# z/OSMF plug-in for IBM TDz

- 2 Icons / Apps for TDz
 - Dashboard
  - Details
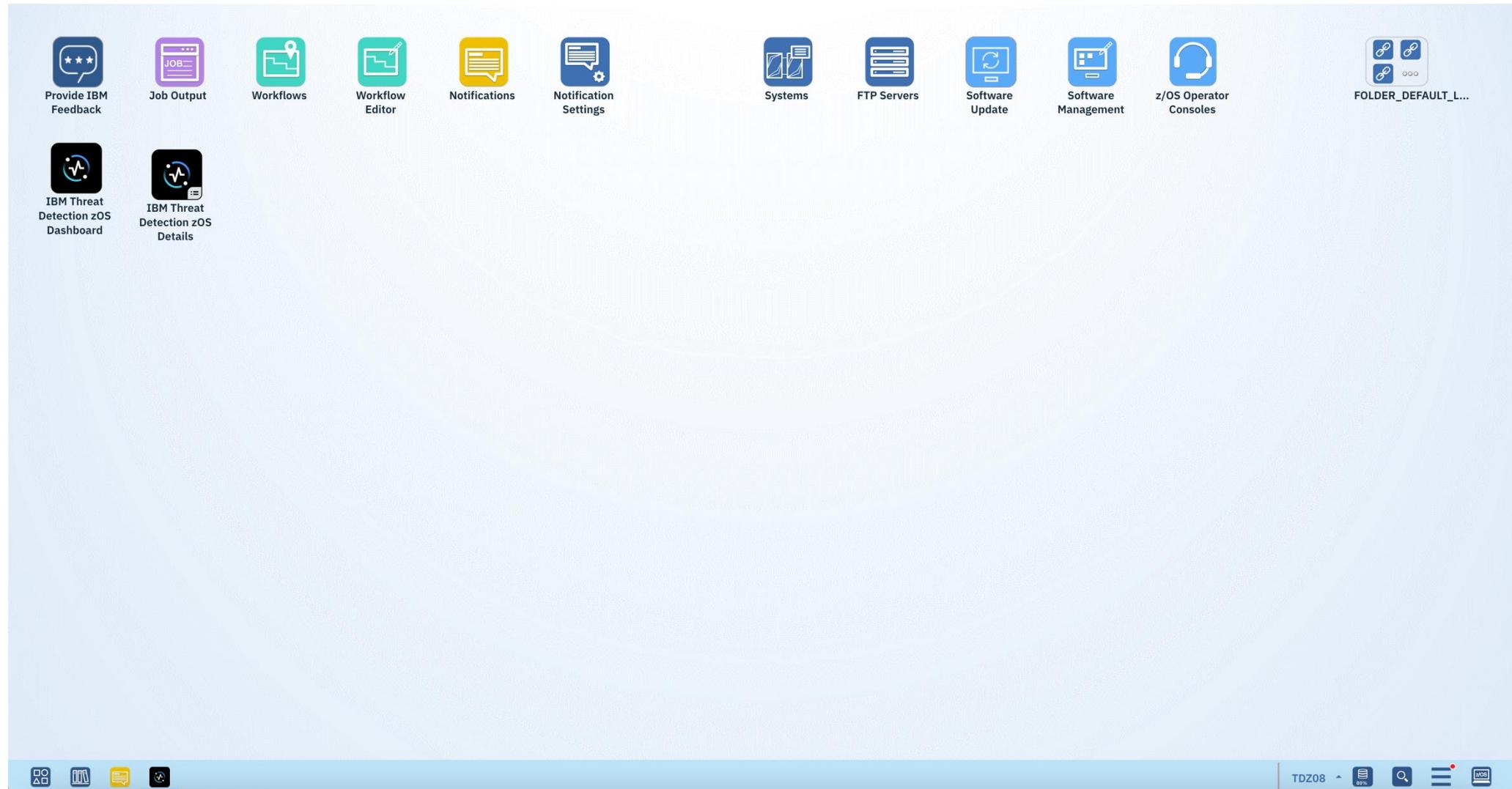
TDz Dashboard – Overview

- Opens in a new window

- Shows anomaly signatures
  - LPAR view
  - Signature type view

- Summary information

- Boundary Date and Interval Display

- Includes Start and End time including Baseline

- No display of signature as counter is **0**/17
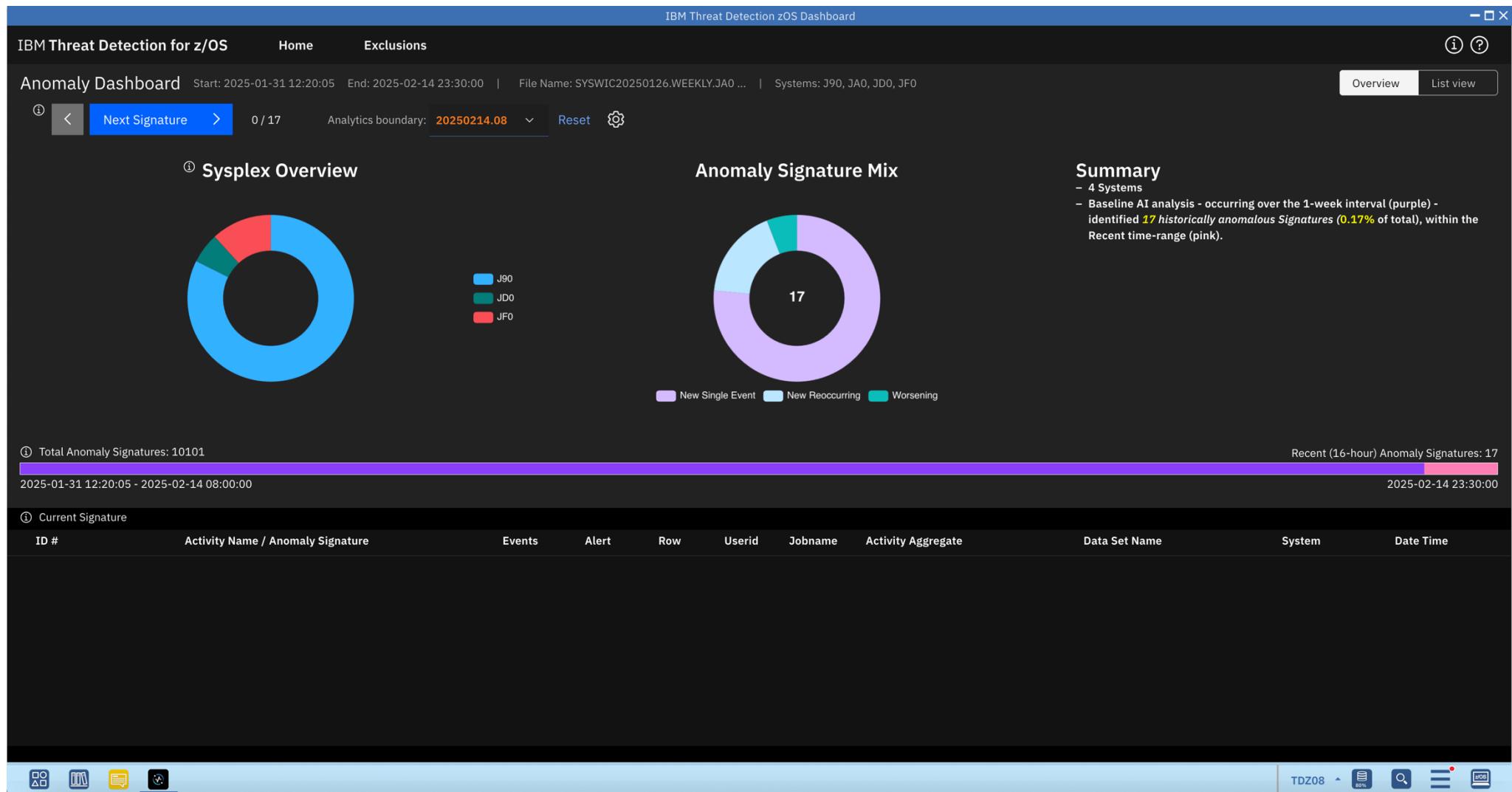
TDz Dashboard – Overview

