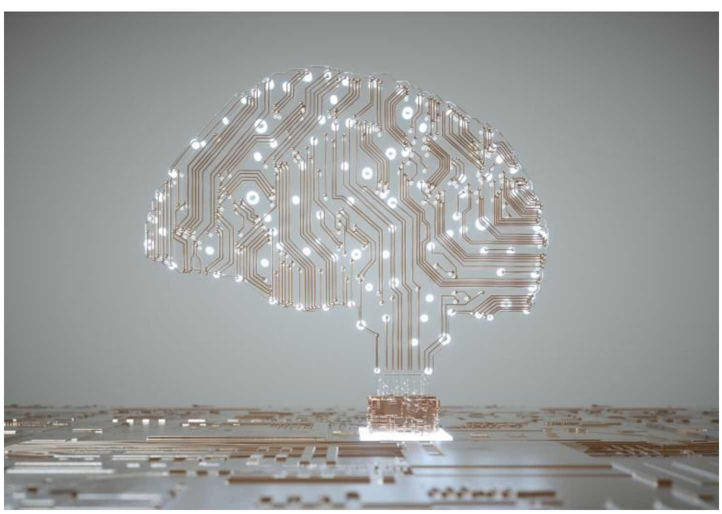
Security for You and A(i)

Justin Loeber
IBM CHAMPION
CEO, Kisco Systems
Board Member, COMMON US
justin@kisco.com

Carol Woodbury, CISSP, CRISC
IBM CHAMPION
IBM i Security SME and Senior Advisor, Kisco Systems
carol@kisco.com

kisco

1



AI is Here!

kisco

2

We Support/Approve of/Embrace AI !!!

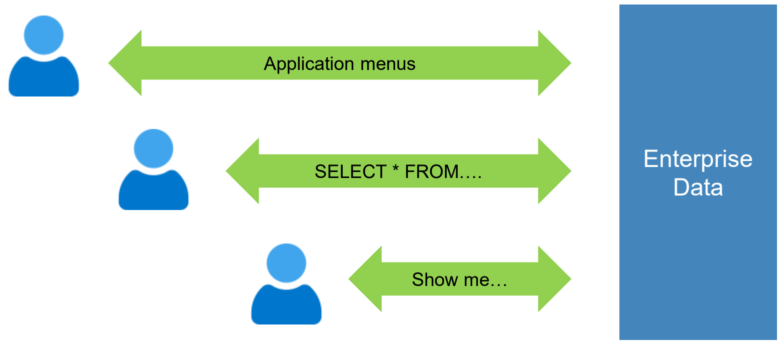
3

3

“Protect Your Data”

4

Users are Getting Closer to the Data



User needs menu access

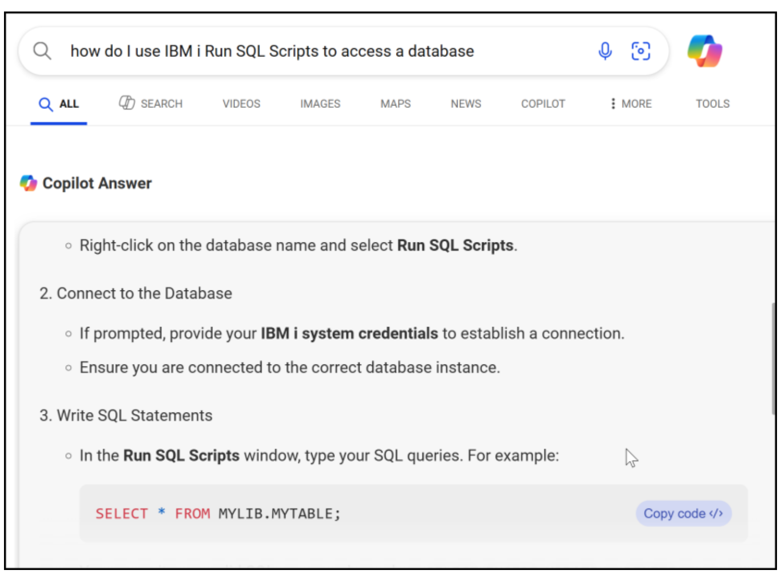
User has to know SQL

User simply asks a question or makes a prompt

The issue is not new… But AI makes it more urgent!

