IBM Security zSecure
IBM MFA for z/OS

Rob van Hoboken – zSecure Architect - Rob.vanHoboken@nl.ibm.com

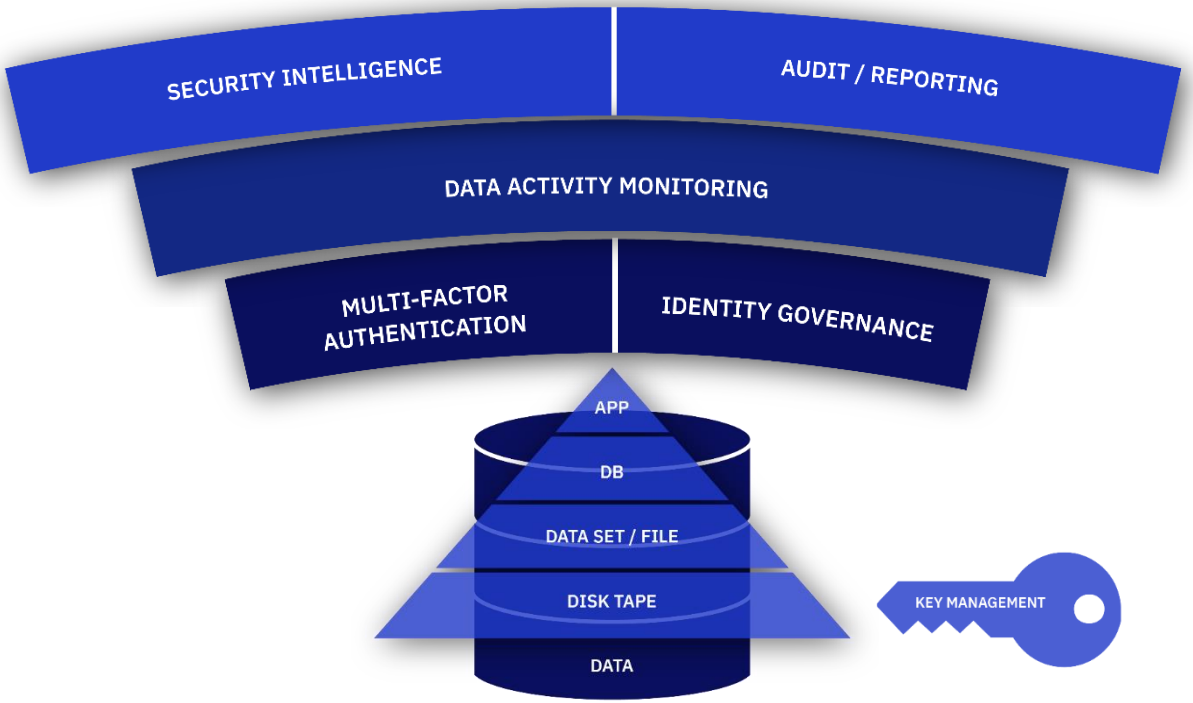
Mike Zagorski – WW Offering Manager – Zagorski@us.ibm.com

IBM

November 2018

Session FK

Protecting Data at the Core of the Enterprise



Relevant IBM Security Solutions:

- Enterprise Key Management Foundation
- IBM Multi-Factor Authentication for z/OS
- IBM Security Identity Governance
- IBM Security Guardium Family
- IBM Security zSecure Suite
- IBM Security QRadar

Encryption is the solid foundation of a layered cybersecurity strategy

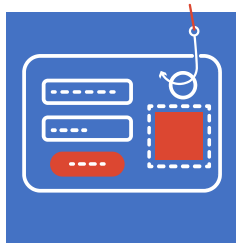
Why is a Multi-Factor Authentication solution needed?

Current Security Landscape

1,935

Number of security incidents in 2015 with confirmed data disclosure as a result of stolen credentials.[1]

(506 worse than prior year)



81%

Number of breaches due to stolen and/or weak passwords.[1]

(18% worse than prior year)

$4 million

The average total cost of a data breach.[2]

60%

Number of security incidents that are from insider threats. [3]

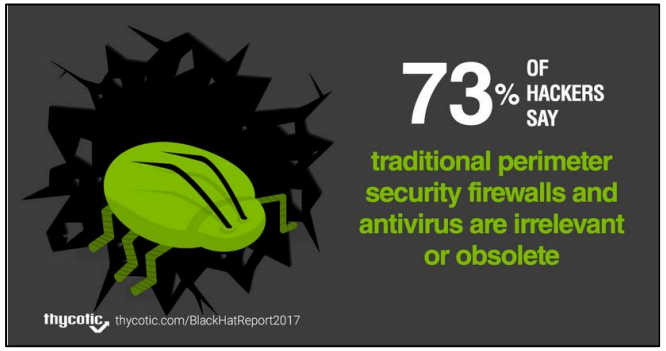
Criminals are identifying key employees at organizations and exploiting them with savvy phishing attacks to gain initial access to the employees' system and steal their account credentials. This puts emphasis on the need for tighter restrictions on access privileges to key data repositories.[1]

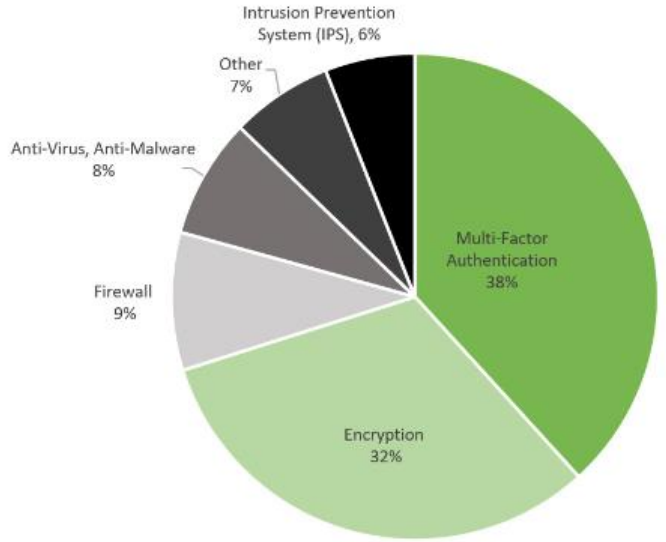
[1] 2017 Verizon Data Breach Investigations Report
[2] Ponemon: 2016 Cost of Data Breach Study: Global Analysis
[3] IBM X-Force 2016 Cyber Security Intelligence Index

Black Hat 2017 Survey[1]

QUESTION: What type of security is the hardest to get past?

68% say multi-factor authentication and encryption are biggest hacker obstacles





[1] thycotic Black Hat 2017 Hacker Survey Report
https://thycotic.com/resources/black-hat-2017-survey/

Compliance

PCI DSS v3.2

8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.

8.3.1 Incorporate multi-factor authentication for all non-console access into the Cardholder Data Environment (CDE) for personnel with administrative access.

Note: This is a best practice until January 31, 2018, after which it became a requirement.

NIST SP 800-171

3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

Note: Network access is any access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).

Note: This requirement is effective December 31, 2017.

Using multi-factor authentication on IBM Z is considered a security ***Best Practice***.

How are users authentication without MFA?

