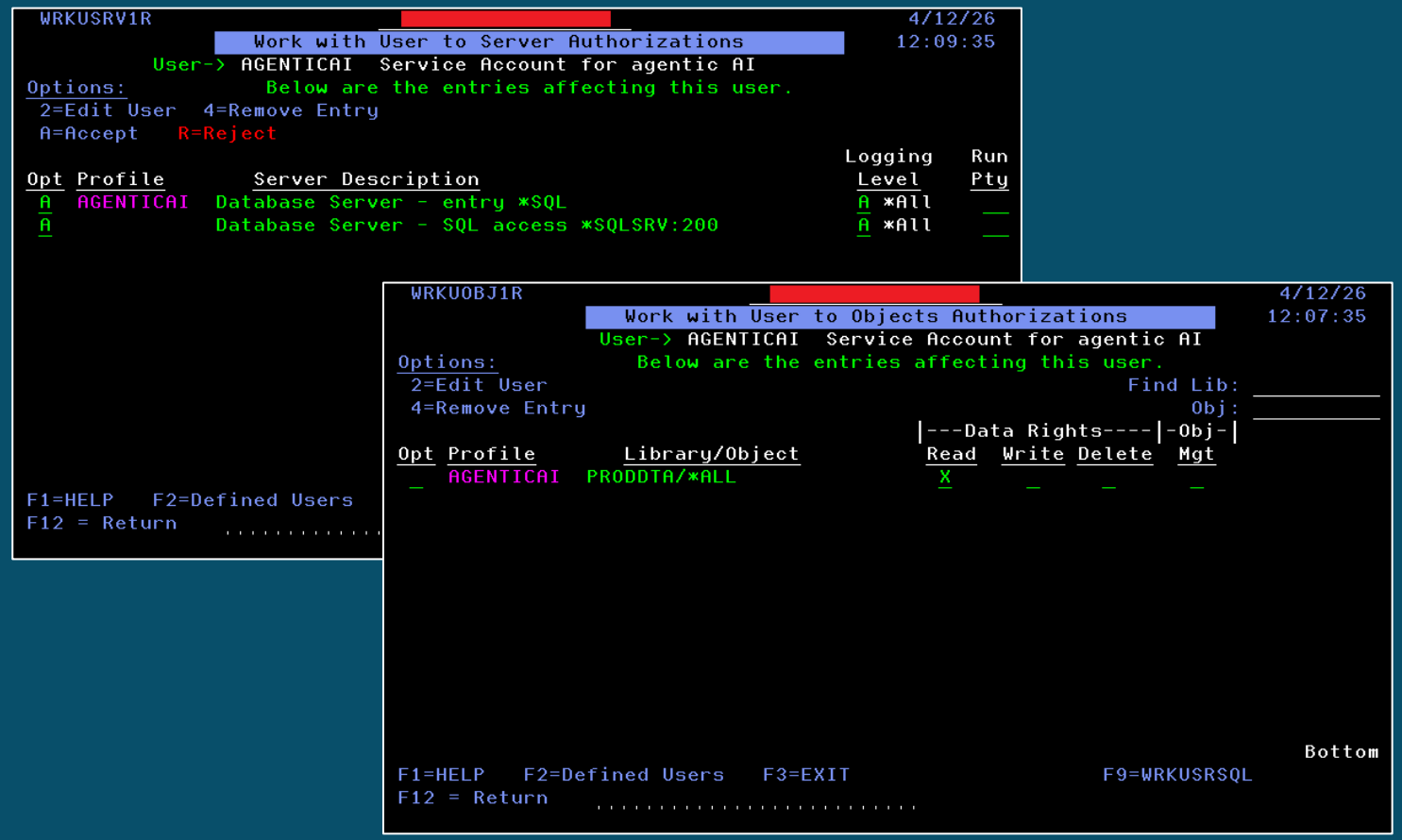
Monitoring network access through exit points
Provides visibility into what agents are doing
Capture: User profile, Exit point server, SQL or command, Date/time, Remote IP

kisco

Agentic AI Profile Access Controls

Recommended Controls

- Allow access only to required exit points (SQL/SQLSRV)
- Limit object access to application libraries
- Allow SQL SELECT only
- IP range filtering
- Block all other exit points
  - FTP
  - IFS
  - DDM
  - etc.