5

Microsoft Copilot – Using SQL

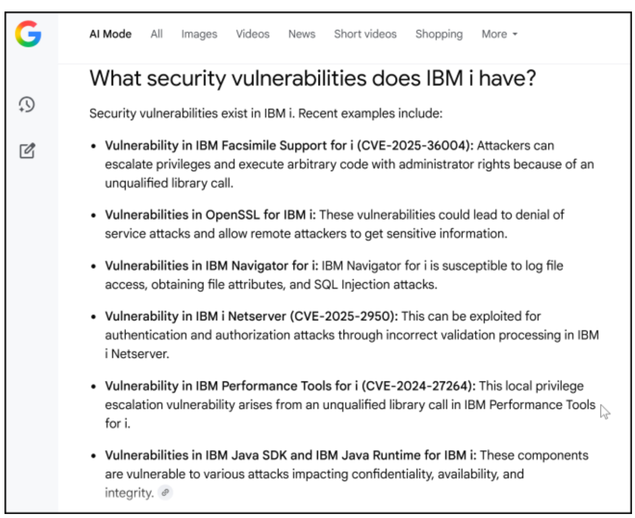


6

Microsoft Copilot – IBM i Vulnerabilities?

7

AI Mode



8

Costs of Organizations Ignoring Security for AI

Global average cost of a data breach = $4.44M

Additional cost when the breach is attributed to shadow AI = $670K

97% of organizations with AI-related breaches say they lacked proper AI access controls

Source: IBM / Ponemon Institute's Cost of a Data Breach 2025

9

Another Reason to Pay Attention to Security

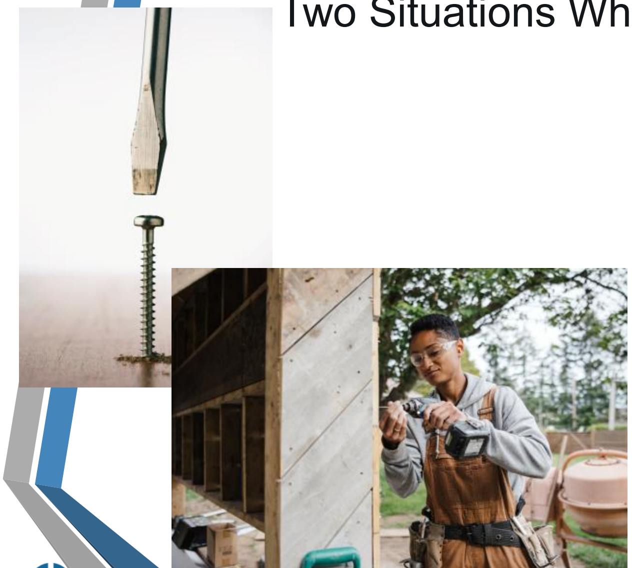
https://www.anthropic.com/glasswing

https://newsroom.ibm.com/2026-05-19-IBM-Brings-Its-Most-Advanced-AI-Powered-Security-Portfolio-to-Clients,-and-is-Strengthened-by-Ongoing-Project-Glasswing-Work

10

10

Two Situations Where AI is Being Applied



Power user wanting efficiency

Novice wanting knowledge/place to start

11

Initial Security Considerations for an AI Project

- What's the Use Case and what data does it require?
- Does it involve confidential or PII (Personally Identifiable Information)?
- Does everyone (from ... pers to users) understand the law ... ing this information as well as the Organiz ... use policies?
- Does your Organizatio ... ha ... t ... poli ... ies and procedures in place to ensure the project ... s 'Secure by design'?
- Does your Organization already implement the concept of 'Least privilege access'?
  - If not, start now!