- Hovering over Sysplex Overview highlights anomaly signatures per LPAR
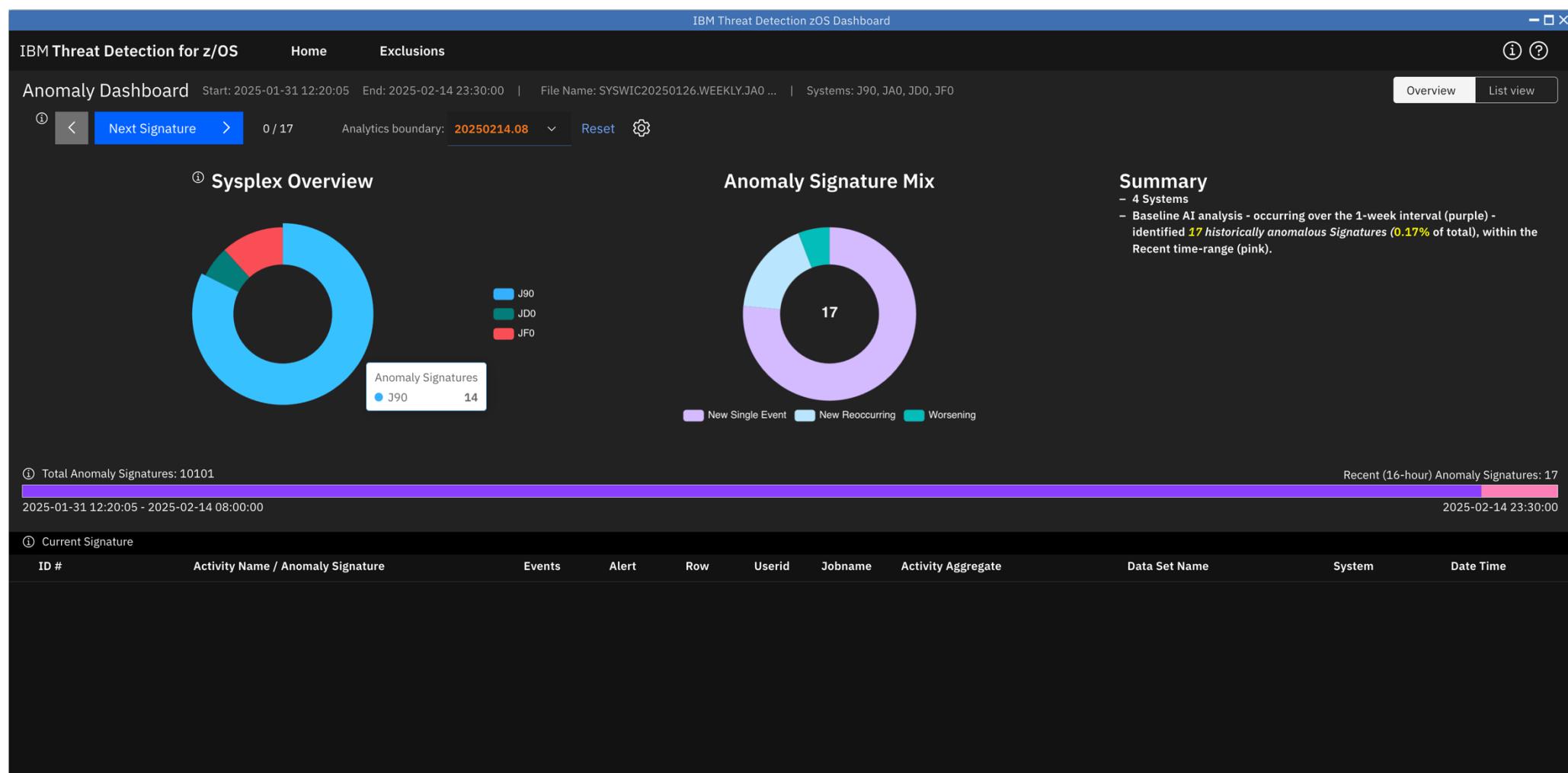
TDz Dashboard – Overview

- Hovering over Anomaly Signature Mix highlights type of anomaly
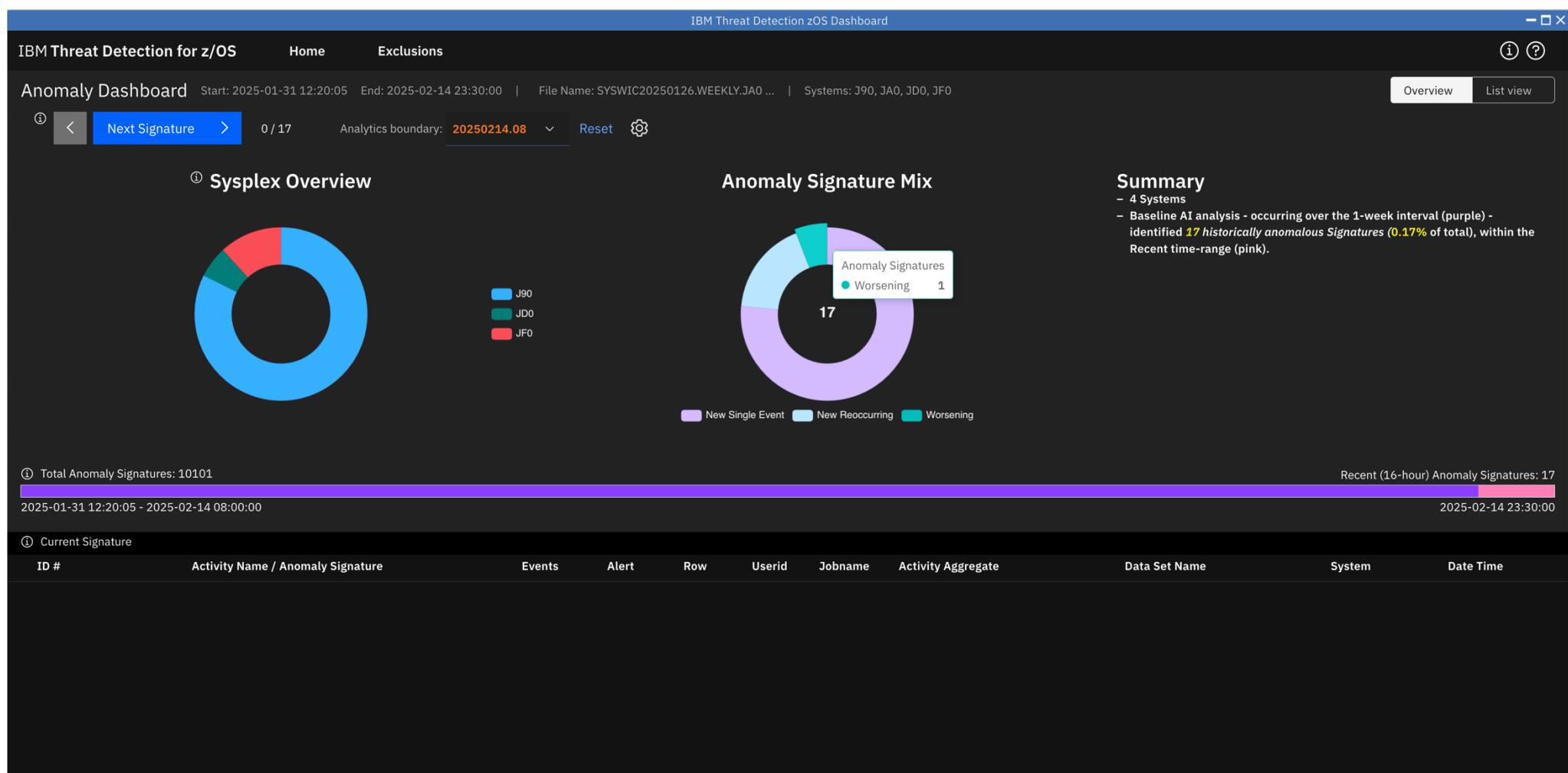
TDz Dashboard – Overview

- Description of signature types

- New Single Event = have not been seen within the basis interval AND have occurred once in the recent interval

- New Reoccuring Event = have not been seen within the basis interval AND have reoccurred in the recent interval