Users authenticate with:

- Passwords
- Password phrases
- Digital Certificates
- via Kerberos

Problems with passwords:

- Common passwords
- Employees are selling their passwords
- Password reuse
- People write down passwords
- Malware
- Key log
- Password cracking

History of Authentication

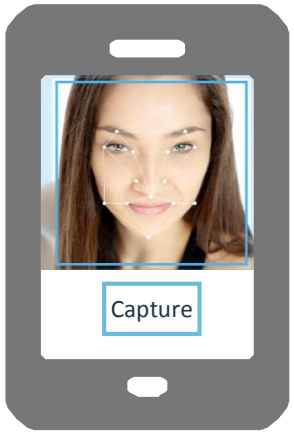
- **1976:** User identification/verification
- **1981:** Password processing support
- **1984:** DES password encryption option
- **1994:** DES as password default
- **1999:** PROTECTED user IDs
- **2004:** Password enveloping and LDAP change log support
- **2005:** Mixed case passwords and Detect or prevent password recycling
- **2006:** Password phrases from 14 to 100 characters in length
- **2007:** Password phrases from 9 to 13 characters in length
- **2008:** Password phrase exploitation and more granularity on password reset
- **2013:** RACF_ENCRYPTION_ALGORITHM health check (Rolled back)
- **2014:** KDFAES password support, Additional special characters, Password phrase only users
- **2015:** Elimination of the need for an ICHDEX01 exit to eliminate the RACF masking algorithm, ADDUSER will no longer assign a default password, RACLINK support of password phrases
- **2016:** Multi-factor Authentication

What is multi-factor authentication?

SOMETHING THAT YOU KNOW
- Usernames and passwords
- PIN Code

SOMETHING THAT YOU HAVE
- ID Badge
- One time passwords
  - Time-based

SOMETHING THAT YOU ARE
- Biometrics



Authentication Systems

In-Band

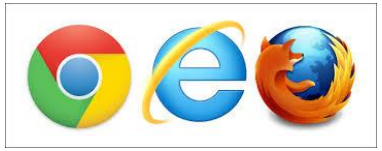
Proprietary Protocol: RSA

RADIUS Based Factors: yubico, Microsoft Azure, gemalto security to be free, DUO, RSA, ONE IDENTITY, Symantec. VIP, okta, VASCO TRUST FOR THE DIGITAL WORLD

TOTP Support: IBM, Google, FreeOTP Open Authentication, DUO Mobile, AUTHY, RAPIDIDENTITY™ OTP with RapidIdentity Mobile App

Out-of-Band

Certificate Authentication:



Password/Passphrase: RACF Password/Passphrase can be used in conjunction with all in-band authentication methods.

Disclaimer: Not everything above has been fully tested, but they *should* work, if not we will investigate.

**Not an all-inclusive list

Who should be protected?

Simple Answer: Everyone with access to the mainframe

System Administrator with access to sensitive data sets

RACF Administrator who controls system-wide authorization

Database Administrator with access to critical data

Law Clerk with access to corporate IP

Financial Analyst with access financial data prior to being made public

Executive with access to corporate strategy

Engineer who is developing the next product breakthrough

Loan Officer who can transfer $10 million dollars

Anyone with access to data that you don't want released to the public!!

User Provisioning with RACF

- **Activate the MFADEF class:**

```
SETR CLASSACT(MFADEF)
```

  - MFADEF Class must be active for MFA authentication processing to occur

- **Define the factor profile:**

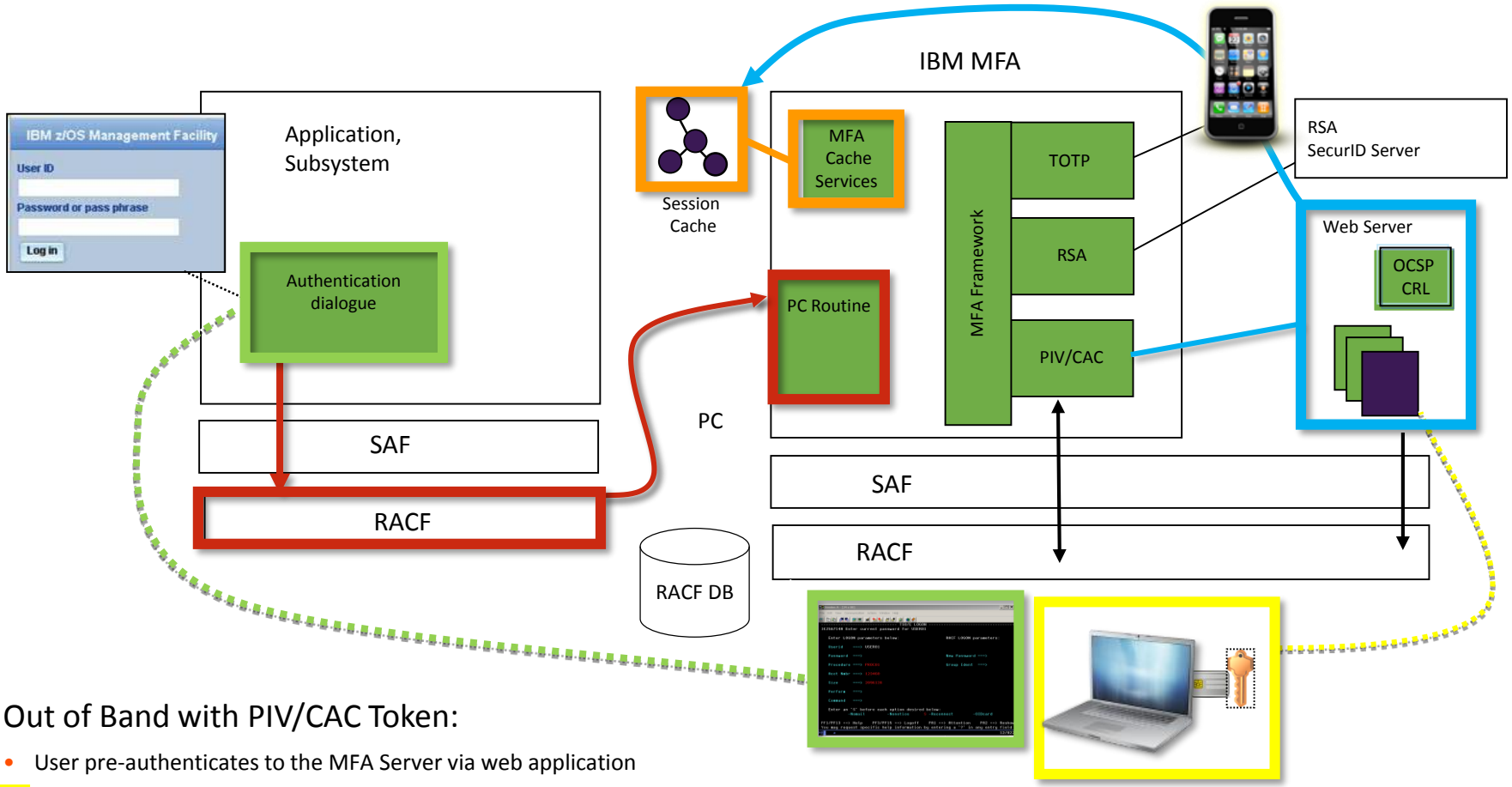
```
RDEFINE MFADEF FACTOR.AZFSIDP1
```

- **Add the factor to a RACF user:**

```
ALU JOEUSER MFA(FACTOR(AZFSIDP1) ACTIVE TAGS(SIDUSERID:JOE1)
```

