

IBM i Threat Landscape 2026

A Fireside Chat with Carol Woodbury

Carol Woodbury, CISSP, CRISC



IBM i Security SME and Senior Advisor, Kisco Systems

carol@kisco.com



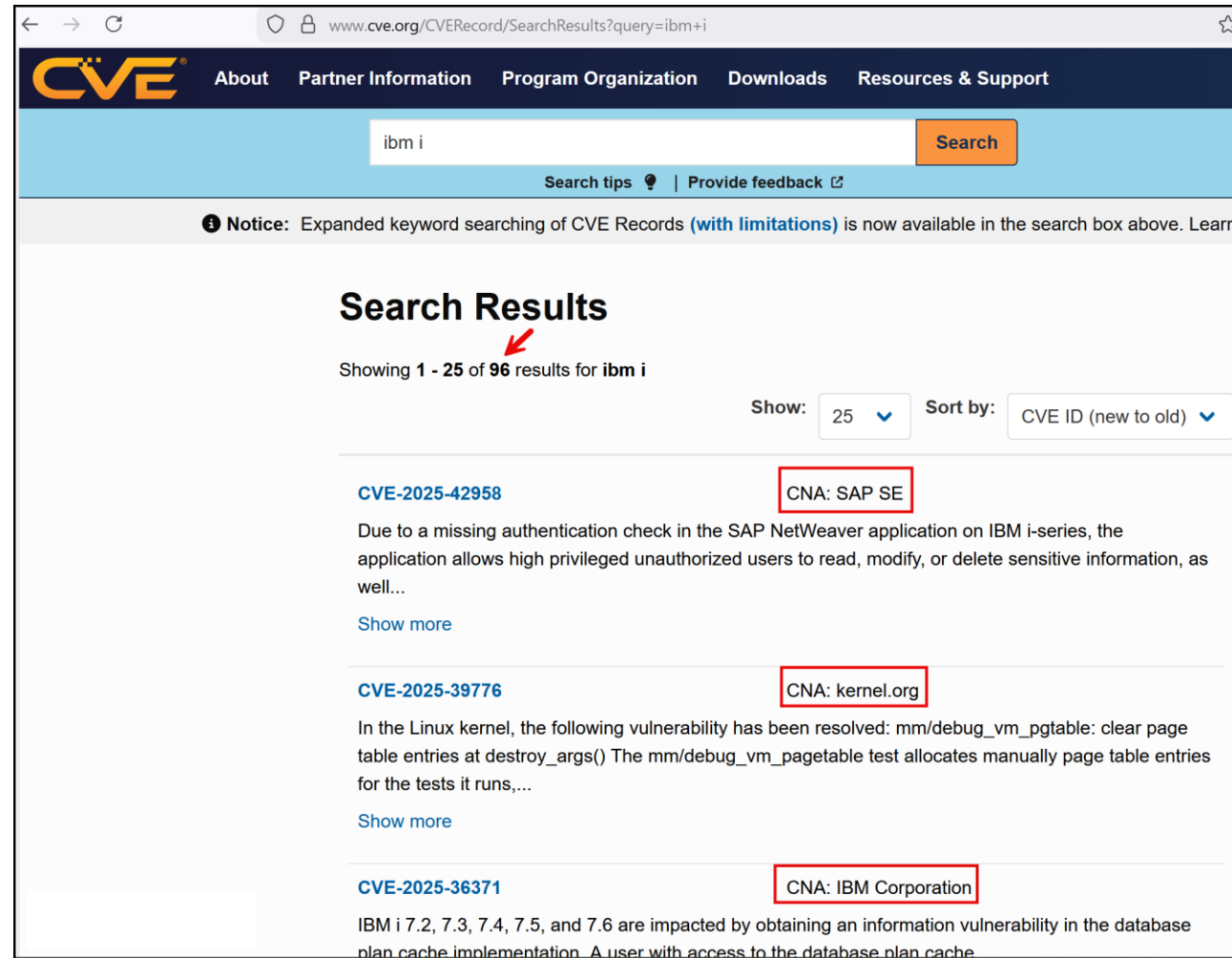
What are the biggest security challenges
facing organizations in 2026?

Denial



Image created with Microsoft co-pilot 1/19/2026

Published Vulnerabilities - CVE.org



The screenshot shows the CVE.org website with a search bar containing 'ibm i'. The search results page displays three entries, each with a CVE ID, a CNA (Common Name Authority), and a brief description of the vulnerability. A red arrow points to the 'Showing 1 - 25 of 96 results' text.

Search Results

Showing 1 - 25 of 96 results for ibm i

Search tips | Provide feedback

Notice: Expanded keyword searching of CVE Records (with limitations) is now available in the search box above. Learn more

Search Results

Showing 1 - 25 of 96 results for ibm i

Show: 25 Sort by: CVE ID (new to old)

CVE-2025-42958 CNA: SAP SE

Due to a missing authentication check in the SAP NetWeaver application on IBM i-series, the application allows high privileged unauthorized users to read, modify, or delete sensitive information, as well...

Show more

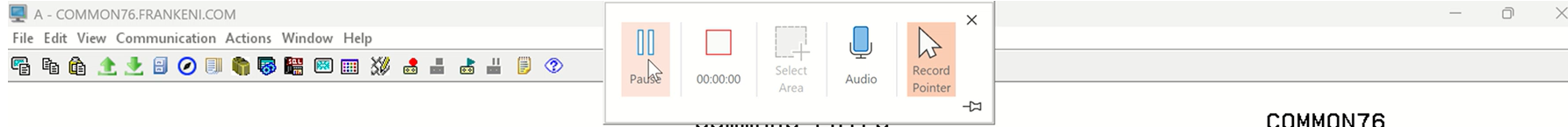
CVE-2025-39776 CNA: kernel.org

In the Linux kernel, the following vulnerability has been resolved: mm/debug_vm_pgtable: clear page table entries at destroy_args() The mm/debug_vm_pagetable test allocates manually page table entries for the tests it runs,...