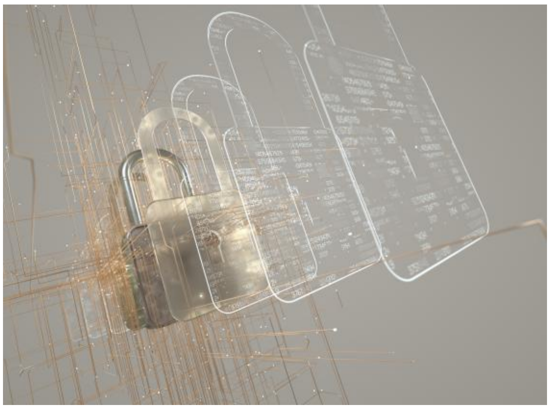
Get Ready

12

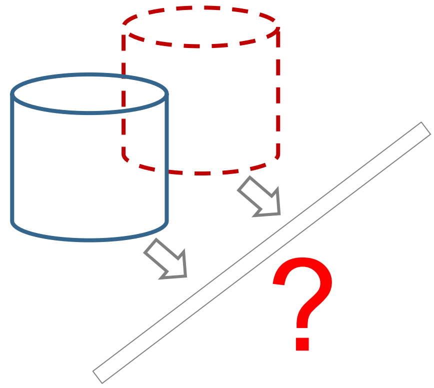
12

Data Must be Protected at Every Phase of an AI Project

Training and re-training phases, developers' gists, MCP configurations, etc.



Unintended consequence #1: Private or Confidential data is leaked, resulting in a breach



Unintended consequence #2: 'wrong' data is fed in resulting in 'inaccurate' results

kisco

13

Shadow AI

Use of AI outside

of the knowledge of IT

https://www.secureworld.io/industry-news/nca-report-humans-cyber-risk

kisco

14

Do NOT Share Secrets!

AI is not your bestie you can share everything with and be assured it goes no further! 15

kisco

15

AI Models Can … and Do … Hallucinate!

5 – 3 = 25

16

kisco

16

Have a Plan and Communicate it!

- What's the AI plan?
- What are the approved tools?
- What's the practice for educating users on the latest social engineering tactics?
  - What do they do if they suspect a threat?
  - What do they do if they're a victim?

17

AI Security Video Resources - fyi

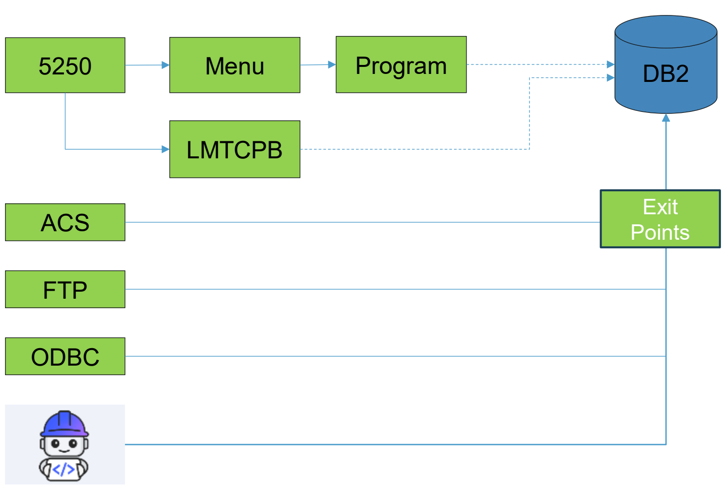
- Shadow AI, 'Identification crisis'
  - https://techchannel.com/techtalk-smb/george-totev/
- Digital twin
  - https://www.bankinfosecurity.com/ai-worker-digital-twins-pose-new-insider-threats-a-29238

18

Agentic AI

19

With Agents Users are Even Closer



Your assistant is another route into the system that will exploit a poorly secured system

