IBM Security solutions for z/OS – a (selective) overview (with a focus on acticity monitoring and alerting & compliance evaluation for Db2)

Günter Weber
CTP - IBM Z Security

IBM Security zSecure Suite
IBM Z Security and Compliance Center
IBM Z Multi-Factor Authentication
IBM Security Guardium S-TAPs for z/OS

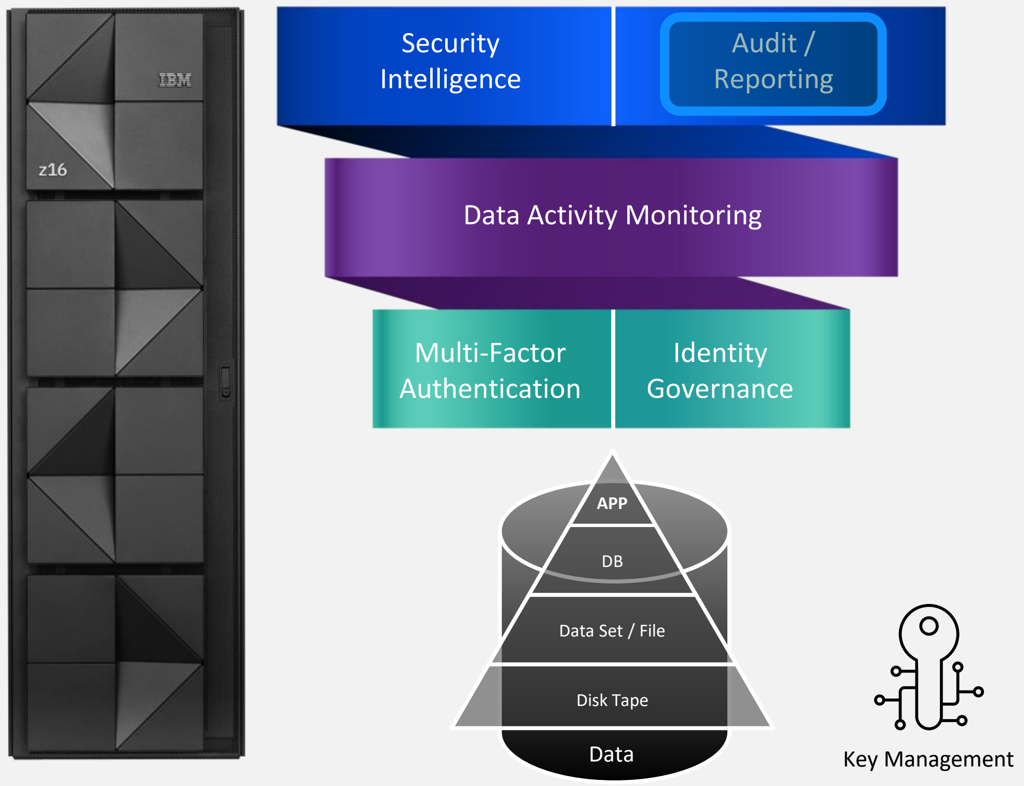
weberg@de.ibm.com

IBM **Security**

CISSP® | Certified Information Systems Security Professional

IBM®

Protecting data at the core of the enterprise



Security Intelligence

Audit / Reporting

Data Activity Monitoring

Multi-Factor Authentication

Identity Governance

APP

DB

Data Set / File

Disk Tape

Data

Key Management

“Encryption is the solid foundation of a layered cybersecurity strategy.”

Relevant IBM Security Solutions:

- IBM Security zSecure Suite
- IBM Z Security and Compliance Center
- IBM Z Multi-Factor Authentication
- IBM Security Guardium Family
- IBM Security Verify Governance
- IBM Security QRadar®
- IBM UKO for z/OS®

Guardium DP & Guardium VA

Why audit? Isn’t the mainframe already secure?

Common arguments:

- “We don't need to audit because we use RACF, Top Secret or ACF/2”
- “We control who is connected to the privileged user groups and we know what those people are authorized to do”

Counter arguments:

- All access products do two things:
  - Prevents people from accessing a resource that is not appropriate for their job
  - Allows people access to the necessary data to do their job
- But access control products do NOT:
  - Prevent a malicious update or an authorized user from accessing sensitive data that is ***NOT*** within the scope of their job

BOTTOM LINE

- You need both robust access control and fine-grained auditing to adequately protect the database environment

Guardium for System z - Components

Guardium Collector appliance for System z

- Securely stores audit data collected by mainframe S-TAP
- Provides analytics, reporting & compliance workflow automation
- Centralized, cross-platform audit repository for enterprise-wide analytics and compliance reporting across mainframe & distributed environments

S-TAP (for Db2, IMS or Data Sets) on z/OS for event capture

- Mainframe probe that collects audit data for Guardium appliance
- Collection policies managed on the Guardium appliance
- Extensive filtering available to optimize data volumes and performance
- Enabled for zIIP processing

Determining what to monitor

Meet compliance requirements

- Monitor privileged user activity
- Monitor the tables that contain sensitive data
- **Monitor the datasets that contain sensitive data**
- Produce alerting when suspicious activity is detected
- Selectively monitor activity (eliminate auditing for batch)

Guardium for System z – Policies/Rules

A Guardium policy is a “set of rules”

There are rules that get executed on the z/OS LPAR

Db2 / IMS or Dataset collection profiles

These collection profiles determine what kind of activity is send to the Guardium collector