Show more

CVE-2025-36371 CNA: IBM Corporation

IBM i 7.2, 7.3, 7.4, 7.5, and 7.6 are impacted by obtaining an information vulnerability in the database plan cache implementation. A user with access to the database plan cache



COMMON76
Request level: 1

Previous commands and messages:

(No previous commands or messages)

Bottom

Type command, press Enter.

==>

F3=Exit F4=Prompt F9=Retrieve F10=Include detailed messages
F11=Display full F12=Cancel F13=Information Assistant F24=More keys

MA

A

MW

18/007

Run SQL – Insert Examples

SQL Examples

Search...

IBM i Services

Security - Db2 for i - Delete attack vector

Security - Db2 for i - Insert attack vector

Security - Db2 for i - Query attack vector

Security - Db2 for i - RENAME attack

Security - Db2 for i - Trigger attack vector

Security - Db2 for i - Update attack vector

Security - Function Usage

Security - Group profile detail

Security - IFS Authority Collection

Security - IFS home directories (detail)

Security - IFS home directories (summary)

Security - Library List security review

Security - Object Ownership

Security - Powerful commands

Security - QPGMR vs QPGMR_NC

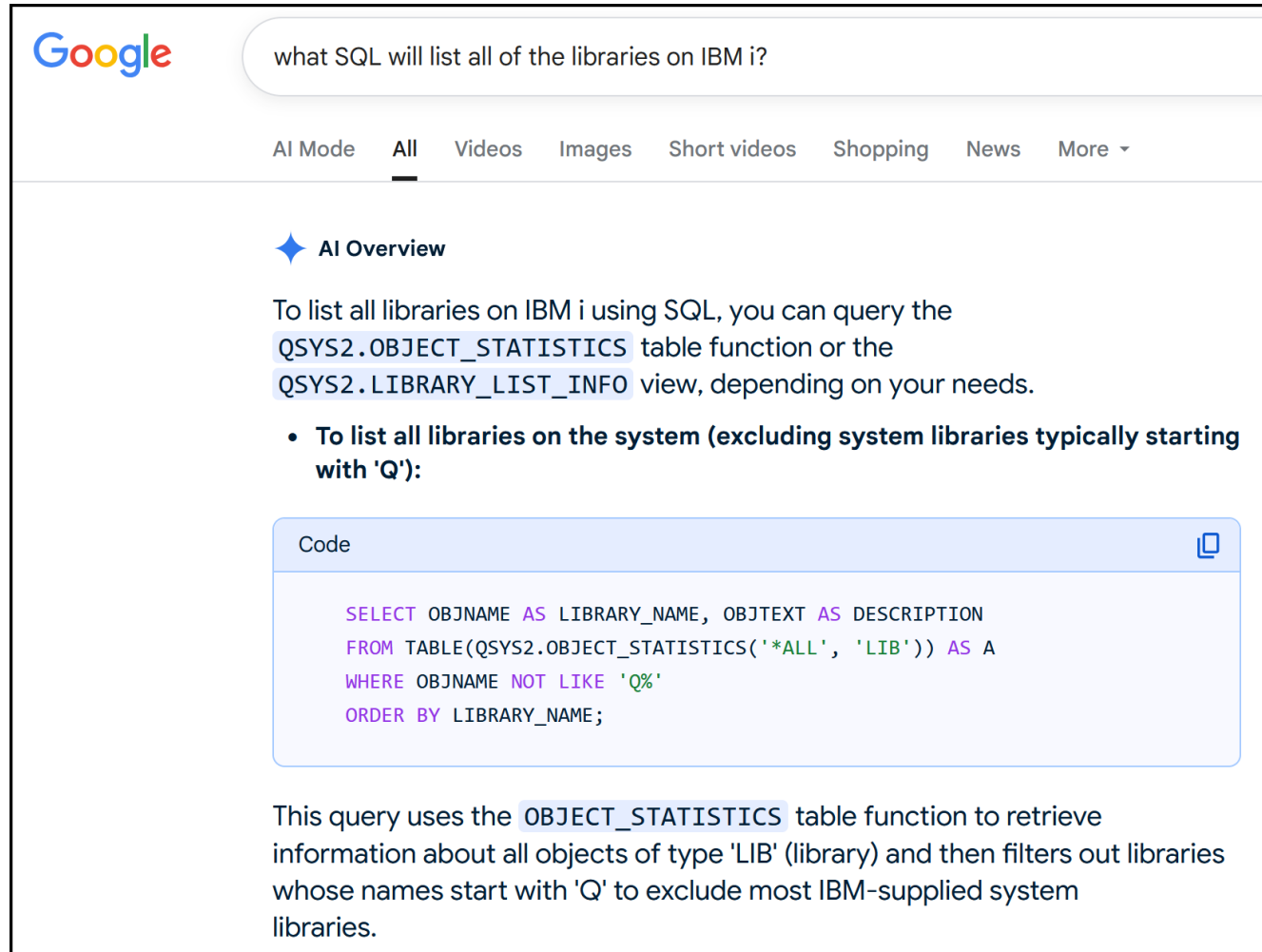
Security - QSECOFR vs QSECOFR_NC

```
-- category: IBM i Services
-- description: Security - Db2 for i - Delete attack vector
-- Use Db2 for i to Inject more Security into your IBM i
-- minvrn: v7r3m0

--
-- Files where ANY user can delete rows
--
WITH libs (lib_name) AS (
  SELECT object_name
  FROM qsys2.object_privileges
  WHERE system_object_schema = 'QSYS' AND object_type = '*LIB' AND user_name = '*PUBLIC' AND
    data_execute = 'YES'
)
SELECT *
FROM libs, qsys2.object_privileges
WHERE system_object_schema = lib_name AND object_type = '*FILE' AND user_name = '*PUBLIC' AND
  data_delete = 'YES' AND ('PF' = (SELECT objattribute
    FROM TABLE (
      qsys2.object_statistics(lib_name, '*FILE', object_name)
    )));
```