- Worsening = see screen shot
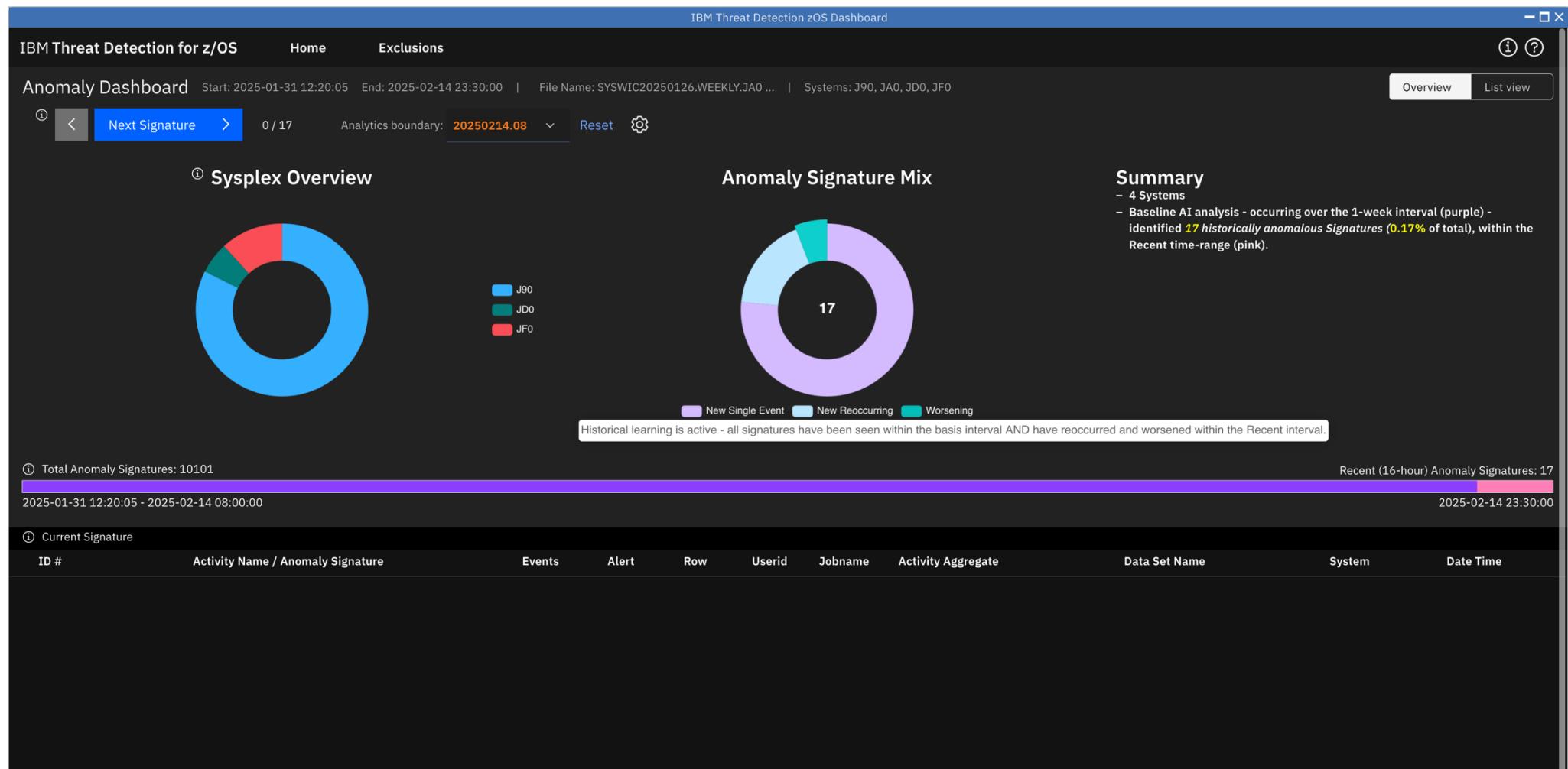
# TDz Dashboard – Overview

- Set Analytics Boundary
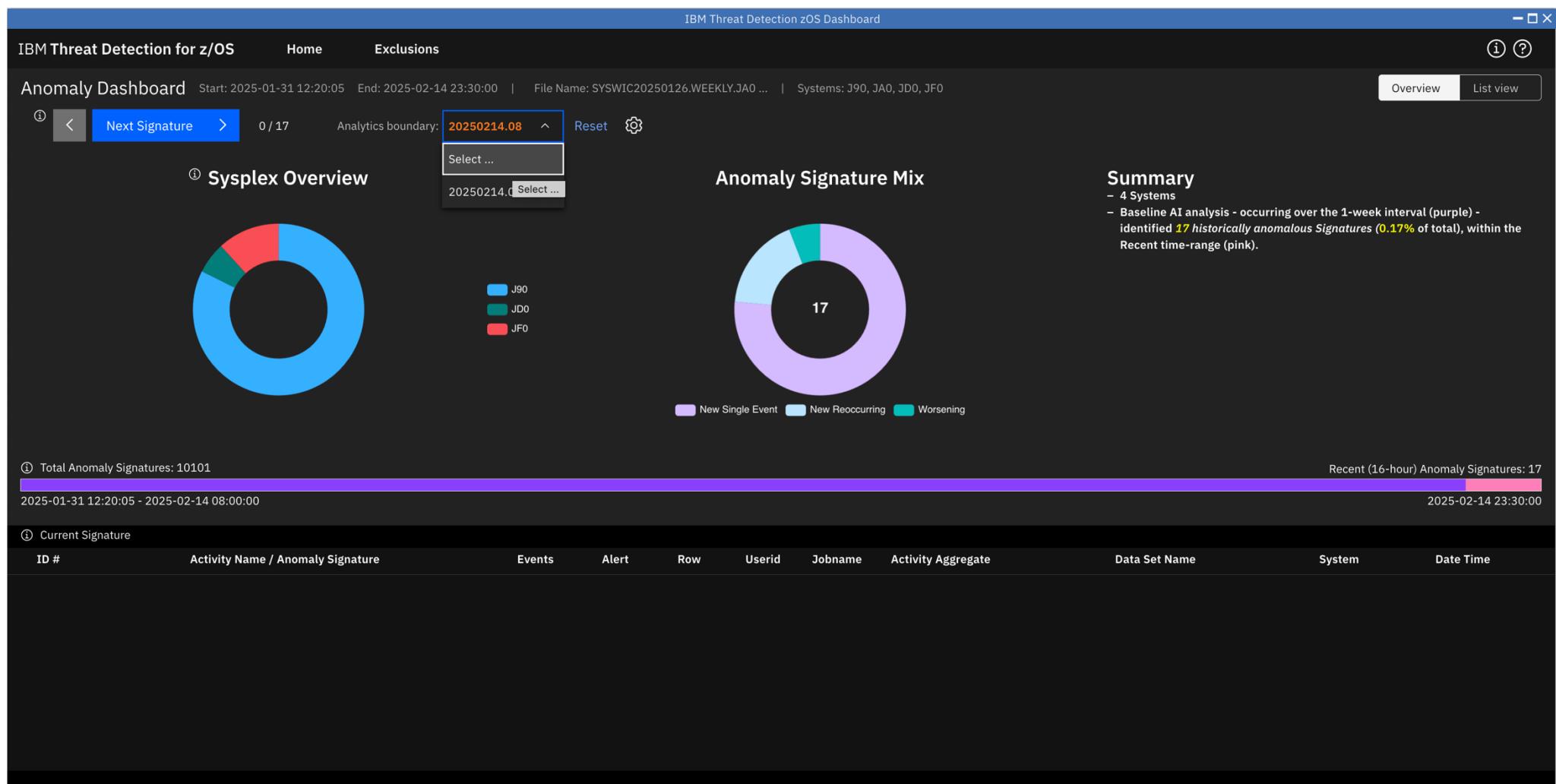
TDz Dashboard – Overview