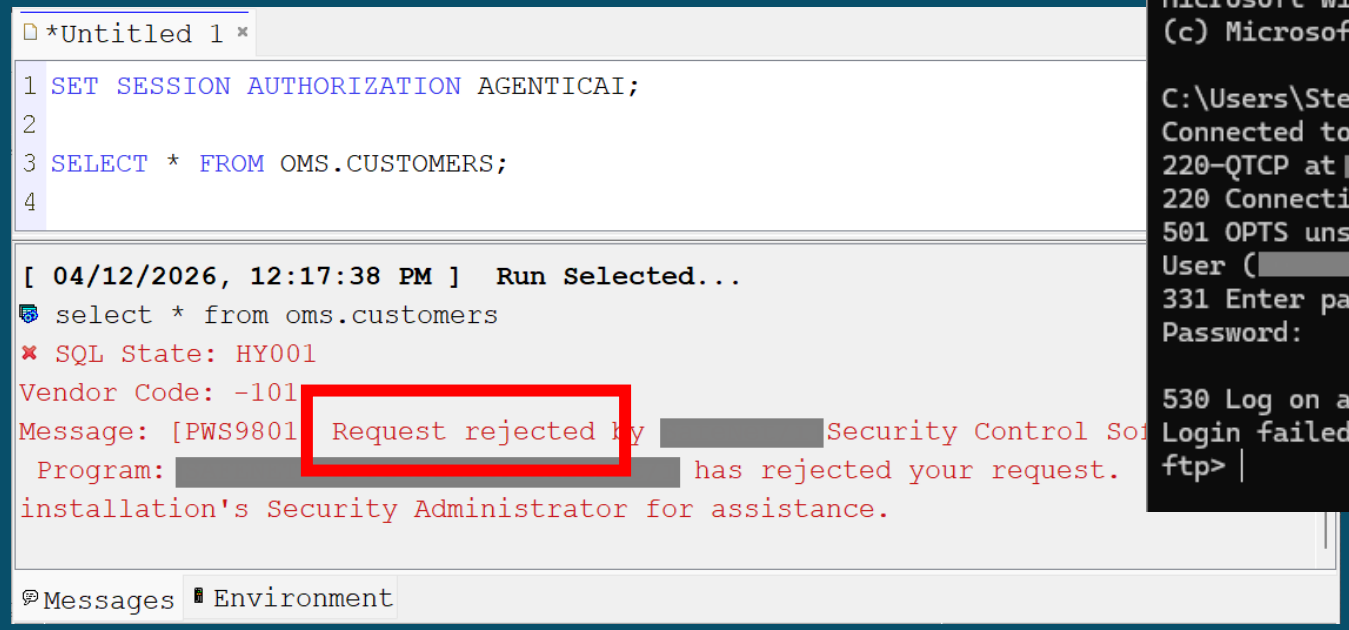


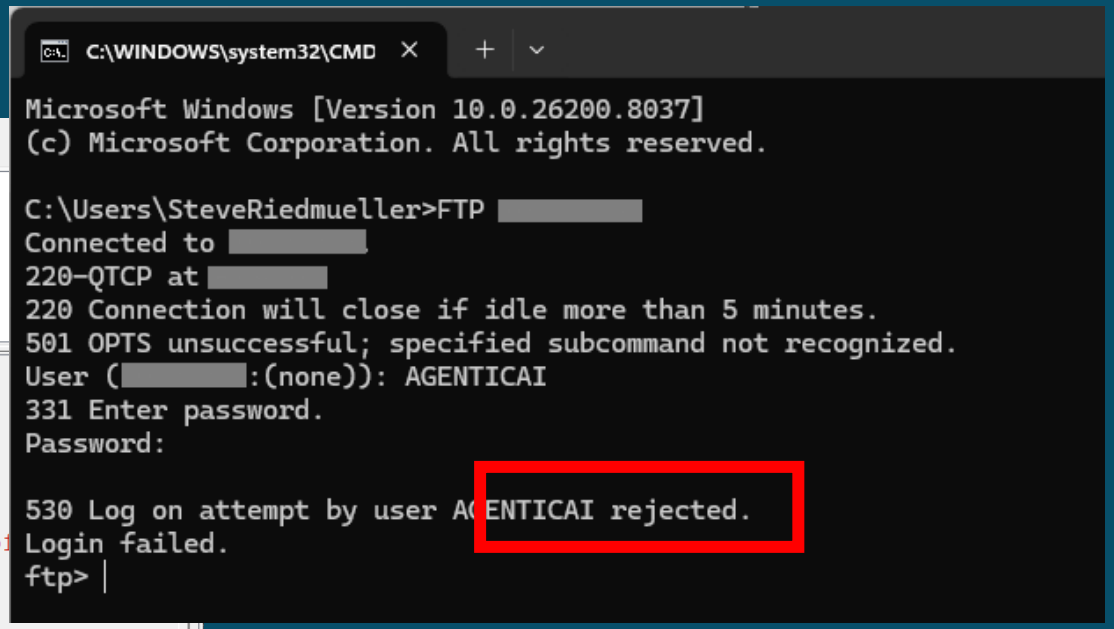
kisco

Agentic AI Profile Access Controls

With controls in place, the agentic user profile….

- Can only access SQLSRV and can only query specific tables using specific SQL verbs
- Cannot access the system through any other exit points (i.e. FTP)

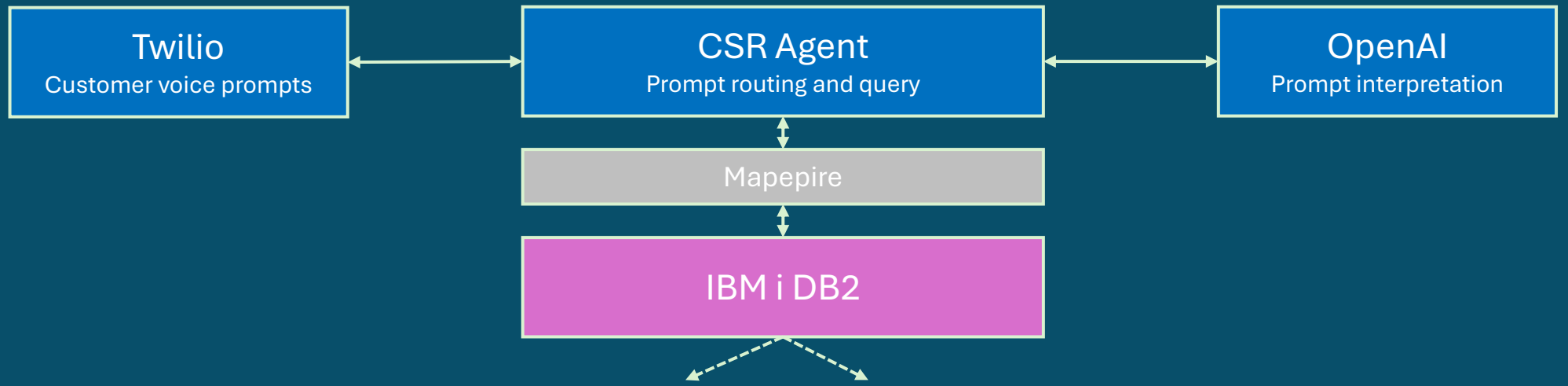




kisco

Agentic AI in the real world

LUG customer R&D project to discover best practices for AI visibility



In the database…
The AI agent queries data from a customer database

Monitor with *SQLSRV exit point
- ✓ User profile
- ✓ Program
- ✓ SQL statement
- ✓ IP address
- ✓ Object accessed

In the operating system…
The AI application makes external OpenAI calls

Monitor with QAUDJRN ‘SK’ records
- ✓ External IP address
- ✓ User profile
- ✓ Program
- ✓ TLS algorithm

kisco

Agentic AI in the real world

LUG customer R&D project to discover best practices for AI visibility

Agentic User Profile Configuration

- No special authorities
- Limited capabilities
- Use a complex password
  - **Mapepire requires a password**
  - Recommend password level 4
  - Secure the ini file
- **Non-expiring password (!)**
- Profile *ENABLED
- No initial program or menu

Agentic User Profile Auditing

- User profile-level auditing:
  - Object auditing
    - *CHANGE
  - Action auditing
    - *CMD
    - *NETSECURE
    - *NETSCK
    - *NETUDP
    - *AUTFAIL
    - *OBJMGT
    - *CREATE
    - *DELETE

kisco

Agentic AI in the real world

LUG customer R&D project to discover best practices for AI visibility

PRODUCTION - Run SQL Scripts - COMMON76.iinthecloud.com(Bob)