Available in ACS 1.1.9.9

A Simple Google Search ...



Google

what SQL will list all of the libraries on IBM i?

AI Mode All Videos Images Short videos Shopping News More ▾

◆ AI Overview

To list all libraries on IBM i using SQL, you can query the `QSYS2.OBJECT_STATISTICS` table function or the `QSYS2.LIBRARY_LIST_INFO` view, depending on your needs.

- To list all libraries on the system (excluding system libraries typically starting with 'Q'):

```
Code
```

```
SELECT OBJNAME AS LIBRARY_NAME, OBJTEXT AS DESCRIPTION
FROM TABLE(QSYS2.OBJECT_STATISTICS('*ALL', 'LIB')) AS A
WHERE OBJNAME NOT LIKE 'Q%'
ORDER BY LIBRARY_NAME;
```

This query uses the `OBJECT_STATISTICS` table function to retrieve information about all objects of type 'LIB' (library) and then filters out libraries whose names start with 'Q' to exclude most IBM-supplied system libraries.

AI Mode

The screenshot shows the Google AI Mode interface. At the top, there's a navigation bar with the Google logo, 'AI Mode', and links for 'All', 'Images', 'Videos', 'News', 'Short videos', 'Shopping', and 'More'. Below this, the search query 'What security vulnerabilities does IBM i have?' is displayed. The response starts with a summary: 'Security vulnerabilities exist in IBM i. Recent examples include:'. This is followed by a list of six bullet points, each describing a specific vulnerability in IBM products. The list includes CVE-2025-36004, OpenSSL vulnerabilities, IBM Navigator for i, IBM i Netserver (CVE-2025-2950), IBM Performance Tools for i (CVE-2024-27264), and IBM Java SDK and Runtime. The interface also features a left sidebar with a Google logo, a clock icon, and a notepad icon.

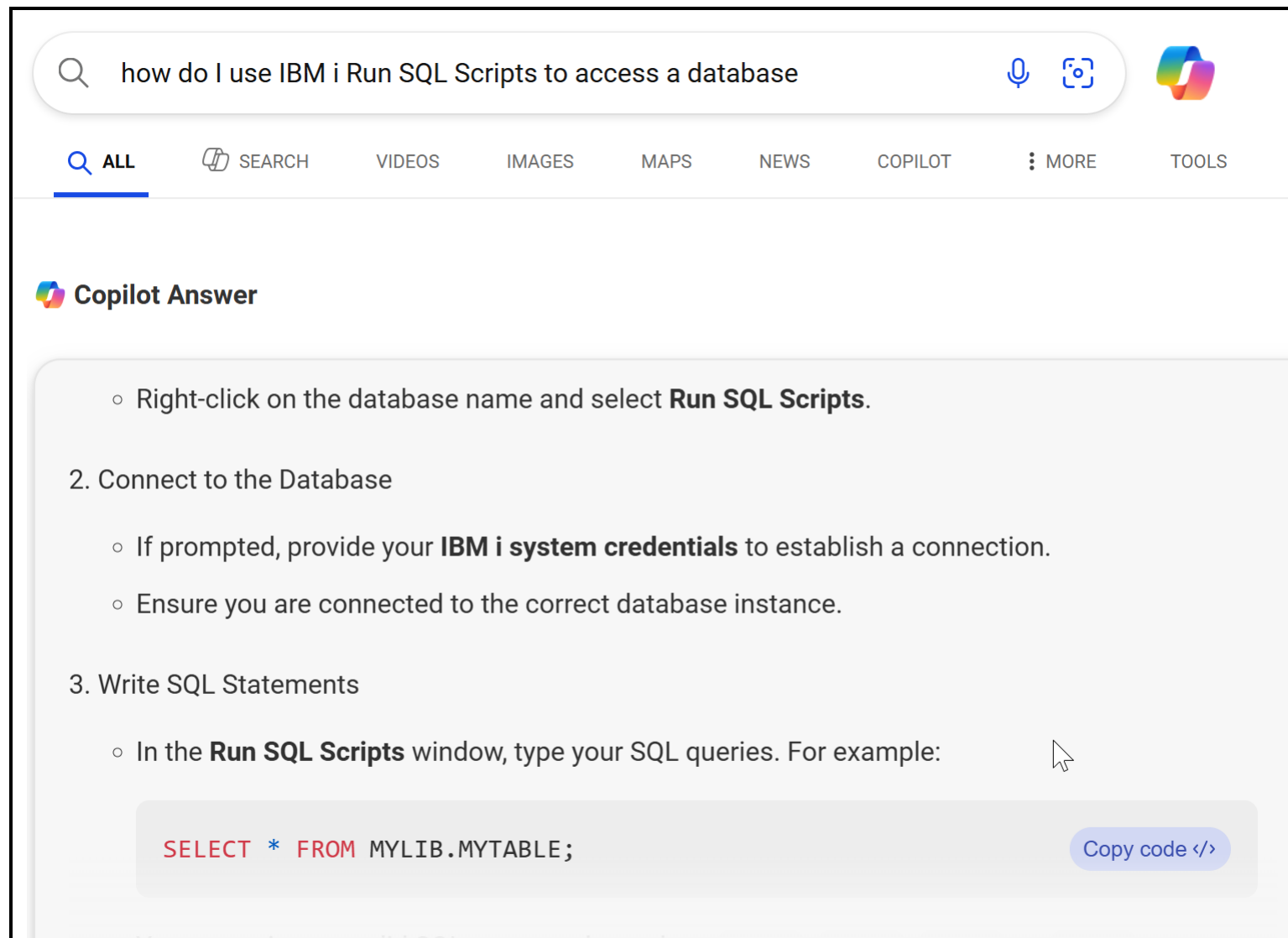
AI Mode All Images Videos News Short videos Shopping More ▾