- Set Analytics Boundary

- Define most recent Interval
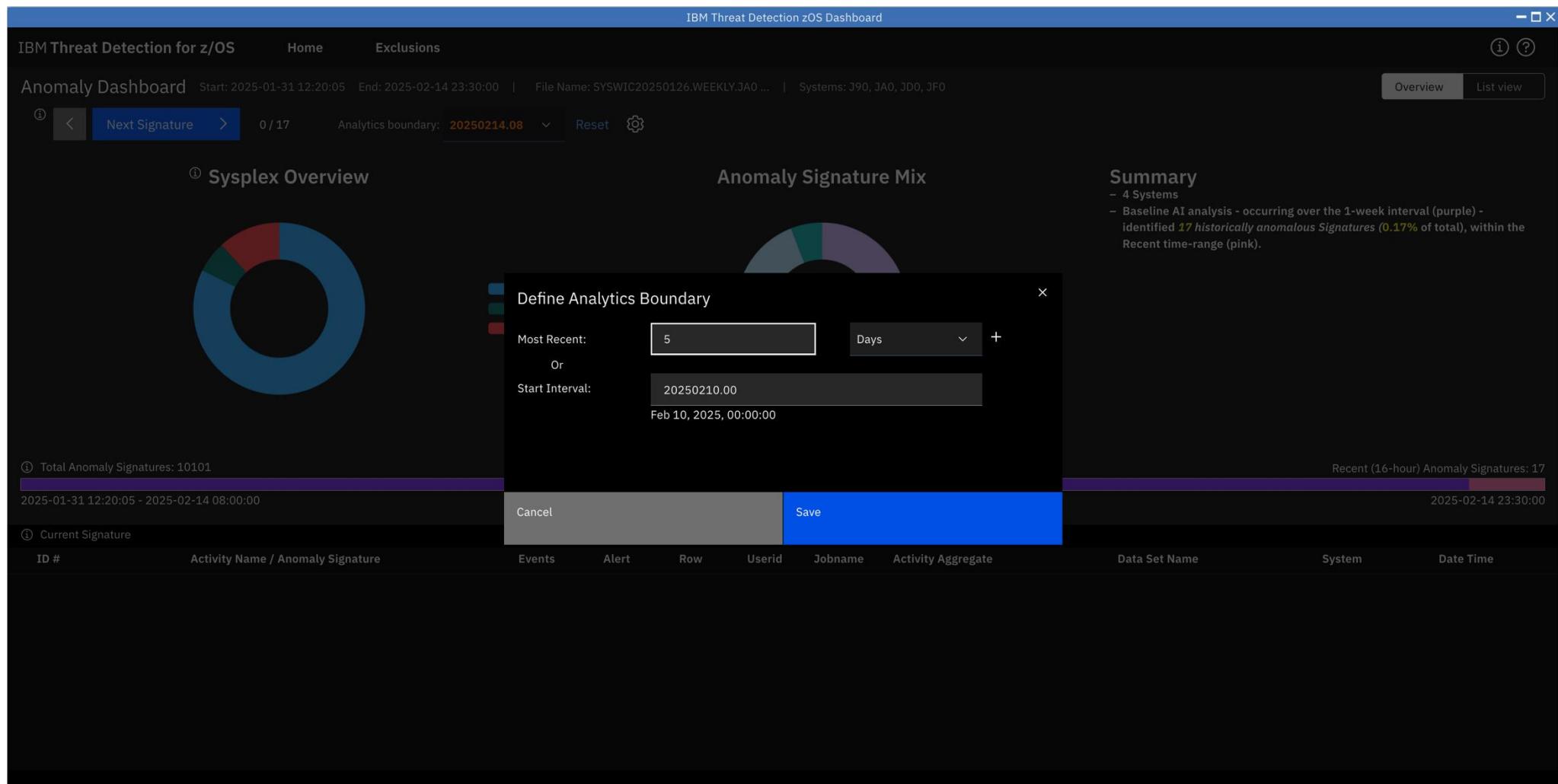
TDz Dashboard – Overview

- Set Analytics Boundary
- Most Recent Interval enlarged
- Number of Signatures increased
- Additional LPAR JF0 shows up
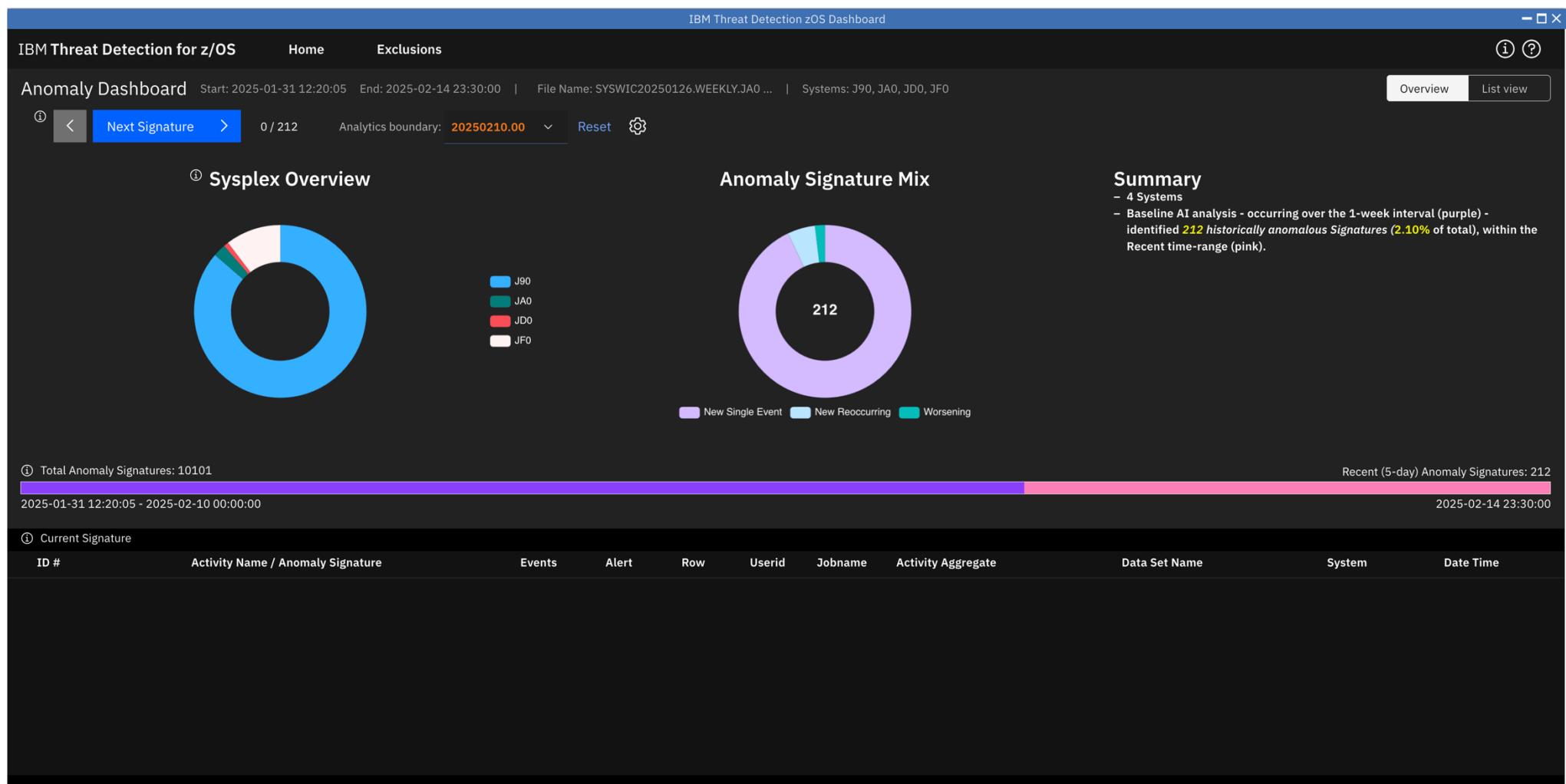
TDz Dashboard – Overview