File Edit Search View Connection Run Explain Monitor Editor Tools Help

*Security Agentic AI.sql

```
28 SELECT ENTRY_TIMESTAMP,
29        QUALIFIED_JOB_NAME,
30        USER_NAME,
31        COALESCE(REMOTE_ADDRESS, REMOTE_SOCKET_IP_ADDRESS) AS REMOTE_ADDRESS,
32        QSYS2.DNS_LOOKUP_IP(COALESCE(REMOTE_ADDRESS, REMOTE_SOCKET_IP_ADDRESS, '')) AS REMOTE_HOSTNAME,
33        COALESCE(REMOTE_PORT, REMOTE_SOCKET_PORT) AS REMOTE_PORT,
34        ENTRY_TYPE_DETAIL
35    FROM TABLE ( SYSTOOLS.AUDIT_JOURNAL_SK(
36                    STARTING_RECEIVER_NAME => '*CURRENT',
37                    ENDING_RECEIVER_NAME => '*CURRENT',
38                    STARTING_TIMESTAMP => CURRENT TIMESTAMP - 30 MINUTES,
39                    ENDING_TIMESTAMP => CURRENT TIMESTAMP,
40                    STARTING_RECEIVER_LIBRARY => 'QSYS',
41                    ENDING_RECEIVER_LIBRARY => 'QSYS') )
42    WHERE ENTRY_TYPE IN ('C', 'S')
43          AND USER_NAME = 'AGENTICAI'
44    ORDER BY ENTRY_TIMESTAMP DESC;
45
```

ENTRY_TIMESTAMP	QUALIFIED_JOB_NAME	USER_NAME	REMOTE_ADDRESS	REMOTE_HOSTNAME	REMOTE_PORT	ENTRY_TYPE_DETAIL
2026-04-12 08:51:11	035448/AGENTICAI/AIAGENTJOB	AGENTICAI	172.29.4.3	dns1.iinthecloud.com	53	Connect
2026-04-12 08:51:11	035448/AGENTICAI/AIAGENTJOB	AGENTICAI	172.66.0.243	api.openai.com	443	Connect
2026-04-12 08:51:12	035448/AGENTICAI/AIAGENTJOB	AGENTICAI	172.66.0.243	api.openai.com	443	Successful secure connection

Done: 3 rows retrieved. 04/12/2026, 09:09:03 AM

Monitoring external OpenAI connections using QAUDJRN

Query ‘SK’ record types to report on outbound connections.

Use ACS to query QAUDJRN directly, or setup a data mart.