What security vulnerabilities does IBM i have?

Security vulnerabilities exist in IBM i. Recent examples include:

- **Vulnerability in IBM Facsimile Support for i (CVE-2025-36004):** Attackers can escalate privileges and execute arbitrary code with administrator rights because of an unqualified library call.
- **Vulnerabilities in OpenSSL for IBM i:** These vulnerabilities could lead to denial of service attacks and allow remote attackers to get sensitive information.
- **Vulnerabilities in IBM Navigator for i:** IBM Navigator for i is susceptible to log file access, obtaining file attributes, and SQL Injection attacks.
- **Vulnerability in IBM i Netserver (CVE-2025-2950):** This can be exploited for authentication and authorization attacks through incorrect validation processing in IBM i Netserver.
- **Vulnerability in IBM Performance Tools for i (CVE-2024-27264):** This local privilege escalation vulnerability arises from an unqualified library call in IBM Performance Tools for i.
- **Vulnerabilities in IBM Java SDK and IBM Java Runtime for IBM i:** These components are vulnerable to various attacks impacting confidentiality, availability, and integrity. ⓘ

Microsoft Copilot – Using SQL



Search bar: how do I use IBM i Run SQL Scripts to access a database

Navigation: ALL, SEARCH, VIDEOS, IMAGES, MAPS, NEWS, COPILOT, MORE, TOOLS

Copilot Answer

- Right-click on the database name and select **Run SQL Scripts**.

2. Connect to the Database

- If prompted, provide your **IBM i system credentials** to establish a connection.
- Ensure you are connected to the correct database instance.

3. Write SQL Statements

- In the **Run SQL Scripts** window, type your SQL queries. For example:

```
SELECT * FROM MYLIB.MYTABLE;
```

Copy code </>

Where Do I Start?