  - Adds factor to the user
  - Activates the factor – JOEUSER is now required to authenticate to RACF with MFA credentials
  - Adds a factor specific tag – SIDUSERID – Associates RSA SecurID user ID with z/OS user ID

- **User is provisioned:**
  - JOEUSER must now authenticate to RACF with an RSA SecurID token and PIN



Out of Band with PIV/CAC Token:

- User pre-authenticates to the MFA Server via web application
  - Leverages web browser support for PKCS#11 HW tokens
  - User enters PIN to unlock the smart card, TLS session with client authentication used to prove knowledge of the private key
  - User authenticates to the Web application and passes to MFA authenticated client cert. MFA matches cert components in the User profile and if valid and generates a Cache Token Credential (CTC) and returns to the web application. The CTC is displayed on the user's browser window
- User enters CTC in the password field on the application authentication dialogue
- Application calls RACF to evaluate the user's credentials, and in turn calls IBM MFA
- MFA checks the session cache to ensure that the user had pre-authenticated and evaluates the CTC. If valid, MFA returns to RACF and logon processing continues

What if something doesn't work?

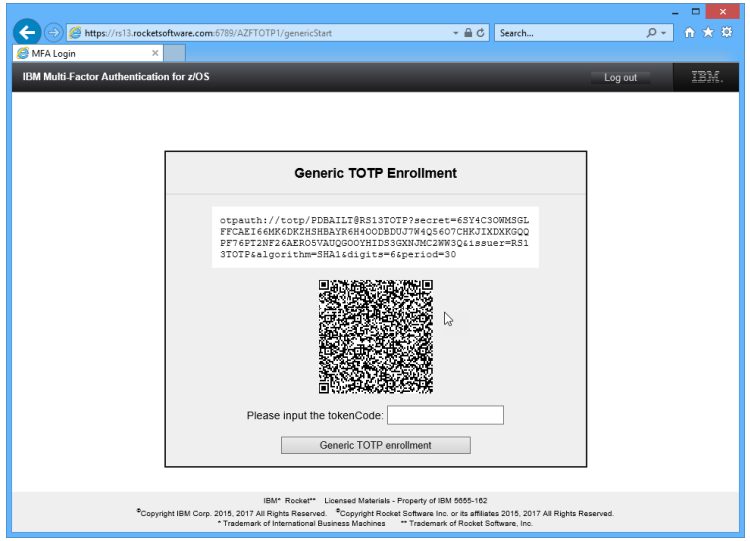
Some applications have authentication properties which can prevent MFA from working properly:

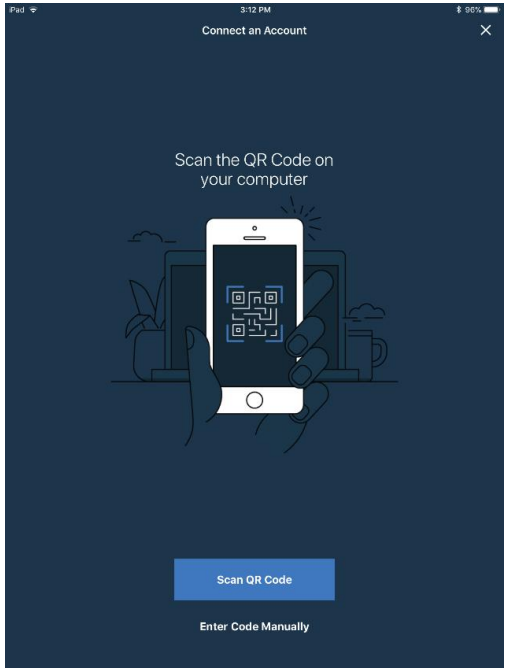
- **No phrase support** – Some MFA credentials are longer than 8 characters
- **Replay of passwords** – Some MFA credentials are different at every logon and can't be replayed

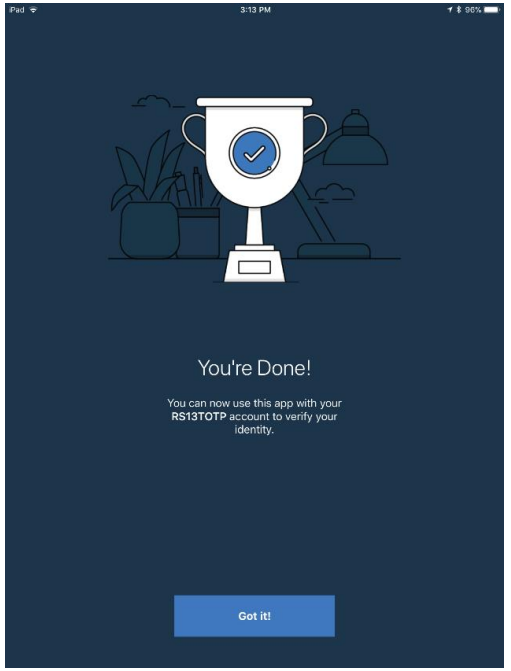
1. Selective Application Exclusion
   - Exempting MFA processing for certain applications:
     - Allows a Security Administrator to mark certain applications as excluded from MFA
     - Allows a user to logon to that application using their non-MFA credentials
2. PassTicket Support
   - Allows the Security Administrator to indicate that an MFA user can authenticate with a PassTicket instead of an ACTIVE MFA factor. New special MFA PassTicket Factor
3. Out-of-Band Support
   - Allows users to authenticate with multiple factors directly to IBM MFA and receive a logon token
   - The pre-authentication logon tokens behavior can be customized as needed
     - Controls to allow tokens to be single use or re-useable and how long a token is valid

IBM MFA for z/OS was architected with this in mind and provides a variety of accommodation mechanisms.