There are rules that get processed on the collector

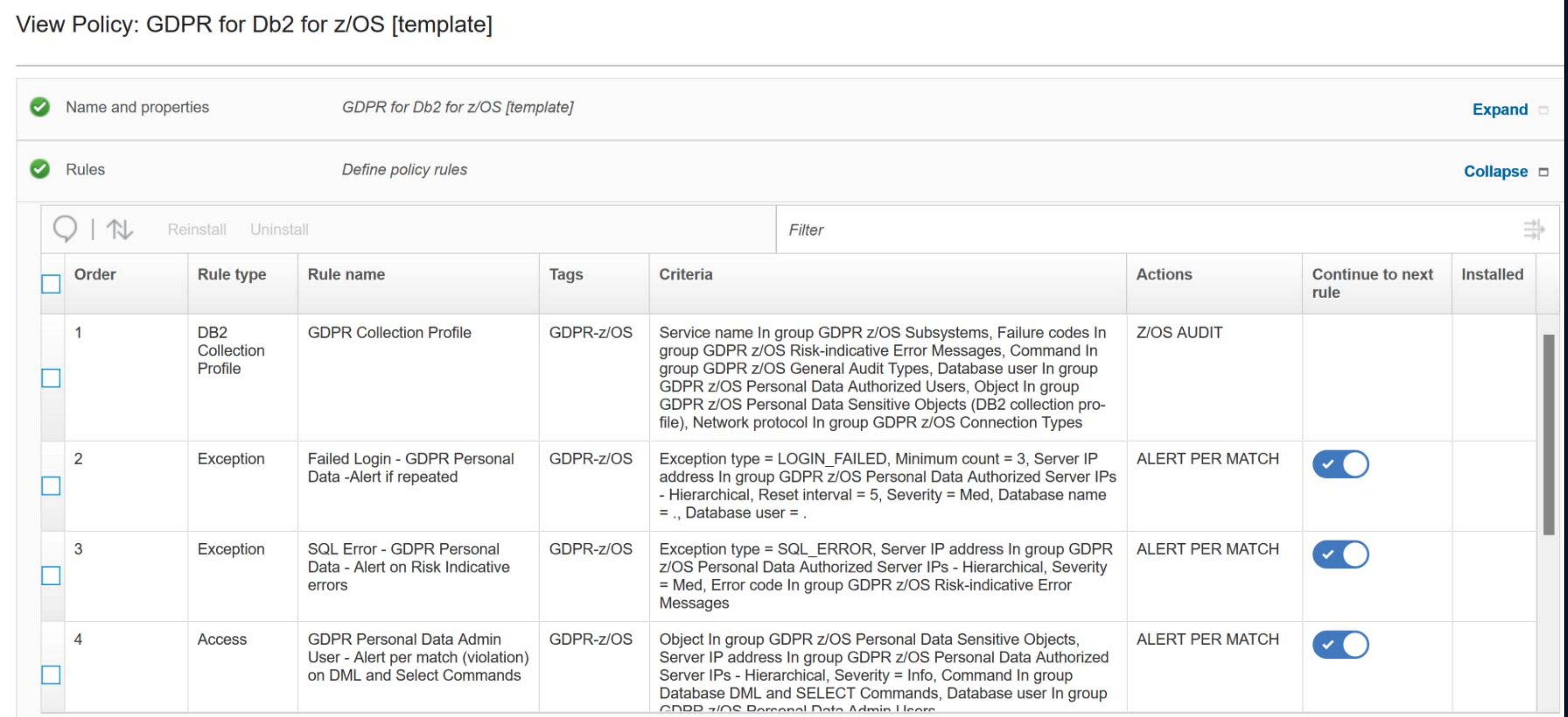
Access Rules that decide if an event:

should trigger an alert (e.g. Email, SIEM-Record)