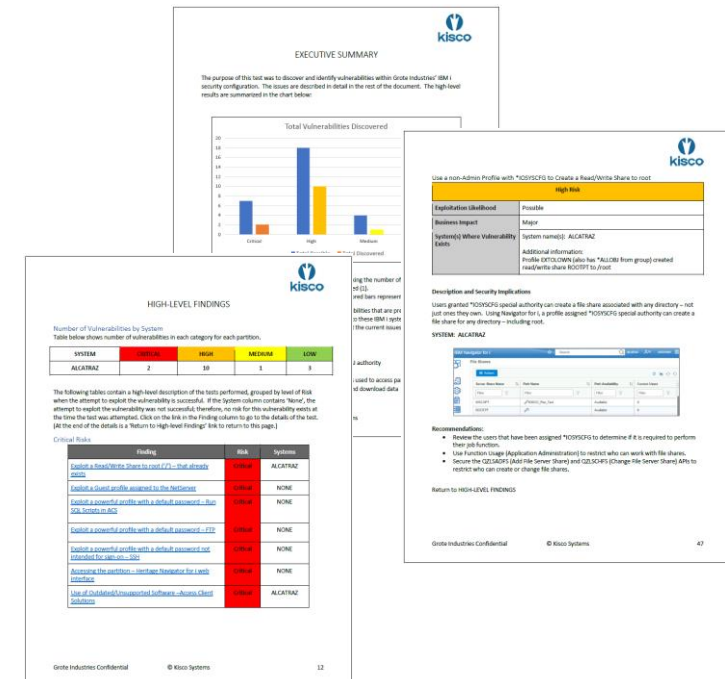
■ IBM i Security Discovery Services

Security Assessment

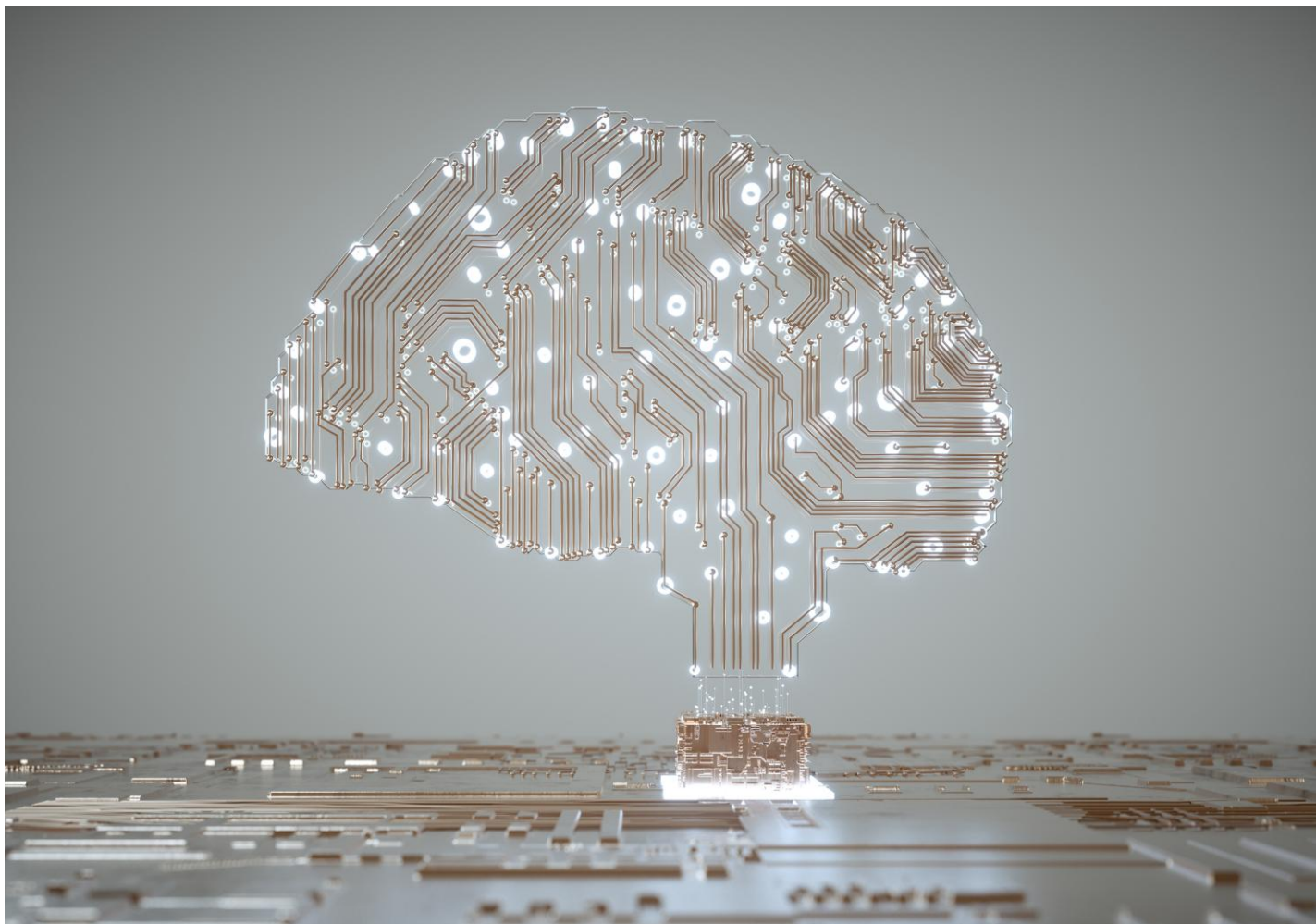
ActVal	Column Labels		
Row Labels	IPG-DEV	IPG-DR	IPG-PRD
All users			
All profiles	500	500	417
CMD line	450	450	414
Default pwd	90	90	109
Inactive	400	400	370
JOB desc			
Named vulnerable	1	1	0
Powerful profiles	200	200	160
OBJ access			
Vuln files	95000	95000	30270
Vuln libraries	1200	1200	771
Vuln objects	250000	250000	134347
PGM adopted auth			
CIS - SECOFR owned	5500	5500	4868
CIS - vulnerable LIB	8000	8000	5896
Priv Users			
All profiles	500	500	417
CMD line	300	300	32
Default pwd	30	30	10
Inactive	250	250	19
Special auth	90	90	33
System Values			
QAUDCTL	*AUDLVL	*AUDLVL	*AUDLVL
QAUDLVL	*SECCFG *SECUN	*SECCFG *SECUN	*SECCFG *SECUN
QCRTAUT	*CHANGE	*CHANGE	*CHANGE
QMAXSIGN	3	3	3
QSECURITY	40	40	50
UP ownership			
PUBLIC auth	3	3	1
Vuln profiles	10	10	8

- IBM i SQL data collection
- Visibility across entire security configuration
- Identify risks and make recommendations

Penetration Test



- Manual testing process from inside network
- Validate cybersecurity controls
- Drive conversations with management



Artificial Intelligence (AI)

AI will Solve Everything



Image created with Microsoft co-pilot 1/19/2026

Considerations when Developing AI Models

- Data can't be 'unlearned'
 - What are your organization's models being trained on?
- Do your developers know the laws and regs they must comply with?
- Do you have clear policies and development procedures to in place to ensure your AI implementation is 'secure by design'?

Shadow AI



Use of AI outside
of the knowledge of IT

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

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

Controlling data access at the source

Proliferation of shadow AI validates business case for implementing stronger controls for SQL, IFS, others