Exit point software may be in place but ‘rules’ are rarely used

20

Reworked Technology

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

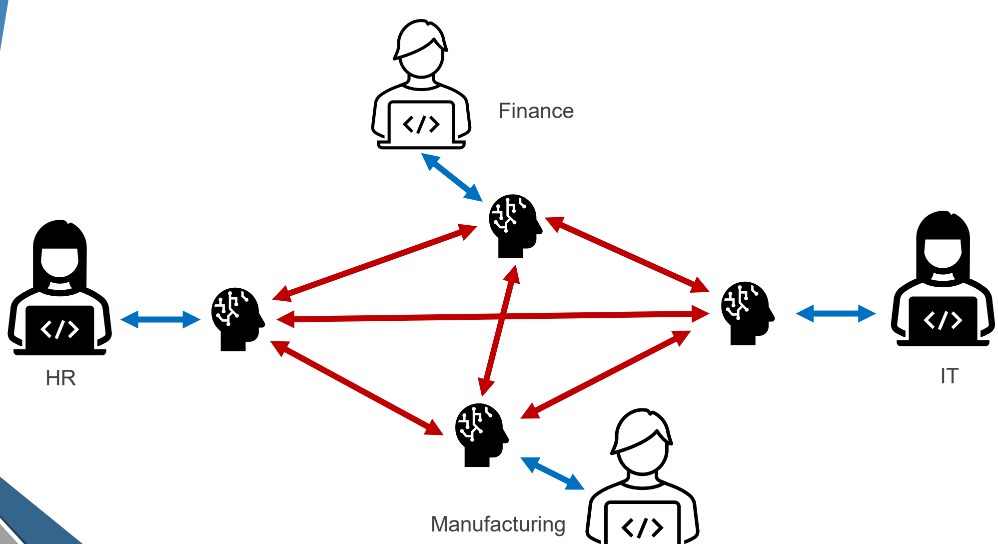
PocketOS was left scrambling after a rogue AI agent deleted swaths of code underpinning its business

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

Look what I did!!!

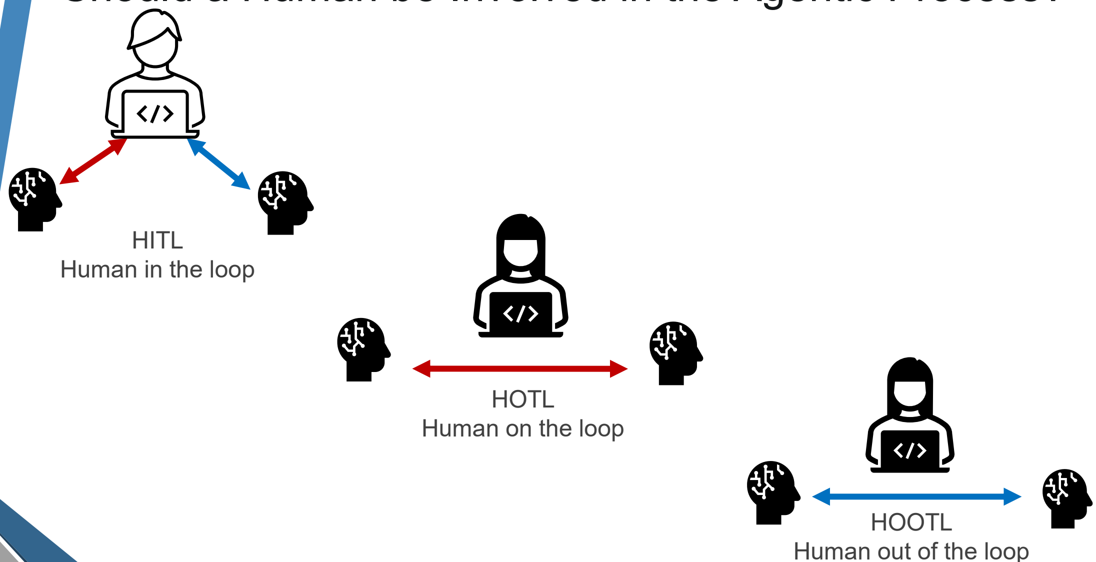
21

Agentic AI



22

Should a Human be Involved in the Agentic Process?