is just collected for a report

is skipped

Guardium for System z – Templates for Monitoring e.g. for GDPR

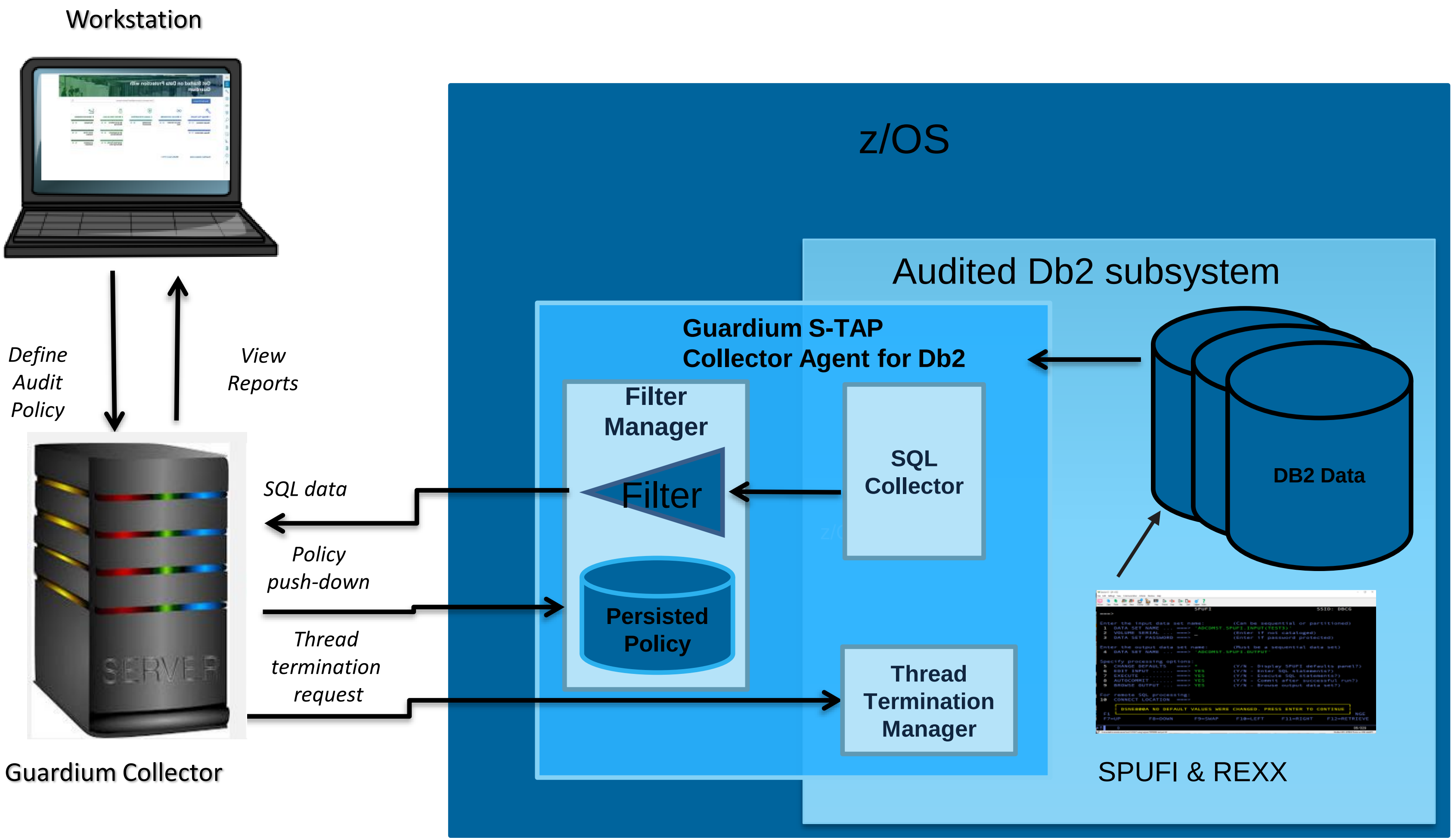


View Policy: GDPR for Db2 for z/OS [template]

✓	Name and properties	*GDPR for Db2 for z/OS [template]*	Expand
✓	Rules	*Define policy rules*	Collapse

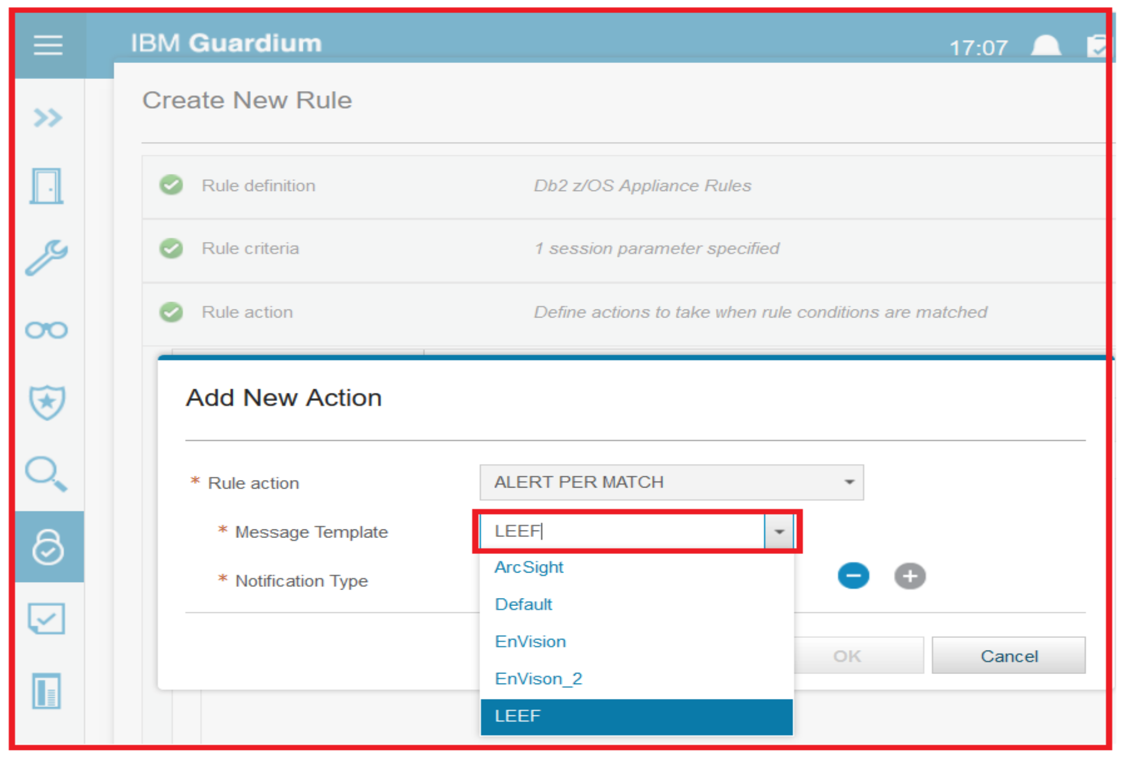
□	Order	Rule type	Rule name	Tags	Criteria	Actions	Continue to next rule	Installed
□	1	DB2 Collection Profile	GDPR Collection Profile	GDPR-z/OS	Service name In group GDPR z/OS Subsystems, Failure codes In group GDPR z/OS Risk-indicative Error Messages, Command In group GDPR z/OS General Audit Types, Database user In group GDPR z/OS Personal Data Authorized Users, Object In group GDPR z/OS Personal Data Sensitive Objects (DB2 collection profile), Network protocol In group GDPR z/OS Connection Types	Z/OS AUDIT		
□	2	Exception	Failed Login - GDPR Personal Data -Alert if repeated	GDPR-z/OS	Exception type = LOGIN_FAILED, Minimum count = 3, Server IP address In group GDPR z/OS Personal Data Authorized Server IPs - Hierarchical, Reset interval = 5, Severity = Med, Database name = ., Database user = .	ALERT PER MATCH	✓	
□	3	Exception	SQL Error - GDPR Personal Data - Alert on Risk Indicative errors	GDPR-z/OS	Exception type = SQL_ERROR, Server IP address In group GDPR z/OS Personal Data Authorized Server IPs - Hierarchical, Severity = Med, Error code In group GDPR z/OS Risk-indicative Error Messages	ALERT PER MATCH	✓	
□	4	Access	GDPR Personal Data Admin User - Alert per match (violation) on DML and Select Commands	GDPR-z/OS	Object In group GDPR z/OS Personal Data Sensitive Objects, Server IP address In group GDPR z/OS Personal Data Authorized Server IPs - Hierarchical, Severity = Info, Command In group Database DML and SELECT Commands, Database user In group GDPR z/OS Personal Data Admin Users	ALERT PER MATCH	✓	