- Select a Signature 5 / 17

- Signature is made up of 2 events

- Underlined Date Time entry leads to detailed analysis

- Change to List View
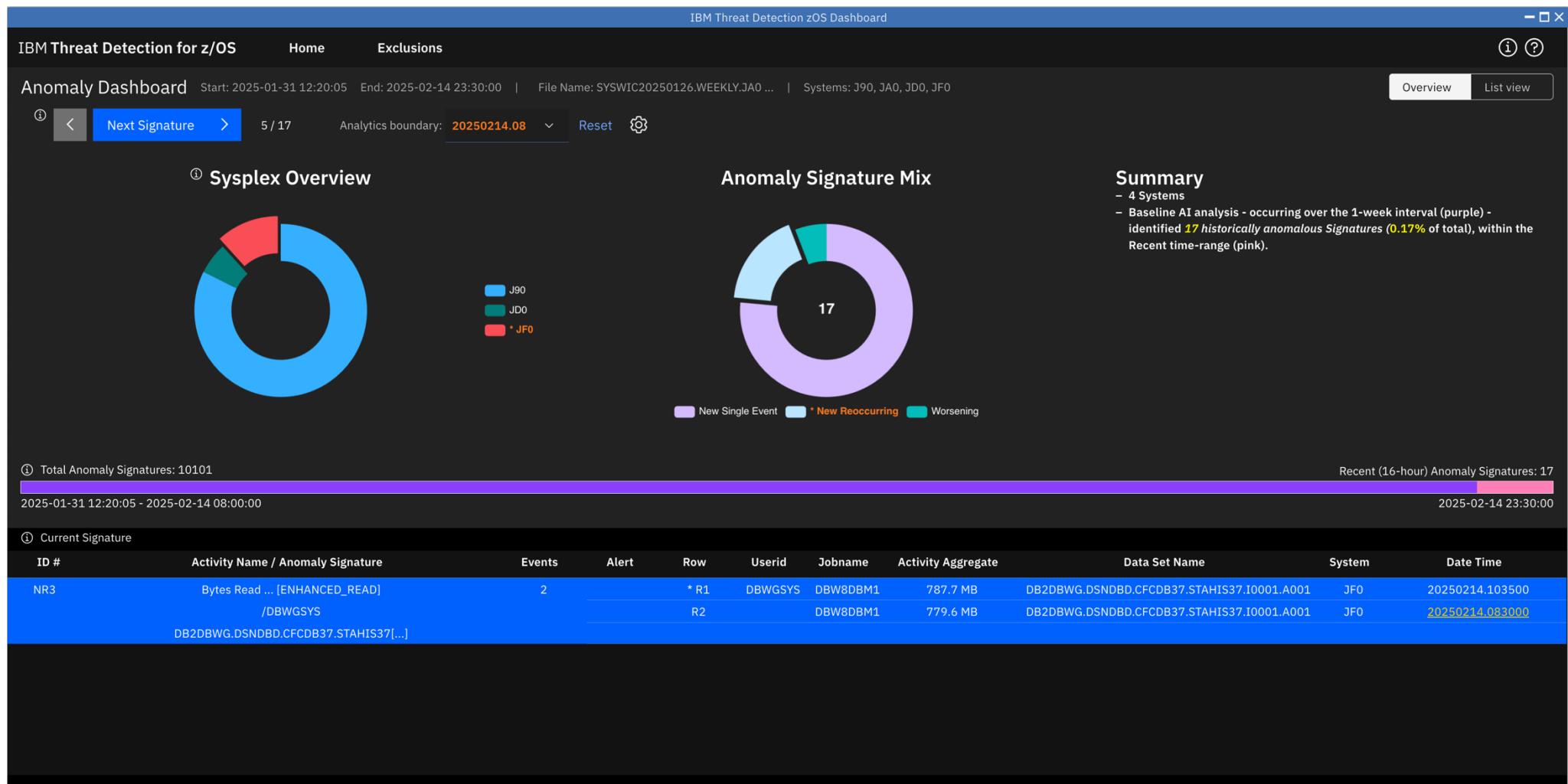
TDz Dashboard – List View

- Same signature presented on list view

IBM Threat Detection zOS Dashboard

IBM **Threat Detection for z/OS**   Home   Exclusions
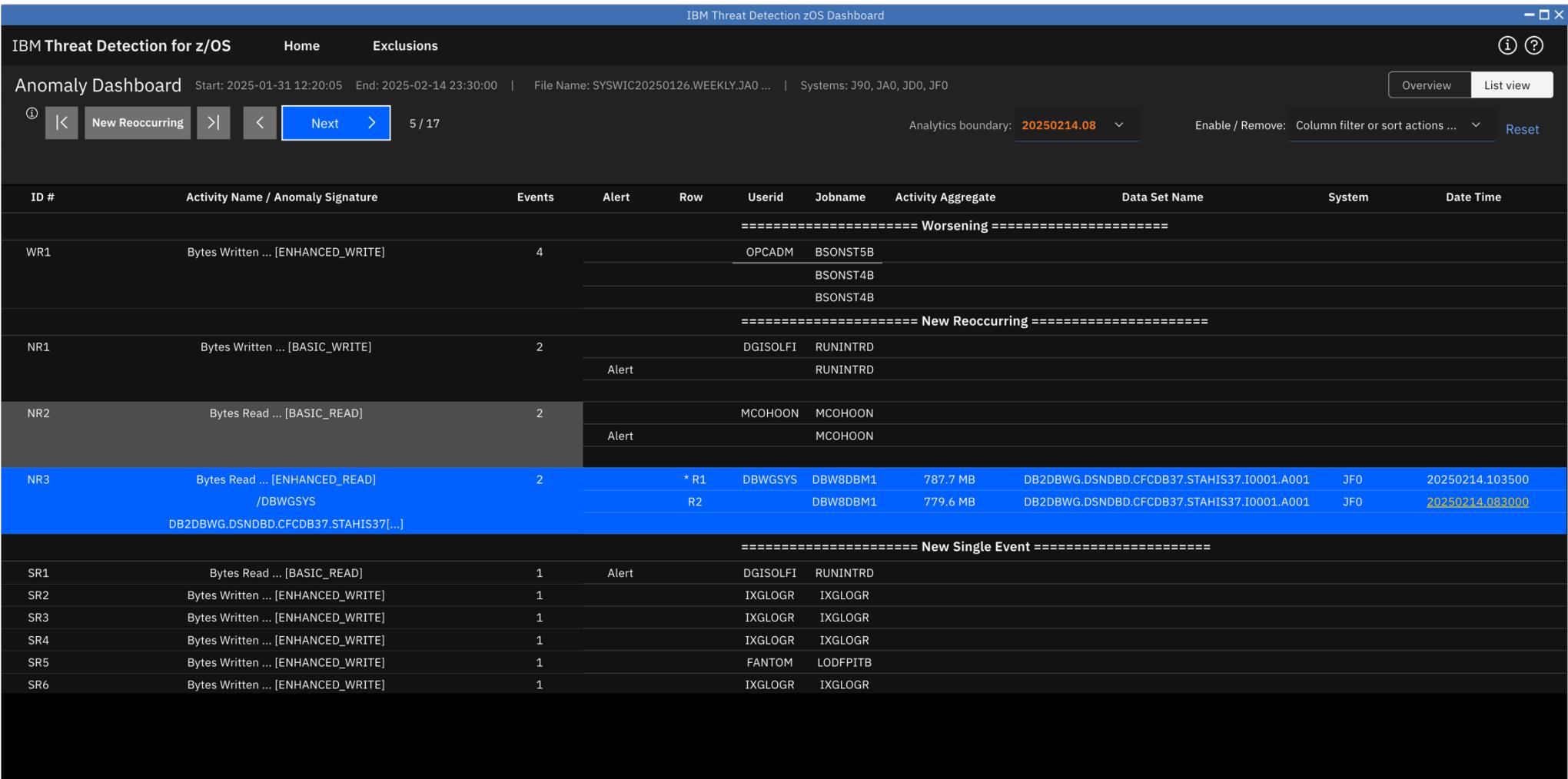
Anomaly Dashboard Start: 2025-01-31 12:20:05 End: 2025-02-14 23:30:00 | File Name: SYSWIC20250126.WEEKLY.JA0 ... | Systems: J90, JA0, JD0, JF0

Overview | List view

|◁ New Reoccurring ▷| ◁ Next ▷ 5 / 17

Analytics boundary: **20250214.08** ▾   Enable / Remove: Column filter or sort actions ... ▾ Reset

ID #	Activity Name / Anomaly Signature	Events	Alert	Row	Userid	Jobname	Activity Aggregate	Data Set Name	System	Date Time
==================== Worsening ====================										
WR1	Bytes Written ... [ENHANCED_WRITE]	4			OPCADM	BSONST5B				
						BSONST4B				
						BSONST4B				
==================== New Reoccurring ====================										
NR1	Bytes Written ... [BASIC_WRITE]	2			DGISOLFI	RUNINTRD				
			Alert			RUNINTRD				
NR2	Bytes Read ... [BASIC_READ]	2			MCOHOON	MCOHOON				
			Alert			MCOHOON				
NR3	Bytes Read ... [ENHANCED_READ]	2		* R1	DBWGSYS	DBW8DBM1	787.7 MB	DB2DBWG.DSNDBD.CFCDB37.STAHIS37.I0001.A001	JF0	20250214.103500
	/DBWGSYS			R2		DBW8DBM1	779.6 MB	DB2DBWG.DSNDBD.CFCDB37.STAHIS37.I0001.A001	JF0	20250214.083000
	DB2DBWG.DSNDBD.CFCDB37.STAHIS37[...]									
==================== New Single Event ====================										
SR1	Bytes Read ... [BASIC_READ]	1	Alert		DGISOLFI	RUNINTRD				
SR2	Bytes Written ... [ENHANCED_WRITE]	1			IXGLOGR	IXGLOGR				
SR3	Bytes Written ... [ENHANCED_WRITE]	1			IXGLOGR	IXGLOGR				
SR4	Bytes Written ... [ENHANCED_WRITE]	1			IXGLOGR	IXGLOGR				
SR5	Bytes Written ... [ENHANCED_WRITE]	1			FANTOM	LODFPITB				
SR6	Bytes Written ... [ENHANCED_WRITE]	1			IXGLOGR	IXGLOGR				

TDz Dashboard – List View

- Select Date Time field

- Indication of the upcoming processing of a specific file

TDz Detail View

- Event ID = 4

- Belongs to Correlated Activity Group 3

- Red mark points to anomaly

- But no alert connected with this anomaly
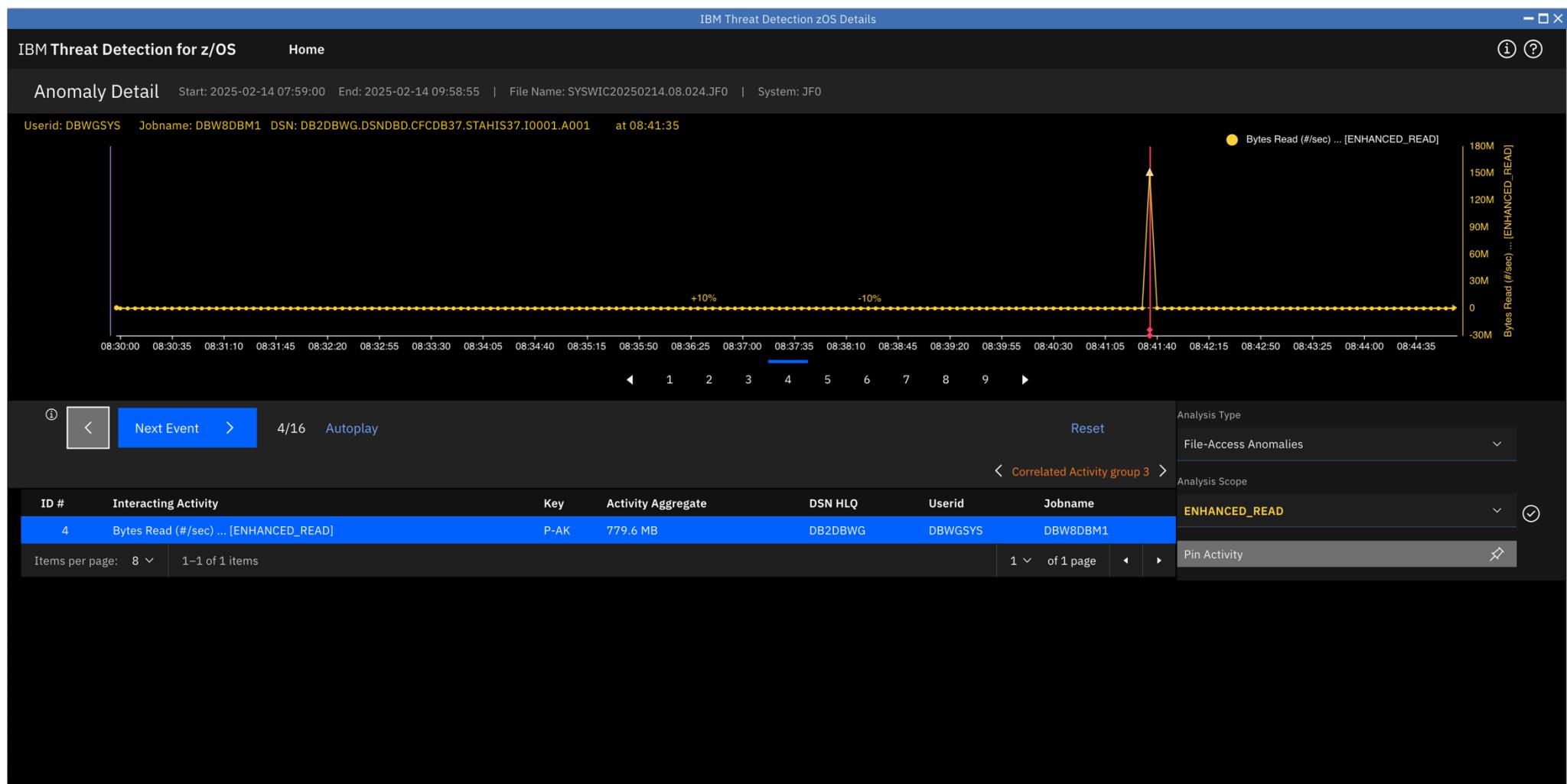
TDz Dashboard – List View

- Back to List View
- Filter on Alerts
- Alert Radio Button appears

TDz Dashboard – List View

- Select Alert Radio Button

- Only Signatures which generated an alert

TDz Detail View

- 50 individual events have resulted in an alert

- All events belong to Correlated Activity Group 2

- Look at the 6 events in this list

TDz Detail View

- View next Event
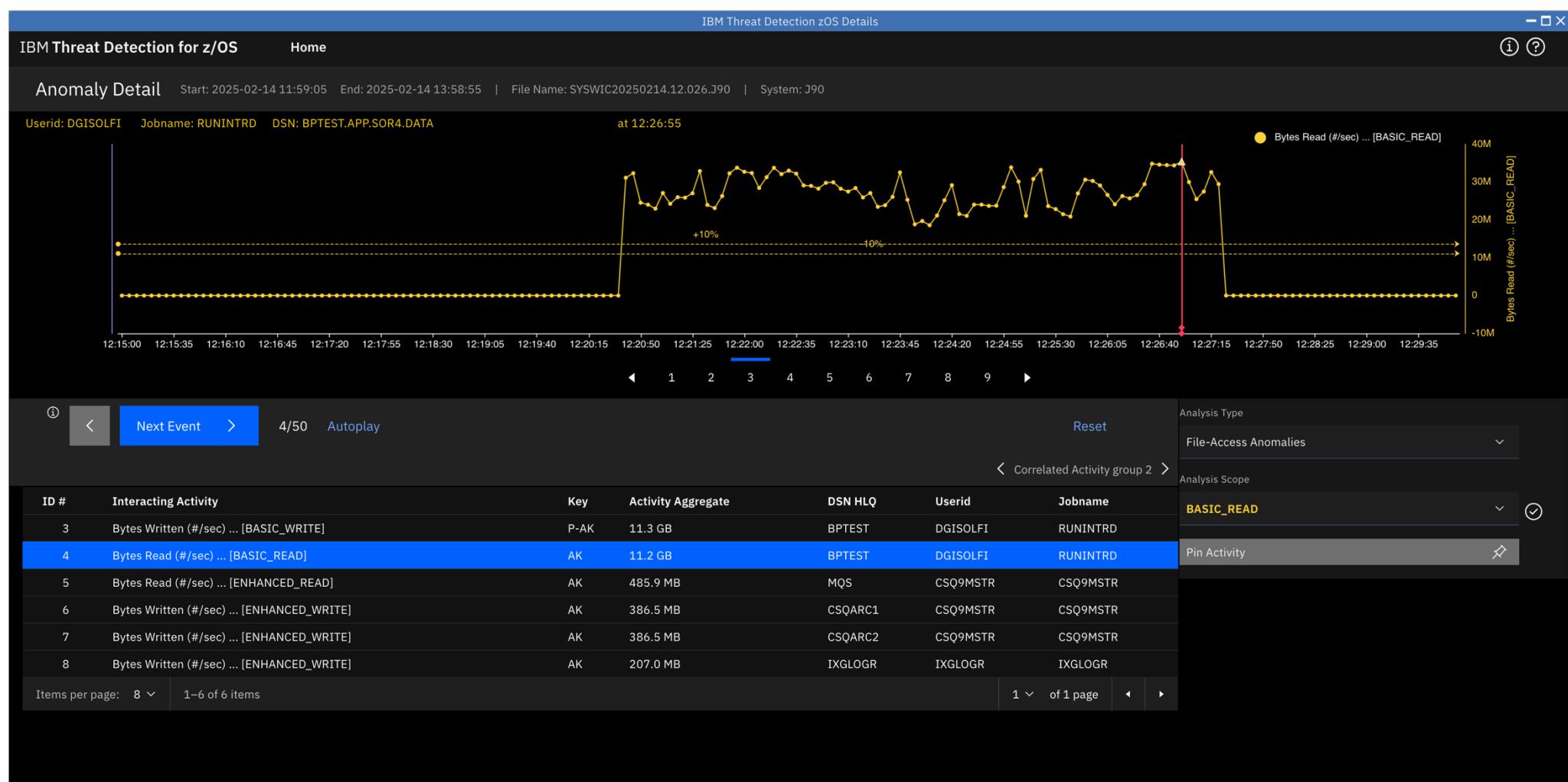
TDz Detail View

- View next Event

- Different pattern but red marker at the same time
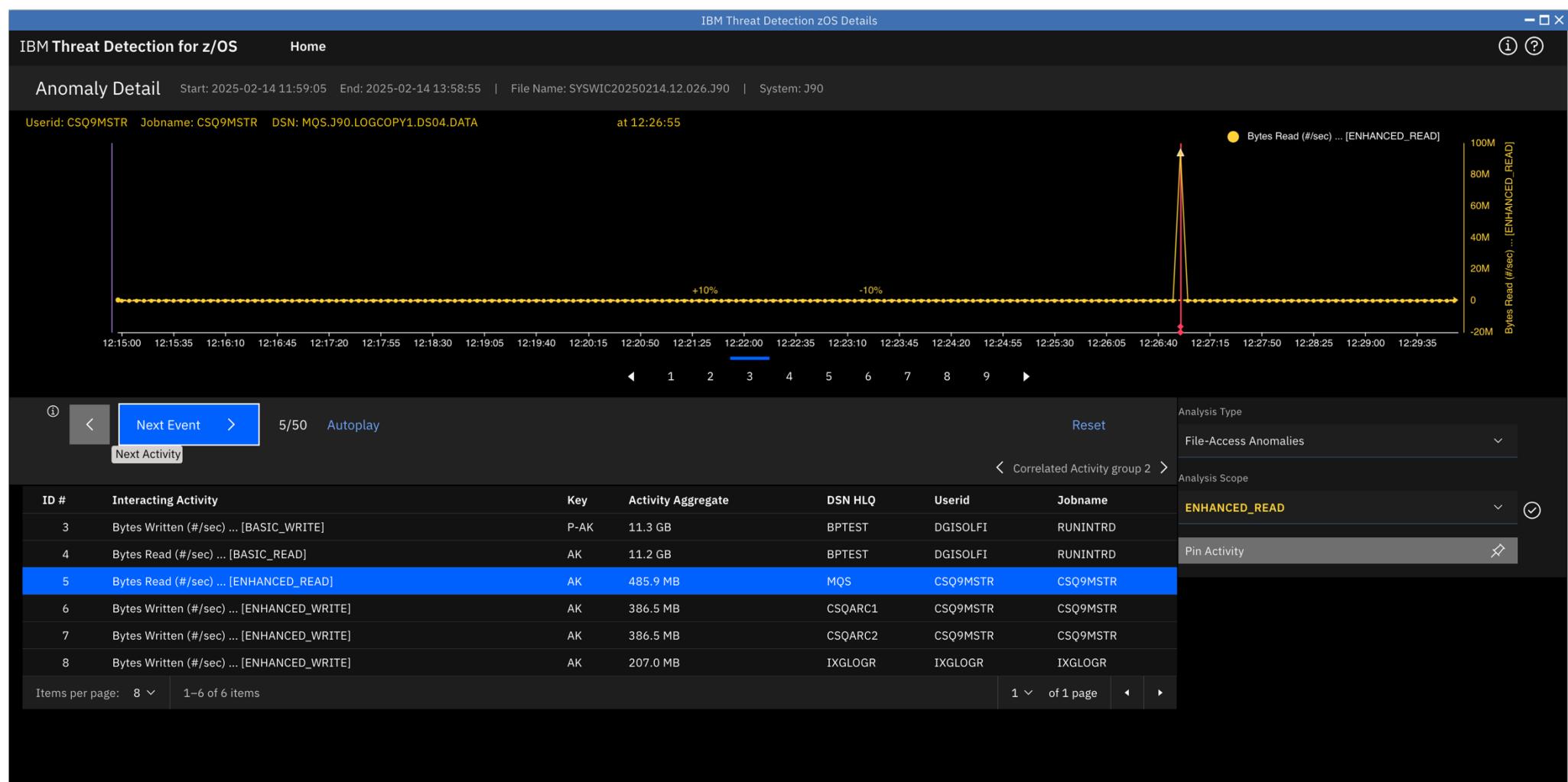
TDz Detail View

- View next Event
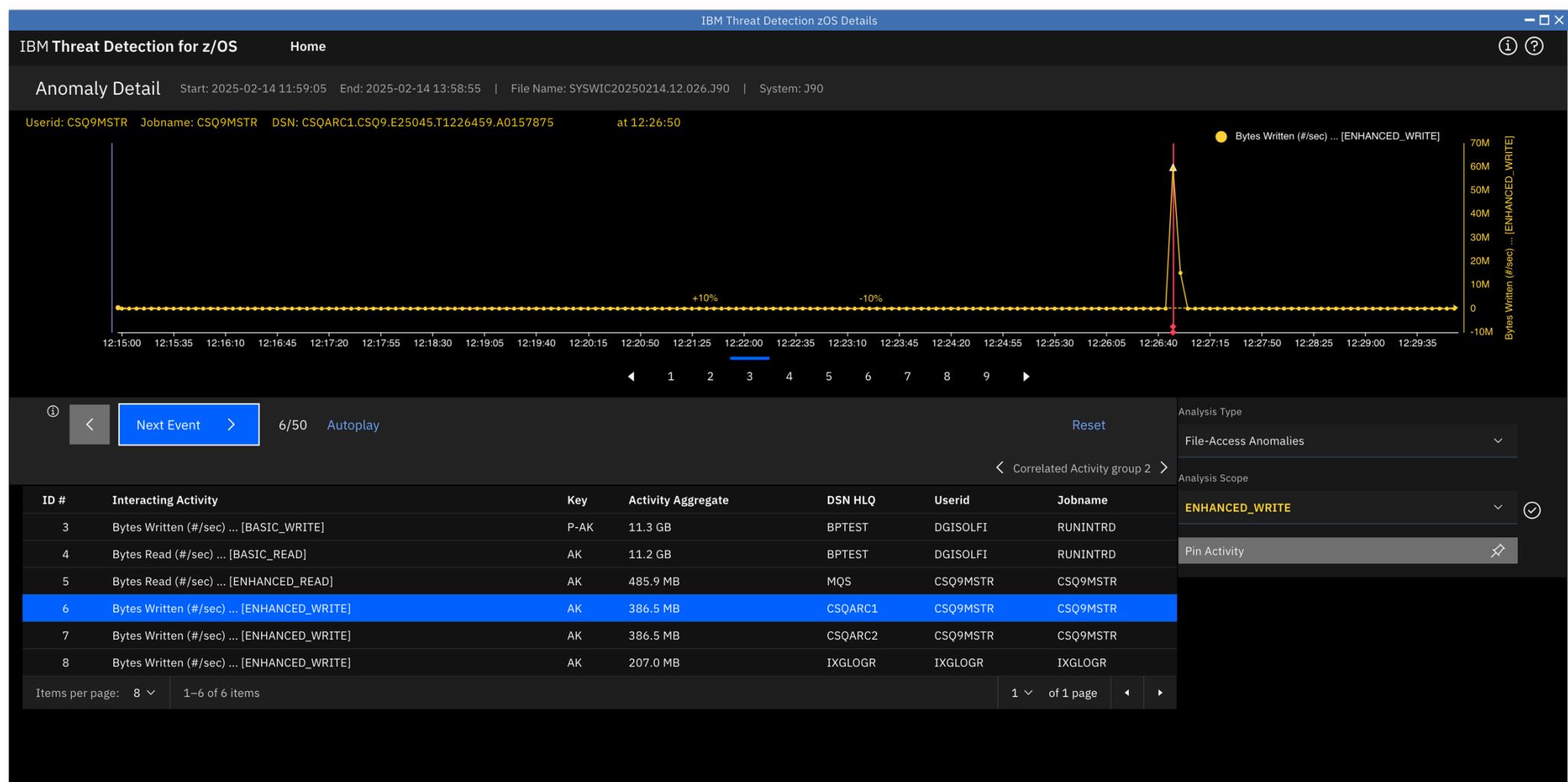
TDz Detail View

- View next Event
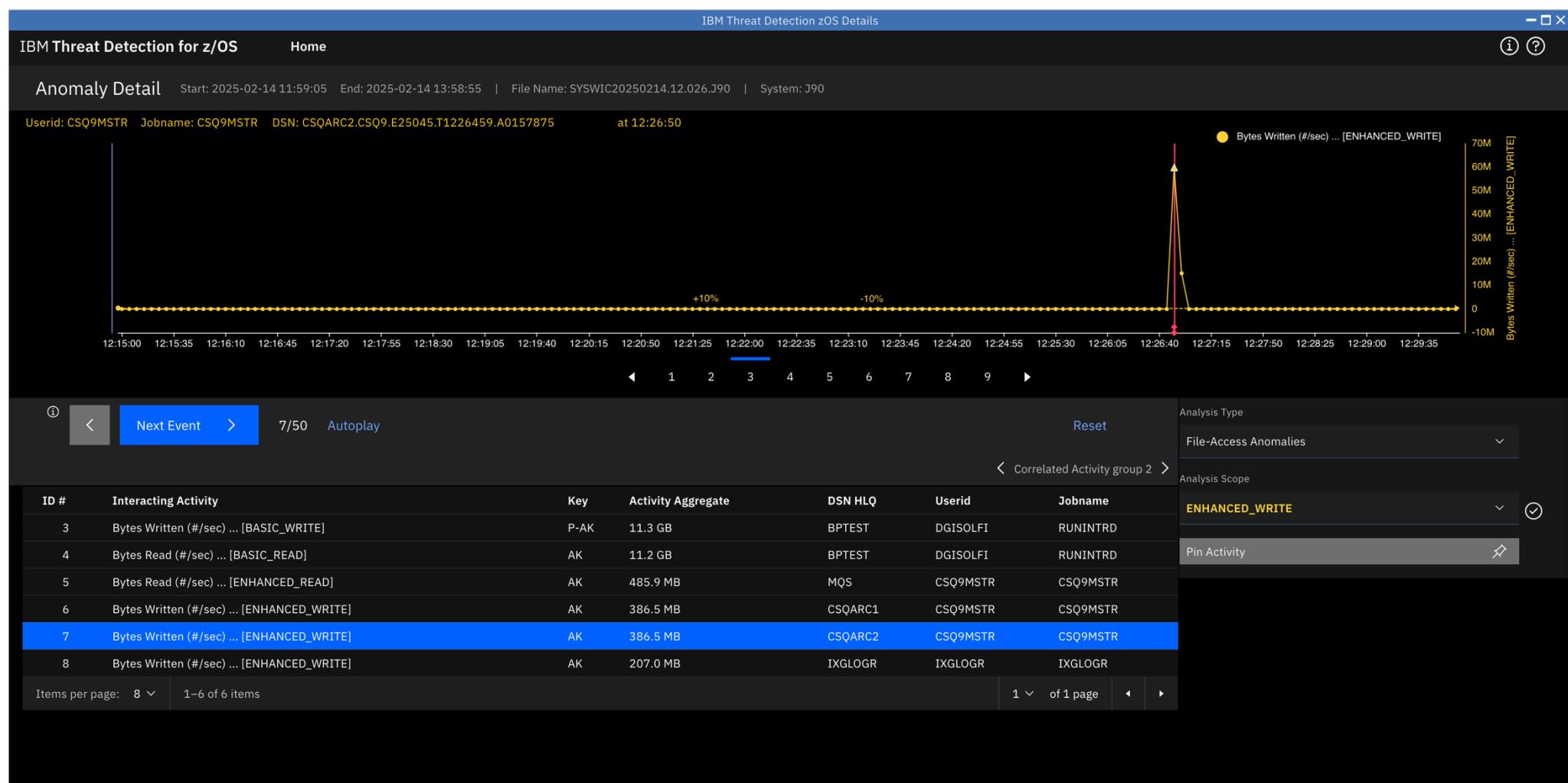
TDz Detail View

- View last Event

- Different
  - Patterns
  - Files
  - UserIds
  - Jobnames

- At almost the same time

- But may be a false positive?

- However event #3 and #4 are highly suspicious

- Let's look at another alert

TDz Dashboard – List View

- Back to List View

- Another alert for the same user and the same job name

- But accessed another dataset

- Go to details

TDz Dashboard – List View

- Further filtering on UserId to see all signatures for this specific UserId could be useful

TDz Dashboard – List View

- Now select SR1

TDz Detail View

- Similar event occurred 20 minutes earlier already

- Hover over red marker for more information

- Investigate user and job

- Probably take immediate action

TDz Dashboard – Exclusions

- Reducing false positives with exclusions

TDz Dashboard – Exclusions

- Opens exclusions tab

- Suggestion list organized in 2 groups
  - userid.jobname
  - HLQ + userid.jobname

- Signatures Column shows the total number of unique signatures matched with the entry

- Scroll down to a high number of signatures

IBM Threat Detection zOS Dashboard

IBM **Threat Detection for z/OS**   Home   Exclusions

Exclusions

You can help to improve the quality of the IBM TDz analytics with the exclusion list. Consider adding the following suggested exclusions to your list by using the check box on each row. Or you can edit the list directly by clicking Edit Exclusion List.

Edit exclusion list ✎

	Exclusion Value	Signatures	Activity Type	Jobname	UserID	Data Set Name	Activity Aggregate
☐	======================= userID.jobname =============================						
	===================== HLQ + userID.jobname =====================						
⌄ ☐	HLQ + userID.jobname: IMSVS.MPR8TN00.*.ENHANCED_WRITE	22	[ENHANCED_WRITE]	AS123400	MPR8TN00	IMSVS.IMSA.D2025031.T1232142.V7ATRCS	2.27 GB
			[ENHANCED_WRITE]	AS135941	MPR8TN00	IMSVS.IMS8.D2025031.T1358214.V3ETRCS	3.07 GB
			[ENHANCED_WRITE]	AS151438	MPR8TN00	IMSVS.IMS8.D2025034.T1512538.V92TRCS	3.23 GB
⌄ ☐	HLQ + userID.jobname: CANDLE.OMEGADM.*.ENHANCED_READ	23	[ENHANCED_READ]	JA56TMS	OMEGADM	CANDLE.PLEX1.JA56RT.HPD20002.D	259.94 MB
			[ENHANCED_READ]	JA56TMS	OMEGADM	CANDLE.PLEX1.JA56RT.HPD20001.D	199.01 MB
			[ENHANCED_READ]	JA56TMS	OMEGADM	CANDLE.PLEX1.JA56RT.HPD20003.D	536.89 MB
⌃ ☐	HLQ + userID.jobname: CSQARC1.CSQ9MSTR.*.ENHANCED_WRITE	6	[ENHANCED_WRITE]	CSQ9MSTR	CSQ9MSTR	CSQARC1.CSQ9.E25032.T0723581.A0154710	370.83 MB
			[ENHANCED_WRITE]	CSQ9MSTR	CSQ9MSTR	CSQARC1.CSQ9.E25032.T0801092.A0154717	392.83 MB
			[ENHANCED_WRITE]	CSQ9MSTR	CSQ9MSTR	CSQARC1.CSQ9.E25032.T0805337.A0154718	542.59 MB
			[ENHANCED_WRITE]	CSQ9MSTR	CSQ9MSTR	CSQARC1.CSQ9.E25032.T0904248.A0154729	574.40 MB
			[ENHANCED_WRITE]	CSQ9MSTR	CSQ9MSTR	CSQARC1.CSQ9.E25032.T1805192.A0154829	614.60 MB
			[ENHANCED_WRITE]	CSQ9MSTR	CSQ9MSTR	CSQARC1.CSQ9.E25037.T0101031.A0155723	887.19 MB
⌄ ☐	HLQ + userID.jobname: CSQARC2.CSQ9MSTR.*.ENHANCED_WRITE	6	[ENHANCED_WRITE]	CSQ9MSTR	CSQ9MSTR	CSQARC2.CSQ9.E25032.T0723581.A0154710	370.83 MB

TDz Dashboard – Exclusions

- 2 different approaches

- Select an entry

- Press „add to exclusion list" button in the blue line

- Confirm your selection

- Exclusion policy file is updated automatically

TDz Dashboard – Exclusions

- Manually change the exclusion list

- Press the Edit exclusion list button

TDz Dashboard – Exclusions

- Manually add your entry to the exclusion list