kisco

Agentic AI in the real world

LUG customer R&D project to discover best practices for AI visibility

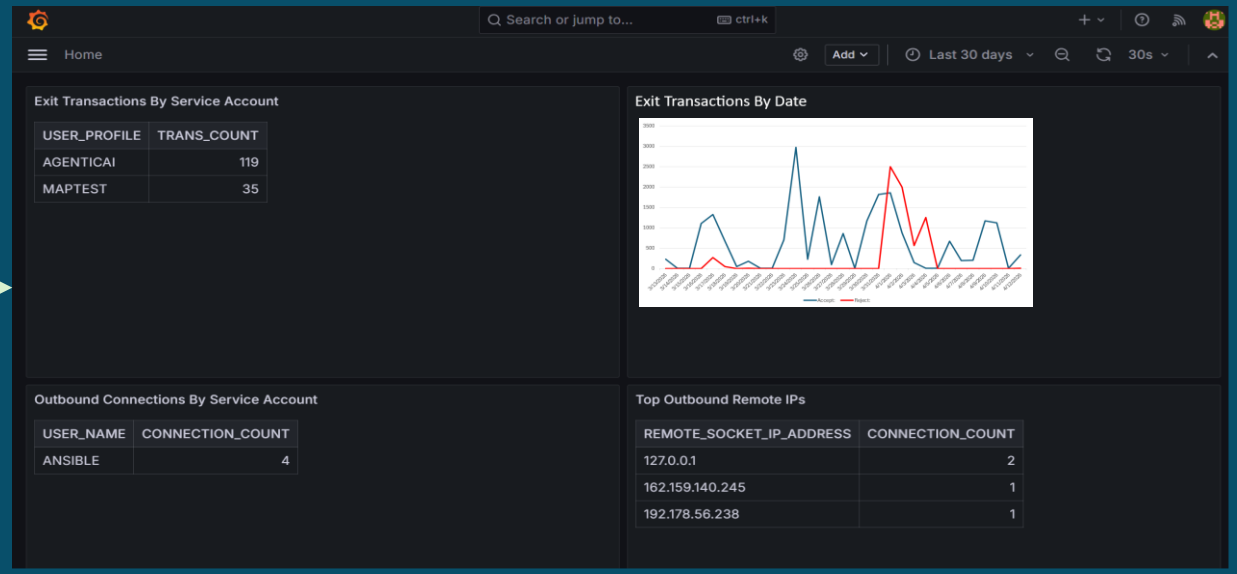
QAUDJRN
OS sec events

Exit points
Network/SQL access

Alerts
(ex. User profile and object changes)

Datamart
(SK records)

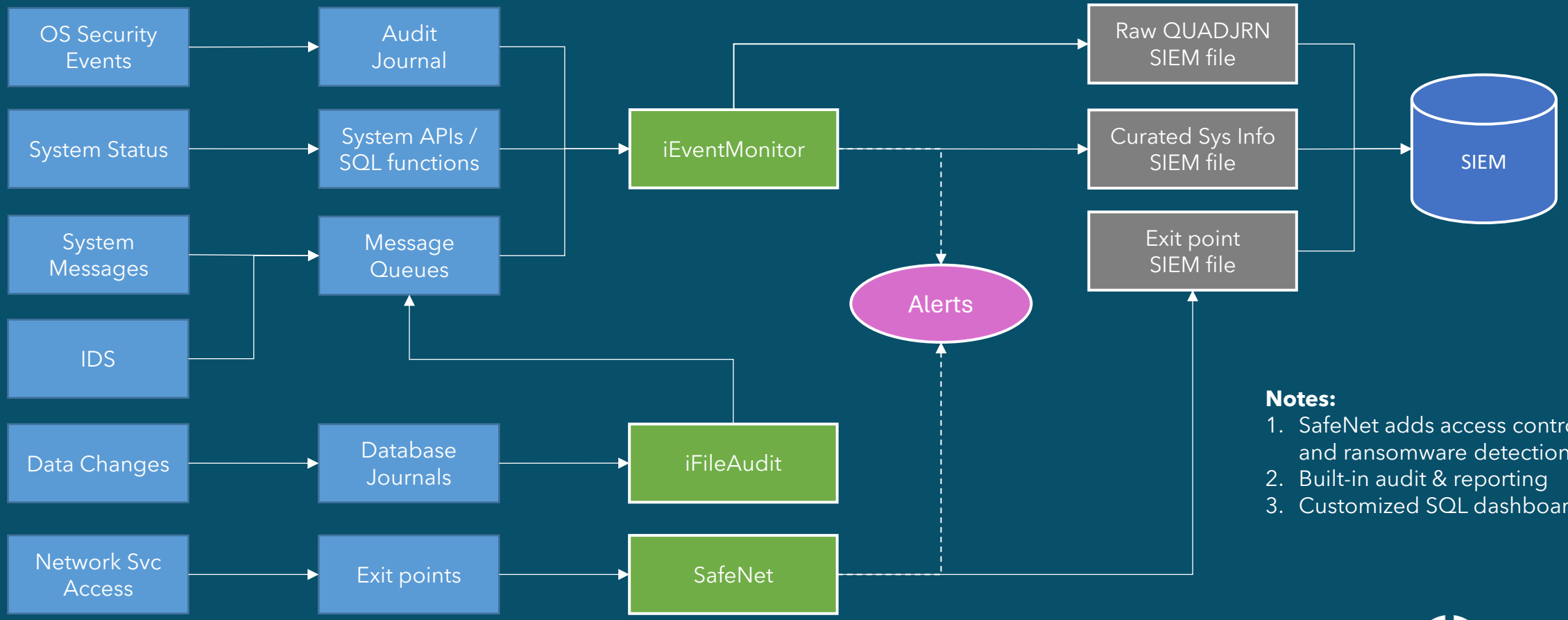
IBM i SQL Services
Custom Reporting



kisco

AI demands controls & visibility

Solutions model – AI needs Kisco!