Guardium S-TAP for Db2 on z/OS Architecture



```
                         SPUFI                                    SSID: DBCG
 ===>

 Enter the input data set name:          (Can be sequential or partitioned)
  1  DATA SET NAME ... ===> 'ADCDMST.SPUFI.INPUT(TEST3)'
  2  VOLUME SERIAL ... ===> _            (Enter if not cataloged)
  3  DATA SET PASSWORD ===>              (Enter if password protected)

 Enter the output data set name:         (Must be a sequential data set)
  4  DATA SET NAME ... ===> 'ADCDMST.SPUFI.OUTPUT'

 Specify processing options:
  5  CHANGE DEFAULTS   ===> *            (Y/N - Display SPUFI defaults panel?)
  6  EDIT INPUT ...... ===> YES          (Y/N - Enter SQL statements?)
  7  EXECUTE ......... ===> YES          (Y/N - Execute SQL statements?)
  8  AUTOCOMMIT ...... ===> YES          (Y/N - Commit after successful run?)
  9  BROWSE OUTPUT ... ===> YES          (Y/N - Browse output data set?)

 For remote SQL processing:
 10  CONNECT LOCATION  ===>

     DSNE808A NO DEFAULT VALUES WERE CHANGED. PRESS ENTER TO CONTINUE
  F1                                                                       NGE
  F7=UP        F8=DOWN      F9=SWAP      F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

Integration with a SIEM / e.g. QRadar or SPLUNK



IBM Guardium

17:07

Create New Rule

Rule definition	*Db2 z/OS Appliance Rules*
Rule criteria	*1 session parameter specified*
Rule action	*Define actions to take when rule conditions are matched*

Add New Action

* Rule action: ALERT PER MATCH

* Message Template: LEEF

* Notification Type

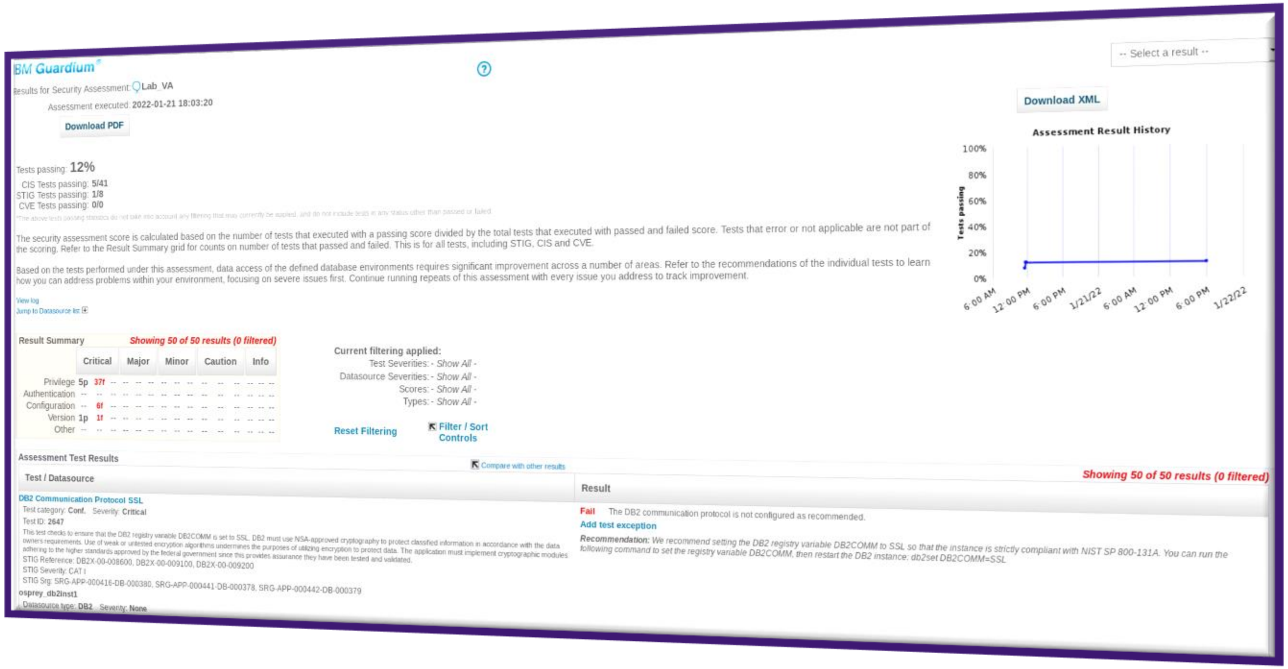
Guardium Vulnerabilty Assessment for Db2

Iterative process

Runs a set of tests to a datasource