23

Agentic AI

- Do all agents *really* need to talk to one another?
- Where/When should humans be involved?
- Configure agents with least privilege access
- How will you detect inappropriate behavior?
- Will make more sophisticated social engineering attacks
  - https://www.securityweek.com/how-hackers-manipulate-agentic-ai-with-prompt-engineering/
- Vibe hacking
  - https://www.bankinfosecurity.com/event-horizon-for-vibe-hacking-draws-closer-anthropic-warns-a-29339
- On the other hand, it can make detection and patching quicker
  - https://www.darkreading.com/application-security/gen-ai-accelerates-triage-of-software-vulnerabilities

24

The Key to Protecting Your Organization…

Protect your Data

Implement Least Privilege Access

Gain Visibility into an Agent's Actions

25

Recommendations when Creating an AI Agent

- 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

26

26

Create the Agent Profile with Least Privilege Access

```
▪ --
▪ -- 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 the Agent profile with only the authority required to perform the task – no more! 27

27

Change the Agent Profile to have these Auditing Attributes

```
--
-- 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.

28

28

Use the Audit Journal to Detect Inappropriate Behavior

```
--
-- 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;
```

29

29

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 'work zone'
- DO entries for objects deleted outside of the Agent's 'work zone'
- ZC entries for objects changed outside of the Agent's 'work zone'

Entries helpful in debugging how an Agent went sideways/rogue:

- 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

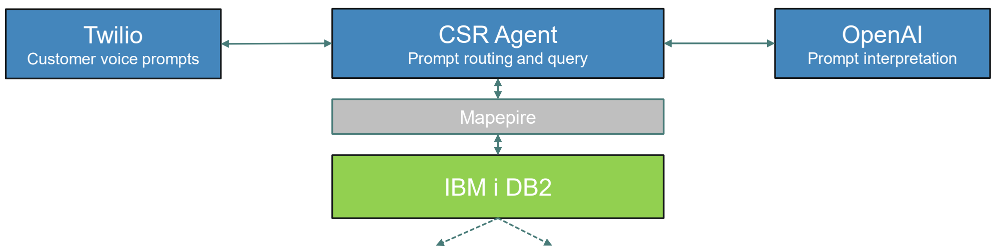
➡ If you have exit program software, review those logs for Agent activity, including failed access attempts

30

30

Agentic AI: A Case Study

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

31

Agentic AI: Agent Profile Configuration

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

32

Agentic AI: Outbound Connections

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

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

*Security Agentic AI.sql

```sql
SELECT ENTRY_TIMESTAMP,
       QUALIFIED_JOB_NAME,
       USER_NAME,
       COALESCE(REMOTE_ADDRESS, REMOTE_SOCKET_IP_ADDRESS) AS REMOTE_ADDRESS,
       QSYS2.DNS_LOOKUP_IP(COALESCE(REMOTE_ADDRESS, REMOTE_SOCKET_IP_ADDRESS, '')) AS REMOTE_HOSTNAME,
       COALESCE(REMOTE_PORT, REMOTE_SOCKET_PORT) AS REMOTE_PORT,
       ENTRY_TYPE_DETAIL
  FROM TABLE ( SYSTOOLS.AUDIT_JOURNAL_SK(
                   STARTING_RECEIVER_NAME => '*CURRENT',
                   ENDING_RECEIVER_NAME => '*CURRENT',
                   STARTING_TIMESTAMP => CURRENT TIMESTAMP - 30 MINUTES,
                   ENDING_TIMESTAMP => CURRENT TIMESTAMP,
                   STARTING_RECEIVER_LIBRARY => 'QSYS',
                   ENDING_RECEIVER_LIBRARY => 'QSYS') )
  WHERE ENTRY_TYPE IN ('C', 'S')
      AND USER_NAME = 'AGENTICAI'
  ORDER BY ENTRY_TIMESTAMP DESC;
```

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.