Example – Provisioning Step w/ IBM Verify





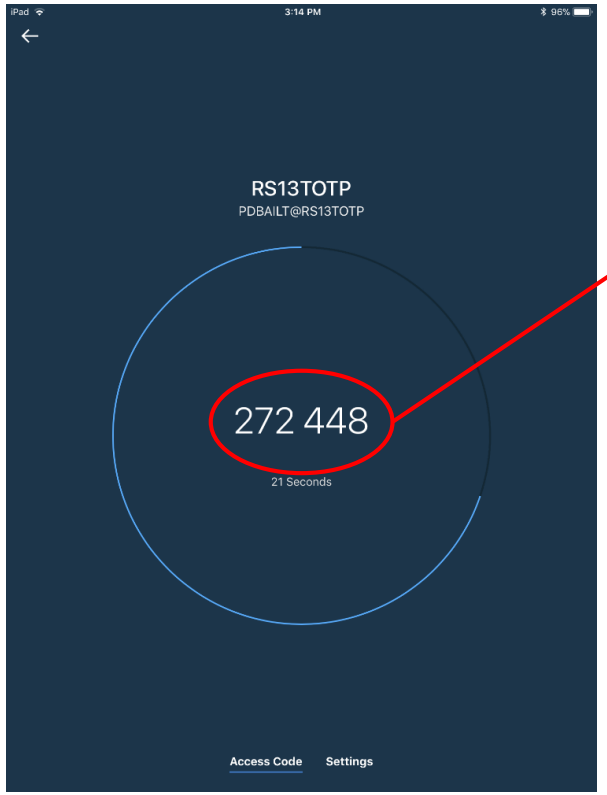


1. User will receive a link to the MFA Webserver which will have a QR code.

2. User scans QR Code

3. Device is provisioned

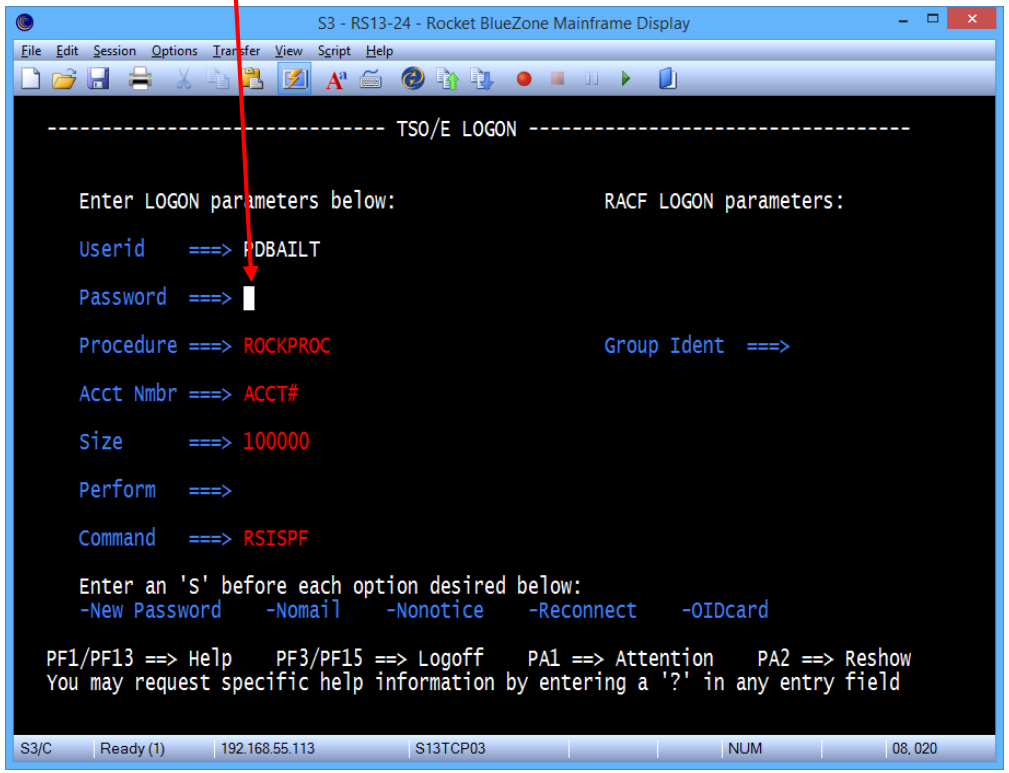
Example – User log in w/ IBM Verify



Password: passw0rd

272448

272448:passw0rd



- User authenticates with compound in-band by entering:
  - The IBM Verify token code (or other TOTP App)
  - A colon (configurable separator character)
  - Their RACF password / password phrase
- All together in the password phrase field

The latest in IBM MFA for z/OS

Remote Authentication Dial-In User Service (RADIUS) based factor support

- Generic RADIUS factor that enables inter-operability with generic RADIUS servers
- SafeNet RADIUS factor that is designed to operate with Gemalto SafeNet Authentication Service servers

High Availability MFA Web Services

- IBM MFA now supports running multiple instances of the MFA Web Services started task in a Sysplex. Thus if an LPAR running MFA Web Services has to be re-IPL'ed or is otherwise out of service for planned maintenance, users can continue to pre-authenticate with MFA web services on one of the remaining instances running within the Sysplex.

Compound In-band Authentication support

- Ability to authenticate with both a token code and a RACF password, enabled per MFA factor (AZFSIDP1, AZFTOTP1, AZFRADP1, AZFSFNP1)

Express Logon Facility (ELF) support

- New integration has been provided, through a new SAF API, that enables ELF users to interface with the IBM MFA smart card support.
- This enhancement requires the presence of a user's smart card when authenticating and prevents RACF user ID-only authentication attempts

Generic TOTP

- The time-based, one-time password factor has been enhanced to support more generic TOTP token applications.
- This introduces support for standard-compliant TOTP third-party applications that run on Android devices.

Bulk provisioning

- Scripts that enable a large number of users to be easily provisioned.
- In particular, this simplifies provisioning PIV/CAC users who can be provisioned and enabled immediately, eliminating the self-service provisioning step.

Strict PCI Compliance

- Ability to configure IBM MFA to operate in a strict PCI-compliant mode. When this mode is activated, messages that "leak" information are not returned.
- The out-of-band pre-authentication process always requires entry of all factor credential data before returning any information about the pre-authentication attempt.

zSecure Update

A comprehensive suite of products

zSecure Audit

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

zSecure Adapters for SIEM

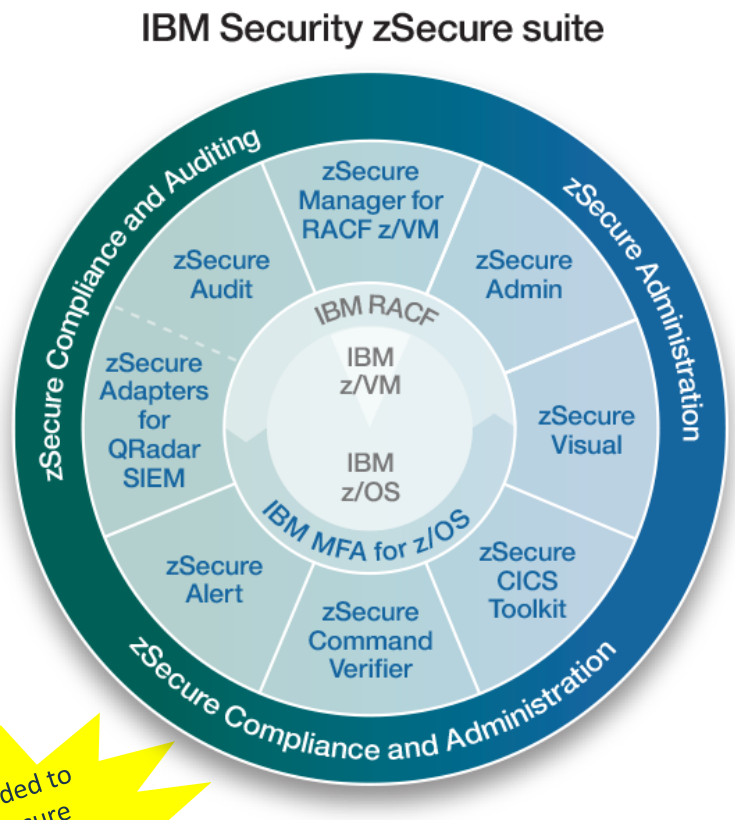
Collects, formats and sends enriched mainframe System Management Facility (SMF) audit records to IBM Security QRadar SIEM

zSecure Alert

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

zSecure Command Verifier

Policy enforcement solution that helps enforce compliance to company and regulatory policies by preventing erroneous commands



Added to zSecure offering list

MFA for z/OS

Multifactor, strong authentication to prevent hacking and improve privileged user controls with RACF integration for easy administration

zSecure Manager for RACF z/VM

Combined audit and administration for RACF in the VM environment including auditing Linux on System z

zSecure Admin

Enables more efficient and effective RACF administration, identity governance, tracking and statistics using significantly fewer resources

zSecure Visual

Helps reduce the need for scarce, RACF-trained expertise through a Microsoft Windows–based GUI for RACF administration

zSecure CICS Toolkit

Provides access RACF command and APIs from a CICS environment, allowing additional administrative flexibility

Note:

- zSecure Audit also available for ACF2™ and Top Secret®
- zSecure Adapters for QRadar SIEM is a capability of zSecure Audit and also available for ACF2™ and Top Secret®
- zSecure Alert also available for ACF2™

IBM MFA Support in zSecure

zSecure Admin and Audit

- Selection and display of MFA fields in RACF profiles. Extra fields and formatting added for easier display.
- Selection and display of new relocate section and MFA information in SMF records.
- New field available in SYSTEM report about presence of RACF MFA support.

zSecure Access Monitor

- Detection and reporting of use of MFA for every RACINIT, including TSO logon.

zSecure Command Verifier

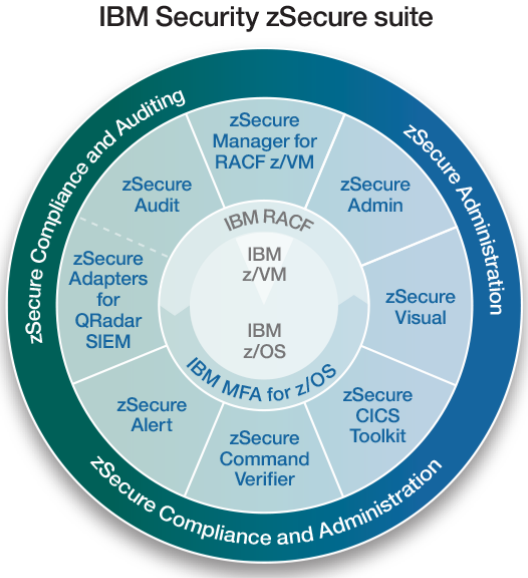
- Support for parsing new command syntax.
- New Policy Profiles to control management of MFA information, and updates to command recording in Command Audit Trail.

zSecure Adapters for SIEM

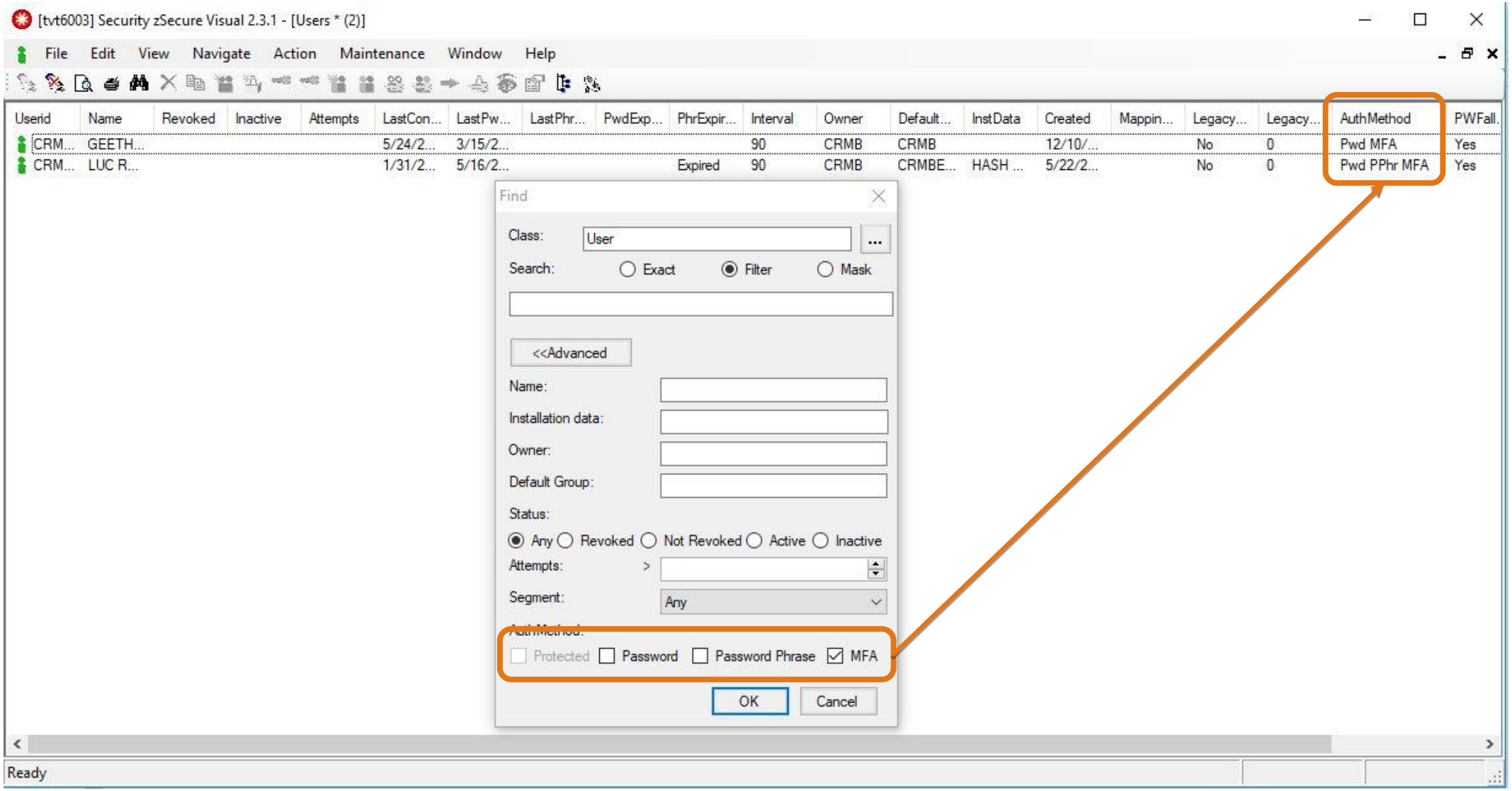
- Include MFA information to QRadar for analytics