Tracks results and offers suggestions to fix discrepancies

Started from the Guardium appliance (creates a remote connection to Db2 datasource)



Results for Security Assessment: Lab_VA

Assessment executed: 2022-01-21 18:03:20

Tests passing: 12%

CIS Tests passing: 5/41
STIG Tests passing: 1/8
CVE Tests passing: 0/0

*The above tests passing statistics do not take into account any filtering that may currently be applied, and do not include tests in any status other than passed or failed.

The security assessment score is calculated based on the number of tests that executed with a passing score divided by the total tests that executed with passed and failed score. Tests that error or not applicable are not part of the scoring. Refer to the Result Summary grid for counts on number of tests that passed and failed. This is for all tests, including STIG, CIS and CVE.

Based on the tests performed under this assessment, data access of the defined database environments requires significant improvement across a number of areas. Refer to the recommendations of the individual tests to learn how you can address problems within your environment, focusing on severe issues first. Continue running repeats of this assessment with every issue you address to track improvement.

Result Summary *Showing 50 of 50 results (0 filtered)*

	Critical			Major			Minor			Caution			Info		
Privilege	5p	37f	--	--	--	--	--	--	--	--	--	--	--	--	--
Authentication	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Configuration	--	6f	--	--	--	--	--	--	--	--	--	--	--	--	--
Version	1p	1f	--	--	--	--	--	--	--	--	--	--	--	--	--
Other	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Current filtering applied:
Test Severities: - *Show All* -