33

Agentic AI: Connects via ODBC

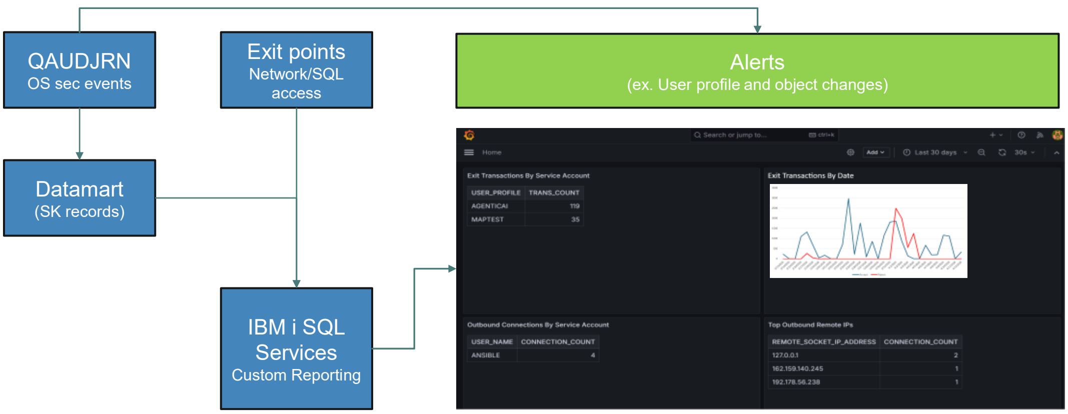
```
               PCTRAND                                        4/12/26   12:19:59
                             Network On-Line Transaction Review
User..:  AGENTICAI                          From Date.:  4/12/2026 (MMDDYYYY)
Server:                                     To Date...:  4/12/2026 (MMDDYYYY)
Status:  _ (A=Accepted, R=Rejected, Blank=All) Start Time:       0  (HHMMSS)
Order.:  D (A=Ascending, D=Descending)
Type option, press Enter.
 1=Details
Sel Stat   User       Format     Server     Date     Time         IP Address
 _  Reject AGENTICAI  ZDAQ0200   *SQLSRV    04/12/26 12.17.41.326 10.242.2.2
 _  Accept AGENTICAI  ZDAQ0200   *SQLSRV    04/12/26 12.17.34.890 10.242.2.2
 _  Accept AGENTICAI  ZDAQ0200   *SQLSRV    04/12/26 12.17.18.920 10.242.2.2
 _  Reject AGENTICAI  TCLP0300   *FTPLOGON3 04/12/26 12.11.23.264 10.242.2.2
```

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

34

Agentic AI: Visibility

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



35

Security Best Practices for AI Projects

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

On IBM i
- Secure your data at every stage of the process
- Implement one agent per process
- Implement least privilege access
- Configure auditing
- Monitor!

36

Redbook – Refresh

- AI, MCP Server and Other Security Considerations

2014

Coming Now!

"Modernizing IBM i Applications"

2026

37

kisco

37

For More Information

[Bob Security Guidance]

[Bob and MCP Servers]

[Github Security Features]

IBM i Services- https://www.ibm.com/support/pages/node/1119123

Memo to Users – 7.5 and 7.6

IBM i 7.6 Redbook - https://www.redbooks.ibm.com/redpieces/pdfs/sg248588.pdf

IBM i Security Reference – PDF

IBM i Security Administration and Compliance, 3rd edition, by Carol Woodbury, 2020 available from Amazon or MCPress Bookstore

Mastering IBM i Security – A Step by Step Approach by Carol Woodbury, 2022 available from Amazon or MCPress Bookstore

Whitepaper: Securing IBM i: A Dual Responsibility

Kisco U – free articles and tutorials, for example …
https://www.kisco.com/u/content/subscribe-to-ibm-notifications-for-ibm-i.html

38

kisco

38

Questions?

Contacts:
justin@kisco.com
carol@kisco.com

39