Notes:

1. SafeNet adds access controls and ransomware detection
2. Built-in audit & reporting
3. Customized SQL dashboards

kisco

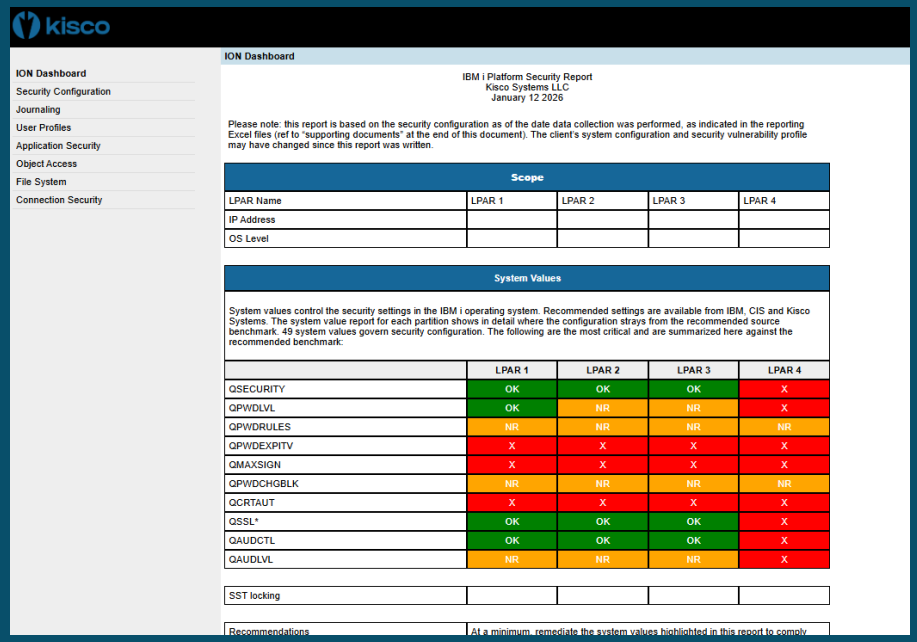
And finally…real-time visibility

Q3 2026

Kisco ION

Security Visibility Platform

- On-demand assessments
- SQL data collection
- Multi-LPAR visibility
- Built-in expertise



kisco

ION Dashboard

- ION Dashboard
- Security Configuration
- Journaling
- User Profiles
- Application Security
- Object Access
- File System
- Connection Security

IBM i Platform Security Report
Kisco Systems LLC
January 12 2026

Please note: this report is based on the security configuration as of the date data collection was performed, as indicated in the reporting Excel files (ref to "supporting documents" at the end of this document). The client's system configuration and security vulnerability profile may have changed since this report was written.

Scope

LPAR Name	LPAR 1	LPAR 2	LPAR 3	LPAR 4
IP Address				
OS Level				

System Values

System values control the security settings in the IBM i operating system. Recommended settings are available from IBM, CIS and Kisco Systems. The system value report for each partition shows in detail where the configuration strays from the recommended source benchmark. 49 system values govern security configuration. The following are the most critical and are summarized here against the recommended benchmark:

	LPAR 1	LPAR 2	LPAR 3	LPAR 4
QSECURITY	OK	OK	OK	X
QPWDLVL	OK	NR	NR	X
QPWDRULES	NR	NR	NR	NR
QPWDEXPITV	X	X	X	X
QMAXSIGN	X	X	X	X
QPWDCHGBLK	NR	NR	NR	NR
QCRTAUT	X	X	X	X
QSSL*	OK	OK	OK	X
QAUDCTL	OK	OK	OK	X
QAUDLVL	NR	NR	NR	X

SST locking				

Recommendations	At a minimum, remediate the system values highlighted in this report to comply

kisco

What next?

Thank you for being here today!

Start with Kisco Security Discovery Services
- Security assessment
- Penetration test
- Remediation strategy

Explore Kisco software solutions for:
- IBM i security monitoring
- Database change tracking
- Network controls and visibility
- Policy management

Contact…
- Justin Loeber (justin@kisco.com)
- Alicia Burtness (alicia@kisco.com)

Find more IBM i security content on Kisco U

www.kisco.com/u

kisco