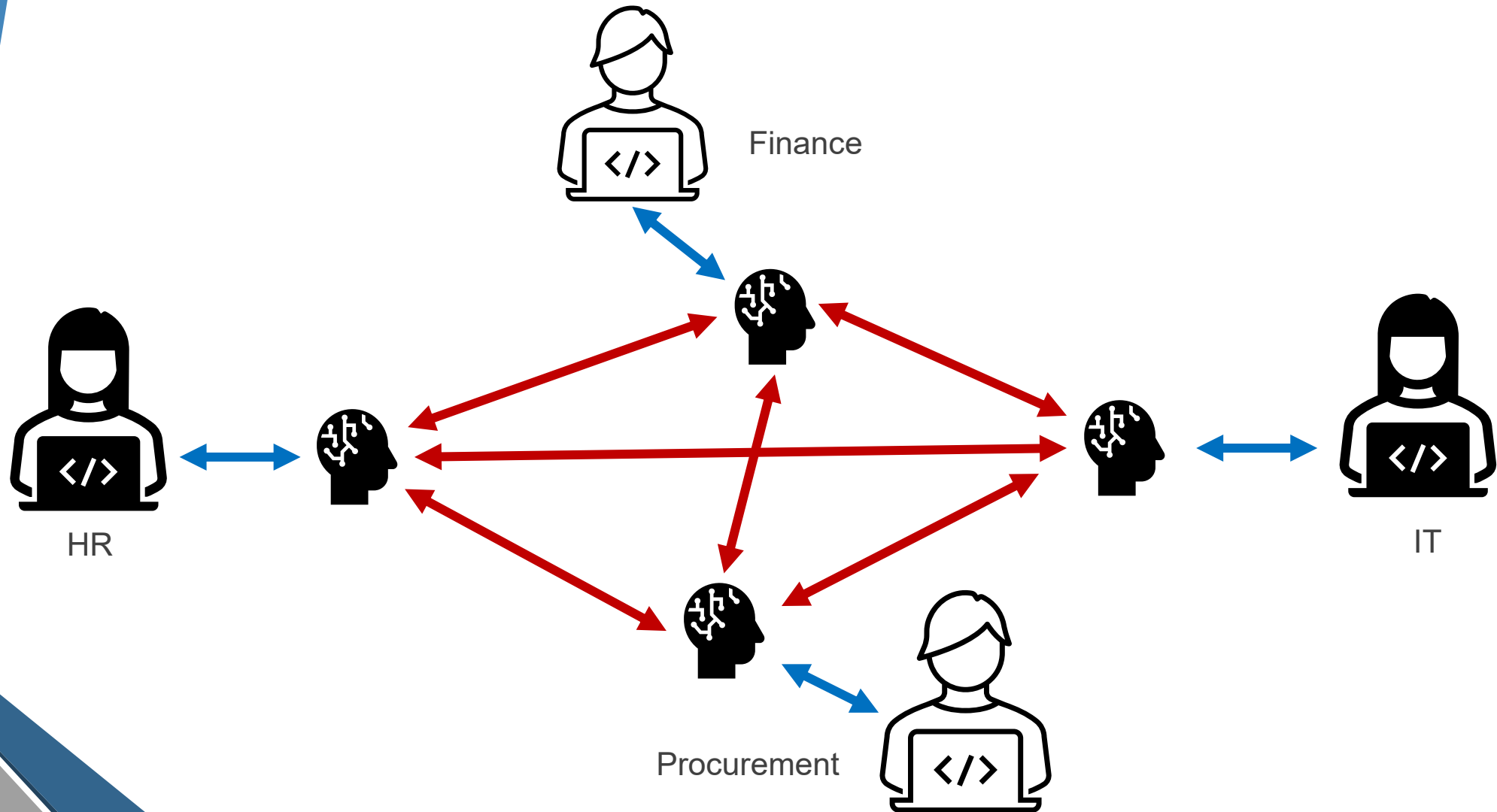
IBM i risks:

- Unsecured *FILE objects
- IFS NetServer shares to /root
- Network services override “Limited Capabilities”

Controls:

- Exit point logging and access controls
- NetServer authorization lists
- Limit number of powerful profiles

Agentic AI



Agentic AI

- Is security considered when agents are being created?
 - Configure agents with least privilege access
 - Do all agents *really* need to talk to one another?
 - <https://www.darkreading.com/remote-workforce/ai-vulnerability-servicenow>
 - How will you detect inappropriate behavior?
 - Are agents logging their actions and are they in compliance with laws and regs?
- 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>
 - <https://www.bankinfosecurity.com/coder-builds-malware-in-week-ai-help-a-30576>
- On the other hand, it can make detection and patching quicker
 - <https://www.darkreading.com/application-security/gen-ai-accelerates-triage-of-software-vulnerabilities>

Agentic AI

- **There's a query behind every agentic interaction**
- IBM's solution for exposing IBM i DB to the agentic ecosystem: **Mapapire**
- Mapapire is effectively ODBC
- Well-known IBM i ODBC security concerns:
 - Bypasses application security
 - Access to ANY *PUBLIC CHANGE/ALL *FILE object (data)
 - Ability to call CL commands even with Limited Capabilities UP

Agentic AI

- Best practices for Agentic AI visibility and control
- Based on customer R&D

Control

Agentic AI user profiles:

- One profile per agent
- Least privilege access
- Non-interactive logon
- Limit access to *SQLSRV
- Control SQL verbs
- Block FTP, IFS, others

Visibility

What are my agents doing?