Datasource Severities: - *Show All* -
Scores: - *Show All* -
Types: - *Show All* -

Assessment Test Results

Showing 50 of 50 results (0 filtered)

Test / Datasource	Result
DB2 Communication Protocol SSL Test category: Conf. Severity: Critical Test ID: 2647 This test checks to ensure that the DB2 registry variable DB2COMM is set to SSL. DB2 must use NSA-approved cryptography to protect classified information in accordance with the data owners requirements. Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data. The application must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated. STIG Reference: DB2X-00-008600, DB2X-00-009100, DB2X-00-009200 STIG Severity: CAT I STIG Srg: SRG-APP-000416-DB-000380, SRG-APP-000441-DB-000378, SRG-APP-000442-DB-000379 osprey_db2inst1 Datasource type: DB2 Severity: None	Fail The DB2 communication protocol is not configured as recommended. Add test exception **Recommendation:** *We recommend setting the DB2 registry variable DB2COMM to SSL so that the instance is strictly compliant with NIST SP 800-131A. You can run the following command to set the registry variable DB2COMM, then restart the DB2 instance: db2set DB2COMM=SSL*

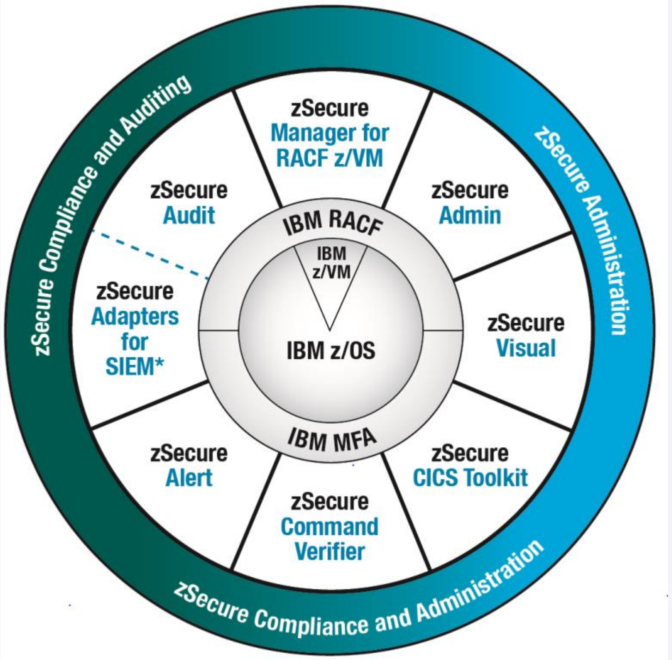
zSecure Alert, Audit & Adapters for SIEM

zSecure Suite Components for Compliance, Audit & SIEM connectivity

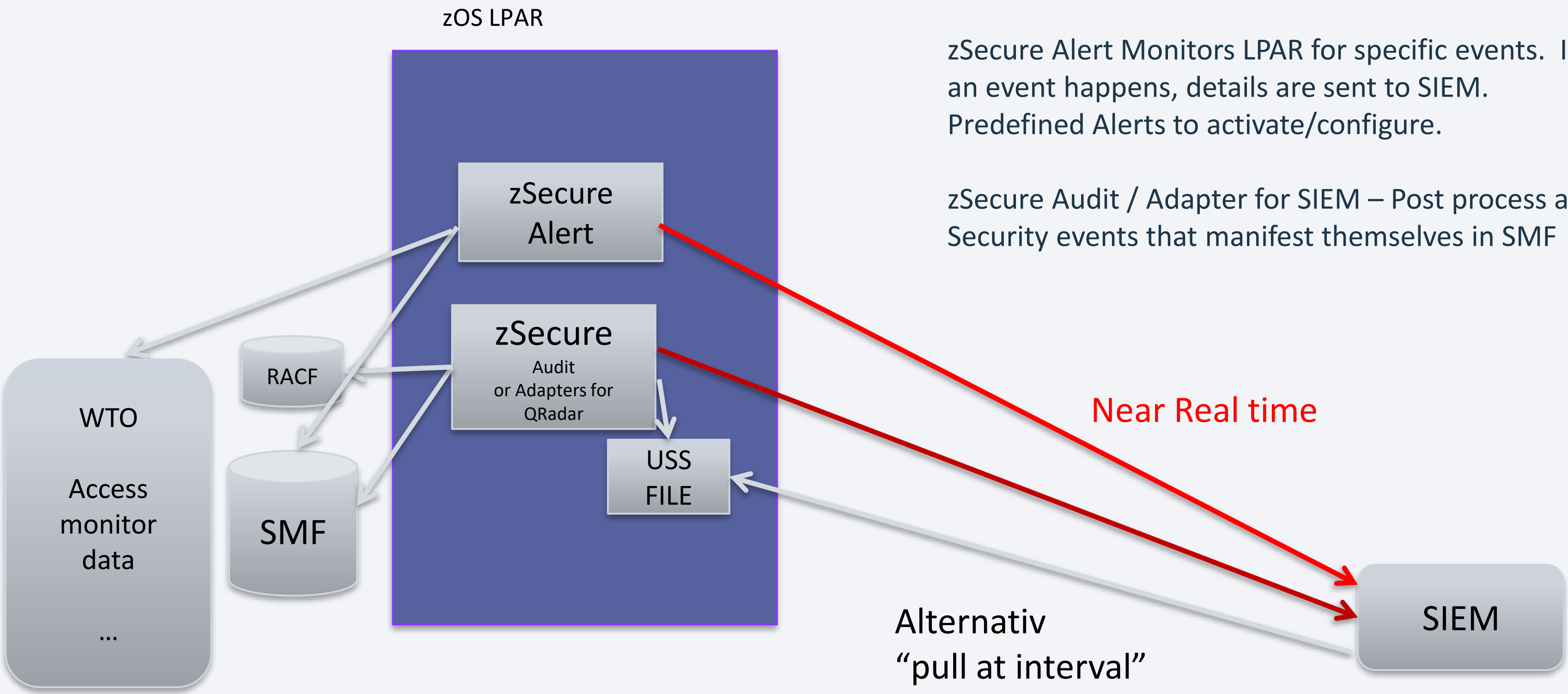
zSecure Audit
Vulnerability analysis for the mainframe infrastructure; automatically analyze and report on security events and monitor compliance

zSecure Adapters for SIEM
Collects, formats and sends enriched mainframe System Management Facility (SMF) audit records to SIEM solutions

zSecure Alert