zSecure Visual

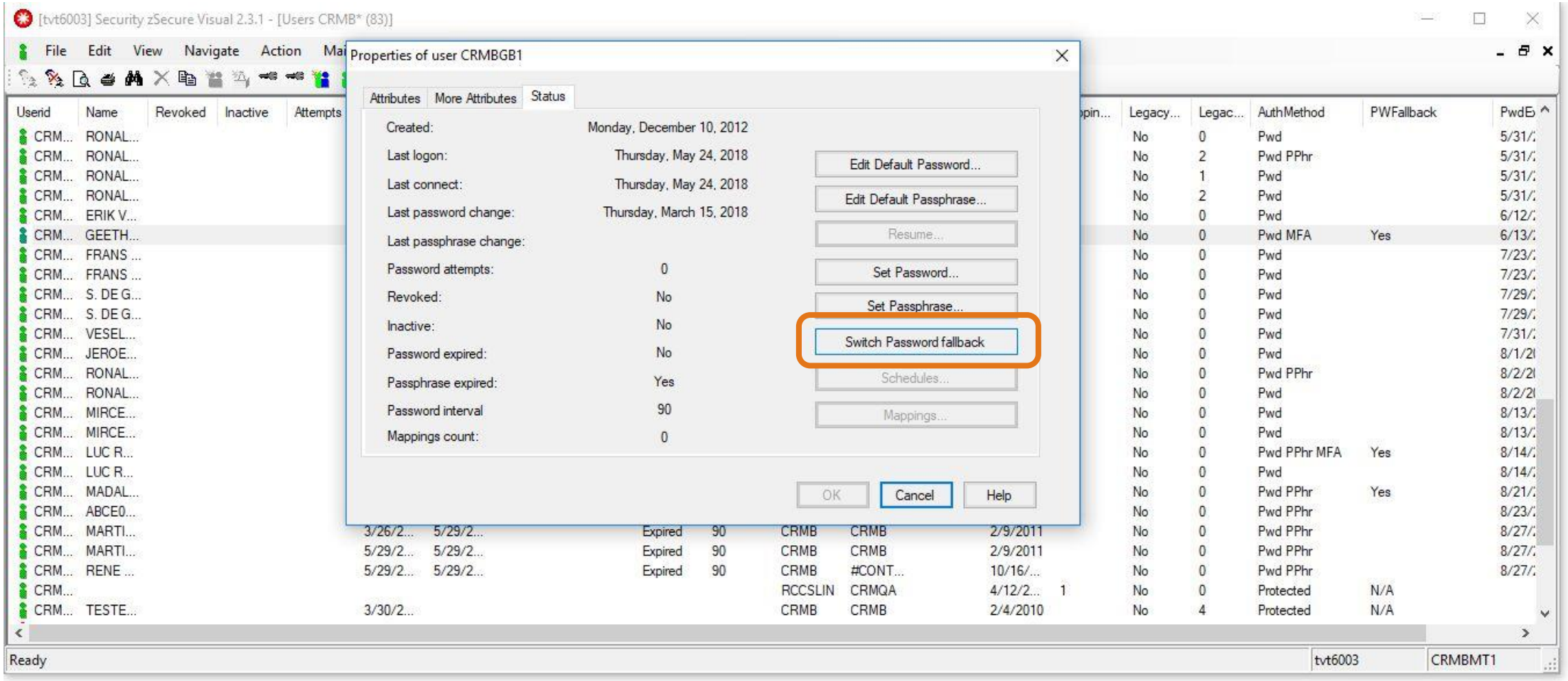
- User context menu extensions for MFA factors and policies; MFPOLICY edit



zSecure Visual – Easy selection on authentication method MFA



zSecure Visual – Switch password fallback – from Properties menu



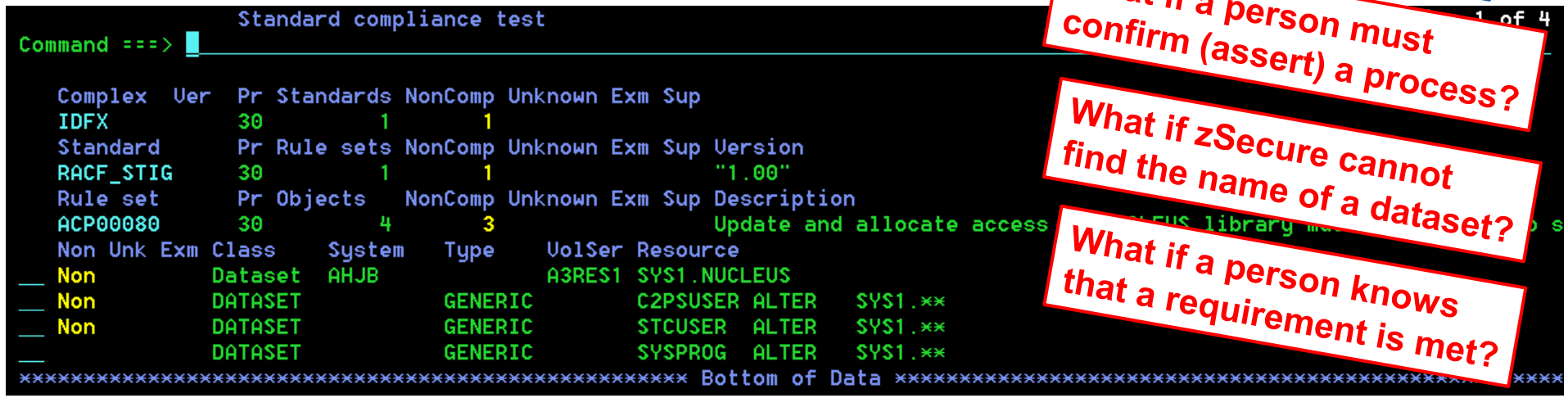
zSecure 2.3.1

- Compliance framework: manual entry of compliance status
  - Assertions
  - Configuration
  - Overrides
- Enhanced STIG support
- (more) z/OS 2.3 Encryption support
- SIEM support without logstreams
- Full audit trail to ArcSight
- KDF-AES password verification
- (more) support for INFOSTOR records in ACF2
  - OMVS, CICS, SAFDEF
- System currency

Existing compliance framework

- Example:

  RACF STIG ACP00080: UPDATE and higher access to SYS1.NUCLEUS must be restricted to systems programmers



Automated checks
Examine the system, and flag it as compliant or non-compliant

What if a person must confirm (assert) a process?

What if zSecure cannot find the name of a dataset?

What if a person knows that a requirement is met?

Support for assertions

- Three types of assertions:
  - Full assertions
    - Automation is fundamentally not possible
    - Users manually confirm (i.e., *assert*) that a requirement is met
    - Example: the ACP audit logs must be reviewed on a regular basis
  - Automations that require configuration info
    - Users provide details about system configuration
    - Checks are performed automatically
    - Example: protection of installation data sets
  - Overrides
    - Users override result produced by zSecure

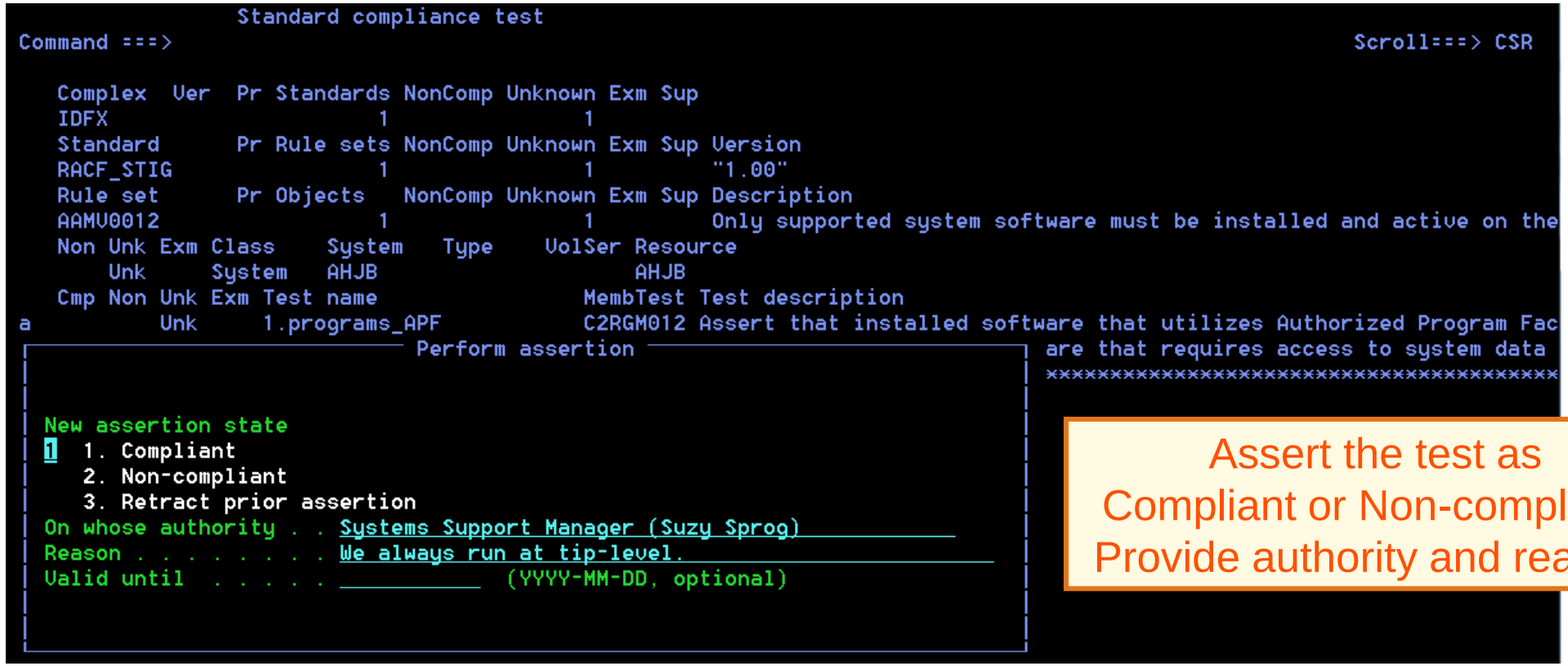
Support for assertions (2)

- Assertions are stored in ASSERT data sets
  - Allocated ASSERT data sets are used during
    - compliance evaluation (using existing COMPLIANCE newlist)
    - new history report (using new ASSERT newlist)
    - new configuration report (using new STANDARD newlist)
  - New assertions are added to a new or existing ASSERT data set
- There can be multiple ASSERT data sets, for example
  - System level
  - User level
- ASSERT data sets can be created automatically

Assertions in action: add a full assertion

- Example:

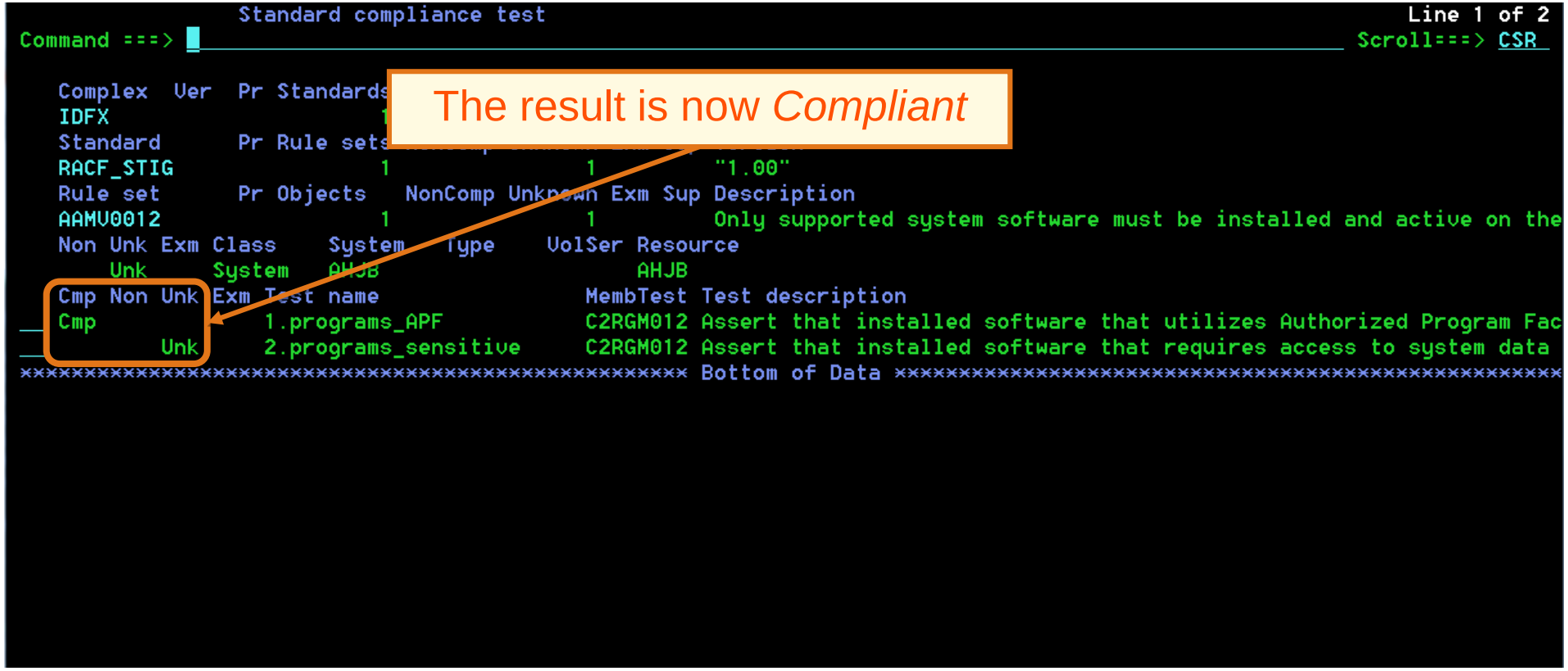
  STIG rule AAMV012: Only supported system software must be installed and active on the system.



Assert the test as Compliant or Non-compliant. Provide authority and reason.

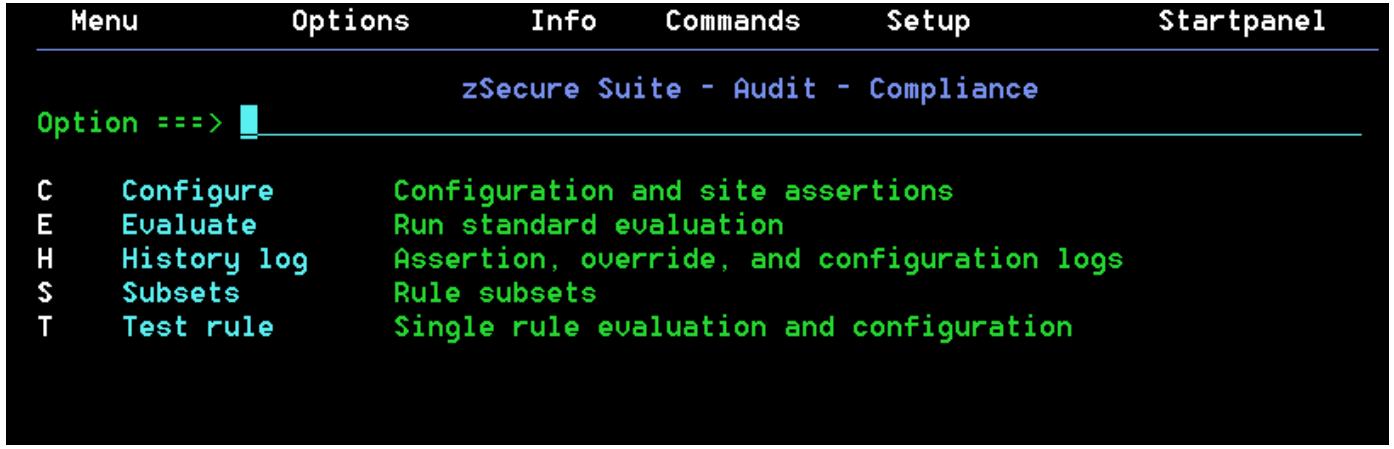
Assertions in action: add a full assertion

- Rerun the report:



Compliance framework: ISPF User Interface

- Complete redesign



- Options E and S are compliance evaluation runs, with actionable reports
- Options C and H are specific for assertions (Full Assertion, Override, Configuration)
- Option T is everything for a single rule member

Pervasive Encryption in z/OS

Support added in zSecure Audit 2.3.1:

- Data sets on disk (VSAM, QSAM, BSAM) can be transparently encrypted
  - HSM migrated data sets also covered (if HSM applies encryption)
- zFS files and information can be transparently encrypted
- DB2 use of key labels for tables and table spaces
- Data in the Coupling Facility can be transparently encrypted
  - CF structure information, RACF profile look-up and encryption status
- Communication Server links can be transparently encrypted
  - Formatting of SMF 119-12 added

Near Real-Time feed for QRadar and other SIEMs

- Enable SIEM Near Real-Time feed for sites that have no SMF logstream implemented
  - New address space CKQEXSMF
  - Similar to C2POLICE
  - New option in CKQRADAR parmmember CKQSPECL:
    ```
    alloc type=SMF ddname=smf0rec getproc=ckqio2pc
    ```
- Shares SMF intercept exits with C2POLICE
- CKQEXSMF address space must be running before starting CKQRADAR
  - Uses similar buffering technique as C2POLICE, maximum of 32 GiB.
  - Data retrieved from start of CKQEXSMF
  - Restart point maintained per retrieving JOBNAME

QRadar and other SIEM NRT support

- Near Real-Time benefits
  - Easier integration and management of SMF data
    - No intermediate storage required
  - Easier handling of time-of-events in QRadar
  - Earlier detection of anomaly
- Now with CKQEXSMF support, no need for INMEM and LOGSTREAMs
- Log Event Enhanced Format (LEEF) consumed by
  - Qradar
  - Splunk
  - others

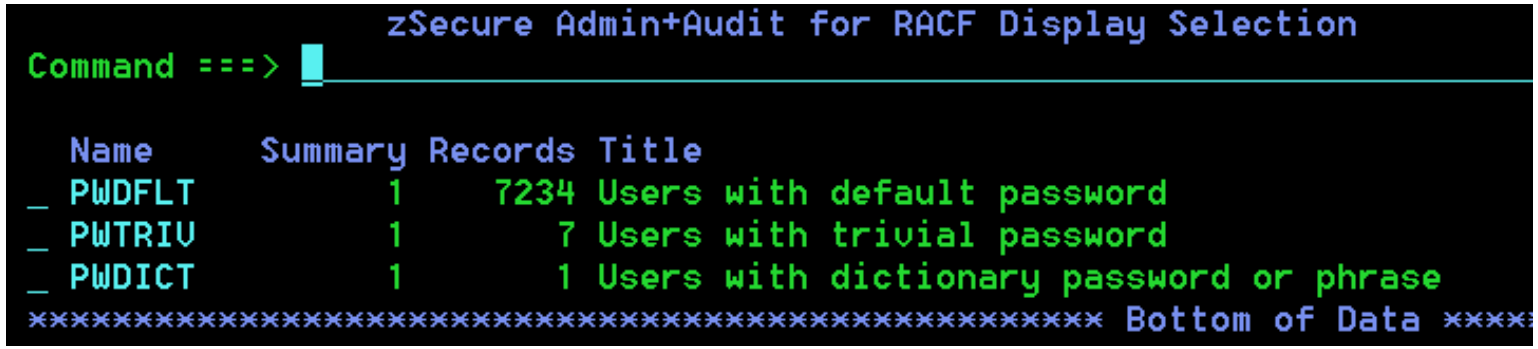
(Full) Audit trail in ArcSight CEF format

- 2.3.0 added CEF support in C2POLICE
- 2.3.1 adds CKQCEF procedure, similar to CKQRADAR
  - Dedicated data conversion and configuration files
    - Members start with CQKCEF
  - Preferred method is to use either INMEM or CKQEXSMF for near real-time data
  - Possible to use batch process and manual data transfer (Sample job CKQCEFJD)
    - Control information can be specified via `//CKQPARM DD *`
    - Options:
      - use high water mark
      - write CEF messages to `//C2RSYSLG DD`
- New started task CKQCEF for near real-time support
  - Can use TCP or UDP for data transfer

Verify Password (and Phrase) when KDF-AES active

- VERIFY PASSWORD directly on the ACTIVE RACF database
  - Requires APF authorization (for example, running CKRCARLX in batch)
  - Requires READ access to `CKR.VERIFY.PASSWORD`
  - Long running task (KDF-AES is designed to take more resources)
  - Allows running on a subset of users (CKAPWUSR)
  - Allows running against a dictionary (CKAPWDCT)
    - Dictionary has maximum size of 500 words/phrases
    - Dictionary has minimum size of 50 different words/phrases
      - Minimum dictionary size not enforced for user with CONTROL access
  - Result of verify is stored in RACF database

- Reporting of results via AU.S – Users:



ACF2 support

- INFOSTOR records
  - USER and GROUP profiles with OMVS information
  - CICS records with SAFELIST, PROTLIST and region options
  - SAFDEF overrides
- UNIX (OMVS) fields in LID and audit panels and reports
- Installation defined fields in LID panels and reports
- TRUSTED reports show many more ACF2 privileges

CARLa improvements

- SIMULATE supports generic specification of dsname / resource
  - SIMULATE SENSITIVE *access* DATASET *dsn*
  - SIMULATE CLASS=DATASET SENSITIVITY=Site*name*… RESOURCE=*dsn*
  - … SENSITIVITY=GDPR-data RESOURCE=(BANKING.REPORTS.**, BANKING.CUSTDATA.**)
- SMF field **action** with value for more SMF record types, for example:

Type	Short Description	Action
14	INPUT or RDBACK Data Set Activity	input
15	OUTPUT, UPDAT, INOUT, or OUTIN Data Set Activity	output
17	Scratch Data Set Status	delete
…	…	…

- DB2_ACCESS newlist for DB2 GRANT and external security analysis
  - 1 observation for each GRANT, PERMIT

Availability

- zSecure version 2.3.1 is Generally Available on September 14, 2018
- Supports z/OS 2.1 – 2.3

We want your feedback!

- Please submit your feedback online at ….
  - http://conferences.gse.org.uk/2018/feedback/nn

- Paper feedback forms are also available from the Chair person

- This session is FK