- *SQLSRV exit points
- All exit points – detect out of scope
- Security Audit Journal
- Outbound SK records to API hosts
- OS actions outside of Agent scope
- Use data mart to control storage size

Current AI Reality

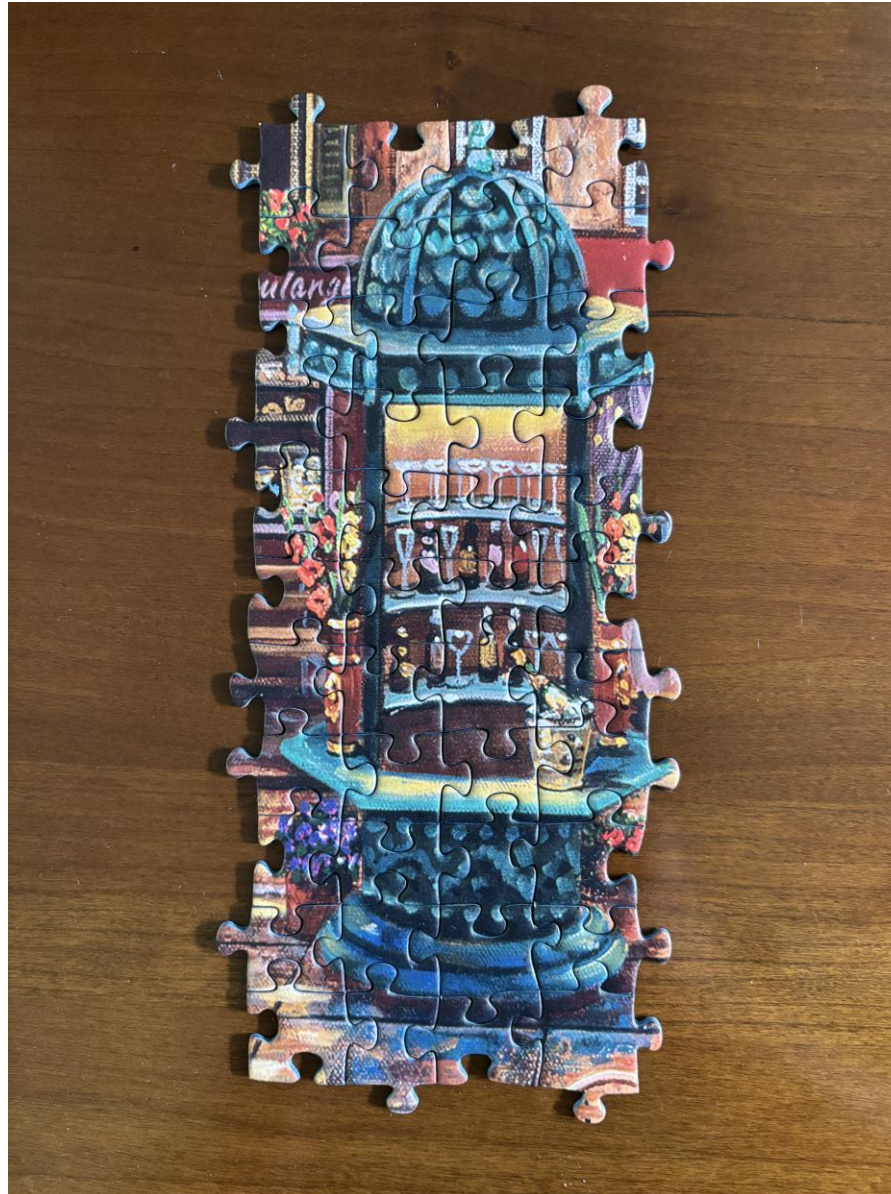


Image created with Microsoft co-pilot 1/19/2026

Lack of Visibility into IBM i Activity



Focused only on IBM i





The Answer to Lack of Visibility?

- Send IBM i information to your SIEM
- And/Or set up alerts of inappropriate activity, for example:
 - Attempts to sign on with ROOT or ADMIN
 - Jobs started with an external IP address
 - Changes to specific fields in specific files

Social Engineering



- Helpdesk resets
 - <https://www.secureworld.io/industry-news/workday-crm-data-breach>
- Sense of urgency or 'emergency' situation (Vishing)
 - <https://www.secureworld.io/industry-news/saas-under-siege-shinyhunters-data-extortion>
- Deepfakes are making social engineering harder to recognize
- Malware inserted into AI summaries
 - <https://www.bankinfosecurity.com/ai-summaries-new-vector-for-malware-a-29299>

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>

Listing Inactive Profiles with SQL



```
46 --
47 -- List User profiles that haven't been used in the last 3 months
48 --
49 SELECT user_name,
50        date(last_used_timestamp) as last_used,
51        timestamp(previous_signon, 0) as last_signon,
52        timestamp(creation_timestamp, 0) as create_time,
53        status,
54        text_description
55 FROM QSYS2.USER_INFO
56 WHERE (last_used_timestamp IS NULL
57        OR last_used_timestamp < CURRENT_TIMESTAMP - 3 MONTHS)
58 AND (creation_timestamp < CURRENT_TIMESTAMP - 3 MONTHS);
```

Authorization Name				Status	Text Description
USER_NAME	LAST_USED	LAST_SIGNON	CREATE_TIME	STATUS	TEXT_DESCRIPTION
#GNOTEST	-	-	2022-01-03 09:07:31	*ENABLED	-
AAATIM4	-	-	2021-07-07 09:01:55	*ENABLED	asdfasdf
AARONC	2020-03-11	2020-03-11 09:03:36	2019-05-06 14:17:45	*ENABLED	-
AATIM	-	-	2018-08-27 07:41:53	*ENABLED	Setsrgee
AATIM3	-	-	2022-10-21 13:18:20	*ENABLED	Test users
ACADMN01	2020-09-15	2020-09-15 16:15:08	2019-05-02 17:05:31	*ENABLED	Admin user for authority collection

Make sure you're looking at the right date. Last used, NOT last sign-on!

Use MFA to Help Prevent Attacks

7.6

Sign On

System : P1386XPV
Subsystem : QINTER
Display : QPADEV0001

User : _____
Password : _____

Program/procedure : _____
Menu : _____
Current library : _____
→ Additional factor : _____

(C) COPYRI

Welcome to IBM Navigator for i

User Name: _____

Password: _____

Additional Factor: _____

Log in

Signon to IBM i

Signon information

System: _____

User: _____

Password: _____

→ Additional Factor: _____

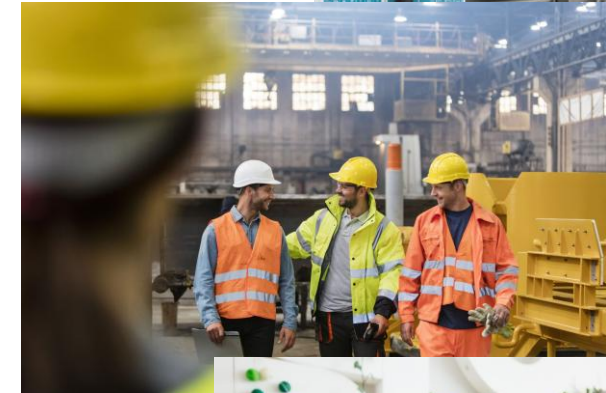
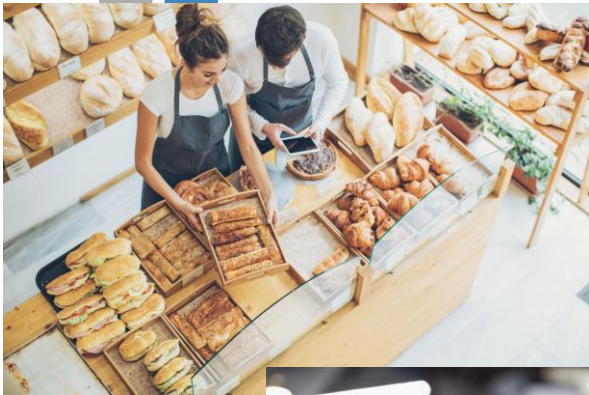
OK Cancel

Additional Factor field added to all sign on displays once system is enabled for MFA and IPLed

MFA Considerations

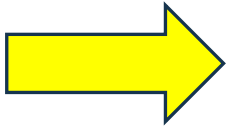
- While not perfect, MFA can help prevent many breaches – especially social engineering attacks.
 - See Verizon's 2025 DBIR (Data Breach Investigations Report)
- Note: Kisco's MFA solution exists prior to IBM i 7.6

Insider Threat



Take Heart! IBM i is ...

Secure*-able*

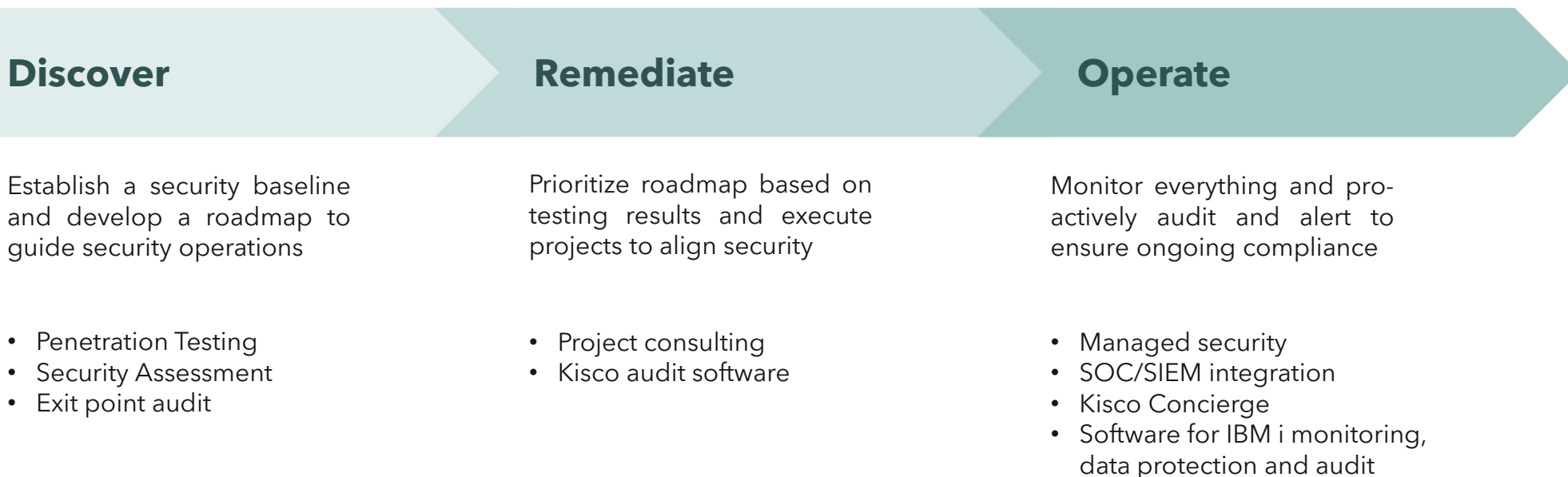


But you need visibility
into what's happening!

What Do We Do...?



Roadmap to get and stay secure



Security Software Portfolio

SafeNet

Use exit points to log and control access to FTP, SQL, IFS and more. Includes MFA ransomware detection

iEventMonitor

Real-time monitoring and alerting of system and security events. Includes SIEM support and task automation.

iSecMap

Monitor security configuration against baseline policies to ensure ongoing compliance

iFileAudit

Uses IBM i database journals to capture and report on changes to critical or sensitive data.

For More Information

[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>

➡ **Contact Kisco Systems:** sales@kisco.com