Real-time mainframe threat monitoring of intruders and alerting to identify misconfigurations that could hamper compliance



zSecure Alert & Audit / SIEMs



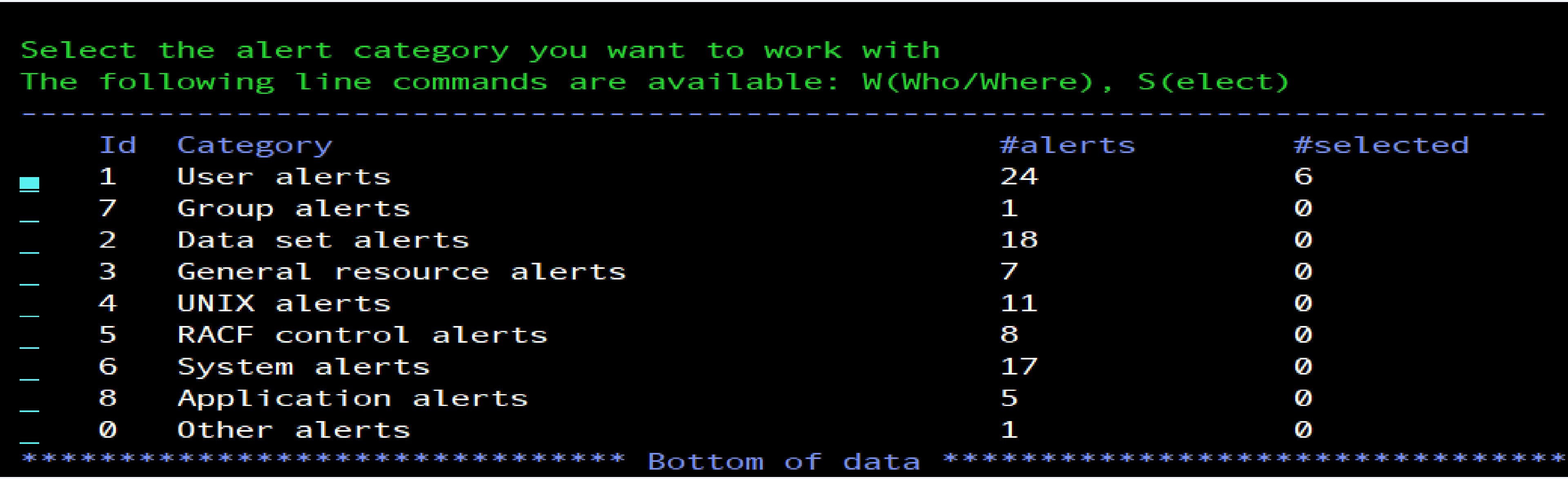
zSecure Alert Monitors LPAR for specific events. If an event happens, details are sent to SIEM. Predefined Alerts to activate/configure.

zSecure Audit / Adapter for SIEM – Post process all Security events that manifest themselves in SMF

zSecure Alert

STC with ISPF based administration

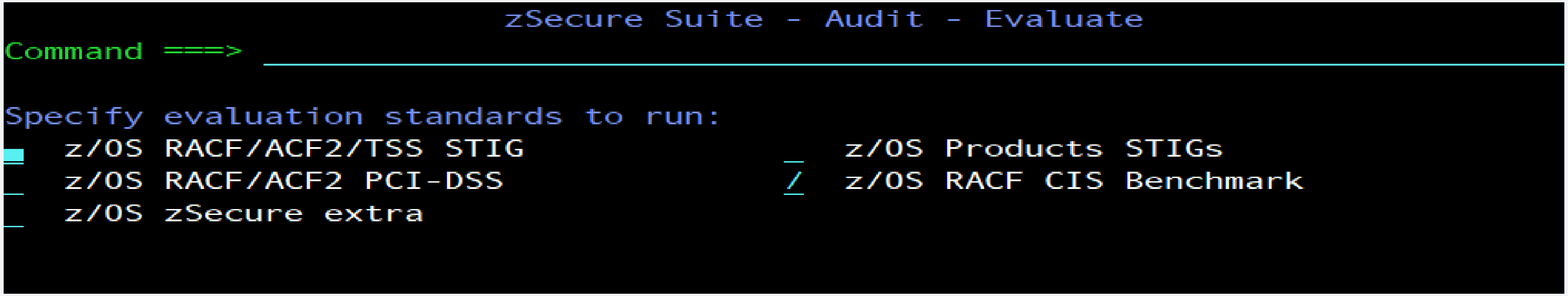
- **predefined AlertS that can be selected / activated**
- **user defined Alerts can be implemented**



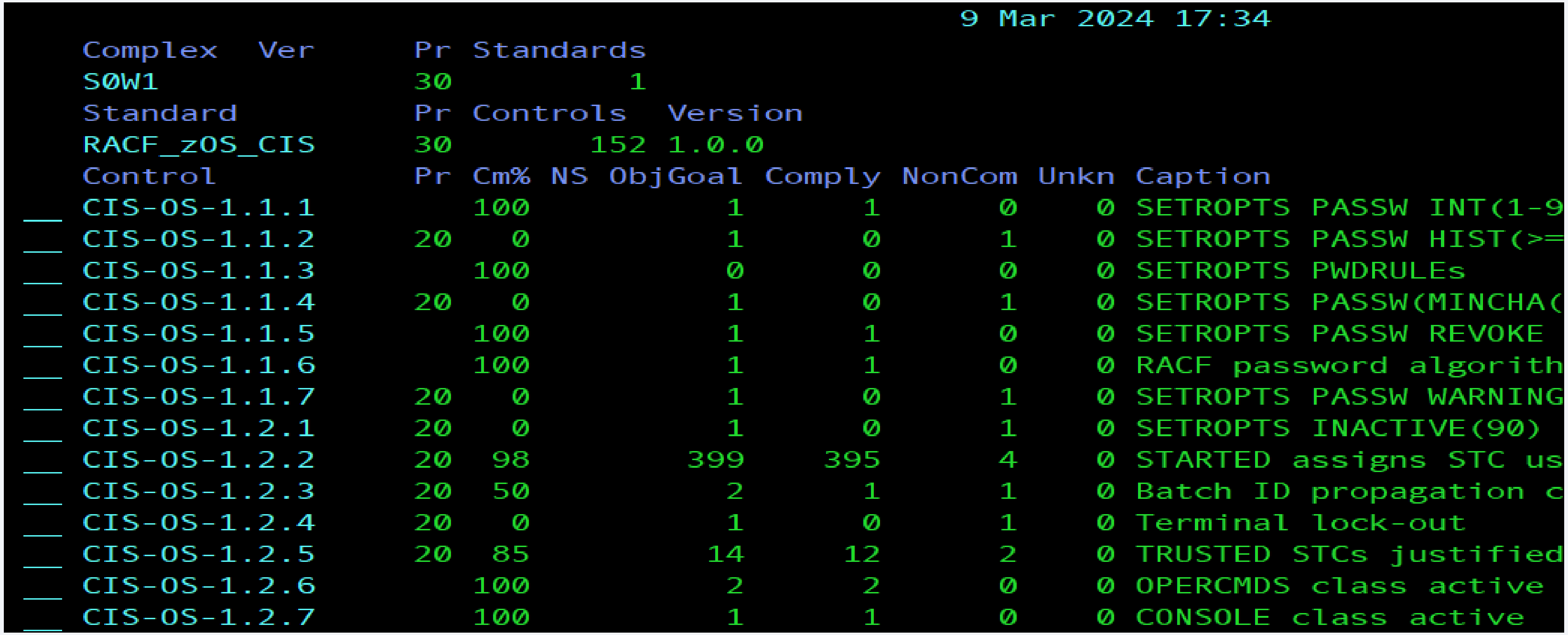
```
Select the alert category you want to work with
The following line commands are available: W(Who/Where), S(elect)
-------------------------------------------------------------------------------
    Id  Category                                   #alerts        #selected
_   1   User alerts                                24             6
_   7   Group alerts                               1              0
_   2   Data set alerts                            18             0
_   3   General resource alerts                    7              0
_   4   UNIX alerts                                11             0
_   5   RACF control alerts                        8              0
_   6   System alerts                              17             0
_   8   Application alerts                         5              0
_   0   Other alerts                               1              0
******************************** Bottom of data ********************************
```

zSecure Audit Compliance Framework

ISPF dialog based validation of various compliance standards (profiles)



