IBM Threat Detection for z/OS

22.10.2025

Jost Mumm
Leading Technical Sales Professional
IBM Deutschland GmbH
+49-171-3045940
jostmumm@de.ibm.com

Agenda

- Motivation for Anti-Malware Software
- IBM Threat Detection for z/OS (TDz) – Solution Overview
- Summary – things to remember

Regulatory Soup / Compliance

In collaboration with IBM Z & LinuxONE clients

Bundesamt für Sicherheit in der Informationstechnik (BSI)

KRITIS

DISA

NIST

BaFin

CCPA

Informationssicherheitsgesetz des Bundes (ISG)

GDPR

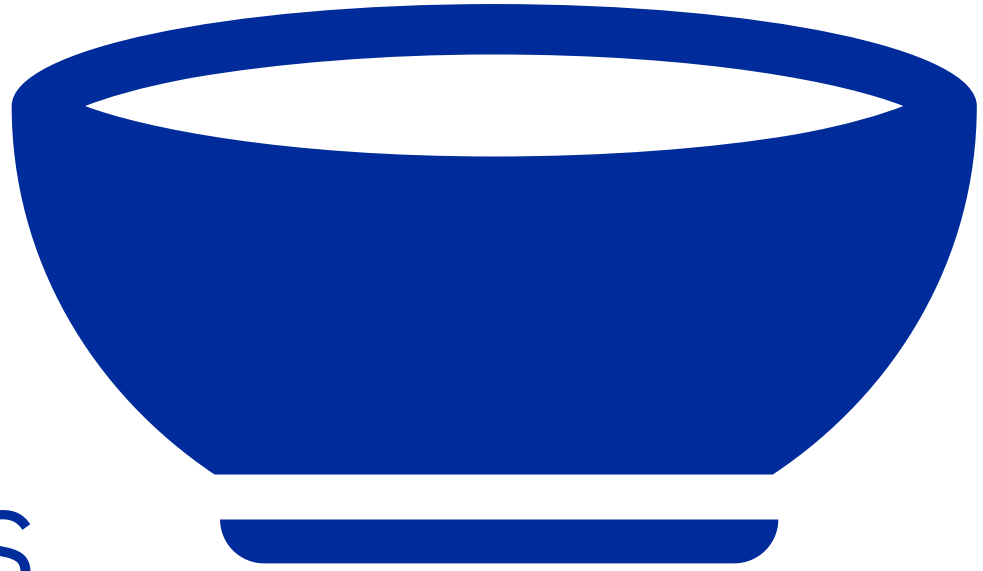
PCI PIN

NIS2

HIPAAç

FFIEC

Interac



PCI

ISO 27001

CCPA

DORA

Local Market (e.g., China)

FedRamp

DISA

PCI DSS

SOX

KVKK

FINMA

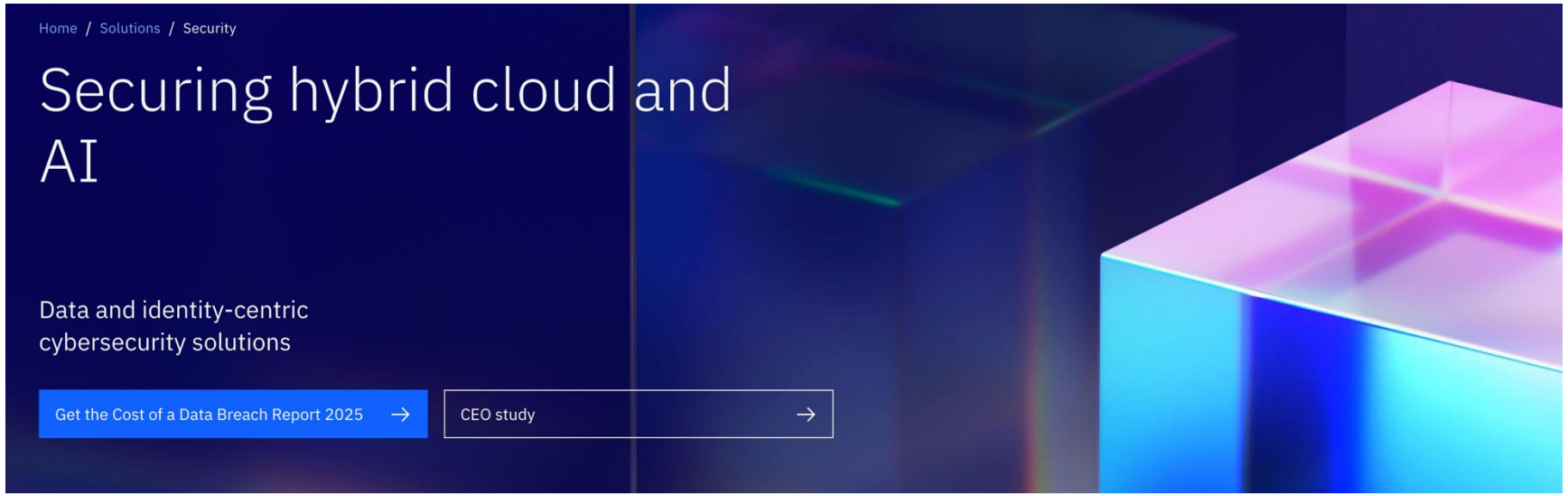
Deutsche Kreditwirtschaft

Cost of a Data Breach

USD 300+ million - Average cost of a “mega breach” involving 30-40M records

“More AI equaled faster identification and containment - Organizations extensively using security AI and automation identified and contained data breaches nearly 100 days faster on average than organizations that didn’t use these technologies at all.”

See https://www.ibm.com/security for the full “Cost of Data Breach Report 2025”



Statement of Direction: Anti-malware for IBM z/OS

"IBM plans to provide a software solution that introduces *cyber anomaly detection* … to provide the option of *quarantine functionality* … to satisfy compliance regulations requiring *anti-malware* … for z/OS."

Full SOD here: https://www.ibm.com/docs/en/announcements/statement-direction-security-zos

IBM TDz is intended to fulfill the "cyber anomaly detection" aspect of this SOD.*

*Statements by IBM regarding its plans, directions, and intent are subject to change or withdrawal without notice at the sole discretion of IBM. Information regarding potential future products is intended to outline general product direction and should not be relied on in making a purchasing decision. The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for IBM products remain at the sole discretion of IBM.

Detection bridges security with resiliency

"Malicious code protection mechanisms include **both signature- and nonsignature-based technologies**. Nonsignature-based detection mechanisms include artificial intelligence techniques that use heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide controls against such code for which signatures do not yet exist or for which existing signatures may not be effective …"

IBM TDz is designed to identify and issue alerts for anomalous data access related incidents which could assist clients in their adherence to the DETECT core function of the NIST Cybersecurity Framework*.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
(CFS Core 2.0, DE.CM-09)

*Client is responsible for its response to alerts issued by IBM TDz, whether automated or manual.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Cybersecurity Framework:
https://www.nist.gov/cyberframework

Emerging regulations

PCI DSS 4.0 - Historically, PCI-DSS regulations have emphasized anti-virus software, calling for confirmed, signature-based scans for specific forms of malware, which did not apply to mainframes. PCI 4.0 expands this greatly to **anti-malware** (mentioning it over 50 times), including **non-signature-based detection**, when combined with **blocking** and/or **quarantining** malicious software.
The full reference is here:
https://east.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss

---

DORA - "The Digital Operational Resilience Act (Regulation (EU) 2022/2554) solves an important problem in the EU financial regulation. Before DORA, financial institutions managed the main categories of operational risk mainly with the allocation of capital, but they did not manage all components of operational resilience. After DORA, they must also follow rules for the protection, **detection, containment,** recovery and repair capabilities against ICT-related incidents…"
See: https://www.digital-operational-resilience-act.com/

IBM TDz is designed to identify and issue alerts for anomalous ICT-related incidents which could assist clients in their adherence to Article 10 (Sections 1 & 2), Detection, of the EU Digital Operational Resilience Act (DORA) requirements.*

* Client is responsible for its response to alerts issued by IBM TDz, whether automated or manual.

Sponsor User Insights (2021-2024)

IBM Design Thinking: Shaped IBM Threat Detection for z/OS Offering

Threat Detection Design Points

- Lightweight AI
- Fit-for-purpose data generation
- Sysplex Wide Analysis
- Built into DNA of z/OS (z/OS Solution Stack)
- Always-On

90

Engagement hours with clients

40

User needs / features prioritized and discussed with 8 clients in regular meetings

75%

Sponsor users want to adopt a capability in this space by the end of 2024.

8 TBs

Amount of data collected across multiple client clients (~45 LPARs)

IBM Threat Detection for z/OS 1.1 delivers AI-driven discovery of anomalies that could be indicative of a cyberattack

Published: 10 September 2024

Availability date: 13 September 2024

- IBM Threat Detection for z/OS 1.1 (5698-CA1)
- IBM Threat Detection for z/OS 1.1 Subscription and support (5698-CAS)

https://www.ibm.com/docs/announcements/AD24-0716

Agenda

- Motivation for Anti-Malware Software
- IBM Threat Detection for z/OS (TDz) – Solution Overview
- Summary – things to remember

IBM Threat Detection for z/OS overview

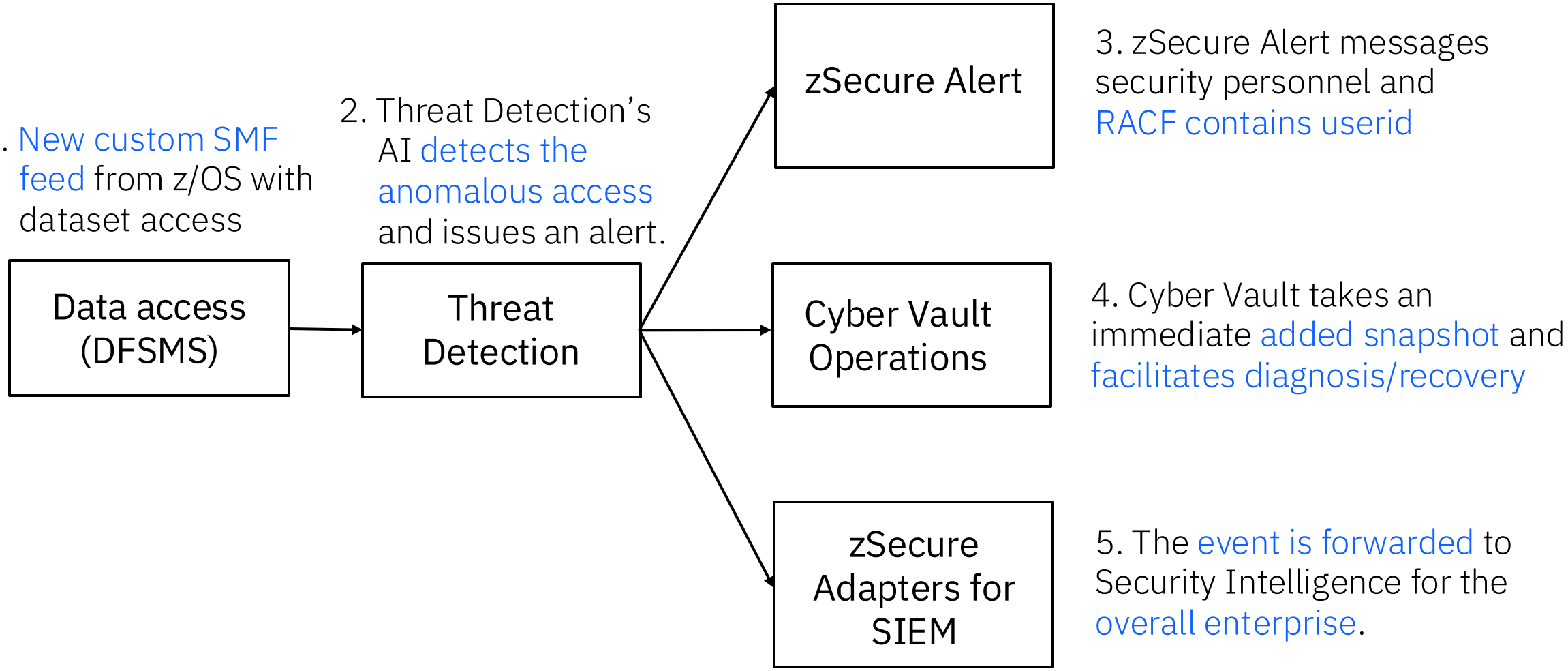
- Detects anomalous, potentially malicious, data access on z/OS
  - Lightweight AI
  - Policy/Exclusion lists for false positive mitigation

- Leverages IBM Z Workload Interaction Correlator (zWIC) facilitated SMF feed at the DFSMS™ level
  - VSAM & non-VSAM reads and writes
  - SMF 98 new subtypes 5-8 records

- GUI dashboard to further explain the anomaly and simplify diagnosis (z/OSMF plugin)

- Notification issued via console message & SMF record, facilitating integration with…
  - GDPS/LCP & its Safeguarded Copy operations
  - zSecure Alert notification expansion
  - zSecure SIEM Adapter feed for SIEMs

z/OS Anti-Malware flow



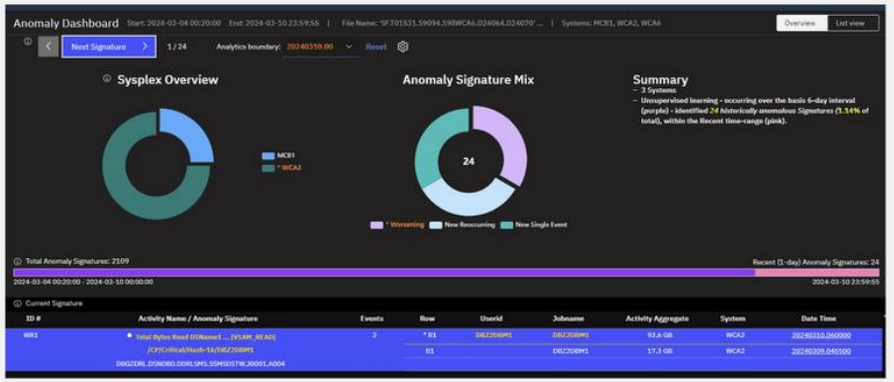
Near-term IBM Z integration roadmap

- 1Q25 zSecure Alert & Adapters for SIEM
- For integration with for Cyber Vault operations and GDPS:
  "IBM intends to extend *GDPS® LCP Manager to consume event notification* from the anti-malware solution for z/OS … to *enable policy-driven actions to be taken* based on the event."
  Full SOD found here: https://www.ibm.com/downloads/cas/DRWZAGYK
- RACF userid containment:
  Provide support for IBM TDz to enable security architects to leverage data access-based threat detection AI, with RACF userid containment, to provide an additional mitigation option against potential cyberthreats.
  Preview for z/OS 3.2: https://www.ibm.com/docs/en/announcements/preview-zos-32-plans-unlock-value-z17
- Backup Resiliency's malicious diagnosis:
  Displaying and filtering IBM TDz records, display user activity in IBM Z Backup Resiliency (IZBR) and drive recovery points analysis.
  Full SOD found here: https://www.ibm.com/docs/en/announcements/statement-direction-z-backup-resiliency-intends-integrate-zos-dfsms-cloud-data-manager-threat-detection-zos
- For integration with Comm Server (Network):
  "IBM intends to add network anomaly detection to its IBM Threat Detection for z/OS product."
  Full SOD found here: https://www.ibm.com/docs/en/announcements/z17-makes-more-possible

LCP Manager integration - **Policy-Driven Automation from TDz Notifications**

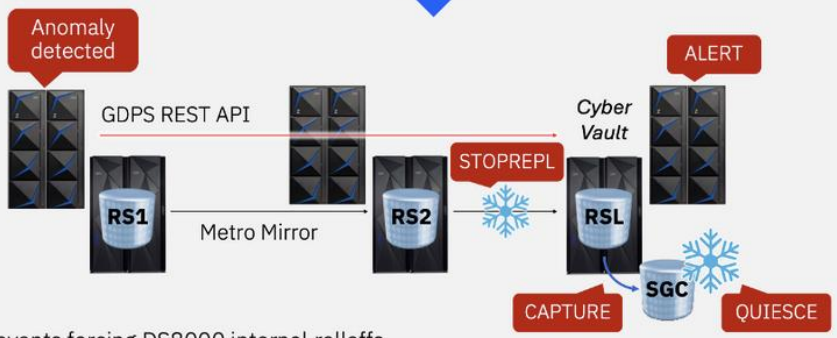
- Triggering policy-based automation actions that can create out-of-cycle copies, quiesce additional backups, and perform other protective actions.
- This capability will be available in both GDPS LCP Manager and Stand-alone LCP Manager.

Threat Detection for z/OS integration



IBM Threat Detection for z/OS
Uses AI to detect z/OS anomalies across a sysplex in near-real time

Standalone LCP Manager
Automated response to Threat Detection events



ALERTS - SDF alerts issued for each event
CAPTURE - Take a new capture for forensic analysis
QUIESCE - Suspend all LCP capture and release operations
STOPREPL - Stop replication into the vault to prevent out-of-space events forcing DS8000 internal rolloffs

BLOG Entry: https://community.ibm.com/community/user/blogs/nathan-brice1/2025/10/01/z-cyber-vault-4q25-update

RACF userid containment

Extending RACF userid revocation

- Subsequent RACF access checks fail
- Sysplex-wide notification signal
- Revocation still occurs on next logon

Providing safeguards

- Protected with a new custom RACF profile
- Supports containment reversal as needed
- Exclusion lists support proactive planning

>> ALTUSER -- >

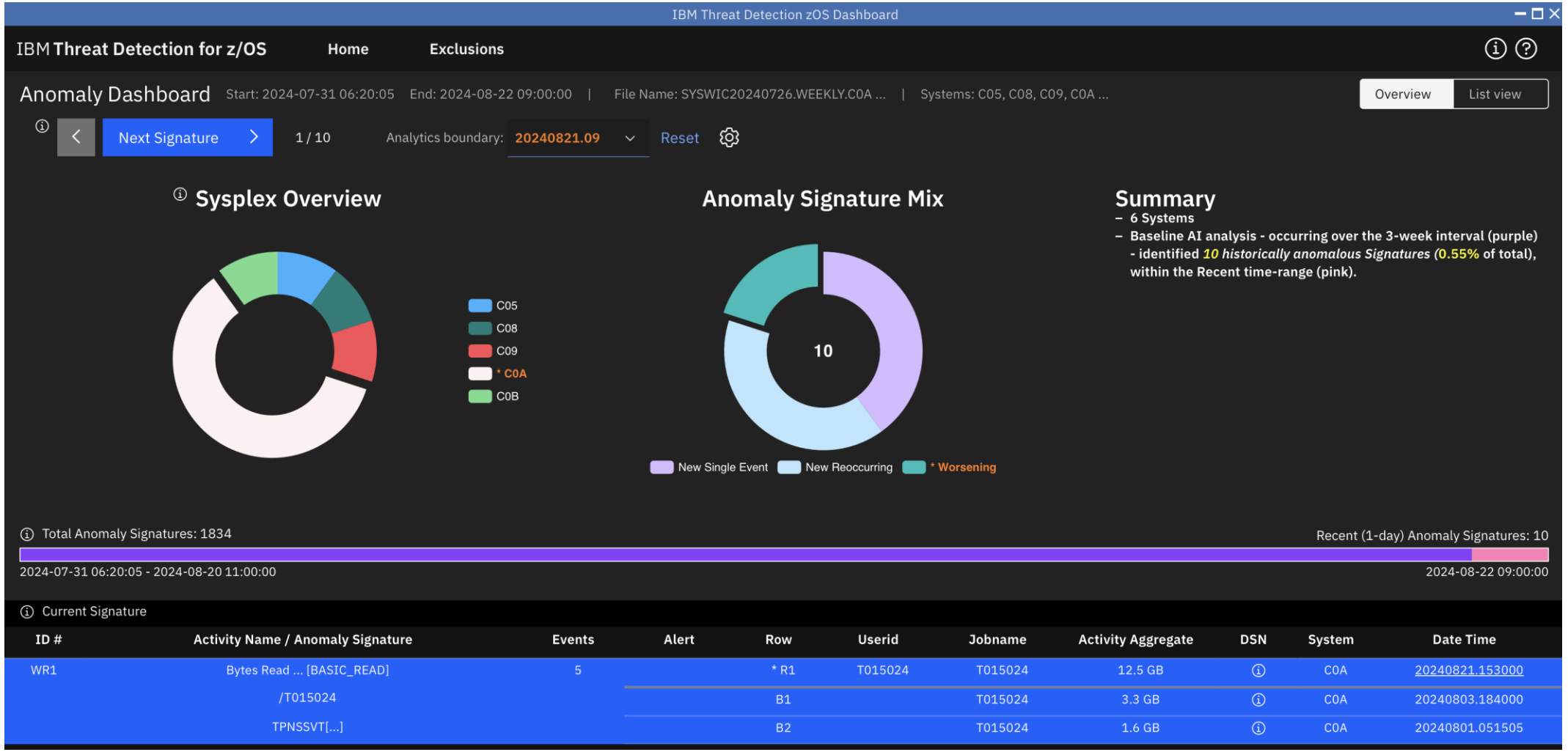
>---------- >

|--- REVOKE(date) | NOREVOKE | CONTAIN | NOCONTAIN | NEVERCONTAIN | ALLOWCONTAIN ---|

- CONTAIN – Causes future access requests to fail and invokes REVOKE without a date
- NOCONTAIN – Reverses access request blockage of CONTAIN but does not directly RESUME
- NEVERCONTAIN – Prevents CONTAIN from affecting a userid
- ALLOWCONTAIN – Removes the NEVERCONTAIN attribute from the userid
- RESUME – Existing keyword essentially the same but fails if CONTAIN is in effect

UI Sample

- Application will run on USS detecting anomalies and issuing alerts
- User can log into the zOSMF plug-in to view details



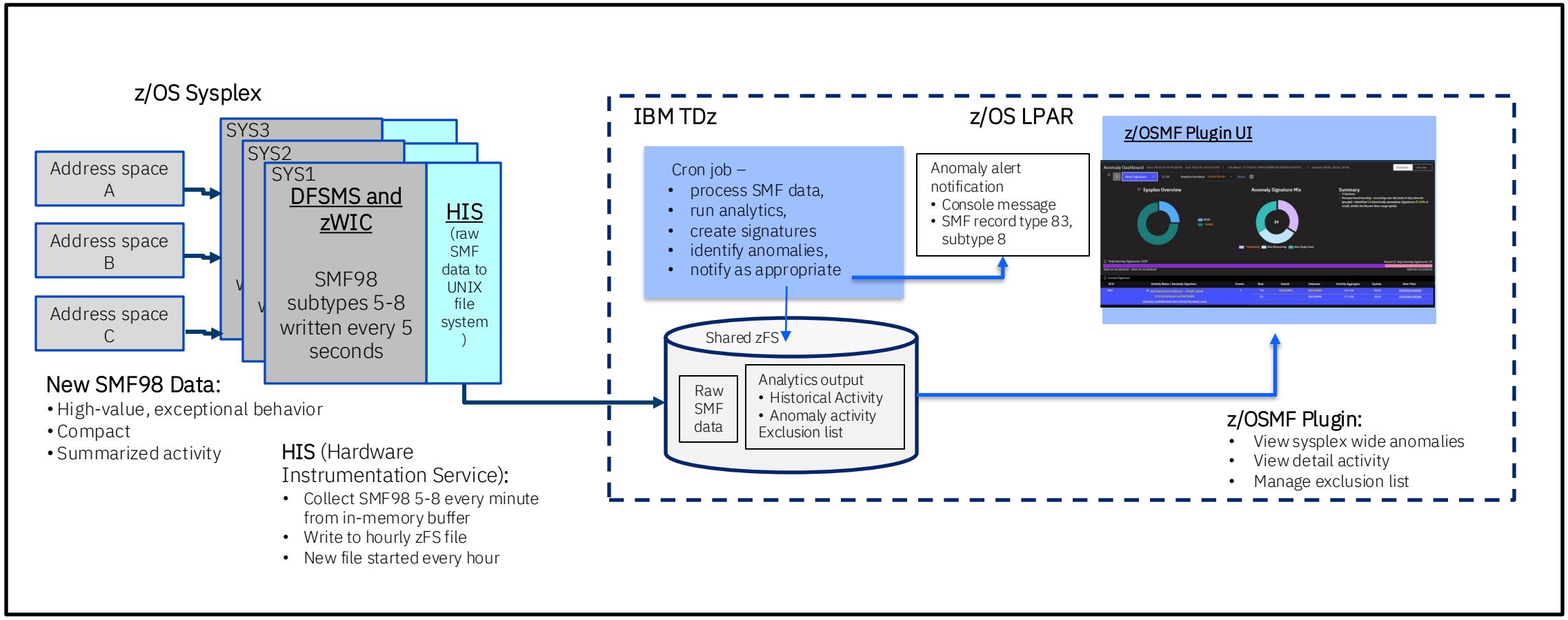
Anomaly message format

Sample Message Text (coincides with new SMF 83 subtype 8 record):

BRY0200W A file access anomaly was detected.
Anomaly ID: SYS1.20240201.092058
Sysplex Name: LOCAL
System Name: SYS1
Time Of Anomaly: 20240201.092058
Userid: JONSMITH
Jobname: STLFMLA
Data Set Name: HLQ1.CRIT.ICAL.INFO
Volser: VLM123
Data Set Activity Type: Enhanced Read
Data Set Activity Size: 32.1 GB

IBM Threat Detection for z/OS

Architecture flow



IBM Threat Detection technical requirements

The Threat Detection tool itself requires:

- IBM z/OS V2.5 or later
  - z/OSMF set up and configured
- IBM Semeru Runtime Certified Edition for z/OS, Version 17 or higher
- IBM SDK for Node.js: version 20.0 or higher

Each participating system that is sending data will need:

- DFSMS with APAR OA66676 applied and configured for the new SMF generation
- IBM z/OS Workload Interaction Correlator with APAR OA66716 applied
- HIS and SMF logstream with in memory enabled

Full documentation found here: https://ibm.biz/tdzdocs

zWIC and zACS entitlement

- **IBM z/OS Workload Interaction Correlator** (zWIC) and **IBM z/OS Authorized Code Scanner (zACS)** are optional priced features of z/OS

- **zWIC and zACS are both entitled with the license of IBM TDz**
  - zACS is an authorized code scanner of Program Call (PC) and Supervisor Call (SVC) routines
  - It prevents unauthorized callers from being incorrectly granted an authorized state

- zWIC documentation can be found at https://www.ibm.com/docs/en/zos/3.1.0?topic=collections-zos-workload-interaction-correlator

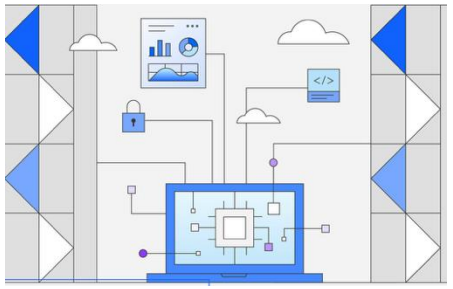
- zACS documentation can be found at www.ibm.biz/zacsdoc

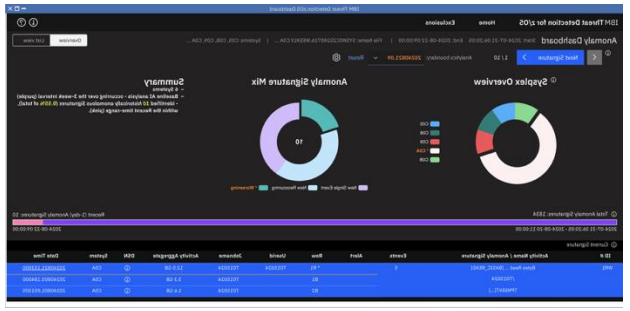
Agenda

- Motivation for Anti-Malware Software
- IBM Threat Detection for z/OS (TDz) – Solution Overview
- Summary – things to remember

Things to remember

- **z/OS Security is more than RACF** or another ESM. There are additional new solutions, like **IBM Threat Detection for z/OS (TDz)** which might **help with Compliance and improve IBM Z Security** for your enterprise.
- **IBM Threat Detection for z/OS (IBM TDz)** is an artificial intelligence software product that brings the **detection** of anomalous, potentially malicious, **data access** to the z/OS platform.
- IBM TDz is not part of the z/OS Base (separate PID - 5698-CA1). There are two priced features of z/OS **(zACS and zWIC)** that are entitled with licensing IBM TDz.
- There are **SoDs** for further integration of IBM TDz
- Documentation of IBM TDz: https://www.ibm.com/docs/en/tdz/1.1.0





Questions?