```
                         zSecure Suite - Audit - Evaluate
Command ===>

Specify evaluation standards to run:
_  z/OS RACF/ACF2/TSS STIG             _  z/OS Products STIGs
_  z/OS RACF/ACF2 PCI-DSS              /  z/OS RACF CIS Benchmark
_  z/OS zSecure extra
```



```
                                                9 Mar 2024 17:34
   Complex  Ver     Pr Standards
   S0W1             30         1
   Standard         Pr Controls  Version
   RACF_zOS_CIS     30      152 1.0.0
   Control          Pr Cm% NS ObjGoal Comply NonCom Unkn Caption
__ CIS-OS-1.1.1        100          1      1      0    0 SETROPTS PASSW INT(1-9
__ CIS-OS-1.1.2     20   0          1      0      1    0 SETROPTS PASSW HIST(>=
__ CIS-OS-1.1.3        100          0      0      0    0 SETROPTS PWDRULEs
__ CIS-OS-1.1.4     20   0          1      0      1    0 SETROPTS PASSW(MINCHA(
__ CIS-OS-1.1.5        100          1      1      0    0 SETROPTS PASSW REVOKE
__ CIS-OS-1.1.6        100          1      1      0    0 RACF password algorith
__ CIS-OS-1.1.7     20   0          1      0      1    0 SETROPTS PASSW WARNING
__ CIS-OS-1.2.1     20   0          1      0      1    0 SETROPTS INACTIVE(90)
__ CIS-OS-1.2.2     20  98        399    395      4    0 STARTED assigns STC us
__ CIS-OS-1.2.3     20  50          2      1      1    0 Batch ID propagation c
__ CIS-OS-1.2.4     20   0          1      0      1    0 Terminal lock-out
__ CIS-OS-1.2.5     20  85         14     12      2    0 TRUSTED STCs justified
__ CIS-OS-1.2.6        100          2      2      0    0 OPERCMDS class active
__ CIS-OS-1.2.7        100          1      1      0    0 CONSOLE class active
```

IBM Z Security and Compliance Center (zSCC)

IBM Z Security and Compliance Center

Designed for users with multiple skill levels, these solutions can automate evidence collection of compliance-related facts from IBM Z platforms.

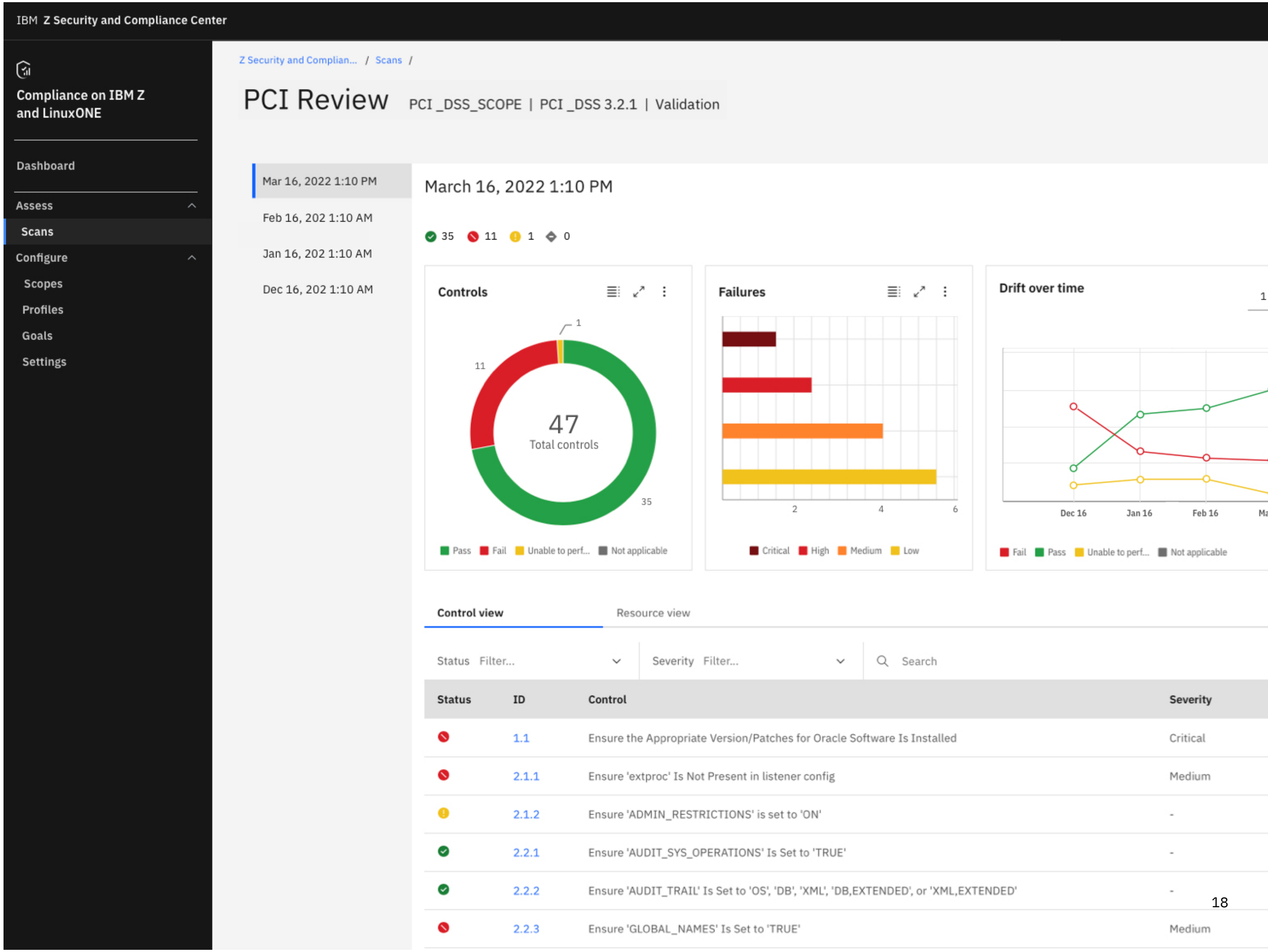
Compliance validation for z/OS and zLinux

The zSCC License
includes zSecure Audit license

Multiple profiles are available :
e.g. PCI, DISA-STIG & **DORA**

CIS benchmark for Db2 will be available soon

Implemented on zCX, OCP or zLinux



IBM Z Security and Compliance Center
Compliance on IBM Z and LinuxONE
Dashboard
Assess
Scans
Configure
Scopes
Profiles
Goals
Settings
Z Security and Complian... / Scans /

PCI Review PCI _DSS_SCOPE | PCI _DSS 3.2.1 | Validation

Mar 16, 2022 1:10 PM
Feb 16, 202 1:10 AM
Jan 16, 202 1:10 AM
Dec 16, 202 1:10 AM

March 16, 2022 1:10 PM

✓ 35 ⊘ 11 ! 1 ◆ 0

Controls
1
11
47
Total controls
35
🟩 Pass 🟥 Fail 🟨 Unable to perf... ⬛ Not applicable
Failures
2
4
6
⬛ Critical 🟥 High 🟧 Medium 🟨 Low
Drift over time
1
Dec 16
Jan 16
Feb 16
Ma
🟥 Fail 🟩 Pass 🟨 Unable to perf... ⬛ Not applicable
Control view
Resource view
Status Filter...
Severity Filter...
Search

Status	ID	Control	Severity
⊘	1.1	Ensure the Appropriate Version/Patches for Oracle Software Is Installed	Critical
⊘	2.1.1	Ensure 'extproc' Is Not Present in listener config	Medium
!	2.1.2	Ensure 'ADMIN_RESTRICTIONS' is set to 'ON'	-
✓	2.2.1	Ensure 'AUDIT_SYS_OPERATIONS' Is Set to 'TRUE'	-
✓	2.2.2	Ensure 'AUDIT_TRAIL' Is Set to 'OS', 'DB', 'XML', 'DB,EXTENDED', or 'XML,EXTENDED'	-
⊘	2.2.3	Ensure 'GLOBAL_NAMES' Is Set to 'TRUE'	Medium

Want an extended Demo and discussion of use cases ?

→ weberg@de.ibm.com

IBM **Security**

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- ibm.com/security/community
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM